COALITION C2 INTEROPERABILITY CHALLENGES

Peter Gorm Larsen
Systematic Software Engineering, Søren Frichsvej 39, DK 8000 Aarhus C, Denmark

ABSTRACT

When military operations are carried out it is essential to be able to share information important for executing the operation in the most efficient fashion. This has always been a challenge even when single country or a single service was involved. However, with the increased focus on asymmetric warfare and the need to gain international political acceptance for military operations coalitions must traditionally be established. As a consequence the challenge for ensuring interoperability between the involved stakeholders has been raised to a higher and more complex level. Different technology providers have advocated for very different solutions as a response to this challenge. However, we believe that there is no silver bullet for this kind of interoperability. The fact of the matter is that there are various ways to exchange and share information and all have pros and cons. This paper describes the various information sharing and exchange techniques currently used and discussed in the military and their relative differences. Knowledge is essential to any rational discussion on interoperability technologies and approaches. This paper attempts to provide that knowledge as an update to [18].

INTRODUCTION

Many organizations and projects around the world are trying to define Network Centric Warfare (NCW) and more importantly how to implement NCW [6][7][17]. Similar concepts have been developed by an ever growing number of nations under names such as Network Enabled Capability (NEC) and Network Based Operations (NBO). From the industry side similar interest exists in getting to a common understanding of how the gains from this promising concept may be achieved [25]. In this paper we will consistently refer to any of these with network centric thinking as NCW. To understand the importance of mastering interoperability in order to get this operational let us start by quoting Supreme Allied Commander – Transformation, Admiral E.P. Giambastiani:

> *"The provision of enabling technology to provide for the seamless exchange of information is critical. Interoperability and interconnectivity will be the key enablers to achieve decision superiority."*

At a high level, implementation of NCW can be split into two types of challenges:

- Revising doctrines and procedures (SOPs) and
- Implementing the means for communicating data between all necessary platforms and systems.

The first challenge must be agreed upon across joint, combined and coalition forces. This needed doctrine includes important issues about who wishes to share what information with whom. In a coalition this is a major challenge because of potential different doctrines operated under by the different coalition forces. The presence of this distributed information creates a considerable amount of security-related issues that then also must be resolved in particular in joint, combined and coalition settings. It is also essential to understand that information sharing does not mean that everybody knows everything or even that everyone should browse for everything. It is easy to cross rather rapidly from information access to information overflow. Instead it is paramount to have the right information available and accessed by the right people at the right time. In order to capture the concept of Communities of Interest (COIs) have been introduced. A COI is a collaborative group of users who exchange information for their shared goals, interests, missions or business processes.

This paper is focused on the second challenge (implementing means for communicating data) in ways that both support the first challenge (abiding by doctrine) and support proper availability of information. In general it is

possible to define different levels of information system interoperability going from level 0 with a man-in-the-loop to level 4 where the entire enterprise is able to exchange information between domains [1]. The levels are:

- **Level 0** – Isolated interoperability in a manual environment between stand-alone systems: Interoperability at this level consists of the manual extraction and integration of data from multiple systems. This is sometimes called "sneaker-net."
- **Level 1** – Connected interoperability in a peer-to-peer environment: This relies on electronic links with some form of simple electronic exchange of data. Simple, homogeneous data types, such as voice, text email, and graphics (e.g., Graphic Interface Format files) are shared. There is little capacity to fuse information.
- **Level 2** – Functional interoperability in a distributed environment: Systems reside on local area networks that allow data to be passed from system to system. This level provides for increasingly complex media exchanges. Logical data models are shared across systems. Data is generally heterogeneous-containing information from many simple formats fused together (e.g., images with annotations).
- **Level 3** – Domain based interoperability in an integrated environment. Systems are connected via wide area networks. Information is exchanged between independent applications using shared domain-based data models. This level enables common business rules and processes as well as direct database-to-database interactions. It also supports group collaboration on fused information.
- **Level 4** – Enterprise-based interoperability in a universal environment: Systems are capable of using a global information space across multiple domains. Multiple users can access complex data simultaneously. Data and applications are fully shared and distributed. Advanced forms of collaboration are possible. Data has a common interpretation regardless of format.

In this paper we will not go into a debate about these because we believe that in order to achieve the NCW vision level 4 is needed.

From a technical perspective, a simple solution would be to look at all the Information Exchange solutions we have today, like military messaging, common data models, tactical data links, etc., and then pick one of them as being the "NCW enabler" that all systems employed in a coalition should implement.

