OPEN
PUBLICATIONS

Interoperability and Standardization in the Exponential Age

Volume 9, Number 6, 2024

ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

DISCLAIMER:

OPEN publications are produced by Allied Command Transformation/Strategic Plans and Policy; however OPEN publications are not formal NATO documents and do not represent the official opinions or positions of NATO or individual nations. OPEN is an information and knowledge management network, focused on improving the understanding of complex issues, facilitating information sharing and enhancing situational awareness. OPEN products are based upon and link to open-source information from a wide variety of organizations, research centers and media sources. However, OPEN does not endorse and cannot guarantee the accuracy or objectivity of these sources. The intellectual property rights reside with NATO and absent specific permission OPEN publications cannot be sold or reproduced for commercial purposes. Neither NATO or any NATO command, organization, or agency, nor any person acting on their behalf may be held responsible for the use made of the information contained therein. The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations. All rights reserved by NATO Allied Command Transformation Open Perspectives Exchange Network (OPEN). The products and articles may not be copied, reproduced, distributed, or publically displayed without reference to OPEN.

Let us know your thoughts on
“Interoperability and Standardization in the Exponential Age”
by emailing us at: ***editor@openpublications.org***
www.openpublications.org

CREDITS

CONTRIBUTING AUTHOR
Dr Michael Gerz

OPEN CAPABILITY LEADER
COL Stefan Lindelauf

OPEN LEAD EDITOR
Dr Mehmet Kınacı

OPEN OPERATIONS MANAGER
LTC Alexios Antonopoulos

ACTION OFFICER
CAPT Dr. habil. Robert KOCH

OPEN EDITORIAL REVIEW BOARD
LTC Tor-Erik Hanssen
CDR Silvio Amizic
CDR Alban Morel
CDR Alan Cummings
LTC Dirk Mathes
LTC Mithat Almaz
Mr Helmar Storm
Ms Klodiana Thartori

TECHNICAL EDITOR
Dr. Maureen Archer

ART DESIGNER
PO1 Isabel Wences

CONTENTS

EXECUTIVE SUMMARY

As disruptive technologies reshape the battlespace, the increasing pace at which technology evolves makes it increasingly difficult to do medium- and long-term planning. A key factor for conducting missions successfully is interoperability across the participating partners. This is particularly challenging for a large organization such as NATO that is comprised of 32 member states, where each member has its own roadmap and procurement processes, and standardization is based on consensus. In this paper, we will consider interoperability and standardization, covering aspects such as strictness, extensibility, integration levels, and testing. Moreover, we will look at some new technological areas, in particular AI and quantum technology, and propose future interoperability activities. The paper shows how standardization within NATO can be improved to achieve future-proof interoperability standards, how interoperability can be improved and faster realized, and which new interoperability requirements imposed by disruptive technologies should be addressed in the future.

Keywords: Interoperability, Conformance, Standardization, Disruptive Technologies, AI, Quantum Cryptography

INTRODUCTION

We are in an exponential age, where technological progress is advancing in many areas at an increasingly rapid pace. Breakthroughs in the fields of big data analytics and artificial intelligence paved the way for automated processing of data, resulting in new ways to conduct military intelligence and accelerated decision-making processes. Quantum technology is already casting its shadows ahead, with major impact on, e.g., cryptography.

The speed at which technology evolves makes it increasingly difficult to do medium- and long-term planning. On the one hand, progress in specific technological areas is not linear. Artificial intelligence (AI) has been hibernating for many years – history has seen two AI winters[1] – until increased computing power, big data, and new algorithms allowed some AI applications to even outperform humans. On the other hand, the implications of new technologies on the battlefield are not yet fully understood. Not everything that is technically feasible may actually be operationally useful. New technologies do not only come along with new capabilities but also with new risks and vulnerabilities caused by their complexity. AI systems are susceptible to deception (counter-AI). The Internet of Things (IoT), in which computing devices embedded in everyday objects (such as a refrigerator) exchange data with other devices and systems, opens many new doors for cyber-attacks. In addition, the cyber domain and its social media allow for large-scale misinformation campaigns.

The term exponential age (Azhar, 2021) was created to describe our current period, in which innovations are developed at an ever-growing speed while we are not able to fully foresee their implications on society, economics, and the military. The gap between what is technically feasible and what is currently in use and well-understood causes uncertainty for decision makers.

Regarding the military world, disruptive technologies, i.e., innovations that significantly alter the way that we operate, will reshape the battlespace. For example, in Allen & Husain (2017), the authors sketched a Hyperwar scenario that is characterized by AI-controlled, autonomous systems. The high degree of automation and the intense use of unmanned vehicles suggest a dramatic increase in the speed of warfare, which makes it challenging to keep humans in the loop for decision-making.

Another term subsuming the latest trends in warfare is coined Multi-Domain Operations (MDO). NATO defines MDO as “the orchestration of military activities across all operational domains and environments, synchronized with non-military activities to enable the Alliance to create converging effects at the speed of relevance.” (NATO Standardization Office, 2023). Multi-domain operations are not a new phenomenon. In fact, joint operations, in which land, maritime, and air forces collaborate, have taken place for centuries. In addition, civil-military cooperation (CIMIC) has always been an integral aspect to achieve military objectives.

[1] *The first AI winter lasted from about 1974 to 1980; the second winter started about a decade later (1987–2000). Please note that the times vary greatly depending on the source.*

What is new is the cyber and information domain and the extended use of the space domain. The cyber domain poses new (hybrid) threats where the physical boundaries of a battlefield no longer apply. Cross-domain information exchange is a key enabler for MDO. It allows for cross-dimensional fusion of data coming from heterogeneous sources (e.g., satellite images, social media content, battlespace sensors, open data about critical infrastructures), all under a unified command and control. The extensive use of unmanned vehicles (especially drones and swarms of drones) and the application of AI significantly enhance reconnaissance capabilities, but it also increases the enemy's capabilities to attack behind the lines. All these new technological capabilities lead to a higher degree of automation and mandate shorter decision processes.

