AiMT

Advances in Military Technology
Vol. 15, No. 1, 2020, pp. 25-42
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01334

Systems Integration in Military Environment

L. Buřita[1*], J. Hrabovský[2], A. Novák[2] and P. Pohanka[2]

[1] *University of Defence in Brno, Czech Republic*
[2] *URC Systems, Brno, Czech Republic*

The manuscript was received on 19 June 2019 and was accepted
after revision for publication as technical information on 21 December 2019.

Abstract:

The article highlights the major concepts of systems integration in a military environment, especially the NATO Network Enabled Capability and Federal Mission Networking. Both concepts were implemented into the Czech Armed Forces and adapted to fit their ambitions, possibilities, tasks and specific goals. The primary goal of this adoption was to achieve the capabilities to work in a coalition environment. The experiences from Intelligence, Surveillance, and Reconnaissance integration projects are presented in the second part of the article. After assessing the current state, development goals are characterized as challenges that need to be addressed with a solution that is described.

Keywords:

communication, data, FMN, interoperability, ISR, NNEC, standard, systems integration

1. Introduction

Systems integration in a military environment is a complex and complicated task. Its main goal is to achieve interoperability amongst the NATO allies and to work, exercise, and fight together without limitations. Significant integration concepts, NATO Network Enabled Capability (NNEC) and Federal Mission Networking (FMN), are described in Chapters 2 and 4. Chapter 3 contains a Czech contribution to both concepts.

The specific approach to system, technical and technological integration issues is discussed in Chapter 5 as regards Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR). The current state of activities is characterized, and further development is indicated. Joint Intelligence, Surveillance, and Reconnaissance (JISR) are defined, according to alliance documents as follows: "*The synchronization and integration of operations and intelligence capabilities and activities, geared towards providing timely information to support decisions. The 'JISR Process Cycle' is a combined intelligence and operations function, requiring extensive cross-Community of Interest (COI) coordination and interoperability at many levels. NATO JISR integrates*

[*] *Corresponding author: Department of Informatics, Cyber Security, and Robotics; University of Defence in Brno, Kounicova 65, CZ-662 10 Brno, Czech Republic. Phone: +420 973 44 21 72, fax: +420 973 44 23 37, E-mail: ladislav.burita@unob.cz*

alliance and national Intelligence, Surveillance and Reconnaissance (ISR) capabilities, policies, procedures and systems to provide information support to leaders, commanders and decision makers through political and strategic domains down to the tactical level." [1].

In Chapter 6, the ISR system integration challenges relating to data formats, transport protocols, application protocols, and information exchange mechanisms are described. The practical experiences of the URC Systems for the Czech Armed Forces (CAF) projects are also presented.

2. Network Enabled Capability

"*The Network Enabled Capability (NEC) is a new art of military operations and combat in the information age. It is the response to current and future challenges of the information age in the military field. From a broader perspective, NEC describes a combination of strategies, modern tactics, methods, and procedures that can be applied in networked military forces to achieve superiority over the enemy. In links sensors, command points, and combat systems operate in a collaborative environment. The NEC must ensure the exchange of information, utilizing communication networks which are interoperable and robust. These networks should also support the collection, fusion, analysis and distribution of information*." [2] (Fig. 1).

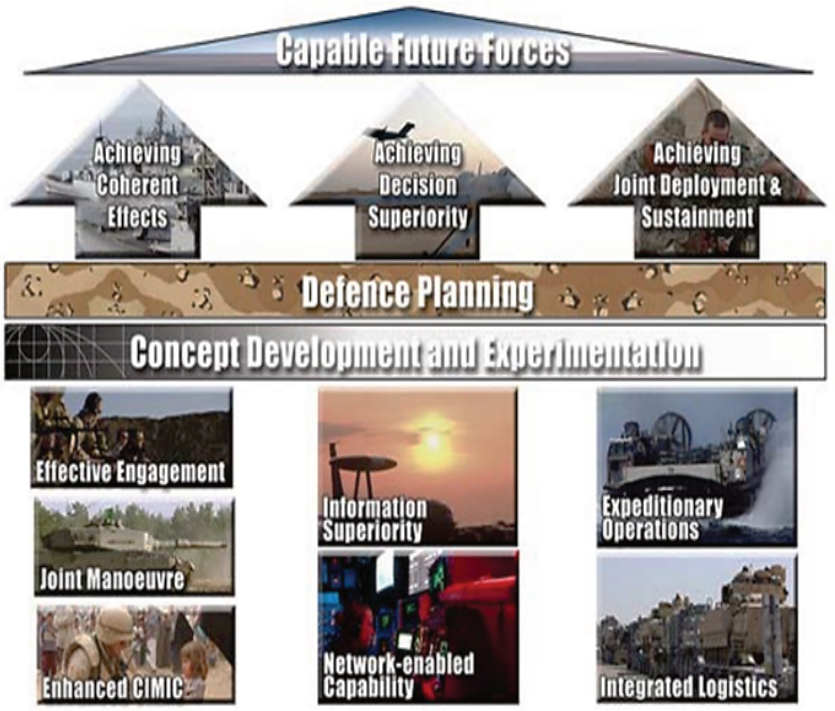

Fig. 1 Concept and goals of the Network Enabled Capability [2]

NNEC is concerned with increased flexible integration of command posts and decision centers, sensors and sensor-systems, shooters, weapon and support systems in a network, to ensure effective operations. NNEC relies heavily upon the state-of-the-art

Communication and Information System (CIS) technology. Success will depend on the ability to adopt and leverage the capabilities provided by technology. A transformation strategy that anticipates technology rather than waits for technology to become available is necessary. However, NNEC as a concept is far more than just CIS.

