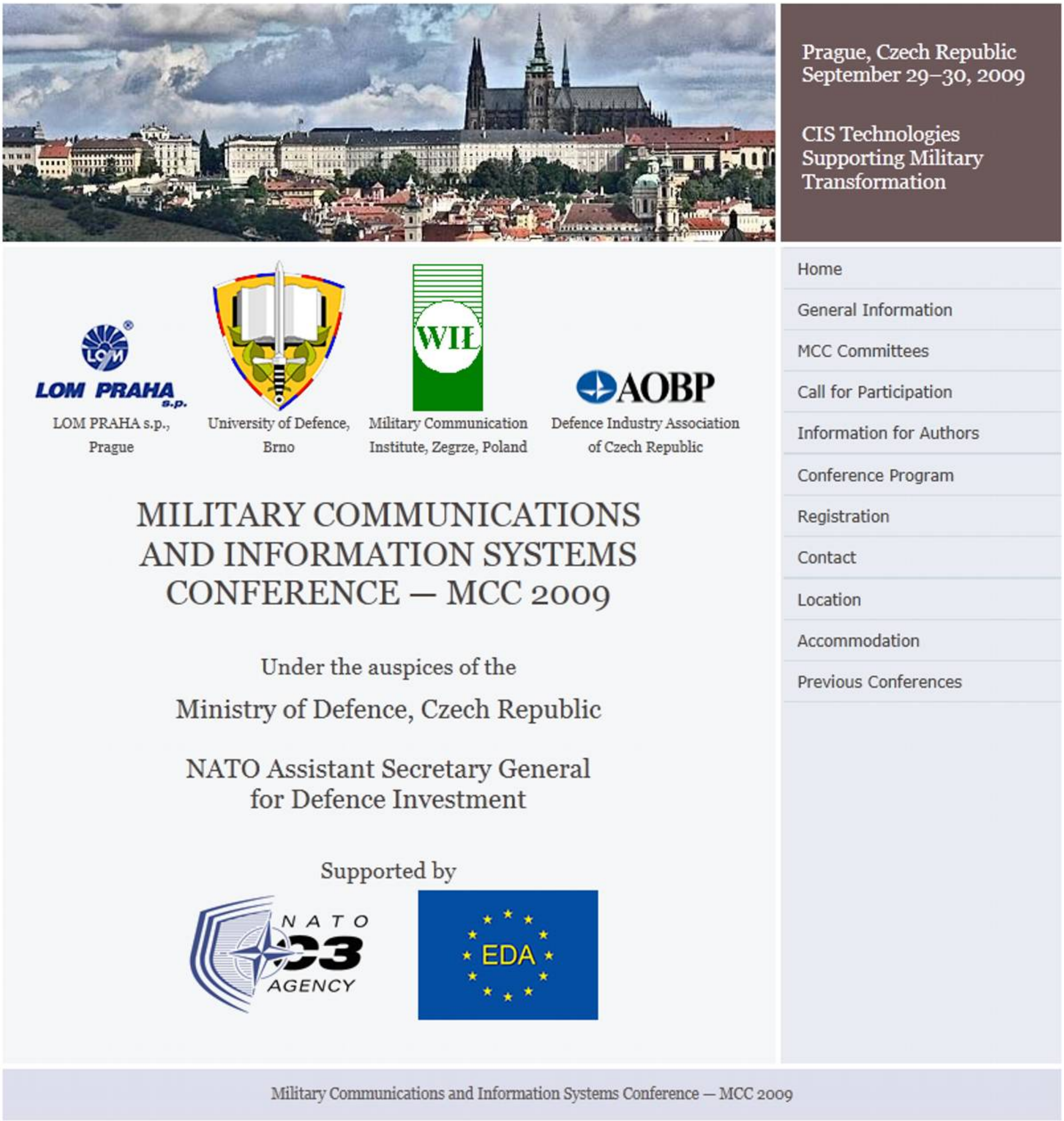


Prague, Czech Republic
September 29–30, 2009

CIS Technologies Supporting Military Transformation

LOM PRAHA s.p., Prague

University of Defence, Brno

Military Communication Institute, Zegrze, Poland

Defence Industry Association of Czech Republic

MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS CONFERENCE — MCC 2009

Under the auspices of the

Ministry of Defence, Czech Republic

NATO Assistant Secretary General for Defence Investment

Supported by

Military Communications and Information Systems Conference — MCC 2009

JASMINE system: network centric concept and practical solution

Tomasz Ziemowit Kosowski, Łukasz Apiecionek
TELDAT, Kijowska street 44, 85-703 Bydgoszcz, POLAND
phone +4852 341 90 (729), fax +4852 341 97 21, TKosowski@teldat.com.pl
phone +4852 341 90 (727), fax +4852 341 97 21, LApiecionek@teldat.com.pl

ABSTRACT

NATO Network Enabled Capability (NNEC [1]) is one of the most common concepts which is developed for the needs of network centric systems in order to facilitate and speed up decision-making process on the battlefield. Systems compliant with the NNEC are designed to collect data from the battlefield with the sensors and systems that provide information and transfer them to an overarching points where decisions are made about actions that should be taken. The actions are made with the help of elements called effectors. All elements of the NNEC environment interact with each other in a distributed concept.

NNEC is a key theme developed by NATO in the process of transformation Allied Command Transformation (ACT [2]). The purpose of this concept is to improve the quality of the information exchange in network centric operations and increase availability and speed of its transmission. Compliance with the requirements of the concept is being implemented by individual countries in different ways.

The purpose of this paper is to present the concept and practical solution of Polish network centric system JASMINE which is based on the concept of NNEC.

Keywords: JASMINE, Network Centric Warfare, NNEC

1. NNEC CONCEPTUAL MODEL

The task of systems based on NNEC concept is, at first step, to collect data from users of the battlefield visualization systems, from sensors mounted in the devices on the battlefield (*military vehicles, command vehicles, aircrafts, choppers, boats, etc.*) and from other platforms which can provide information.

The collected information is sent then to higher level command posts, which act in parallel way, where the basis for their decisions shall be taken. The most important alteration, introduced in the NNEC, compared to a traditional hierarchical approach to decision-making process is the dissipation of the decision nodes in the network topology of the mesh-type.

NNEC conceptual model was presented in Figure 1. The model consists of seven basic components [1]. The fulfillment of all of them determines obtaining network centric environment consistent with the NNEC, which provides improved quality of decisions, cohesion of the effects and common deployment and sustainability. The model reflects the cycle of decision-making process within the NATO. Data and information is collected and processed to provide situational awareness, which is assessed on the basis of knowledge of the opponent and the likelihood of action that he may take. Direction of possible actions determined in the joint environment, with a military and political support. Actions are taken by means of the elements referred to as Effectors in order to achieve the desired effect.

Component Information Sphere is assigned as responsible for the collection of information that is exchanged. Collectors task is to collect and process data which has not been previously processed. Decision Makers process and recognize collected data to select the appropriate action, which is then performed using elements from Effectors component. Human Process component includes all elements associated with human interaction on the network. Information Assurance / Security component is responsible for data security and certainty of delivery.

All these components are combined and can work together with the help of NATO's

Network and Information Infrastructure (*NII*), which describes the structure of a network in context of the communication, opportunities for exchange of data, personnel and processes responsible for gathering, processing, storage, distribution and management of information. It's task is to provide connections between individuals and organizations. NII consists of four layers [1]: communication, network, computers, services.

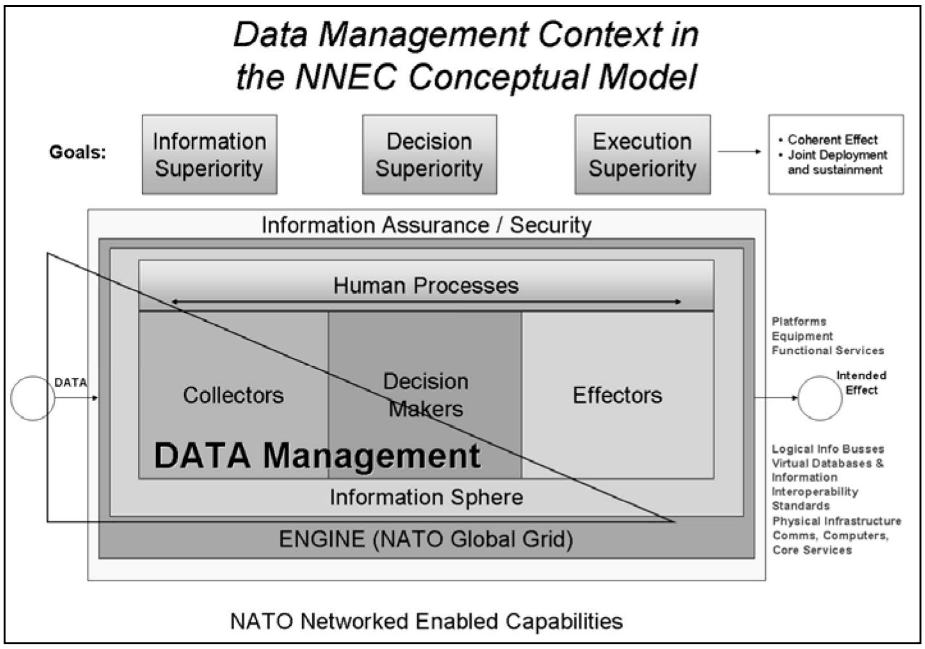


Figure 1. Diagram of the flow of the information in the NNEC [2]

NII covers all possible locations, including military stationary command posts, mobile platforms, static network as well as units on the battlefield. As a point of access to external systems, Information Exchange Gateway [1] element is used.

The NII module operates within second and third layer of the Open System Interconnection model [3] and consists of the following set of communication services [1]: satellite communications, wireless communications, tactical radio links, tactical data connection.

As a transport layer protocol IP is used, calling communication EoIP – Everything over IP – everything through Internet Protocols [4]. It is assumed that the network must ensure the quality of the transmission – Quality of Service (*QoS*) rules, coding and data management services, Service Level Management (*SLM*).

For NII layer the network access points are defined, which should be able to work with the following set of protocols:

- Internet Protocol (*IP*) version 4 and 6;
- Open Shortest Path First (*OSPF*) version 2;
- Border Gateway Protocol (*BGP*) version 4;
- Transmission Control Protocol (*TCP*);
- User Datagram Protocol (*UDP*);
- IP tunneling, IP version 4 through version 6.

