INTEGRATING COTS TECHNOLOGIES INTO A SCALABLE MOBILE EMERGENCY COMMAND POST

Stoyan AVRAMOV

Introduction

In terms of emergency command and control, the September 11 terrorist attacks against the United States provide a textbook example of the complexity of the task. A number of organizations needed to coordinate their activities while existing infrastructure elements and capabilities were lost. Timely response was critical. The life of first responders was at great risk.

Yet, this type of emergency situations is not necessarily limited to large-scale terrorist attacks. Nor is it limited to the United States. Although September 11 may be seen as extreme in intensity, the resulting emergency is neither unique nor did it pose extreme resource requirements. Earthquakes, floods, landslides, massive forest fires and other natural calamities, as well as man-made disasters may call for greater involvement of disaster relief assets in coordinated response of variety of national and international organizations.

Adequate response requires advance preparation of assets, emergency management plans, related infrastructure, and elaborate training.[1] In countries, transitioning to market economy and effective democratic governance, two additional factors call for adapting national emergency management arrangements [2]:

- Necessity for coordinated response of several organizations of the security sector [3] with (hopefully) complementing capabilities to counter new security threats; and
- Harsh financial restrictions.

These two factors, together with the set of interoperability requirements, call for extensive use of commercial-off-the-shelf (COTS) technologies in emergency command and control. This article describes an ongoing effort in developing and

demonstrating the capabilities of COTS technologies, integrated to provide cost-effective on-site command and control in various emergencies.[4] Using our experience in military command and control and recent architecture development guidance,[5] we designed a Scalable Mobile Emergency Command Post in response to a structured definition of operational, system and technical requirements. The following sections of the paper briefly presents major operational, system, and technical architecture issues, as well as the approach chosen to deal with the problem of information assurance. The proposed C2 architecture may be easily scaled to better fit requirements of a particular customer. It has been tested in laboratory environment and highly acclaimed at technical exhibitions. The concept will be further tested during an international disaster relief exercise, to be conducted in the summer of 2003 in Bulgaria under the coordination of the State Agency for Civil Protection of the Republic of Bulgaria.

One of the objectives is to test and demonstrate compatibility and interoperability of various communications and information COTS technologies and products, as well as opportunities for scaling of the provided emergency management set. During the exercise we shall test 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 demonstration is expected to prove that this is a cost-effective approach to providing basic communications and information services in all phases of emergency command and control, allowing also effective integration within national information and communications systems and infrastructure. One side effect is the display of opportunities to integrate products of a number of technology leaders, legacy and advanced systems into a complex emergency management system.

As a result of the demonstration during the exercise the research team, jointly with representatives of the Civil Protection Agency and other potential customers, shall be able to define requirements for procurement of a tailored mobile emergency management set, further development, concept experimentation and technology demonstrations.

COTS Integration and Demonstration Concept

A number of advanced commercially available communications and information technologies have been integrated in a *Mobile Emergency Management Command Post*. During emergencies it shall provide 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.

The emergency management command post, presented on Figure 1, includes:

- One *System Communications Module* with
  - Dedicated workplace
  - Extended number of interfaces
  - Software for monitoring and diagnostics of system performance
- 3-4 *Basic Communications Modules*, each of them consisting of
  - Dedicated workplace
  - Standard set of interfaces
- 2-3 *Universal Communications Modules* with minimum number of interfaces

