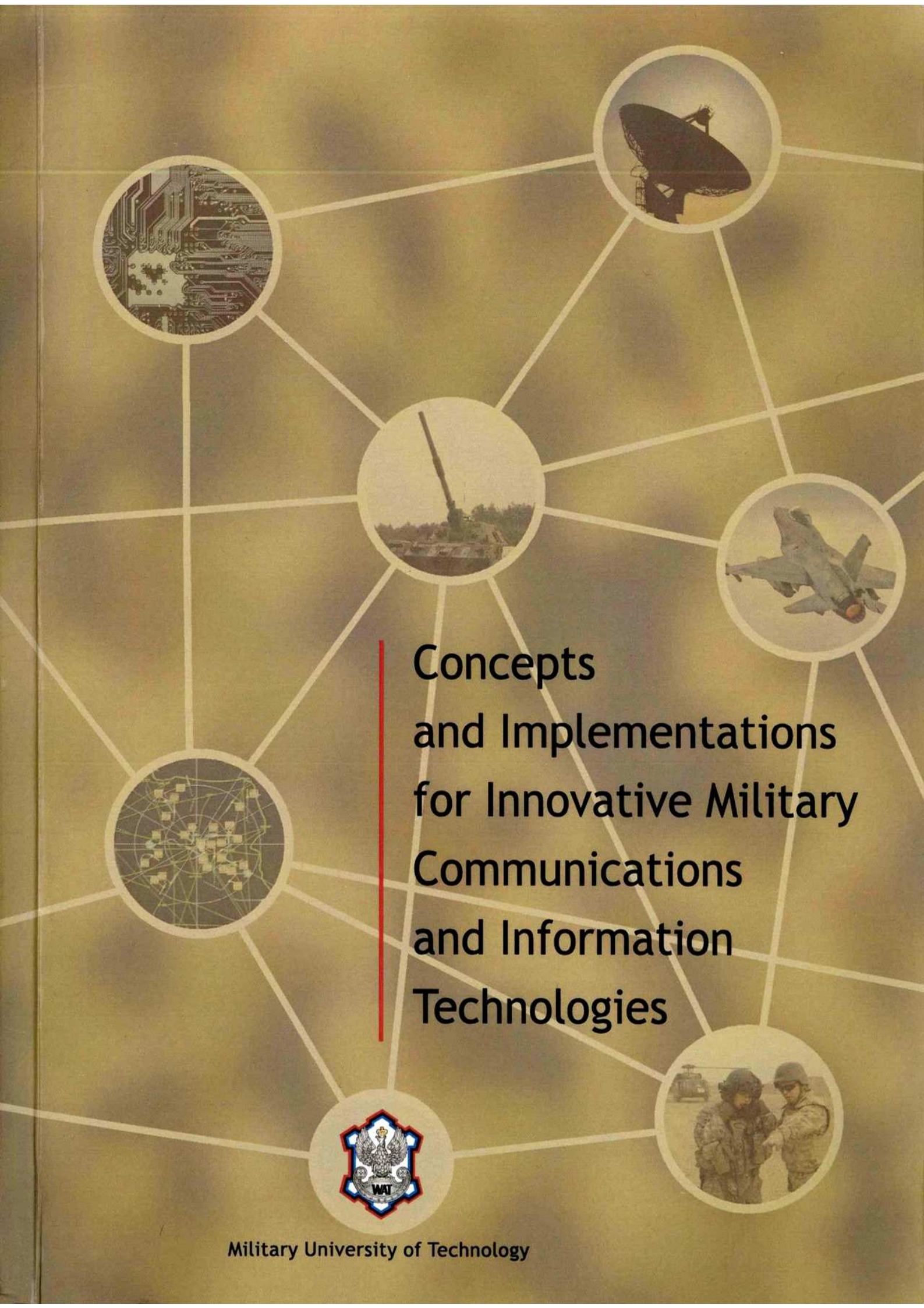

Concepts and Implementations for Innovative Military Communications and Information Technologies

Military University of Technology

Concepts and Implementations for Innovative Military Communications and Information Technologies

Warsaw 2010

Reviewers:
Prof. Jürgen Grosche
Assoc. Prof. Milan Šnajder

Editor:
Marek Amanowicz

Co-editors:
Markus Antweiler
Peter Lenk
Andrzej Najgebauer

© Copyright by Redakcja Wydawnictw Wojskowej Akademii Technicznej.
Warsaw 2010

ISBN 978-83-61486-70-1

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: BEL Studio Sp. z o.o., ul. Powstańców Śląskich 67b, 01-355 Warszawa

Warsaw 2010

Contents

Foreword

The efficiency of present and future military operations strongly relies on Command, Control, Communication and Computers Intelligence, Surveillance and Reconnaissance (C4ISR) systems' ability to facilitate decision superiority – the state in which better-informed decisions are made and implemented faster then an adversary can react. This requires significant changes in many areas including the procedural and technological domains. Significant efforts are made world-wide to achieve real progress in these areas that lead to elaboration and implementation of innovative communications and information technologies in military systems. Selected results of such activities are presented in this book.

The book contains the papers originally submitted to the 12th Military Communications and Information Systems Conference (MCC) held on 27-28 September 2010 in Wroclaw, Poland. This annual event brings together experts from world-wide research establishments, industry and academia as well as representatives of the military Communications and Information Systems (CIS) community. The conference provides a useful forum for exchanging ideas on the development and implementation of new technologies and services into military systems. It also creates a unique opportunity to discuss these issues from different points of view and share experiences amongst European and NATO CIS professionals. The 2010 conference was an important part of the Military Communications and Information Systems Week that also included the NATO Research and Technology Organization Symposium on Military Communications and Networks.

The papers included in this book are divided into nine sections that correspond to the conference sessions and are assigned to the following topics: *Network Centric Concepts and Solutions, Information and Knowledge Management, Semantic Interoperability, Web Services Provision in Disadvantaged Grids, Information Assurance and Security, CIS Simulation and Technology Demonstration, Tactical and Mobile Ad-hoc Networks, Software Defined and Cognitive Radio* and *Wireless Communication.* These papers cover a wide spectrum of CIS technologies that are at the focus of the military and reflect the current state-of-the-art in these areas.

The first group of contributions consists of 5 papers related to ***network centric concepts and solutions***. A discussion on how to get the essential information to the decision maker in a timely fashion and with the level of required assurance is a subject of the paper *R3 – Getting the Right Information to the Right People, Right*

in Time. Exploiting the NATO NEC by R.A. Poell and P.C. Sanjuan-Szklarz. The authors describe a filtering process where task-based user information requirements, described in an information consumer profile, is used to extract from all information available only that part that is relevant for the tasks the user is executing. Reliability of information, trustworthiness of producers of information and the validity of information in time are considered, as well. The next paper, *Supporting NATO Network Enabled Capability through the Utilization of Portals* by M. Uysal, O. Cetinkaya, and Y. Yildirim, investigates the possible approaches for building collaborative web applications using the provided services. The authors propose an approach using Web Services for Remote Portlets (WSRP) to integrate an existing application to a portal with minimum effort. The third paper, *Practical Solution for Integration of Single Soldier Equipment with Information System on the Battlefield* by R. Pałka, M. Piotrowski, K. Muchewicz and P. Baturo, depicts the Dismounted Soldier System "JASMINE" designed for teams of soldiers cooperating and fighting together in order to fulfil mission objectives. This solution provides for a single soldier capabilities of exchanging operational information about the location of friendly units, sending and receiving orders, reporting events, facilities, obstacles, etc. S. Kawaletz and K. Rein in the paper *Methodology for Standardizing Content of Military Reports Generated in Different Natural Languages* discuss a methodology for automatic analysis of military reports, including the extraction of the information contained in the reports and the conversion of this content into standardized Battle Management Language (BML) reports in order to support information fusion to create a joint situational picture. The final paper in this group, *Robots to the Ground* by T. Remmersmann, B. Brüggemann and M. Frey, describes how robots were integrated in a command structure by using Battle Management Language. The discussion includes information about which orders were implemented and which changes had to be applied to BML for commanding robots. It also includes information about how reports are sent back by the robots to the C2 system and information about how the task scheduling is handled.

