Design methodology of a military messaging system

Metodología de diseño de un sistema de mensajería militar

Gustavo Pérez V. [1]
Stefany Marrugo Ll. [2]

Abstract

The paper describes the design methodology of a military messaging system. The system's design is characterized by its coherence among security, transmission medium, and design protocol, which allow added value in the strategic operations center. The system allows using a selected data base for subsequent applications of operations research tools and simulation. The system was designed with a low bandwidth communications network (HF / VHF / UHF and satellite phone calls) as the transmission media. The messaging system security is based on a public key cryptographic system. The paper also shows some of the test results of the system's functionality.

Key words: Military Messaging System, strategic Messaging System, Messaging System design, design methodology, communications network.

Resumen

El documento describe la metodología de diseño de un sistema de mensajería militar. El diseño del sistema está caracterizado por su coherencia entre la seguridad, el medio de transmisión y el protocolo de diseño, lo que permite obtener valor agregado en el centro estratégico de operaciones. El sistema permite utilizar una base de información seleccionada, para posteriormente aplicarle herramientas de investigación de operaciones y simulación. El sistema fue diseñado tomando una red de comunicaciones de bajo ancho de banda (HF/VHF/UHF y telefonía satelital), como medio de transmisión. La seguridad del sistema de mensajería está basada en un sistema criptográfico de clave pública. El documento muestra además, algunos de los resultados obtenidos en las pruebas de funcionalidad del sistema.

Palabras claves: Sistema de mensajería militar, Sistema estratégico de mensajería, diseño de sistema de mensajería, metodología de diseño, redes de comunicación.

Date received: November 19th, 2010. - *Fecha de recepción: 19 de Noviembre de 2010.*
Date Accepted: December 14th, 2010. - *Fecha de aceptación: 14 de Diciembre de 2010.*

[1] Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial - Cotecmar.
E-mail: smarrugo@cotecmar.com
[2] Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial - Cotecmar.
E-mail: gustavoperezv@gmail.com

Introduction

Among the projects executed by the R&D plus innovation direction at COTECMAR, prototype was developed of a Messaging system for the exchange of short information and with non-synchronic character between tactical units in the field of operations and the strategic Command and Control Center.

The Messaging system is a comprehensive part of a set of sub-systems that make up the Command and Control Main System, and it is supported by different technologies and existing communication infrastructures to carry out its purposes.

The objective of this document is to describe the design methodology of the Messaging System developed by clearly showing the advantages obtained by making a coherent design of all the components of said system, which was elaborated by bearing in mind the requirements from Command and Control and the restrictions in the means available, seeking to satisfy and provide the necessary connectivity (via different transmission media), interoperability, and security in the transportation of information.

Theoretical Framework

The need for a reliable communications system is ever-more important in military operations, given that the potential effectiveness of combat systems supporting the mission depends to a greater extent on adequate coordination. Also, implementing the concepts posed by the Network Centric Warfare (NCW) according to which the complete availability of information at the indicated time and place is the most relevant factor, relying fully on a communications infrastructure with sufficient capacities for transportation of information (*Snyder, 1993*).

Although telecommunications are frequently characterized through attributes like bandwidth, data transference rate, or error rate, its main value within the Command and Control context is derived from the possibility of establishing connectivity not merely among the commanders involved in the mission, but also among the different participants who are under their charge and the network of sensors or devices supporting the acquisition of relevant information for the purposes of the operation. Additionally, the exchange of information on a safe communications infrastructure is an indispensable requirement in the military setting, to the point that the interception of communication can mean the difference between victory and defeat (*Hutcherson, 1994*).

A messaging system is a form of text-based communication, in real or differed time, between two or more individuals (units or entities). The text is sent through devices connected to a network.

Currently, it is common to find messaging systems on the internet, offering easily accessed specific services, most of which are based on TCP/IP.

For the specific military case, messaging is the main path of data communication between Command and Control center and the operational tactical units.

