19TH International Command and Control Research and Technology Symposium

C2 Agility: Lessons Learned from Research and Operations.

A Message Exchange Protocol in Command and Control Systems Integration, using the JC3IEDM

Suggested tracks:

Primary: Topic 4 - Experimentation, Metrics, and Analysis.

Alternate: Topic 3 - Data, Information and Knowledge.

Patrick B. A. Lara, Lt. Cdr.

Military Institute of Engineering

Ricardo Choren N., D. Sc.

Military Institute of Engineering

Student Paper (Master´s degree with two years in the program)

Point of Contact:
Patrick Baptista Amaral de Lara
Military Institute of Engineering
Praça General Tibúrcio, 80 - Urca.
Rio de Janeiro, Brazil. 22290-270
(+5521)97120-5686/2546-7094
patricklara@gmail.com

ABSTRACT

A Joint Operation scenario can be described as a heterogeneous war environment, in which there is a need to update shared situational awareness, based on a constant exchange of information among computer systems. However, such a system may have data in different schemata and a military operation integration infrastructure may present several limitations. Moreover, this scenario presents specific demands regarding some integration requirements (Lam and Shakararaman, 2004). These requirements are necessary for obtaining Agility (Alberts, 2011) in the exchange of information. This paper presents a protocol to address such limitations in order to accomplish an integration scenario. The proposed protocol addresses two levels of interoperability: data and infrastructure requirements. It is based on service-oriented architecture (Taylor et al., 2010), which is considered suitable for the integration of command and control systems (C2S) (Lund et al., 2007). The protocol uses the JC3IEDM (MIP, 2012) as a meta-model to describe message payload. To address agility requirements, it uses a XML serialized through SOAP. The advantages of this protocol are to allow independence from computer languages and platforms during C2S data exchanges. This paper presents approaches of integration, compares their technologies, points out their advantages, proposes requirements, and provides the design of a protocol to allow interoperability in Joint Operations.

1. INTRODUCTION

Command and control is the art and science of the study of operation of a chain of command, which consists of three components: authority, processes and structure, according to the Brazilian Military Command and Control Doctrine (Jobim, 2006).

Command and control systems (C2S) with superior performance enable commanders to become victorious in joint efforts by helping them to apply their skills in critical time and select the best strategy to succeed in a given situation. Two features are essential: the human element and the need for relevant information, timely and accurate. The human element provides the ability to infer what is important; it is the essential element for absorbing and reacting to information, which makes its importance constant over time (Shalikashvili, 1995).

Technology has improved mobility, weapons, sensors and C2S, and continues to reduce the time and space needed for operations, increasing the pace of operations and generating large amounts of information. Inability to process this information may impair the reactions of the fighting force. The use of C2S systems designed to assist human capabilities and limitations is essential to maintain a winning the C2 capacity for the commander (Shalikashvili, 1995).

Situational awareness shared among military units is essential to network-enabled operations (NEC). This form of operations requires greater access to information, which in turn requires ensuring that units in need of information have access to it. Such an operating environment focused on rapid reaction requires more adaptable and efficient solutions to the exchange of information, to create and update dynamically a good operational scenario (Jobim, 2006). This paper presents an initial solution to the problem, using a set of messages and rules to manage traffic between C2S, with the proposal to allow the exchange of data between systems via messages.

Defining a protocol for exchanging messages is a complex task. For example, consider the Long-Range Identification and Tracking system (LRIT), where a multinational group took about five years to achieve stabilization at the Interface Data Exchange (IDE) protocols (IMO, 2012). This paper aims to solve the problem by presenting requirements and a set of messages and their rules to make a message handling protocol, capable of enabling data exchange among systems. This student paper proposes XML-formatted messages and the use of Service Oriented Access Protocol (SOAP) messages in a military networked environment. The challenge is how to minimize the overhead caused by the time wasted on the reading messages process. This step could be essential to reach a satisfactory performance in C2 systems integration.

The rest of the paper is organized as follows: section 2 presents the command and control systems integration; section 3 presents the proposed approach; section 4 discusses related work; section 5 presents conclusions of the study and future work; and the sources referenced are listed in section 6.

2. C2S INTEGRATION

The Force Commander needs accurate and timely information to operate, in order to guarantee that the soldiers will have access to information they need. The C2S system thus is a major tool to support Joint Force Commanders allowing gathering, transport, process and dissemination of information (Shalikashvili, 1995).

