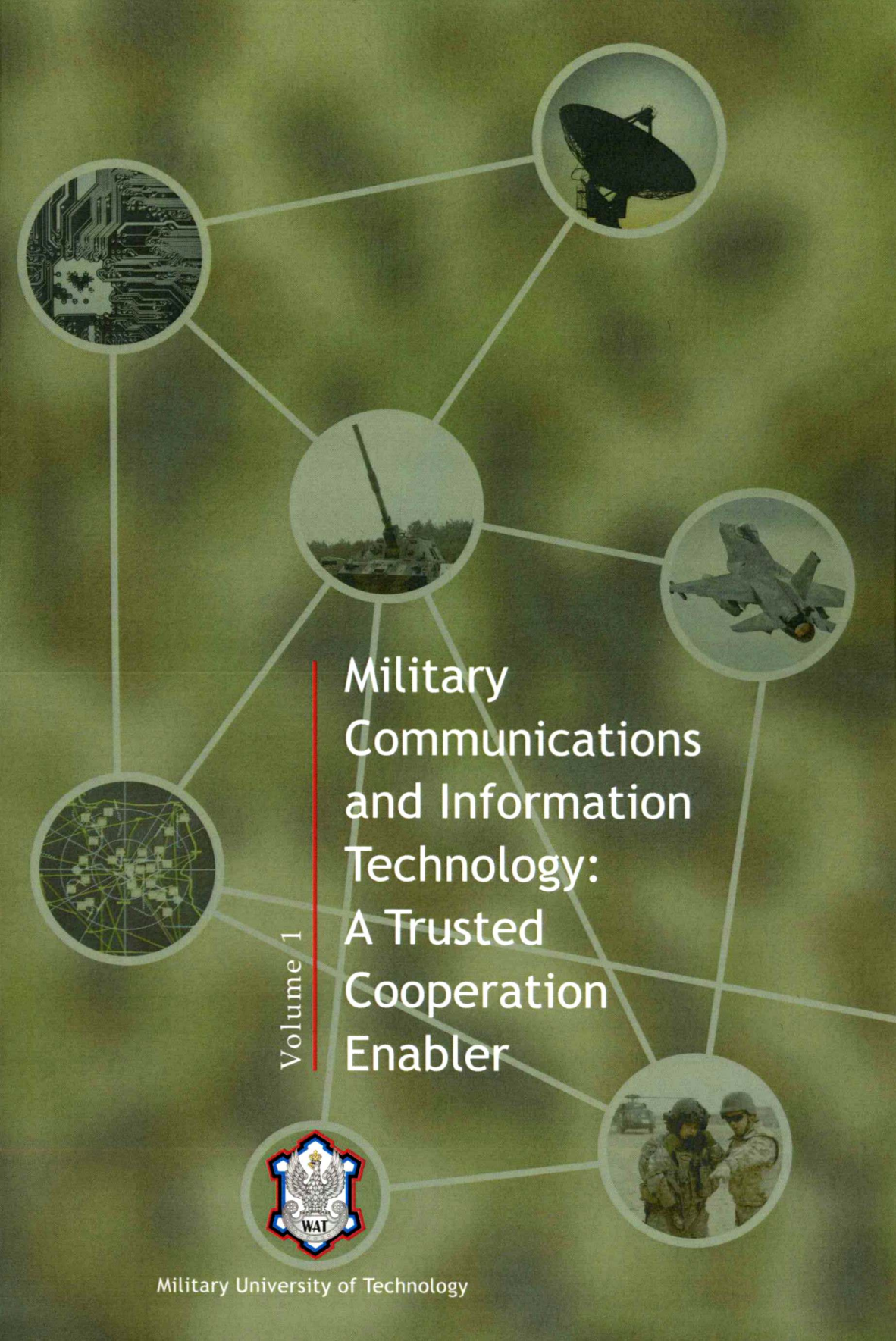

Military Communications and Information Technology: A Trusted Cooperation Enabler

Volume 1

Military University of Technology

Military Communications and Information Technology: A Trusted Cooperation Enabler

Volume 1

Warsaw 2012

Reviewers:
Prof. Milan Šnajder, LOM Praha, Czech Republic
Prof. Andrzej Dąbrowski, Warsaw University of Technology, Poland

Editor:
Marek Amanowicz

Co-editor:
Peter Lenk

ISBN 978-83-62954-31-5
ISBN 978-83-62954-51-3

Publication qualified for printing without editorial alterations made by the MUT Publishing House.

DTP: *Martyna Janus*
Cover design: *Barbara Chruszczyk*

Publisher: Military University of Technology

Press: P.P.H. Remigraf Sp. z o.o., ul. Ratuszowa 11, 03-450 Warszawa

Warsaw 2012

Contents

Foreword

Modern military operations are conducted in a complex, multidimensional and disruptive environment. The challenging political and social environment of the operations necessitates establishing coalitions, consisting of many different partners of differing levels of trust, e.g. partners from NATO nations, as well as non-NATO nations and others such as the local government bodies and local forces. Tight collaboration with these partners and the guarantee that the appropriate information is shared within the community is vital to the mission efficiency. This also requires understanding of these differences and greater trust as well as acceptance of the greater risk involved.

Dynamic environmental changes and limitations of the technical infrastructure assets creates additional challenging issues for the effective collaboration of the coalition partners. The fragile nature of the communications infrastructure, especially at the tactical level, requires robust methods and mechanisms to deal with long delays, communication failures or disconnections and available bandwidth limitations.

These all necessitate a better understanding of the environmental conditions and appropriate procedural actions, as well as strong technological support, to provide the required levels of interoperability, flexibility, security and trusted collaboration in connecting heterogeneous systems of all parties involved in the action.

Many research efforts aimed at the elaboration and implementation of innovative communications and information technologies for military systems, enabling trusted information exchange and successful collaboration in disadvantaged environments, have been undertaken world-wide. The latest selected results of such activities that include novel concepts for military communications and information systems, as well as innovative technological solutions, are presented in this book.

The book contains the papers originally submitted to the 14th Military Communications and Information Systems Conference (MCC) held on 8–9 October 2012 in Gdansk, Poland. The MCC is an annual event that brings together experts from research establishments, industry and academia, from around the world, as well as representatives of the military Communications and Information Systems community. The conference provides a useful forum for exchanging ideas on the development and implementation of new technologies and military CIS services.

It also creates a unique opportunity to discuss these issues from different points of view and share experiences amongst European Union and NATO CIS professionals.

The papers included in this book are split into two volumes, each contains selected issues that correspond to the conference topics, and reflect the technology advances supporting trusted collaboration of all parties involved in joint operations. The first volume is focused on: *Concepts and Solutions for Communications and Information Systems, Communications and Information Technology for Trusted Information Sharing, Information Technology for Interoperability and Decision Support Enhancement and Information Assurance & Cyber Defence,* while the latter on the following: *Tactical Communications and Networks, Spectrum Management and Software Defined Radio Techniques, Mobile Ad-hoc & Wireless Sensor Networks and Localization Techniques.*

The editors would like to take this opportunity to express their thanks to the authors and reviewers for their efforts in the preparation of this book. We trust that the book will contribute to a better understanding of the challenging issues in trusted collaboration in modern operations, scientific achievements and available solutions that mitigate the risk and increase the efficiency of information exchange in hostile and disruptive environments. We believe that the readers will find the content of the book both useful and interesting.