The next group of six papers are focused on ***information and knowledge management*** issues. The first paper in this group entitled *Knowledge Management in Military Organizations* submitted by *L. Burita, P. Do, V. Ondryhal and M. Kuric* describes the results achieved within the MENTAL project conducted by the Czech Army research establishment. It defines the knowledge management (KM) system's ontology as well as specifies the KM functions and implementation technologies. The next paper, *The Next Era of Decision Superiority – Leveraging Stream Computing and Low-Latency Decision Making* by M. Donovang-Kuhlisch and M.K. Small, *introduces state-of-the-art edge stream computing technologies as a framework for delivering network-enabled decision superiority that create* a capability to achieve and share situational awareness in real-time They show that integrating stream processing and social networking in the value network of collective endeavours enables a new quality of decision making and predicts a path to the anticipated

next era of decision superiority. In the following paper, *Information and Knowledge Management in C2 Systems – The gap between theory and practice is not all that big* by J.M. Kaster and B. Kuhbier, the authors discuss the challenges of information and knowledge management implementation within the transformation process of the German Armed Forces leading to improved Command and Control (C2) systems' design. They show that *consistent coupling of knowledge and workflow management can significantly contribute to meeting the* military requirements. The fourth paper in this group entitled *Security and QoS Policy-Based Management for Federation of Systems delivered* by R. Piotrowski, D. Duda and J. E. Śliwa, deals with a joint security and quality-of-service (QoS) policy management issues. It describes the network management system, based on the XACML architecture with elements responsible for QoS provision, that was elaborated within a framework of research project "ISyD". An emphasis is put on joined policy and management functions, facilitating their dynamic modification according to operational situation changes. The next paper, *Using BML and Advanced Text Analytics for Natural Language Text-based Information to Support Information Fusion* by K. Rein and M. Donovang-Kulisch, is focused on coping with the flood of information pouring in from a large variety of sources, including open sources of information such as websites, blogs or electronic newspapers. The authors describe how information from diverse sources and in different languages may be converted to a standard format in Battle Management Language in order to facilitate fusion and create a common operational picture. They discuss various tools that are needed in the process of this conversion to allow for rapid processing, thereby winning a distinct informational advantage in the field. The final paper in this section, *Is Speech Technology Ready for Use Now?* by U. Uebler and D. Kolb, deals with the question of meaningful of available speech technology products to the potential users. The authors give an overview of the tasks that speech recognition can solve and discuss the level of usability for each of the tasks.

The third group, composed of four papers, discuss ***semantic interoperability*** questions. The first paper in this section, *Ontological Layers to Support NNEC Semantic Interoperability* by S. Kuehne, deals with the conceptual structures that can be used to enable one C2 system or application to use information generated by another. Sven proposes a framework that introduces a set of layers for organizing ontological content within NATO. Each of these layers represents a specific level of abstraction and corresponds to an organizational level while the ontological content is distributed across the different layers according to a management and review process. The following paper by the same author is entitled *Semantic Interoperability Use Case Demonstrator for Maritime Situational Awareness.* It gives a report on a use case for an MSA-related scenario that combines an automated routine gathering and analysis of information with an operator-driven investigation of vessels. The use case consists of two parts – an automatic information aggregation and enrichment phase for all vessels within an area, and a user-driven investigative

phase that allows a closer inspection of potentially suspect vessels. The paper also describes a functional demonstrator that illustrates how NATO's efforts in the area of semantic interoperability could leverage commercially available technology and services to develop functional, semantically-enabled applications that use heterogeneous information sources. The next paper in this group, *Semantic Web Service Discovery and Information Fusion Using OWL-S and SPARQL Formal Specifications over NATO JC3IEDM and TIDE Services* by D. Nogalski and M. Chmielewski, discuss the question of automatically discovering and consuming available information sources to achieve information superiority in an area of conflict. The information sources could differ from each other in terms of technology, protocols, data formats and specially semantics: legacy databases, standalone applications, web applications etc. As soon as they are connected to the network they can be automatically interrogated by agents to extract the required information. The authors demonstrate the results of the ontology design allowing the services offered by the legacy systems and provided by NEC-based systems to collaborate in order to achieve information superiority. The last paper in this group, *Mobile Semantic Explorer: a software tool for finding ontology-annotated resources* by M. Rój, R. Dawidziuk, P. Cieślak, depicts a Semantic Resource Explorer (SRE), which allows easy inquiry, search and browsing of resources – such as software components, data elements or services. The authors assume that the resources are annotated with ontology--based descriptions. They describe features of the SRE and illustrate how it can be used in practical situations. Some applications of the tool to query for and browse ontology-described services are also discussed in the paper.

Web services provision in disadvantaged grids issues constitute the theme of the next group of four papers. T. Hafsøe, F.T. Johnsen and M. Rustad in the paper on *Automated QoS-aware Service Selection and Orchestration in Disadvantaged Grids* discuss the question how Web services technology can be extended with the necessary QoS support by leveraging semantic technologies. They show that use of a decentralized service discovery mechanism enables a robust means of discovering Web services and the associated QoS metadata. The paper describes a novel two-step algorithm for QoS-aware semantic matchmaking, which allows automated service selection and orchestration based on QoS criteria. The following paper in this group, *Efficiency of Compression and Binary Encoding of SOAP Messages in Disadvantaged Networks* by T. Podlasek, J.E. Śliwa and M. Amanowicz, describes the comparison of compression techniques, which increase SOAP efficiency in a disadvantaged environment. The authors present the functionality of three mechanisms – Gzip compression algorithm, Fast Infoset and Efficient XML Interchange encodings. Particular attention is paid to the EXI standard that gives satisfactory results when compared to the other two. The authors describe the results of experiments that were carried out in experimental environment with test implementations and include a brief description of services used for testing, as well as the architecture and configuration of the test bed. The third paper entitled

Adaptation Framework for Web Services Provision in Tactical Environment contributed by J.E. Śliwa, M. Amanowicz and K. Gleba, presents the concept of an adaptation framework for web services provision in a disadvantaged environment. It is focused on presenting general assumptions and functionality of the proxy with emphasis on semantic description of the context of the service call and SWRL rules that are used to make appropriate decisions in terms of adaptation. The proxy can make SOAP message content modifications and decide which protocol to use to send the prepared message. The goal of these modifications is to limit the size of messages sent in the disadvantaged network, thus minimizing the delay related to the transmission process. Additionally the proxy offers store and forward capabilities that allow storing the message until it is received by the user (or the timeliness limit is exceeded). The authors demonstrate that the use of dynamic adaptation framework improves information sharing possibilities in a federated tactical environment. The final paper in this section, *A Concept of Video Service Realization in Disadvantaged SOA Environment* by P. Caban and J.E. Śliwa, depicts the results of a study on the influence of network degradation on provisioning of the video streaming service. Video streaming is implemented as a web service with an interface that enables requests for a particular video source with the required video quality defined by its resolution and frame rate. In response, the service returns a link as a URL address, where the requested service is accessible. The result of technical experiments are discussed in the paper and some practical recommendations for the video streaming service implementation in a tactical environment are also presented.

The first of eleven papers in the **information assurance and security** group is entitled *Risk-aware Approach to Network Configuration for Policy Compliance* and is contributed by K. Wrona, G. Hallingstad and S. Oudkerk. The authors depict a prototype system implementation that addresses cyber defence in a Protected Core Networking environment by analysing current risks and then reconfiguring the network to re-establish an acceptable level of risk. This is done through the collection of sensor data, the analysis of this data with respect to risk, simulation of possible reconfiguration in order to find the best response, and finally reconfiguring the network using a policy-based network management approach. The next paper, *Information Assurance in Coalition Mission Environment* by L. Apiecionek, M. Woźniak, M. Romantowski and W. Znaniecki, describes an architecture for an Information Exchange Gateway that provides two-way, automatic exchange and protection of information. The implementation aspects of the Network Guard service that supports co-sharing of information and data at all the levels and is based on accredited security procedures is also discussed in the paper. Further, the paper describes how the Guard provides and manages protection (high/low level of security or not categorized) of information between different enclaves. The third paper in the group, *Ontology of Threats and Vulnerabilities in Heterogeneous Networks in the Context of NNEC* by K. Samp, W. Hołubowicz, M. Choraś and R. Renk, deals with the security challenges in networked systems. The authors

define a security ontology representing vulnerabilities and threats of heterogeneous networks with particular focus on the NATO NEC concept. Two applications of the security ontology are discussed in the paper; i.e., intrusion detection based on Complex Event Processing and Network Security Assessment Tool for security evaluation and risk assessment. The following paper, *Enhancing Response Selection in Impact Estimation Approaches* contributed by G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke and E. Tyugu, presents a methodology and prototypical implementation for dynamically modifying the weighting of metrics for evaluating the effects of pre-defined countermeasures against computer network attacks. Instead of a fixed linear combination of metrics the authors introduce Pareto optimal combinations of the individual metrics and the combined cost measure. This allows a more flexible way of emphasizing the importance of individual metrics in different situations. The first results of the methodology implementation in a simulation environment are also presented and discussed. The fifth paper in this section submitted by P. Bereziński, M. Małowidzki, T. Dalecki and M. Mazur is entitled *Automatic Configuration of Windows Security with Security Templates*. The authors discuss the automatic configuration of the operating system security that is based on security templates and associated system tools. They discuss the differences and security settings of some available templates, and identify areas where those templates could be improved, yielding a more secure system configuration. The following paper, *The Analysis of Influence of Different Factors for Cryptographic Data Management System Efficiency* by T. Czajka and M. Gawroński, deals with the efficiency issues of cryptographic key management systems. The authors present the guiding principles for development of Electronic Cryptographic Data Management Systems (ECDMS) and point out the difficulties connected with designing of new systems. An analysis of different factors like: number of cryptographic devices, profile of data protection systems, throughput of the random number generator, etc., that influence the efficiency of electronic key management systems is also discussed in the paper. The next contribution, *A Multi-core AES Cryptoprocessor for Multi-channel SDR* by M. Grand, L. Bossuet, G. Gogniat, B. Le Gal and D. Dallet, presents a multi-core architecture for cryptographic processors that meet the security needs of modern military communication systems. The architecture is especially designed for use in multi-channel Software Defined Radio devices. It provides support for GCM, CCM, CTR and other block cipher modes applied to the AES algorithm. The results of tests of the architecture implementation presented in the paper show that it provides a good trade-off between flexibility, performances and resource consumption. The eight paper in this group, *Designing Authenticated Encryption Modes of Operation* by R. Gliwa and W. Oszywa, is focused on authenticated encryption modes, which simultaneously provide both privacy and authenticity of the message. The authors introduce two kinds of authenticated encryption modes: single-pass modes and two-pass combined modes. They also consider a few most important properties; i.e., error propagation, synchronization, parallelizability, keying material