To ensure the continuous and uninterrupted flow and processing of information, joint combatants should have C2S that are interoperable, flexible, agile, mobile, disciplined, survival and sustainable (Shalikashvili, 1995). There are more principles then those listed above. Other relevant principles must be encompassed or applied when appropriate. They are: integration, ease of maintenance, mobility, modularity, planning, prioritization procedures, readiness, responsibility, agility, simplicity and capacity (Blair, 1996).

Joint and multinational operations are complex and are comprised of various military organizations operating as a Force. Multinational forces may have differences in C2S, language, terminology, doctrine and standards of operation that may cause confusion. The confusion increases the demand for information and also the level of uncertainty. The lower the level of the interface between various commands, the greater will be the uncertainty as well the demand for systems of C2S. The Joint Force Commander must ensure that great care is taken in structuring the multinational force before operations, to avoid unnecessary confusion within friendly forces.

2.1 JC3IEDM

A protocol provides rules for the handling of information. The data is treated as having value as sources of information. The problem of representation of information for C2S has mature solutions, for example the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) (MIP, 2012). However, the model does not provide a solution to the need for dynamic exchange data between systems. This dynamic is defined, as previously mentioned in a protocol for message handling, using the meta-model of JC3IEDM.

According to the Multilateral Interoperability Programme (MIP), Data interoperability requires a rigorously defined semantic vocabulary. The JC3IEDM is embedded in a structured context that defines the standard elements of information that compose the basis for interoperability among automated Command and Control Information Systems (C2IS), as long as the C2IS can accommodate the model's information structure.

"The MIP nations agreed with requirements to define only the information that is to be exchanged rather than all of the information that would normally be required in a national system. Consequently, JC3IEDM is first and foremost an information exchange data model. The model can also serve as a coherent basis for other information exchange applications

within functional user communities. The general pattern is to use a subset of JC3IEDM and add functional extensions." - The Multilateral Interoperability Programme (MIP, 2012). JC3IEDM is used by NATO in their joint operations in the integration of C2S of participating countries.

2.2 JC3IEDM Chosen Entities

JC3IEDM should be considered as a consolidated model. However, the model does not provide a solution for the dynamic data exchange between systems. This dynamic is defined, as previously stated, in a protocol for exchanging messages, using the JC3IEDM. (MIP, 2012)

Figure 1 shows a part of the model that contains the chosen independent entities of the data model and their relationships for this study, with a brief description of their typical meanings.

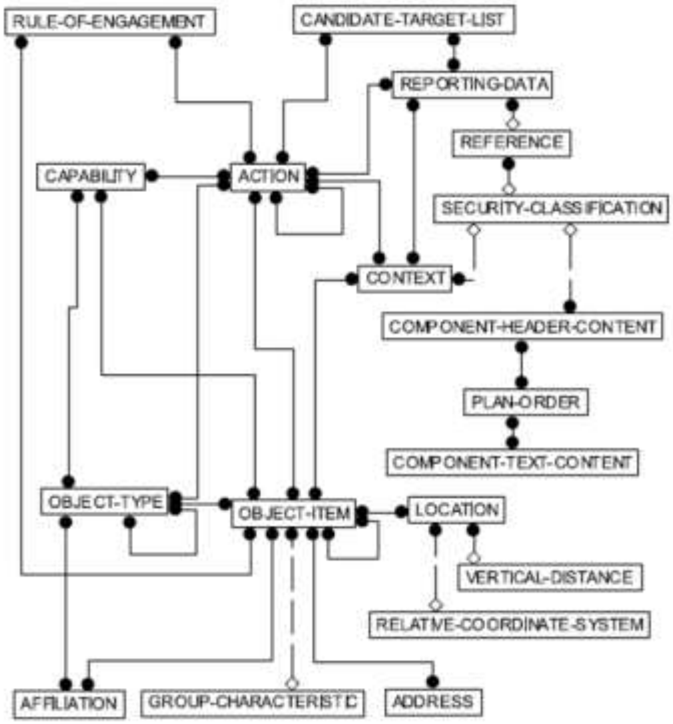

Figure 1. Independent entities of JC3IEDM (MIP, 2012)

- **ACTION** - An activity, or the occurrence of an activity, that may utilize resources and may be used against an objective.