"*The focus on networks is highlighted in the first tenet, pointing to the need for a 'robustly networked force' to enable improved information sharing. The size, scope and reach of the network(s) required are determined by the missions, force structures and concepts of operations involved. The focus on information points to the need to exploit robust networking capabilities to improve information sharing; to enhance the quality of information shared, collaboration, and shared situational awareness. The focus on people and the benefits of working together in a networked environment is highlighted in portions of the third and fourth tenets. These highlight the role of improved information sharing and shared situational awareness in allowing people to work together in new more effective ways and thereby to improve speed of command, leading to dramatic increases in mission effectiveness.*" [2] (Fig. 2).

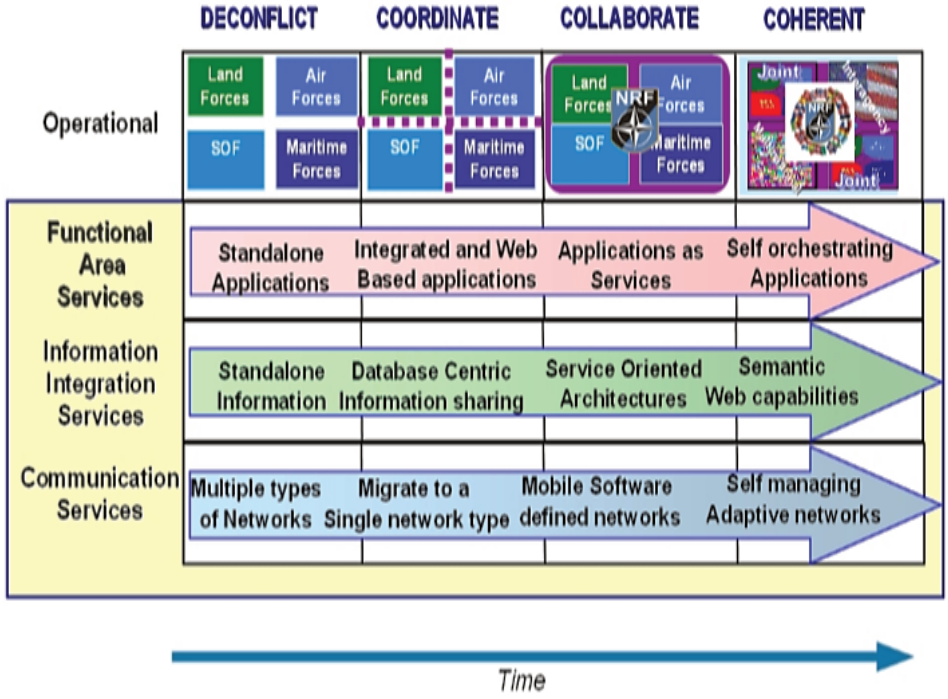

Fig. 2 Roadmap of the implementing NNEC [2]

3. Network Enabled Capability in the CAF

The Czech national strategy of building the NEC has been understood from the outset in its complexity not only as a contribution of the Czech Republic to increasing its army capabilities, but also as a fulfilment of its commitment to NATO and its allies. The basic document was the Strategy of the NEC development of the CAF, which was accepted at the Ministry of Defense Board in October 2007 with the following conclusions [3]:

- NEC is one of the basic conditions needed to achieve the operational capabilities of the CAF,
- the implementation of the NEC integration projects confirms the plan of the solution,
- the management structures of the NEC CAF were established,
- each armament project must be integrated into the NEC.

A set of ambitions was specified:

- availability of information,
- creating Community of Interest in NEC program,
- build a dynamic information environment,
- shared knowledge and understanding of the operational situation,
- credibility and cooperation,
- staff ready to implement NEC.

Tasks for building an integrated NEC environment were carried out through defense research and development projects and follow-up acquisitions to integrate sensors and weapon systems. The realization of these projects was one of the greatest achievements of the NEC CAF creation and was successfully finished by companies Delinfo, VTULaPVO, PRAMACOM–HT, ERA, RETIA, URC, VVU, TTC Telekomunikace, and Tieto Enator.

In the area of IS, the core of the integrated environment of the NEC of the CAF became The Operational and Tactical System of Command and Control of the Ground Forces (OTS VR PozS) with its two components: Staff Command and Control Information System (C2IS) and Battle Management Vehicular (BMV) IS. To ensure interoperability under the Multilateral Interoperability Program (MIP), two mechanisms of information exchange through the MIP communication interface (MCI) were used: the Message Exchange Mechanism (MEM) and the Data Exchange Mechanism (DEM). The MEM provides the data-push needed for database exchange (replication of database content) in the MIP environment.

While still valid, the NNEC concept has been vastly overtaken by the FMN framework for the last five years. A new strategy of the CAF was proposed for building NNEC in 2010. Several NNEC projects were terminated; funds were reallocated into new projects, more connected with FMN goals [4].

4. Federated Mission Networking

"*Federated Mission Networking is a capability aiming to support command and control and decision-making in future operations through improved information-sharing. It provides the agility, flexibility and scalability needed to manage the emerging requirements of any mission environment in future NATO operations. Federated Mission Networking is based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities.*" [5].

FMN is an effective means to enable sharing of information in a coalition environment. Coalition crisis response operations may range from support to disaster relief and humanitarian assistance, enforcement of sanctions and embargoes to counter terrorism, peace enforcement and military defense. Crisis response capabilities and forces must be rapidly available and sustainable. As a result, capabilities which enable crisis response must be agile, and interoperable in military interaction with non-military entities.

"*The FMN framework is a governed, managed, all-inclusive structure providing a permanent ongoing foundation with processes, plans, templates, enterprise architectures, capability components and tools needed to prepare (including planning), develop, deploy, operate, evolve and terminate mission. Mission Networks are established using a flexible and tailored set of non-material (i.e. policy, processes, procedures and standards) and material (i.e. static and deployed networks, services, supporting infrastructures) contributions provided by NATO, NATO and non-NATO nations and entities*." [5].