A key factor for conducting missions successfully is interoperability across the participating partners. Achieving and maintaining interoperability is particularly challenging for an organization such as NATO that is comprised of 32 member states, where each state has its own roadmap and procurement processes, and standardization is based on consensus among the stakeholders. In addition, doctrines, processes, and technical solutions in the land, air, and maritime forces are quite different, complicating interoperability in multi-domain operations. Thus, key questions are whether the current standardization processes are adequate to ensure the provision of assertive forces in the future and what measures need to be taken to maintain NATO's technological lead.

This paper provides the following added values for NATO: (1) It shows ways in which the standardization within NATO can be improved to achieve future-proof interoperability standards. (2) It explains how interoperability can be improved and be realized faster. (3) It highlights new interoperability requirements imposed by disruptive technologies.

The paper is structured as follows. In section 2, we introduce the basic concepts of interoperability and discuss aspects such as the strictness of standards, their extensibility for future capabilities, and support for different integration levels. Section 3 considers the standardization process and emphasizes the need for testing support. Interoperability needs emerging from new technologies are sketched in section 4. An overview of recommendations is given in section 5. Finally, the paper concludes with a summary in section 6.

INTEROPERABILITY CONCEPTS

Interoperability is “the ability of two or more systems or components to exchange information and to use the information exchanged” (Standards Coordinating Committee of the IEEE Computer Society, 1990). A later definition describes it as the “ability of a system or a product to work with other systems or products without special effort on the part of the customer. Interoperability is made possible by the implementation of standards”. (IEEE, 2016)

Both definitions from IEEE focus on the interaction of technical systems. However, the concept of interoperability can be extended to also cover human actors that exchange and use information to cooperate within the scope of a specific process. Accordingly, NATO defines interoperability as “the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.” (NATO Standardization Office, 2023) It also provides a more technically oriented definition: “The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units”. (NATO Standardization Office, 2023)

It is worth noting that whenever interoperability between systems is not achieved, humans must compensate for the deficiency. However, it may not always be obvious for the operators when their systems fail to interoperate, no matter whether by missing functionality or design/implementation errors. The lack of interoperability may cause unnoticed information loss or information falsification. This may happen in particular if information is shared between different domains or communities of interest (COIs) that use different standards based on the information exchange requirements for their specific doctrines and processes.

Interoperability can be achieved by supporting a commonly agreed upon standard. *Conformance* means a process, product, or service complies with the requirements of a given specification.

A critical aspect when developing systems is testing. *Conformance testing* is used to determine the extent to which an implementation conforms to its specification. Conformance tests may be done in-house by the vendor, by a customer, or by an independent third party (e.g., a certification authority). Conformance testing implies black box testing; that is, no information is given about the internal structure of the system under test.

Interoperability testing aims at ensuring that a system is able to work with another system. Active interoperability testing allows intervening in the communication between the participating systems to provoke specific errors and observe the resulting behaviour of the systems. In contrast to this, passive interoperability testing is restricted to monitoring end-to-end behaviour of systems.

2.1 Conformance vs. Interoperability

It is worth noting that successful conformance testing of a given number of systems does not necessarily ensure interoperability between them. First, testing of any kind can never be exhaustive for any system of reasonable complexity. Testing

can prove the existence of errors, but not their absence.

Second, many standards are quite comprehensive, and system developers may decide to support these standards only partially. For instance, APP-11 (NATO, 2015) defines a message catalogue with more than 400 different message formats. Depending on the intended use, systems developers may decide to support only a small fraction of them in their command and control information systems (C2IS). Such a tailoring also happens in Federated Mission Networking (FMN). But even if the stakeholders agreed on a fixed set of message formats, each message format has dozens of fields that may or may not be supported, leading to potential information loss. The same applies to other standards such as APP-6 (NATO, 2017) that defines a complex toolbox for depicting tactical symbols. The underlying core problem is optionality in standards. System developers (or the commissioning customers) may pick and choose parts as deemed appropriate. Consequently, the common intersection is not clearly defined.

Third, standards may offer multiple technical ways to achieve the same objective. For instance, a standard may allow subscribing to an information topic in different technical ways or supporting multiple ways to cluster information logically. Of course, alternatives should be avoided whenever possible, but practice proves the opposite. For the implementers, alternative approaches cause significant overhead, as all options must be considered in order to achieve interoperability with all standard-conforming systems.

2.2 Levels of Interoperability

Interoperability can be achieved on multiple levels. In the past, NATO has defined five levels of interoperability (see **Fig. 1**).

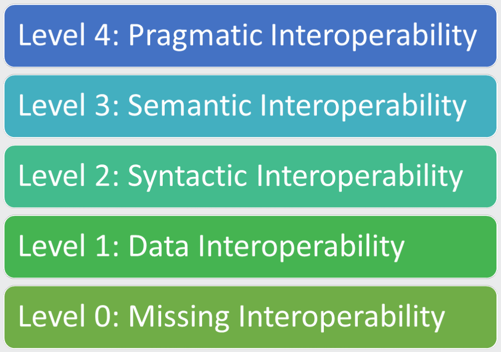

Level 4: Pragmatic Interoperability
Level 3: Semantic Interoperability
Level 2: Syntactic Interoperability
Level 1: Data Interoperability
Level 0: Missing Interoperability

Fig. 1. *Levels of Interoperability*

The lowest level of interoperability, level 0, effectively means that there is no connection between the systems. All communication must take place via human interaction. When level 1, data interoperability, is achieved, data can be shared across the systems, but their analysis is still subject to the human operators. On level 2, syntactic interoperability, data are exchanged in a standardized format such as XML or JSON (JavaScript Object Notation). Syntactic interoperability enables systems to process data only in a generic way, because the actual meaning of the data is not known. Level 3, semantic interoperability, requires a common information model so that the exchanged data can be interpreted unambiguously within a given context. A common semantic model enables key functionalities of C2IS and decision support systems. Finally, level 4, pragmatic interoperability, is achieved if processes are harmonized among the partners and their systems. For instance, if one party sends information to another one, the resulting behaviour of the receiver is predictable to the sender (within certain bounds).

