RUGGEDIZED COMMERCIAL IT MODULES FOR FIELD C2 POSTS IN COALITION OPERATIONS AND EMERGENCIES [1]

Velizar SHALAMANOV and Stoyan AVRAMOV

Abstract: The article describes a set of communications and IT modules that has been successfully tested in a number of emergency management exercises. The modules integrate advanced, commercially available technologies, and may serve as a pool of building blocks in the creation of advanced C4 systems for a variety of multinational, multi-agency operations, e.g. peacekeeping, stabilization operations, post-conflict reconstruction, disaster relief, humanitarian operations, etc. The authors argue that when this concept is combined with a smart approach towards development and management of a common *architecture* of the operation, it leads to cost-effective solutions to a number of interoperability, security and information sharing issues in coalition and emergency operations.

Keywords: Network-Centric Warfare, Combined Operations, Multi-Agency Operations, Multilateral Interoperability, COTS, Advanced Technology Demonstrations, Emergency Management Scenarios, C4ISR Architecture.

‘Network Centric Warfare’ (NCW) is a key concept for the new type of operations not only for the military, but also for the security sector as a whole.[2] Furthermore, this concept may be considered as a platform for integration of the elements of the security sector on operational level, which in turn could lead to integration in many other aspects, for example – in the acquisition of C4ISR systems.[3]

The organizations in the security sector of a country have different missions, tactics, platforms, and culture; these often differ even between the same type of services, but from different countries. However, the establishment of an integrated C2 system for NCW operations requires, among other things, interoperability of the building blocks of C4ISR infrastructure. There is a need for interoperability of modules, as well as interoperability of planning procedures in order to be able to deploy effective C2 systems in coalition military and emergency operations.

The main scenario involves military from different nations, deployed initially for a peace operation, and after certain period that operation is transformed in an operation for support to civil authorities in establishing good governance and critical services (disaster relief, humanitarian support, post conflict reconstruction, etc.). The second phase of this scenario involves not only military, but police, civil protection units, fire brigades, border guards and customs. Foreign military and security services work alongside with newly formed or reformed local security services. Important element of the successful transition is the smooth transition from the coalition C4ISR infrastructure to national security-related infrastructure and national government administration infrastructure to provide good governance of the country.

In such scenario, real time information sharing is critical. The number of players includes the military, local authorities, international organizations, business organizations and NGOs, involved in reconstruction. Active opposition is to be expected; active operations against the process of reconstruction are also possible. Therefore, the C2 system has to be ruggedized, with secure communications and information processing. Certainly, part of the systems will be based on COTS technologies; in some cases only COTS could provide a bridge between different military systems, based on open standards and kind of proxy servers, supporting meta representation of information, negotiated by all players.[4]

Experience in Bulgaria, based on participation in operations in Cambodia, Bosnia, Kosovo, Afghanistan, Iraq, and many exercises (including participation in the multinational exercises ‘Combined Endeavour’ and ‘Cooperative Guard’), as well as SEEBRIG [5] and Civil Protection exercises, leads us to search solution based on “coalition” IT systems. This article outlines a solution based on ruggedized COTS modules to support main information functions and able to access military and commercial communications networks for reach-back and integration trough proxy servers, supporting meta representation of common recognized operational picture and combined with architectural approach for C4 infrastructure planning and real-time management.

The approach proposed is to support further the objectives of the *Multilateral Interoperability Program (MIP)* in the achievement of *international interoperability of Command and Control Information Systems* (C2IS) at all levels from corps to the lowest appropriate level, in order to support *multinational, joint and multi-agency operations* and the advancement of digitization in the international arena, including NATO, by adding COTS dimension, specific for non-military elements and transition from military to civilian infrastructure in on-going and future operations.

Modules for Field C2 Posts in Coalition Operations and Emergencies

Using the experience in command and control and recent architecture development guidance, a Scalable Mobile Emergency Command Post was designed in response to a structured definition of operational, system and technical requirements. It has been tested in laboratory environment, as well as in the field during an international disaster relief exercise.[6]

The proposed C2 architecture may be easily scaled to better fit the requirements of a particular customer due to the integration of advanced commercially available information and communications technologies, standards and interfaces – IEEE 802.11 High Speed Wireless as communication media; TCP/IP with QoS for basic routing in the system; H.323 or SIP VoOIP for voice communications and voice/ video teleconferencing; SNMP for monitoring and management; MPEG for video surveillance, GPS, ASTERIX, NMEA-183 for location, identification and management of moving objects; Ethernet 10/100 Mbps for general purpose communications; POTS/DTMF, ISDN PRI/BRI for phone and fax services; RS-232/422 for connectivity with sensors and local information sources. Software environment can use HTTP, FTP, POP3, SMTP servers and clients; MS WinXP, MS Office and WEB are preferred interface for applications.