Marek Amanowicz
Peter Lenk

The Concept of Integration Tool for the Civil and Military Service Cooperation During Emergency Response Operations

Łukasz Apiecionek, Tomasz Kosowski, Henryk Kruszyński,
Marek Piotrowski, Robert Palka

Research & Development Department,
TELDAT Sp. J., Bydgoszcz, Poland,
{lapiecionek, tkosowski, hkruszynski, mpiotrowski, rpalka}@teldat.com.pl

Abstract: Civil-Military Co-operation is tool which allows achieving common aims by forces designated originally for different purposes. The most common example of such cooperation are emergency response operations, conducted, for example, during natural disasters. Despite the obvious need for the right tool which could support simultaneously soldiers and civilians, one can see that usually, in Poland, means of communications and methods of operations for sharing the information are created ad hoc, according to situation and given resources. In given examples of emergency response plans one can find description of using only cell and stationary phones for communication [1].
Instant collection and dissemination of information, efficient collaboration and common emergency situational awareness are factors needed in order to secure effective cooperation with both military and civilian organizations. This can be achieved only by study of NATO doctrines and concepts, such as NNEC [2-4], EU NEC [5] or CIMIC [6], and newest technology capabilities, regarding both hardware and software.
Based on that study, a specially designed information system can be introduced that is scalable, flexible, interoperable and extendable. Crisis Management System Jasmine is a solution for army and other civilian forces requirements, which highly increases awareness and speed of decision process. Described in the article solution can be used as a support for different operations managed and executed both on the field and stationary posts.
Keywords: Command and Control Information Systems, NNEC, CIMIC, EXPEDITIONARY OPERATIONS, Web Portal, Web Services, operational level, emergency response operations

I. Introduction

Civil-Military Co-operation is tool which allows achieving common aims by forces designated originally for different purposes. The most common example of such cooperation are emergency response operations, conducted, for example, during natural disasters. Despite the obvious need for the right tool which could support simultaneously soldiers and civilians, one can see that usually, in Poland,

ways of communications and methods of operations for sharing the information are created ad hoc, according to situation and given resources. In given examples of emergency response plans one can find description of using only cell and stationary phones for communication [1]. Instant collection and dissemination of information, efficient collaboration and common emergency situational awareness are factors needed in order to secure effective cooperation with both military and civilian organizations. This can be achieved only by study of NATO doctrines and concepts, such as NNEC [2] [3] [4], EU NEC [5] or CIMIC [6], and newest technology capabilities, regarding both hardware and software.

II. Collaboration of different types of crisis management units during natural disasters in Poland [7-8]

Collaboration of different types of response forces during natural disasters, combined and joint engagements is regulated as crisis management, which is understood primarily as an activity of public administration:

- Crisis prevention.
- Preparing to take control over crisis situations through planned actions.
- Responding in the event of an emergency.
- Removing the effects of crisis.
- Reconstruction of resources and critical infrastructure.
- Cooperation during joined and combined engagements.

In Poland, there are several administrative levels, which must share information: country, state, county, municipality. Their tasks are:

- Preparation of crisis management or combined, joint engagements plans.
- Preparation of structures used in emergency or other situations.
- Preparation and maintenance of teams necessary to perform tasks included in the plan for management.
- Maintaining the databases needed in the process of management.
- Preparation of solutions in the case of the destruction or disruption of critical infrastructure.
- Ensuring consistency between the management plans and other plans drawn up in this regard by the competent public authorities.
- Evaluation and forecasting of threats (*real and potential*).
- Surveillance, monitoring and decision function both during performing missions and planning.

On each of the levels of information, management process can be proceed in two main situations:

- to monitor the situation when no events of a crisis or other emergency happen,
- to response in case of any emergency.

During an emergency situation there is a need to generate reports at a specified interval. In these reports two groups of information can be distinguished: about important events and actions of special units and about rescue – for example fire fighting ones. Frequently they are statistical in nature, however, in some cases, they may contain certain elements in more details. Reports should be accessible in accordance with established security policies for all units working together within the different departments: military and police, fire, medical services, and organized to support the civilians.

Rescue teams are a separate core of emergency response, their activities are focused on actions in the field, where on the basis of given orders they are planning their tasks. They also need to collect all kind of information which is forwarded according to data flow structure.

III. Concept of realization

Described ways of collaboration impose directed implementation of solution. Many people and organisations need to collaborate at different levels and share common information.

Implementation should be flexible and have clear, consistent architecture from business point of view. Furthermore it should be capable and ready for future expansion. It should contain independent services which are responsible for different topics and areas in defined communities of interests. Shared information should be exchanged with established and acceptable workflow.

Moreover system should be able to connect to multiple sources and gain various data from different interfaces. It is not so important from civilian point of view, however, this feature is a must for military troops and their need of cooperation with forces from other nations, using other systems of C3IS and derivative class.

Besides flexible data management, software users will need strong social collaboration. All these conditions implicate usage of **Service Oriented Architecture** in the design and production stage.

Service Oriented Architecture is concept promoted by **NATO Network Enabled Capability** [2] (Fig. 1) and **EU Network Enabled Capability** [5] pointed as right one for military command systems. Although crisis management solution can not be defined as strictly military, however mentioned principles are appropriate in all information management systems. Main assumption of NNEC and EU NEC is modularity of business services for greater flexibility. Software systems are built from components with defined interfaces, which interior is undefined from business point of view. Every component represents service with defined scope of action.

Furthermore, it is assumed that already existing and fielded software components of **JASMINE System** [9-10] (Fig. 2) will be used. They will be implemented on both the server, individual workstation and other, dedicated devices sides to extend capabilities and functionalities of the Web Portal and devices.

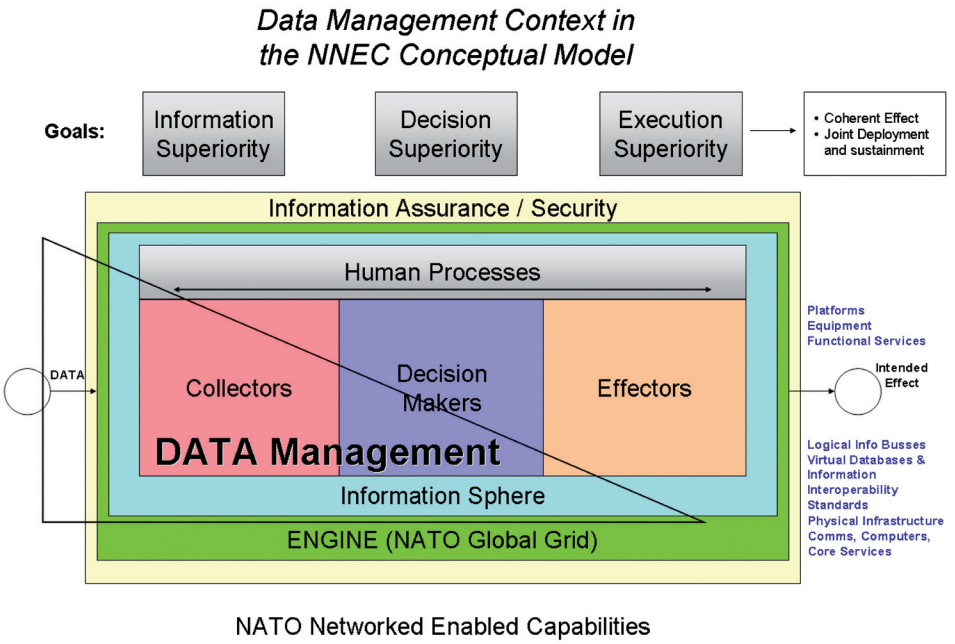

Figure 1. The flow of the information in the NNEC model [2]

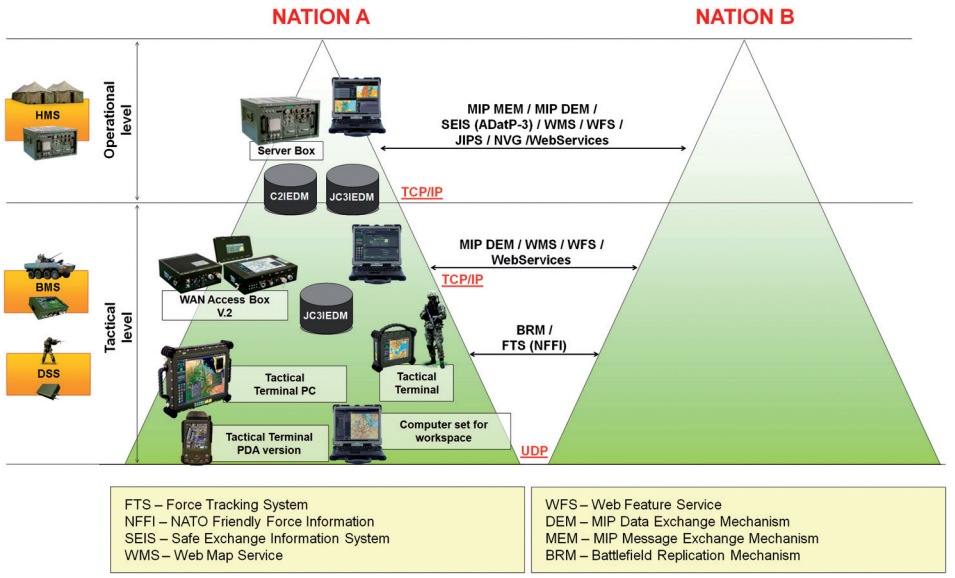

Figure 2. JASMINE System

The system contains many nodes and each of them can be dedicated to different tasks. That means, that both hardware and software should be carefully selected to complement each other. It is possible to identify, in general (Fig. 3):

- nodes of groups of people acting directly with consequences of disasters or designed plans,
- nodes which are responsible for planning and giving the orders to nodes lower in hierarchy.