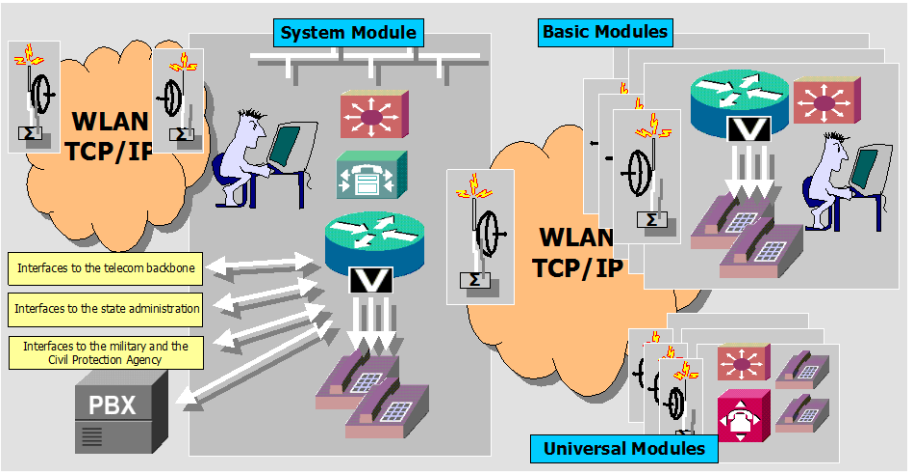

Figure 1: Structure of the mobile emergency command post

Basic Operational Features

This set of the emergency management system is intended to provide on-site command and control. It supports the work of an 'Emergency HQ' with three to five workplaces. It is mobile and may be quickly deployed in the field. Alternatively, the command post may be used in a fixed (stationary) version.

Furthermore, the command post may be embedded in a more complex C3 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 ruggedized for high performance under weather and mechanical impacts in the field during various emergencies, operations other than war, etc.

System Architecture Issues

In mobile emergency management, the command post uses high-speed wireless communications in either ISM or licensed frequency bands. If necessary, it can be connected to the telecommunications backbone using SATCOM and/or VSAT. When the emergency management set is used in stationary conditions, digital and analogous dial-up and leased lines connections may be established. The set provides capabilities for simultaneous work in stationary and mobile communications networks.

System Communications Module

This is the main communications module in the emergency management command post. It provides monitoring and management of the whole communications infrastructure. This module provides also all necessary interfaces to the telecommunications backbone and other networks. One possible configuration of the Systems Communications Module with some of the technical products used is represented on Figure 2. It is also possible to use other commercially available products.

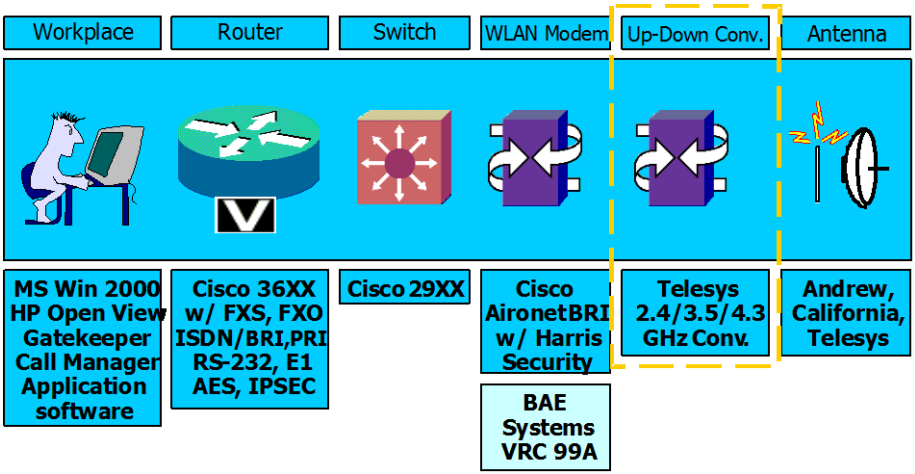

Figure 2: Configuration of the Systems Communications Module

The Systems Communications Module includes

- Workplace – PC with software for management and monitoring the performance of the whole communications infrastructure. It may be additionally used as server for system applications;
- Router – provides the main functions for routing within the system, as well as the main communications interfaces within the system and to other

systems;

- Switch – provides effective network connectivity to other workplaces within the System Module;
- WLAN Radio Modem – This is the main device providing remote communications access with packet switching and routing in the radio environment. It has embedded capabilities to guarantee secure information exchange;
- UP-DOWN Converter – allows the implementation of commercially available tools designed for ISM frequency bands in licensed bands used by the respective agencies. It can provide the necessary power levels;
- Antenna - provides antennae systems with directional or omnidirectional pattern in the respective frequency band.

