Laying the Foundation for Coalition Interoperability through NATO's C3 Technical Architecture

Frederick I. Moxley, Ph.D.
Defense Information Systems Agency
5600 Columbia Pike
Falls Church, Virginia 22041, USA
moxleyf@ncr.disa.mil

Lucien Simon
NATO C3 Agency
Rue de Geneve 8
B-1140 Brussels, BE
lucien.simon@nc3a.nato.int

Elbert J. Wells
U.S. Mission to NATO
Autoroute de Zaventem
1110 Brussels, BE
ewells@mailsrv2.mitre.org

Abstract

Current projections indicate that in the future, the ability to share information between military systems will ultimately determine whether or not a mission will be a success or a failure. Based on the probability that conflicts will continue to occur involving allied command structures that utilize diverse information systems, it has been surmised that information interoperability will be the crucial factor for success when conducting future combined and joint military operations. This paper describes an architectural approach that lays the structural foundation necessary to attain interoperability between diverse C3 systems and provides the rationale on why this approach has been proposed for use throughout NATO.

Introduction

NATO has recognized that future military information systems will need to interoperate with one another more effectively than ever before[1]. Unforseen contingencies and international conflicts have elevated the need to provide accurate information to the warfighter upon demand, i.e., wherever and whenever needed.

However, in order to make this a reality, coalition information system services of the future will need to be fused together, having the ability to retain their own national identities and operational independence, as well as interoperate with one another in a more effective and seamless manner.

Unfortunately, achieving and sustaining interoperability among diverse systems is not, nor has it ever been an easily attainable objective. As indicated by [Wentz, 1997], historically speaking, interoperability has been one of the most difficult areas to deal with.

Interoperability is a broad and complex area of endeavor that cuts across many functional domain areas and applications. Often deemed elusive due to the level of complexity entailed when integrating diverse system components together, the real challenge lies in the overall scope and extent of the system, as well as the level of interoperability and integration so desired [Moxley, 1996].

Nevertheless, Integrating diverse military system components cohesively together within a coalition environment can add significantly to the level of complexity entailed. For instance, when different parts of a system are built separately by independent developers, the end results often vary greatly. This is often attributed to flaws in the design

[1] See item 4 of the *Defense Capabilities Initiative* issued during the Washington Summit on 23-24 April 1999.

specification and/or how it has been interpreted during various stages of system development.

The term used synonymously with design specification today is architectural design. The architectural design is concerned with determining the architectural style of the system as opposed to the detailed design of individual algorithms and data stores. Architectural design also involves the high-level decomposition of the system into components and the relationships and interactions of these components which usually determines the specific architecture of the system [Moxley, 1996]. If misinterpreted or designed poorly, chances are the system(s) once fielded will function improperly as well.

When put in the context of a coalition environment, the ratio for failure increases significantly due to the sheer number of diverse factors that must be taken into account and reckoned with accordingly (e.g., language differences, level of training, number of system developers and integrators involved, type of experience, etc.).

Architectural Views & Interoperability

In 1996, the U.S. Department of Defense (DoD) first introduced the concept of architectural views under the guise of a C4ISR Architecture Framework[2]. Known independently as the Operational, System, and Technical architectural views. All three views, when logically combined together, expanded on the de facto definition pertaining to architecture within the realm of information technology[3]. Up until that time, there had been no common approach for architectural development throughout the U.S. DoD.

As a combined effort, NATO in turn refined each one of these architectural views and incorporated them into what is now known as the NATO Policy for C3 Interoperability. All three views as defined below, are considered critical elements of the NATO C3 Interoperability Environment:

Operational View – This view describes the tasks and activities, organizational and operational elements and information flows required to accomplish or support military or consultation function.

System View - This view is generated from the Operational View by the responsible host nation or design authority. It describes and identifies the system(s), both internal and external, and interconnections required to accomplish or support the military or consultation function. This view maps information flows, hardware and applications to user locations and specifies the connectivity, performance and other constraints.

Technical View – This view, generated by the Host Nation or equivalent authority, describes the arrangement, interaction and interdependence of the elements of the system and takes into account the technical constraints imposed by the Systems View. It provides the minimal set of rules governing the selection of the appropriate standards and products from the implementation Domain.

The NATO C3 Interoperability Environment (NIE) encompasses the standards, products and agreements adopted by the Alliance to ensure C3 interoperability. It serves as the basis for the development and evolution of C3 Systems.