  Examples: Order of Operation, Operation Plan, Order of Movement, Movement Plan, Aerial Fire Support, events (i.e. unknown aircraft approaching) or incident (i.e. enemy attack).

  Rules in Model: Dynamics (how, what, when, something that will be done, what is being done or has been done).

- **LOCATION** - A specification of position and geometry with respect to a specified horizontal frame of reference and a vertical distance measured from a specified datum.

  Examples: points, sequence points, polygon, circle, rectangle, ellipse, polygon area, sphere, cone and block space. LOCATION specifies location and dimensionality.

  The Model Rules: positioning objects and creating shapes (where).

- **OBJECT-TYPE** - An individually identified class of objects that has military or civilian significance.

  Examples: type of person (i.e. by rank), type of material (i.e. self-propelled "howitzer"), type of facility (i.e. airport), or type of organization (i.e. Armored Division).

  The Model Rules: identifying classes of things (who and what).

- **OBJECT-ITEM** - An individually identified object that has military or civilian significance.

  Examples: a specific person, or a specific unit.

  The Model Rules: identifying things individually (who and what).

- **REPORTING-DATA** - The specification of source, quality and timing that applies to reported data.

Using a significant part of the data model shown above, called Service Oriented Architecture, permits a synergy between the available data and services offered by specialized suppliers. Web services allow platform independence and programming language because they uses XML for definitions and communication. They also enable a strong definition of messages and services through WSDL documents. The use of HTTPS for transport will also facilitate the passage of information through firewalls without the need of using other ports.

3. THE PROPOSED APROACH

The study aims to identify available approaches of integration systems, compare their technologies, pointing out their advantages and disadvantages, and propose a model of generic protocol for exchanging messages between situational awareness systems in Joint Operations, using the JC3IEDM.

The project has been developed through a survey, including a case study with a model to exchange messages on a system of maritime situational awareness already developed, simulating the exchange of information between C2S. We looked for the type of information that the source system needs. After this phase, we designed the model to exchange messages from a source to the destination C2S.

The research considers the following assumptions:

a) The protocol is conceptual, but its implementation may be accomplished through a layered architecture on a services layer (Erl, 2009), which would implement the interfaces of the messages and business rules governing its processing; and

b) The architecture Publish/Subscribe (Bass, 2003) is suitable for allow the maintenance of situational awareness in operational environments (Amorim, 2011).

A high-level view (see Figure 2) shows the proposed architecture, where the protocol allows for messages exchanging information through a system of systems (SoS), composed of three systems of military situational awareness, defined as clients, and a C2S, the main consumer of message content.

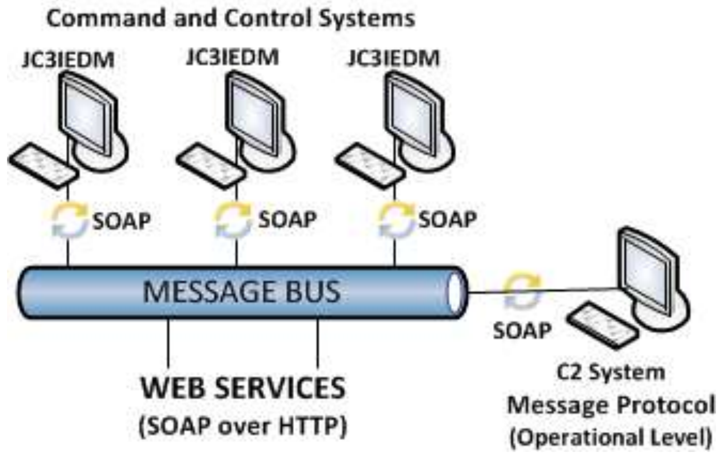

Figure 2. High Level Architecture

The study was conducted comparing the four main approaches in the area of integration, and how it is used to exchange messages between systems based on SOA standards, considered the state of art in the field of systems integration.

The study presented a proposed integration model through a generic protocol, using the concepts of JC3IEDM to exchange messages among existing systems of maritime situational awareness, both those already in use and those available for study.