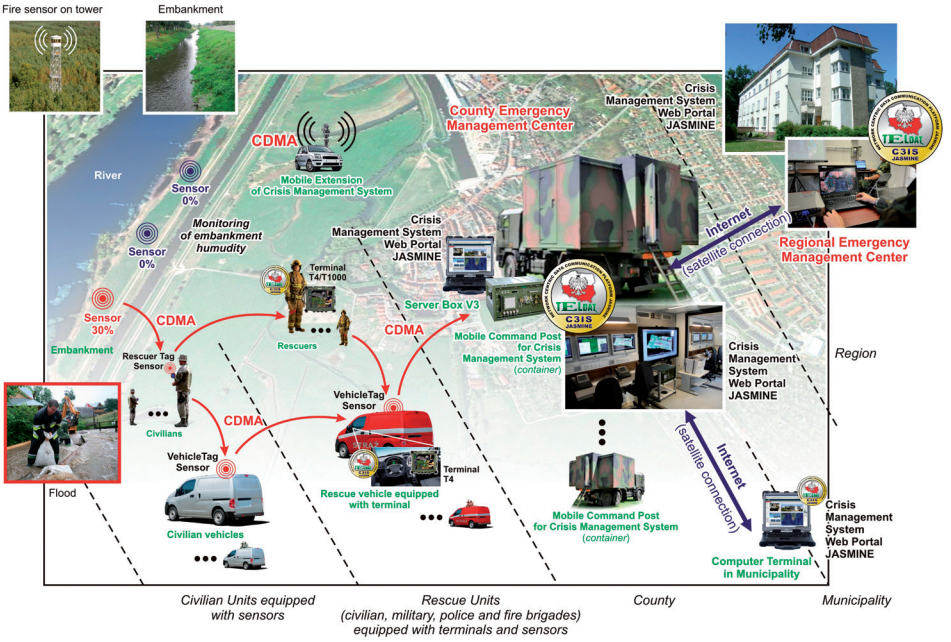

Figure 3. Nodes structure in crisis management

Because the most important thing in this type of information management systems is fast and reliable data delivery, proper communication medium should be selected. Such medium has to assure good quality and, usually, bandwidth. Among all kinds of radio means there should be pointed out that because of commonness, great coverage and possibility to easily add mobile ad hoc points, good option are cellular networks (*for example Code Division Multiple Access – CDMA technology* [11]).

Groups of people should be able to use mobile hardware designed to resist difficult weather conditions and physical damage in spite of incidental falls. Hardware should be equipped with support for preselected communication medium. That is why in Crisis Management JASMINE System there exist two types of mobile terminals, equipped with CDMA modems: T1000 and T4 (*which is the smaller one*). Furthermore, some users will be able to use dedicated device called Rescuer TAG, which is capable to send messages, about position of different accidents, to the system.

Technical specification of dedicated hardware equipment (*Fig. 4*) includes many features. The most important ones are low weight, small LCD, touchable screens,

CDMA, WIFI and Bluetooth support. They contain built in camera or two, depending on version. They have the possibility to work long on battery and be able to work under heavy conditions. They were also tested for falling from 1 m height and they are able to withstand it (even when they are switched on).

Figure 4. Tactical Terminals: T4, T1000 and Rescuer Tag

Stationary nodes on different administrative levels are equipped with dedicated, ruggedized servers. Servers should be also built in mobile manner.

Mobile terminals require additional equipment – designed for touchable sceen applications. Software and servers should provide information to other nodes, with some kind of SOA interface, it assures that functionalities can be quickly expanded. The most compatible, with this idea, solution, seems to be based on WebServices.

The more granular the components (*the more pieces*), the more they can be reused. When functions in a system are made into stand-alone services that can be accessed separately, they are beneficial to several parties. This architecture also provides a way for consumers of services, such as web-based applications, which are the most common and known example of using SOA, to be aware of available SOA-based services.

The best solution for desired needs is a Web based server that can be used to customize portals and content management sites for collaboration. It should be versatile in number of features:

- **management of content:** capabilities for managing various files types, audio, video and images, support for terms and keywords, content organizer, ability to define content types and re-use them across site,

- **application integration:** possibility to use services like Web 2.0 [12] blogs and wikis,
- **social computing:** like blogs and wikis, rich member profiles, tagging and comments, activity feeds, people search, workspaces,
- **business intelligence:** possibility to use scorecards, dashboards and self-service analysis functionality.

Users use the workstations that run Web browsers and additional software components that allow them to take advantage of the functionality offered by the Crisis Management JASMINE System.

The same analysis has been performed for software dedicated to mobile terminals. The best choice leads to using JASMINE software components to create applications designed for common database and communication infrastructure.

Web Portal consists of different components responsible for data presentation, database storage, services that automate user work as well as other components of the system.

Crisis Management System Web Portal JASMINE is a platform designed for collaboration and working with groups of files which allows concurrent cooperation on documents and their exchange between different organisational units or users. The system includes a set of services that leverages the power of the engine and integrates them with the JASMINE system components used in software part of Crisis Management System. Thus creates a platform on which different units of various types can work regardless of number of functional groups.

On workstations, software components have an ability of connecting directly to system native data sources and provide user with functions capable of data presentation and manipulation. Furthermore, in the context of other data sources on the server, native ways of replicating data between other command posts are used.

In addition, software components, which work directly on files allow users to manipulate them on workstations, while the outcome of their work is stored on the server as files or in database.

IV. System functionalities

Crisis Management System design has been based on previous experiences with very well tested and flexible JASMINE System. It uses existing components regarding infrastructure of communication and database, what means that it is able to exchange data over different of military protocols.

Crisis Management System Web Portal JASMINE is a portal with many subpages connecting with various services. This is the basement for work of all forces involved in emergency situations or combined engagements. We can distinguish user modules specialized in user-friendly service of organizational and individual cells – which are part of the functional structure of crisis management network.

System supports different dedicated modules responsible for wide area of interests. Each module was designed to fulfil needs of unit dealing with one kind of tasks:

- **Video Streaming Web Part** (*Fig. 5, part 1*): possibility to receive video streams from rescuers or unmanned aerial vehicles,
- **Web Operational Client** (*Fig. 5, part 2*): supports the process of coordinating the work of all of the staff regarding operational data, plans of emergencies, provision of maps and other topographic documents, the daily operations, situation map,
- **Mail Web Part** (*Fig. 5, part 3*): possibility to edit, receive and send mails to predefined contacts from Contacts Manager, ability to create multiple inboxes and automatic filters for incoming messages,
- **Contacts Manager Web Part** (*Fig. 5, part 4*): possibility to manage all contacts, used in sending and receiving messages, documents and files, contacts can represent both individuals and logical units,
- **Calendar Web Part** (*Fig. 5, part 5*): possibility to create and manage tasks scheduled for time and date and assigned to individuals and units,
- **Collaboration Web Part** (*Fig. 5, part 6*): supports creating, editing and managing documents of all kinds, with the possibility to collaborate within group of individuals and units, ability to use templates and generate reports in many forms,
- **Documents View Web Part** (*Fig. 5, part 7*): supports viewing and navigating documents of all Microsoft Office kinds,
- **File Explorer** (*Fig. 5, part 8*): ability to manage files within Web Portal, sending to recipients**,**
- **Message Communication Web Part**: possibility to send and receive text messages using own protocol and JCHAT, XMPP,
- **Documents Exchange Web Part**: ability to send all documents, prepared in other Web Parts, with the help of different protocols.