The set of modules is intended to provide on-site command and control and communications and information services to users from variety of governmental agencies and non-governmental organizations in a cost-effective manner. It allows for integration within the existing communications and information environment adhering to both applications specific security regulations and general information assurance requirements.

Furthermore, the command post may be embedded in a more complex C2 architecture or to interoperate with communications and information systems of various generations. It provides advanced interfaces to end-user devices, sensors, users of information, and visualization tools. It is designed with sufficient reliability and is ruggedized for high performance under weather and mechanical impacts in the field during various emergencies, operations other than war, etc.

The basic set of modules for the C2 Post includes:

Control Center Wireless Module (CCWM). This is the main communications module in the set. It provides monitoring and management of the whole deployed communications infrastructure. This module provides also all necessary interfaces to other local C2 networks and systems such as phone interfaces, LAN interfaces, ASTERIX converter for radar data exchange, GSM and/or VHF/UHF interfaces for voice and/or GPS data exchange.

Universal Communications Wireless Module (UCWM). This module is the ‘power horse’ of the C2 post. It provides to end users dedicated workplaces with PCs and standard set of interfaces – phone service, teleconferencing capabilities, mobile wireless connectivity.

Access Point Wireless Module (APWM). This module provides the basic communications media for data exchange among all modules in the field. It is based on the IEEE 802.11 high-speed wireless standard and provides 11 Mbps (up to 54 Mbps) connectivity. The use of such COTS standard allows providing connectivity in the serviced area for laptops and PDAs equipped with wireless adapters, too.

Backbone Connection Wireless Module (BCWM). This module provides the necessary connectivity of the C2 Post to the existing national public or government communications infrastructure via several interfaces – digital and analogous dial-up and leased lines; long range RF or Wireless links in ISM or licensed frequency bands. The main communications equipment for the backbone connectivity, however, is supposed to be broadband VSAT terminal. Through the use of commercial VSAT services it is possible to provide not only backbone reach-back but also Internet access, VoIP phone connections, teleconferencing capabilities, etc.

Video Wireless Module (VWM). Providing video surveillance capabilities, this module allows to remotely monitor disaster areas and/or dangerous zones. It is equipped with Hi-resolution TV cameras and stand-alone IP video server. Through implementation of the H.323 standard it is possible to send real time video surveillance information across the system, as well as to the Internet.

Moving Objects Control Module (MOCM). This module is equipped with precise GPS receiver and UHF/VHF transmitter. Using a server-side application on the Control Center Wireless Module, it is possible to monitor in real time the location of ground and airborne moving objects equipped with this module. It is possible to use public operators’ GSM media for data exchange too, thus providing near global coverage for monitoring and control of moving objects.

Practical Scenarios of Testing and Evaluation of the Modules

The modules were tested and evaluated during exercises and experiments in a variety of scenarios. Three of these scenarios are described bellow.

International Civil Protection Exercise

The objectives during this international disaster relief exercise, conducted in the summer of 2003 in Bulgaria under the coordination of the State Agency for Civil Protection of the Republic of Bulgaria, was to test and demonstrate the compatibility and the interoperability of various COTS communications and information technologies and products, as well as the opportunities for scaling of the provided emergency management set. During the exercise we tested the applicability of COTS technologies to meet current and future requirements of governmental organizations such as the State Agency for Civil Protection, to fit in their concepts of operations and to provide interoperability with legacy systems and equipment.

The deployed C2 post included one Control Center Wireless Module (CCWM), one Universal Communication Wireless Modules (UCWM), one Access Point Wireless Module (APWM) and one Video Wireless Module (VWM). In this environment the deployed communications infrastructure was able to provide the command post and two emergency responder's posts with an extensive set of communication services – high-speed data exchange for e-mail and file transfers; phone connectivity between all users; voice and video conferencing capabilities; high-resolution real time video surveillance capabilities.