In terms of functional division in the module NII one can distinguish:

- Enterprise Services Management (*ESM*) – a network performance monitoring, configuration and problems detection;
- Messaging – an opportunity to exchange information between users or applications;
- Discovery – the process of finding information or services;
- Mediation – software that helps to insure, translate, aggregate, combine and integrate

data and metadata;
- Collaboration – allows users to share selected network capabilities;
- User Assistant – automatic aid opportunities services;
- Information Assurance / Security – a feature that ensures the confidentiality, integrity, availability, identification, authentication, logging events, and information security of users, applications and networks;
- Storage – the physical and virtual space for storing data on the network;
- Application – Infrastructure for the storage and management of distributed features that work in real-time.

NNEC describes data concepts as a shared space of data, which provides it for further processing to the services. Data consists of pure information and information about services as well, which is known as a data directories. Data directories provide information about points of access to the services and their configuration.

2. JASMINE SYSTEM AS A PRACTICAL IMPLEMENTATION OF NNEC

JASMINE system structure is based on a component model. The NNEC concept indicates the dispersion of decision-making places, so elements of JASMINE system were designed to be able to work at all military levels, starting from the highest to the brigade level or even at the mobile battlefield unit [5] [6]. The system consists of hardware and software. JASMINE is a hardware platform appropriate for the software modules which contains Management Software for JASMINE system, C3IS JASMINE and IOS TELDAT. This division appeared because of the need for fast and stable delivering of common operational picture. IOS TELDAT is responsible for providing software control over the hardware. The fact of clear separation of this component makes the hardware testing easy, fast and reliable. Management Software for JASMINE is a diagnostic and management component which includes the end-user services for configuration and monitoring hardware layer and for setting security policy. C3IS JASMINE components represent current trends in network centric systems and they are consistent with the NNEC concept and with the most common interoperability standards that are used in the NII layer. Network and communication layers of NII are implemented in JASMINE, as well as some of the NNEC components. The rest of the NNEC elements is implemented in the software modules.

The main advantage of the JASMINE system is its high flexibility and easy way of configuration, which shortens the time needed for achieving operational condition. JASMINE system equipment and its interoperability have been tested on the national and international exercises, where the wide range of provided services were presented [7] [8]. The system was also tested in the mobile solutions [9] [10].

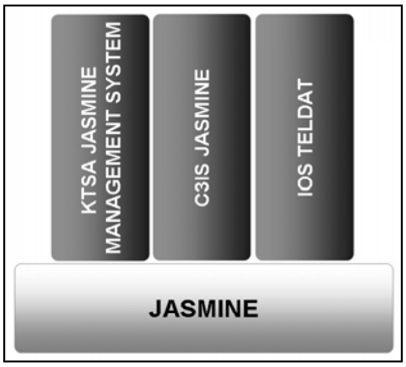


Figure 2. JASMINE subsystems

2.1. NII component realization in JASMINE system

JASMINE system design was prepared in accordance with NNEC concept, so following layers can be distinguished: network, communication, computers and services. There are three version of JASMINE system in network layer: mobile, shelter and predefined for mobile vehicle. Most important components are Router Box, LAN Backbone Box, WAN Box, Server Box, LAN Access Box, WAN Access Box – IP integrator for radio connections, IOP-SHDSL, IOP-OPTO, WLAN for wireless connection, VoIP Terminal, VHF/HF Gateway. They are used for building high efficient network designed for all military levels. These networks work in IP technology in battlefield conditions.

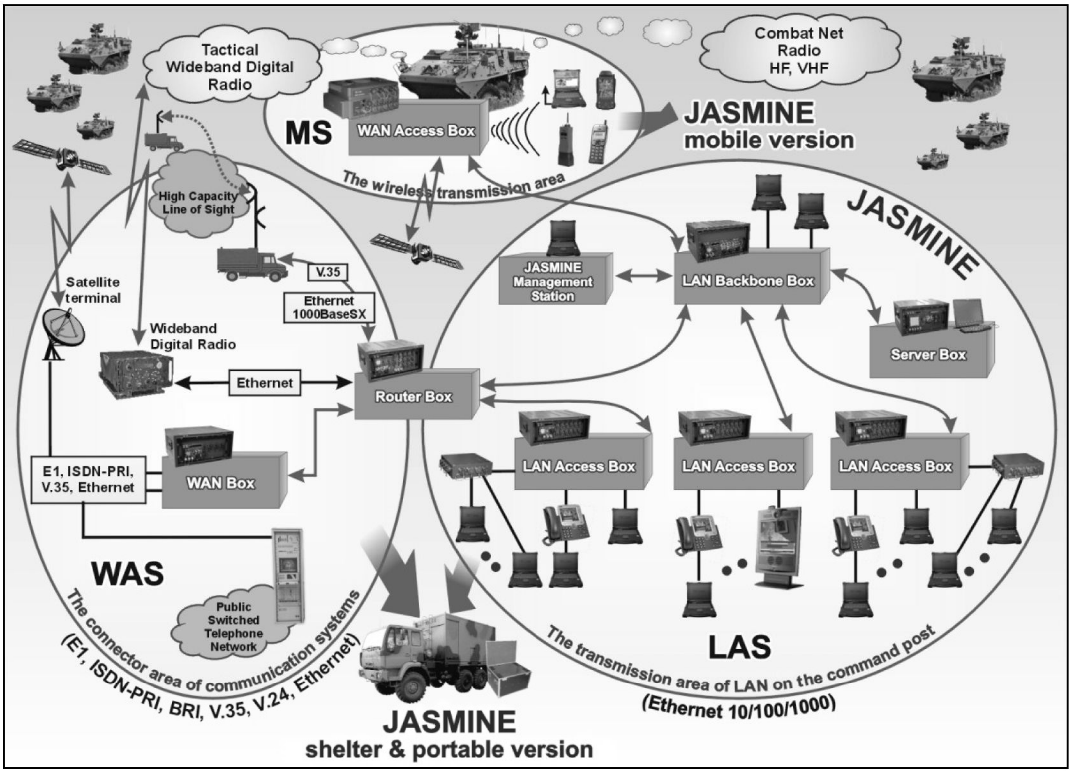


Figure 3. The idea of military command and communication using JASMINE system

In NII communication layer JASMINE system provides full IP platform on every level. NNEC SIOP (*Service InterOperability Points [4]*) implementation in JASMINE could work in all, mentioned in documents [4], protocols: IPv4 and IPv6, OSPF v2, BGP v4, TCP, UDP. Additionally, JASMINE SIOPs are able to work with many other protocols for increasing interoperability with different systems. Their implementation provide such additional protocols as RIP v1 and RIP v2, EGP, EIGRP. It provides also IPv4 tunneling through IPv6, IP in IP tunneling and GRE (*Generic Routing Encapsulation*) tunneling. Moreover there is possibility for building separate network using VRF (*Virtual Routing Forwarding*) technology. Connection to other systems could be made using interfaces described by NNEC concept [1]. QoS working with ToS (*Type of Services*) field of IP header is used for delivering IP packets in appropriate quality level. JASMINE system provides all kind of required communications types: satellite, wireless, VHF and HF radio and cable connections. There are components which are dedicated for operator workstation and server machine. Hardware platform is a baseline for providing services according to appropriate security levels. C3IS JASMINE system contains most of main services. This component is responsible for interoperability with Command, Control, Communication and Information Systems. It consist of the following systems:

- Database System Services:
  - SRV B2/B3 – services providing access to Multilateral Interoperability Programme databases in versions B2 and B3;
- Configuration and Management System:
  - Viewer – services managing other modules work;
  - Guard – services protecting work of other modules;
- Data Forwarding and Exchanging System:
  - MEM – additional services for Microsoft Outlook, creating support for sending and receiving messages using Message Exchange Mechanism Multilateral Interoperability Programme, version B2 and B3;
  - AES – Automatic Email Services creating additional replication channel for text messages;
  - ADatP-3 Gateway – services for operational data replication via ADatP-3 messages;
  - UKP3 (*On-board Communication System version 3*) Gateway – services providing access to UKP3 system;
  - NFFI (*IP1, IP2, SIP3*) –NATO Friendly Force Identification services enabling basic friendly operational data replication;
  - OPWS – services providing operational data forwarding from SRV B2/B3 module to end client, located in WWW browsers, via WebServices, giving the possibility of common operational picture visualization in WWW browser;
  - JCOP Gateway – access services for JIPS [16] protocol enabled systems;
- Operational Data Replication System:
  - BRM – prioprietary, TELDAT company solution. Services and protocol for optimized operational data replication via radio and other small bandwidth channels;
  - BRM Mobile –BRM services scaled for mobile tactical terminals of PDA type;
  - DEM B2/B3 – replication services compliant with Multilateral Interoperability Programme version B2 and B3;
- Conversion and Transformation System:
  - ADTA – units aggregation services;
  - ADatP-3 Manager –ADatP-3 files management services;
- Geographic Features Services:
  - TELDAT GeoServices – services providing geographic features via Web Map Service [18] and Web Feature Service [19] protocols.

Additional software: JASMINE Modules Management is prepared for quick and easy configuration of JASMINE system. Using graphical representation and drag and drop technology JASMINE components can be connected and later configured. KTSA Data Communications Resources Management System is a software prepared for monitoring and managing working network. It provides network monitoring tools using SNMP (*Simple Network Management Protocol*).

2.2. Information sphere component realization in JASMINE system

To achieve the objectives of Sphere Information component, requirements were divided into two groups of data: management data and operational data. For the purposes of the first group TELDAT Battlefield Directory server was developed, which is compatible with the LDAP standard, which makes it possible to use its services by many popular clients, such as email clients. From the point of view of operational data the database was developed based on the structure taken from the Multilateral Interoperability Programme C2IEDM and JC3IEDM model, both indicated by NATO [2]. The database (*databases*) can be accessed through the common interface, the service modules SRV B2 and B3.

2.3. Information assurance / security component realization in JASMINE system

Requirements of the Information Assurance / Security component generated the need to provide encryption and reserve access to data. Therefore, in the JASMINE system, to ensure confidentiality and integrity of the data, following elements were used: IPSec with the DES (*Data Encryption Standard*), 3DES (*Triple DES*) and AES (*Advanced Encryption Standard*) encoding, with MD5 (*Message-Digest algorithm 5*) and SHA (*Secure Hash Algorithm*) hashes and the AH (*Authentication Header*) and HMAC (*Keyed - Hash Message Authentication Code*) authorization. Additional component features include events logging and recording UKP3 subsystem voice chats, which allows monitoring of undesirable events in the network - such as security breaking trials, or other anomalies. Access to the system and its services is protected by cryptographic cards and authorized PIN codes. In order to add user authentication, RADIUS server service was used, working on IOS TELDAT, and the public key architecture (*called Public Key Infrastructure*) was implemented. So access to services is protected by the relevant certificates.