Another way of structuring interoperability levels is to distinguish between organizational, informational, and technical aspects (see **Fig. 2**) (GridWise Architecture Council, 2008).

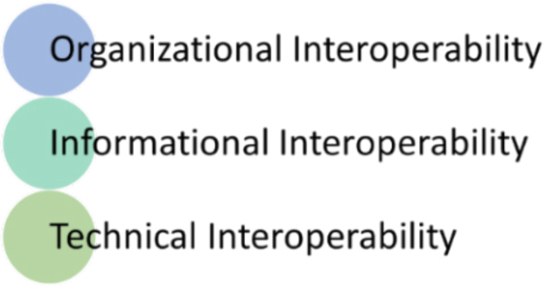

Organizational Interoperability
Informational Interoperability
Technical Interoperability

Fig. 2. *Logical Grouping of Interoperability Levels*

Technical interoperability is achieved if physical and logical connectivity of the systems is given, data can be exchanged across the network(s), and the structure of the data is interpreted equally on both sides (syntax). *Informational interoperability* is available if there is a common understanding of the concepts represented by the exchanged data and the information exchange is tailored to and put into the context of a specific business context (semantics). Finally, *organizational interoperability* relates to aligned business processes and procedures, the sharing of strategic and tactical objectives across the stakeholders, and the common alignment to political and economic objectives that are expressed as policies or regulations (pragmatics)[2].

2.3 Strictness of Interoperability Standards

Ideally, an interoperability solution should strive for the highest level of interoperability, i.e., pragmatic/ organizational interoperability. However, reality shows that stakeholders quite often have diverging national doctrines that cannot be fully harmonized in the standardization process. This may lead to a solution that is underspecified or provides a degree of flexibility that, in principle, runs counter to the interoperability objective. When following the discussion on C2 information exchange standards such as the one developed by the Multilateral Interoperability Programme (MIP) (MIP, 2023), stakeholders have two diverging points of views: some prefer an exchange solution that supports a broad spectrum of concepts and use cases, where the users determine how to best exploit it. Others prefer a strictly business, process-driven approach.

The first option leads to the optionality problem described above, whereas the second option may result in overhead if the individual business processes have a strong overlap. When considering the management of the different types of *Recognized Pictures*[3], it is challenging – some may claim impossible – to specify exactly which battlespace objects can be part of a specific picture – and which cannot.

2.4 Evolution of Interoperability Solutions

Interoperability solutions may evolve on different levels, and not all changes may be considered “disruptive”. For instance, an exchange specification may change on the technical level to adapt to new technological trends. Examples from history are the migration from custom network protocol stacks to the Internet protocol stack or the switch from SOAP (Simple Object Access Protocol – which is used by NATO’s Web Service Messaging Profile) to an exchange based on Representational State Transfer (REST). A current trend is the increased use of JSON (JavaScript Object Notation) instead of XML (Extensible Markup Language). This trend is driven by the shift to web browser applications that are based on

[2] *In the military domain, rules of engagement may be such policies/regulations.*

[3] *A recognized picture contains situational information to share an understanding of a current, predicted, prescribed, or past situation in a defined geographical area of a theatre of operation. NATO defines several domain and functional pictures, e.g., Recognized Ground Picture, Recognized Air Picture, and Recognized Engineer Picture.*

JavaScript. Changes to technical interoperability solutions are useful to align with the latest industry best practices, to lower implementation costs for new developments, to ensure continued technical support and, in particular, to counter IT security vulnerabilities imposed by outdated technologies.

Informational interoperability must be touched whenever the participating partners have a new or changed information demand. Although the systems must be adapted to the new exchange semantics, the latter does not necessarily affect the process automation implemented in the systems. New information may be simply passed through to the operational user.

Changes on the level of organizational interoperability have the greatest impact and typically imply corresponding changes on the level of informational interoperability. New technical capabilities may have local implications or can be far-reaching. For instance, the use of AI as a means to speed up object detection does not necessarily affect the overall military process. In contrast, Manned-Unmanned Teaming (MUM-T) calls for an entirely new operational processes for command and control.

A key feature of any interoperability solution is extensibility. Interoperability standards must be adaptable to a changing operational or technological environment. Therefore, it must be possible to exchange additional information that was not foreseen when the initial standard was published, without breaking backwards compatibility with existing systems that cannot be updated to the latest version of the specification. Some data interchange formats have built-in means to handle extensions (e.g., extensible and dynamic topic types (XTypes) in OMG Data Distribution Service (DDS) (Object Management Group, 2020). Other languages, such as XML Schema, enforce strict validation rules. However, when defining an XML schema, it is possible to introduce custom extension points. This approach has been used, e.g., by the MIP 4 Information Exchange Specification (MIP4-IES)[4].

2.5 Means to Achieve Interoperability

Interoperability can be achieved in two ways. The first approach is standardization of the system interfaces. Standardization requires cooperation among the various stakeholders, including industry and academia.

The second approach is product harmonization. If all partners use the same product (suite), interoperability is ensured by homogeneity. This approach results in vendor lock-ins. Nevertheless, it is not uncommon. For instance, STANAG 4677, Joint Dismounted Soldier System, relies on the loaned radio concept, which means that one nation shares its radio equipment with another nation to ensure interoperability on the network level.