As a result of field research conducted in Brazilian Navy organizations, we have obtained the necessary requirements for Command and Control of a Joint Operation at the Operational level. It was emphasized that delay in data flow impedes the progress of actions during the Combined Operations exercises. As an overview: the protocol should operate as a message handling service, allowing for exchange of information between the systems to be integrated. Based on field research and previous experiences in maritime systems of situational awareness, the requirements for the protocol were established.

The protocol should route messages between systems. Its interface should be available for communication between systems, via standard Internet protocol.

The protocol must store and archive messages header information in "log" files for subsequent audits and statistical analysis of the system operation.

The protocol should not read the information contained in the messages, and should not store or archive any information from the systems. The protocol should protect the contents of the messages.

Users responsible for the operation and maintenance of the system should not be able to access the information contained in the messages.

The protocol should read only the message header. The protocol should not perform any filtering function on the information contained in the messages.

The protocol must use the Requestor User or the Provider User parameters included in the messages to determine where to forward the message.

Also were defined as requirements:

- The protocol should allow the system to request and send the position of friendly forces;

- The protocol should allow the system to ask and update the position of friendly forces, in a predefined time;

- The protocol should allow the system to perform a position request regarding a specific known unit; and

- The protocol should allow the system to perform location request per geographical area.

Integration of heterogeneous systems has been approached with different views (Hohpe and Woolf, 2003). Among the solutions studied is possible to identify three approach layers of the problem: the application layer, in which the proposed work will focus on; the security layer, which will be reserved for a study in future work; and the communication layer, where we see the use of several different technologies, being typically used: CORBA (Vinoski, 1997), RMI (Downing, 1998) and Web services (Curbera, 2002). Besides these mentioned technologies, there are also design patterns for building integration solutions (Hohpe and Woolf, 2003), which serve as a guide for the development of this type of solution. The development of the generic protocol for message handling followed the concepts of JC3IEDM, a data model defined by NATO to allow interoperability between command and control systems.

The table below shows the main advantages and disadvantages discovered in the comparison of technologies for integration that were studied.

Table 1. Comparing technologies for integration

Technology vs. Integration	CORBA	JAVA RMI	Web Services
Initial Project Difficulty	High	Low	Low
Interoperability (independence of language and platform)	High	Low	High
Expected Performance	Excellent *	Very Good *	Good **

* Packets (message headers) are reading binary.

** Expected more overhead during packets reading.

The service-oriented architecture (SOA) with the use of Web Services technology was chosen because of ease of learning and implementing this technology. It has good interoperability, regardless of the programming language and platform used, although the expected performance is not the best possible. To increase the performance, the size of message should be minimized. A middleware for managing message queues is also necessary, and is available as an open source and free distribution software.

Regarding JC3IDEM study was carried out on the model and ratified ideas based on previous work (Callai, 2006). It was determined that the operational vision should be focused on what are the processes of command and control for joint operations, while the technical vision should worry about what formats are to be used.

Command and Control systems exchange messages (information) through mechanisms classified as MEM (Message Exchange Mechanism), or message-driven pre-formatted. The DEM (Data Exchange Mechanism) has focused on the information modeled from the perspective of object orientation, physically implemented in a database. Based on this model, a simpler model was created, to facilitate understanding~~,~~ and facilitate implementation in academic study projects.

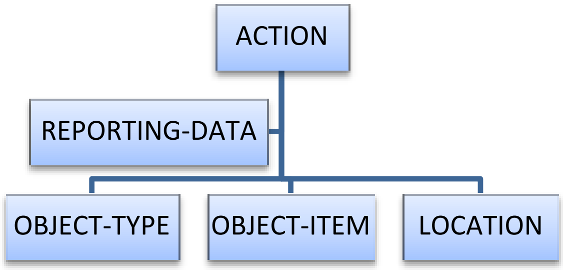

Figure 3. Used Part of the JC3IEDM

3.1 INTEGRATION REQUIREMENTS

W. Lam and V. Shankararaman (Lam and Shankararaman, 2004) listed important non-functional requirements as ten common types of integration requirements in enterprise integration. Analyzing our problem, we selected four of them to apply on the message protocol requirements. Also defined as requirements were:

- **TIMELINESS** – Urgency of the communication or integration between applications. A large amount of time spent on data exchange reflects on the precision and the relevance of the information in the situational awareness scenario, at the operational level. To maintain timeliness, the protocol should only route messages between systems. Its interface should be available for communication between systems, via standard Internet protocol. The message protocol must use the Requestor User or the Provider User parameters included in the messages to determine where to forward the message.