2.4. Collectors component realization in JASMINE system

The need for Collectors component, resulted in the creation of sensor devices interfaces in WAN Access Box and WAN Access Box V.2 UKP. In addition, the reporting of incidents by JASMINE VoIP Terminals, located on-board, was added. There exist buttons on VoIP Terminal which can send preset alarms when pressed. Besides sensor device interfaces, Light Chemical Detector for moving troops was developed. It was scaled to serve on the battlefield with tactical terminal of PDA type. All of these items inform about the occurrence of any incidents, which are then transmitted to the C3IS JASMINE system regardless of their source of origin.

2.5. Decision makers component realization in JASMINE system

The elements that are able to make decisions about future actions can be both services, operating within the system, and operators who can access system through a unified system interface - client application C3IS JASMINE. Each service on their own resolve process of assisting during issuing decision. The decision is based on the collected data.

2.6. Effectors component realization in JASMINE system

In order to implement the Effectors component, effectors interfaces in WAN Access Box devices and WAN Access Box V.2 UKP were implemented. These interfaces operate on a base of configurable events function, caused by elements of Collectors component.

In Data Manipulation and Presentation System the client applications has been distinguished, which are the point of access for end-users. Dedicated for a computer set is C3IS JASMINE application, which allows full control and visualization of operational data in accordance with the applicable standards of APP-6A [21], MIL-STD-2525B [22] and MIP Presentation rules [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37].

2.7. Human process component interfaces realization in JASMINE system

Human Process Component is in correlation with almost every other component. Thanks to the common client application interfaces, which are a point of access for human enabling management and manipulation of data within the system, operators are involved in the operations of many of the other components within the JASMINE system.

3. DATA MANAGEMENT AND DATA PROVIDING IN JASMINE SYSTEM

Maintenance and management of data in the JASMINE system is carried out in accordance with the NNEC concept. There is a shared space, represented by the database and access interfaces, which allow complete control over it. The role of interface is fulfilled by services SRV B2 and SRV B3, while the database is consistent with both MIP database models C2IEDM and JC3IEDM, which are recommended by the idea of NATO [2]. With additional modules, responsible for access to standardized interfaces, external systems are able to exchange information with other systems using, for example, protocols like NFFI IP1, IP2, SIP3 (*module NFFI - NATO Friendly Force Tracking [11] [12] [13] [14] [15]*), JIPS (*JCOP Gateway module [16]*), Data Exchange Mechanism Block 2 [17] and Data Exchange Mechanism Block 3 [18], MEM Block 2 and Block 3 [19] [20], NATO Vector Graphics [38] and ADatP-3 [39].

4. CONCLUSIONS

JASMINE system is a platform ready for the realization of any mission led by NATO in NNEC technology. In consequence of this and the fact of integration of hardware and software platform it constitutes a comprehensive network solution which is able to deliver an integrated common operational view. Supplied components perfectly fit in the presented approach to achieve network centric aims on battlefield. The single network architecture - IP technology - provides a simple, fast and secure access to services. A wide range of components allows the construction of a secure network and the classification of user access to both information and services. Overview of the different layers of concepts and elements of the NNEC in JASMINE context fully shows that JASMINE is designed in accordance with that concept, making it possible to easily extend the system in emerging standards for interoperability. The multitude of available logic and physical interfaces, allows combining the sophisticated, multi-networks and various systems to provide a free exchange of data, meeting the same idea of network centric on battlefield.

BIBLIOGRAPHY:

[1] ISSC NATO Open Systems Working Group, Allied Data Publication 34(ADatP-34) NATO C3 Technical Architecture Volume 2. Architectural Descriptions and Models. Version 7.0, 15.XII.2005

[2] Maj. Yavuz Fildis, J. Troy Turner, *NATO Network Enabled Capability (NNEC) Data Strategy*, 2005

[3] International Organization for Standardization, *ISO-IEC 7498-1:1994(E) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, 1996

[4] P. Copeland, M. Winkler, *Technical note 1197 Analysis of Nato Communications standards for the NNEC*, 2006

[5] W. Zawadzki, *JAŚMIN wkracza do armii*, Nowa Technika Wojskowa nr 5/2007

[6] H. Kruszyński, *Zastosowanie systemu JAŚMIN*, Nowa Technika Wojskowa nr 9/2006

[7] H. Kruszyński, Ł. Apiecionek, M. Dziamski, *JAŚMIN w warsztatach Combined Endeavor 2008*, RAPORT nr 06/2008

[8] M. Piotrowski, R. Palka, T. Z. Kosowski, *Interoperacyjność polskiego oprogramowania w praktyce,* Nowa Technika Wojskowa nr 7/2008

[9] T. Wachowski, *Mobilny JAŚMIN*, Nowa Technika Wojskowa nr 1/2008

[10] Ł. Pacholski, *Mobilny JAŚMIN na Żubrze-WD,* Nowa Technika Wojskowa nr 12/2008

[11] R. Porta, V. de Sortis, *Working Paper EPW002038-04 NFFI Service* Interoperability *Profile 3 (SIP3) GENERAL DESCRIPTION (version 1.0.0)*, 2008

[12] V. de Sortis, *Working Paper EPW002038-05 NFFI Service Interoperability Profile 3 (SIP3) TECHNICAL SPECIFICATIONS (version 1.0.0)*, 2008

[13] R. Porta, *REF. EPW002625-WP02 Friendly Force Tracking Hub (FFT-HUB) Functional Specifications (vers. 1.0)*, 2009

[14] *AC322(SC5)N(2006)0025 - Interim NFFI Standard for Interoperability of FTS*, December 2006

[15] *STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems*

[16] D. Dufour, J. Varanda, M. Postal, *Inf ormation Standard Definition Version 0.5.3 JCOP*, 2009

[17] Multirateral Interoperability Programme, *The C2 Information Exchange Data Model (C2IEDM Main)*, 2005

[18] Multirateral Interoperability Programme, *The Joint C3 Information Exchange Data Model (JC3IEDM Main)*, 2007

[19] *Mip Implementation Rules Annex C - Appendix1-ADatP-3_Message-Definitions B12-2 v1.0 03-Baseline_2.0*, 2006

[20] *Mip Implementation Rules Annex C - Appendix2-MIP_Messages-Definitions-1.0 03-Baseline_2.0*, 2006

[21] *APP-6A (STANAG 2019, Edition 4) Military Symbols for Land Based Systems*, 1999

[22] *MIL-STD-2525B, U. S. Department of Defense Interface Standard, Common Warfighting Symbology*, 1999

[23] *MIR - Annex F Control feature geometry rules*, 2006

[24] *MIR - Annex F Control feature geometry rules rationale,* 2006

[25] *MIR - Annex F Equipment storage rules,* 2006

[26] *MIR - Annex F Facility geometry rules,* 2006

[27] *MIR - Annex F Organisation storage rules,* 2006

[28] *MIR - Annex F Task and event geometry rules,* 2006

[29] *OWG Block 2 Core List for Equipment (APP 6 A, App E) with prioritization,* 2006

[30] *OWG Block 2 Symbology Core List with prioritization,* 2006

[31] *MIR Annex F Appendix 2-2 Generic geometry rules*, 2008

[32] *MIR Annex F Appendix 3-2 Control Feature geometry rules*, 2008

[33] *MIR Annex F Appendix 4-2 Facility geometry rules*, 2008

[34] *MIR Annex F Appendix 5-2-01 Action Task geometry rules*, 2008

[35] *MIR Annex F Appendix 5-2-02 Action Event geometry rules*, 2008

[36] *MIR Annex F Appendix 8-2 Convoy geometry rules*, 2008

[37] *MIR Annex F Main*, 2008

[38] *http://tide.act.nato.int/mediawiki/index.php/NATO_Vector_Graphics_(NVG)_Data_Format*

[39] *Allied Data Publication Number 3*

Means for operational data exchange in JASMINE System

Krzysztof Muchewicz, Łukasz Sierakowski
TELDAT, Kijowska street 44, 85-703 Bydgoszcz, POLAND
phone +4852 341 97 00 (785), fax +4852 341 97 21, KMuchewicz@teldat.com.pl
phone +4852 341 97 00 (759), fax +4852 341 97 21, LSierakowski@teldat.com.pl

ABSTRACT

Automation of business processes, effective exchange of information, fast reaction to the developments are the challenges that all the business and administration organizations face nowadays. The above mentioned are becoming increasingly important in the armed forces. These needs are met by Jasmine System produced by TELDAT Public Co. in Bydgoszcz. It allows to create ad hoc data communication networks, provides equipment and software necessary for battlefield communication. Jasmine system is composed of the devices and software produced by TELDAT. One of the elements of JASMINE system is C3IS JASMINE Command Support System (SWD C3IS JAŚMIN).

Services allowing operational data exchange provided by JASMINE system's C3IS JASMINE software module are presented in the article.

Keywords: C3IS Systems, Interoperability, MIP, NFFI, Data Exchange

INTRODUCTION

JASMINE system is a network-centric data communication system, dedicated for mobile (*field*) command posts and points of strategic, operational and tactical level. It allows to create ad-hoc, complex data communication networks, provides equipment and software necessary for communication on a battlefield. JASMINE system consists of the devices and software produced by TELDAT. One of the elements of JASMINE system is C3IS JASMINE Command Support System (*SWD C3IS JAŚMIN*).

Along with the increase of operations level by NATO countries, the need for effective command system based on international standards is growing. C3IS JASMINE meets these needs. The element that makes a command support system efficient are operational data exchange services. On one hand they enable creating Common Operational Picture (*COP*) on different command levels, on the other hand they are necessary for effective cooperation with the systems of other countries which means with the armies of allied nations. This article covers services of operational data exchange provided by JASMINE system.

1. SYSTEM ARCHITECTURE

This chapter discusses architecture of C3IS JASMINE software module which is a part of C3IS JASMINE Command Support System. This element makes operational data exchange services available and they are the main subject of this work. C3IS JASMINE software module services related with operational data exchange are marked in the WAN Access Box area.

The picture below presents construction diagram of C3IS JASMINE software module – services made available by the module and relations between the services. In a rectangle on the left that indicates WAN Access Box device area there are marked services that reside in this device.