The problem with this approach is that each of these solutions has their pros and cons and there is not a single one of them that solves all the communication challenges in a NCW scenario. Each of the existing solutions also have an origin from one of the military services and thus the other services may be reluctant to just take it over without adjusting it to fit their needs.

The second choice could then be to design and implement a completely new solution that solves all the communication challenges in a NCW coalition scenario. The downside to this solution is that it will be very expensive because all existing systems will have to implement this new Information Exchange solution.

The third and most realistic choice is a combination, i.e. implementing solution(s) that allow flexibility for integration with existing operational systems. This means to evolutionary upgrade to the existing systems in such a way that reuse of information exchange standards and paradigms are made to the extent where it makes financial sense given the user needs.

This introduction is followed by a small example illustrating the desired interoperability for coalition operations. This is followed by a section on the fundamentals for establishing such interoperability. Afterwards three sections explain the different leading paradigms for exchanging such information today. Another section is then used to discuss pros and cons of these different paradigms. Then a section demonstrates what the company Systematic Software Engineering has been providing in the area of military interoperability so far. Finally a few sections are devoted new potential paradigms to be used in the future and some concluding remarks are given.

A SMALL EXAMPLE

In order to get a better common feel for the interoperability challenge a small simple example will be presented. Imagine we have a flying sensor (e.g. a NATO AWACS) that has derived more information about the

situation on ground than a given allied ground-based shooter has access to. Commanding the shooter to take action and fire against a new target naturally needs to follow the order of engagement and the doctrines operated under. However, there is no doubt that from an allied or coalition force perspective it would be advantageous to be able to provide the ground-based shooter with the best possible awareness about the situation.

The communication challenge is to find out how to enable this exchange of information to occur in a fashion where the sensor and the shooter agree upon the semantics of the data exchanged between them somehow. Conceptually this may seem very simple but it is inherently complex because there are many ways in which this exchange can occur and there are many different standard data formats that are used by the different platforms. When more military services are involved in a coalition, more stakeholders and more platforms are considered the overall complexity is increased by orders of magnitude.

FUNDAMENTALS

Traditionally, whenever the development of a new military platform is initiated an interoperability analysis is conducted in order to clarify what the information exchange requirements are towards other existing platforms. However, history shows that over time these requirements are likely to change. This implies that expensive updates must be made to these platforms to accommodate for new information exchanges requirements to be enabled.

In a NCW setting, the underlying assumption is that a network like the Global Information Grid (GIG) [3] exists where all different platforms can connect as nodes in a network and share information with the other nodes. However, physically hooking up to a network does not imply that the different systems “by magic” will be able to unambiguously exchange the necessary information with each other. In order to achieve full interoperability it is necessary that each system have a common understanding of the semantics of the data exchanged.

In order to enable the dissemination of information to friendly forces in a fast manner, NCW advocates that friendly units can make use of the GIG to get hold of desired information without necessarily knowing who provided the information.

In order to achieve information exchange there is a number of fundamental things that need to be brought into place, going up different layers:

1. Physical layer (Combat radio, Ethernet, etc.);
2. Protocol (TCP/IP, X.400, etc.);
3. Data structure;
4. Semantic understanding of data.

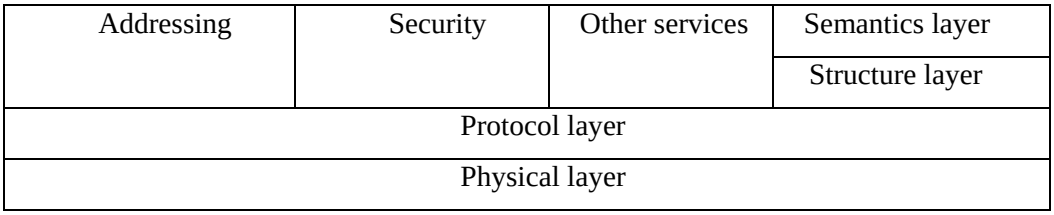

Figure 1. Interoperability Layers

These four layers are illustrated in Figure 1. In order to exchange any data at all, layer 1 and 2 are prerequisites. These layers are important to establish reliable connectivity between the different communicating nodes. The different interoperability paradigms have different approaches for initializing the addresses that can be used for exchanging information. It is also worth noting here that the technological improvement in IPv6 (Internet Protocol version 6) is likely to eventually become the standard to be used throughout the defense infrastructure at layer 2. However the focus of this paper is being able to exchange structured data that is interpreted the same way by the sender and the receiver, i.e. they have the same semantic understanding of the structured data.

