VERSITA

Central European Journal of **Computer Science**

Command and control information systems semantic interoperability using a canonical messaging approach

Darko Galinec[1][*], William Steingartner[2][†], Danijel Macanga[3][‡]

1 Department of Informatics and Computing,
  Zagreb Polytechnic for Technical Sciences, Zagreb, Croatia

2 Department of Computers and Informatics,
  Faculty of Electrical Engineering and Informatics,
  Technical University of Košice, Letná 9, 04200 Košice, Slovakia

3 Ministry of Defence,
  Zagreb, Croatia

Abstract: In presence of rapid development of information and communications technology (ICT) able to increase data processing, much more data can be stored, used and/or mediated and disseminated. Today, information and knowledge become a resource of strategic importance in complex systems, both business and military. On the other hand the question of credibility of the collected data arises: complex systems have to deal with an increasing access to information with less knowledge about their origins and their quality. Due to this lack of information on information, contemporary organizations suffer from organizational indifference. In this paper the ways and means for ensuring semantic interoperability in order to achieve information superiority in complex systems are examined, with special emphasis to military systems using Command and Control Information Systems (C2IS). Canonical messages (canonical intermediaries) based on canonical forms (canonical data models and formats) reduce the number of transformation maps that system must create and manage. An approach based on canonical messaging within the military domain is presented: Multilateral Interoperability Programme (MIP). If implemented correctly and consistently it should lead to achievement of information superiority.

Keywords: canonical messaging • command and control information system • integration • semantic interoperability

© Versita Sp. z o.o.

1. Introduction

By following the hypotheses of Peter F. Drucker and Dirk Baecker we can observe the dawn of the so called next society. The crucial driving force of the corresponding change is the evolution of computer communication as new media of dissemination: Much more data than ever before can be saved, activated and disseminated. In addition, bits

* E-mail: darko.galinec@tvz.hr
† E-mail: william.steingartner@tuke.sk (Corresponding author)
‡ E-mail: danijel.macanga@morh.hr

and bytes cannot be read like books because they have to be mediated and reproduced by resource consuming software and hardware. Finally, computer communication manifests and presses ahead the detemporization, virtualization, and poly-contextuality of information, and is therefore said to be the major driver for an unmanageable complexity of communication [20].

In the military, most decision situations possess a degree of ambiguity and uncertainty and are not easily captured in a static or stochastic model. This has led to an increased use of "fuzzy sets" in analyzing decisions, not in an attempt to quantify the unquantifiable, but as a way to formalize our way of dealing with the unquantifiable and imprecise [1, 5]. The concept of fuzziness is related to the idea of the "fog of war" introduced by Carl von Clausewitz. In his discourse On War, Clausewitz presents two concepts leading to difficulties in conflict, friction and fog. Friction is the effect of numerous minor incidents which reduce the level of performance so the intended goal is not reached [2]. There are physical and psychological aspects of friction. Friction due to a hostile physical environment is usually more obvious; it is caused by darkness; bad weather or terrain, physical exertion; degraded command and control, logistics, maintenance, or weapon systems; or merely chance bad luck; or psychological factors, such as stress produced by the interaction of combatants and the environment of war. Another source of friction is the "fog of war." Fog is the uncertainty of war, caused by factors such as inaccurate, incomplete or contradictory information, deviations in weapon system efficacy, actions of the enemy, and the enemy's nebulous capabilities and intentions [4]. Operational decision-maker usually faces decisions under conditions of uncertainty – intrinsically imprecise decisions under adverse conditions would normally be faced in military operations.

2. Information superiority and situation awareness

Information superiority is that degree of dominance in the information domain which permits the conduct of operations without effective opposition [24].

Sound thinking and decision making are more than mere loose ends of network-centric warfare. Moreover, success in competition on the military cognitive plane will not necessarily follow success on the technological plane. Therefore, what is needed is a coherent strategy to build battle-wise forces.

2.1. Superiority in decision making

Decision superiority – "the process of making decisions better and faster than an Adversary" [24] (p. 19) – is essential to executing a strategy based on speed and flexibility. Decision superiority requires new ways of thinking about acquiring, integrating, using and sharing information. It necessitates new ideas for developing architectures for command, control, communications and computers (C4) as well as the intelligence, surveillance and reconnaissance assets that provide knowledge of adversaries. Decision superiority requires precise information of enemy and friendly dispositions, capabilities, and activities, as well as other data relevant to successful campaigns.

Battle space awareness, combined with responsive command and control systems, supports dynamic decision making and turns information superiority into a competitive advantage adversaries cannot match. Persistent surveillance, ISR management, collaborative analysis and on-demand dissemination facilitate battle space awareness. Developing the intelligence products to support this level of awareness requires collection systems and assured access to air, land, sea and space-based sensors.

Decisions to apply force in multiple, widely dispersed locations require highly flexible and adaptive joint command and control processes. Commanders must communicate decisions to subordinates, rapidly develop alternative courses of action, generate required effects, assess results and conduct appropriate follow-on operations. A decision superior joint force must employ decision making processes that allow commanders to attack time-sensitive and time-critical targets. Dynamic decision making brings together organizations, planning processes, technical systems and commensurate authorities that support informed decisions. Such decisions require networked command and control capabilities and a tailored common operating picture of the battle space [24].