The demonstration proved the cost-effectiveness of this approach to providing communications and information services in all phases of emergency management. One side effect was the display of possibilities to integrate products of a number of technology leaders, legacy and advanced systems into a complex emergency management system.

Distribution of Recognized Air Picture

The role of aviation in crisis management is becoming more eminent. It is important, though, to have in the field reliable information on the aviation activities in the emergency area. Currently, this information is available to civil ATC[7] authorities and to the military in their stationary control centers. One important task solved with the proposed set of modules is the provision of capabilities to receive, distribute and represent a recognized air picture. The information can be received from either the civil ATC system or from the Air Force systems (such as ASOC[8]) using the standard ASTERIX protocol for radar data exchange. Converting this data to IP it is possible to distribute the information across the emergency management network. Such ASTERIX to IP converter is provided in the Control Center Wireless Module (CCWM). The functionalities of this module were demonstrated during several test and evaluations, including the NATO/Partnership for Peace exercise *Cooperative Key'2003*. The converted recognized air picture information was delivered to each Universal Communication Wireless Module (UCWM), where it was displayed in real time using COTS software.

Links to Military Field C2 System

Currently, the only modern military tactical communications system in the Land Forces of Bulgaria is the Field Integrated Communication Information System

(FICIS). Therefore, it is very important to demonstrate the interoperability between FICIS and other systems. Our plans are to test the interoperability of FICIS with COTS systems and to provide extended set of communications services to and from FICIS. The use of a full set of modules is expected to provide:

- Two way phone service with a common numbering plan;
- Internet service to FICIS users;
- Voice and video teleconferencing services;
- Using FICIS communications media as a backup;
- Distributing real time recognized air picture to the FICIS users;
- Control of moving objects equipped with Moving Objects Control Module (MOCM) from FICIS users.

In this scenario the research team, jointly with representatives from the Land Forces, the developer of the system and other potential customers, shall be able to define possible issues, requirements for further development, concept experimentation and technology demonstrations.

Architectural Approach to Planning C2 Systems Utilizing the Set of Ruggedized Modules

The existence of a pool of ruggedized, tested and certified modules is only part of the issue of supporting network centric operations in coalition environment.

There is a need to improve the process of life-cycle management of C4 systems in the security sector, with focus on guaranteed interoperability, increased resource efficiency, and security in coalition environment. To provide compatibility of process management, the research team adhered to architecture oriented planning and the related standardization on the design and implementation of C4ISR systems.[9] A comprehensive methodology was developed, based on practical requirements to the planning of C4 for combined, joint and multi-agency crisis management operations. The main idea is to use knowledge-based design of modular systems, as well as planning and system management of respective configurations in crisis management operations in real time.

The implementation of the architectural approach is based on flexible computer aided environment for C4 planning and management, using commonly maintained open architecture definitions.[10] In addition to the set of modules, it is necessary to maintain:

- Commonly agreed architecture definitions;
- Commonly agreed methodology for C4 Planning;
- Environment to support C4 planning based on the above definitions and methodology;

- Tools for real time knowledge-based management of the system in order to reflect changes in the situation;
- Specialists in C4 planning and management with common training, based on common set of certified courses.

Key in building interagency and multinational C4 configurations is the issue of interoperability and security. Formally, the approach is based on several knowledge bases and processes:

- Functional tasks (FT) knowledge base (KB) with related Information Structures (IS) KB, used for definition of network (NW) named Operational Architecture (OA), where OA = NW(FT,IS);
- Information Functions (IF) KB and related Implementation Modules (IM) KB for definition of the System Architecture (SA), where SA=NW(IF,IM);
- Technical/ Software Units (T/SU) KB for synthesis of IM in real Technical Architecture (TA), where TA=NW(IM,TU,SU);
- OA KB for development of specific OA from existing KB for FT and IS (FT/IS – OA KB -> OA);
- SA KB for transforming of specific OA in relevant SA (OA-SA KB ->SA);
- TA KB for transforming of specific SA in relevant TA (SA-TA KB ->TA);
- Configuration Management (CM) KB for interpretation of specific System Plan (SP) of developed OA/SA/TA in the process of real-time management of deployed C4 system or C2IS (SP – CM KB -> C2IS).

There are serious efforts under way to systemize, formalize and standardize FT, IS, IF, IM, TU, SU starting from the operational players involved and ending with the developers of equipment and software. Systemization, formalization and standardization of OA, SA, TA and CM KB constitute a rather more serious challenge and precondition for the development of effective tools to support C4 configuration and network management in coalition environment.