requirements and pre-processing capability. They discuss the pros and cons of using Cipher Block Chaining and Counter encryption modes of operation and provide recommendations on how these modes should be applied to a message in order to achieve the authenticated encryption. The following paper entitled *The Cube Attack in the Algebraic Cryptoanalisys of CTC* contributed by P. Mroczkowski and J. Szmidt, deals with an algebraic cryptanalysis methodology. The authors applied the cube attack combined with the *meet-in-the-middle* principle to a reduced variant of Courtois Toy Cipher 2 (CTC2) consisting of five rounds and 255-bit key. The experimental results of recovering the key are also presented and discussed in the paper. The next contribution in this section *Emission Security of Laser Printers* by A. Przybysz and K. Grzesiak, presents some results of experiments aimed at the examination of compromising emanations of laser printers, which include the electric field strength measurement and the reconstruction of printed images. The authors provide some practical solution that allow to minimize the probability of the electromagnetic leakage of information. The eleventh and last paper in this group, *The New Biological Models of Security in Communications Networks based on Artificial Immune Systems* contributed by A. Pawlak, deals with a question of the development and implementation of artificial immune system design for secure communications. The author depicts the essence of artificial immune system and discusses some of its potential uses. The simulation results of the system modelling are also shown in the paper.

The next group of seven papers discuss ***CIS simulation and technology demonstration*** issues. The first paper in this section, *Aggregation of Simulation Networks and Tactical Communication Systems in the Global Simulation Federation* by V. Andrassy, P. Nečas and I. Petz, deals with aggregation of existing simulation systems and Command and Control (C2) assets. The authors discuss the benefits of such an approach and conclude that it becomes an indispensable tool for planning, preparation and training for deployment of well equipped and well trained coalition troops. A. Sikora and E. Niewiadomska-Szynkiewicz in their paper on *Ad hoc Networks Simulator for Rescue Mission Planning* investigate issues concerning ad-hoc network modelling and simulation. They present a software platform for parallel and distributed simulation, and computer-aided design of reliable networks that can be used in rescue as well as military actions. The paper describes the design, performance and potential applications of this tool as well as presents the results of its application to rescue mission planning. The third paper in this group, *Preparation of Terrain Data for the Needs of Multi-resolution Battle Space Simulation System* by T. Tarnawski, J. Koszela, M. Mańko, M. Niedziela and H. Ostap, deals with preparing geographic data for a multi-resolution battlefield simulation system. In such a system, several different simulators are federated together. One of important issues in ensuring that all simulators operate on the same state of the battlefield is the preparation of consistent digital terrain data in formats appropriate for each simulator – as it is rarely the case that a simulator is able to utilize a standard GIS

format. In a specific case described in the paper, special purpose terrain data files were prepared for the use with simulation systems VBS2 and SSWSO Złocień, while the base data came from widely accepted military standards, i.e.: VPF and DTED. The following paper, *Lesson Learned from Information Assurance and Delivery in the Project "Multinational Interagency Situational Awareness – Extended Maritime"* by B. Jasiul, P. Olofsson, J.E. Śliwa, M. Sjoblom, R. Goniacz and R. Piotrowski, presents an architecture that provides mechanisms for secure exchange of information in a Web-based SOA environment. The authors introduce a mechanism for cross--domain authentication and authorization based on SAML assertion and discuss the results of experiments performed within the MISA EM project. The fourth paper in this section is entitled *A VSAT and DCIS Module for Small Footprint Deployments* and is contributed by S. Onganer. The author presents a Command and Control (C2) communications demonstration system using commercial-off--the-shelf (COTS) products. The system consists of an Internet Protocol (IP) based highly Deployable Communications Information System (DCIS) module and its associated Very Small Aperture Antenna Terminal (VSAT) and an anchor station hub terminal. The paper contains a description of the system's design and provides the results of the tests performed within a NATO CIS exercise. The next paper, *Practical Verification of Selected QoS Supporting Implementations for NEC Compliant Networks* by P. Łubkowski, J. Krygier and K. Maślanka, presents a study of selected QoS supporting mechanisms and components elaborated for NEC-compliant network. It describes the concept of the QoS platform introduced by the authors and its major components implemented in a testbedding environment. The main focus of the paper is on empirical verification of the QoS supporting mechanisms, including: QoS-aware applications, SIG proxies, Network Resource Managers and an Admission Control module. The seventh and the last paper in this group entitled *Automatic Localization and Continuous Tracking of Mobile Sound Sources Using Passive Acoustic Radar* is authored by A. Czyżewski and J. Kotus. The authors describe a concept, practical realization and applications of the passive acoustic radar (PAR) for localization and continuous tracking of fixed and mobile sound sources such as: cars, trucks, aircrafts and sources of shooting or explosions. They present and discuss the results of practical examinations of the sensitivity and accuracy of the developed PAR conducted in an anechoic chamber and in typical reverberant conditions. The functionality and acoustic properties of the proposed solution are also shown in the paper.

The first of thirteen papers in the ***tactical and mobile ad-hoc networks*** group is entitled *Middleware for Tactical Military Networks* and is contributed by Ch. Barz, N. Jansen, M. Spielmann and D. Thomas. The authors present an approach to a middleware concept that allows for the coordination of C2IS applications and network protocol layers. Besides passing down the applications' communication and QoS requirements, they follow an extended approach that also provides the applications with well-adjusted information about the network environment that can be used

by the applications to adapt their functionality according to the available communications resources. The discussion is aimed at informing the middleware about application knowledge (e.g. mission information about the planned movement of troops) to enable the middleware to account for this additional information when configuring the network layers. A middleware design that comprises these functionalities is presented and its main interfaces and components are also discussed in the paper. J. Toelle and H. Schmidt in the paper on *Reliable Service Availability using Anycast* consider a question of the use of anycast in tactical networks to reduce traffic consumption by transparently offering local caches. The authors discuss the limitations that have to be taken into account for implementation of an anycast service in practice. As an example for a service that might be offered via anycast they consider the distribution of Certificate Revocation Lists (CRL). The next paper in this group, *The Effective Use of the Peer-to-Peer System within a Tactical Network* by J. Dołowski and M. Amanowicz, presents an idea of using a structured Peer-to-Peer system within a tactical network. They propose some improvements to the standard Chord structure allowing it to use in degraded environment. The authors introduce the Vivaldi algorithm and a cross layer mechanism that supports the node in obtaining essential information about its surroundings. A general approach for evaluating of the concept by computer simulation is also discussed in the paper. The following paper on *Implementation, Validation and Practical Verification of SIP QoS-aware Application for the Federated Tactical Systems* is contributed by P. Łubkowski and D. Duda. They consider the signalling layer as a tool to create a standardized interface to the advanced capabilities of QoS-enabled network based on the IP protocol. The authors adopt this concept for a federation of systems environment and propose the enhancement to the standard Session Initiation Protocol (SIP) allowing explicit signalling of QoS requirements by QoS-aware terminals. They depict a testbeding environment established for the concept verification and validation and discuss the results of performed experiments. The fifth paper in this group, *Verification of Admission Control Implementation in Federated Testbedding Environment* by D. Duda, P. Pyda, A. Stańczak and M. Amanowicz, is focused on Admission Control development issues and presentation of test results of its implementation. The proposed Admission Control implementation constitutes a key module of the QoS IP network. It allows evaluation of the user application's demand for specific QoS parameters and is responsible for checking the availability of network resources necessary to handle a specific request. The authors present and discuss some results of the AC mechanism verification for selected end-user's services. The next paper, *Smart Antennas and MAC Layer Routing in Ad Hoc Networks* by T. Paso and J.-P. Mäkelä, discuss a question of utilizing smart/directional antennas in mobile ad hoc networks. The authors propose a novel medium access control (MAC) layer routing method to utilize smart antennas in tactical time division multiple access (TDMA) based ad-hoc networks to increase the network capacity and improve the quality