All modules should allow to work with the formalized documents that are created from predefined templates. Each module will have a typical set of the documents templates characteristic for its job. It enables to work through a web browser with the following types of MS Office documents: MS Word, MS Excel, MS PowerPoint.

A. Information sharing and dissemination

Portal functionality, beyond the storage of files, provides an implementation of the documents relevant access policy, archiving, sharing management information, business processes and publishing content. Portal fully integrates with the operating system. Documents can be easily managed from a file manager built into the operating system (*Explorer*) or from File Explorer Web Part. Documents in the portal can also be viewed directly from the operating system.

Crisis Management System Web Portal JASMINE allows coordination of information between multiple types of databases through integration with JASMINE System.

Figure 5. Web Portal JASMINE – main page

B. Communication among users

Crisis Management System allows communication between users in different levels, specialties and affiliation. Methods of communication are different for various purposes and depend on demand. They include:

- **Instant text messaging** – communication via text messaging available via the Internet or via a web browser application (including JCHAT, XMPP protocols).
- **E-mail** – communication using e-mail.
- **Video** – communication using video image coupled with the transmission of voice (*videoconference*). As for voice chat would be possible with one or more people.
- **Forums** – communication using forums or newsgroups.

V. Practical implementation

In current paragraph there will be described imaginary example of Crisis Management System practical implementation (*Fig. 6*). It has to be assumed that exist few nodes in system. We have stationary nodes with dedicated Crisis Management System Web Portal Jasmine servers, each dedicated for different administrative level:

- country one, where all main decisions and general planning takes place,
- county node, where all information from given area is collected and analyzed,
- the same goes for level of district and municipality, but areas of responsibility are smaller,
- nodes located in military forces command post,
- nodes located in fire fighters command post.

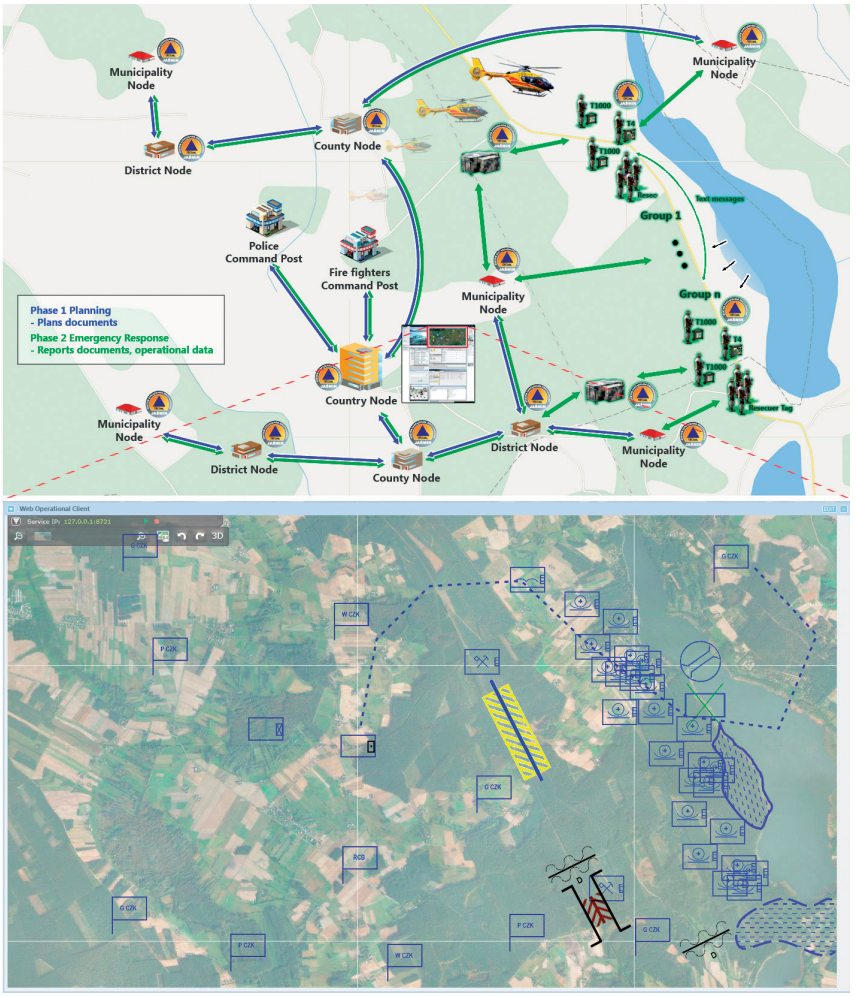

Figure 6. Example – situation presenting cooperation during crisis management

Furthermore there are many terminals T4 and T1000, handed out to people divided into groups. Each group leader receives *T4*, the bigger version of mobile equipment, which can be mounted in vehicle. Others receive either smaller version – *T1000* or *Rescuer Tag*. The first phase relies on plans preparations. Country node, during this process, sends messages to nodes located lower in hierarchy with orders to fulfil local plans for crisis situations. Nodes in local areas receive message and, according to templates, start to fill in their smaller versions of bigger plan. Next they send drafts to country node, which combines documents altogether.

Stage two starts when flood begins. Troops data is being sent to dangerous areas, where they collect information and insert on map operational symbols representing localization of different accidents. Operational crisis view is shared between all nodes and troops. Furthermore they send each other (*between groups*) text messages which describe current situation and status. These messages are being used by local areas county and other nodes to generate reports which are next being forwarded to country node. Country node displays current view and combines it with all text information, gathered from bigger surface. It decides, according to previously created plans, that it is time to ask for help additional forces and sends email to fire fighting troops and request documents to police. Special forces are coming to designated areas and decide to call emergency – flying vehicle to evacuate most injured civilians. Aircraft arrives, which can be seen on the map, takes survivors and, according to route drawn on map, returns to base via safest path.

VI. Summary

For many years till now, NATO is constantly developing many doctrines and concepts that describe effective collaboration within information organisations and with the outside world. It is very important that all rules are taken into account during planning and execution phase of all tasks resulting from civil-military cooperation.

Considering all aspects presented in the article, described system, based on components of JASMINE, altogether with dedicated hardware and Crisis Management System Web Portal Jasmine fulfils all needs regarding efficiency, information quality and collaboration. Furthermore, using proven and common communication technology, it assures its reliability. Everything described as part of Crisis Management System proves that technologies such as Service Oriented Architecture, Web Services, Web Portals are crucial to ensure system scalability, flexibility, interoperability and future development.

Crisis Management System JASMINE is dedicated information system that meets all essential requirements of every level nodes dealing with natural disasters. It is a right tool for right people to secure collaboration of unit's sections and groups as well as cooperation within civilian, military and other, special organizations.