Numerous standards have been introduced in the defense context in order to achieve a common understanding of the structured data. However, these standards evolve over time and different platforms may not support the

full standard and as a consequence even using standards for exchanging information may not solve the interoperability challenge. In particular funding of the various different platforms is not synchronized and as a result multiple baselines for each standard will be operational at the same time. This results in potential interoperability problems.

Below three different paradigms for exchanging information in a defense context are considered from an historical perspective and the pros and cons for each of them are discussed.

MILITARY MESSAGING

Instead of using personal-based email solutions an organizational approach has been invented for military messaging. Historically military messaging dates back to the earliest days of teleprinter equipment when protocol standards such as ACP127 were developed for the protocol layer. With the emergence of commercial standards such as X.400, the defense market adopted this standard and extended it to form ACP123/STANAG4406. Many nations have or are in the process of implementing systems that are compliant with this for military messaging. So historically military messaging originally was based on principles for unambiguous communication between people rather than systems, but subsequently it has also been used automatically between systems.

For the exchange of military messages within the NATO community, networks, such as NICS TARE (NATO Integrated Communications Systems Terminal Relay Equipment) and NMS (NATO Messaging System), are established to ensure the safe exchange of messages between NATO headquarters and member nations.

Systems supporting military messages need to guarantee a number of critical requirements due to the mission critical nature of the nature of the information exchanged. This includes:

- Survivability;
- Proof of sender's identity;
- Proof of delivery;
- Content integrity;
- Non-disclosure.

On top of platforms like those mentioned above different standards have been defined for Message Text Formats (MTFs). Each of these standards defines the precise syntax and rules for formatting messages in a structured form. Most of these standards are textual based. The three most well known standards today are:

- **USMTF**: This was the first MTF to be defined and it is being maintained by DISA (Defense Information Systems Agency) in the US.
- **ADatP-3**: This is the NATO standard MTF format being maintained by NATO's Information Exchange Systems Branch and NATO Standardisation Agency.
- **OTH-Gold**: This is an MTF standard maintained by the US Navy Center for Tactical Systems Interoperability.

MTF's are semantically complete messages making it easy to implement either manual or automatic validation of whether the information in a given message can be released from a security point of view.

More recently XML variants for each of these standards have been produced. The advantage of the XML variants is that the plethora of tools supporting XML can be used. However, from a bandwidth perspective the XML variants are less attractive because the messages are significant larger when wrapped inside XML. Recent work has made progress here by experimenting with using binary encoding of XML data and in that way limit the bandwidth problems with XML representation of data [26].

Each of these standards exists in different versions (called baselines) and each of the systems automatically processing such baselines need to go through a formal certification process ensuring conformance. Products exist that can manage the simultaneous use of multiple baselines and thus have the advantage of enabling a loose coupling between the systems [15].

The nature of information exchanged using military messaging is mostly high-level commands, orders and situation awareness. Thus, military messaging is typically used for non-real-time exchanges. However, the interoperability using military messaging principles are still increasing which SAP's recent interest in the exchange of AdatP-3 messaging for logistic purposes also demonstrates [30].

COMMON DATA MODELS

The Multilateral Interoperability Programme (MIP) [5] was initiated to support coalition forces with multinational combined and joint military operations. The origin for this work was the army side, but significant efforts have been made to extend that to the other military services as well. In MIP a definition has been made for a common data model called "Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM)"[1]. This is a common data model that is used to exchange information between the command and control systems about plans, orders and situation awareness from different nations. The exchange is made using MIP Data Exchange Mechanism (MIP DEM) which essentially is a contract-based protocol that automatically replicated updates in the common data model to the parties identified in the contracts. The contracts express constraints about with whom different parts of the information will be shared.

Historically the MIP initiative started off as a voluntary, independent activity in 1998 with six countries that wished to tackle the interoperability between the army from different nations. In 2002 the Army Tactical Command and Control Systems (ATCCIS) was merged with MIP. In 2004 the data modeling activities in the NATO Data Administration Group (NDAG) joined the data modellers in MIP resulting in the JC3IEDM. Today there are 26 different countries involved in MIP. In September 2005 the US military acceptance of the C2IDM standard was also endorsed by Lieutenant General James J. Lovelace.