of service. They present and discuss the results of performance of the proposed protocol evaluation performed with the OPNET simulator. The following paper in this group, *Performance Enhancement of Wi-Fi Ad-hoc Network for VoIP Support* is contributed by J. Romanik, P. Gajewski and J. Jarmakiewicz. The paper deals with the issue of increasing the quality of VoIP services in military networks. The authors introduce a set of mechanisms intended to improve the network performance, like channel utilization measurement, adaptation of MAC protocol parameters, closed network mode with a Resource Manager and Admission Control. They present and discuss the results of simulation experiments performed using the OMNET simulator which were focused on evaluation of the efficiency of the proposed solution. The next paper, *Distributed TDMA MAC Protocol Design and Implementation for Ad hoc Networks* by H.P. Tuomivaara, presents design, implementation and evaluation of a distributed time division multiple access (TDMA) medium access control (MAC) protocol for wireless ad-hoc networks. The author combines the network wide synchronization algorithm with a straightforward distributed TDMA MAC protocol. He discusses the issues of the distributed TDMA MAC implementation on a wireless open access platform (WARP) and presents the results of the performance evaluation of the proposed solution. The ninth paper in this section, *Integration of MAC Relaying and IP Routing Protocols in Ad-Hoc Networks: Multimetric Approach* contributed by J. Krygier, M. Bednarczyk and K. Maślanka, proposes a novel link quality aware routing protocol for mobile ad-hoc networks (MANETs) resulting in robust delivery and high performance by finding a reliable path with strong links. The results of an evaluation of the efficiency of the protocol using the OPNET simulation are presented and discussed in the paper. The following paper, *Clustering in Mobile Ad-hoc Networks* by R. Fallier, B. Scheers, presents the ongoing research at the Belgian Royal Military Academy in the domain of topology control in mobile ad-hoc and wireless sensor networks. The authors are focused on clustering algorithms and try to answer some questions related to use of the clusters in MANET with many mobile nodes and the influence of speed of the mobile nodes on the network performance. They shortly discuss pros and cons for clustering in MANETs and present several scenarios used for the evaluation of the algorithms. Finally, they present a discussion on the obtained results and specify some implementation criteria for selection of the clustering algorithm. The next paper in this group, *The Algorithm for Distribution of Large-size Data in the Wireless Ad-Hoc Sensor Network* by R.O. Schoeneich, M. Golański and M. Siwko, describes an algorithm for distribution of large-size data in a wireless ad-hoc sensor network (WASN). The algorithm provides replication and large-size data allocation using the concept of decomposition into small pieces and random distribution in the WASN. The authors established a dynamic network partitioning, which implies data replication and partition-tolerant data storage. The paper presents an algorithm, and performance measurements made using low level network metrics, such as total number

of transmitted packets, and high level data availability ratio. The twelfth paper in the group, focused on tactical networks, is entitled *On Mobility Service in the ISDN System* and is contributed by M.I. Śliwka and P. Kaniewski. They discuss the issue of effective relocation of subscribers in a tactical communication network. The authors introduce a mechanism that supports the users' mobility in tactical ISDN network. The paper presents a concept of a subscriber mobility module and its design principles. The final paper in this section, *Controller Area Network based On-board Data Acquisition System on Military Aircraft* by J. Bajer, P. Janu, R. Jalovecky, is aimed at the design of a data acquisition system architecture based on the Controller Area Network (CAN) standard and its optimization for use on a military aircraft. The authors present a design and implementation of the system. The paper shows some problems that arise from the CAN implementation and describe a brand new method of network communication management. The paper also contains the results of technical verification of the system.

Software defined and cognitive radio issues constitutes the theme of the next group of four papers. The first paper in this group is entitled *Universal Frequency Domain Baseband Receiver Structure for Future Military Software Defined Radios* and was authored by H.T. Saarnisaari. The paper deals with the design issues of implementation of several waveforms in software defined radio. The author describes a universal frequency domain baseband receiver structure, which simplifies the design process. The paper explains how the structure should be used for multicarrier and single carrier signal demodulation, fast synchronization even with large carrier frequency offset, channel estimation, interference cancellation and spectrum sensing as well as briefly discusses the possible contents of blocks. The following paper in this group, *Universal Software Radio Peripheral as an Eight Channels Receiver and DSP Platform in a Passive Radar* by G. Haza, B. Szlachetko and A. Lewandowski, presents an application of two Universal Software Radio Peripheral (USRP) boards in an eight channel receiver and DSP preprocessing platform for an experimental multistatic passive radar. The authors describe a method to achieve this goal by applying modifications on the FPGA structure and the software driver. They present and discuss some results of signal processing for passive radar using the proposed eight channel receiver. The next paper, *Dynamic Spectrum Management for Military Wireless Networks* by M. Suchański and P. Gajewski, deals with the efficiency issues of spectrum allocation during mission planning and supervision. The paper depicts two types of architectures: Coalition Joint Spectrum Management Planning Tool (CJSMPT) applied for legacy systems, and Dynamic Intelligent Management of Spectrum for Ubiquitous Mobile-access Network (DIMSUMNet) applied for modernized equipments. The authors describe a general concept of cognitive radio (CR) as well as some standardization works on opportunistic spectrum access (OSA). They also discuss the challenges of realization of OSA based cognitive radios. The final paper in this section is entitled *Cognitive Techniques for Finding Spectrum for Public Safety Services* and is authored by T. Braysy, J. Lehtomäki, B. Calvet, S. Delmas and Ch. Moy.

The paper presents possible alternatives to enhance public safety and security (PSS) communication network capabilities by implementing dynamic spectrum access. The authors consider a set of techniques introduced in the cognitive radio domain and evaluate their potential value in the PSS context. The matter is discussed from the point-of-view of European Commission Security initiative funded Euler project, where a WiMAX based interoperable backbone networking waveform is designed, implemented and demonstrated in SDR platforms.

The final set of eight papers contained in this book discuss some questions related to ***Wireless Communications*** techniques implementation in a military environment. The first paper in this group, *Modulation and Decoding Choices for OFDM Systems in Multipath Fading and Jamming* by S.M. Kiviharju and H. Saarnisaari, investigates an orthogonal frequency division multiplexing (OFDM) system with coherent and non-coherent reception in different multipath fading and jamming environments, in terms of complexity and bit error rate performance. The authors use realistic channel estimation and frequency domain equalizers for the coherent reception and discuss the results of performance evaluation of the considered systems. The next paper, *A Modified Direct-Sequence Spread Spectrum Modulation Scheme for Burst Transmissions* by B. Scheers, V. Le Nir, presents a novel direct--sequence modulation scheme for spread spectrum communication systems defined as the Delay-and-Add-Direct-Sequence (DADS) modulation. The authors study the performance of the DADS technique in Additive White Gaussian Noise (AWGN) and flat Rayleigh channels, as well as the influence of some important parameters in the modulation scheme. The following paper in this section is entitled *New Technologies for UAV Communication* and is contributed by V. Sliusar. The author discusses a question of the UAV-communication channel multiplexing in the case of nonorthogonal frequency-division multiplexing (N-OFDM) and gives some recommendations on implementation of the considered technique. The next paper, *Radio Channels Sounding for Outdoor Urban Environment Using OFDM Signals* by J. Łopatka and R. Bott, deals with some questions raised within the execution of European Defence Agency (EDA) project on Wireless rObust Link for urban Forces operations (WOLF). The paper describes problems related with propagation of radio signals in an urban environment. The authors describe the methodology of channel sounding and discuss the obtained results. The fifth paper in this group entitled *A Stochastic Model of Channel Correlation in MIMO Systems* is contributed by K. Kosmowski and J. Pawelec. The paper presents a simple stochastic model of the MIMO channel for Monte Carlo simulation. This model includes a partial correlation between the paths in the channel. The paper comprises also a comparison with popular channel models (Kronecker, Weichselberger) and the comparison of BER performances and average mutual information obtained for channels generated according to mentioned models. The following paper, *Modeling of Correlation and Fading Phenomena in Multiple Antenna Systems* by J. Pawelec, K. Kosmowski, presents new equations and BER curves obtained

via Monte Carlo simulation for multiple input/output (MISO and MIMO) systems affected by flat but near-to-fast fading and channel cross-correlation. The authors evaluate the system's performance degradation in respect to the idealized state without correlation and fading and justify the existence of an irreducible error zone. The last two papers in this section deal with the multilayer antenna design issues. M. Bugaj and M. Wnuk in the paper entitled *Multilayer Aperture-Coupled Stacked Patch Antenna – Analysis and Measurements* depict a methodology that can be applied for designing of aperture-coupled microstrip antennas. The authors describe the simulation model of the antenna and discuss an impact of its parameters on the antenna's bandwidth. The last paper in this book, *The Analysis of Multilayer Conformal Antenna Operating in X-band* by J. Bugaj and M. Wnuk, is focused on analysis of conformal multilayer antenna in cylinder shape with radius (R) working in X-band. The authors present and discuss the empirical results of the impact of the parameter R on the antenna's bandwidth and its radiation pattern.

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 readers will find the papers dealing with the most recent research results in the area of military information and communication systems both useful and interesting.

Marek Amanowicz
Markus Antweiler
Peter Lenk
Andrzej Najgebauer

Practical solution for integration of single soldier equipment with information system at the battlefield

Marek Piotrowski, Robert Palka,
Krzysztof Muchewicz, Pawel Baturo

TELDAT, Kijowska street 44, 85-703 Bydgoszcz, Poland

Abstract: The purpose of this paper is to present the concept and a practical solution for a single war fighter in the modern digitalized battlefield. Dismounted Soldier System JASMINE is a TELDAT solution designed for teams of soldiers cooperating and fighting together in order to fulfil mission objectives. System delivers complete integration of solider, combat suit, equipment and command support system. Furthermore, it provides for a single soldier capabilities of exchanging operational information about location of friendly units, sending and receiving orders, reporting events, facilities, obstacles and so on.

In summary, DSS JASMINE system raises safety of soldiers and allows commanders to gather information and react immediately when situation change during a mission progress.