A typical number and type of communications interfaces required in the field are listed in the Table 1:

Table 1. Interfaces in the System Communications Module

Type	Number
For local workplaces and interfacing local systems	
Ethernet 10/100 Mbps	8
For local users of telephone services	
POTS/DTMF FXS	4
For local or remote interface to PSTN or PBX	
POTS/DTMF FXO	4
ISDN/BRI	2
ISDN/PRI (w/ voice)	1 (optional)
For remote access to the telecommunications backbone	
V.35 / 2 Mbps	1
For interfacing the military and other governmental agencies	
V.35 / 2 Mbps	1 (optional)
ISDN/PRI (w/ voice)	1 (optional)
POTS/DTMF FXO	2
POTS/DTMF FXS	2
Ethernet 10/100 Mbps	2
For interfacing Air Traffic Control Authorities and the Air Force	
V.35 (w/ ASTERIX-IP converter)	2

Basic Communications Module

The basic communications module in the emergency management set provides a workplace for the users in the system—the emergency responders—and the basic communications interfaces to the local systems. One possible configuration of this module with the implemented technical devices is presented on Figure 3.

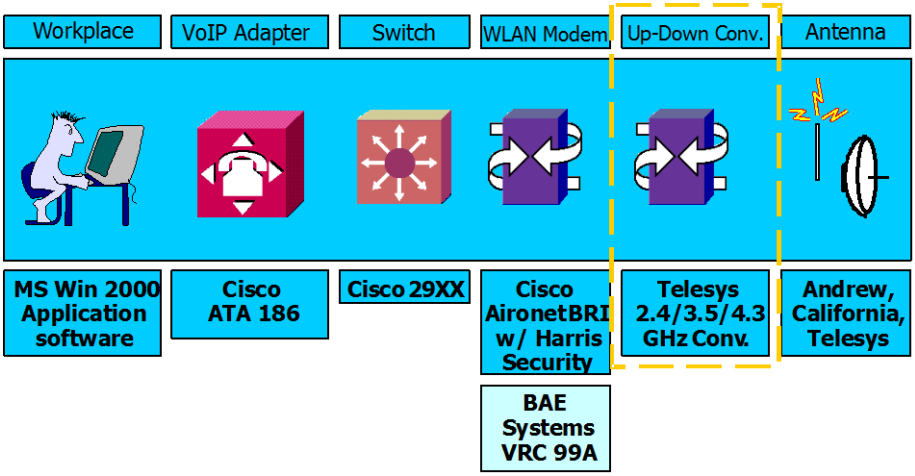

Figure 3: Configuration of the Basic Communications Module.

The module includes:

- Workplace – PC with user-oriented software applications;
- VoIP adapter providing the necessary voice communications;
- Switch providing effective network environment for other workplaces in the basic module;
- WLAN Radio Modem – This is the main device providing remote communications access with packet switching and routing in the radio environment. It has embedded capabilities to guarantee secure information exchange;
- UP-DOWN Converter – allows the implementation of commercially available tools designed for ISM frequency bands in licensed bands used by the respective agencies. It can provide the necessary power levels;
- Antenna - provides antennae systems with directional or omnidirectional pattern in the respective frequency band.

The following types and number of interfaces are required for implementation in field conditions:

- 8 Ethernet 10/100 Mbps interfaces for local workplaces and interfacing the local systems;
- 2 POTS/DTMF FXS interfaces for local users of telephone services.

Universal Communications Module

The universal communications module in the emergency management set provides the minimum number of services to single users in the system and the interface to a few local workplaces. A possible configuration of the universal module is presented on Figure 4. The figure also lists possible technical devices.