The goal of introducing the FMN concept into the CAF is to ensure the capabilities of the commanders and command staff to work in the coalition network and to provide them the common operational picture of the battlefield situation. The result will be a lasting, standardized solution that will link alliance partners at military missions and enable them to plan and manage operations jointly.

5. Integration Projects in the ISTAR CAF Environment

There are ongoing programs and projects in the CAF to fulfill Intelligence, Surveillance, and Reconnaissance (ISR) capabilities towards fulfilling ambitions to develop systems fully compliant with the Information and Communication Technologies (ICT) environment of the CAF and NATO to support ISTAR environment.

5.1. The Current State of the ISR Implementation

The key research and development project of the ISR implementation in the CAF was ISWM C4ISTAR (Integration Software Module for C4ISTAR). The project was active during 2014-2017. Development of the project was finished by the deployment to the CAF environment during 2017. The solution was designed for, but not limited to, ISR headquarters (HQ) on brigade, battalion and company level.

The developed SW tools consist of the application and integration layers. The application layer covers operational requirements of the ISR process on ISR HQ and tactical intelligence cycle in the unit level. The ISWM C4ISTAR is fully compliant with the Czech BMS C2IS (Command and Control IS). For the data and information exchange between ISWM C4ISTAR and C2IS, the following standard-based data formats are used: APP-11 for textual messages and NATO Vector Graphics (NVG) for operational pictures, common textual messages including attachments as images, PDFs, office documents, etc. All the mentioned data are exchanged online between both systems. The application layer of ISWM C4ISTAR is based on a multi-layer architecture, and its functionality is exposed as web services for easy integration with any other system.

The integration layer serves as an integration middleware with the functionality of Sensor Service Bus (SSB). The purpose is to provide reliable online data transmission both on LAN and non-reliable radio networks with limited bandwidth. Standard-based technology, Data Distribution Service (DDS), is employed to meet these requirements. The middleware is designed to integrate ISR HQ with both direct subordinate units and sensor platform, as well as coordinating units. The integration layer can also be used on the platoon level or for a dismounted soldier. Several approaches were used to integrate assets and other information systems into the ISTAR CAF environment:

- passive radio surveillance mobile complexes are integrated directly,

- passive radar surveillance systems (e.g. SDD, VERA,) are integrated indirectly via Cooperative ESM Operations (CESMO) by the employment of SW module "ISR Client",
- passive radar surveillance systems (e.g. SDD, VERA,) are coordinated via CESMO Fusion Cell (CFC)/Signal Identity Authority Cell (SIAC), which is a successor of ISR Client,
- applications for combat intelligence support (part of BMS C2IS) are integrated via online exchange of APP-11 messages and NVG operational pictures,
- integration of imagery assets MBK, UAV RAVEN, LOV-Pz-Del (artillery reconnaissance system) is based on the exchange (both online and offline) of imagery files.

The selected sensors of land forces were integrated during the first stage of the implementation of the ISR process support. Those sensors produce both standardized and proprietary sensor data, information and ISR products. The integration and application layers of ISWM C4ISTAR enable the transformation of data and information to the standard-based ISR products compliant to STANAG 4559 NATO Standard ISR Library Interface (NSILI). The main goal of STANAG 4559 NSILI is [6] "To promote interoperability for the exchange of NATO ISR product". To fulfill this goal, STANAG 4559 NSILI defines use cases, informational architecture, and the format of ISR products, its metadata and services to query and publish ISR products.

ISWM C4ISTAR interoperability in the coalition environment was tested on several events, such as the Coalition Warrior Interoperability exploration, experimentation, examination, exercise (CWIX) 2017 and 2018 and the main NATO ISR trial, Unified Vision 2018. Those tests were focused, but not limited, on NSILI integration, as well as on BMS interoperability, NVG exchange, APP-11 messages exchange, the consummation of geographic and meteorological services, imagery data sharing etc. Practical experience and recommendations for the ISR systems interoperability mentioned in the following sections are based on the experience from those events. The output of the ISWM C4ISTAR project is available not only for the CAF, but also to other customers as an application ISRMAN – ISR Management.

5.2. Further Development of ISR Capabilities

The ISR implementation in the CAF should continue, and the following projects should be established. Some features should be improved based on the previous experience. Some new functionalities need to be delivered, e.g.:

- full support of standard-based intelligence cycle and ISR process,
- implementation of the key ISR standards, especially STANAG 4559 NSILI, edition 4,
- replacement of combat intelligence support (part of BMS C2IS). Based on the experience, this support should be part of the ISR (combat intelligence) information system rather than BMS,
- integration of sensors and combat intelligence branches like tactical OSINT, HUMINT and MASINT.

To fulfill those requirements, processes, data models and interfaces defined in several allied publications must be implemented. These standards cannot be implemented as defined in the environment of the CAF; they should be adopted to possibilities of the

CAF – its ambitious, capabilities, organizational structures and available sensors. However, the goal is to utilize the standards maximally to be ready to integrate the national ISR systems into the coalition environment. These standards comprise:

- AJP 2.1 – Allied Joint Doctrine for Intelligence Procedures,
- AJP 2.7 – Allied Joint Doctrine for Reconnaissance and Surveillance,
- AIntP-14 – JISR Procedures in Support of NATO Operations,
- AIntP-16 – Intelligence Requirement Management & Collection Management,
- AEDP-05 – NATO Standard ISR Library Interfaces and Services – Business Rules and Use Cases,
- AEDP-17 – NATO Standard ISR Library Interface,
- AEDP-18 – NATO Standard ISR Streaming Services,
- AEDP-19 – NATO Standard ISR Workflow Architecture.