"The implementation of communication networks in military settings confronts important challenges that must be considered before reaching a practical application. In the first place, diverse types of airborne units exist, like airplanes and helicopters, which are in the combat space, implying different degrees of mobility that must be managed. Meanwhile, land or naval units face variable environmental settings that affect in different ways the propagation of radio-frequency signals. These conditions faced by the tactical units translate into limited bandwidths, intermittent connections, and a high probability of delay in information transmissions, situations that must be considered when implementing a data communications system" (*Michael J. Ryan, 2002*).

A messaging system seeking to satisfy military needs must comply with the following general requirements:

- Privacy.
- Authenticity.

- Certification.
- Integrity.
- Non-repudiation.
- Availability

The communications system developed is able to facilitate interconnection through the communication networks that are currently part of the existing technological infrastructure, adequately integrate their functionality, and satisfy the requirements of the joint operations undertaken. Additionally, the communications system permits data exchange via different transmission media and among equipment from different manufacturers, guaranteeing the system's interoperability.

Design Methodology

In general, the design of the components of the messaging system was carried out in parallel manner. However, each component was developed by following a particular methodology.

To develop the architecture for the information system, an incremental debugging scheme was used based on the architecture centered design method (ACDM), developed by Anthony Lattanze at Carnegie Mellon University, and architecture points of view were those elaborated by Nick Rozanski and Eoin Woods.

For the communications design protocol, we kept in mind criteria like: security, bandwidth restrictions and data optimization (selection of particular data of the operation under execution), which would permit assigning greater added value to the Command and Control system. Likewise, we considered the design of the architecture of the Command and Control system for information access, bearing in mind security mechanisms. The design protocol was based on the methodology described in the book "Design and Validation of Computer Protocols" (*Gerard J.Holzmann, 1991*).

Software design was carried out by using the Rational Unified Process (RUP) methodology, which is a software development process and along with the Unified Modeling Language (UML) constitutes the standard methodology most often used for analysis, implementation, and documentation of systems aimed at objects. The messaging system developed comprises six different applications that interoperate bearing in mind the protocol and security criteria, bandwidth restrictions, and data optimization previously proposed. Four of these applications were developed in Visual C++ language and two others in Visual C#.

The methodology employed in designing the system's security was based on public code cryptography (elliptic curves, due to code size), both for data messages and for network administration messages. During the design of the system's security, we kept in mind aspects like: the confidence ratio based on the levels of the staff that plan the operations and the processes of Authentication, Authorization, and user access to the network, with encrypted mechanisms.

The messaging system developed is formed by different network elements, which are:

- The tactical units
- The access nodes
- The messaging node
- The security node
- The Command and Control node (SIC2)

These network elements develop specific functions within the messaging system to permit safe and reliable exchange of information, so that said information is transmitted exactly to where it is required and at the moment requested.

The Messaging System permits data exchange via different transmission media and among equipment from different manufacturers, guaranteeing interoperability of the system.

Due to security reasons, the System will provide access to the messaging services according to parameters of authentication, authorization, and certification, which must be configured and negotiated in each case in the security node.

The messaging node implements all the necessary functionality for message management and

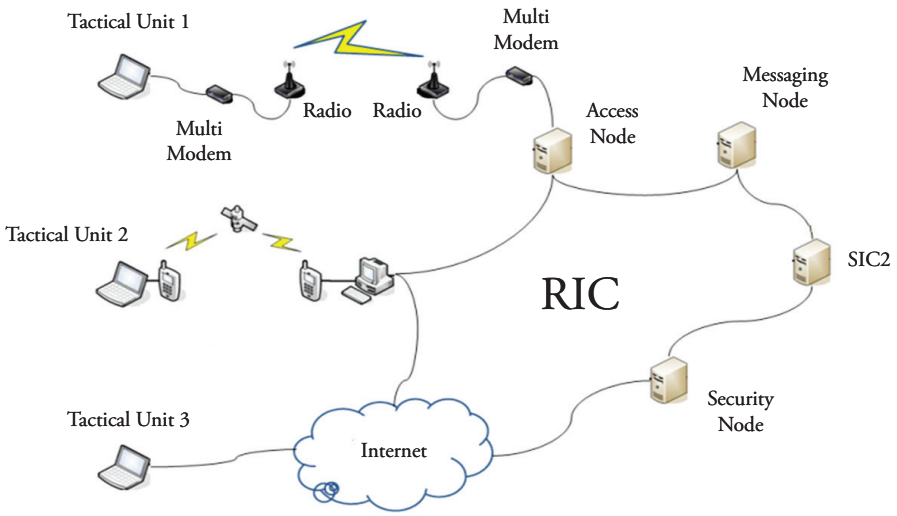
permits their exchange between the tactical units and the SIC2 node, for which adequate formats and technologies have been established to permit proper information exchange.