- **RESILIENCE and RECOVERY** – Resilience is ability of the integration infrastructure to recover in event of failures. By reaching more redundancy there will be a decrease on the possibility of a failure on the message delivery. To reach these requirements, the protocol must store and archive messages header information in "log" files for subsequent audits and statistical analysis of the system operation. The protocol should only read the message header, and should not perform any filtering function on the information contained in the messages, helping to guarantee higher RESILIENCE on the message delivery.

- **SIZE** - Volume of data that the integration between applications must handle. Large file size results in raising the expected overhead. To avoid large overhead, the protocol does not read the information contained in the messages body (only in the header), and does not store or archive any information from the systems. The protocol should protect the contents of the messages from unidentified users.

- **FREQUENCY** – Frequency of data exchange needed between applications.

Directly affects the operations. The real time frequency is required for the Request / Response services. For Publish / Subscribe services can be defined a slightly longer time to interactions.

3.2 MESSAGE EXAMPLES

This subsection presents three examples of messages. The scenario is a Joint Force Operation, where Army, Navy and Air Forces are cooperating to reach the same objective. Armed Forces need to share information to maintain an updated Situational Awareness.

In the first example, a request of position is made (LOCATION) of an operative unit (OBJECT-ITEM), defined by its unique identifier (ObjId). The second one presents the message, carring a request for verification of placement of units within a given area defined by the geographical coordinates of its two end points, northeast and southwest geographic area points (neLat, neLong, swLat and swLon). The third example is a response for a Position Request Message, called Position Report M. The "<!--Optional:-->" field, formatting of tags and spacing of them was changed to fit the message examples to the paper size.

3.2.1 Position per Unit Request Message

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/
soap/envelope/" xmlns:web="http://web.jc3v314/">
<soapenv:Header/>
   <soapenv:Body>
      <web:location>
         <objId>?</objId>
      </web:location>
   </soapenv:Body>
</soapenv:Envelope>
```

3.2.2 Units per Area Request Message

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/
soap/envelope/" xmlns:web="http://web.jc3v314/">
   <soapenv:Header/>
   <soapenv:Body>
      <web:request>
         <areaRequest>
            <areaCode>?</areaCode>
            <description>?</description>
            <messageId>?</messageId>
            <neLat>?</neLat>
            <neLon>?</neLon>
<requestTimestamp>?</requestTimestamp>
            <requestor>?</requestor>
            <swLat>?</swLat>
            <swLon>?</swLon>
         </areaRequest>
      </web:request>
   </soapenv:Body>
</soapenv:Envelope>
```