Awareness of the growing operational and strategic importance of decision superiority must exist, which has some but not all of the elements of the superiority in cognitive capacity and performance that we call battle-wisdom. It also tells us that responsive command and control systems, collaborative analysis, and on-demand dissemination of information are important to decision superiority. This official explanation of what is required for decision superiority fails to stress

human cognition – how people think and how well they decide. It is as if battle-wisdom – the capacity to integrate reliable intuition and rapid reasoning and the abilities to anticipate, decide quickly, seize opportunities, and learn in action – is assumed, needing only better intelligence sensors, information networks, and processes to succeed. It calls for commanders to communicate their decisions to subordinates, without recognizing that the subordinates may well be better informed than their superiors to decide what to do. The networking is not that it enables commanders to promulgate orders but that it informs those "on the edge" and permits them to collaborate, accept responsibility, and take initiative. The key to decision superiority lies not in the information network but in the human [10].

2.2. Decentralization of decision making

The value of self-directed learning can be undermined if individuals lack the trust and confidence of their superiors and are not granted the authority to make decisions. Many strong businesses are distributing decision making authority to those on the front lines, a practice that not only enables an organization to act with greater agility and speed but also imparts confidence to those who make the decisions. Businesses in the 1980s and 1990s were swamped with new management theories – to name a few: total quality management, continuous improvement, right-sizing, core competence, process engineering, strategic alliances, competitive strategies, learning organizations, empowerment, flattening of hierarchies, cross-boundary teaming etc.

None of these theories alone induced sustainable organizational change without the mutual commitment of leadership and rank-and-file employees. For reform to be sustainable, an organization must put into practice certain values and principles concerning information, people, and trust: transparency; open information-sharing; cross-boundary communication and collaboration; an understood mission and values; a culture that rewards taking responsibility; a commitment to learning; and a willingness to give talent room and to give people the confidence and authority to make decisions.

Organizations that need to wait for bureaucratic procedures, chain-of-command review, or decisions from on high before acting on an opportunity may not be able to survive in fluid and unfamiliar situations [10].

Information superiority (IS) is that degree of dominance in the information domain which permits the conduct of operations without effective opposition [23].
Situation Awareness (SA) has several dimensions and is closely related to Decision Support Systems. SA is the perception of environmental elements within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. It is also concerned with perception of the environment critical to decision-makers in complex, dynamic areas from aviation, air traffic control, power plant operations, military command and control (C2). SA involves being aware of what is happening to understand how information, events, and actions will impact goals and objectives, both now and in the near future. It directly depends on Information Superiority and Common Operational Picture (COP). COP is a single identical display of relevant (operational) information (e.g. position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads, etc.) shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situation awareness [23]. Situation awareness may be expressed and presented as follows:

$$SA = f(IS, COP). \tag{1}$$

2.3. Defence chief information officer's role and responsibility

Within defence organizations, situation awareness is generally divided into two categories – real-time battlefield situation awareness (e.g., US Blue Force Tracking) and a broader, less real-time capability often associated with either a balanced scorecard or "dashboard" for senior leadership:

- Battlefield SA – one of the biggest problems the US system has faced is the exponential growth in both usage and data feeds (data from various sensors). The system was not initially designed to support this environment and was developed in a very "stovepipe" fashion. The future of this and similar systems is their ability to adapt quickly to changes in mission, environment, and data streams. The primary *role* of the Chief Information Officer

(CIO) in this environment should be to define and enforce data interoperability standards to enable the system to be agile. Functional proponents and functional oriented developers will seldom see the value or long-term impact of developing to an enterprise vision. This is the prime function a Defence Chief Information Officer (DCIO) can bring to the battlefield systems. However, as further discussed below, linkage of the value of an enterprise ICT approach to mission accomplishment is critical. In the case of battlefield SA, that value is likely best expressed in terms of agility to changing mission situations and interoperability with current and future coalition partners.

- Enterprise *SA* – in addition to the standards work mentioned above, the DCIO has several additional functions that should be performed in support of this broader Situation Awareness requirement. The most basic function is to work with the mission leads to develop an IT Strategy [8]. Also, key pieces of the IT Strategy are the Enterprise Architecture [19] and the Enterprise Sourcing Strategy [6]. One of the keys to CIO success in transitioning from an infrastructure services operator to a full mission partner is developing a mission performance mindset. Mission performance metrics and how ICT impacts those mission performance metrics is one of the more challenging aspects of CIO life for most defence CIOs, but is also the area that is most powerful in linking ICT capabilities to mission capabilities. The Mission Performance section should be expanded as an Enterprise dashboard for the senior non-IT leadership within the organization.

2.4. DCIO's typical challenges

There exist two main challenges for DCIO:

- Credibility – many warfighters and mission leaders have had poor experiences with the stability and responsiveness of central ICT organizations and, therefore, the CIO lacks credibility to "sit at the table". Linking IT performance to Mission Performance metrics is a critical 1st step in establishing that credibility.

- Knowledge – many DCIOs lack the mission understanding to communicate the value of ICT capabilities to the mission in terms the non-ICT leadership understands. There are several ways to overcome this, either by bringing more mission personnel into the ICT organization or detailing a senior ICT manager to work with and even deploy with combat unit to fully understand the mission challenges and vocabulary.

Based on the results of business process analysis, CIO as a leader of ICT function in a complex system can and should initiate process change, streamline the processes or suggest introduction of the new processes if necessary, in order to improve overall business process [9].

Military organizations have been, and will continue to be, challenged to improve the tactics, techniques, and procedures (TTPs) associated with executing their mission. ICT has played a major role in the evolution of TTPs over the past 15 years and that IT role is increasing with the adoption of Net-Enabled Warfare concepts. However, leaving the application of ICT to support business process improvement in the hands of the knowledgeable functional proponent has resulted in numerous marginal systems and an extensive array of stove-piped applications.

Too often, an emerging technology or the latest "gadget" that is purported to solve all their problems overly influences the well-meaning functional lead. Functional proponents, who are paid to be functional experts and not ICT experts, are even more prone to fall into the trap of "peak of inflated expectations". DCIOs have an opportunity and an obligation to take a leading role in the effective and efficient application of ICT to mission process improvement across all functional areas [18].