To ensure the interoperability of the ISR system within FMN environment, all relevant instructions and recommendations must be satisfied. There are two documents relevant to the ISR area in FMN Spiral 2, "Service Instructions for Coalition Shared Database" (Coalition Shared Database is the former name for NSILI) and "Procedural Instruction for JISR Reporting". Moreover, FMN instructions are relevant for the other aspects of interoperable ISR IS implementation as they also cover [5]:

- procedural instructions for CIS Security, Distributed Collaboration, Information Management, Recognized Environmental Picture, Service Management and Control, Situational Awareness,
- service instructions for Audio and Video-based Collaboration, Communications, Data Links, Digital Certificates, Directory Data Synchronization, Distributed Time, Domain Naming, Friendly Force Tracking, Geospatial Information, Informal Messaging, Joint C3 Information Exchange, Recognized Maritime Picture, Service Management and Control, Text-based Collaboration, Web Authentication, Web Hosting.

6. ISR System Integration Challenges

The key concept for ICT system integration is interoperability. It is "The ability to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objectives" [6]. In the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) Volume 1: Architecture descriptions, four degrees of interoperability are defined:

- "*degree 1: Unstructured Data Exchange (DE). Involves the exchange of human-interpretable unstructured data such as the free text found in operational estimates, analysis and papers,*
- *degree 2: Structured DE. Involves the exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch,*
- *degree 3: Seamless Sharing of Data. Involves the automated sharing of data amongst systems based on a common exchange model,*
- *degree 4: Seamless Sharing of Information. An extension of degree 3 to the universal interpretation of information through data processing based on cooperating applications*." [7].

NC3TA Reference Model for Interoperability (NMI) uses Levels of Conceptual Interoperability Model (LCIM) and defines seven levels of conceptual interoperability:

- *level 0: Stand-alone systems have No Interoperability,*
- *level 1: The Technical Interoperability: A communication protocol exists for exchanging data between participating systems,*
- *level 2: The Syntactic Interoperability: a common data format is applied,*
- *level 3: The Semantic Interoperability: the meaning of the data is shared,*
- *level 4: The Pragmatic Interoperability: the interoperating systems are aware of the methods and procedures that each system is employing,*
- *level 5: The Dynamic Interoperability: the state of the system will change as it operates on data over the time, and this includes the assumptions and constraints that affect its data interchange,*
- *level 6: The Conceptual Interoperability: the assumptions and constraints of the meaningful abstraction of reality are aligned."* [8].

In the article, we are focusing on levels 1 to 3 in the conceptual interoperability model. Levels 1 and 2 are essential to achieve at least an ability to integrate systems. There are many standards in a military environment which are focused on data formats only, but they address neither the transport protocol, nor the mechanism of exchange (for example APP11 messages or imagery data formats discussed further).

6.1. Data Formats

The data format defines the logical and physical structure of data being transferred. There are many data formats which can be binary or text-oriented. Structure or position can define the meaning of each element. Different separators can be used to separate individual values. Each data format must define its structure and data elements, headers, mandatory data elements, the format of the data elements, allowed values of the data values, rules and relations among data elements, separators, control sequences, etc. to achieve syntactic interoperability.

The meaning of data elements like bits, bytes, textual elements, etc. must also be defined to achieve semantic interoperability. To illustrate the variability of data formats, we list some examples – JPEG File Interchange Format (JFIF), Extensible Markup Language (XML) and comma-separated values (CSV) file:

- JFIF is an image file format standard for exchanging JPEG encoded files. A JFIF file consists of a sequence of markers or marker segments such as Start of Image, APP0 marker, additional marker segments, Start of Scan and End of Image [9]. JFIF is an example of a byte-oriented data format,
- XML is [10] a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is a textual data format,
- CSV file [11] is a delimited text that uses a comma to separate values. A CSV file store tabular data (numbers and text) in plain text. Each line of the file is a data record. Each record consists of one or more fields, separated by commas.

Data formats can be common or domain specific. In the next chapters we will focus on data formats specific for military and especially for ISR applications.

6.1.1. Common Military Data Formats

A lot of data standards are applied in a military environment. They include both common military and ISR specific ones. Enterprise common data formats like PDF, Office formats, images, video etc. are also used in the military environment, but it is challenging

to employ them into automated data processing. To encourage data and metadata harmonization within NATO allies, NATO Core Data Framework [12] was established. Its purpose is to provide the context and guidance for the use of standardized syntactic specifications in data exchange.

Common military data formats include for example APP-11 messages, NVG for operational pictures, NFFI/FFT for blue force tracking etc. These formats are well known in the military environment, and they are already implemented and adapted in the CAF. The implementation has been confirmed on many events (experiments, trial, etc.). Some of the standards (NVG, NFFI) cover not only data formats, but also transport protocol and mechanism of exchange.

APP-11 [13] specifies the Message Text Formats (MTFs) (also called character-oriented messages) used in NATO operations and exercises to exchange structured textual information between allied forces. Many NATO messages are also used to exchange information nationally. The messages are built on the underlying technical standard ADatP-3 which specifies the rules that govern the construction of the messages. The latest version of the APP-11 catalogue consists of over 400 messages covering every aspect of NATO operation that can be exchanged using the latest XML technology or slash-separated messages.

The **NATO Vector Graphic** (NVG) is used for [14] encoding and sharing operational pictures and tactical plots which consists of battle-space information, represented by military symbology, for overlay on a geographic display. NVG consists of a data format for the encoding of battlespace objects into overlays and protocol for the automated exchange of the overlays. NVG is XML based format, the elements of NVG are represented by its type (point, line, arrow, etc.), label, position and symbol code. The symbol code uniquely defines associated graphic symbol from APP-6 symbology. The code is an alphanumerical sequence (e.g. SFGPUCR---EF***) where each character (or characters subsequence) symbolizes [15] the unit identity, Dimension, Status, Function, Size of the Unit and additional information.