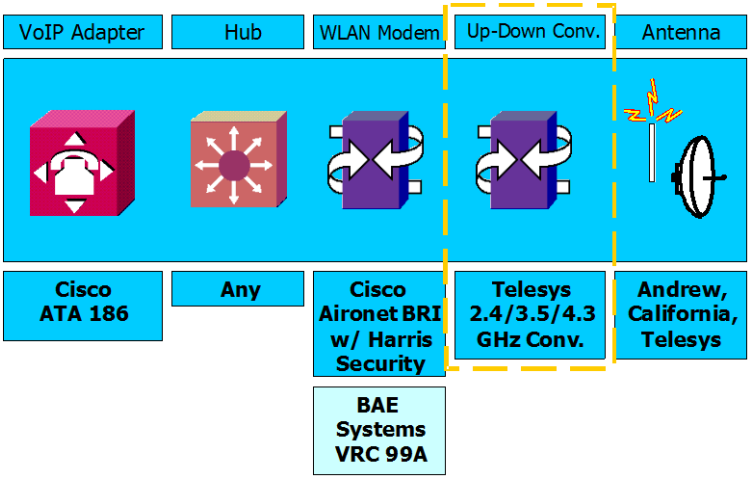

Figure 4: Configuration of the Universal Communications Module.

The module includes:

- VoIP adapter providing the necessary voice communications;
- Switch or HUB to provide effective network environment for other workplaces within the universal module;
- WLAN Radio Modem – This is the main device providing remote communications access with packet switching and routing in the radio environment. It has embedded capabilities to guarantee secure information exchange;
- UP-DOWN Converter – allows the implementation of commercially available tools designed for ISM frequency bands in licensed bands used by the respective agencies. It can provide the necessary power levels;

The following types and number of interfaces are required for implementation of universal modules in field conditions:

- 4 Ethernet 10/100 Mbps interfaces for local workplaces and interfacing the local systems;
- 2 POTS/DTMF FXS interfaces for local users of telephone services.

Technical Architecture

In order to standardize the technical devices within the emergency management set and to provide for its efficient and effective scaling, we developed the three types of modules following a set of technical requirements and standards.

Communications protocols and standards

For routing in the system	TCP/IP with QoS, PPP
For voice and voice teleconferencing	H.323, VoIP
For monitoring and management	SNMP
For information assurance	IPSEC, AES, WEP
For video surveillance and video teleconferencing	MPEG
For location, identification and management of moving objects	GPS, ASTERIX, NMEA-183

Communications interfaces

General purpose	Ethernet 10/100 Mbps
For phone and fax services	POTS/DTMF, ISDN BRI
For connectivity with sensors and local information sources	RS-232 / Up to 115 Kbps

Software environment

Servers and protocols	HTTP, FTP, POP3, SMTP
General purpose applications	MS Win2000, XP; MS Office
Preferred interface to applications	WEB based

Information Assurance Issues

Accounting for known security problems in the WLAN technology,[6] the research team is developing additional measures to be applied in specific scenarios, the sensitivity of the information exchange, and the requirements of particular customers. Generally, security in the Mobile Emergency Management Command Post is

provided through cryptographic protection and through implementation of a set of additional software methods and tools for information assurance. The implementation of crypto devices is presented on Figure 5.

Among the additional software tools there can be implemented commercially available tools [7] for :

- Network monitoring & control;
- Intrusion detection;
- INFOSEC control;
- Crypto keys management;
- Call management;
- Voice recording;
- Data logging.