3. Basic notions of data integration

Movement from a monolithic data integration infrastructure to a hub approach can be inhibited by a number of barriers. The most significant of these is related to the organizational structure and how data integration projects are funded and managed. The hub approach may require that individual project teams give up decision rights regarding choices of tools, architecture and design approaches, and definitions of business rules and semantics of the data. Clear communication of the benefits of the hub approach and strong governance models to ensure leverage of the standards established for the hub – such as tools and canonical forms – are critical to success. For most organizations, it will be impossible to move immediately from a complex and chaotic data integration infrastructure to a comprehensive hub-based approach.

A more pragmatic approach is to start with a small and synergistic set of data flows with common characteristics, and then expand outward over time to include more of the data integration landscape [7].

3.1. Data integration approaches

Historically, organizations have approached data integration in an application- or project-specific manner. Project teams focused on their specific requirements, building tightly bound, point-to-point interfaces between data sources and targets of interest, generally without regard for future adaptability and without considering the data integration processes developed by other project teams. This occurred naturally due to the diversity of different use cases and project types requiring data integration work (ranging from business intelligence and data warehousing to data sharing within enterprise) and the distribution of teams and individuals involved in designing and building data integration solutions. Unfortunately, across the whole of an organization's application and data portfolio, the result was a very complex environment of diverse data flows and a number of significant challenges [7] (p. 2):

- Overlapping and redundant interfaces to individual data sources and applications.

- High degree of interdependency between data integration processes and applications because of tight binding.

- Lack of standardization in how data integration processes are developed.

- No visibility into the complete lineage of data or relationships between data flows across the enterprise.

- Diverse and redundant approaches for how data quality rules are applied.

- No consistency in semantics of the data across project boundaries.

- Limited adaptability in the face of changing requirements because of the fragile and complex environment.

Data integration activities have not been managed and governed from an enterprise perspective. As a result, organizations experience: higher deployment costs due to a lack of reuse; higher costs of ongoing support and enhancement due to extreme complexity; and higher levels of risk from a lack of visibility of data lineage and the potential for inconsistency in business rules for data transformation, calculations and data quality controls. Consequence of those challenges and contemporary pressures to increase reliability and consistency of data delivery is that organizations are seeking alternative deployment approaches for data integration capabilities [7] (p. 2).

As an alternative to point-to-point and project-specific data integration development and deployment, an increasing number of organizations are moving to a delivery approach in which data integration processes are managed in a cross-project/application fashion (Figure 1). Sometimes referred to as a "data integration hub," in reference to a "hub and spoke" architecture, this approach is being adopted to address the challenges already stated. This approach is sometimes referred to by other names, including "data delivery hub" and "data broker architecture." In a hub-based approach to data integration, data being extracted from multiple sources flows through a centralized model (the hub) and is delivered from the hub to various consuming applications. The hub serves as a clearing house for data moving between combinations of sources and targets. Data may flow through the hub on a scheduled, batch basis or in a real-time and granular fashion. As an architectural approach, the data integration hub may make use of several concepts to facilitate data flow, simplify the overall data integration infrastructure and improve the governance of deployment.

3.2. Appliance of data integration concepts

These concepts may, or may not, be applied, depending on the organization's requirements and goals [7] (p. 4):

- Persistence of data flowing through the hub: Organizations may choose to make the hub a location for physically persisting data flowing through the enterprise. By persisting data, the hub may take on an operational data store (ODS) style. The decision to persist data in the hub may be driven by requirements to support access to integrated views across multiple sources, or to support redelivery of data in scenarios where technical issues prevented initial delivery.
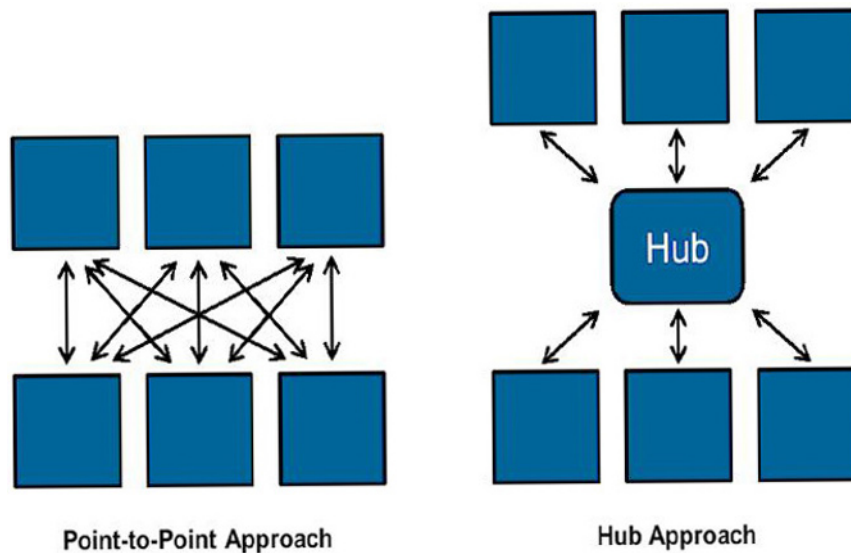
Figure 1. Traditional data integration implementation approaches vs. a data integration hub [7] (p. 3).

• Canonical forms (canonical data models and shared-message data formats): The data integration hub, whether or not data is persisted, can adopt concepts of common formats and definitions that are used as the "translation point" between the differing syntax and semantics of the participating sources and targets. By enforcing agreed canonical forms for the data being shared, data arriving from sources is mapped and transformed into the appropriate canonicals, and then further mapped from the canonicals into the delivery targets. Sources and targets participating in the hub architecture need to know only the relationship between their local representation of the data and the relevant canonical forms, not all the specifics of the targets that may consume their data.