NATO Friendly Forces **Indicator (NFFI) and Friendly Force Tracking (FFT)** is [16] the capability to monitor the precise location and identification of friendly forces in NATO-led operations in near-real time, and to exercise Command and Control (C2) on these forces, as required. FFT, Blue Force Tracker (BFT) and Force Tracker (FT) are deployed land-force sensors that track unit position and automatically report unit position and status information to the chain of command in near real-time. NATO Friendly Force Information (NFFI) and Friendly Force Information Message Text Format (FFI MTF) are two XML based message formats that support FFT of ground tracks in NATO.

6.1.2. ISR Specific Data Formats

The set of ISR standards is maintained by STANREC 4777 Ed. 2 – NATO ISR Interoperability Architecture (NIIA) [17]. Its implementation guidance, AEDP-02 NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) lists about 25 key ISR standards. We mention only the ones which are the most significant for the CAF and with which we have had practical experience:

- **STANAG 4545 – NATO Secondary Imagery Format (NSIF)** provides implementation guidance that is designed for the distribution, storage, and interchange of secondary imagery products (not designed for downloading raw products from a primary sensor),

- **STANAG 4559 – NATO Standard ISR Library Interfaces (NSILI)** promotes interoperability of NATO ISR library interfaces and services for the exchange of shared ISR data, products and schemas,
- **STANAG 4609 – NATO Digital Motion Imagery Standard (NDMIS)** provides guidance for consistent implementation of Motion Imagery Standards to achieve interoperability in both the communication and functional use of Motion Imagery Data. STANAG 4609 documents the structure for data, which includes formats, encodings and containers, and the content of data, which includes common and application-specific information that populates these structures,
- **STANAG 4658 – Cooperative Electronic Support Measure Operations (CESMO)** exists to enable the warfighter to rapidly share and receive Electromagnetic Spectrum (EMS) threat information. The use of the EMS by modern systems such as Integrated Air Defense Systems (IADS), Low Probability of Intercept (LPI) radars, and digitally modulated communications systems poses a steadily increasing threat to today's warfighters,
- **STANAG 5516 – Tactical Data Exchange – Link 16** provides guidelines on how to ensure interoperable use of Link 16 Tactical Data Links (TDLs) to disseminate information. Link 16 employs the Joint Tactical Information Distribution System (JTIDS) and Multifunctional Information Distribution System (MIDS) data link terminals.

6.1.3. Data Formats Mapping and Metadata Harmonization

The already mentioned standards are intended for specific intelligence branch or even specific scenario or use-case. Because of this variety, those standards are not always harmonized or even compatible. For example, basic intelligence reports, intelligence summary (INTSUM) and intelligence report (INTREP) are defined both in APP11 messages catalogue and in STANAG 4559 NSILI. They both are completely different, as they are intended for different use cases. Basic rules for high-level metadata harmonization are part of NIAA [17], the example is shown in the Tab. 1.

Even with those rules set, there is a lot of low-level and implementation issues which must be solved on the implementation level, e.g.:

- the different logical and physical structure of byte-oriented imagery metadata according to STANAG 4545 NSIF are mapped to XML elements in STANAG 4559 NSILI metadata,
- the list of countries is defined in STANAG 1059, but NSILI also uses IW code for International Water,
- the security classification differs in EOB definition and NSILI. NSILI is missing COSMIC TOP SECRET for example.

To generalize these issues: textual values have been mapped to the list of values, so mapping must handle values which are not in the list of values; typos must be resolved; some values of attributes need to be split or merged. The data types and even the length of attributes differ. Some attributes are mandatory in one data format and optional in another: numerical values are converted to textual and vice-versa etc.

6.2. Communication Interface

"*Communication or transport protocol is a system of rules that allow two or more entities of a communications system to transmit information. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery*

methods. Those rules are separated into abstract layers in the reference ISO model, which defines physical, data link, network, transport, session, and presentation and application layer." [18].

Many standardized protocols are used to exchange data over (IP) network like UDP and TCP/IP on the transport layer. On the application layer, HTTP including secured HTTPS version, web services in different flavors (SOAP services defined by WSDL, REST services with JSON content, simple XML over HTTP), CORBA, FTP, XMPP and other protocols are used. Specific military and ISR protocols are used as well especially for communication with sensors. They include Tactical Data Link (TDL) family of protocols, most significant of which is Link 16 both via hardware terminals or software emulation via JREAP-C, ISR Link STANAG 7885. The transport protocol is also defined in the CESMO network and other standards.

Variety of application protocols has an impact on the complexity of the network configuration, its security and interoperability. FMN defines required standards to be supported, both military and industry ones, in the FMN Standards Profile. For example, SOAP 1.1, WSDL 1.1, XML 1.0, Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding, Web Services Addressing 1.0 etc. are used for Web Services [19]. The actual trend is to utilize Web Services as a communication protocol as one uses XML based data formats and HTTP transport protocol. There are several reasons why Web Services have gained such a widespread adoption. In addition of the interoperability, there is the possibility to use XML labelling for security marking and Sensor Web adoption led by the MASINT Working Group.