REFERENCES

[1] "Miejski plan reagowania kryzysowego. Plan główny. Załącznik nr 6.4", Ośrodek koordynacyjno-informacyjny ochrony przeciwpowodziowej. Regionalny zarząd gospodarki wodnej w Krakowie. http://oki.krakow.rzgw.gov.pl/Content%5CEdukacja%5Cpdf_ogr_skutkow%5CLPSOPiP_miasto_Krakow%5C6.Zalaczniki%5C6.4_Miejski_plan_reagowania_kryzysowego.pdf
[2] ISSC NATO Open Systems Working Group, Allied Data Publication 34 (ADatP-34) NATO.
[3] Maj. Yavuz Fildis, J. Troy Turner, NATO Network Enabled Capability (NNEC) Data Strategy, 2005.
[4] P. Copeland, M. Winkler, Technical note 1197 Analysis of Nato Communications standards for the NNEC, 2006.
[5] EXTRACT FROM THE NEC VISION EU NEC VISION REPORT, www.eda.europa.eu/WebUtils/downloadfile.aspx?FileID=1152
[6] AJP-9, NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE, 2003.
[7] „Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym" (Dz.U. z 2007 r. nr 89, poz. 590, z późn. zm.), 2007.
[8] „Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2009 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego i wojewódzkich centrów powiadamiania ratunkowego" (Dz.U. 2009 nr 130 poz. 1073), 2009.
[9] W. Zawadzki, „JASMIN wkracza do armii", Nowa Technika Wojskowa nr 5/2007.
[10] H. Kruszynski, „Sieciocentryczna platforma teleinformatyczna", Bellona, Ministerstwo Obrony Narodowej, nr 2/2011.
[11] J. Bannister, P. Mather, S. Coope, „Convergence Technologies for 3G Networks: Ip, Umts, Egprs and Atm", 2004.
[12] T. O'Reilly, „What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software", http://oreilly.com/web2/archive/what-is-web-20.html, 2005.

Application of CID Server in Decision Support for Command and Control

Krzysztof Muchewicz, Marek Piotrowski,
Henryk Kruszyński, Robert Palka

Research & Development Department,
TELDAT Sp. J., 85-640 Bydgoszcz, Poland,
{kmuchewicz, mpiotrowski, hkruszynski, rpalka}@teldat.com.pl

Abstract: In brief, Combat Identification (CID) is the capability to differentiate entities in a combatant's area. Effective CID is a crucial factor for minimizing casualties and improving performance of military forces. A lot of solutions have been already created and applied on various military scenarios. Two of them are NFFI and Link 16. Although they prove to be useful on ground and air respectively, it has been identified that one cannot use information from both systems on air to ground arena. From this scenario the idea of CID Server has grown. First implementations have been created. Also NATO recognized the need for standardization and has started development of corresponding STANAG document.

This article organizes knowledge about CID Server and presents CID JASMINE, which is a realization of CID Server concept.

The main idea of CID JASMINE is to provide effective solution that will satisfy all requirements for CID Server both in national and multinational environment. To make it possible, the topic of CID has been deeply analyzed. Also existing CID solutions and capabilities have been studied. After that, advanced programming techniques and patterns have been applied to achieve goal.

The final CID JASMINE will be a leading product in its category. Its first beta version was tested during CWIX exercise and first official release is planned at the end of 2012.

Keywords: Combat Identification; Friendly Force Information; CID Server; JASMINE System; CID JASMINE

I. Introduction

"In combat, the only thing worse than enemy fire is incoming friendly fire."

The above statement from Marine Corps Sgt. Aldo Wong best describes the importance of the subject of Combat Identification (*CID*). Developing solutions for identification of objects on battlefield is crucial to minimize casualties and improve performance of military forces. In brief, definition of CID is as follows:

Combat Identification (CID) is the process of attaining an accurate characterization of entities in a combatant's area of responsibility to the extent that high-confidence, real-time application of tactical options and weapon resources can occur.

CID capability consists of following elements:

Combat Identification (*CID*) = Situation Awareness (*SA*) + Target Identification (*TI*) + Non-materiel alternatives.

A lot of CID solutions have been already created and applied on various military arenas. This includes: non materiel solutions like doctrine, training and materiel solutions e.g. sensors and C2 Systems. Two of them that should be mentioned are NFFI and Link 16. They have been already deployed and well tested, among others in Afghanistan. Although they prove to be useful on ground and air arenas respectively, it has been identified that one cannot use information from both systems on air to ground scenario. From that the need of CID Server has grown. The CID Server is one of CID solutions that improve combat identification process by collecting CID data from different sources and providing it on demand to consumers.

First implementation of CID Server has been created by USA (*BAE Systems, [1]*) and Germany (*CIGAR from ESG, [2]*). Also NATO recognized the need for standardization and has started development of STANAG document [3][4]. Since the idea of CID Server is still young, there is only slight knowledge about possible features and its applications. The minimum is to provide Friendly Force Information from ground units to fighter aircraft. However, possible applications could be much wider and include all scenarios when the decision of engagement is weighed.

Also TELDAT, an innovative company from Poland, has started development of its own CID Server product – CID JASMINE. The main goal of this article is to present concept of CID JASMINE and to show its main features according to existing CID and CID Server solutions.

The CID JASMINE product will be based on existing components of JASMINE System, both software and hardware. As a hardware component CID JASMINE will use Server Box V.3, which is an efficient and powerful military Server station. Dedicated CID JASMINE software will work on Microsoft Windows 2008 Server operating system. All software elements are based on the SOA architecture and build upon MessageBus. Position Location Information (*PLI*) will be received using NFFI IP1, IP2 (*NATO Friendly Force Information, Interoperability Profile 1 and 2*) and Link 16. It will be provided using Link 16 and NFFI SIP 3 (*Service Interoperability Profile 3*). CID Server capabilities will be successively extended to all available CID solutions, like VMF (*Variable Message Format*) and BRM (*Battlefield Replication Mechanism*). CID JASMINE will also provide operational picture and expose it using NVG (*NATO Vector Graphics*) protocol and web client application. This will enable to use CID information created by Server directly from Web Browser user interface. Therefore CID JASMINE will not only be a set of functional services but it will also provide operational picture on tactical level. The architecture and implementation of CID JASMINE will be focused on quality parameters of product.

The article is organized as follows. Section 2 presents general definition and information concerning Combat Identification. Section 3 gives short overview

of selected CID solutions. Section 4 presents general CID Server concept. Section 5 describes the main ideas, features, architecture of CID JASMINE.

II. Combat identification

In this section the main facts concerning Combat Identification (*CID*) are introduced. The general definition is given below:

Combat Identification (CID) is the process of attaining an accurate characterization of entities in a combatant's area of responsibility to the extent that high-confidence, real-time application of tactical options and weapon resources can occur. The objective of CID is to maximize combat/mission effectiveness while reducing total casualties (due to enemy action and fratricide) [5].

Another definition is as follows:

Combat Identification (CID) is the capability to differentiate potential targets mobile and fixed, over large areas with corresponding long distances as friend, foe, or neutral in sufficient time, with high confidence, and at the requisite range to support engagement decisions and weapon release [6].

It can be seen from above definitions that CID is a very general term that touches various operational and functional topics. The main motivation to develop CID in military forces is to minimize friendly fire accidents and to help prevent unnecessary combat losses. However CID is required also for other reasons. It is needed among others to:

- effectively field fighting forces,
- support to rapidly and positively identify enemies, friends, and neutrals in the battlespace,
- manage and control the battle area,
- optimally employ weapons and forces,
- minimize casualties.

The importance of CID has grown in the modern times since there is much more attention about personnel loss than, for example, in the beginning of 20th century.

Below some aspects of CID are shown. First operational and functional capabilities are presented then description of system-of-systems concept is given in accordance to CID.

A. Operational capabilities

CID is applicable in the following areas:

- Air to air,
- Air to surface,
- Surface to Surface,
- Surface to air.

Surface area includes land and sea. The subsurface is known as ground and maritime. In each of the these CID need is essential for commanders. CID capability is required for all mission scenarios. However, in different ones it can be implemented differently. The next picture presents various actors on various mission areas.