Organizationally, NATO has defined interoperability as the ability of systems, units, or forces to provide services to, and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively [NATO, 94].

[2] See C4ISR Architecture Framework, Version 1.0
[3] See IEEE Std 610.12 for complete definition.

The primary organization within NATO that addresses interoperability policy and procedures is the NATO Consultation, Command and Control Board (NC3B). Structurally, the NC3B consists of eight sub-committees, two of which play an important role in the context of this paper. The first, the Interoperability Sub-Committee (ISC) is responsible for establishing C3 systems interoperability policy and implementing C3 standardization objectives deemed necessary for improving interoperability. Underneath the ISC are four working groups (i.e., AC/322-SC/2-WG/…). Each in their own right helps to perpetuate interoperability policy and standardization initiatives throughout the alliance.

The second, known as the Information Systems Sub-Committee (ISSC) is, at the moment, comprised of five working groups (i.e., AC/322-SC/5-WG/…) that primarily address and support information system implementation throughout all of NATO.

When examining NATO's overall interoperability structure collectively, we see that NATO has an interoperability framework that can be divided into three distinct categories:

1) Policy: The NATO Policy for C3 Interoperability represents the policy layer. It is a policy that addresses all overarching and essential C3 interoperability issues, the NATO Interoperability Framework, identifies each of the respective authorities and associated responsibilities, links existing interoperability documents, and defines the relationship with the NATO Standardization Organization (NSO) and other relevant organizations;
2) Execution: The NATO C3 Interoperability Management Plan (NIMP) and the five year Rolling Interoperability Programme (RIP) comprise this layer, and;
3) Products: The NATO C3 Interoperability Environment (NIE) comprises this layer [Vogt, 2000].

In 1997, the NC3B identified several goals and objectives that were considered necessary to attain interoperability between NATO common funded C3 systems. In response to these goals and objectives, the NC3B ISSC formed the NATO Open Systems Working Group (NOSWG)[4], tasking them to develop a technical architecture on behalf of NATO. The technical architecture would become known as the NATO C3 Technical Architecture (NC3TA).

Upon completion, the NC3TA would provide the structural foundation necessary to attain information interoperability between NATO C3 systems and national systems, as well as address interoperability concerns for all NATO common funded systems. Furthermore, the NC3TA would also perpetuate the development of a common core for the Bi-SC Automated Information System (AIS)[5].

The NATO C3 Technical Architecture

To facilitate the creation of the NC3TA, the NOSWG first assessed the merits of each national architectural effort early on, gleaning as much as practically possible from each. Each had technical merit, but differed in overall content and composition. As a result, the

---

[4] NC3B/ISSC/AC/322(SC-5WG/4)DS/1, NATO HQ, Brussels, Belgium 1997.

[5] The two NATO Strategic Commands (SC)(i.e., SHAPE and SACLANT).

NOSWG decided to develop the NC3TA in accordance with the definition for a technical architectural view[6] as much as feasibly possible. By definition, this meant that it would provide the minimal set of rules governing the selection of appropriate standards and products from the implementation domain. Moreover, the NC3TA would also extrapolate, as well as improve upon existing approaches from each one of the contributing national technical architectural efforts.

Overall Structure and Content

In contrast to national technical architectural efforts, the NC3TA is unique in that it is comprised of a five volume set that consists of the following[7]:

Volume 1: *Management* – This volume provides the management framework for the development, as well as the configuration control of the NC3TA. It includes the general management procedures for the application of the NC3TA in NATO C3 systems development;
Volume 2 : *Architectural Models and Description* – This volume is partly derived from the NOSE and NOSIP, and principally supports a NATO technical framework to provide a common basis for the establishment of the architecture for NATO information system projects. It also offers a vision on the use of emerging off-the-shelf technologies;
Volume 3: *Base Standards and Profiles* – This volume contains all of the current open system and communication standards applicable to NATO information systems, as well as guidance for their use;
Volume 4: *NATO C3 Common Standards Profile* – This volume mandates the subset of standards that are critical to interoperability. It provides the link between degrees of interoperability as described in the NATO policy for interoperablity of C3 systems, and standards selection;
Volume 5*: NATO C3 Common Operating Environment* – This volume is the NCSP standards-based computing and communication infrastructure.