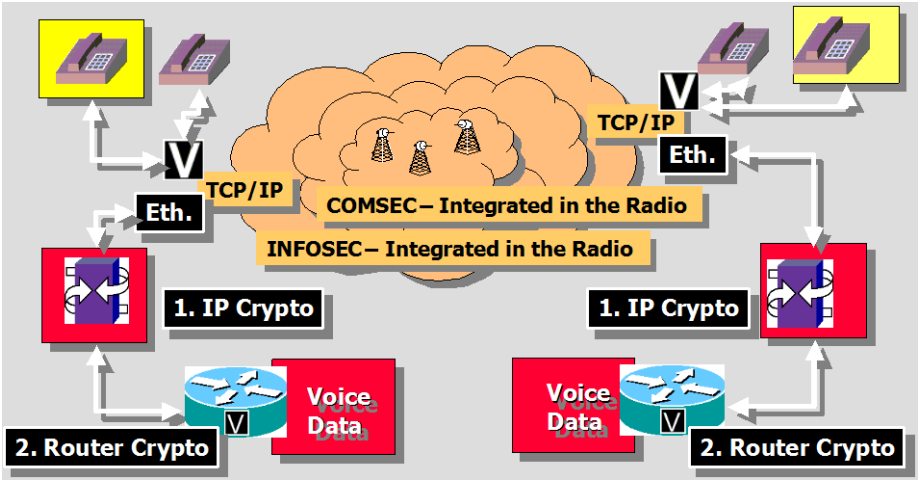

Figure 5: Possible protection of information in the emergency management set.

In sum, there are remaining challenges, i.e., to provide secure information exchange when a number of governmental agencies are involved. Nevertheless, the currently available mobile emergency management set provides adequate, cost-effective solution to the needs of first responders in variety of emergencies. Our efforts were successful through extensive use of advanced commercial-off-the-shelf technologies and systems.

Notes:

[1] Andrew Borden, "Command and Control in Crisis Management," *Information & Security* 10 (2003): 15-23.

[2] Todor Tagarev, "From Military Capabilities to Capabilities of the Security Sector," *Military Journal* 110, 2 (2003): 23-29.

[3] Although not unique for the post-communist countries, this factor is listed here because of the impact of the rapid restructuring of individual organizations and the security sector as a whole. For definition of 'security sector' the reader may refer to the "Report of the Ad Hoc Working Group on Security Sector Reform to the Working Table III" (Budapest: Stability Pact 27 November 2001), <http://www.stabilitypact.org/stabilitypactcgi/catalog/view_file.cgi?prod_id=5664&prop_type=en>.

[4] For an independent parallel development the reader is referred to Robert K. Ackerman, "Mobile Command Center Controls First Responses: Command and communications are no longer a military exclusive," *SIGNAL* 56, 10 (June 2002): 37-40. Related R&D in Europe within the 6th Framework Programme follows several tracks, i.e., in the GMES thematic area to stimulate satellite-based information services by development of sensors, data and information models, and disaster management technologies, <http://fp6.cordis.lu/fp6/home.cfm>.

[5] The Bulgarian Government has not issued elaborated guidance on developing C4ISR architectures. Therefore we currently adhere to *DoD Architecture Framework*, Volumes I, II and III, Version 2.1, First Draft (Washington, DC: DoD Architecture Framework Working Group, October 2000).

[6] *Wireless LAN Security White Paper* (The Wireless LAN Alliance, August 1999), <http://www.wlana.com/resource/whitepaper.html> (20 March 2003); Torben Rune, *Wireless Local Area Networks* (30 September 1998), <http://www.netplan.dk/New/index.asp?ArticleID=2834> (20 March 2003); B. Justin Ross, *Containing the Wireless LAN Security Risk* (Portland, OR: SANS InfoSec Reading Room, 4 November 2000), <http://www.sans.org/rr/wireless/wireless_LAN.php> (23 March 2003).

[7] See also Andrej Lúc, "Analysis of Spread Spectrum System Parameters for Design of Hidden Transmission," *Radioengineering* 4, 2 (June 1995); *Technical Considerations for Converging Data, Voice, and Video Networks*, White Paper (Cisco Systems, 3 July 2000), <http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/tecon_wp.htm> (23 March 2003).

STOYAN AVRAMOV is Head of the C4ISR Laboratory at 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 PhD degree in Radar Systems and Technologies from Zhukovsky Air Force Engineering Academy, Moscow, 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, systems design and prototyping C4ISR systems. *Address for Contacts*: Space Research Institute – Plovdiv Branch, "Ivan Vazov" Str. 50 A, Plovdiv 4000, Bulgaria.
E-mail: stav@digsys.bg.