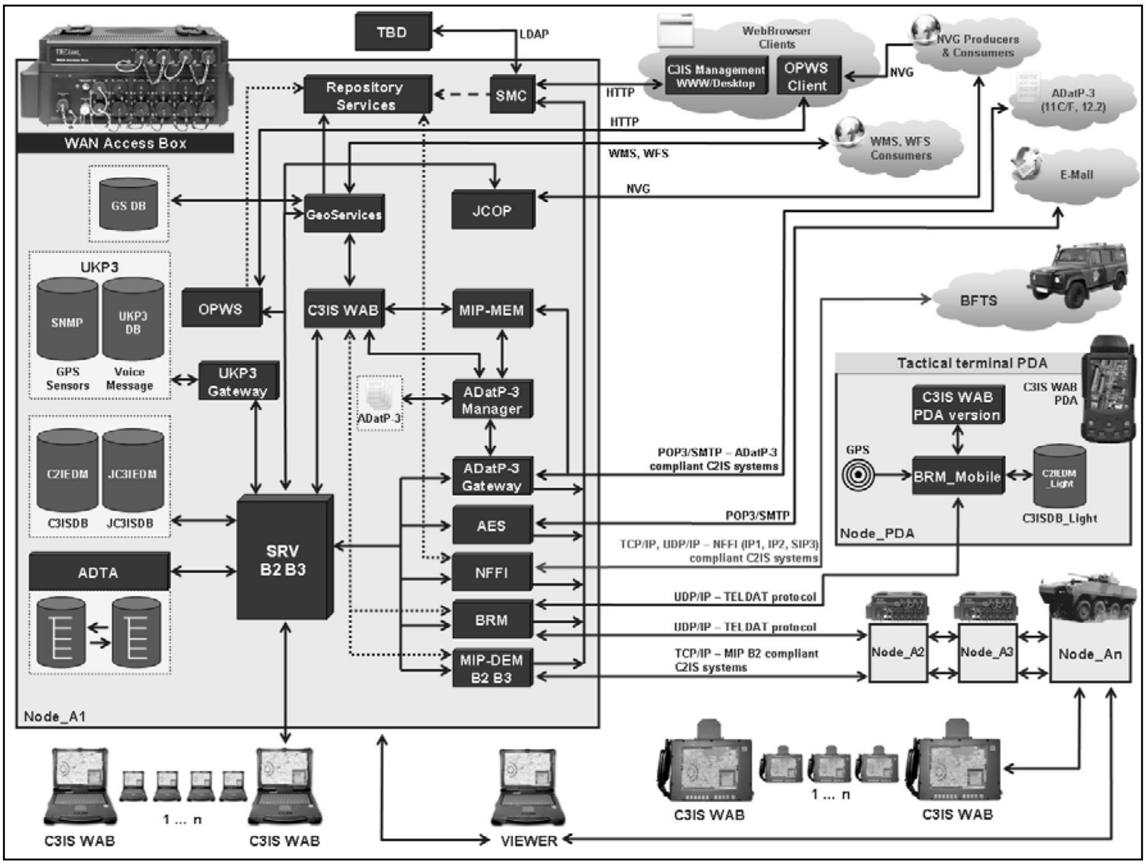


Figure 1. Relations between services in C3IS JASMIN software module

Below we list the services as seen in Figure 1, which are responsible for operational data exchange:

- JCOP – mechanism based on WEB services, compliant with NVG;
- MIP-MEM - ADatP-3 message exchange mechanism developed by MIP;
- ADatP-3-Gateway – ADatP-3 message automated exchange by means of e-mails;
- NFFI – information exchange mechanism of friendly forces position;
- BRM – Battlefield Replication Mechanism – battlefield information exchange mechanism;
- MIP-DEM B2/B3 – data exchange mechanisms based on MIP specification in both Baseline 2 and Baseline 3 version.

Apart from the above mentioned services, SRV plays an important role in operational data exchange. It is the central point of data exchange which integrates and coordinates the remaining services. SRV can operate in B2 or B3 mode of MIP specification. It means that SRV can make data available in accordance with data models C2IEDM in B2 and JC3IEDM in B3. In fact SRV integrates those two models, allowing data exchange between versions B2 and B3 of MIP/DEM. JASMINE can therefore serve as a mediator of data exchange between the systems that are compliant with B2 and B3 MIP. ADTA service, also shown in Figure 2, was especially created for that purpose. It is worth pointing out that C3IS JASMINE is the only system that enables this kind of transformation.

All the data received by any data exchange service is recorded in a common data store and transferred to the other modules (*including data presentation*), accordingly to business rules and specific needs of particular data exchange services.

2. APPLICATION OF DATA EXCHANGE MEANS

C3IS JASMINE system provides many data exchange mechanisms depending on the command level (*Figure 2 – tactical, operational*), equipment possibilities, needs and requirements of particular missions or operational conditions.

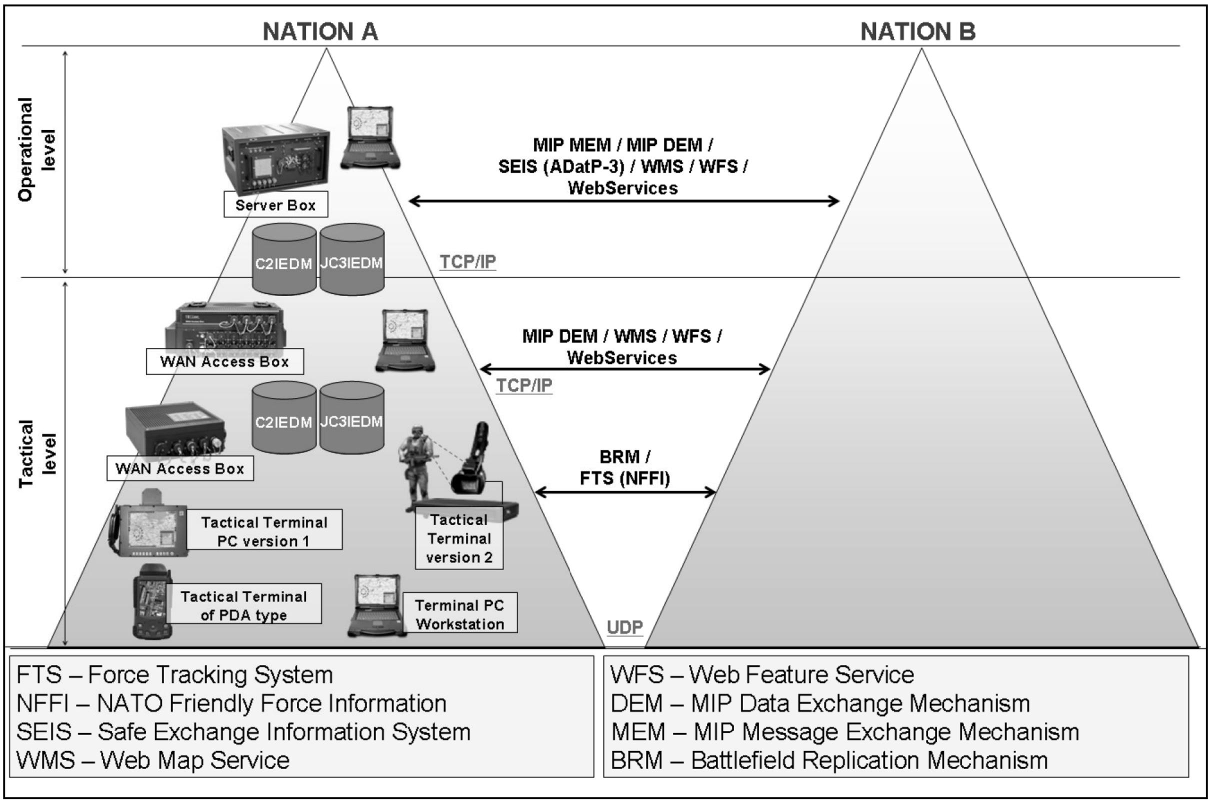

NATION A
NATION B
Operational level
Tactical level
Server Box
C2IEDM
JC3IEDM
MIP MEM / MIP DEM / SEIS (ADatP-3) / WMS / WFS / WebServices
TCP/IP
WAN Access Box
MIP DEM / WMS / WFS / WebServices
TCP/IP
C2IEDM
JC3IEDM
WAN Access Box
BRM / FTS (NFFI)
Tactical Terminal PC version 1
Tactical Terminal version 2
Tactical Terminal of PDA type
Terminal PC Workstation
UDP
FTS – Force Tracking System
NFFI – NATO Friendly Force Information
SEIS – Safe Exchange Information System
WMS – Web Map Service
WFS – Web Feature Service
DEM – MIP Data Exchange Mechanism
MEM – MIP Message Exchange Mechanism
BRM – Battlefield Replication Mechanism

Figure 2. Data exchange on particular command levels in JASMINE system

A soldier, a unit or a vehicle needs fast mechanisms for exchanging information about position of friend and enemy forces and sensors. On the operational level such detailed data are not necessary. However, there is a need for making plans and orders, analysing aggregated information about the position and status of the armies.

Another challenge for a command system is its interoperability i.e. ability to cooperate with other systems. Numerous international operations, the need for cooperation during peacekeeping and stabilization missions, created various information exchange protocols and standards. The most important ones, used by NATO countries, have been implemented in JASMINE system.

Implementation of various mechanisms is the result of communication equipment on particular command levels (*e.g. fast connection at division level or slow, radio connection of a soldier kit*). Moreover, on different command levels, different operational data groups might be required. On the level of a soldier these are mainly: position of friendly and enemy units or occurrences such as sniper or bomb attack. On the level of a division appear tasks of forces grouping, indicating assembly positions, making plans and orders etc.

3. DATA EXCHANGE ON THE OPERATIONAL LEVEL

This chapter describes utilization of MIP/DEM replication mechanism for operational data exchange on the operational level.

MIP Programme is a voluntary initiative to achieve interoperability of C2IS systems at all the command levels in order to support multinational operations. Within this programme, specification has been developed, providing cooperation of different systems. Its implementation consists of two parts:

- data model which constitutes a communication language;
- description of communication mechanism DEM – Data Exchange Mechanism.

Data model developed by MIP was created in the process of evolution. The first specification had been developed in the 70s before MIP programme was created. It was LC2IEDM model of ATCCIS initiative. LC2IEDM was adopted by MIP and was a base for Command and Control Information Exchange Data Model (*C2IEDM*). In 2004 MIP started cooperation with NATO Data Administration Group (*NDAG*). As a result of that cooperation, in 2008, Joint Consultation Command and Control Information Exchange Data Model (*JC3IEDM*) came into being. Data model developed by MIP determines all the information that are necessary on the battlefield. As it was created in a long analysis process and has been already implemented and tested, it is not only useful as data exchange mechanism elements but also as a base for building a system and determining its requirements and functionality. Systems capable of cooperating with MIP, can exchange information about:

- current situation on a battlefield;
- plans and orders;
- abilities, equipment and status of units;
- many others.