The Chairman of the NOSWG meets regularly with other NC3B working groups in order to ensure that all areas of technical concern (e.g., security, data, communications, etc.) are taken into account by the appropriate working group bodies [Simon, 1999]. This simple working group cross evaluation and coordination procedure serves as only one of the preliminary fail-safe steps that is required as a part of the overall NC3TA management process described in Volume 1.

Consistently updated, Volume 2 reflects various architectural models such as the Technical Reference Model (TRM), the NATO Common Operating Environment Component Model (NCM), as well as definitive descriptions or reference pointers to new and emerging technologies such as JAVA and XML. The descriptions provided are primarily derived from the NOSE and NOSIP, and essentially serve as reference material to the system developer, implementor, and end-user. Editorial updates are made primarily through the NC3 Agency.

The encyclopedic nature of Volume 3 serves as another reference document. It too is derived from the NOSE and NOSIP and contains all of the current references on communication and information standards. This volume will also be maintained in an HTML version on the web.

Due to their impact on the systems design, development and implementation for all NATO common funded systems, the two remaining volumes, Volumes 4 & 5 of the NC3TA are considered extremely important. Volume 4, although considered to be quite mature,

[6] For more details, see the NATO C3 Interoperability Environment (NIE).
[7] For a complete description, see NC3TA ver.1.

will undergo periodic updates in order to ensure that the evolution in standards are incorporated to benefit the developer/end-user community on a regular basis. The definitive process for submitting and incorporating candidate standards for consideration into the NCSP is outlined through the “change proposal” section of Volume 1. Volume 4 also has focused on attaining degrees of interoperability through an interoperability profiling procedure that is being worked in coordination with other affiliated sub-committee working groups.

In conjunction with Volume 4, Volume 5 is probably the single most important document within the NC3TA. Due to its significance, the NC3B ISSC formed an Ad hoc NATO Common Operating Environment Working Group that would fall under the purview of the NOSWG. This ad hoc working group would primarily address the technical aspects of creating and instantiating a NCOE.

To note the relevance of the NCOE, in accordance with the NATO Policy for C3 Interoperability, all NATO authorities are required, and the nations are encouraged to implement C3 Systems using the mandatory standards and products as specified in the NATO C3 Common Standards Profile (NCSP) and the NATO Common Operating Environment (NCOE) [Wells, 1999].

Once the NC3B approves future versions of the NCOE, those products that are identified for incorporation will be mandated for all NATO Common Funded Systems. Currently, version 1 of the NCOE does not specify any products.

Significant Features of the NCOE

Volume 5 of the NC3TA is considered evolutionary and therefore a living document. Although it will eventually specify particular products for incorporation into the NCOE, as previously indicated, at the present time is does not. However, these products once selected, will be primarily chosen from an off-the-shelf based “Basket of Products.” This basket of products will eventually populate the various service layers of the NCOE Component Model (NCM). The NCM capitalizes on the top-down layered approach provided by the Technical Reference Model (TRM) as described in Volume 2 of the NC3TA.

The principle components of the NCM include Networks Services, Kernel Services, Infrastructure Services, Common Support Application Services, Application Programming Interfaces, Data Component Definition, Support Services and Mission Applications.

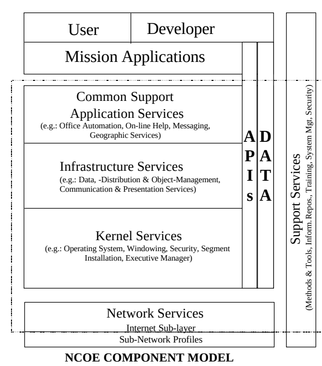

Figure 1 - NCOE Component Model

Network Services – Network services constitute the basic transparent interfaces between the platform and the underlying networking infrastructure, to include the IP layer services;

Kernel Services – The kernel services are that subset of the NCOE component segments, which are required for all workstations and servers. At a minimum, this sub-set would consist of the operating system, windowing software, security services, segment installation software and an executive manager;

Infrastructure Services – Infrastructure services are those services that directly support the flow of information across NATO systems. Infrastructur services provide a set of integrated capabilities that the applications will access to evoke NCOE services;

Common Support Application Services – are those services necessary to view data in a common way (share data) across the network. These service essentially promote interoperability among various mission applications;

Application Programming Interfaces – Applications are integrated into the NCOE through a common set of APIs . The APIs are invoked by the applications and services as required;
Data Component Definition – The data component refers to the way in which data is taken into account in the NCOE and is related to the main components of the NCOE (Common Support Application Services, Infrastructure Services, Kernel Service) and even, out of NCOE components stricto sensu, to Mission Applications;

Support Services – These services include methods and tools, information repository, training services, system management and security.