The access node is in charge of carrying out gateway functions among the different communication technologies integrated in Command and Control systems. There will be as many as it is convenient to reach the territorial coverage of the theaters of operations.

For the tactical units, two types of applications were developed, depending on the means of communication: one for radio-communications and another for IP communications. The radio-communications application accesses the network through the access node.

The following figure shows a general scheme of the messaging system developed.

Figure 1. Messaging system general scheme



Theoretical Framework

The first step in the process of the design protocol is to analyze the operational setting and establish the set of communication requirements. The requirements are established in general terms including the following:

- Global operational setting (peace/exercise/war).
- Number of platforms (with prevision for additional participants).
- Deployment of the platforms.
- Data to be transmitted and received by each platform (or group of platforms if this is how matters are facilitated) and their characteristics in terms of:
  - ✓ Type of platform.
  - ✓ Quantity.
  - ✓ Security, including requirements of privacy, authenticity, integrity, and non-repudiation.
  - ✓ Type of message.
  - ✓ Network administration messages

For proper network operation, it is essential to have coordinated use of cryptography; hence, the availability of the codes is totally indispensable for communications to be possible.

Information exchange in the system

The system's technical functions encompass network management and exchange of tactical information related to the following 11 tasks of operational aspects; these technical functions are:

- Information exchange of the System and of

Network management.
- Precise Identification and Location of Participants (PILP).
- Air surveillance.
- Surface surveillance (Maritime).
- Submarine surveillance (Maritime).
- Land surveillance.
- Electromagnetic surveillance.
- Electronic warfare (EW)/ Intelligence.
- Mission management.
- Control.
- Information management.

Types of Messages

The types of messages derived from the design protocol are:

Table 1. Types of existing messages in the protocol of the messaging system prototype

Type	Name of Message
01	Position of Vessels, Submarines, and Boats
02	Position of Airplanes and Helicopters
03	Position of land units
04	Contact report
05	Code request
06	Code delivery
07	Chat
08	Chat reception
09	Connection request
10	Connection data
11	Connection report
12	Table of processes
13	Publication of Tactical unit IP codes
14	Delivery of configuration
15	Disconnection
16	Verification of tactical unit IP status
17	Response of verification of status
18	Publication of tactical unit Radio codes
19	Verification of tactical unit Radio status
20	Response to initial broadcast

These messages contain the following information: A clearly transmitted heading (without cryptography) and encrypted data.

It is important to highlight that the data in each type of message were carefully selected to provide the basic information according to the type of message and additional data that permit feeding operational analyses and simulation processes in the operations center, which gives added value to the system developed.

Identification of Vocabulary Format of Protocol Messages

According to protocol services, all the information needs are gathered in the following types of messages:
- Link control messages
- Participant identification and location messages
- Contact messages
- Tactical unit configuration messages
- Informal messages (chat)

Message data may be "Free Text" or "Fixed Format". Free Text messages are primarily used for chatting, although other types of data may also be exchanged as long as the participants agree on the format.

Fixed Format messages, as the name indicates, have a defined format, onto which information may only be introduced in the fields disposed for such purpose.

The message label indicates its function.

These 20 types of messages (see Table 2) gather the information necessary to obtain the tactical panorama in the Command and Control node, according to the strategic level this implies.