The implementation of the architectural approach also relates to the "system of systems" concept, where different subsystems and sub-networks are integrated through proxy servers, providing such an external view as desired for external users and keeping internal representation of subsystem/ sub-network only for internal use. In this sense, the whole C4 system may be considered as a network of proxy servers, where platforms with sensors or weapons/ impact tools are on the lowest level, while web-based proxy servers, consolidated in clusters, provide (and use) services in specific functional areas.

C4 system management could be performed from a number of sites on the network, according to the security policy and a plan of the critical part of the network (the system), available to an authorized team.

The implementation of the approach also assumes the existence of meta representation of the C4 system and its management, i.e., knowledge about the system itself.[11] On the user level, the C4 system is envisioned as a set of web services, while on the C4 system management level detailed configuration and mapping is performed to provide proper content and services to the appropriate users, according to their profile.

This concept emphasizes the importance of security and translation services in providing proper information sharing in a distributed network environment with specific hierarchy on different nodes. Combining virtual flat networks with vertical hierarchies presents considerable challenges for security and horizontal information sharing.

If there is a division between proprietary systems and COTS systems, it could be organized along lines of vertical and horizontal communication. While vertical communication could be formalized and well planned within a single organization (service), horizontal communication is often arranged on a case-by-case basis; it is rather informal and involves organizations with different equipment and even culture. The proposed set of modules is certainly applicable for vertical communications, but it is driven primarily by the needs of horizontal communications, in particular in ad-hoc coalitions of organizations and nations.

The implementation of the architectural approach requires adequate tools and environment, dedicated education and training, related research, and adequate organization of C4 planning in coalition environment. This area is influenced by operational requirements for new type of capabilities, their networking and C2, on one hand, and by emerging information and information management technologies, on the other. Commercial information technologies that form the common space for horizontal information sharing in coalition environment also form a natural environment for development of the C4 planning disciplines.

Natural way to develop the architectural approach is through joint (public) funding, in a transparent and accountable way, by academic institutions, working closely with functional (operational) experts and the IT industry.

There is another important application of the architectural approach. It can be used to optimize existing systems in an organization, thus its use in system reengineering. In this case, existing systems can be considered as pools of available equipment to be used in an optimal way and, in addition, we optimize the acquisition of additional—

primarily COTS—equipment and software. Hence, the architectural approach is a tool for reengineering and change management, while the success of its implementation depends on the quality of support tools and the level of training of implementation teams.

Conclusions

The new concept of NCW, combined with new types of multinational transition operations, poses serious challenges to the planning and the management of coalition C4ISR infrastructure. COTS information technologies, used to develop a set of mobile modules and proxy servers, provide promising solutions in achieving integration and security of field systems and allow information sharing in coalition operations, even in cases when military and civilian agencies work together in transitions from peacekeeping operations to stabilization operations and post-conflict reconstruction.

The set of modules, described herein, and the architectural approach for C4ISR infrastructure planning and management that draws on our experience in planning and managing IT structures of manned and unmanned space flights, have successfully performed in exercises and advanced technology demonstrations. Extensive future implementation, however, hangs on the success of several more steps:

- Approval of meta representation of a common operational picture;
- Approval of common architecture, standards and procedures for planning and management of dynamic IT infrastructure;
- Training and career paths for IT infrastructure planners.

These could be achieved through common efforts of military and civilian agencies, the IT business and the academic community, led by the network of Chief Information Officers of the organizations, participating in coalition operations. It is possible to use emergency management and civil-military emergency planning (for protection of population and critical infrastructure) as test-bed for development of the concept of integrated and secure "information sharing in coalition environment." The importance for the society facilitates public- private partnerships while, given the diversity of risk and treats, the role of the academic community is indispensable.

The recently established Scientific-Coordination Council—an advisory body to the Standing Committee for Protection of the Population in the Events of Major Natural and Man-Made Disasters under the Council of Ministers—and the framework agreement between Bulgaria's State Agency for Civil Protection and the Center for National Security and Defense Research of the Bulgarian Academy of Sciences establish a solid foundation for implementation of this concept. The success of the implementation may be extended to the whole national security sector, as well as internationally.