  – o The lack of shared-message formats is a significant barrier to effective application integration and an impediment to enterprise efforts to increase agility. It is common for each interface between a pair of applications to have a unique message format, with the same business object (e.g., person or facility) represented in a unique way in each message. As new applications are added to the enterprise portfolio, the number of interfaces rises exponentially – resulting in inflexibility and significant maintenance costs. For example, many enterprises store person information in different systems, with little or no consensus on how this data is represented. With point-to-point interfaces between n systems, the number of transformations needed is $n(n-1)$.

  – However, if a shared, canonical view of person is used, data from each of the source systems is transformed into this format and then transformed again from the canonical format to the target format, requiring 2n transformations. As the number of systems exchanging data rises, so do the advantages of using canonical, shared-message formats. The key to managing workload is to define and implement shared-message formats. However, despite the advantages of canonical message formats, they may not be appropriate for every situation. In some instances, it may be difficult or even impractical to translate between the canonical format and the format of data coming into or out of an application [13] (p. 2).

• Data quality controls: With data quality a concern for all organizations, the centralization of data flow through the data integration hub creates the opportunity for a consistent approach to monitoring and improving data quality. Data quality rules can be applied to data flowing through the hub, ensuring that data quality issues are identified and addressed before data is delivered to consuming applications and processes. Some organizations may choose not to apply data quality resolution in the hub, but rather continue to let individual data sources and consumers address this issue. In these cases, the hub becomes merely a collection area, rather than a data quality control point.

The concept of a hub-based approach to integration is not new – this concept has been applied for many years in the application integration discipline, and has been directly supported by application integration middleware technology based on the principles of routing messages through central broker architecture. The concept of canonical forms is commonly seen in such application integration scenarios. As part of the ongoing unification of the application integration and data integration disciplines, these concepts are increasingly being adopted by Information technology (IT) leaders driving data integration initiatives.

4. Mulitalateral interoperability programme

Senior leaders consider information sharing a means to the goal of reaching new customers and new markets, and attaining growth and innovation objectives. IT must respond by reimagining information architecture, improving system integration and updating current interoperability approaches. Interoperability is the ability of diverse systems and organizations to work together – to interoperate [11]. There are different levels of interoperability – from the simple to the complex. Most IT groups focus on the technical aspect (also known as "syntactic interoperability"), which is the basic form that focuses on the data formats and protocols necessary for exchanging information in support of business processes. XML (Extensible Markup Language) and SQL (Structured Query Language) standards are considered tools for syntactic interoperability.

4.1. Interoperability by design

When IT focuses exclusively on technical interoperability, integration problems often arise because of redundant information models and incompatible semantics. Just as organizations experienced poor results from SOA (Service-Oriented Architecture), cloud computing will generate minimal benefits unless organizations make an effort to improve information quality, rationalize their information models and evolve beyond syntactic interoperability.
At the other extreme is semantic interoperability – a form of information sharing in which two or more systems automatically interpret the information exchanged meaningfully and accurately in order to produce useful results. Semantic interoperability will only be achieved gradually over a span of many years, one class of data at a time [17] (p. 5). In military, semantic interoperability is seen as an ideal way of exchanging military information among applications and units at a level of granularity and coding sufficient for the receiving system to use the information for military decision support, research, quality assessment and sophisticated business intelligence. Because many integration problems occur when the focus is limited to technical interoperability (e.g. low-level data exchange standards), and given that semantic interoperability is still years away.
Organizations should pursue an incremental path – called interoperability by design. Interoperability by design is an approach where the same standard supports both the technical and information needs for information sharing [17] (p. 5).

4.2. MIP structure

Multilateral Interoperability Programme strategy to achieve interoperability of cooperating national Command and Control Information Systems at all levels of command, in support of multinational, combined and joint operations in order to provide a focus for the MIP Programme of work is necessary [16]. MIP is an interoperability organization established by national C2IS system developers with a requirement to share relevant C2 information in a multinational/coalition environment. As a result of collaboration within the programme, MIP produces a set of specifications which, when implemented by the nations, provide the required interoperability capability.
MIP has a three-tiered structure: two Management levels and one Task-Execution level. The Management levels consist of an oversight Steering group and a Programme Management group. In late 2009 the programme structure was reorganised from Multidisciplinary Working Parties into two Integrated Product Teams (IPT). The first is IPT-3 and it is responsible for the In Service Support to Block 2 and Block 3 MIP products. The second team is IPT- Futures, and it is responsible for the development of a future specification using the latest system architecture concepts. ACT (Allied Command for Transformation) Members of SEE (Staff Element Europe), DPC (Defence Planning Command & Control) attend the MSG and the PMG meetings. DMSWG (Data Management Services Working Group), formerly NDAG (NATO Data Administration Group) cooperates in the development of the main data model called JC3IEDM (Joint Command,

Control and Consultation Exchange Data Model) honouring the agreement signed with MIP in February 2004. The JC3IEDM is NATO STANAG 5525 [15].

MIP provides a venue for system level interoperability testing of national MIP implementations as well as providing a forum for exchanging information relevant to national implementation and fielding plans to enable synchronization. MIP is NOT empowered to direct how nations develop their own C2IS.

Key points:

- MIP focuses on interoperability of command and control (C2) systems, which includes the Land view of Joint operations, but encourages contributions from Air, Maritime and other Communities of interests (Cols).

- MIP specifications are based on operational requirements developed into a fieldable interoperability solution.

- MIP assures the quality of the specification through operational and technical testing of national implementations.