Guidelines for Message Exchange

To control the exchange of messages, privacy, integrity, authenticity, and non-repudiation services must be implemented, requiring the following guidelines:

Table 2. Message labels

TYPE	NAME OF MESSAGE	TYPE OF OPERATION
01	Position of Vessels, Submarines, and Boats	Participant identification and location messages
02	Position of Airplanes and Helicopters	Participant identification and location messages
03	Position of land units	Participant identification and location messages
04	Contact report	Contact messages
05	Code request	Link control messages
06	Code delivery	Link control messages
07	Chat	Informal messages
08	Chat reception	Informal messages
09	Connection request	Link control messages
10	Connection data	Link control messages
11	Connection report	Link control messages
12	Table of processes	Link control messages
13	Publication of Tactical unit IP codes	Link control messages
14	Delivery of configuration	Tactical unit configuration messages
15	Disconnection	Link control messages
16	Verification of tactical unit IP status	Link control messages
17	Response of status verification	Link control messages
18	Publication of tactical unit Radio codes	Link control messages
19	Verification of tactical unit Radio status	Link control messages
20	Response to initial broadcast	Link control messages

a. Privacy is implemented through cryptographic procedures of the data transmitted; these procedures will be performed via code mechanisms through elliptic curves.

b. Every station on the network must generate its own private code, and through a procedure it must generate a public code that stems from the product of its own private code and the ellipsis point; thereafter, it must publish such in the security node delivering it certified.

c. Every station requiring delivery of a message must have a public code from the addressee, which is sent by the security node at the moment of the connection and, with a procedure generate the private code of the communication that results from its own private code, the addressee's public code, and the point of the curve, to proceed to encrypt with AES.

d. The authenticity is made on the security node and it is conducted through an encrypted message that the security node can decrypt if and only if the originator is whom it says it is.

e. Integrity is given if the decrypted message has a coherent meaning inasmuch as the cryptogram is related to all the contents of the message.

f. The functionality of "non-repudiation" is given through the messaging node, which registers all the events of all the communications of the system.

g. The transmitting station must codify the data by using the code resulting from the point of curve *p*, and the code from addressee *Kb*; for its part, the addressee does the same to determine the code with the same point on curve *p* and the code from originator *Ka*, then encrypts using symmetric AES.

$$Mns\ Ak = A\ \{Ka*(p*Kb)\} \quad (1)$$

$$Msg\ Bk = B\ \{Kb*(p*Kb)\} \quad (2)$$

h. The transmitting unit encrypts the message with the code resulting from its own code, the addressee's code, and the ellipsis point, and it is directed to the messaging node for its distribution.

i. The messaging node receives the message and stores it encrypted and when the addressee unit is connected it proceeds to send the message, which is already encrypted with the addressee code.

j. The tactical nodes send the encrypted messages with the addressee code, through the messaging node.

k. At the start of a communication, every station must carry out an identification and authentication procedure on the security node.

l. The messaging node must lead to registering communication with the following data: Type of message, identification of originator, identification of addressee, group date hour sent, group date hour delivered to the addressee, the code gram and the verification digit of "pending".

m. Messages of interactive communications (chat) are considered informal, but are also controlled by the messaging node.

n. Every tactical unit, when started, sends a verification message to the security node to corroborate the status of its publication of codes.

o. The security node responds to the verification message affirmatively or negatively, depending on whether it has or not published the valid code.

p. The tactical units may request disconnection from the network at any time, an important situation to keep the system from sending messages, but have them stored by the messaging node.

q. When a tactical unit is going to start operating or has any novelty in its configuration, it must send a configuration message to the Command and Control node. The message includes the relevant aspects of the conditions in which the unit operates.

r. The staff preparing the order of operations must generate and publish the codes of all the units participating in such. This is done through the message "publication of codes", which is sent to the security node with the code destined for said purpose.

s. Upon a message of publication of codes, the security node respond with a message "connection data" that contains the table of public codes, including the published code, and the table of identification of all the units reporting.

t. The tactical units once configured and with its codes reported, may request connection to the network through the message "connection request" sent to the security node.

u. The security node, after authenticating it, responds to this last message by sending it a message with the updated tables of public codes and identification.

v. Likewise, every time a unit requests connection, the security node will send a message "connection report" to the "Command and Control" and "messaging" nodes. This message contains the identification of individuals connecting, their IP (in case it is

a tactical unit via radio, will place the IP of the corresponding access node) and the tables of public codes and identifies.