To ensure interoperability with different stakeholders, it is also possible to define different service/integration levels. This way, a system may provide information in different ways, depending on the capabilities of the consumer:

- For tight integration, the consumer system may use a standardized Application Programming Interface (API).

- If this is not feasible for ad hoc partners, the system may provide an export functionality that allows retrieving data in, e.g., Open Office format.

- If this is also not purposeful, as a third option, the provider may supply a web interface to its system.

The support of different integration levels can be considered a hybrid approach of standardization and product harmonization. It can be a valid approach for exchanging information with third parties, for instance, in civil-military cooperation.

[4] *MIP = Multilateral Interoperability Programme*

STANDARDIZATION

Standardization is "the process of developing and implementing specifications based on the consensus of the views of firms, users, interest groups, and governments". (Sherif, 2006). NATO is using the definition based on ISO/IEC[5] Guide 2:2004; therefore, standardization is "the activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context". Standardization has significant benefits for the customers, as they avoid vendor lock-ins. On the manufacturers' side, standardization is a double-edged sword. On the one hand, standardization may open new markets. A coordinated initiative from different companies, each contributing its specific products and solutions, may enable a new eco-system (for instance, smart homes or industry 4.0). On the other hand, standardization means that competing products converge and innovations may become more difficult to realize. Thus, a market leader may lose market share to its competitors and will look for new ways to distinguish its own products, e.g., by introducing proprietary extensions.

3.1 Standardization & Interoperability Challenges

Standardization in the military world is facing several challenges:

- **Consensus-Based Approach.** The development of interoperability solutions is consensus-based, i.e., the participating stakeholders must approve the resulting standards. This holds in particular for NATO standardization bodies, in which approvals must typically be unanimous. Consensus does not necessarily lead to the technically or operationally most sophisticated solution but may result in compromises. One reason for this may be that one or more parties want to save investments that have already been made.

- **Slow Ratification Process.** Due to the consensus-based approach, the ratification of a new standard can take a lot of time (2 to 3 years is not uncommon). Minor concerns raised by one of the stakeholders may delay the overall process. In NATO, the responsibility for fulfilling new information exchange requirements is also shared across multiple working groups. This contributes to the slowdown and bears the risk that the final solution does not meet the initial demand.

- **Outdated technologies.** The fact that it can take years for an initial proposal to become a ratified standard may also mean that the final product is already technically outdated when it is finally approved.

- **Lack of harmonization across standards.** In the military domain, there are many different interoperability solutions addressing specific operational needs. An overview of the major standards used for command & control, seen from a land perspective, is

[5] *ISO = International Organization for Standardization*
IEC = International Electrotechnical Commission

given in **Fig. 3.** These standards use different technologies but also different semantics. This makes it difficult to ensure that information is exchanged correctly and without data loss between the different communities.

- **No synchronization of schedules.** The military standards are developed at different times and are updated following the specific roadmaps of their communities. Federated Mission Networking (FMN) defines so-called spirals that specify procedural and technical instructions for collaboration in a mission network. As a rule of thumb, a new spiral is issued about every two years. These spirals refer to specific standards that are to be supported by the mission partners. In that regard, FMN defines a baseline for different solutions developed by other standardization bodies. However, FMN is not responsible for synchronizing the latter.

3.2 Standardization and Testing

The specification of an unambiguous standard is important to achieve true interoperability across heterogeneous systems. However, the cost-effective and error-free implementation in the national systems is also a key success factor.

Thus, the standardization activities should not be restricted to delivering a specification but should also include the development of an extensive test suite and, ideally, a reference implementation. The relationships between the three components are depicted in Fig. 4.

By developing all three elements in parallel, the quality of each of them improves. In particular, this holds if the test suite and its individual test cases are specified in a formal manner and can be executed automatically. Specifying test cases and developing reference implementations (there may be multiple implementations based on different technology stacks) during the specification phase may raise questions about the specification that can be disambiguated in time. If the test suite and the reference implementation are developed by different teams, running the test suite against the reference implementation may also unveil different interpretations of the specification.

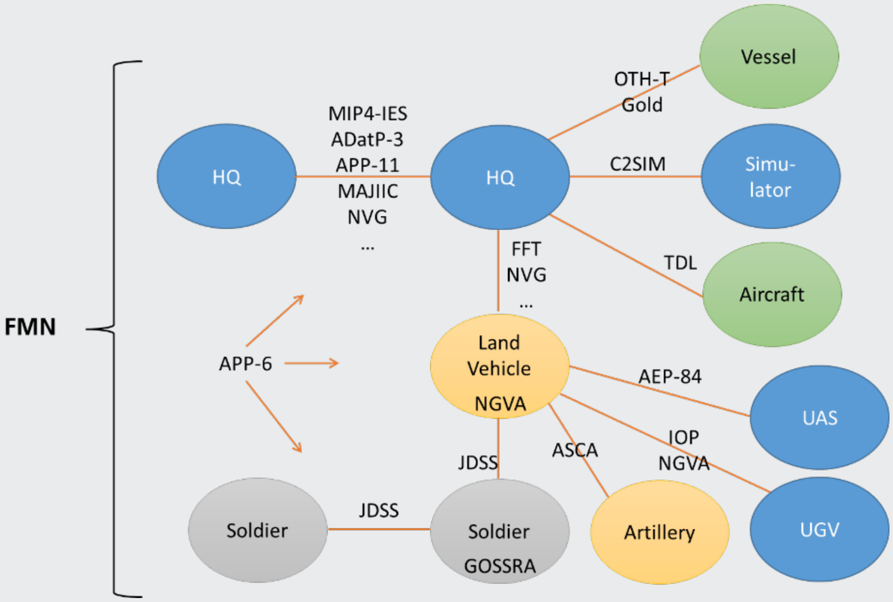


Fig. 3. *Babylonian Variety of Standards for Command and Control [Source: Fraunhofer FKIE]*