One of the most debated and often discussed features of the NCOE is known as segmentation. Segmentation can be defined in terms of the functionality that is seen from the perspective of the end-user. Segmentation allows the user(s) to easily add only those required modules that are deemed necessary by the end-user community. In this way, the end user may view the NCOE as a set of building blocks in which a system is built. Since the NCOE is not a system in and by itself, it can be more easily understood as the foundation for building open systems through such inherent features as segmentation. The overall concept for segmentation is predicated on national[8], as well as commercially[9] viable efforts.

As noted previously, one of the goals and objectives of the NC3TA is the development of a common core. In direct response to this need, the Bi-SC AIS core will eventually be implemented utilizing those standards and products stipulated by the NCSP and NCOE. However, to do so will require that the basket of products be populated in the NCOE. The initial version of the NCOE was released in July of 1999. The next version of the NCOE, with its basket of products will list those mandatory products for use by the Bi-SCs. The projected timeframe for the next version (2.0) of the NC3TA is for December 2000.

Conclusion

Interoperability has long been an elusive and sought after goal. Especially, within the realm of coalition information systems. However, a well defined architectural approach can lay the structural foundation necessary to attain interoperability for diverse military information systems in the future. When all five volumes of the NC3TA are finalized, it is anticipated that the structural foundation will be in place for future coalition systems to build systems upon for years to come.

References

[Wentz, 1997] Larry Wentz. *Lessons From Bosnia: The IFOR Experience*. National Defense University Press, Washington, D.C., 1997, 434.
[Moxley, 1996] Frederick I. Moxley. *On the Specification of Complex Software Systems*. Proceedings of the Second IEEE

[8] For more details see DII COE at www.disa.mil
[9] See logo certification

International Conference on Engineering of Complex Computer Systems, October, 1996.

[Vogt, 2000] Bernd Vogt, (Col., GE). *An Outline of NATO C3 Standardization Interoperability Policy Issues*. Proceedings of the CIS Interoperability Conference, March, 2000.

[Wells, 1999] Elbert J. Wells, *The NCOE: Keystone to NATO Interoperability*, Proceedings of the London AFCEA Technet Conference, October, 1999.

[Simon, 1999] Lucien Simon (LtCol, FR). *NOSWG Briefing on the NATO C3 Technical Architecture*, Chairman's Report to the NC3B ISSC. NATO HQ, Brussels, Belgium, October, 1999.

[NATO/DOD, 1994] *Joint Publication 1-02*, Joint Chiefs of Staff, Washington, D.C., 1994.

[NC3TA, 1999] *NATO C3 Technical Architecture (NC3TA), Version 1.0., 30 July, 1999.* NATO HQ, B-1140 Brussels, Belgium.

This paper does not necessarily reflect the views of the US government or DISA. The ideas are those of the authors and are intended to provoke thought and discussion regarding the subject matter.

About the Authors

Frederick I. Moxley is a Senior Technical Advisor within the Defense Information Systems Agency (DISA), United States Department of Defense (DOD). He has several years of experience designing, developing, implementing and managing a variety of software systems for DOD, as well as other agencies throughout the federal government. His research interests include distributed software system architectures, artificial intelligence, and software design methodologies. Dr. Moxley holds advanced degrees in Telecommunications and Computer Information Systems and Sciences.

Lieutenant Colonel (Armament) Lucien Simon is chairman of the NATO Open Systems Working Group of the NATO C3 Board's Information Systems Sub-Committee. He joined the NATO C3 Agency in September 1997 as a French National Expert. In 1997, he graduated from the French Joint Defence Staff College. From 1993 to 1996 he was Programme Manager for the French Army CCIS after having been responsible for various activities within the French CCIS domain. He graduated in the field of armament engineering and holds a post-graduate degree in Computer Science.

Elbert J. Wells has over 20 years experience in the development and implementation of U.S. national and NATO C3 Systems. He is currently at the U.S. Mission to NATO where he is responsible for Information System matters. Previous NATO assignments included tours at the former STC and NACISA. Previous U.S. national assignments included the position as project manager of the U.S. Navy Research & Development Distributed C2. El holds Master Degrees in both Electrical Engineering and Computer Science.