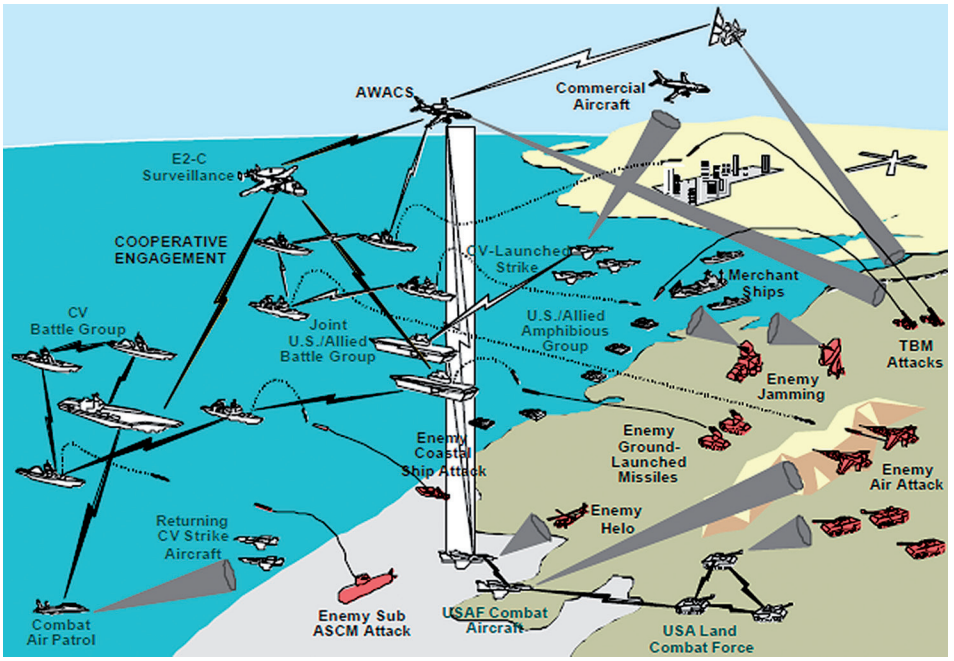

Figure 1. CID Application on mission areas, source [5]

To deliver CID capability, it is required to provide solutions that implement it. The CID concept can be implemented with two main types of solutions: materiel and non-material.

Non-materiel solutions contain:

- doctrine;
- tactics, techniques, and procedures (*TTP*);
- training.

Non-materiel solutions often need to be augmented by materiel solutions. Materiel solutions can be characterized as:

- sensor systems – cooperative and non-cooperative (*like radar signal modulation, high-range resolution radar, electronic support measures*),
- command, control, and communications (*C3*) systems, in particular these could be digital data links and radios, each of which contributes a portion to the CID solution.

One can see that, in the given description, CID is viewed as capability rather than a single program or system. This is the approach of "system-of-systems". CID

is a result of a process that appropriately and accurately characterizes the entities present in a combatant's area of responsibility. Effective CID can vary depending on the conditions of the battlespace. The following scenarios can be identified:

- In some cases the required identification is used only to rapidly distinguish among friendly, neutral, and enemy forces with confidence high enough to support weapon employment decisions.
- At other times, identification of target class (*e.g., cruise missile, fighter, or bomber*) or target recognition (*e.g., target vs. decoy*) is required to select the correct defensive or offensive tactical weapon response.
- In other cases, a more precise characterization that identifies specific target parameters, such as platform type (*e.g., MiG–29 vs. MiG–21*) and intent (*e.g., an active interceptor vs. a defector*), is required to select optimal defensive weapons and to support weapon release decisions.

In all cases, the goal for CID is to provide the level of identification that is necessary for Weapon Delivery Assets to make correct decisions.

B. Functional capabilities

The functional capabilities for CID include:

- foe identification (*including platform type, class, nationality, allegiance, and intent information*),
- friend identification,
- neutral identification,
- interoperability.

From the above one should put special attention on interoperability, since it is crucial for CID System to operate in multinational environment. To achieve interoperability, CID solutions have to be build upon standards, in particular NATO standards. Different solutions can be applied to obtain described above functionalities, both materiel and non-materiel.

C. CID system-of-systems

From presented earlier classification, CID can be seen as a capability, not a single system or program. Therefore CID implementation can be described as "system-of-systems". It can be seen as collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new more complex system which offers broader functionality. All of these systems are critical contributors to a system-of-systems approach in providing both situational awareness and identification to use lethal weapons in the battlespace. The functional capabilities of all CID systems must work synergistically to provide a robust, high-confidence.

III. Overview of selected CID solutions

Below selected CID solutions are presented. All of them belong to the group of materiel, C3 solutions. First two solutions are well known and broadly used NATO standards. The third is a radio replication mechanism that is an element of JASMINE System. All this mechanisms will be adopted in CID JASMINE.

A. Friendly Force Information – NFFI

NFFI standard was created in 2005 and has been developed until today by NATO Consultation Command and Control Agency (*NC3A*). It has been created to improve and simplify Real-time Friendly Force Tracking in the multinational environment. It enables tracing and identifying friendly forces in near-real time. NFFI is divided into three parts:

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

Information is exchanged via IP1 and IP2 using formal messages that contain basic track information like identifier, system parameters, position and report time.

Development of SIP3 protocol was started in 2006. SIP3 is based on Web services. More information about NFFI can be found in [7][8].

B. Tactical Data Link – Link 16

Link 16 is a military tactical data exchange network created and used by the United States and adopted by some of its Allies and by NATO. Its specification is part of the family of Tactical Data Links. It uses the transmission characteristics and protocols, conventions, and fixed-length or variable length message formats defined by MIL-STD 6016, STANAG 5516. Link 16 information is primarily coded in so called J-series messages. This messages are binary data words with well-defined meanings. In particular, Link 16 can be used to report and to pull CID information. More details about Link 16 can be found in [9][10].

C. National solutions – BRM

BRM data exchange mechanism has been created to enable exchange of operational information on tactical command level, mainly in the low-bandwidth radio networks. It has been developed by TELDAT Company and is applied in JASMINE System. BRM is based on UDP protocol and it combines high performance with flexibility and great capacity to exchange operational information. It supports exchange of data according to MIP *C2IEDM and JC3IEDM* data models.

BRM mechanism is used in C3IS JASMINE System on tactical and dismounted soldier level, therefore this system can be used to exchange and provide CID information. More information about BRM can be found in [11].

IV. CID server concept

In Section III we have presented various systems that provide and exchange CID information. NFFI and Link 16 have been adopted in NATO and are used also in Afghanistan. Although being very useful, they are limited to specific areas and scenarios. As a way to improve CID, especially in ground to air scenarios, CID Server concept has been created. CID Server collects information from different land CID sources:

- CID Sensors,
- BFT systems,
- Situation Awareness systems (*SA*).

CID Server provides this information on demand, for specific area.

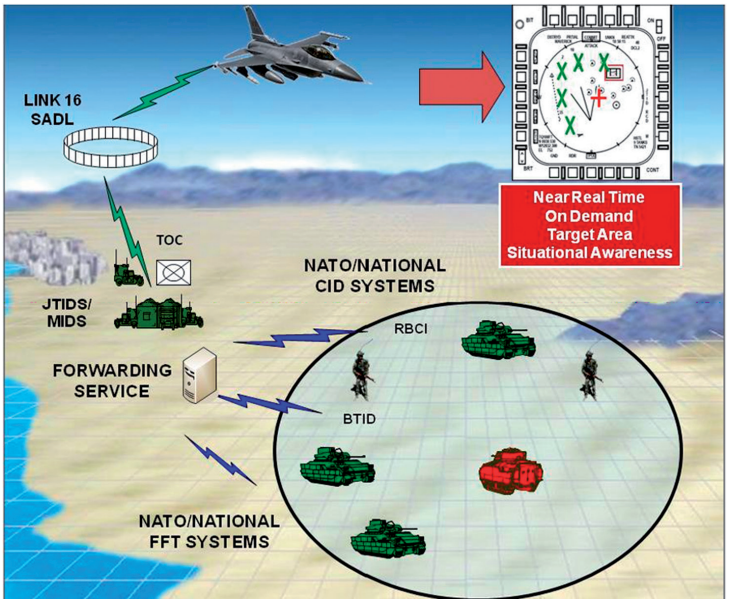

Figure 2. CID Server application, source [3]

The primary goal of CID Server is to support non-engagement decisions, whenever a risk of exposing own forces exists. This is because FFT, cooperative CID and SA systems might only provide near real-time situation awareness information.

CID Server will use various communication protocols for receiving and providing information. In modern military operations, interoperability will be one of the most important features of CID Server. Therefore it should support international standards. To satisfy this, the service should be agnostic on:

- data source/system (*friendly force tracking [FFT], combat identification [CID], situational awareness [SA] system*),
- receiving platform/system (*aircraft, ship, artillery battery, fire support cell, etc.*),
- communication means (*tactical data link, local area network [LAN], etc.*).

