A Protocol for Command and Control Systems Integration

Patrick Lara and Ricardo Choren
Military Institute of Engineering, Praça General Tibúrcio, Rio de Janeiro, Brazil

Keywords: Command and Control, Enterprise Integration, JC3IEDM, Message Protocol, SOAP, Systems Integration.

Abstract: Integration of Command and Control (C2) systems is a real need in any Joint Operation. Solutions are typically based on data exchange, usually using the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), a data model established by NATO. The use of this model with service oriented architecture (SOA) has been consolidated as one of the key factors to achieve command and control systems integration. However, these solutions require great computer process capacity and broadband networks, which are usually hard to find in military tactical environments. This paper presents approaches of integration systems available, comparing their technologies, pointing out their advantages and disadvantages, and finally proposes requirements for a generic protocol to allow message handling between command and control systems, using the JC3IEDM.

SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

Command and control (C2) is the art and science in the study of the operation of a chain of command, which consists basically of three components: authority, processes and structure (Amorim, 2011). Command and control systems with superior performance enables commanders to remain victorious in the joint efforts, 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, with its ability to infer what is important, the essential elements absorbs and reacts to information, which makes it an important factor constant over time (Shalikashvili, 1995).

Technology has improved mobility, weapons, sensors and C2 systems (C2S), and continues to reduce the time and space, increasing the pace of operations, generating large amounts of information. If we cannot process this information, it may impair the reactions of the fighting force. The use of C2S systems designed to assist human capabilities and limitations is essential to keep the C2 commander capacity victoriously (Shalikashvili, 1995).

The situational awareness shared between military units is essential for the ability to network-enabled operations (NEC). This requires greater access to information, ensuring that the units in need of information have access to it. Nevertheless, the operating environment focusing in rapid reaction requires more adaptable and efficient solutions for the exchange of information, to create and update dynamically an operational scenario.

This paper presents an initial solution to the problem, using a set of messages and rules to manage traffic of information between C2S, with the proposal to allow the exchange of data between systems via messages. The definition of a protocol for exchanging messages is a complex task. For example, we have the LRIT system (LONG-RANGE IDENTIFICATION AND TRACKING SYSTEM), where a multinational group took about five years to achieve stabilization at the Interface Data Exchange (IDE) protocols (IMO, 2012). This paper therefore aims to solve the problem by presenting a set of messages and the respective rules governing the traffic between systems to enable data exchange. The challenge in this type of solution is how to minimize the overhead caused by the time wasted on the reading messages process. This step could be mandatory to reach a satisfactory performance in C2S 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 presents examples of the messages handled by the Protocol on a scenario; section 5 discusses the related work; section 6

Lara P. and Choren R..
A Protocol for Command and Control Systems Integration.
DOI: 10.5220/0004970404840489
In *Proceedings of the 16th International Conference on Enterprise Information Systems* (ICEIS-2014), pages 484-489
ISBN: 978-989-758-029-1
Copyright © 2014 SCITEPRESS (Science and Technology Publications, Lda.)

presents conclusions of the study and the future works; and the references are listed in section 7.

2 C2S INTEGRATION

The Force Commanders needs accurate and timely information to operate, guaranteeing that the soldiers will have access to the information they need. The C2S system is a major tool to support Joint Force commanders (JFC) 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 listed above. Other relevant principles are 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 gather 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 JFC must ensure that great care is taken in structuring multinational force before operations to avoid unnecessary confusion within friendly forces (Blair, 1996).

2.1 JC3IEDM

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

According to the Multilateral Interoperability Programme (MIP, 2012), Data interoperability requires a rigorous defined semantic vocabulary. The JC3IEDM is embedded in a structured context that defines the standard elements of information that compose the basis for interoperability between automated Command and Control Information Systems (C2IS), as long as 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 JC3IEDM is used by NATO in their joint operations in the integration of C2 systems of participating countries (MIP, 2012).

JC3IEDM should be considerate as a consolidated model. However, this model does not provide a solution for the dynamic Data exchange between systems. This dynamic exchange is defined, as previously stated, in a protocol for exchanging messages, using the data model JC3IEDM.

2.1.1 JC3IEDM Chosen Entities

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.