For the protocol of the messaging system a strategic level has been considered so that the types of messages that should be transmitted are only those referring to the tactical panorama, given that this strategic level merely requires supervision functions and not direct command, although if the command is executed such must be executed through the chain of command and not directly.

System's Security

To design the system's security, we adopted a public code cryptography scheme to ensure the data transmitted from and to the systems, minimizing exposure of sensitive information and, thus, avoiding the possibility of communications in transit of being intercepted and decoded.

The security implemented for the prototype of the messaging system developed, although based on public code cryptographic security, is able to protect the whole system, given that to perform any process within the system, it is necessary to conduct a series of validations, authentications, authorizations.

Description of the Security System

The security of the messaging system is based on that all processes are authenticated, authorized, and certified by an ECDH public code cryptographic system.

Verification processes made in the security system are:

- In case a user is completely new for the system, that user must register (publish codes) before accessing the system's functionalities, through a confidence mechanism.
- Access to the Messaging System is restricted by the use of codes assigned to users. Only units previously authenticated and authorized may enter the system.
- Access of these units to work operations on the system will be according to the roles, permits, and profiles previously established. Authenticated users must be authorized according to the profiles, roles, and permits defined.
- To access the system, the established digital signatures must be used to guarantee the integrity of a message and, thus, be able to associate it with the author to ensure that the contents have not been modified and its origin is validated.

In the messaging system developed, the security node is in charge of performing all these validations. Once the unit is authenticated, it is removed from the system and notification is sent to all the active elements on the network, reporting the event. All the messages (notifications) will be encrypted.

Encrypting algorithm used

The elliptic curve cryptography (ECC) used in the messaging system is defined as a variant of asymmetrical or public code cryptography based on the mathematics of elliptic curves. Its authors argue that ECC could be quicker and may use shorter codes than ancient methods -like RSA - while providing an equivalent level of security. The use of elliptic curves in cryptography was proposed independently by Neal Koblitz and Victor Miller in 1985.

Asymmetrical or public code cryptography systems use two distinct codes: one may be public, the other is private. Possessing the public code does not provide sufficient information to determine the private code. These types of systems are based on the difficulty in finding the solution to certain mathematical problems. One of these problems is the so-called discrete logarithm. Finding the value of b given equation ab = c, when a and c are known values, may be a problem of exponential complexity for certain large-size finite groups; while the inverse problem, discrete exponentiation,

can be efficiently evaluated by using, for example, binary exponentiation.

An elliptic curve is a flat curve defined by an equation in the form of:

$$y^2 = x^3 + ax + b \tag{3}$$

With the set of points G that form the curve (*i.e.*, all the solutions of the equation plus a point O, called point on the infinite) plus an additive + operation, an abelian group is formed. If coordinates x and y are chosen from a finite field, then we are in the presence of a finite abelian group. The problem of the discrete logarithm on this set of points (PLDCE) is thought to be more difficult to solve than that corresponding to the finite fields (PLD). Thus, the lengths of codes in elliptic curve cryptography can be shorter with a comparable level of security.

The following shows a brief mathematical introduction to the algorithm:

Let p > 3 prime. The elliptic curve

$$Ey^2 = x^3 + ax + b \tag{4}$$

over Z_p is the set of solutions (x, y) $\in Z_p \times Z_p$ in the congruence

$$y^2 = x^3 + ax + b \pmod{p} \tag{5}$$

Where $a,b \in Z_p$ are constants so that

$$4a^3 + 27b^2 \neq 0 \pmod{p} \tag{6}$$

An additive operation is defined as follows: Considering that $P = (x_1, y_1)$ and $Q = (x_2,y_2)$ are points on E and O is a point on the infinite. If $x_2 = x_1$ and $y_2 = -y_1$, then $P + Q = O$; on the contrary $P + Q = (x_3, y_3)$, where $x3 = \lambda_2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, and

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \\ \dfrac{3x_1^2 + a}{2y_1} \end{cases} \tag{7}$$

Finally, we define

$$P + O = O + P = P \forall P \in E \tag{8}$$

With this we may show that E is an abelian group with element identity O. It is worth noting that the inverse of (x, y) (written as -(x, y) given that the operation is additive) is (x, -y), for all $(x, y) \in E$.