Keywords: DSS, NNEC, C3IS JASMINE, LCG1, NFFI, MIP, JC3IEDM

1. Introduction

JASMINE System [1] is a network centric platform designed to build networks in IP (Internet Protocol) [2] technology for mobile environment utilized at all levels of command chain. System secures all necessary capabilities for information technology required at stationary command posts, command vehicles, combat vehicles and even single soldiers. JASMINE system is produced in three versions:

- **Shelter** version – deployed in an electromagnetic proof container transported on a vehicle, dedicated for headquarters;
- **Portable** version – dedicated for field stationary command posts located in tents, or trenches, developed temporary for the duration of a mission;
- **Onboard** version – deployed in mobile command vehicles and single soldiers fighting at the tactical level.

JASMINE system architecture is modeled on the concept of NATO Network Enabled Capability (*NNEC*) [3]. NNEC imposed that JASMINE structure and information processing is based on nodes that provide services. These services are consistent with the concept of SOA (*Services Oriented Architecture*)[4], reside

inside software modules and render many functionalities at a user level. As a result, JASMINE system is very flexible, scalable and can be easily adjusted to user needs and requirements regardless of level of command, providing diversity of services at the same time.

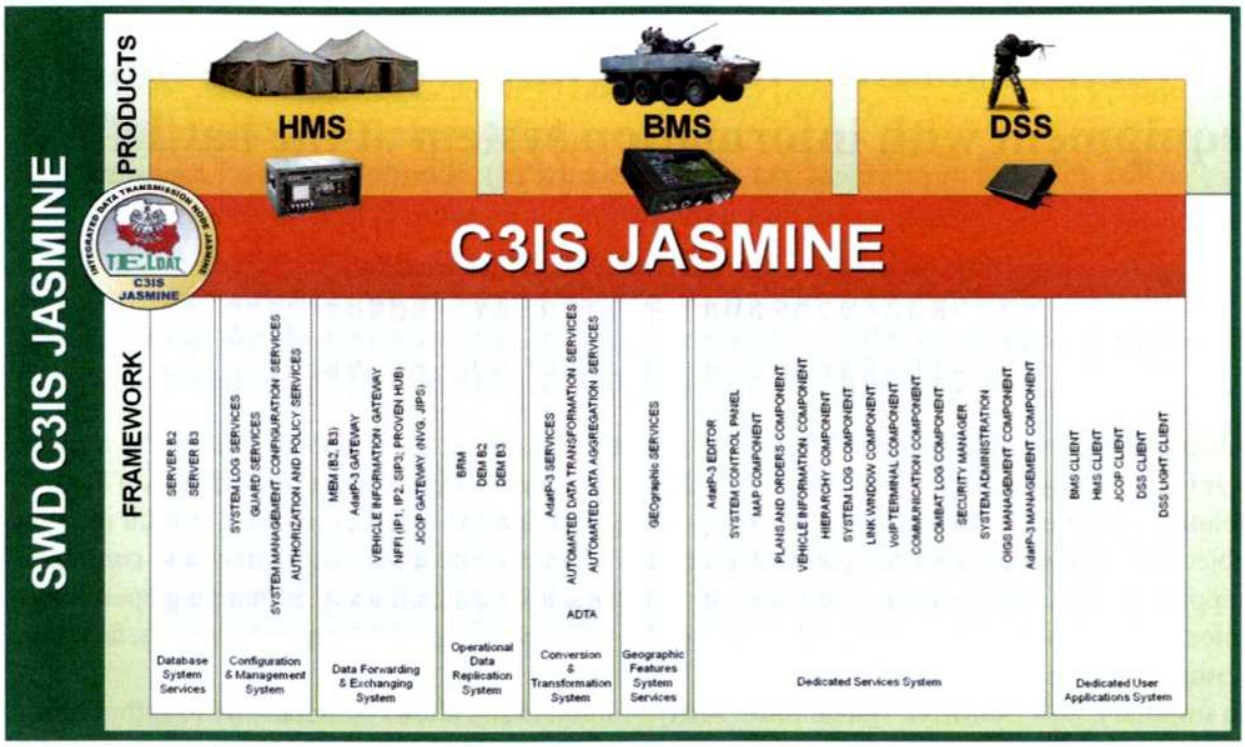

Figure 1. C3IS JASMINE services and dedicated products (© *TELDAT*)

Command Support System C3IS JASMINE consist of three dedicated products based on a C3IS JASMINE framework:

- **Headquarter Management System C3IS JASMINE** – designed to support planning and control of army actions and exchanging information on operational – brigade and upper level.
- **Battlefield Management System C3IS JASMINE** – designed to support planning and control of army actions and exchanging information on tactical level particularly on the armored vehicles.
- **Dismounted Soldier System C3IS JASMINE** – dedicated for a single soldier. This product allows sharing information from the top to bottom and ensures situation awareness on each command level. DSS gives opportunity to take information from reconnaissance direct to commanders.

C3IS JASMINE is based on MIP (*Multilateral Interoperability Program*) [5] database models such as C2IEDM (*Command and Control Information Exchange Data Model*) [6] and JC3IEDM (*Joint Consultation Command and Control Information Exchange Data Model*) [7]. Other services can store and retrieve data from that database which acts as a common interfaces and increases interoperability between different standards and protocols. C3IS JASMINE supports automated

transformation between MIP Block 2 and Block 3, operational data exchange via international standards such as NFFI (*NATO Friendly Force Information*), ADatP-3 (*Allied Data Publication Number 3*) [8], NVG (*NATO Vector Graphic*) [9], and DEM (*MIP Data Exchange Mechanism*). Furthermore, Battlefield Replication Mechanism *(BRM)* is a company protocol capable of replication of MIP compliant data over various means of communication like HF and VHF radios or satellite terminal, copper cable, optic fiber and others.

JASMINE system provides complete solution consisting of hardware and software specially adjusted for every command level.

2. Single Soldier Combat Suit Composition

The Combat Suit of DSS JASMINE system is divided into six subsystems:

- **Data Processing Subsystem** (*DPS*) – a main device of DPS is a Tactical Terminal which is used by DSS C3IS JASMINE to make decision on battlefield is accordance with NNEC concept.
- **Data Manipulation Subsystem** (*IMS*) – allows data input to system by a single soldier. IMS consists of HID manipulator, LCD touch screen and laser aiming device. This subsystem provides easy way for the soldier to manipulate operational information in a hard battlefield environment.
- **Sensors Management Subsystem** (*SMS*) – dedicated to connect various sensors such as LCD (*Light Chemical Detector*), GPS (*Global Positioning System*), inertial navigation and video camera. SMS controls sensors which automatically provide information for soldier system and after processing in DPS disseminates to other soldiers and commanders.
- **Power Management Subsystem** (*PMS*) – supplies power to soldier equipment and provides constant working over six hours on each battery. Soldier can plug two batteries at the same time and exchange battery without need of turning off any devices.
- **Information Presentation Subsystem** – (*IPS*) shows information on various displays such as HMD (*Helmed Mounted Display*) or LCD 6" panel. Soldier uses mainly HMD during an action because this view does not involve his hands and it very easily gives access to manipulate operational data. However, with more comfortable view a soldier can be provided on the LCD panel that usually is used after a mission.
- **Data Distribution Subsystem** *(DDS)* – this is a significant subsystem which allows soldier communicate with commanders and other soldiers. Equipment that is used in SDS is a personal radio with IP *(Internet Protocol)* capabilities.

Figure 2. Example of soldier's combat suit (© *TELDAT*)

All equipments from six subsystems are deployed on one soldier and weight is below two kilograms. Moreover, not every subsystem is necessary to be used at the same time. DSS JASMINE system can be deployed in three variants:

- **First variant** is when we get Tactic Terminal version 4, two manipulators, GPS, power supply, two displays and personal radio like SPEARNET from ITT.
- **Second variant** consist of a Tactical Terminal PDA and a personal radio with GPS included.
- **Third variant** is when soldier carries only a personal radio with GPS included.

These variants can work together and can be mixed in one squad. That approach gives opportunity to reduce cost of equipment and training efforts.