The above mentioned advantages and the origin of C2IEDM and JC3IEDM became foundation for implementing them in JASMINE system and other ones as data exchange models, and also as a base while applying command support system. Thanks to such an approach SRV service integrates different mechanisms of data exchange and discloses full operational data compliant with JC3IEDM model to all the services constituting C3IS JASMINE software module. On the operational level it enables data exchange with the systems of other countries or other producers that are compliant with MIP. Data can also be transferred to the elements of the systems that are responsible for visualization, it can be aggregated and passed to higher command levels or in form of orders passed lower to the tactical level. In the previous chapter, transformation possibilities between B2 and B3 models were presented. TELDAT Public Co. is the pioneer in this field and as the first on the market offered this possibility in JASMINE system. Developing of this functionality was possible thanks to understanding and adaptation of data models C2IEDM and JC3IEDM. JASMINE system implements both models, however it is not limited by them and discloses additional data groups not taken into account in these models, such as combat occurrences diary or text messages. Such information can also be passed on the operational level and exchanged within the system.

Data Exchange Mechanism (*DEM*) is the other product of MIP programme. It is the only automatic mechanism of replication supported by MIP, providing automatic and complete data replication between operational data bases C2IEDM or JC3IEDM. The standard has already been introduced in three versions and is still being developed and improved. Currently, the latest and recommended version is 3.10 Baseline 3.

DEM protocol operates in networks applying IP technology and it is based on TCP/IP protocol. That is why, for proper, stable and efficient performance, it needs fast and stable transmission links which together with other limitations cause DEM to be applied above the tactical level. Data exchange with DEM is based on so called Operational Information Group (*OIG*). OIG are semantically coherent data groups disclosing particular view of a battlefield situation or including a planned situation.

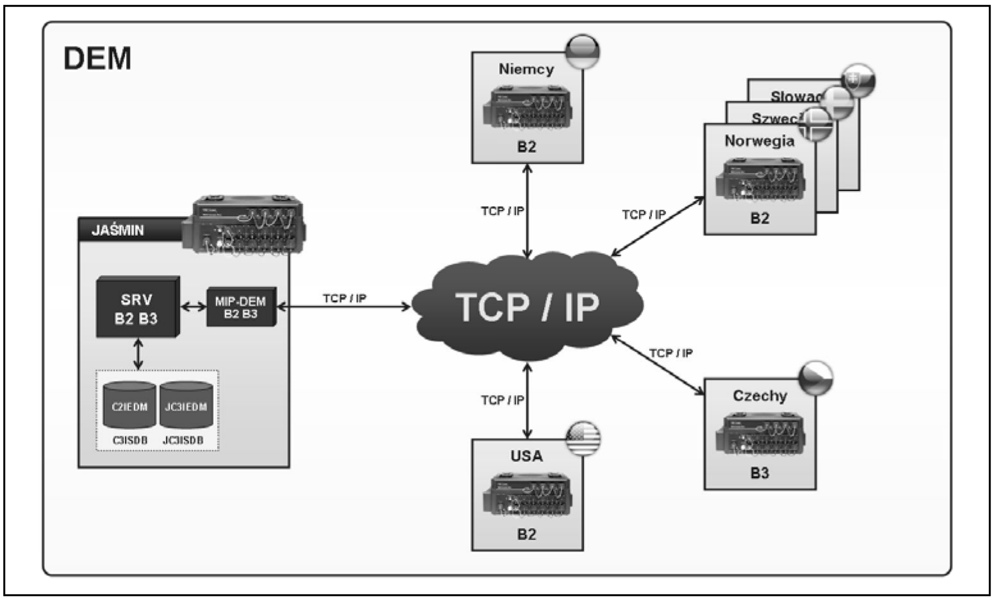


Figure 3. Exemplary architecture of DEM network

JASMINE system fully supports data exchange in DEM standard in Baseline 2 and Baseline 3 versions, including the latest 3.10. It gives a user an opportunity to work and exchange information with numerous systems that support data exchange by means of DEM.

The other alternative operational data exchange mechanism, supported by JASMINE system is Message Exchange Mechanism (*MEM*). MEM enables sending ADatP-3 messages (*e.g. OWNSITREP, ENSITREP, INTREP, INTSUM, SITREP, FRAGO*) picturing current battlefield situation, audio and video files, drawings and documents in strictly precised format of electronic message (*e-mail*). Unfortunately this mechanism does not provide automation of data transfer (*message has to be manually created*). Within MEM, a few ADatP-3 messages were created, e.g. MIPSYSMAN improving making and controlling a connection, allowing users management and controlling delivery and opening a message.

The best source of information on MIP programme is website ***www.mip-site.org***.

4. DATA EXCHANGE ON THE TACTICAL LEVEL

This chapter presents selected ways of operational data exchange on the tactical level. Selected functionalities illustrate capabilities of the JASMINE system, to the best of its advantage, in respect of information exchange and interoperability.

4.1. BRM and NFFI

Engineers of TELDAT company, in order to provide information exchange on the tactical level, started research and implementation work on a new innovative protocol. The goal was set to work with unstable, low capacity radio lines and send the most data in the shortest time possible. As the result of the research, BRM (*Battlefield Replication System*) was developed.

BRM is based on UDP protocol (*User Datagram Protocol*). The advantage of using this particular protocol is its simplicity, lack of additional tasks and transmission speed it provides. BRM protocol eliminates drawbacks of UDP, adding many new improvements and providing high security of transmitted data. Similarly to DEM, BRM allows exchange of the most important operational data between bases (*both in versions for C2IEDM and JC3IEDM models*). BRM application provides data delivery reports, ensures effectiveness of line use adapting transmission parameters to constantly changing conditions of environment.

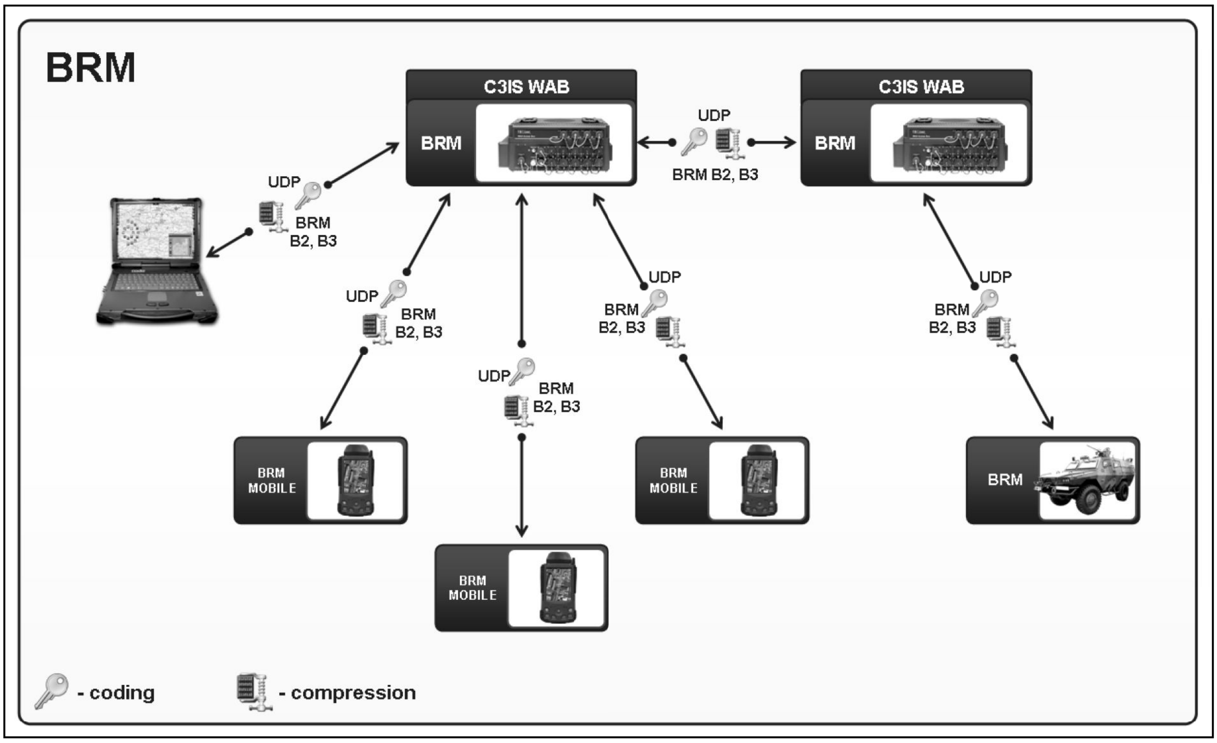


Figure 4. Exemplary structure of BRM network

Each data transmission is ciphered with a singly-generated symmetrical key. BRM protocol was designed to use, to the highest extent, transmission capabilities of low capacity radio connections. BRM also has mechanisms of auto-negotiations and detecting connection availability, adaptation of transmission settings and provides data exchange between the systems of Windows family in both stationary and mobile versions.

During several armed conflicts and stabilization missions, fast and effective locating of friendly forces and units, poses serious problems. NFFI became the solution to these problems. It was created to provide interoperability between the armies of Force Tracking System (*FTS*).

NFFI standard is divided into 3 parts:

- Interface Protocol 1 (*IP1 – TCP*);
- Interface Protocol 2 (*IP2 – UDP*);
- Service Interoperability Profile 3 (*SIP3 – WebServices*).

JASMINE system supports in 100% all the currently available communication protocols

(*IP1, IP2, SIP3*) within FFT (*Figure 5*), providing full interoperability on the battlefield and during stabilization operations.