A conceptual illustration of how the current MIP interoperability solution works is illustrated below (Figure 2).
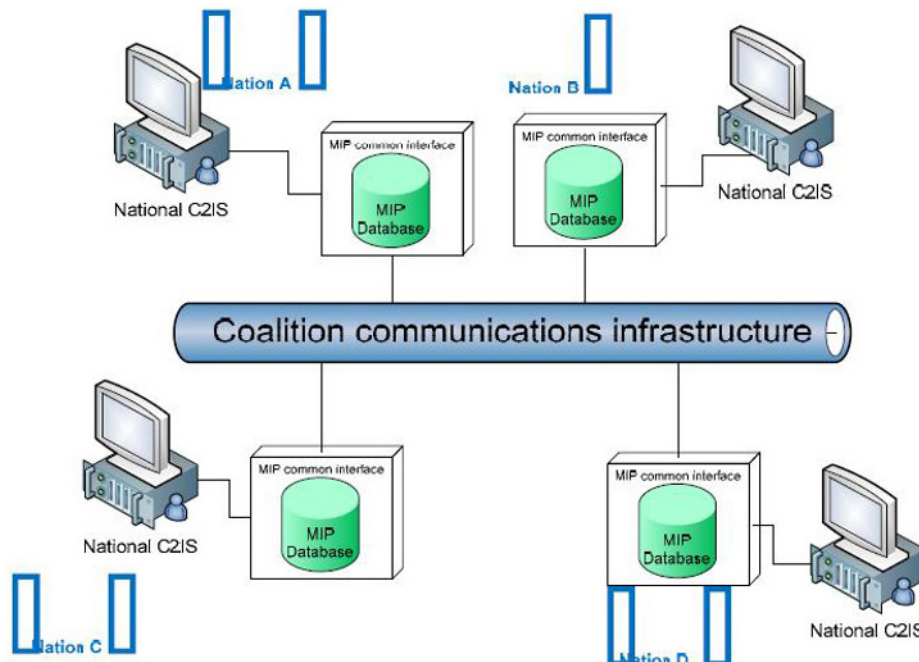

Figure 2. Different coalition C2IS connecting via the current MIP solution.

The MIP solution refers to two or more national C2IS exchanging information by employing their respective implemen-tations based upon the agreed MIP technical specifications[1] and supporting procedural and operational documentation. The vision for the Multilateral Interoperability Programme is to become the principal operator-led multinational forum to promote international interoperability of Command and Control Information Systems (C2IS) at all levels of command. The MIP scope is to deliver a command and control interoperability solution in network-centric environment focused on the Land operational user in a Joint environment including the requirements of Maritime and Air communities. The MIP scope is derived from considering the constraints and limitations of the MIP solution [16].

---

[1] *The technical specification includes a common data model and agreed exchange mechanisms*

4.3. A canonical message for conveying information

Typically, military organizations organize a canonical message around a business entity types, like a person, facility, unit, weapon, action, coordination system, plan-order or target. MIP uses canonical message for information interchange between nations. A canonical message is a generally agreed-on standard for conveying information.

The objective of a canonical message is to be able to convey information about all the events associated with such entities, independent of the applications in which those events occur. The term "application-specific business objects" used in this process refers to data having the format, structure and semantics native to the source and target applications. The term "generalized business object" is also used to refer to the canonical intermediary that it recommended organizations use to reduce the number of messages and relations (i.e. links or interfaces between properties of an object) its technology created and managed.

4.4. Canonical intermediaries for reduction of the number of interface components

Organizations transition from point-to-point to mediated interfaces to reduce the number of assets for connecting applications that they must create and manage. Estimation is that the exclusive use of a point-to-point approach results in $3n$ to $4n$ interfaces, where n is the number of applications in an organization's portfolio. This means that as many as 2,000 point-to-point interfaces will exist for a portfolio of 500 production applications (and some portfolios are much larger) [21] (p. 3).

Organizations began deploying mediation technology, such as integration brokers and ESB (Enterprise Service Bus) suites, to reduce the number of connections they needed to support their production applications, and to simplify the creation and management of those interfaces [21] (p. 3).

Establishing the use of canonical messages is not without challenges. More than 50% of organizations that have deployed mediation technology do not use canonical messages. Users elect not to use canonical messages for multiple reasons [21] (p. 5):

- They are pragmatic. They do not want to be bothered with creating a canonical intermediary, because they know they are developing a one-off interface that will not be used for other projects.

- They realize that the interface they are creating will likely be reused, but they do not realize they are creating a maintenance nightmare by using a point-to-point, rather than a canonical, message.

- They are focusing on the most expedient solution to meet project deadlines, thus electing to defer the problem to the future.

A canonical message is an intermediary. An interface that employs a canonical messaging transforms data from the format, structure and semantics native to the source application to that of the established canonical intermediary, and from the canonical intermediary into the format, structure and semantics that the target applications require. Using a canonical intermediary significantly reduces the number of messages and relations an organization must create and manage to integrate applications. This is important because implementing the transformation is the most time-consuming aspect of creating an interface. Figure 3 illustrates the difference for a situation in which five applications manage information about the same business entity. Each line in Figure 3 denotes a relation between applications. The number of relations and messages increases nonlinearly with the number of applications that manage information about the same business entity, i.e. for n applications that manage information about the same business entity, the number of messages and relations arising from point-to-point interfaces is $\frac{n(n-1)}{2}$ [21] (p. 4).