Tab. 1 Example of metadata mapping [17]

ISR DSAR	IMWG					MWG		SEWWG
4559 ISR libraries	4545 NSIF/ NITF	4609 Motion Imagery	4607 GMTI	7023 NPIF	4676 NITS	4715 Biometrics	4716 MASINT REP	4658 CESMO
NSIL_METADATASECURITY.policy	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK – N/A]	[BLANK]
NSIL_METADATASECURITY.classification	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK – N/A]	[BLANK]
NSIL_METADATASECURITY.releasability	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK]	[BLANK – N/A]	[BLANK]
NSIL_SECURITY.policy	FSCLSY, ISCLSY, SSCLSY, TSCLSY [2]	Classifying Country [6]	Packet Security – Classification System (P5) [2]	Authority (A-4.2/3)	Security.security PolicyName	Source of Classification (BEI)	Message Security Policy (3-9)	[BLANK]
NSIL_SECURITY.classification	FSCLAS, ISCLAS, SSCLAS, TSCLAS [1]	Security Classification [14]	Packet Security – Classific	Mission Security Classification (A-4.2/1);	Security.security Classification	Classification (BEI)	Message Classification (3-10)	Message Header: Classification

In this article, we will mention only XML labelling, which is essential for communication between different security domains. The Information Exchange Gateway (IEG) concept is defined within NATO to facilitate [20] secure communication between different security and management domains. IEG consists of demilitarized zones (DMZ), firewalls and content guards including XML Guard. XML Guard allows only XML elements to go through with proper labelling. Mechanism of security marking is defined in ADatP-4774 Confidentiality Metadata Label Syntax for XML-based content, and the support of this mechanism is being integrated into other standards like STANAG 4559 NSILI. This approach makes communication protocols which are not XML/HTTP based like CORBA obsolete.

Exchange mechanism defines how the data are exchanged and the workflow of the exchange, which is not defined in most of the ISR standards. For example, STANAG 4545 NSIF or APP11 messages define the data format, but they do not prescribe how those data are handled or how they are physically stored. Imagery data, textual messages and other data can be transferred by various communication interfaces such as email, FTP, XMPP and others, but there are no detailed rules defined in the relevant STANAGs for information exchange among multiple systems. For example, the relevant imagery standards define an exchange mechanism between UAV and the ground station, but the dissemination from the ground station to other consumers is not standardized.

On the other hand, AEDP-17 defines use-cases and scenarios for ISR products publishing and/or querying, NVG defines web services and operations for capabilities manipulation which can be seen as a definition of exchange mechanism. NFFI, CESMO and TDL also define specific communication interface. Thus, multiple communication interfaces have to be implemented within a system.

6.3. FMN and Interoperability

Implementation of FMN is divided into a time-boxed spiral. Each spiral specifies a set of capabilities and functionalities to be implemented in the given time. For each FMN functionality area, for example, web services, both industry and military ones, are prescribed as a set of standards to be implemented and supported. For the ISR, the most relevant documents are FMN Spiral 2 Procedural Instructions for JISR Reporting and FMN Spiral 2 Service Instructions for Coalition Shared Database. Those instructions are linked to the other service instructions such as Communications Services, Distributed Time Services, and Domain Name Services etc.

6.4. Practical Experience with ISR System Integration

Practical experience with ISR systems integration has been gained on several national and international trials and experiments including CWIX 2017, CWIX 2018, UV 14, UV 16 and UV 18. Those experiences show that we are challenging a lot of issues like the integration of non-standard and legacy systems, a variety of standards and its versions, security-related issues, different level of maturity of individual standards, dependencies among standards, and different level of their implementation among allies and specific situation of the CAF. Most of those issues are discussed in the next chapters.

6.4.1. Integration of Non-Standard and Legacy Systems

Integration of non-standard and legacy systems is a very difficult task, and in some cases, it is impossible – e.g. legacy system without support by a vendor. The concept of SOA, ESB, SSB and adapters can allow and simplify the integration of the legacy and

non-standard system. Those concepts are applicable and they can help to solve even other mentioned issues.

6.4.2. Variety of Standards and its Versions

There can be issues with interoperability even in cases where standards for interoperability are followed and implemented. Each system can implement a different version of the standard. Vendor or nations can also implement non-compliant improvement of the standard. Those improvements might be embedded into a further version of the standard but with some modification during the standardization procedure so already implemented information system (IS) might remain non-compliant.

The acquisition process in a military environment is a long-term process due to the need for operational tests, certifications etc. Thus it is difficult to upgrade IS easily by "only" following the latest version of the standard because the upgrade can affect an operational area. On the other hand, each standard also has a long-term promulgation period which leads vendors to implement proprietary or not yet standardized version because of operational needs. Usually there are multiple versions of the standard in use at the same time – for example, following versions of standards are used in parallel: NVG 1.4, 1.5 and 2.0, APP-11 baseline 12, 14 and 15, NSILI edition 3 and edition 4, CESMO (v5, X1, B1), APP6 B, C, D, etc. As mentioned earlier, FMN Spirals and NIAA prescribe standards and their versions which should be used but the usage is not enforceable.

Long-term periods of acquisition and promulgation can be illustrated as a cause of interoperability issues, based on the example of supported versions of the STANAG 4559 NSILI in the Alliance Ground Surveillance (AGS) System. AGS support STANAG 4559 NSILI Edition 3 with CORBA interface only because in the time of AGS design this version was actual. The focus of the AGS is not on STANAG 4559 NSILI but on aerial surveillance itself. Thus, compatibility with NSILI edition 4 is not the priority. In settings where the implementation of STANAG 4559 NSILI started later according to edition 4 (like the CAF) and needs to be interoperable with AGS, both Web Service and CORBA interfaces should be implemented, even though the CORBA support becomes obsolete in the future version of the STANAG 4559 NSILI. Actually, the CAF decided to implement only the Web Service interface and postpone CORBA interface implementation.

It seems that the implementation of standards and versions mentioned in the actual version of NIAA could solve the issue of a variety of standards and its version. That would be possible only if all nations follow this approach, which is not a realistic assumption. Hence, there is a need to identify potential partners for the implementation of the interoperable solution and then to discuss the standards and versions which will be implemented or adapted on both sides. In some cases, the decision of interoperable integration is not done successfully.

Anyway, efforts should be focused to implement actual NIAA recommended standards and standards commonly used in the ISR community. Moreover, it is useful to participate in relevant working groups to gather actual information about used standards and ongoing standardization work and participate in standardization and ratification process itself. The best way to test interoperable solution is participation in allied experiments like CWIX and tests like UV. Within ISR community, participants are

encouraged to execute bi-directional VPN-based tests. There is also testing infrastructure as a legacy of MAJIIC program, which can be reactivated, and Germany is preparing its own STANAG 4559 NSILI certification and testing infrastructure in 2020.