Test events such as the Coalition Warrior Interoperability eXercise (CWIX) (NATO ACT, 2022) are an excellent opportunity to test interoperability with other partners. However, the effort for preparing and conducting the tests is high and, in case of technical problems that require an in-depth error diagnosis, the test schedule gets disturbed easily. Interoperability test events are

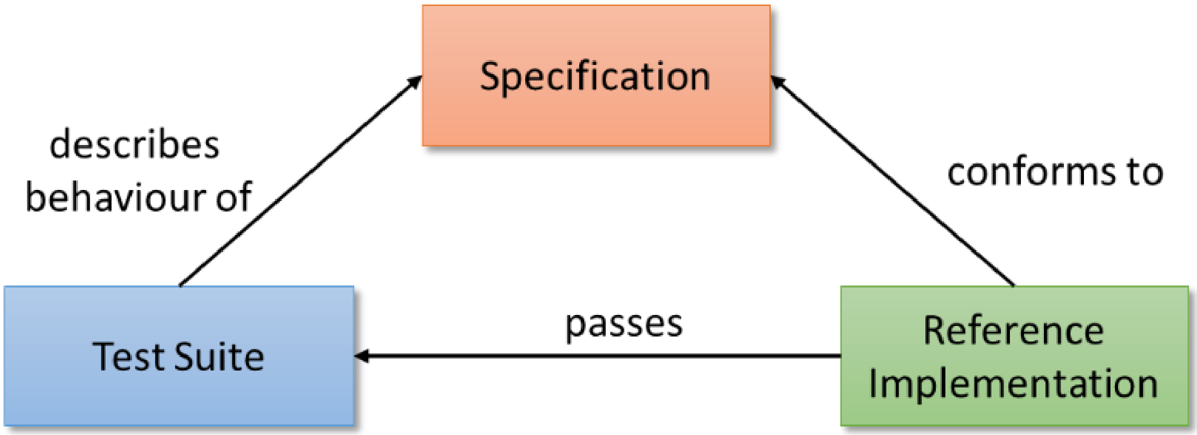


Fig. 4. *Triangle of Specification, Test Suite, and Reference Implementation*

time-consuming and, in the worst case, the more mature systems must wait for the most unstable one.

Therefore, providing test cases to the system implementers at an early stage is critical to speed up implementation. Also needed are test tools that allow executing the test cases with the systems being tested. In addition, many problems in national systems can be tracked down by running conformance tests, locally and independently from any available test partners. For instance, the MIP Test Reference System (MTRS) (Gerz, Bau, Vogt, & Vogt, 2009) allowed to test conformance to the MIP Baseline 3 interoperability specification over the Internet. In total, more than 300,000 test runs were executed by more than 50 different C2IS.

Testing complex cyber-physical systems is challenging, especially if many physical systems are supposed to interact with each other. Field tests are expensive and do not scale well. Therefore, there is a need to provide permanent test beds and sophisticated simulators for physical components. They are needed for technical tests as well as initial operational tests.

EMERGING INTEROPERABILITY NEEDS

NATO has identified several emerging and disruptive technologies (EDTs) that represent both risks and opportunities. Currently, NATO focuses on nine technological areas: artificial intelligence (AI), data, autonomy, quantum-enabled technologies, biotechnology, hypersonic technologies, space, novel materials and manufacturing, and energy and propulsion (NATO, 2022).

In the following, we will address some new interoperability needs that result from the above-mentioned, IT-related technological areas. The list in no way claims to be complete.

4.1 Smart Sensors and AI Services

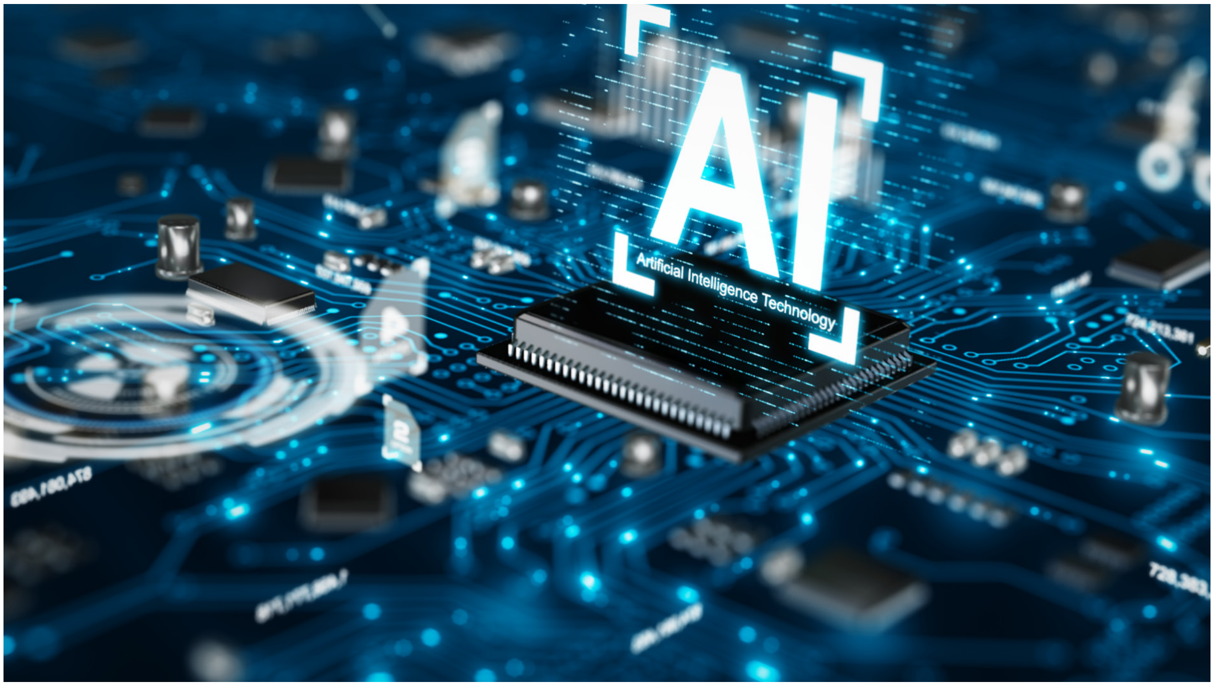
Advances in artificial intelligence will allow for a lot of sensor data processing on the tactical edge. Today, video cameras installed in land vehicles can be controlled in a standardized manner, delivering a video stream in a commonly agreed-upon format. Using AI methods, it is possible to analyse these video streams and to automatically detect and identify objects, e.g., enemy tanks. Object detection may be implemented as a stand-alone service within the vehicle architecture. Vendors may also decide to integrate AI-based capabilities right into their sensor systems (that become "smart" sensors) to distinguish themselves from the competitors. In either case, there is a need to standardize the interface to avoid vendor lock-in and to enable flexible vehicle integration.