Using canonical messaging is not without challenges. Foremost is the fact that it requires much more design time effort. Domain experts participate to identify the events associated with the business entity that are required now, as well as the events that may be required in the future, for both source and target applications. Data architects participate to reconcile conflicts in semantics and to propose the data structure of the canonical intermediary. Additionally, ESB suites provide varying degrees of support for the creation and management of canonical messages. Some products import XML-based vertical specification such as HL7 (Health Level Seven) and RosettaNet messages and transform the XML into a graphic representation of that message. Some tools will propose (based on property names) a graphical representation of source-to-target associations used in the transformation map. Also, some tools offer registry/repository functionality that is supplemented with asset life cycle management functionality.
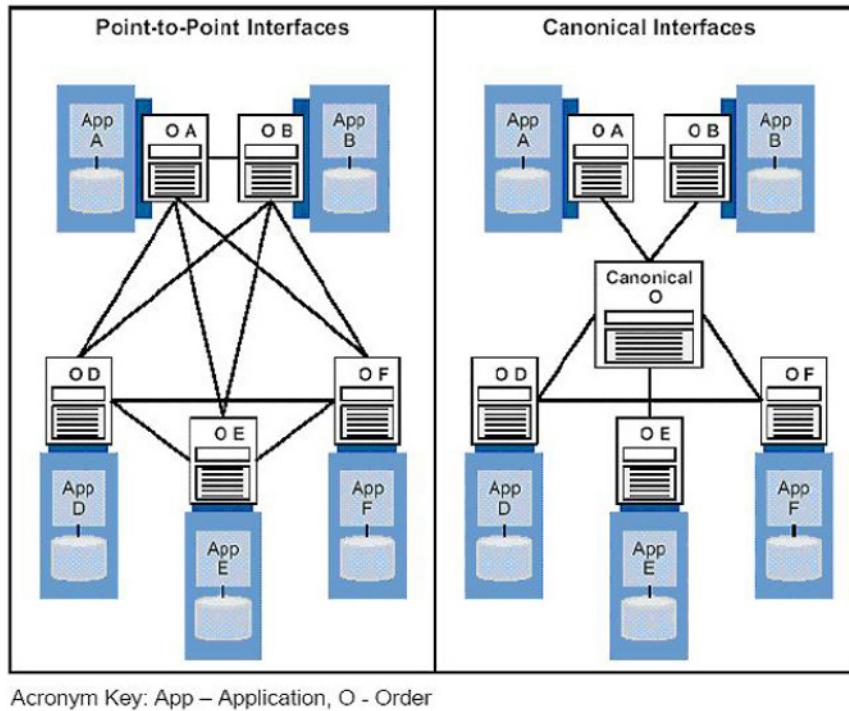
Acronym Key: App – Application, O - Order

Figure 3. A comparison of point-to-point and canonical interfaces, adapted from [21] (p. 4).

4.5. The Use of Canonical Messages

Canonical messages are useful for implementing the data consistency and multistep process application integration pattern. Additionally, the loose coupling created by canonical messages enables applications using the canonical message to be removed and replaced more easily. However, canonical messaging is recommended only for those situations in which information about business entities and their associated events is conveyed across more than four applications. Suppose that n applications share a business entity. If point–to–point messages to convey information across n applications are used, then $\frac{n(n-1)}{2}$ messages are created. Each relation is unique to the application pair between which information is conveyed. In contrast, the use of canonical messaging reduces the number of relations between applications to n through the use of a single canonical message for this scenario. When the number of business entities that are shared across four applications is considered, then the savings grows significantly. If data are being moved between just two applications and the number of sources or targets for this data is unlikely to increase, then there is no advantage in developing a canonical intermediary. In addition to application–to–application integration, canonical messages are frequently used for business–to–business integration [21] (p. 5). They should be used when:

- Conveying the same information with multiple trading partners.

- The number of transformations is large.

- The B2B integration being implemented is strategy or long term.

In addition to data consistency integration, canonical messages are useful when creating business object services. Like canonical messages, business object services are organized around business entities, and expose operations on the data associated with that business entity.

- To provide the greatest potential for reuse, the data exposed by business object services should be assembled from the business entity's properties across all the applications that manage information about that business entity. It

requires establishing a canonical intermediary containing the format, structure and semantics of the intermediary as well as create, retrieve, update, delete (CRUD) functions to manipulate the data of the canonical intermediary.

The aim of the Multilateral Interoperability Programme is to achieve international interoperability of Command and Control Information Systems at all levels from corps to battalion, or lowest appropriate level, in order to support multinational (including NATO), combined and joint operations and the advancement of digitization in the international arena [22] (p. 2).