According to the Hasse theorem, the number of points #E contained in E is close to p. More precisely, the following inequality is satisfied:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p} \tag{9}$$

Given that it is known that any prime order group is cyclical, what is required is to find a subgroup of E in the order of q (q prime) to have an isomorphism with Z_p where the problem of the discrete logarithm is untreatable. In this instance, being α a generator of the cyclical group (which could be any element of the group different from O, the identity), we may calculate the "powers" of α (which are written as multiples of α because the operation of the group is additive).

Algorithm of Code Generation

In the cryptographic use, a specific base point G is selected and published to use with the curve *E(q)*. A random integer k is chosen as private code, and then the value $P = k*G$ is shown as public code (note that the supposed difficulty of the PLDCE implies that k is difficult to deduct from P). If the tactical unit A (TUA) and the tactical unit B (TUB) have private codes *kA* and *kB*, and the public codes PA and PB, then TUA could calculate $kA*PB = (kA*kB)*G$; and TUB can obtain the same value given that $kB*PA = (kB*kA)*G$.

This permits establishing a "secret" value that both TUA and TUB can easily calculate, but that is very complicated to derive by a third party. Additionally, TUB cannot learn anything new on kA during this transaction, so that code used by TUA continues being private.

The methods used in practice to encrypt messages based on this secret value consist in adaptations of older cryptosystems from discrete logarithms originally designed to be used in other groups. Among those we could include Diffie-Hellman, ElGamal, and DSA.

Performing the necessary operations to execute this system is slower than for a factorization system or full-module discrete logarithm of the same size. In any case, the authors of ECC systems believe that the PLDCE is significantly more complicated than the factorization problems or of PLD and, thus, the same security may be obtained via shorter code lengths by using ECC, to the point that it may be faster than, for example, RSA. The results published until now tend to confirm this, although some experts remain skeptical.

Elliptic curve cryptography has been broadly recognized as the strongest algorithm for a given code length, for which it may be useful on links with very limited bandwidth requirements.

NIST and ANSI X9 have established minimum requirements of code size of 1024 bits for RSA and DSA and 160 bits for ECC, corresponding to an 80-bit code symmetrical block. NIST has published a list of recommended elliptic curves of five different code sizes (80, 112, 128, 192, and 256). In general, the ECC over a binary group requires an asymmetrical code double the size of that corresponding to a symmetrical code.

Analysis of Confidence

Certicom is the main commercial company for ECC; this organization has 130 patents and has issued licenses on technology to the National Security Agency (NSA) for 25 million dollars. Certicom has also sponsored several challenges to the ECC algorithm. The most complex solved, until now, is a 109-bit code, which was broken by a team of researchers in early 2003. The team that broke the code used a parallel massive attack based on the 'birthday attack', through more than 10,000 Pentium-type PCs working continuously during 540 days. It is estimated that the minimum code length recommended for ECC (163 bits) would require 108 times the resources used to solve the problem with 109 bits.

Communications Network

The need to offer a reliable and efficient communications system is ever-more important in military operations, given that the different systems supporting a mission depend greatly on a communications infrastructure with enough capacity for transport of information that guarantees the availability of such at the indicated time and place.

The messaging system developed contemplates data exchange by networks with different transmission media, from high and low bandwidth, considering security mechanisms like information encryption, for information transference through an asynchronous communications mechanism where data transmission takes place in deferred time and in real time.

The data communications system is supported by the current network infrastructure, which defines characteristics for information transference and integration of services, aspects that should be kept in mind to obtain the maximum advantage from the resources offered by said network. Likewise, the system is supported on the RF communication systems (tactical radios), which should guarantee the necessary measures to maintain the operational channel.