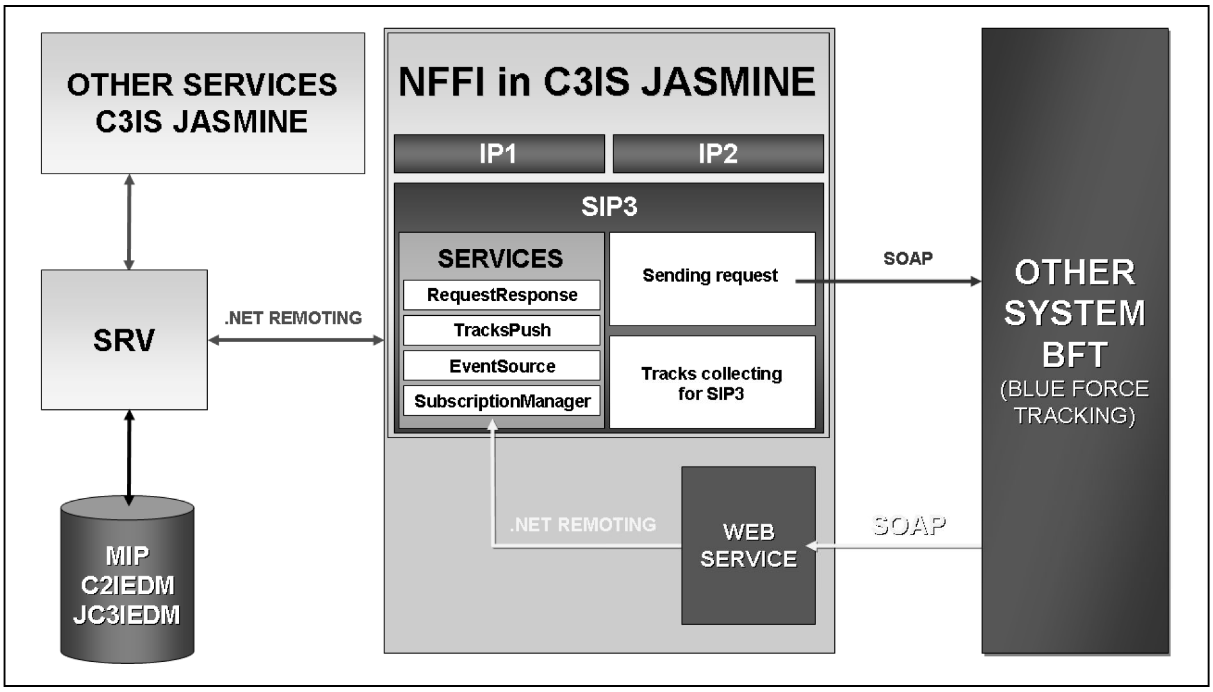


Figure 5. Structure of NFFI module

JASMINE system supports NFFI HUB solution that provides connecting and exchanging data between many NFFI systems.

5. SUMMARY

The article presented architecture and capabilities of JASMINE system in respect of operational data exchange. Particularly selected elements of functionality connected with data exchange and interoperability were described. C3IS JASMINE Command Support System is a modern, based on the best standards and technologies command system. It implements the most important existing mechanisms providing interoperability and it is exceptionally flexible and capable of meeting particular needs. On account of these features C3IS JASMINE system can be applied on all command levels down to a single soldier.

BIBLIOGRAPHY:

[1] Multirateral Interoperability Programme, *The C2 Information Exchange Data Model (C2IEDM Main)*, 2005

[2] Multirateral Interoperability Programme, *The Joint C3 Information Exchange Data Model (JC3IEDM Main)*, 2007

[3] Multirateral Interoperability Programme Baseline 3, *ANNEX A – MIP DEM SPECIFICATION 3.8, 2008*

[4] Multirateral Interoperability Programme Baseline 2, *ANNEX A – MIP DEM SPECIFICATION 2.6, 2006*

[5] R. Porta, V. de Sortis, *Working Paper EPW002038-04 NFFI Service* Interoperability *Profile 3 (SIP3) GENERAL DESCRIPTION (version 1.0.0)*, 2008

[6] *Vincenzo de Sortis, NFFI Service Interoperability Profile 3 (SIP3) Technical Specifications* (VERSION 1.1.5)

[7] R. Porta, *REF. EPW002625-WP02 Friendly Force Tracking Hub (FFT-HUB) Functional Specifications (vers. 1.0)*, 2009
[8] *AC322(SC5)N(2006)0025 - Interim NFFI Standard for Interoperability of FTS*, December 2006
[9] *STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems*
[10] *Mip Implementation Rules Annex C - Appendix1-ADatP-3_Message-Definitions B12-2 v1.0 03-Baseline_2.0*, 2006
[11] *Mip Implementation Rules Annex C - Appendix2-MIP_Messages-Definitions-1.0 03-Baseline_2.0*, 2006
[12] W. Zawadzki, *JAŚMIN wkracza do armii*, Nowa Technika Wojskowa nr 5/2007
[13] H. Kruszyński, *Zastosowanie systemu JAŚMIN*, Nowa Technika Wojskowa nr 9/2006
[14] H. Kruszyński, Ł. Apiecionek, M. Dziamski, *JAŚMIN w warszatach Combined Endeavor 2008*, RAPORT nr 06/2008
[15] M. Piotrowski, R. Palka, T. Z. Kosowski, *Interoperacyjność polskiego oprogramowania w praktyce,* Nowa Technika Wojskowa nr 7/2008
[16] T. Wachowski, *Mobilny JAŚMIN*, Nowa Technika Wojskowa nr 1/2008
[17] Ł. Pacholski, *Mobilny JAŚMIN na Żubrze-WD,* Nowa Technika Wojskowa nr 12/2008
[18] H. Kruszyński, *Jaśmin pomoże armii,* Nowator nr 1/2009
[19] Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, François Yergeau, *Extensible Markup Language (XML) 1.0 (Fifth Edition)*, 11/2008
[20] Multirateral Interoperability Programme, *ANNEX B – MIP ESMTP SPECIFICATION, 2008*

XML Guard as a base service utilized to provide Information Exchange Gateway Functional Services in IEG JASMINE

Robert Palka, Marcin Woźniak
TELDAT, Kijowska street 44, 85-703 Bydgoszcz, POLAND
phone +4852 341 97 31, fax +4852 341 97 21, RPalka@teldat.com.pl
phone +4852 341 97 00 (759), fax +4852 341 97 21, MWozniak@teldat.com.pl

ABSTRACT

Operations carried out on behalf of NATO require wide range data exchange between NATO and national command systems of C3 type (Command, Control and Communication). This kind of data exchange should be executed with establishing specified gateways in both NATO and national systems for which, common data exchange protocols and standards will be set. On that assumptions, Information Exchange Gateway concept was created within NATO. It is a suggested solution for effective data sharing between enclaves of different level of security and supervision realized by means of administered and trusted set of services. These services support co-sharing of information and data at all the levels and based on accredited security procedures provide and manage protection (high/low level of security or not categorized) of information between different enclaves.

Keywords: IEG, IEG scenarios, NNEC, NATO Security policy, XML Guard, Labeling

1. IEG CONCEPT IN RELATION TO NNEC

NATO is in the act of adaptation NNEC concept (*NATO Network Enabled Capability*) and discarding the idea of building systems in favor of creating services. NNEC is one of the fastest developing and spreading concepts designed for network-centric purposes and intended to speed up and simplify decision making on the battlefield. To achieve the goals of this concept, the main challenge to be faced was automated networks connection. It needs the implementation of Information Exchange Gateways which will fill the existing air gaps, one-way data diodes or in some rare cases the existing non-administered two-ways connections.

At the strategic level, the task of IEG is to support the process of political consultation and allow national planning and more effective orientation of operations and at the operational level it is to support daily operational planning and management. At the tactical level, thanks to IEG we will get an improved presentation of information for commanders and better understanding of their intentions, possibility of sharing information with coalition members, dispersed cooperation and network integration of collectors, decision makers and effectors.

2. GENERAL PRINCIPLE OF OPERATION IEG

According to NATO concept, in IEG we can distinguish three basic functional elements [1]:

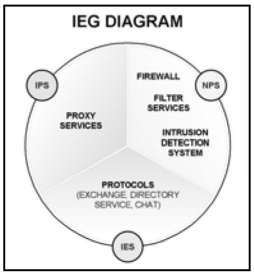

IEG DIAGRAM
IPS
NPS
FIREWALL
FILTER SERVICES
PROXY SERVICES
INTRUSION DETECTION SYSTEM
PROTOCOLS (EXCHANGE, DIRECTORY SERVICE, CHAT)
IES

Figure 1. IEG Diagram – prepared on the basis of [1]

a) NPS (*Node Protection Service*) – its task is to protect physically IEG infrastructure. It is usually executed by a specialized firewall with implemented mechanisms of protection against attacks;
b) IPS (*Information Protection Service*) – its task is to protect and control the flow of information. IEG characteristic does not require this service to be in physical proximity of IEG. It is only required that the whole traffic into and out of IEG is managed by this service by means of NPS;
c) IES (*Information Exchange Service*) – it has to provide the flow of information between the protected node and an outside, authorized (*using IPS*) organization. Only the information that IES can transfer should be transported by IEG. The example of this kind of information are e-mail service protocols, http, directory services, Web service and many more.

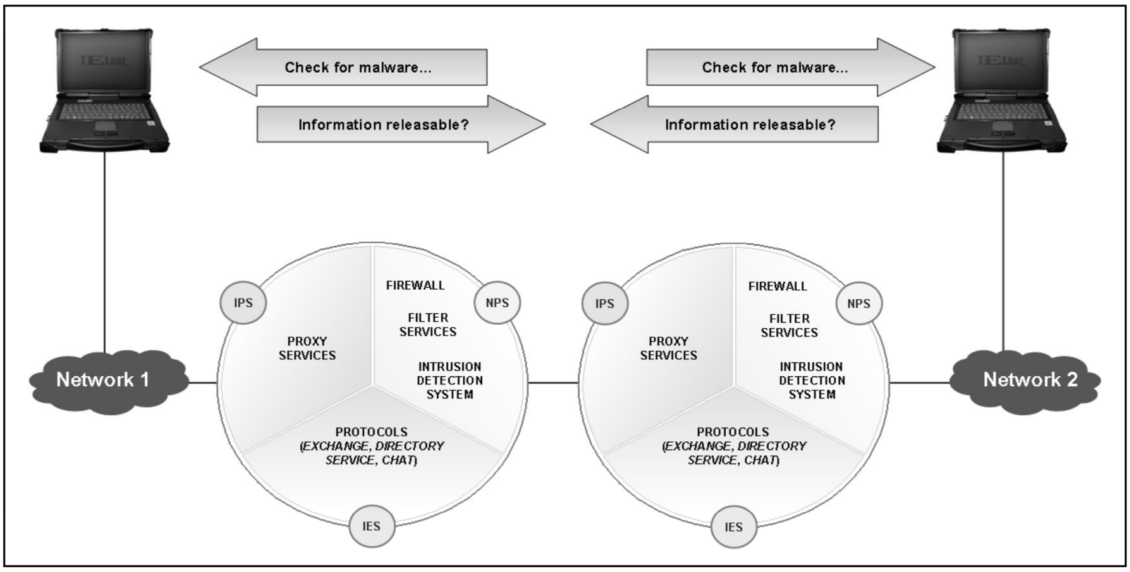


Figure 2. IEG operation display - developed on the basis of [3]

IEG is installed to protect its own network from possible attacks, viruses and intruders. At the same time it checks the flow out to make sure that the information can be disclosed.