Figure 4 shows in more details MIP concept based on the use of canonical messages where data are exchanged between commands through staff collaboration and automated information exchange based on canonical messaging. Tactical picture is shared using C2ISs which exchange data using Common Information Model (e.g. Canonical Data Model) and MIP Common Interface (containing shared-message data formats) of MIP solution: specifications, standard operating procedures and documents. Messages and data from sources have to be mapped and transformed into the appropriate canonicals, and then further mapped from the canonicals into the delivery targets in order to achieve effective command and control for operations and common understanding.
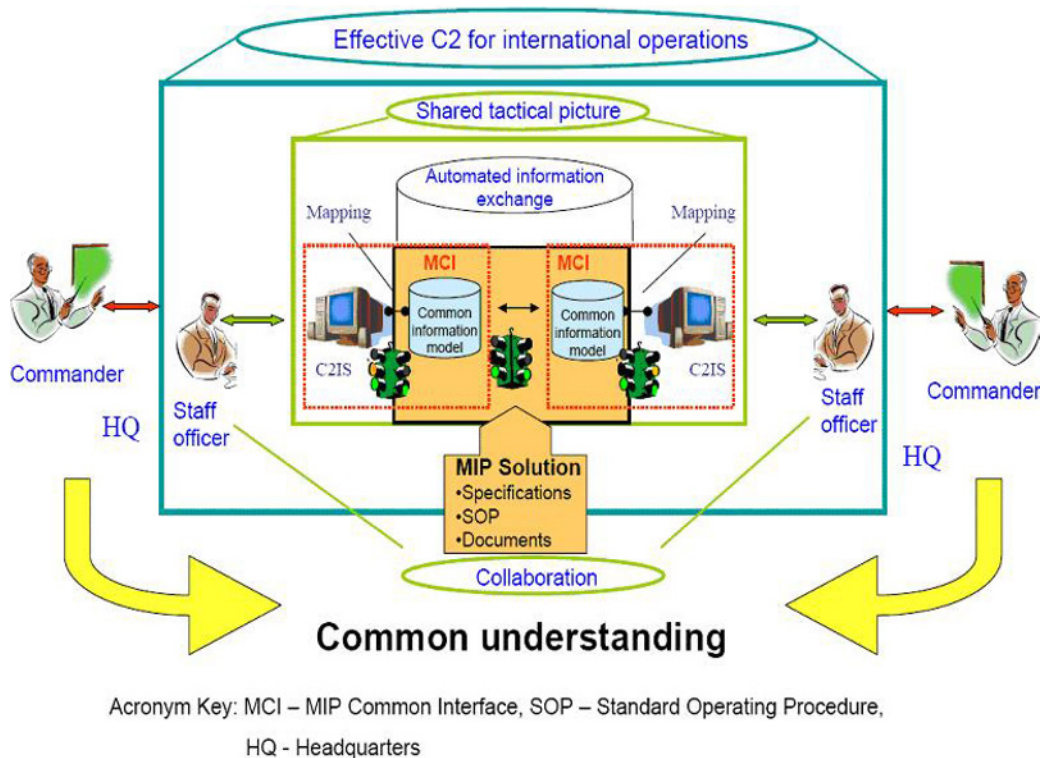

Figure 4. The MIP concept [22] (p. 3).

4.6. MIP Constraints, limitations and mission

Constraints:

- Resources:
    - Time available to work on the MIP specification.
    - Availability of operational and technical human resources.
    - Lack of centralized funding.

- Governance based on consensus.

Limitations:

- A focus on Land interoperability requirements for two reasons:

    – Historical interoperability capability gap in the Land environment.

    – Current operational focus on Land operations.

Mission:
MIP is to further develop and improve interface specifications in order to reduce the interoperability gap between different C2IS.

4.7. MIP Tasks, main products and documents

- Support fielded MIP solutions.

- Further improve the MIP solution by adopting modern development approaches and standards[2].

- Harmonize with NATO and leverage other appropriate concepts, profiles and standards[3].

- Improve flexibility in using the MIP solution in ad-hoc coalitions.

- Extend the scope of MIP interoperability.

- Engage Maritime, Air and other CoIs to cooperate with MIP.

- Examine better ways of structuring the MIP programme.

The main products from the programme are:
The Joint Consultation, Command & Control Information Exchange Data Model (JC3IEDM) promulgated by NATO as STANAG 5525[4].
Documents:

- Operational documents:

    – Instructions on how to use the MIP solution.

    – Record of incorporated Information Exchange Requirements.

    – The programme's Exchange Mechanism specifications and associated procedures.

- Technical documents: Guidance for nations and CoIs on how to implement the MIP specification within the context of their national C2IS.

- Supporting documents: Procedures for testing the MIP specification.

The programme does not include the following aspects of C2IS development:

- National C2IS hardware and software.

- National C2IS software designed to implement and process the MIP specification. However, MIP provides test events to enable nations to evaluate their own systems against MIP specifications.

- Any responsibility for manning and operating national C2IS [16].

---

[2] *Examples of approaches and standards include the NATO Architectural Framework (NAF), Model Driven Development, Service Orientation and common standards (XML, UML, RDF, etc.).*
[3] *Examples include NNEC, APP-11, APP-6, etc.*
[4] *STANAGs are NATO standardized agreements. STANAG 5525 establishes a common data model that NATO nations individually ratify and implement in their own C2IS.*

4.8. Components of MIP

MIP should be understood in the context of its 3 integrated components:

- Organization – An international military data interoperability organization that meets to define common information exchange requirements (IERs), which can be exchanged between different national C2IS.

- Specifications – Delivering an assured capability for interoperability of information. MIP facilitates interoperability through defining/developing common technical standards and associated documentation. MIP intends to further develop and improve interoperability standards in order to support understanding in a common working environment.

- Materiel development
    - A forum for national implementers to synchronize their MIP C2IS material fielding plans.
    - An organization that assists in testing national C2IS in accordance with MIP specifications, which is focused on fielded solutions and iterative development [16].

5. Conclusion

C2IS semantic interoperability is one of the postulates for information superiority acquirement in military. In this contribution approaches to semantic interoperability achievement are analyzed. Some main characteristics of situation awareness (function) and information superiority and common operational picture (arguments) are given. The application of canonical messaging for the semantic interoperability in military is investigated and elaborated and the MIP concept and model based on canonical messaging is presented along with analysis of why and when it should be enforced.

The interoperability of information is essential and an assured capability for this is vital. The successful execution of fast moving operations needs an accelerated decision–action cycle, increased tempo of operations, and the ability to conduct operations simultaneously within combined/multinational formations. Commanders require timely and accurate information. Also, supporting C2 systems need to pass information within and across national and language boundaries. Additionally, forces must interact with non-governmental bodies, and international and national aid organizations. IT must act as a force multiplier to enhance operational effectiveness at each level of command by enabling the sending, receiving, filtering, fusing, and processing of ever-increasing amount of digital information [14].