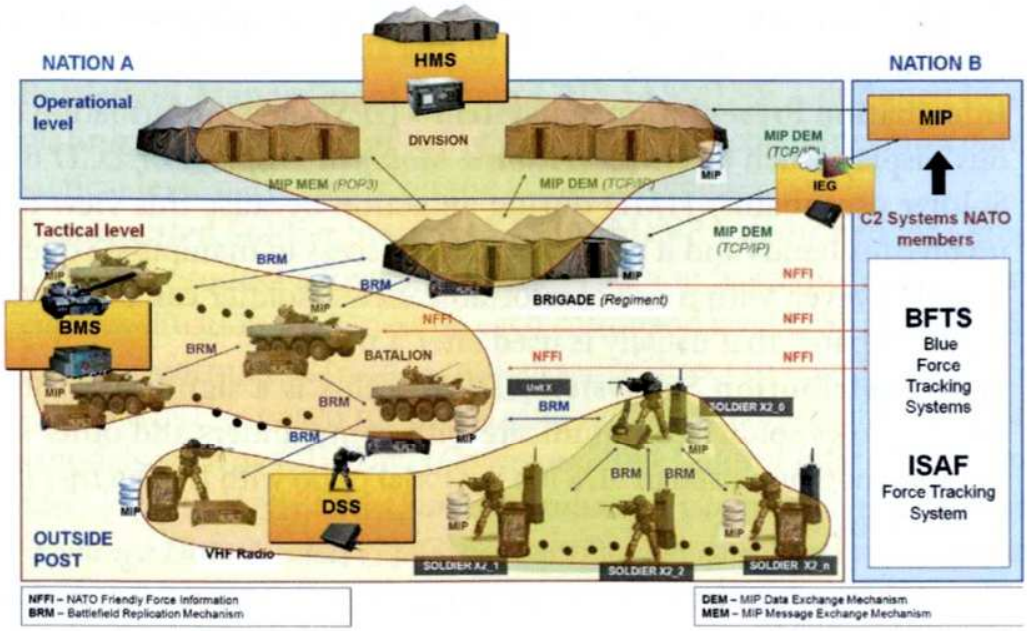

Figure 3. C3IS JASMINE data flow, interoperability and product scopes (© *TELDAT*)

Normally on a battlefield a compliance a dismounted soldier leader carries version 1 while other member of his section are equipped with version 3 and optionally version 2. All soldiers can maintain voice communication during combat mission. Moreover soldiers' leader can monitor subordinates movement, receive orders and report back to superior unit about current mission progress and events. Section members equipped with PDA have similar capabilities but with some limitations.

DSS JASMINE is well prepared to integrate new devices with equipment that already is carried by a soldier. Nowadays main focus is to improve collaboration between combat identification devices in Polish forces.

3. Single Soldier Command Support System

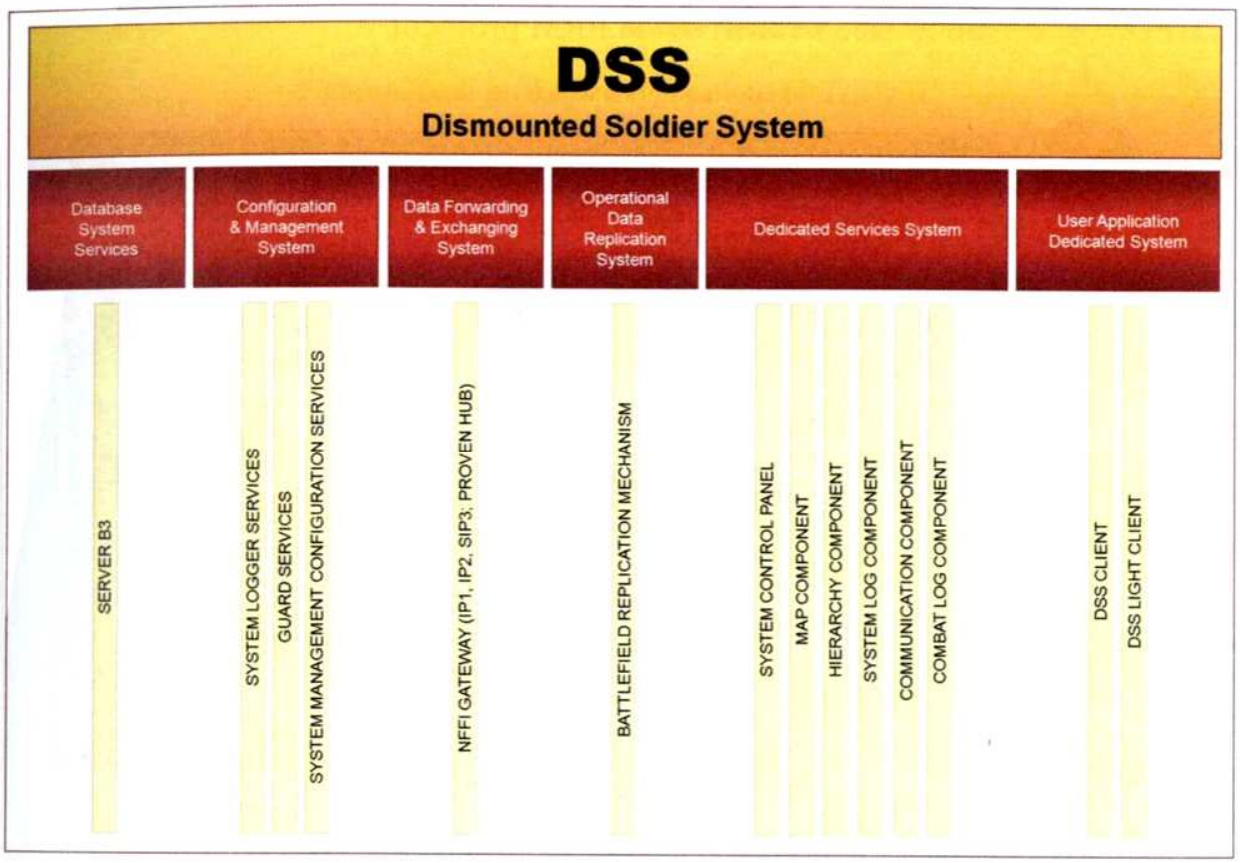

Figure 4. DSS C3IS JASMINE services (© *TELDAT*)

DSS C3IS JASMINE System is a set of software services selected from C3IS JASMINE framework. Main services are listed below:

- Application server SRV.B3 implementing MIP B3 JC3IEDM database model for operational data storage;
- Battlefield Replication Mechanism (BRM) for operational data exchange between data distribution points (command posts, vehicles, soldiers);
- NFFI gateway providing information to and from Friendly Force Tracking Systems;

- DSS Client application dedicated for combat suit tactical terminal;
- DSS Light Client application dedicated for PDA tactical terminal.

Soldier is equipped with a personal radio which provides voice and data communication between crew members.

In order to replicate data using unstable radio means of communication a specialized replication mechanism was invented by TELDAT company. BRM is able to effectively and efficiently exchange JC3IEDM compliant data over a radio communication media. Moreover it provides integration with BMS JASMINE system. Therefore operational data can be shared between armoured vehicles and combat sections.

DSS C3IS JASMINE software system currently supports interoperability with NFFI IP1,IP2 and SIP3 standards. DSS JASMINE system can directly receive FFT tracks from force tracking systems of other nations as long as IP connection is provided. Alternatively, on BMS level data can be transformed from NFFI to JC3IEDM and send to DSS JASMINE via BRM protocol.

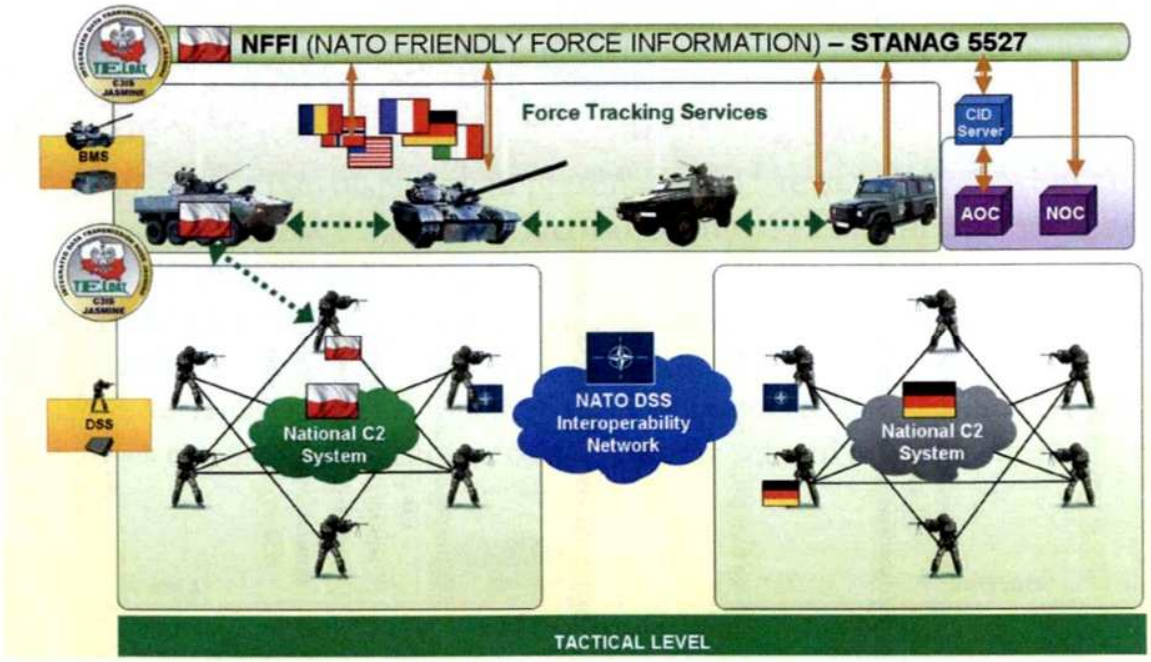

Figure 5. Diagram of DSS system interoperability (© *TELDAT*)

Because C3IS JASMINE framework has a modular construction it is both flexible and extensible at the same time. As a result, once new interoperability standard is developed a new service in C3IS JASMINE framework can be implemented. Therefore, TELDAT is monitoring national and international enterprises in order to support up to date interoperability.

Nowadays, NATO Land Capability Group 1 – Dismounted Soldier introduced JDSSDM (Joint Dismounted Soldier System Data Model) [10] as a subset of JC3IEDM and is currently working on Data Distribution Service. As soon as DDS mechanism is agreed and specified TELDAT is going to provide a service that is able to exchange operational data with NATO DSS systems.