3.2.3 Position Report Message

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/
soap/envelope/" xmlns:ws="http://ws/">
  <soapenv:Header/>
  <soapenv:Body>
    <ws:positionReport>
      <positionReport>
        <areaCode>?</areaCode>
        <description>?</description>
        <latitude>?</latitude>
        <longitude>?</longitude>
        <messageId>?</messageId>
        <requestTimestamp>?</requestTimestamp>
        <requestor>?</requestor>
      </positionReport>
    </ws:positionReport>
  </soapenv:Body>
</soapenv:Envelope>
```

4. RELATED WORK

K. Lund (Lund et al., 2007) stated that there is a focus on the establishment of a service-oriented architecture (SOA) to increase interaction within the allied forces. However, this solution has been adopted for environments with great data communication capacities, which is the opposite characteristic from military tactical networks. The study also recommends the architectural principles and technologies that are best suited to implement this infrastructure information. Also recommended is the use of Internet Protocol (IP) as a common protocol for use in all types of networks technologies, chosen to facilitate interoperability, the easier for all types of network. As presented above, SOA is commonly performed through web services using XML-formatted documents, but it is designed to be used in broadband networks and not in military networks with limited capacity. XML documents tend to be big, having a significant overhead. This paper proposed requirements to make a message handling protocol, and few XML-formatted messages there expected to reduce this overhead caused by the use of Web Services in tactical networks environment. The main idea was to make SOA possible for use by all military levels, from strategic to tactical networks.

5. CONCLUSIONS AND FUTURE WORKS

This paper proposes a study of the requirements of a protocol and the examples for XML-formatted messages that must be handling in a protocol, to allow a satisfactory performance during the integration process of command and control systems. The solution has two main approaches, both equally important, to establish a protocol. The first one, the data model, which is supposed to be known, common, and consolidated by all C2 systems, and the second one, the integration technology used to allow the message handling, where usually Web Services are used, despite overhead expected in the reading messages process.

SOA enables a strong decoupling between clients and servers, and is supported by the existence of various tools for project development. The use of the Web Services technology allows a greater decoupling between the systems, which leads to independence from programming language and platform of the existing C2 systems.

The data model JC3IEDM defines a pattern for information modelling, allowing the use of the same vocabulary to all systems. Data is routed through objects in messages handled by the protocol, using request/response and publish/subscribe patterns, which gives systems the capability either to refresh data on demand, or to update periodically. The requirements of the protocol and the message examples listed above are designed to reduce impact during joint operations, allowing success on the battlefield.

This solution to the problem presented is an initial one, using a set of messages and rules to manage traffic between C2S, using the protocol requirements listed on section 3 to minimize overhead caused by the use of Web Services. These requirements were based on previous experience of specialists in maritime situational awareness systems and on knowledge of the command and control doctrines contained in the publications listed on section 6.

The future work will be based on designing the complete system protocol architecture to allow message handling in runtime. The implementation of an encryption layer is also desirable; that should be strong enough to ensure the conduction of joint operations exercises without any interference, internal or external. This security layer must be designed and implemented without compromising the performance of the message exchange protocol.

6. REFERENCES

Alberts, D. *The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors*, The Command & Control Research Program (2011).

Amorim, C. *Joint Operations Doctrine ("Doutrina de Operações Conjuntas" in Portuguese)*, Ministry of Defense, Brazil (2011).

Bass, L. et al. *Software Architecture in Practice*, Pearson Education Inc., India (2003).

Blair, D. *Joint Doctrine for Employment of Command operational / Tactical , Control , Communications and Computer Systems*, Joint Chiefs of Staf, USA (1996).

Callai, A. *The NATO data model for information exchange of Command and Control ("O modelo de dados da OTAN para intercâmbio de informações de Comando e controle" in Portuguese)*, Escola de Comando e Estado-Maior do Exército, Brazil (2006).

Curbera, F. et al. *Unraveling the Web Services Web: An Introduction to SOAP, WSDL, and UDDI*. IEEE Internet Computing (Mar./Apr. 2002).

Downing, T. *Java RMI: Remote Method Invocation*. IDG Books Worldwide, Inc. Foster City, CA, USA (1998).

Erl, T. *SOA Design Patterns*, Prentice Hall Service-Oriented Computing Series (2009).

Hohpe, G. and Woolf, B. *Enterprise integration patterns: Designing, building, and deploying messaging solutions*. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA (2003).

International Maritime Organization (IMO). *Long-Range Identification and Tracking System (LRIT)*, Technical Documentation Rev. 5, London, UK (2012).

Jobim, N. *Military Command and Control Doctrine ("Doutrina Militar de Comando e Controle" in Portuguese)*, Ministry of Defense, Brazil (2006).

Johnsen, F. et al. *Semantic Service Discovery for Interoperability in Tactical Military Networks*, The International C2 Journal, N.1, VOL.4 (2010).

Lam, W. and Shakararaman, V. *An Enterprise Integration Methodology*. IT Professional Magazine (Mar/Apr. 2004), 40-48.

Lund, K. et al. *Using Web Services to Realize Service Oriented Architecture in Military Communication Networks*, IEEE Communications Magazine (2007), 47-53.

Multilateral Interoperability Programme (MIP), *The Joint C3 Information Exchange Data Model* (JC3IEDM Main IPT3 V3.1.4), Greding, Germany (2012).

Shalikashvili, J. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, Joint Chiefs of Staf, USA (1995).

Taylor, R.N. et al. *Software Architecture: Foundations, Theory, and Practice*. John Wiley & Sons, Inc. (2010).

Unger, R. *National Strategy of Defense ("Estratégia Nacional de Defesa" in Portuguese)*, Ministry of Defense, Brazil (2008).

Vinoski, S. *CORBA: Integrating Diverse Applications Within Distributed Heterogeneous Enviroments*. IEEE Communications Magazine (Feb. 1997), 46-55.