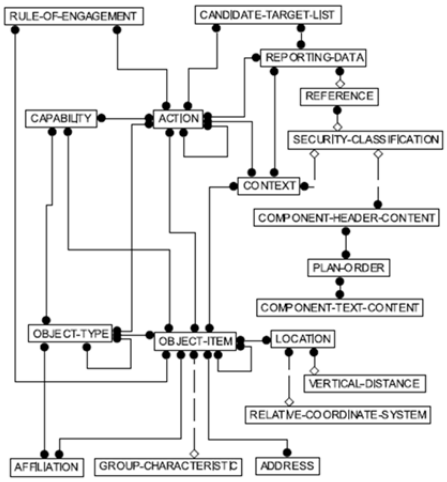

Figure 1: Independent entities of JC3IEDM.

ACTION - An activity, or the occurrence of an activity, that may utilise resources and may be used against an objective. Examples: Order of Operation, Operation Plan, Order of Movement, Movement

Plan, events or incident (i.e. enemy attack).

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.

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, type of facility, or type of organization.

OBJECT-ITEM - An individually identified object that has military or civilian significance. Examples: a specific person, or a specific unit.

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

Using a significant part of the data model shown above, herewith Web Services technology, it is believed that there is a synergy between the available data and services offered by specialized suppliers. Web services allow platform independence and programming language because it uses XML to definitions and communication. It also enables 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 specific 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 systems situational awareness in Joint Operations, using the JC3IEDM.

The project has being developed through a survey, which was prepared a case of study with a model to exchange messages on a system of maritime situational awareness already developed, simulating the exchange of information between C2 systems. We looked for what type of information that the source system needs. After this phase, we designed the model to exchange messages from a source to the destination C2 systems.

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; e

b) The architecture Publish/Subscribe (Hohpe and Woolf, 2003) is suitable for allow maintenance situational awareness environments war.

A high-level view (see Figure 2) shows the proposed architecture, where the protocol allows for messages to exchange information through a system of systems, composed of several systems of military situational awareness, defined as clients, and a C2 System, the main consumer of message content.

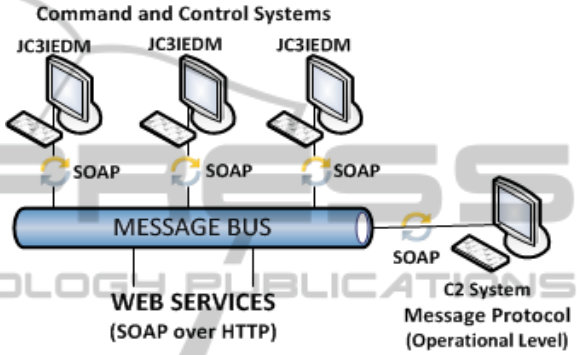

Figure 2: High Level Architecture.

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

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

As a result of field research conducted in the Brazilian Navy organizations, we obtained the necessary requirements for command and control of a joint operation at the operational level. It was emphasized that the delay in the data flow holds the progress of actions during the Combined Operations exercises.

In an overview, the protocol should operate as a message handling service of messages, allowing for exchange of information between the systems to be integrated. Based on the field research and previous experiences in maritime systems of situational awareness, the functional requirements for the message protocol were established. Protocol should:

a) allow the system to shall request and send the position of friendly forces;

b) allow the system to ask and update the position of friendly forces, in a predefined time;

c) allow the system to perform the position request a specific unit known; and

d) allow the system to perform location request per geographical area.

W. Lam and V. Shankararaman listed ten common types of integration requirements in enterprise integration. Analysing our problem, we selected four of them to apply on the message protocol requirements (Lam and Shankararaman, 2004).

Also were defined as requirements:

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

2) Resilience and recovery – Resilience of the integration infrastructure in event of failures. Reaching more redundancy will help to guarantee the higher 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.

3) Size – Size of data that the integration between applications must handle (related to volume). Big file sizes reflects on raising the expected overheads. To avoid big overheads, 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. Users responsible for the operation and maintenance of the system should not be able to access the information contained in the messages.

4) Frequency – Frequency of integration 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.

We found that the integration of heterogeneous systems has been approached with different views on the search for solutions. The development of the generic protocol for message handling uses the concepts of JC3IEDM, a data model defined by NATO to allow interoperability between command and control systems.

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, despite 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, as an open source and free distribution software.