Defining a standardized interface for a class of smart sensors is not a trivial task, especially as the capabilities are expected to improve rapidly. In the case of object detection, the result of the analysis may be a bounding box[6] associated with a specific image in the video stream, where the bounding box is supposed to contain the detected object. If the sensor data is fused with data from other sensors, the result may be a location and its accuracy.

To enable automatic processing of the result, it is also necessary to standardize the object types. If two systems identify the same type of battle tank, they should also return the same result. This requires a standardized object taxonomy that is specified down to the level of individual model types. While semantic reference models such as the MIP Information Model (MIM) (MIP/Fraunhofer FKIE, 2023) distinguish between battle tanks and armoured personnel carriers, it would also be necessary to differentiate between a Russian T-90 and an M1 Abrams. Obviously, defining and maintaining such a detailed object taxonomy is challenging.

Moreover, current interoperability standards do not adequately support automated/AI-based components as information providers. Predominant C2 interoperability standards that are designed for the operational/strategic level assume that information is provided and assessed by organizations/persons. This is also reflected in the metadata, such as those provided by the NATO Core Metadata Specification (NCMS) (NATO, 2022). Future interoperability standards should consider that sensors and automated services may contribute raw, pre-processed, fused, or

[6] *A bounding box defines the location and size of an object in a 2D or 3D space. In 2D images, bounding boxes are commonly represented by rectangles.*



aggregated data/information to the information space. Thereby, at any time, the human decision maker must be able to recognize the source and processing chain of the given information.

In order to assess collected items of intelligence, the Admiralty System is used in the military domain (Wikimedia Foundation, 2018). It allows specifying the reliability of the source (e.g., Completely reliable, Fairly reliable, Not usually reliable) and the level of confidence on the information (e.g., Confirmed by other sources, Possibly True, Improbable) in a standardized way. While the categorization makes sense for human appraisal, it is not applicable to AI systems. For instance, a system may report that it detected an object of a specific type with a confidence score of 81.9%. It is important to note that the score of two different systems cannot be compared. In addition, the system that classified the object as type X with 81.9% may also classify it as type Y with a score of 78.3%.

Within a large, distributed organization such as NATO, the development and operation of AI services could be supported by further interoperability activities. Beside the necessity of standardized APIs, a workshop at the Spring 2022 TIDE Sprint (NATO ACT, 2022) has unveiled the need for harmonized training data. It may also be useful to standardize a (cloud) environment for training and deploying AI models. Finally, AI models themselves may be subject to standardization to ensure that all mission partners get the same decision support.

4.2 Multi-Domain Operations

Multi-domain operations mandate information exchange across different domains (land, air, maritime, space, and cyber). Historically, each domain and specific community of interest (e.g., logistics) has developed their own internal processes and interoperability solutions. This has the effect that communication inside the system of systems is standardized and well understood, but interaction with systems and processes outside the stovepipe is limited.

In order to support multi-domain operations, it is necessary to first identify the operational requirements and the cross-domain processes that are necessary to achieve a given objective. Next, the specific information exchange requirements must be determined. When a requirement for an information exchange is identified, the existing landscape of already established information flows within each domain/community needs to be analysed. What systems are used? Which standards do they support? Where does the information originate?

NATO has already recognized the need to harmonize the various interoperability standards for command and control. The NATO Data Management Capability Team of the C3 Board is describing tools, processes, and best practices in the NATO Core Data Framework (NCDF) to achieve cross-COI information exchange. The objective is to harmonize standardization efforts. On the technical level, the NCDF describes different exchange patterns (e.g., publish-subscribe and request-response) and provides recommendations about which (NATO) standards could be used to achieve the desired behaviour. Additionally, it recommends XML as syntax for the exchange (unless there are severe bandwidth considerations) and provides XML naming and design rules.

On the semantic level, the NCDF proposes to make use of a semantic reference model. The motivation for using a common reference model is that many concepts can be reused when defining information exchanges. This allows a simplified sharing of information across different COIs. The MIM has been used extensively in this role to model cross-COI information exchanges.

The objectives of the NCDF are ambitious and may not be achievable in the short or medium term. Nevertheless, the harmonization of the various standardization activities is highly desirable and should be enforced.

4.3 Quantum Cryptography

Quantum technology, with quantum computing, quantum sensing, and quantum communication as its specializations, is one of the most promising disruptive technologies, for which the implications on economy, society, and the military are still subject to speculation.

While some claim that quantum technology is still in its infancy, there is already an urgent need to act in order to protect systems against breaching and information from leakage in the years to come. The reason for this is that the entire IT landscape is secured by cryptography, largely in terms of public-key algorithms. This includes server certificates for secure communication between a web server and its clients as well as personal certificates used for signing and encrypting documents.