Description of the Communications Network

The networks available for the development of the messaging system were:

- IP network with repeaters located in high places, with incomplete coverage of the possible theaters of operations.
- VSAT network with fixed and mobile land stations to cover theaters of operations outside the prior coverage.
- Low orbit satellite telephone network to complement the coverage previously exposed.

These networks imply an availability of restricted bandwidth, which was proven through experimentation. For VHF and UHF with a 25-KHz theoretical bandwidth, we accomplished a velocity of 2.4 kbps in the tests and bearing in mind these results, we measure performances. With low orbit satellite telephone service we experimented with IRIDIUM in two services: short bus data and data kit, obtaining the following performance: a velocity of 9.6 kbps with some restrictions:

1. Necessity for clear skies and without obstacles.
2. We noted low availability, especially in jungle zones.

It is worth noting how limited the bandwidth is for any of the means used by the tactical units to transmit information; thereby, becoming a limiting factor of the design.

Coherence among designs

To view the coherence among the most important components of the messaging system developed, the following figure shows the interrelation among them and their spiral development, to accomplish optimization of the system.

Figure 2. Spiral design diagram

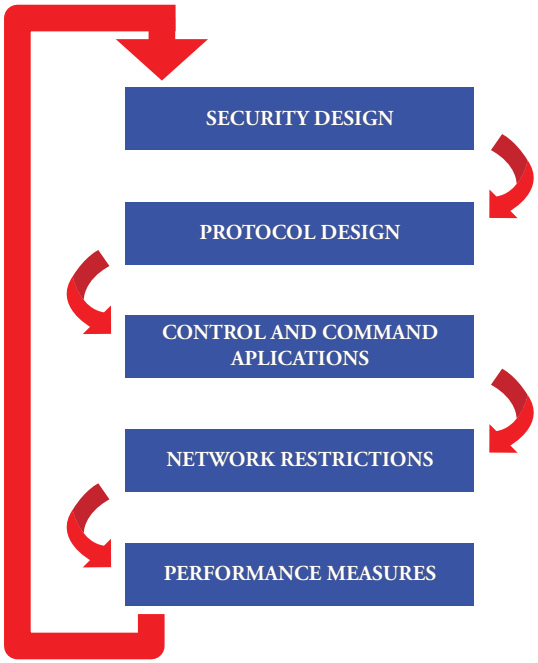


Figure 3. Tactical panorama

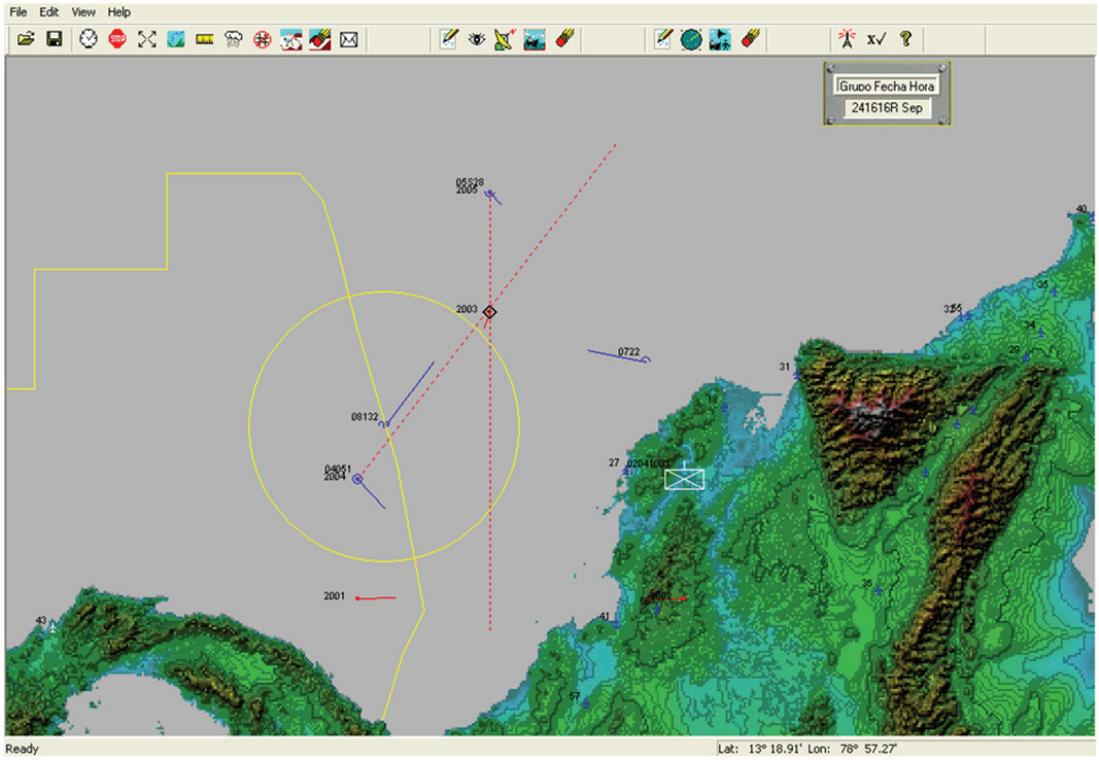


Figure 2 shows how the designs of the system's components create relationships of interdependence and as they advance on the spiral, the system's performance improves, adjusted to the restrictions established.

Results

Figure 3 shows a tactical panorama for a situation of intervention among a vessel, a submarine, an airplane, a helicopter (identified in blue) and an army company (identified in white) from the same forces.

The operation is of maritime interdiction in which the units have made their reports of position and configuration to the Command and Control node. Additionally, they have made contact reports, thus:

- An Electronic Support Measure (ESM) detection report from the submarine (this detection appears in red dotted line in Figure 3).
- An ESM detection report from the surface unit, correlated with the prior report.

The surface unit launched the helicopter to intercept the contact identified in the Command and Control center, from the ESM correlation.