From a functional perspective the JC3IEDM data model includes a modular approach that can be used to filter the types of data that are exchanged. However, since it is exchanging information using database replication it also means that the coupling is close in the sense that all parties in an exchange must refer to the same "common" data model. In order to optimize the use of bandwidth this also means that the updates themselves are not necessarily semantically complete. This also means that it can be distributed to the different nodes in near real-time.

One of the principles in the JC3IEDM is to store the full history making it a kind of "war-diary" as well, which means that data stored in JC3IEDM format will keep growing, so systems need an archiving mechanism to keep running.

TACTICAL DATA LINKS

Tactical Data Links (TDLs) have been used for many years for exchange of tactical command and control functionality as well as for near real-time exchange of information about the situation awareness. In order to be able to support encryption and jamming resistance modern TDLs such as Link 16 [4] cover all the four layers from Figure 1 above in a fixed non-modular solution including expensive hardware terminals. Typically the physically layer is limited to Line Of Sight (LOS) although relaying is possible for some TDLs.

The terminals used for TDLs are basically radios that broadcast information to the other systems in the same network participation group. Thus, using TDLs there is no history logged about what happened and this makes good sense when the newest information is the only relevant information.

The messages communicated over TDL's are divided into different families and the J-series family of messages (covering VMF, Link 16 and in the future Link 22) is the most well-known. In Figure 2 it is illustrated how the roadmap is for the J-series family including requirements from other older TDLs are fed into the J-series family. Note that the origin for VMF is the army; the origin for Link 16 is the air force whereas the origin for Link 22 is the navy (as a successor of Link 11).

J-series is the TDL that is expected to be most used in a NCW setting in the future. In order to support near real-time exchange of data within a limited bandwidth the messages exchanged over TDLs are binary-encoded.

[1] Note that the currently used draft for this is called C2IEDM Edition 6.1.5e (C2 Information Exchange Data Model) and that is the version that is currently used for events such as CWID [20] to demonstrate the strengths of this technology between coalition forces.

Since almost all platforms only support a subset of for example Link 16 this provides significant interoperability problems between platforms. Thus, if a system is able to understand Link 16 there is no guarantee that it will be able to understand the Link 16 messages provided by a different platform.

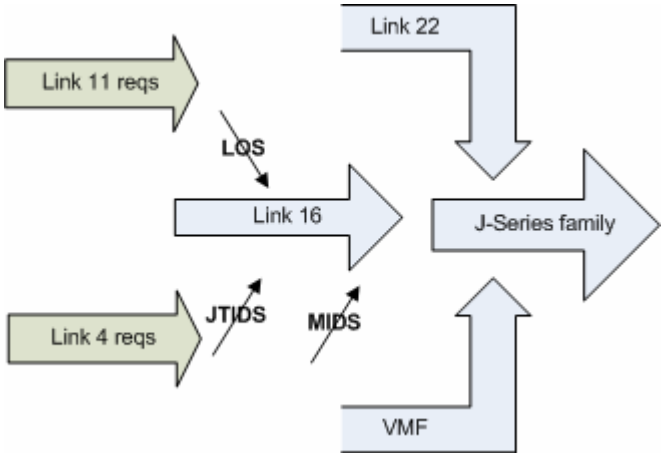

Figure 2. TDL roadmap

PROS AND CONS

Having presented three different paradigms for exchanging information in a defense context Table 1 below summarize the findings above.

Paradigm	Pros	Cons
Messaging	Loose coupling Manual security Proper baselines	Not real time Alternative standards Man-in-the-loop
Data model	Modularity Near real-time	Closer coupling Data size keeps growing, Full history
Data link	Near real time Jamming resistant	Lack of modularity Expensive Lack of baselines

Table 1: Pros and cons for interoperability

As it can be seen from Table 1 above messaging gives a looser coupling between the communicating entities and because messages communication are semantically complete it is easier to define manual security filters filtering messages out. In the MTF community there has always been a proper handling of baselines which is an advantage when different entities use different baselines. On the negative side MTF's have typically not been exchanged in real-time because it has typically involved a man-in-the loop. It is also a concern that different standards exists although tools may ease dealing with that in a coalition context.

For the common data models we have a closer coupling because the databases must have the same structure, but on the other hand more modularity is enabled. Traditionally the exchange of such data models have been more real-time and only deltas may be exchanged. We consider it a disadvantage that the standard prescribes that the full history must be preserved because this means in principle that the overall data size keeps growing.