Figure 6. Dedicated client applications (© *TELDAT*)

Dismounted soldier can be equipped with PDA or combat suit tactical terminal. Because of specific terminal technical capabilities two different client application were developed *(DSS Client, DSS Light Client)* in order to satisfy user needs.

Figure 7. DSS Client application screenshot (© *TELDAT*)

Above is presented a screenshot showing current position of friendly units on a battlefield and text messaging between two individuals. On the left side of the

picture one can notice information from Soldier Information Service about state of soldier's equipment.

4. Solution capabilities and functions

DSS JASMINE system was designed to provide following capabilities and functions that are inevitable to secure safety and increase effectiveness of soldiers:

- *ensuring common operational picture on a level of a single soldier;*
  System is able to provide dismounted soldier leader with operational data from higher command level, and present them on the map. Therefore leader is aware of friendly forces such as armored vehicle, own squad members and other squads current locations.
- *automated aggregation of subordinate dismounted soldiers;*
  Location reports regarding all soldiers within a section can be automatically gathered and aggregated at the dismounted soldier leader or superior vehicle level. Afterwards, that information can be send to other units at the adjusted time period making the best usage of radio bandwidth.
- *combat suit constant monitoring;*
  All equipment included in combat suit is constantly being monitored and all information about current state and capabilities are displayed in client application. As a result soldier has all information about its equipment gathered in one place without need to check it manually.
- *providing voice communication;*
  Personal radio provides VoIP communication for section members. They can communicate with each other during combat mission all the time.
- *video transfer;*
  Soldier that are equipped with vide camera mounted on their helmet can transfer life video to other soldiers or commanders in armored vehicles. This service is performed on demand by a receiver.
- *Mission planning;*
  A deployment version number 1 of DSS JASMINE system allows soldier to receive mission plans and orders prepared in accordance with STANAG 2014. Situation is displayed on the screen where, for example, mission objectives, planed actions or location of medical and extraction points are presented.
- *Instant messaging;*
  Dismounted soldier leaders and soldiers equipped with PDA can send and receive text messages. Soldiers can type messages themselves or use predefined ones. Moreover, text reports can be sent to an armoured vehicle and automatically synthesised by onboard communication system on VoIP terminals.
- *Battlefield situation reporting;*
  During combat action soldier carrying tactical terminal can instantly report spotted enemies, obstacles, events etc that are automatically disseminated

to superior commanders for analysis and allows them to perform a suitable action.

5. Summary

Dismounted Soldier System JASMINE is a company solution for a single soldier. This solution is integrated with JASMINE platform *(hardware)* as well as C3IS JASMINE system *(software)*. Furthermore, DSS JASMINE allows to exchange operational information with other systems such as BMS JASMINE and NATO nation tactical systems. Therefore it is not a separate product but a supplement of a Teldat's vision of a digitalized battlefield operations.

Our solution was successfully tested during Coalition Warrior Interoperability Exercises 2010 in the operational scenario. DSS C3IS JASMINE interoperability and adjustment of client application was our main priority to test during the exercise.

Next step for our DSS JASMINE solution is a deployment in real combat situation. Polish Armed Forces are planning to equip soldiers in Afghanistan mission with DSS JASMINE system. Main goal to achieve is to increase safety of polish war fighters. Near real-time knowledge of current units and soldiers position, radio communication and messaging are the most required capabilities to secure this.

REFERENCES

[1] JASMINE system – *Instruction of Exploitation JASMINE System 14 IX 2009*
[2] IP – Internet Protocol – *(http://en.wikipedia.org/wiki/Internet_Protocol)*
[3] Maj. Yavuz Fildis, J. Troy Turner, NATO Network Enabled Capability (NNEC) Data Strategy, 2005
[4] SOA – Sernice-Oriented Architecture – *(http://en.wikipedia.org/wiki/Service-oriented_architecture)*
[5] MIP – Multilateral Interoperability Programme – *(http://www.mip-site.org/)*
[6] Multirateral Interoperability Programme, *The C2 Information Exchange Data Model (C2IEDM Main)*, 2005
[7] STANAG 5525 – *Joint C3 Information Exchange Data Model (JC3IEDM)*
[8] 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
[9] NVG – *http://tide.act.nato.int/mediawiki/index.php/NATO_Vector_Graphics_(NVG)_Data_Format*
[10] LCG1 Relation to MIP & NFFI, M.G. van der Meijden, TNO Defense & Safety, 26-27 XI 2009.

Information assurance in coalition mission environment

Łukasz Apiecionek, Marcin Woźniak,
Michał Romantowski, Wojciech Znaniecki

TELDAT, Kijowska street 44, 85-703 Bydgoszcz, Poland

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 Secuirity policy, Network 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]:

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.

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.

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.

6. Structure of IEG JASMINE

IEG JASMINE is a product of TELDAT company, pursuing NATO directives for building Information Exchange Gateways.

Figure 1. Functional division within IEG JASMINE (© TELDAT)

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.

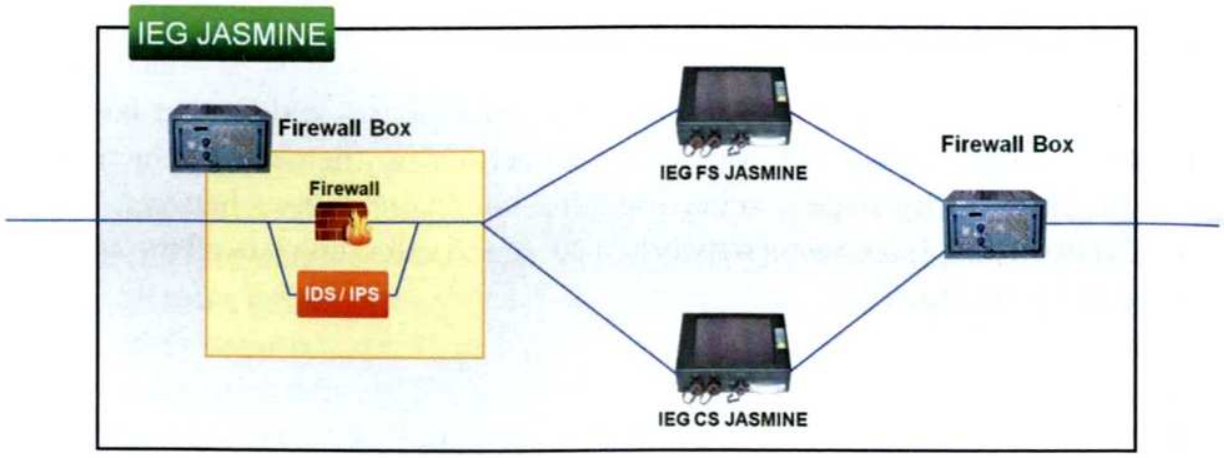

Figure 2. Structure of IEG JASMINE (© TELDAT)

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

Implementation of security policy for functional services in IEG environment consists in creating so called Module (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 Nework 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 Network Guard core and several dedicated modules inside it servicing particular communication protocols. Utilization of Network Guard core service by other services is compliant with SOA paradigms (Service Oriented Architecture). It also allows to assume that if a particular Network Guard module 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 3. Kinds of security labels – developed on the basis of [4] (© TELDAT)

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.

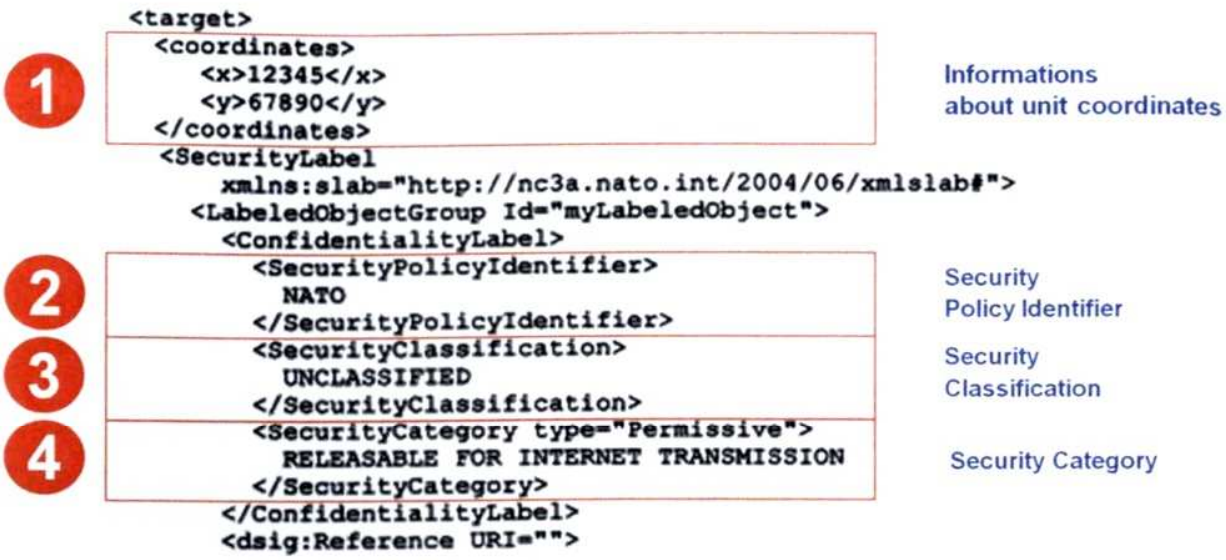

Figure 4. Exemplary labelling of a part of XML document – developed on the basis of [4] (© TELDAT)

7.3. NETWORK GUARD Service

Network Guard (farther reffered to as 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 Guard point of view one network is of high level of security whereas the other of the low one.