Server should support existing data exchange standards, therefore NFFI and Link 16 shall be supported. Following protocols have been identified as applicable for CID Server:

- Link 16,
- NFFI IP1, IP2,
- NFFI SIP3,
- VMF,
- Cooperative sensors,
- National standards for exchanging PLI (*Position Location Information*) from SA systems.

A. CID server NATO standardization

The lack of a system of this type has been identified in NATO, and work on the standardization has been started. Draft version of STANAG was created: "NATO STANDARD FOR SERVICES TO FORWARD FRIENDLY FORCE INFORMATION TO WEAPON DELIVERY ASSETS" [3][4].

This STANAG provides guidance for implementation of existing interoperability and data exchange standards, interface profiles, and both business rules and forwarding rules for collecting PLI and forwarding it to users in the appropriate systems.

Currently there are no fielded CID systems capable of providing friendly PLI to the service for forwarding to weapon delivery platforms. For the foreseeable future, only FFT and SA systems are capable of providing the necessary information. The service is primarily based on conveying friendly PLI to weapon delivery platforms through Link 16, the only NATO-wide, standardized tactical data link (*STANAG 5516*).

The service is planned to be based on an open architecture to provide connectivity of all FFT, CID, and SA technologies and as much as possible:

- use existing ground and air systems and infrastructure,
- require no modification of existing systems,
- be expandable/adaptable to emerging PLI Sources (*e.g. MMW, RBCI*),
- be NATO and Coalition interoperable.

The work on STANAG for CID Server will last at least until the end of 2012.

B. CID server usage scenarios

Below some of the usage scenarios for CID Server are listed:

- Air-to-surface – in this scenario CID data from ground actors is pushed into CID Server and exposed to fighter aircrafts. Aircrafts use CID information to identify targets and to support engagement decision.
- Ground-to-ground – in this scenario CID data from CID Server is consumed by Weapon Delivery Assets on battlefield. CID information supports decision about weapon usage.

- Multinational – in this scenario CID Servers from different countries and systems can exchange information with each other and enable CID when forces from various countries cooperate on battlefield.

The use cases described above are presented on the next picture.

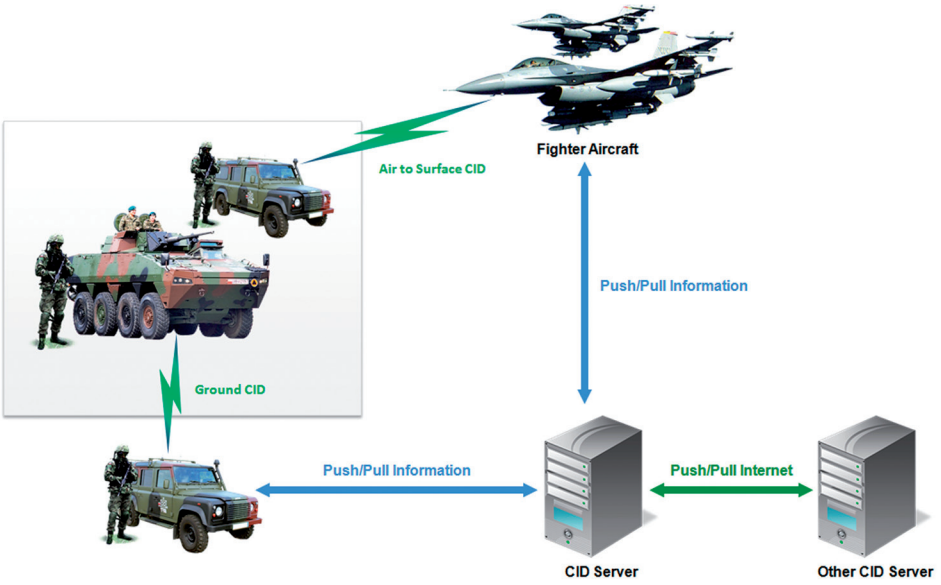

Figure 3. CID Server use cases

C. *CID server application in NATO operations*

Since the idea of CID Server has grown during Afghanistan mission, its usability in NATO operations is the main motivation for its development. Different nations have various CID capabilities, both cooperative and non-cooperative, that are specific and not based on NATO standards. This capabilities cannot be used in multinational environment. It would be very non-efficient to replace this national solutions and create new ones dedicated for NATO missions. Therefore creation of one solution – CID Server – that will mediate between different solutions from different vendors and countries, will simplify the goal of unification and cooperation of NATO forces. Such an application of CID Server might be a goal in a long term.

In a short term CID Server will use already proven solutions like NFFI and Link 16. This will be still very valuable for improving CID capabilities of joint forces NATO operations.

Another important capability is an ability to exchange information between different CID Servers. This can be made using already existing NATO standards and protocols (like NFFI) however STANAG document can simplify this task.

V. CID JASMINE concept and implementation

CID JASMINE is an implementation of the concept of CID Server from TELDAT Company. CID JASMINE is a part of JASMINE System.

According to NNEC concept elements of JASMINE system was 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. The system consists of hardware and software. 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 during the national and international exercises, where wide range of provided services were presented. More information about JASMINE System can be found in [12].

The CID JASMINE product is based on existing components of JASMINE System, both software and hardware. As a hardware component CID JASMINE uses Server Box V.3, which is efficient and powerful military Server station. Dedicated CID JASMINE software works on Microsoft Windows 2008 Server operating system.

All software elements are based on the SOA architecture that is build upon MessageBus. The next picture presents functional features of CID JASMINE.

Figure 4. Functional capabilities of CID JASMINE

PLI information is received using:

- NFFI IP1, IP2 – land tracks is send to CID JASMINE using UDP or TCP protocol;
- Link 16 – messages containing information about paths of different types of objects can be provided to CID JASMINE. Some of the possible messages are J3.5, J3.2.

The information is provided for consumers using:

- Link 16 – there are dedicated Link 16 messages that enable to provide information on demand, according to given area;
- NFFI SIP 3 – based on Web Services this protocol allows to pool for tracks information for specified area.

CID Server capabilities will be successively extended to all available CID solutions, (*like VMF and BRM*). Link 16 communication will be implemented over JREAP C protocol. The timeline for CID Server is presented on the next diagram.

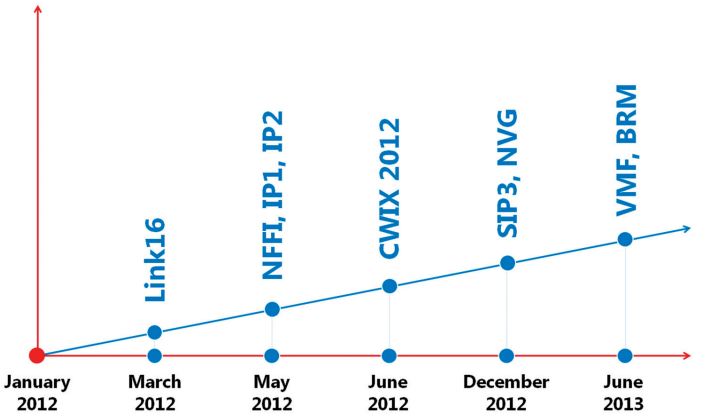

Figure 5. CID JASMINE Timeline

CID JASMINE provides also operational picture and exposes it using NVG protocol and Web Client application. This enables to use CID information created by Server directly from Web Browser user interface. Therefore CID JASMINE is not only a set of functional services but it also provides operational picture on tactical level.

The architecture and implementation of CID JASMINE is focused on quality parameters of product, in particular:

- Performance – Server process a lot of real time data.
- Scalability – it is possible to scale CID JASMINE to multiple computer stations. This is achieved using MessageBus infrastructure and SOA architecture.
- Reliability – Server Box V.3 is a military server that satisfies all quality and reliability parameters for military equipment. Also development of CID JASMINE software has been focused on reliability.