Finally the tactical data links have had an exchange of data that is near real time from its birth and some of them are made jamming resistance and the cost of modularity (all layers are combined in the same TDMA

schedule principle). The major disadvantages here is the lack of dealing with baselines and subsets in a proper manner and then TDLs have always been relatively expensive compared to the alternative paradigms.

SYSTEMATIC SOFTWARE ENGINERRING

For more than a decade Systematic Software Engineering has been a leading provider of interoperability solutions for defense forces all over the world. Historically this started off with support for various standards in the area of military messaging. The original IRIS messaging solution developed with integration for common popular email systems in the IRIS Organisational Messaging product [15] and today this technology is used by 26 countries in the world and it is virtually the de facto standard for military messaging in the NATO region. The IRIS messaging solution is a collection of tools used to define and automatically process structured military messages. These tools are able to handle a range of international standards supporting operations from the highest echelon HQs down to tactical combat radio based environments. In fact the main standards (USMTF and ADatP-3) are being maintained and further developed using one of these tools. From a coalition interoperability perspective the main asset in this tool suite is the ability to be able to support multiple baselines for multiple MTFs simultaneously. This enables coalition forces using different baselines of MTFs to unambiguously exchange information between each other.

In the area of common data models Systematic Software Engineering have been involved in the MIP programme virtually from the beginning. Here the IRIS Replication Mechanism IRM [16] is able to perform near-real-time sharing of large amounts of information between military organizations in a coalition. Systematic Software Engineering also provides a MIP Gateway that makes it easy to integrate with a national C2 system, as illustrated in Figure 3.

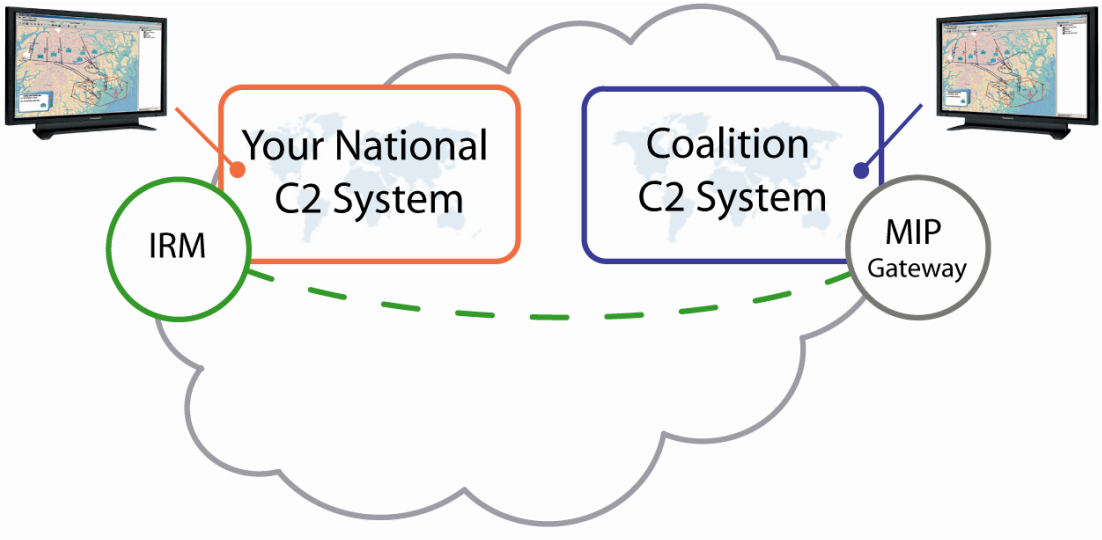

Figure 3: IRM - MIP Integration

Using a contract-based approach the different countries agree about what information they wish to automatically share with which other countries. The coalition interoperability is tested yearly at MIP Test events and IRM is the product used most widely among the national C2 solutions. More recently progress has been made in compressing the messages exchanged for example making it viable to exchange target information between tanks over low-bandwidth tactical radios. In order to ease the data mapping between the standard C2IEDM standard format and formats used inside national systems the IRIS product suite also contains the IRIS Mapping Tool (IMT).