Organizations that have deployed mediation technology to simplify the creation and management of existing point-to-point interfaces often discover that they have transferred the point–to-point nature of the interfaces into the messaging layer. Using a canonical messaging approach, where appropriate, will substantially reduce and simplify interface transformations (by decreasing the number of transformation maps that an organization must create and manage), which is the most time-consuming aspect of developing interfaces [21] (p. 1).

Due to complexity of the interoperability solution: process (operational), semantic (systems and data) and technical (computers and networks) author seeks appropriate model for C2IS integration, focusing on the semantic interoperability. The role of the DCIO along with the challenges he meets in his endeavor to deploy systems which could lead to information superiority is described as well. In effort to examine the possibilities of information superiority achievement, place and role of MIP are investigated, contributing though to the understanding and knowledge about the interoperability approaches to semantic interoperability in the military.

The MIP programme is not a formal NATO programme. It is a voluntary and independent activity by the participating nations and organizations [15]. In this connection the MIP's approach focused on semantic interoperability of C2ISs, aimed at advancement of Network–Centric Warfare (NCW) which is based on NNEC (NATO Network Enabled Capability) is presented and shortly described. According to The Institute for Defense & Government Advancement (IDGA) [12, 14] MIP was successful in establishing multinational joint C2 common core data standards that can enable and accelerate achieving transformational data strategies for international and national information sharing. MIP's C2 data sharing standard was adopted in 2007 by NATO, as STANAG 5525.

According to the authors' best knowledge MIP is world's unique approach to interoperability in information superiority achievement and military international cooperation. The MIP's approach and solution presents world's military "state of the art" interoperability solution and aims to become the model for information superiority achievement, interconnecting different coalition C2ISs at all levels of command in the network–centric environment.

Acknowledgment

References

[1] Binaghi E., Rampini A., Fuzzy decision making in the classification of multisource remote sensing data, Optical Engineering, 32, 1193–1204, Atlanta, USA, 1993

[2] von Clausewitz C., On War, translated by Howard M., Paret P., Princeton University Press, Princeton, USA, 1989

[3] Clements S.M., The One with the Most Information Wins? The Quest for Information Superiority, Graduate School of Logistics and Acquisition Management, Air Force Institute of Technology, Wright–Patterson Air Force Base, Ohio, USA, 1997

[4] Department of the Air Force (DAF): Basic Aerospace Doctrine of the United States Air Force, II, AFM 1-1. Essay C: Human Factors in War, 17–23, Washington, USA, 1992

[5] Dockery J.T., The Use of Fuzzy Sets in the Analysis of Military Command, In: Decision Information. Ed. Tsokos Ch.P. , Thrall R.M. , Academic Press, New York, USA, 1990

[6] Dreyfuss C., Maurer W., Cohen L., Business Value of Services in Sourcing Initiatives, Gartner, Inc., 2008

[7] Friedman T., Data Integration Hubs: Drivers, Benefits and Challenges of an Increasingly Popular Implementation Approach, Gartner, Inc., 2011

[8] Gartner Executive Program: IT Strategy: A CIO Success Kit , Gartner, Inc., USA, 2009

[9] Galinec D., Ferek-Jambrek B. (2008): Process Transformation for Reaching Agility: Chief Information Officer Role, In: Proceedings, CECIIS 19th International Conference 2008, Faculty of Organization and Informatics, Varaždin, 317–324, 2008

[10] Gompert D.C., Lachow I., Perkins J., Battle-Wise: Seeking Time-Information Superiority in Networked Warfare, Center for Technology and National Security Policy National Defense University, Washington D.C., USA, 2006

[11] Institute of Electrical and Electronics Engineers: Interoperability, IEEE Glossary, http://www.ieee.org/education_careers/education/standards/standards_glossary.html#sect9, Accessed: 15th December 2011

[12] The Institute for Defense & Government Advancement (IDGA): About IDGA, available at http://www.idga.org/, Accessed: 29th June 2009

[13] James G.A., Managing Multiplying Messages, Gartner, Inc., 2002

[14] Multilateral Interoperability Programme (MIP): Interoperability, available at http://www.mip-site.org/, Accessed: 30th June 2009

[15] Multilateral Interoperability Programme (MIP): MIP Organisation, available at https://mipsite.lsec.dnd.ca/Pages/MIPOrganisation.aspx, Accessed: 27th September 2011

[16] Multilateral Interoperability Programme (MIP): MIP Vision & SCOPE (MV&S), PMG Edition 6.3, Montebello, Canada, 2009

[17] Newman D., Reimagining Enterprise Information Architecture: Improve Information Sharing Through Interoperability by Design, Gartner, Inc., USA, 2011

[18] Ringdahl B., Improving Business Processes Executive Summary for Defense Sector – May 2009 EXP Report, Gartner, Inc., USA, 2009

[19] Robertson B., Enterprise Architecture Research Index: Integrating EA with Business Strategy, Gartner, Inc., 2009

[20] Swiss Sociological Association: "Identity and organization" Workshop, available at http://www.inderscience.com/mapper.php?id=116, Accessed: 29th June 2009

[21] Thompson J., Lheureux B. J., How a Canonical Messaging Approach Can Help You Simplify and Reduce Interface Assets, Gartner, Inc., USA, 2011

[22] Uekermann R., Multilateral Interoperability Programme (MIP) Concept: Meeting of Subject Matter Experts, IT-AmtBw D2 VorhV MIP, Koblenz, DE, 2007

[23] US Department of Defense: DOD Dictionary of Military and Associated Terms, Joint Chiefs of Staff (JCS), Washington D.C., USA, 2009

[24] US Department of Defense: National Military Strategy of the United States, Joint Chiefs of Staff (JCS), Washington D.C., USA, 2004