Considering that, for particular connection, there will exist different information security requirements, operational needs and data to be transported, therefore gateways will vary for particular cases.

3. SCENARIOS OF USING IEG

To name and categorize different network connections, they are reffered to as Scenario from A to E with some sub-scenarios. The scenarios do not impose using different equipment for each of them. Particular implementations IEG can realize different scenarios or be dedicated for a predestined one. IEG also does not assume "friendliness" or "unfriendliness" of an organization out of the point it protects. All the information transmitted to outside organizations as well as internal resources have to be protected by all means.

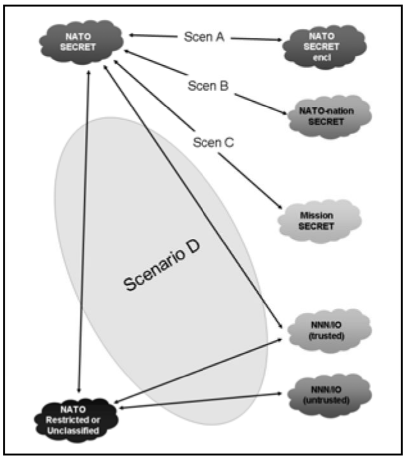


Figure 3. IEG scenarios approved by NC3B (NATO C3 Board) – prepared on the basis of [3]

Thanks to such an approach the gateway can support connections for different scenarios with other NATO Secret individuals such as the ones possessed and managed by nations (*Scenario A*), with points working at national security level (*Scenario B*), with coalition points that have or do not NATO participants (*Scenario C*) and with points of non-governmental organizations (*Scenario D*). In future, NATO intends to introduce other scenarios.

4. OPERATED PROTOCOLS

In order to categorize protocols and standards of the data necessary to exchange between the networks, the protocols have been divided into main protocols that will be supported by each IEG implementation. They include directory services, e-mail services and Web services. Each IEG can also provide functional services according to particular operational needs. These functional protocols include, however are not limited to: tactical data links, MIP DEM (*mainly used by C2IS Land Components*) and XMPP (*instant message sending protocol used by JCHAT*).

Proper performance of IEG requires correct labelling of information allowing to verify if particular data can be shared. If the information cannot be labelled, other means of filtering and changing have to be introduced, also with the participation of operator.

5. IMPLEMENTATION PLANS OF NATO

NATO IEG will be introduced in consecutive phases within next few years in order to establish the most important connections for the needs of the mission by 2014. The priority stage is achieving automated connections between NATO Secret network and ISAF Secret network in 2010, and extending it to all the required protocols by the year 2012.

Type of scenario	Type of connection	2009	2010	2012	2014
Scenario A	NATO Secret – NATO Secret	FOC			
Scenario B	NATO Secret - National Secret		IOC	FOC	
Scenario C1	NATO Secret - Mission Secret (np: ISAF Secret)		IOC	FOC	
Scenario C2	Mission Secret – National Secret				FOC
Scenario C3	Mission Secret – Non Government Organizations				IOC
Scenario C4	Mission Secret – Non-NATO Nation Secret				FOC
Scenario C5	Mission Secret – Mission Secret				FOC
Scenario D	NATO Secret – NATO Restricted			IOC	FOC
Scenario D	NATO Secret – Non Government Organizations				IOC
Scenario D	NATO Restricted – Non Government Organizations				IOC

Figure 4. Implementation of consecutive scenarios by NATO - developed on the basis of [3]

In the chart above, abbreviation IOC (*Initial Operational Capability*) was used to name IEG with minimal number of supported functional protocols and FOC (*Full Operational Capability*) to name fully operational IEG which supports all the protocols recognized as necessary and obligatory for control and supervision in a given scenario.

Looking at the time scope, one can see that IEG is only in the initial phase of implementation by NATO and in the following years we will observe the development of supported functional protocols and adaptation of solutions for particular scenarios. Certainly during IEG implementation process, NATO will gain great experience and verify the applied approach. It will also turn out if the suggested solutions work out in practice and whether it will be possible to use the same IEG for different scenarios.

6. STRUCTURE OF IEG JASMINE

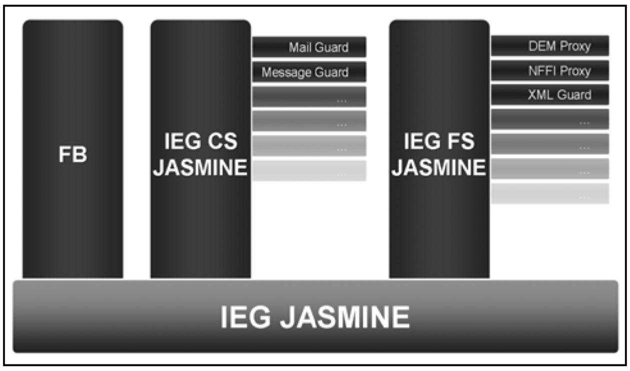


Figure 5. Functional division within IEG JASMINE

IEG JASMINE is a product of TELDAT company, pursuing NATO directives for building Information Exchange Gateways. IEG JASMINE has a module structure – each of its components fulfills particular goals set in the specification. The basic module is Firewall Box which is responsible for security control at the lowest network level and serves directly as NPS (*Node Protection Service*) in IEG model. Firewall Box's functions include intrusion detection and prevention system IDS/IPS. Basic task of the module is the analysis of network flow in respect of the content and directing it to destination modules.

IEG CS (*Core Service*) JASMINE module is responsible for controlling the flow of information for the basic services: e-mail, directory services and messaging. IEG FS (*Functional Service*) JASMINE module is responsible for filtering all the additional services supported by C3IS JASMINE system.

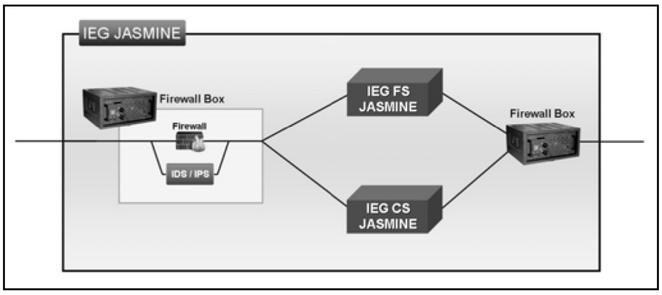


Figure 6. Structure of IEG JASMINE

The chart shows physical location of particular modules within IEG JASMINE. One can clearly see the main role of FB module (*Firewall Box*), which is the first obstacle for all the attacks from outside. It also allows filtration and directing packets to other modules. After filtering of the packets and applying security policy by IEG FS and IEG CS there comes a final filtration of the packets by the second FB module placed on the other side. Such a scenario is used for both directions movement.

7. IMPLEMENTATION OF FUNCTIONAL SERVICES

7.1. Structure of IEG FS JASMINE

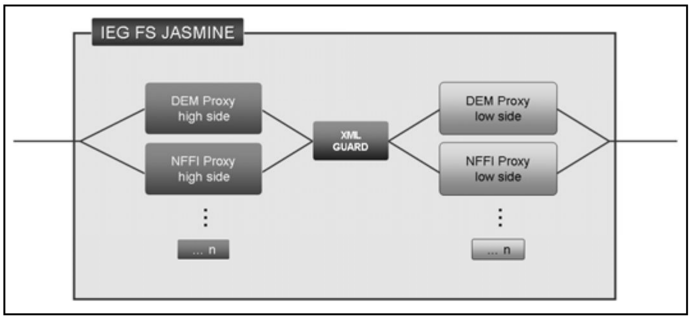


Figure 7. Structure of IEG FS JASMINE

Implementation of security policy for functional services in IEG environment consists in creating so called Proxy (*mediator*) service for the protocol realized by a particular mediator. Performance of this service is based on two assumptions:

a) for the traffic from secret domain towards XML Guard, this service is assigned to change data of particular protocol into XML format and apply security policy (*place in XML data appropriate security label*);

b) for the traffic towards particular secret domain, Proxy should change XML data into the format specific for a particular protocol.

Structure of IEG FS JASMINE is based on the central service XML Guard and several dedicated guards servicing particular communication protocols. Utilization of XML Guard service by other services is compliant with SOA paradigms (*Service Oriented Architecture*). It also allows to assume that if a particular XML Guard service passes the tests and receives appropriate security accreditation it will be easier to receive such in case of another service based on its operation.

7.2. Realization of security policy using XML Security Labeling

XML Security Labeling (*farther referred to as security labels*) is a NATO standard used to define security policy. Generally speaking a security label is a document compliant with XML standard describing security classification and the importance level of digital data. Such a label can be enclosed to any digital source. It often contains information about digital signature of the document in a form compliant with XML-Sig standard. According to the way of placing the label we can distinguish three types of labels: packed, packing and split.

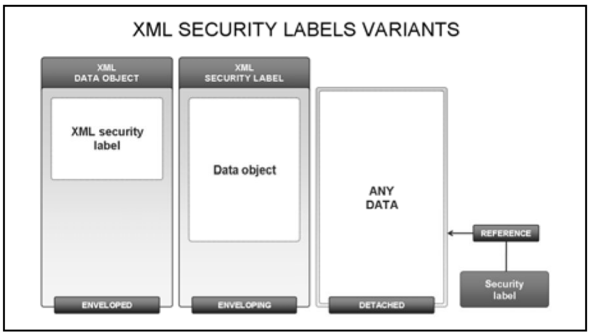
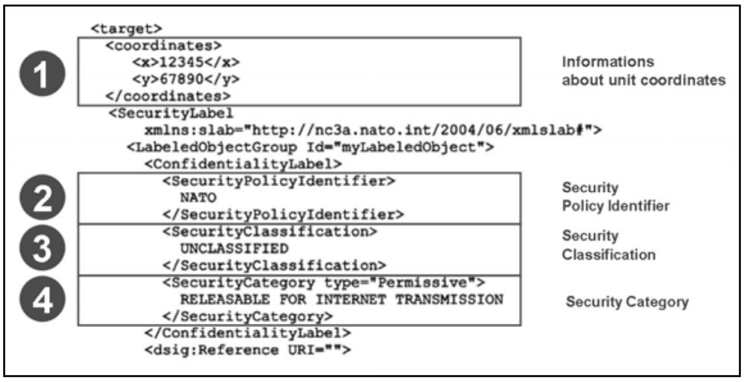