In the area of TDL's Systematic Software Engineering have assisted the Danish Armed Forces for many years in integrating such messages into their C2 systems. More recently Systematic Software Engineering has become involved in the development of Link 16 software for the Joint Strike Fighter aircraft. Ideally the know-how built-up over the years for mastering multiple baselines inside Systematic Software Engineering may be

able to improve the future implementations of TDLs such that a higher level of interoperability between coalition platforms can be achieved.

Finally it is worthwhile mentioning that Systematic Software Engineering provides a C2 framework called SitaWare that can cheaply be integrated with national command and control systems that is closely integrated with the different interoperability solutions mentioned in this section.

WEB SERVICES

One of the modern technologies that recently have found its way from the civil sector into the defense world is web services [10][12]. This is an enabling technology for the more general Service Oriented Architecture (SOA) that is the overarching architectural approach [11]. SOA is a system architecture that is based on services that enable consumers to extract information via these services whenever needed. The main advantage about SOA is the loose coupling that makes it easy to accommodate changes in the future usage.

SOA includes technologies called UDDI (Universal Description, Discovery and Integration) and WSDL (Web Service Description Language) that enables users to publish and find providers of information that is important for the consumer at a given point of time.

The protocol used for exchanging information with web services is called “Simple Access Object Protocol” (SOAP) [14]. The data format used inside SOAP is XML. However, web services are at the syntactic level, and thus it is still necessary to agree upon the semantics of the structured data that is delivered by the services. Thus, here it is easy to imagine that the structured data formats in military messaging, common data models as well as the message formats from TDLs can be the data formats wrapped inside XML used for the web services. In this way the semantics of the exchanged data is defined by the legacy standards.

Thus, instead of using the database replication protocol currently used in the MIP community it is possible to imagine the same data elements to be exchanged via web services. The same holds for the military messages where the XML variants of the different military standards could be used as the exchange message formats used by web services instead of them being sent over mail protocols.

On the other hand in situations where you wish to be able to subscribe to some kind of live feed in order to have a near real-time situation display on your console TDLs or MIP replication would be you choice.

In the same way the concepts for contract-based exchange of information could be enabled using web services for other types of data exchange mechanisms. This is already started for the Battle Management Language (BML) [13] that has provided web services access to an older version of JC3IEDM [28]. This also shows how the simulation community is gaining interest in the interoperability of command and control systems.

Recently US government initiatives aiming at more systematical acquisition of systems that are prepared for a network centric thinking has been initiated and this is to a large extend based on SOA ideas [19].

SEMANTIC WEB AND ONTOLOGY

A new promising technology that is beginning to find its way into defense applications is called semantic web [9]. Semantic web is suggested as a way to achieve better and easier interoperability, without the need of common data models. The main advantage from an interoperability point of view is the concept of ontology that can be used for semantically linking different data together [8]. In the future this may be one approach for bridging the gap between different dialects of military standards. This has for example been experimented with in a NATO net centric setting as well as for the JC3IEDM data model mentioned above [27]. It is envisaged that semantic web may be easier to manage than changing data models, but this still has to be demonstrated in real life [29].

IS IT POSSIBLE TO MAKE A WONDERBOX?

When information is available in different formats an alternative to getting the systems to agree upon the right format to use could potentially be to have an automatic mapping from one format to the other. Generalizing this one can conceptually imagine a “wonderbox” that has services that are capable of transforming between the differing formats. This is a fascinating concept but naturally it also has a number of challenges to be able to work in the desired fashion. These include:

- How will the wonderbox be able to accommodate different low-level protocols?
- What to do with lack of field data in the incoming data format?
- What to do with data that are not semantically complete, but needs to be aggregated from more sources?
- Will it be possible to use the wonderbox with near real-time exchange of data?

In the civil sector COTS products exist today for enterprise integration and it is plausible that this technology and the experience gained in producing it that an interoperability wonderbox can be produced for use in the defence sector.

It is probably going to take some time before we are going to see a fully-fletched wonderbox. However, companies like Systematic Software Engineering are gradually building up insights in producing parts of the full solution such that it is possible that it will be reality in the future.

ADVANCED CONCEPT TECHNOLOGY DEMONSTRATION PROJECTS

In order to make evolutionary progress with respect to interoperability the US Department of Defense have traditionally carried out Advanced Concept Technology Demonstration (CSDT) projects. At the moment Systematic Software Engineering is involved with three of these projects in an interoperability setting. Since these projects are examples of the kinds of initiatives we believe are necessary in order to enhance the interoperability between coalition forces we will briefly mention these three:

THE COSMOS PROJECT

The COSMOS (Coalition Secure Management and Operations System) project [22] is centered around setting up a Joint Task Force (JTF) quickly enabling the sharing of essential information among the coalition partners. This covers all stages of coalition operations including planning, deployment, execution and redeployment. In order to enable sharing of data between independent coalition Command and Control systems the C2IEDM standard is used with the Systematic products SitaWare and IRM supporting that.