This issue is addressed in NIAA where the concept of backward compatibility is defined. Backward compatibility is the process of ensuring that systems using different editions of a standard can still work well together. A standard that is backward compatible is interoperable with older versions of itself.

6.4.3. Different Maturity Levels of Individual Intelligence Branches

The maturity level of standards and implementation of individual intelligences branches differ. For example, imagery standards, as well as NSILI, are in operational use; CESMO is being tested on trials; AGS is under development. On the other hand, some standards for OSINT or MASINT are not so mature: they are in specification or ratification process yet. As a result, relevant sensors are either not integrated or they are not integrated in a proprietary way.

6.4.4. Dependencies among Standards

Another issue is a dependency between some standards, which means that a specific version of one standard is referenced or linked to a specific version of another standard. For example, metadata of video sequences in STANAG 4559 NSILI are linked with STANAG 4609 edition 3. Thus, it is hard to process any other version of STANAG 4609-compliant data. Moreover, the change (upgrade) of one standard requires an upgrade to another standard which is a complex task as those standards can be maintained by different working groups and used for different use-cases and scenarios.

The solution is to design standards independent of any other specific standard or design common ISR metadata model which would cover all intelligence branches with the focus of metadata harmonization. The ontology and semantic technologies should be used for this kind of a task because the hard-coded mapping of individual attributes only moves the dependency and linkage to the next level. The ontology and semantic technologies enable mapping based on the meaning of the attributes, so it is a much more flexible solution.

6.4.5. The Specific Situation of the CAF

There are several specifics related to ISR implementation and integration in the environment of the CAF. Some intelligence branches are not developed. The implementation is in the beginning, for example acoustic intelligence (ACINT) and some intelligence branches like MASINT, OSINT, and HUMINT, are not fully integrated to the C4ISTAR environment of the CAF.

On the other hand, IMINT and especially EW are well developed in the CAF. The CAF is a very strong player in the CESMO community. The maturity in CESMO implementation, however, can lead to a paradox situation where the CAF misses integration partners. With regard to imagery intelligence, UAV RAVEN and UAV Scan Eagle support standard imagery products such as STANAG 4545 NSIF and STANAG 4609 so they can be integrated into C4ISTAR environment. However, additional development is needed to process those standard-based data and information in the C4ISTAR environment of the CAF. Other imagery sensors, such as MBK or LOV-Pz-Del etc. produce non-standard images (non-standard in the context of ISR interoperability, images itself are standard-based JPG) which can be enriched with relevant metadata – technical

parameters can be obtained from EXIF information, other metadata can be added by IS of a given platform.

Not all sensors of the CAF are already integrated into the C4ISTAR environment: some of them are unable to integrate due to technology or legal reasons. When a new sensor is acquired or an existing one is upgraded, it should be integrated into the C4ISTAR environment. Some ISR interoperability and/or integration standards are a low priority for the ACF, for example, maritime standards like OTH-G.

6.5. Tactical Radio Networks

In the military environment, it is nowadays essential to share data among nodes in operation. Sharing data in a military environment is also affected with aspects such as limited bandwidth (high latency, low speed) and general degradation of communications (packet loss), real-time or near-real-time requirements, and operations in a hostile environment with risks such as EW/SIGINT interception and jamming. Those aspects should be covered on operational, communication and security level. From the perspective of our article, relevant communications standards are STANAG 5066 – Profile for HF Radio Data Communications, STANAG 4406 – Military Message Handling System (MMHS), family of tactical data links, especially STANAG 5516 – Tactical Data Exchange – Link 16, STANAG 7085 – Interoperable Data Links for ISR Systems, STANAG 4660 – NATO Interoperable Command and Control Data Link and others. All of these aspects are also partially covered by CESMO network (STANAG 4658 – Cooperative Electronic Support Measure Operations), STANAG 7023 – NATO Primary Imagery Format and other standards specific to individual intelligence branch. Nevertheless, parts of the standard or standards related to the communication and security are in many cases classified, so these aspects are out of the scope of this article.

We have developed and used software component – communication adapter for effective and reliable communication to support the mentioned aspects of military communication. This component is based on the Data Distribution Service (DDS) which uses the publish/subscribe communication model and is the only standard-based protocol for UDP. DDS uses multicast, which is more suitable for unreliable communication links with limited bandwidth and high latencies when sending data to multiple locations. The essential feature of DDS is the automatic discovery of participants, which greatly simplify the network configuration on a software level, and support for QoS. Other features are strong type definition that eases integration and also provides type extensibility to support backward and forward compatibility that enables a system to evolve. The principle of the communication adapter is to intercept all inner-node communication routed outside of the node and send it efficiently and reliably on physical radio link to different node or nodes. Communication adapter on the receiver node receives data and sends them to applications within that node. Communication adapter can route data, prioritize messages, resume unfinished transfers, track message transfer and cancel transferring messages. Due to the auto-discovery feature, it supports Plug&Play nodes registration and node configuration through multicast.

One can encounter problems with networks if they cannot use multicast or if a part of the network does not support multicast. In that case, we faced problems with the configuration of the network components and ineffective data transfer. For that reason, we consider more efficient network resource alternative to DDS which is DDS-XRCE (Extremely Resource Constrained Environment) along with software gateways that allow proper routing between network segments with different network configuration.

The conclusion is that the usage of DDS on radio links is feasible with the proper configuration of its parameters and QoS settings. Integrators should be aware of problems with more complex configurations within networks without multicast. Also, the usage of DDS is limited to one security domain; the traffic will not be accepted by the IEG as it is not HTTPS and XML based. DDS-XRCE is a very promising initiative for constrained environments.