Figure 8. Kinds of security labels - developed on the basis of [4]

In a peculiar case, when the security label is a part of XML document, security classification may concern not only the whole document but also its particular fragments denominated by means of XPath expressions. It gives a user additional possibilities of creating security policy, by granting different secret classification to the pieces of information within one document. Sending information about location of a unit may serve as an example. Its coordinates are available to everybody (*NATO UNCLASSIFIED clause*) whereas information about its name is classified, which can be seen in a fragment of XML document.



```
<target>
  <coordinates>
     <x>12345</x>
     <y>67890</y>
  </coordinates>
  <SecurityLabel
      xmlns:slab="http://nc3a.nato.int/2004/06/xmlslab#">
    <LabeledObjectGroup Id="myLabeledObject">
      <ConfidentialityLabel>
        <SecurityPolicyIdentifier>
          NATO
        </SecurityPolicyIdentifier>
        <SecurityClassification>
          UNCLASSIFIED
        </SecurityClassification>
        <SecurityCategory type="Permissive">
          RELEASABLE FOR INTERNET TRANSMISSION
        </SecurityCategory>
      </ConfidentialityLabel>
      <dsig:Reference URI="">
```

1
Informations
about unit coordinates
2
Security
Policy Identifier
3
Security
Classification
4
Security Category

Figure 9. Exemplary labelling of a part of XML document - developed on the basis of [4]

7.3. XML GUARD service

XML-Labeling Guard (*farther reffered to as XML Guard or Guard*) is a service that provides data transport between different domains based on secrecy labels (*XML Security Labels*). The purpose of its origin was automation of data transfer process between two networks which realize different levels of security. From the XML Guard point of view one network is of high level of security whereas the other of the low one.

The main task of XML Guard is protection of information confidentiality, its coherence and availability. The two latter goals are realized by allowing access to the domain of high security only requests with determined format and specified content. This operation is called access policy of XML Guard (*Access Control Policy*). Its worth pointing out that XML Guard does not prevent from viruses and unwanted data (*viruses, Trojan horses*).

Confidentiality of transferred information in XML Guard service is based on application of access policy to accessible data that exist in the domain of high secret – the main factor is the classification of particular source access degree. In practice XML Guard may disclose such information, block it or delete from it a piece of unsuitable secrecy degree.

7.4. Scenarios of use supported by XML GUARD

In XML Guard specification, two basic scenarios of use have been determined, as described below [4].

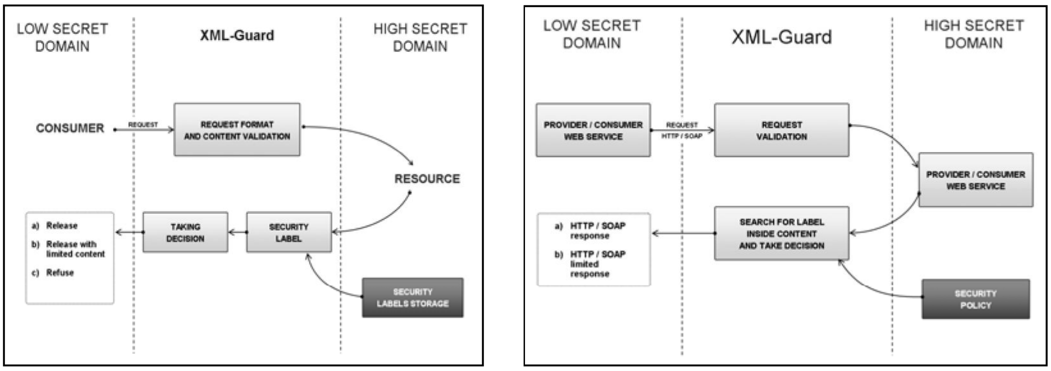


Figure 10. Scenarios supported by XML-GUARD- transfer of documents from a high to a low security level domain and two-way communication using Web Services - developed on the basis of [4]

In first scenario, action is originated by a user from a low security domain, using standard www browser. He tries to download a source from a high security domain. It can refer to any digital document – www site, WORD file or a picture. It is assumed that for each of these documents there exists an adequate security label located in the high security domain.

In second scenario both a producer and a consumer (*their roles are interchangeable*) communicate by means of web services with HTTP protocol using SOAP messages (*W3C2000*). In this case XML Guard functions as so called network proxy – here proxy of HTTP protocol. It stops any other flow, whereas http messages are subjected to check-out process based on access policy. SOAP messages sent from a high secrecy domain to a low secrecy domain have to contain appropriate safety labels to control information flow by XML Guard.

7.5. Architecture of IEG FS JASMINE

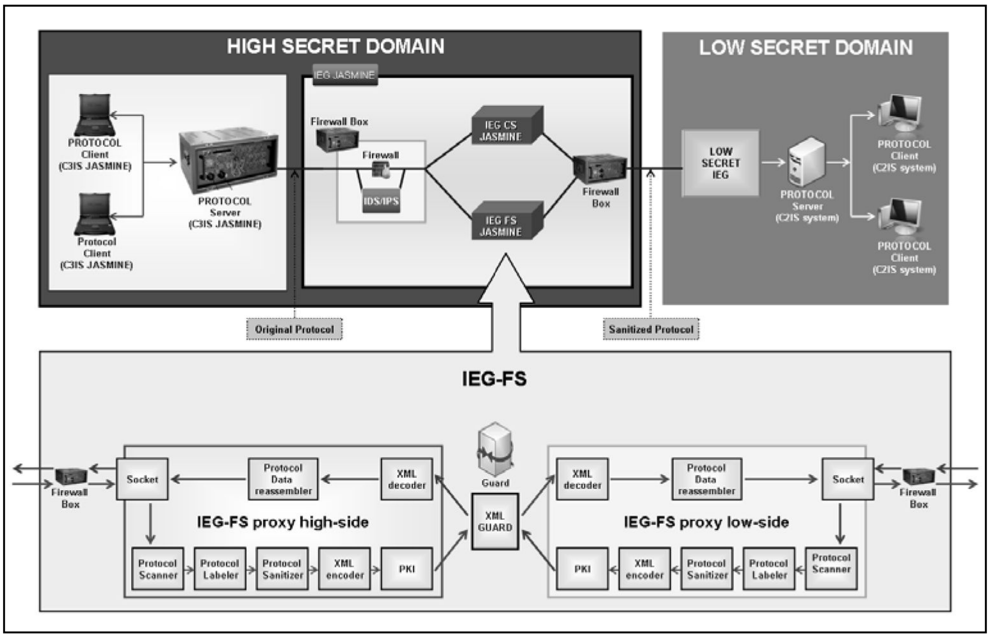


Figure 11. The way of realization of IEG for functional services – prepared on the basis of [5]

Realizing IEG for functional services one should assume that there are two security enclaves, ours – of a high security level and extraneous – of a low security level. IEG FS JASMINE device is assigned, for a given communication protocol, to protect us from releasing a high security clause information to the domain where such information must not get. At the same time IEG is designed to protect us from all kinds of attacks within operated data exchange protocol which may origin in another enclave.

IEG operation must be transparent for both connecting points from two different security enclaves within particular communication protocol. During data transfer from our domain (*picture above*), IEG FS JASMINE captures flow of a particular protocol and analyses it. Then individual elements are labelled on the basis of data sent in a particular protocol or generally accepted convention and handed to XML Guard service in XML format. The service then filters the content of delivered XML data on the basis of prior labelling of elements and security policy. The next step is to create, from the changed XML data, a data packet compliant with a particular communication protocol and send it to the receiver. The situation is analogical in the opposite direction. However, more stressed is protection from attacks by means of a particular communication protocol than obtaining unwanted information according to its classification.

8. SUMMARY

Information Exchange Gateways are NATO standardized approach, solving information protection problems and a technical key incorporating the goals of NNEC concept. After preparing for operation, Information Exchange Gateway provides two-way, automatic exchange and protection of information. It substantially increases capabilities of commanders on all the levels, giving them access to essential information regardless of the kind and classification of the network they are in.

As seen in a presented architecture, XML Guard service is central for realization of IEG for the needs of functional services. Making, implementing and providing it with appropriate security accreditation allows development of the remaining mediators of other functional protocols. TELDAT Company will successively implement and expand a list of functional services protocols as soon as the demand for such occurs. We actively take part in MIP WG (*MIP Working Group*) in Greding and we know that for command systems it is necessary to make Proxy for MIP DEM B2 and B3. Additionally our participation in the development of consecutive versions of NFFI protocol specification (*NATO Friendly Force Information*) and growing interest in BFT systems (*Blue Force Tracking*) draws a conclusion that Proxy for NFFI IP1, IP2 and SIP3 is inevitable.

In case of functional services, considering XML Guard application, the destination solution is to base all the controlled communication protocols on XML format. Thus a default data labelling can be introduced already on the level of a particular protocol (*e.g. NFFI*). It would simplify the realization of dedicated guards for specific functional services. However because of the existing adopted data exchange standards (*e.g. MIP DEM*) it is not always possible. One should keep it in mind when creating new versions or completely new data exchange protocols (*e.g. MIP XEM (XML Exchange Mechanism)*).

BIBLIOGRAPHY:

[1] "Guidance document on the implementation of gateways for information exchange between NATO and external CIS communities" version 1.21 dated 16th February 2007 AC/322(SC/4)N(2007)0007, MULTI REF

[2] "INFOSEC Technical and Implementation Directive for the Interconnection of Communication and Information Systems (CIS)" AC/322-D/0030-Rev4

[3] Information Exchange Gateways: One Step closer to NNEC?, Maj Andreas Geistlinger, March 18th 2009

[4] Technical Note 1330 - XML-LABELLING GUARD HIGH LEVEL DESIGN EDITION 1 (A. Thümmel S. Oudkerk)

[5] MIP-DEM IEG Proxy - http://tide.act.nato.int/mediawiki/index.php/MIP-DEM_IEG_Proxy

[6] H NC3A XML-Labelling Guard - Introductory briefing (Sander Oudkerk – Philippe Lagadec)

[7] Technical Note - XML SECURITY LABELING SYSTEM PROTOTYPE ARCHITECTURE (Helge Lagreid, Maarten Gerbrands, Andreas Thümmel)

[8] Multilateral Interoperability Programme http://www.mip-site.org

[9] Information Exchange Gateway (IEG) http://tide.act.nato.int/mediawiki/index.php/Information_Exchange_Gateway_(IEG)

[10] Information Exchange Gateway for Functional Services (IEG-FS) http://tide.act.nato.int/mediawiki/index.php/Information_Exchange_Gateway_for_Functional_Services_(IEG-FS)