Two projects of the Center for National Security and Defense Research—on C2 support modules for emergency management (sponsored by State Agency "Civil Protection" and performed jointly with the Institute for Parallel Processing) and on architectural approach for C4 planning (sponsored by ICT Development Agency in the Ministry of Transport and Communications)—provide good starting point for further development of the presented concept.

Notes:

[1] The work briefly described here has been supported by research contracts with the Standing Committee for Protection of the Population in the Events of Major Natural and Man-Made Disasters to the Council of Ministers (Project NKS 14/2004/ES7) and the Executive Agency for ICT Development Agency at the Ministry of Transport and Communications (project # IRD 13/2004).

[2] In the latter case, the terms 'Network Enabled Operations' and 'Network Enabled Capabilities' are often preferred.

[3] C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. Velizar Shalamanov, "C4ISR Infrastructure – Armed Forces and Industry Modernization Tools," in *Privatization and Restructuring of Defence Industries, with a particular Focus on the Progress Achieved in South Eastern Europe* (Sofia-Brussels, Economic Policy Institute and NATO Economics Directorate, March 2002), 118-135.

[4] David Perme, Mark Whelan, and William P. Loftus, "Achieving Interoperability of Command and Control Systems Using Translation Gateways," *Information & Security: An International Journal* 10 (2003): 97-104, <http://cms.isn.ch/public/docs/doc_545_259_en.pdf> (19 April 2005).

[5] SEEBRIG—the South-East European Brigade—is part of the Multinational Peace Force in South-Eastern Europe, <http://www.seebrig.pims.org/>. This Brigade has units from seven countries. Its headquarters is currently in Costanta, Romania. For details see Todor Tagarev, "Shaping the Security Environment in South-Eastern Europe: Bulgarian Armed Forces and National Security Policy," in *Almost NATO: Partners and Players in Central and Eastern Europe*, ed. Charles Krupnick (Lanham, Md.: Rowman & Littlefield, 2003), 119-155.

[6] Detailed system and technical description of an earlier version is provided by Stoyan Avramov, "Integrating COTS Technologies into a Scalable Mobile Emergency Command Post," *Information & Security: An International Journal* 10 (2003): 87-96, <http://cms.isn.ch/public/docs/doc_544_259_en.pdf> (19 April 2005).

[7] ATC – Air Traffic Control.

[8] ASOC – Air Sovereignty Operations Center.

[9] A short list of official documents used includes: Joint Technical Architecture; Common Operation Environment; *DoD Architecture Framework,* version 1 (Washington, DC: DoD Architecture Framework Working Group, February 2004).

[10] Velizar Shalamanov, *Dissertation on Life Cycle Support of Management Support Information Systems* (Air Defense Radioelectronics School of Higher Education, Institute of Cybernetics, March, 1991) (in Russian).

[11] Velizar Shalamanov, "Environment and Methodology for Development of Intelligent Systems for Complex Situation Assessment and Prediction," in *Proceedings of AFCEA-Europe Prague Seminar* (Prague, Czech Republic, 1992), 31-34.

VELIZAR SHALAMANOV is Senior Research Fellow and Head of the C4 section of the Institute for Parallel Processing of the Bulgarian Academy of Sciences. He is advisor to the President of the Bulgarian Academy of Sciences on security and defense issues and Chairman of "George C. Marshall"-Bulgaria. From November 1998 till July 2001 Dr. Shalamanov was Deputy Minister of Defense, responsible for defense policy and planning. He has more than 150 publications in the areas of CIS architecture and development, information warfare, decision support, national and regional security policy, defense planning and reengineering. Dr. Shalamanov is co-founder of the AFCEA-Sofia Chapter and the Business Executives for National Security – Bulgaria. He serves on the International Advisory Board of DCAF. *E-mail:* Shalamanov@GCMarshall.bg.

STOYAN AVRAMOV is Research Fellow and Head of the C4ISR Laboratory of the Space Research Institute of the Bulgarian Academy of Sciences. He graduated from the Bulgarian Air Force Academy in 1984 with a M.Sc. Degree in Electronics Engineering and Received a Ph.D. degree in Radar Systems and Technologies from the Zhukovsky Air Force Engineering Academy in Moscow, Russia, in 1991. Until 1995, he served in the Bulgarian Air Force in a variety of positions related to the development of automated C2 systems. Dr. Avramov is member of the Editorial Board of *Information & Security: An International Journal*. He specializes in technology integration, system design, prototyping, and advanced technology demonstrations. *E-mail*: stav@digsys.bg.