The prediction of the reach of the helicopter radar may be noted in Figure 3, as made at the Command and Control center, with a 50% probability of detection, taking as a base the data from the configuration report, which includes the characteristics of its search radar and the characteristics of the target sought.

Another important factor is that position simulations are made (in function of time) in the Command and Control center, both of its units and of the contacts, guaranteeing a very good approximation to what will happen in real time.

Conclusions

Herein, we introduced the design of a messaging system, characterized by the coherence among its components, designed to obtain the tactical panorama in a strategic center.

Through this development, we showed that it is possible to have a military messaging system by using a low bandwidth communications network. We obtained a security level that satisfied the system's requirements, using public code cryptography, with a code space of 2192, which guarantees privacy between "secret" and "ultra secret" levels (according to NSA).

The messaging system developed guarantees privacy, integrity, certification, authenticity, and non-repudiation of the information transmitted and of the factors intervening in Exchange processes of such.

Finally, it must be highlighted that the messaging system contemplates mechanisms to support the asynchrony of the military reports made.

References

HUTCHERSON, N. (1994). C*ommand & Control Warfare: Putting another tool in the war-fighters database.* Alabama: Air University Press.

MCCABE, J. D. (2007). *Network analysis, architecture, and design*. Burlington: Morgan Kauffman.

MICHAEL J. RYAN, M. R. (2002). *Tactical communications for the digitized battlefield*. Norwood: Arthec House, Inc.

New York: Institute of Electrical and Electronics Engineers, Inc. Teare, D. (2007). Designing for Cisco Internetwork Solutions (DESGN). Indianapolis: Cisco press.

RUSSELL, M. (10/08/2004). http://www.ibm.com/. Recovered 07/07/2010, from Quality busters: Forget the environment. The importance of non-functional and operational requirements: http://www.ibm.com/developerworks/web/library/wa-qualbust1/

SNYDER, F. (1993). *Command and Control: The Literature and Commentaries*. Washington D.C: National Defense University Press Publications.

Software Engineering Standards Committee of the IEEE Computer Society. (1998). IEEE Guide for Developing System Requirements Specifications.

United States Department of Defense. (2003). MIL-STD-961E, Defense and program-unique specifications format and content.