THE ASAP PROJECT

The ASAP (Actionable Situational Awareness Pull) project [23] aims to design, develop integrate and demonstrate transition software that provides a “smart pull” capability to the tactical, operational and/or a strategic user on the GIG. It is important that it is easy for the Communities of Interest to get access to the necessary information in a timely fashion. In order to do this web services are employed over the SIPRNET. Just like for the COSMOS project the C2IEDM standard and the SitaWare, IMT and IRM products are being used.

THE FCT PROJECT

The FCT (Foreign Comparative Testing) project [24] is established to enable the adoption of foreign products that may do things better faster and/or cheaper. In this project Systematic Software Engineering provides SitaWare as a competitor to US Army designed solutions and it is believed that products such as this that has a proven track record for more countries will enhance the overall coalition interoperability.

CONCLUDING REMARKS

As have been demonstrated there is at present no single silver bullet for information sharing and interoperability. In addition it is not simply a technical challenge; it also requires doctrine considerations to achieve the optimal sharing of information among coalition forces. However, there is a tendency of convergence towards fewer standards, and this may improve the interoperability in the future. This tendency has specifically been demonstrated both in the MIP replication context (where the older ATCCIS and NDAG data models no longer exists) and the TDL context (where Link 1, Link 4 and Link 11/11B are expected to disappear eventually).

We strongly believe that instead of reinventing the wheel it may make good sense to consider what is out there today operationally and then in addition consider the innovations made in the civil sector for inspiration.

We believe that the interoperability capabilities should be based on standards as well as driven by the operational needs of the users. In Figure 4 a conceptual overview of our envisaged interoperability approach is shown. It includes both legacy military messaging, legacy TDLs and it is envisaged that common data models

will be used as the central repository of information. Whether the same common data model is used internally in the national systems or they will be based on a legacy data model will differ from case to case based on the cost of changing the legacy data model versus mapping between the common data model and the legacy data model. We also envisage that principles from SOA including web services will be used to exchange information with the repository. If the wonderbox concept is able to demonstrate its use in an operational concept we believe that would be a part of the equation as well.

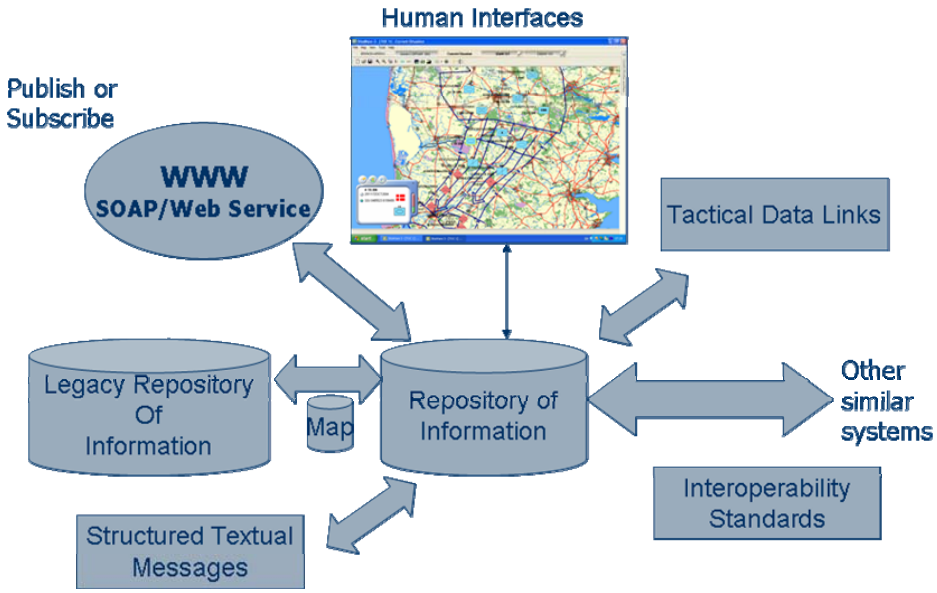

Figure 4: Envisaged overall interoperability approach

From a technical perspective it is necessary to master all the different interoperability technologies and approaches and knowing when to apply what judging from pros and cons for the different alternatives.