7. Conclusions

To conclude the article, we summarize the lessons learned on several international ISR system integration events and recommend guidance to make integration of ISR systems easier and more flexible. We strongly recommend to follow the allied publications, e.g. AJP 2, AJP 2.7, AIntP-14 and AIntP-16. Unfortunately, it is not possible to fully implement all the standards. The standards must be adopted to the possibilities of the CAF: its ambitions, capabilities, organizational structures and available sensors. However, the goal is to utilize standards maximally to integrate the national ISR systems into the coalition environment.

Final recommendations:

- to ensure the interoperability of the ISR system within an allied environment, FMN procedural and service instructions as well as NIAA recommended standards and its version should be implemented,
- the concept of SOA, ESB, SSB and adapters architecture can allow and simplify integration of the legacy and non-standard systems,
- participation in working groups to gather actual information and to engage the standardization process,
- participation in experiments like CWIX and tests like UV, as well as participation on hackathons under TIDE to verify interoperability of the developed ISR system,
- ISR integration projects in the CAF should follow standards and recommendations based on experience,
- all ISR and ISR-like sensors should be implemented into a common and integrated C4ISTAR environment of the CAF compatible with NATO ISR environment, following FMN instructions,
- utilize VPN-based test with other vendors which is a cheaper and faster way of testing compared to official NATO experiments,
- build a testing environment and infrastructure as an enabler for rapid development and testing,
- use the technologies such as DDS for radio networks and utilize their strong self-discovery mechanism to make the configuration of the system easier.

Acknowledgement

The article presents the results of the research in the research project [21] and set of research and implementation projects of the Company URC Systems, Czech Republic for the CAF, but on the security grounds, it is not possible to include the relevant references.

References

[1] *Joint Intelligence, Surveillance and Reconnaissance* [on line]. NATO Communications and Information Agency. [viewed 2018-12-12]. Available from: https://www.ncia.nato.int/Our-Work/Pages/Joint-Intelligence-Surveillance-and-Reconnaissance.aspx

[2] BUCKMAN, T. *NATO Network Enabled Capability* [Feasibility Study] [on line]. Brussels: NATO, Consultation, Command and Control Agency, 2005. 29 p. [viewed 2018-12-14]. Available from: http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf

[3] *Building strategy of NEC in the Czech Armed Forces* (in Czech). Prague: Ministry of Defence CR, 2007, 214-20/2007/DP-1341.

[4] VANĚK, V. (ed.). *History of the Signal Troops 2007-2017* (in Czech). Prague: Ministry of Defence CR, VHÚ, 2017. 119 p. ISBN 978-80-7278-720-3.

[5] *Federated Missions Networking* [on line]. NATO: Allied Command Transformation. [viewed 2018-06-12]. Available from: http://www.act.nato.int/fmn

[6] NATO-AEDP-17:2018*, NATO Standard ISR Library Interface.*

[7] NATO-STANREC 4777:2018, *NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture.*

[8] TURNITSA, C.D. Extending the Levels of Conceptual Interoperability Model. In *Proceedings of the IEEE Summer Computer Simulation Conference*. IEEE CS Press, 2005.

[9] HAMILTON, E. *JPEG File Interchange Format,* 1992. 9 p. [on line]. [viewed 2019-04-14]. Available from: https://www.ijg.org/files/jfif3.pdf

[10] *Extensible Markup Language (XML) 1.0 (Fifth Edition)* [on line]. W3C Recommendation, 2008 [viewed 2019-04-14]. Available from: http://www.w3.org/TR/xml/

[11] *CSV, Comma Separated Values (RFC 4180*) [on line]. Sustainability of Digital Formats: Planning for Library of Congress Collections. [viewed 2019-04-14]. Available from: https://www.loc.gov/ preservation/digital/formats/fdd/fdd000323.shtml

[12] *Framework for Future Alliance Operations*. [on line]. [viewed 2019-10-10]. Available from: https://www.scribd.com/document/408763215/180514-ffao18-pdf

[13] *APP-11 and ADatP-3* [on line]. [viewed 2019-04-14]. Available from: https://systematic.com/defence/capabilities/c2/interoperability/app-11-and-adatp-3/

[14] ADatP-4733:2017*, NATO Vector Graphics (NVG) 2.0.2-ADatP-4733 Edition A Ver 1*, *NATO Standardization Office.*

[15] NATO joint military symbology APP-6(C). *NATO Standardization Agency* [on line]. 2011, 558 p. [viewed 2019-04-14]. Available from: https://www.awl.edu.pl/images/en/APP_6_C.pdf

[16] *Friendly Force Tracking,* US-Army Stand-To [on line]. 2016 [viewed 2019-04-16]. Available from: https://www.army.mil/standto/archive_2016-02-24

[17] NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA). *NATO Standardization Agency* [on line]. 2005, vol. 1, 33 p.

[viewed 2019-04-16]. Available from: https://www.uvsr.org/Documentatie%20UVS/Reglementari%20internationale/Alte%20documente/AEDP-02v1.pdf

[18] SAIFUDDIN A. Telecommunication Protocols [on line]. [cited 2019-04-20]. Available from: https://itstillworks.com/telecommunication-protocols-8509890.html

[19] WELLS E. *STANDARDS & PROFILES FOR COALITION INTEROPERABILITY* [on line]. [viewed 2019-04-20]. Available from: https://docplayer.net/48422285-Standards-profiles-for-coalition-interoperability.html

[20] *Information Exchange Gateways*. [on line]. [viewed 2019-10-10]. Available from: https://www.nexor.com/information-exchange-gateways/

[21] *Development of systems C4I and cyber security*, KYBERBEZ (DZRO K-209). Ministry of Defence of CR, Prague, 2016-2020.