Regarding JC3IDEM study was carried out on the model, which was confirmed ideas based on previous work. It was found 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 to be used.

The C2 systems exchange messages through mechanisms classified as MEM (Message Exchange Mechanism), or message-driven pre-formatted. The DEM (Data Exchange Mechanism) has focused on the information modelled from the perspective of object orientation, physically implemented in a database. Based on this model, a simpler model was created, to facilitate their understanding, and allow its implementation in academic study projects.

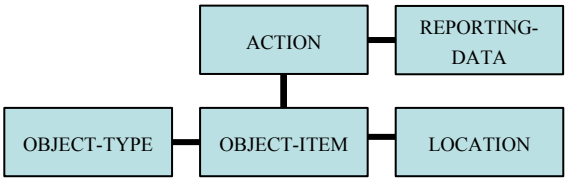

Figure 3: Used Part of the JC3IEDM.

Using the part of data model shown above and the Web Services technology, it is believed that there is a synergy between the available data and services offered by specialized suppliers. Web services allow platform independence and programming language because it uses the XML format for definitions and communication. It also enables a strong definition of messages and services through WSDL documents. The use of HTTPS for transport will facilitate the passage of information through firewalls without the need to use specific ports.

4 EXAMPLE

This subsection presents three examples of messages. The scenario is a Joint Force Operation,

where Navy, Army and Air Forces are cooperating to reach the same objective. The Armed Forces need to share their informations 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 carries 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 are points (neLat, neLong, swLat and swLon). The third example is a response for a Position Request Message, called Position Report Message. The formatting of tags and spacing of them was changed for fit to the paper columns.

4.1 Position per Unit Request Message

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

4.2 Units per Area Request Message

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.o
rg/
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>
```

4.3 Position Report Message

```
   <soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.o
rg/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>
```

5 RELATED WORK

Lund et al. presented that there is a focus on the establishment of a service-oriented architecture (SOA) to increase interaction within the allied forces (Lund et al., 2007). However, this solution has been adopted for environments with great data communication capacities, which is the opposite of 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 IP as a common protocol for use in all types of networks technologies, chosen to facilitate interoperability, the easier for all types of network. The main idea was to make SOA possible to take by all military levels, from strategic to tactical networks.

As presented above, SOA is commonly performed through web services using XML-formatted documents, but are designed to be used in broadband networks and not in military networks with limited capacity. The XML documents tend to be large, 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.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

6 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 approaches, both equal 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 is typically used Web Services, despite of all overhead expected on the reading messages process.

SOA enable a strong decoupling between clients and servers, and count with 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 independent programming language and platform for 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 give systems the capacity of data refresh on demand, or update periodically. The requirements of the protocol, and the message examples listed above are design to reduce this impact during joint operations, allowing their success in battlefields.

This is an initial solution to the problem, using a set of messages and rules to manage traffic between C2S, using the protocol requirements listed on section 3 to minimize the overhead caused by the use of Web Services. These requirements were based on a previous experience of specialists in maritime situational awareness systems and on the knowledge of the command and control doctrines contained in the publications listed on section 7.

The future work will be based on design the complete system protocol architecture to allow the message handling in runtime. The implement 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.

REFERENCES

Amorim, C., 2011. *Joint Operations Doctrine*, Ministry of Defence. Brazil, 1st edition.

Blair, D., 1996. *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems*, Joint Chiefs of Staf. USA, 1st October 1996 edition.

Erl, T., 2009. *SOA Design Patterns*, Prentice Hall PTR. USA, 1st edition.

Hohpe, G. and Woolf, B., 2003. *Enterprise integration patterns: Designing, building, and deploying messaging solutions*, Addison-Wesley Professional. USA, 1st edition.

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

Lam, W. and Shakararaman, V., 2004. In *An Enterprise Integration Methodology, IT Professional Magazine*. IEEE.

Lund, K. et al., 2007. In *Using Web Services to Realize Service Oriented Architecture in Military Communication Networks, IEEE Communications Magazine*. IEEE.

Multilateral Interoperability Programme (MIP), 2012. *The Joint C3 Information Exchange Data Model (JC3IEDM) Main v.3.1.4*. Germany, version 3.1.4.

Shalikashvili, J., 1995. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, Joint Chiefs of Staf. USA, 1st edition.