REFERENCES

[1] System of Systems Interoperability, E. Morris et al, Technical report, CMU/SEI-2004-TR-004, http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr004.pdf.

[2] NATO C3 Technical Architecture (NC3TA) Reference Model for Interoperability, The Hague, NL, 2003.

[3] Global Information Grid (GIG) Capstone Requirements Document, Washington, DC, 2001.

[4] Tactical Data Exchange – Link 16, STANAG 5516, edition 3.

[5] Multilateral Interoperability Programme Web Site: http://www.mip-site.org/home.htm.

[6] Network Centric Warfare Developing and Leveraging Information Superiority by David S. Alberts, John J. Garseka and Frederick P. Stein, http://www.dodccrp.org/publications/pdf/Alberts_NCW.pdf.

[7] Power to the Edge – Command, Control in the Information Age, David S. Alberts and Richard E. Hayes, http://www.dodccrp.org/publications/pdf/Alberts_Power.pdf.

[8] W3C, OWL Web Ontology Language, http://www.w3.org/TR/owl-features/.

[9] The Semantic Web Community Portal, http://www.w3.org/2001/sw/.

[10] Understanding SOA with web services, E. Newcomer and E. Lomow, Prentice-Hall.

[11] Zapthink, XML, web services and service orientation, http://www.zapthink.com/.

[12] Web Services Interoperability organization, http://www.ws-i.org/.

[13] Standardizing Battle Management Language – Facilitating Coalition Interoperability, S.A. Carey, M.S Kleiner, M.R. Heib, R. Brown, http://www.alionscience.com/pdf/Battle_Management.pdf.

[14] SOAP version 1.2, Part 1 Messaging Framework, http://www.w3.org/TR/soap12-part1/.

[15] IRIS Organisational Messaging - The Complete Military Messaging Desktop, http://www.systematic.dk/UK/Products/IOM+for+Outlook/.

[16] Sharing Information with IRIS Replication Mechanism, http://www.systematic.dk/UK/Products/IRM/.

[17] Net-Centric Vision for our Products, http://systematic.dk/uk/products/net-centric+vision/.

[18] Untangling Technology Debates on Information Sharing and Interoperability by F.D. Jørgensen, P.G. Larsen, J.M. Stadtmueller, MILCOM'05, October 2005, New Jersey.

[19] Net-centric Enterprise Solutions for Interoperability, US Department of the Navy, http://nesipublic.spawar.navy.mil/

[20] Coalition Warrior Interoperability Demonstration, 2006, http://www.cwid.js.mil/c/extranet/home.

[21] Network-Centric Warfare, http://www.oft.osd.mil/library/library_files/document_318_NCW_GateFold-Pages.pdf.

[22] The COSMOS (Coalition Secure Management and Operations System) Project, http://www.les.disa.mil/c/extranet/home?e_l_id=32.

[23] The ASAP (Actionable Situational Awareness Pull) Project, http://www.les.disa.mil/c/extranet/home?e_l_id=54.

[24] The FCT (Foreign Comparative Testing) Project, http://www.dtic.mil/ndia/marketplace/palmer.pdf.

[25] NCOIC (Network Centric Operations Industry Consortium), http://www.ncoic.org/home.

[26] Towards Binary XML for Military Messaging, Bjørn Reese, from XML for Binary Interchange: Addressing Machine-to-Machine Interoperability & Tactical and Mobile Computing, September 2004, http://www.mitre.org/news/events/xml4bin/pdf/systematic.pdf.

[27] Semantic Interoperability MOVES Research Agenda, Curtis Blais, https://www.movesinstitute.org/openhouse2005/presentations/Blais03.pdf

[28] Web Services based on the C2IEDM – Data Mediation and Data Storage, Andreas Tolk, Saikou Diallo, Kevin Dupigny, Bo Sun and Chuck Turnitsa, 2005 Spring Simulation Interoperability Workshop, April, 2005.

[29] Towards a Formal Ontology for Military Operations, Eric Dorion, Christopher Matheus and Mieczyslaw Kokar, 10th International Command & Control Research and Technology Symposium, 2005.

[30] Coalition Warrior Interoperability Demonstration, SAP, http://www.sap.com/industries/defense-security/pdf/CS_Coalition_Warrior.pdf.