Once quantum computers become sufficiently powerful, the existing asymmetric cryptography algorithms will no longer be secure. Therefore, under the term post-quantum cryptography (PQC), researchers and standardization bodies are in search of new methods that will withstand attacks from quantum computers.

The circumstance that quantum computing may also pose a threat today or in the near future is highlighted by a theorem of Michele Mosca

(Mosca & Piani, 2022). This theorem assumes that products and data need to be secured for a given period that depends on their sensitivity. It also assumes that the migration of existing products to post-quantum cryptography will require some time. If the sum of both periods is greater than the time it takes to build a sufficiently powerful quantum computer, then the products and data will inevitably become insecure.

While the standardization of PCQ is in the hands of standardization bodies such as the National Institute of Standards and Technology (NIST), which expects to publish a standard by 2024, NATO and its members should immediately start analysing the impact on existing interoperability standards and develop a migration strategy for both their standards and their systems. The migration of the individual systems will not take place simultaneously but gradually. Following the logic of Mosca's theorem, those systems that process data with a long-term security classification should be migrated with priority. Systems that encrypt data with a short relevance period can be adapted later.

4.4 Sensor Networks

With technological advancements regarding energy-efficient sensors and low-power radio communication, we can expect self-organizing networks of uncrewed vehicles and deployed sensor nodes in the air, on the ground, above the sea, and under water. Such sensor grids would be able to perform large-area reconnaissance and reconfigure its network if a sensor fails.

4.5 Manned-Unmanned Teaming

In future scenarios, manned and unmanned vehicles will act together, where one or more commanders will task one or more unmanned vehicles. This may be the case for convoy travel as well as for combat actions, in which multiple battle tanks fight together. Such scenarios raise operational questions (command structures, ergonomics, etc.), questions of security and safety, questions of ethics, as well as technical interoperability issues that are not sufficiently covered by today's standards.

4.6 Automation / Decision Support

Intelligent decision support will mandate that even more information is available in a machine-processable format. For instance, rules of engagement (ROEs) must be considered during the planning process. However, current interoperability standards only allow to exchange ROEs as free text. Thus, they cannot be evaluated by decision support systems.

RECOMMENDATIONS

In this section, recommendations are made to ensure interoperability under the influence of emerging technologies. They are primarily based on the explanations given in the previous chapters. Section 5.1 lists cross-cutting recommendations, whereas section 5.2 refers to the specific technological areas sketched in chapter 4.

5.1 Recommendations for Improving the Standardization Process

In order to improve interoperability in an increasingly complex system environment, measures can be taken at different stages. They relate to the specification phase as well as the implementation and testing phase.

Standardization Phase

The following recommendations regard the design of future specifications:

- Consider IT security aspects from the very beginning. Some interoperability standards assume that participating systems operate in a secure network. They provide little or no means for securing the information exchange. This is against the principles of Zero Trust, namely “never trust, always verify”. Adding security measures at a later point in time can be difficult and costly.

- Do not reinvent the wheel but look at available solutions and adopt them. This applies, for example, to the security aspects mentioned above, for which there are already established and proven methods and tools.

- Separate aspects of technical interoperability (protocols and syntax) from aspects of informational interoperability (semantics) to facilitate reuse of common information concepts (shared vocabulary) and to be able to adapt to changing technological platforms. This separation is supported by Model-Driven Development (Model-Driven Architecture in the terminology of the Object Management Group (OMG, 2023)).

- Make interoperability solutions extensible, e.g., by using type systems with built-in features for extensible types or by defining custom extension points (see 2.4).

- Make interoperability solutions self-descriptive. Systems should be able to provide information on their capabilities (supported interoperability services, supported versions of the interoperability specifications, technical information on their interfaces, etc.). This information would ideally be provided by a service registry in a client-server architecture.

- Develop a test suite and reference implementation(s) in parallel to the specification so that the implementation phase can be shortened significantly once the standard is approved. As a side effect, this approach also leads to clearer and error-free standards (see 3.2).

The following recommendations refer to the standardization process, i.e., how specifications should be developed:

- Set up a multidisciplinary team comprising of operational and technical subject matter experts; do not spread responsibility across multiple boards and keep the people who originally raised the demand in the loop until the operational validation of the solution is done.

- Develop a conformance statement template (in a team formed by future procurers and industry) that allows specifying which parts of a comprehensive standard are actually supported by a given system. It can be used later as a contractual part during the procurement process (see 2.1).

- Synchronize standardization activities with other, relevant standardization bodies; establish liaison officers for that purpose.

Implementation & Testing Phase

The rapid adoption of new standards can be supported in the following ways:

- Provide test tools for conformance testing at an early stage. This allows vendors to test their systems in-house when they are still immature and not ready for interoperability tests with other stakeholders. Conformance test tools make it possible to focus on more complex technical and operational tests during international exercises.

- Provide permanent test beds for interoperability testing. International exercises such as CWIX take place once a year for a limited number of weeks. However, there is a need to test throughout the entire year since systems are subject to regular updates.

- Provide simulators for testing cyber-physical systems of systems. This allows vendors to test their individual components that are supposed to interact with third-party cyber-physical components.

5.2 Recommendations for Supporting New Technologies

Emerging and disruptive technologies mandate new, and adaptations to existing, interoperability solutions.

Automated Systems, Smart Sensors, and AI Services

- Define standardized, extensible taxonomies of objects for individual use cases, such as object detection with cameras on the battlefield. These taxonomies shall be harmonized with existing interoperability solutions.

- Ensure that future interoperability solutions across all echelons consider (smart) sensors and AI services as first-class contributors to the information space. Presently, this is not the case. For instance, the messages in the NATO Message Catalogue (APP-11) are not designed for information sharing by automated systems. It must be possible to express whether the information source delivers raw, pre-processed, fused, or aggregated data/information.