CID JASMINE is developed in connection with STANAG for CID Server. The development of STANAG will be observed and all important conclusions will be implemented.

The first official release is planned at the end of 2012.

A. CWIX 2012

First tests of the product has taken place during CWIX 2012 exercise. Link 16 Gateway, which is a part of CID JASMINE has been extensively tested with systems from various countries and vendors. Below there is a list of CWIX capabilities that where test partners for CID JASMINE:

- 2012-DEU – CIGAR3;
- 2012-FRA – COCCA;
- 2012-FIN – JADEC2;
- 2012-ITA – AF AC2IS BladeRunner;
- 2012-DNK – C-Flex;
- 2012-NATO – ACCS LOC1 ARS;
- 2012-POL – PAFLINK16;
- 2012-NATO – NC3A-IETV-NIRIS;
- 2012-NATO – TEDS JCTD/CWP;
- 2012-NATO – NLVC (FLAMES), including JTLS.

All test where successful. Performed tests covered exchanging Link 16 messages over JREAP protocol and visualization of exchanged information.

B. Unification of identifiers

CID Server uses various protocols and each of them use its own identifiers for battlefield objects. CID JASMINE will solve this issue in the following way:

- For all types of information received by CID JASMINE the original information will be preserved.
- If it will be necessary to map information between different protocols and it will be impossible to translate identifiers, then new identifiers will be generated according to configuration.
- Once created mappings for identifiers will be stored for future use, to guarantee that each piece of information will be mapped in one way.
- System will provide user interface for configuring and manually manipulating all mappings.

Presented above strategy will be used not only for identifiers mappings but for all parameters of battlefield objects that require mappings.

C. Performance and reliability

The quality of CID Server depends mainly on the two factors:

- Quality of Data Services, i.e. the services that are responsible for storing and providing data.
- Quality of internal communication infrastructure.

This two elements will be supported in CID JASMINE in the following way:

- Data Store will be based on relational database, however it will be supported with object oriented database and additional caching mechanism. On this area TELDAT engineers has broad experience gained during developing Data Services for tactical command systems (BMS JASMINE).
- Communication and messaging infrastructure will be provided by Message Bus, the TELDAT middleware solution that provide robust, scalable and reliable infrastructure for interconnecting system services.

Provided mechanisms will guarantee proper quality:

- The performance of system will be based on scalability of data services and Message Bus. It will be possible to add new physical servers that will work as cluster for CID JASMINE during mission, without interrupting the server.
- Reliability will be assured by reliable-messaging that is part of TELDAT Message Bus solution.

VI. Summary

As has been presented in the article, Combat Identification is a basic capability for modern forces. CID Server is one of the solutions that extend CID capabilities and in some scenarios it is essential. The importance of CID Server has been noticed by NATO nations and also by NATO itself. First solutions have been implemented and STANAG development has been started.

CID JASMINE is an implementation of CID Server from TELDAT company. The main advantages of CID JASMINE will be:

- Interoperability – it supports all required interfaces and protocols;
- Performance and quality – based on the proven components of JASMINE System and SOA architecture it provides powerful platform for CID data exchange.

CID JASMINE is a net-centric product and an element of NNEC compliant architecture of JASMINE System. It consists of hardware and software elements and therefore it is a complete product ready to use on the field, in particular in NATO operations.

REFERENCES

[1] http://www.baesystems.com/capability/BAES_034933/combat-identification-iff
[2] http://www.esg.de/
[3] "NATO Standard for Services to Forward Friendly Force Information to Weapon Delivery Assets", Draft, January 2011, NATO Standardization Agency.
[4] "NATO Standard for Services to Forward Friendly Force Information to Weapon Delivery Assets", Draft, August 2011, NATO Standardization Agency.

[5] Join Warfighting Science and Technology Plan, February 2000, Department of Defence, http://www.wslfweb.org/docs/dstp2000/jwstppdf/00-title.pdf
[6] Join Warfighting Science and Technology Plan, 1997, Deparment Of Defence, http://www.fas.org/spp/military/docops/defense/97_jwstp/jw4c.htm
[7] V. de Sortis, NFFI Service Interoperability Profile 3 (*SIP3*) Technical Specifications (*VERSION 1.1.5*).
[8] STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems.
[9] STANAG 5516, Edition 6, TACTICAL DATA EXCHANGE – Link 16.
[10] "Departament of Defence Interface Standard for the Joint Range Extension Application Protocol (*JREAP*)" MIL-STD 3011.
[11] "Means for operational data exchange in JASMINE System", Military Communications and Information Systems Conference MCC 2009, 29-30 September 2009, Prague, Czech Republic.
[12] T.Z. Kosowski, Ł. Apiecionek, "JASMINE system: network centric concept and practical solution", Military Communications and Information Systems Conference MCC 2009, 29-30 September 2009, Prague, Czech Republic.
[13] W. Zawadzki, „JASMIN wkracza do armii", Nowa Technika Wojskowa nr 5/2007.
[14] H. Kruszynski, „Zastosowanie systemu JASMIN", Nowa Technika Wojskowa nr 9/2006.
[15] H. Kruszynski, L. Apiecionek, M. Dziamski, „JASMIN w warsztatach Combined Endeavor 2008", RAPORT nr 06/2008.
[16] Multilateral Interoperability Programme, The Joint C3 Information Exchange Data Model (*JC3IEDM Main*), 2007.
[17] „Sposoby wymiany danych operacyjnych w systemie JAŚMIN", XVII Konferencja Naukowa Automatyzacji Dowodzenia w Gdyni, czerwiec 2009 r.
[18] „Practical Solution", Nowa Technika Wojskowa – Future Soldier, 2010 r.
[19] „Command and Control Portal as a unified way of collaboration of different staff cells in army headquarters on operational level as well as cooperation with external civil organisations", proceedings of the Military Communications and Information Systems Conference MCC 2011, 17-18 October 2011, Amsterdam, Netherlands, p. 53-68.
[20] „Reliable and effective management of hardware and software in battlefield environment", proceedings of the Military Communications and Information Systems Conference MCC 2011, 17-18 October 2011, Amsterdam, Netherlands, p. 169-180.
[21] "Portal systemu wspomagania dowodzenia, jako sposób współpracy różnych komórek sztabu szczebla operacyjnego oraz kooperacji z zewnętrznymi organizacjami cywilnymi", XIX Konferencja Naukowa „Automatyzacji Dowodzenia", 2011 r., współautor.
[22] D.J. Bryant, D.G. Smith, "Impact of Uncertain Cues on Combat Identification Judgments", Defence R&D Canada, Technical Report.
[23] Joint Center For Lessons Learned, Rethinking Combat Identification, vol. IV, Issue 3, June 2002.
[24] Combat Identification Systems, Strengthened Management Efforts Needed to Ensure Required Capabilities, United States General Accounting Office, June 2001.
[25] "Technologia Web Portali we wspomaganiu pracy komórek sztabu z uwzględnieniem procesu tworzenia obrazu z rozpoznania", Seminarium w AON, 2011 r.

Military Communications and Information Technology: A Trusted Cooperation Enabler presents a broad range of topics in communications and information systems (CIS) technologies that significantly contribute to increase effective cooperation of all parties involved in coalition military operations performed in hostile and disadvantaged environments. The book gives an overview of the state-of-the-art in emerging and disruptive technologies, including perspectives from academia, research and technology entities, as well as industry.

Military Communications and Information Technology: A Trusted Cooperation Enabler is published in two volumes. The first volume is focused on: *Concepts and Solutions for Communications and Information Systems, Communications and Information Technology for Trusted Information Sharing, Information Technology for Interoperability and Decision Support Enhancement and Information Assurance & Cyber Defence, while the latter on the following: Tactical Communications and Networks, Spectrum Management and Software Defined Radio Techniques, Mobile Ad-hoc & Wireless Sensor Networks and Localization Techniques.* The contents of the book reflect the thrust of current research as the CIS military community strives to enable effective collaboration in all dimensions of the modern battlespace that contribute to increase the missions efficiency.

ISBN 978-83-62954-31-5
ISBN 978-83-62954-51-3