The main task of 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 Guard (Access Control Policy). Its worth pointing out that Guard does not prevent from viruses and unwanted data (viruses, Trojan horses).

Confidentiality of transferred information in Network 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 Network Guard may disclose such information, block it or delete from it a piece of unsuitable secrecy degree.

7.4. Scenarios of use supported by NETWORK GUARD

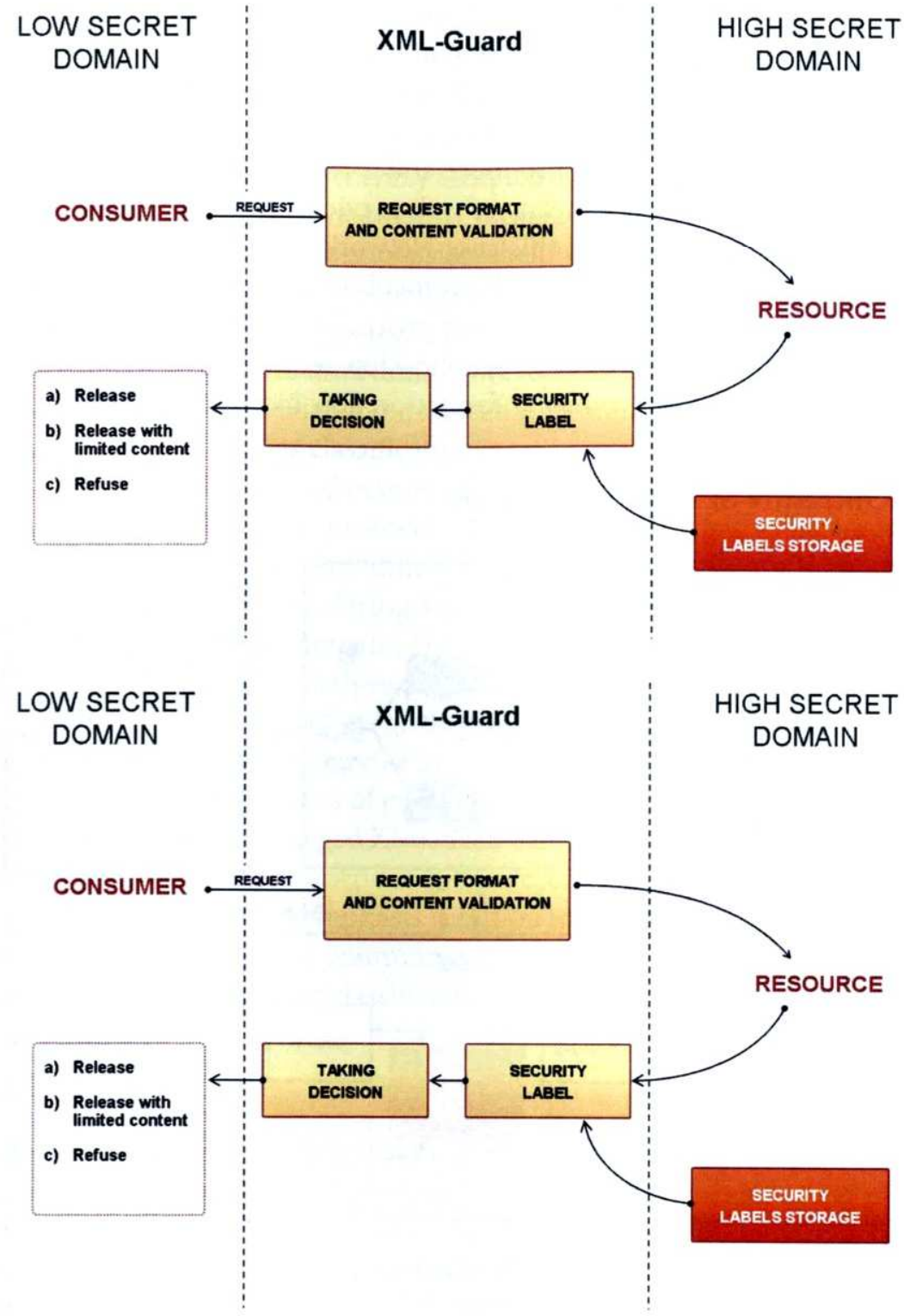

Figure 5. Scenarios supported by XML-GUARD- transfer of documents from a high to a low security level domain and two-way communication using Web Services – developed on the basis of [4] (© TELDAT)

Based on specification, two basic scenarios of use have been determined, as described below [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 Network 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 Guard.

7.5. Architecture of IEG FS JASMINE

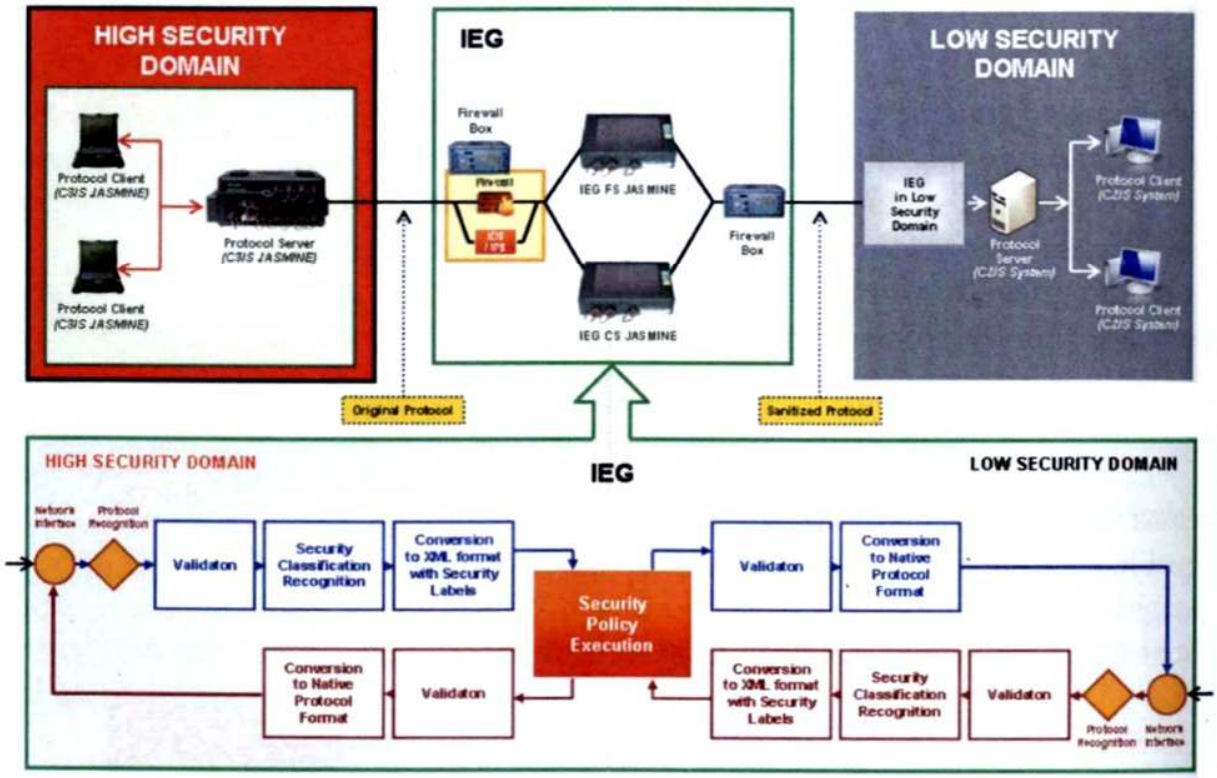

Figure 6. The way of realization of IEG for functional Service – prepared on the basis of [5] (© TELDAT)

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 Network Guard Core (marked as red) 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.

IEG FS JASMINE is placed between the two communicating systems by means of a specific communication protocol. Operation of IEG has to be transparent for both systems but at the same time it should control the flow of messages and decide on their content considering security clause of the enclave it is in. During data transfer from our domain, IEG FS JASMINE intercepts the movement of a particular protocol and analyses it. After that, particular elements are labelled on the basis of data transferred in a given protocol or generally adopted convention and passed to Network Guard service in XML format. Now the content of provided XML data is filtered on the basis of prior labelling and applied security policy. Next step is to create, from the changed XML data, data packet compliant with particular communication protocol and send it to the receiver. The other way the situation is analogical, however more emphasis is put on misappropriation attempt protection by means of a particular communication protocol than receiving unwanted information considering their classification

8. Sumary

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, Network 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 suc-

cessively 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 allow to draw a conclusion that Proxy for NFFI IP1, IP2 and SIP3 is inevitable.

In case of functional services, considering Network 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)).

REFERENCES

[1] MULTI REF "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.

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

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

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

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

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

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

[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)