- Provide means to trace aggregated/fused information back to their sources in order to enable the operator to understand how information was determined (explainability).

- Ensure that metadata standards properly reflect the needs of sensor and AI-based services. This includes aspects such as reliability, confidence, and accuracy.

- Provide a platform to share training data and trained AI models across all stakeholders.

Multi-Domain Operations

- Continue harmonization of the various interoperability standards for command and control as promoted in the NATO Core Data Framework. In particular, harmonization of the MIP Information Model and the NATO Message Catalogue would greatly reduce the

risk of information loss and corruption at the domain boundaries.

- Consider and prioritize the harmonization in the context of cross-domain processes and information exchange requirements. Take into account that each domain and community of interest may have its own specific information needs and not all information has to be shared across boundaries.

Quantum Cryptography

• Develop a migration strategy to replace current cryptographic solutions with post-quantum cryptography ones. Work on this strategy should start as soon as possible as the time that is available to migrate the systems is not known. This initiative should be raised together with the Federated Mission Networking (FMN) community. However, please note that post-quantum cryptography affects all IT and communications systems, not just the ones run in mission networks.

• Identify interoperability standards and systems that need to be migrated. Prioritize them according to how long the data encrypted by them needs to be protected.

• Follow the standardization activities in the NIST and analyse the availability of commercial and free PCQ solutions (appliances, applications, and third-party libraries).

SUMMARY AND CONCLUSIONS

In this paper, we introduced several concepts related to interoperability and discussed different aspects that make interoperability standards future-proof and allow interoperability with partners on different levels of integration. Standardization of complex solutions mandates multi-disciplinary teams in which operational subject matter experts and technical staff work hand in hand – from the requirements analysis to the operational validation. In order to speed up the realization in national systems, standardization bodies should assist the implementers with test suites and test tools as well as software artefacts and reference implementations. For testing complex cyber-physical systems of system, there is a need to provide permanent test beds and simulators for physical components.

New technologies such as Artificial Intelligence and Quantum Computing require adaptations to existing, and the specification of new, interoperability solutions. Current interoperability standards are not well-prepared for scenarios, in which smart sensors and AI services contribute information to the common operational picture. Research on quantum computing requires actions and a migration roadmap in the field of cryptography even before the technology becomes actually operational.

Ai

REFERENCES

Allen, J. R., & Husain, A. (2017, July). On Hyperwar. Processings of the U.S. Naval Institute, 143(1). Retrieved December 21, 2022, from https://www.usni.org/magazines/proceedings/2017/july/hyperwar

Azhar, A. (2021). The Exponential Age: How Accelerating Technology is Transforming Business, Politics and Society. Diversion Books.

Gerz, M., Bau, N., Vogt, A., & Vogt, R. (2009). Automated Conformance Testing of C2IS. NATO RTO Information Systems Technology Panel Symposium (IST-087/RSY-020). Stockholm, Sweden.

GridWise Architecture Council. (2008). GridWise® Interoperability Context-Setting Framework. Retrieved from https://gridwiseac.org/pdfs/GridWise_Interoperability_Context_Setting_Framework.pdf

IEEE. (2016, September 23). Standards Glossary. Retrieved from Standards University: https://www.standardsuniversity.org/article/standards-glossary/#I

MIP. (2023, January 11). Retrieved from Website of the Multilateral Interoperabilility Programme: https://www.mip-interop.org/

MIP/Fraunhofer FKIE. (2023, January 10). Retrieved from MIP Information Model Portal: https://www.mimworld.org

Mosca, M., & Piani, M. (2022). 2021 Quantum Threat Timeline Report. Global Risk Institute. Retrieved January 11, 2023, from https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

NATO. (2015, November 23). APP-11 - NATO Message Catalogue - Edition D Version 1.

NATO. (2017, October 16). APP-06 - NATO Joint Military Symbology - Edition D Version 1.

NATO. (2022, November). ADatP-5636: NATO Core Metadata Specification (NCMS). Edition A, Version 1. Retrieved January 10, 2023, from https://nso.nato.int/nso/nsdd/main/standards?search=5636

NATO. (2022, December 8). Emerging and disruptive technologies. Retrieved from https://www.nato.int/cps/en/natohq/topics_184303.htm

NATO ACT. (2022). Federated Interoperability. Retrieved from Allied Command Transformation: https://www.act.nato.int/federated-interoperability

NATO ACT. (2022, April 8). TIDE Sprint Advances NATO Readiness, Resilience, and Relevance. Retrieved from Allied Command Transformation: https://www.act.nato.int/article/tide-sprint-advances-nato-readiness-resilience-and-relevance/

NATO Standardization Office. (2023, November 10). NATOTerm - The Official NATO Terminology Database. Retrieved from NSO Public Website: https://nso.nato.int/natoterm/Web.mvc

Object Management Group. (2020, February). Extensible and Dynamic Topic Types for DDS. Version 1.3. Retrieved from https://www.omg.org/spec/DDS-XTypes

OMG. (2023). MDA - The Architecture Of Choice For A Changing World. Retrieved May 03, 2023, from https://www.omg.org/mda/

Sherif, M. (2006). Standards for telecommunications services. In K. Jacobs (Ed.), Advanced Topics in Information Technology Standards and Standardization Research (pp. 183-205). Hershey, PA: Idea Group Publishing.

Standards Coordinating Committee of the IEEE Computer Society. (1990). IEEE Standard Computer Dictionary. New York, USA: The Institute of Electrical and Electronics Engineers. Retrieved Jan 05, 2023, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=182763

Wikimedia Foundation. (2018, September 25). Admiralty code. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Admiralty_code

OPEN
PUBLICATIONS

Risk Acceptance in Future Warfare across
Domains

www.openpublications.org