LAUREA UNIVERSITY OF APPLIED SCIENCES | Together we are stronger |

PLEASE NOTE! THIS IS SELF-ARCHIVED VERSION OF THE ORIGINAL ARTICLE

To cite this Article: Rajamäki, J. (2012) Redundant Multichannel Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations. In Vincenzo Niola, Zoran Bojkovic, M. Isabel Garcia-Planas (Editors) Mathematical Modelling and Simulation in Applied Sciences. 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE '12) April 18-20, 2012, Rovaniemi, Finland, 56-61.

URL: http://www.wseas.us/e-library/conferences/2012/Rovaniemi/INEE/INEE-09.pdf

Laurea University of Applied Sciences
Ratatie 22, 01300 Vantaa, Finland
Phone +358 (0)9 8868 7150
Fax +358 (0)9 8868 7200
firstname.surname@laurea.fi
www.laurea.fi
Business ID 1046216-1
Domicile Vantaa

Redundant Multichannel Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations

JYRI RAJAMÄKI
Laurea SID Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
jyri.rajamaki@laurea.fi http://www.laurea.fi

Abstract: - All Public Protection and Disaster Relief (PPDR) organizations across Europe have multiple similar needs. A common cyber secure voice and data network for PPDR brings synergy and enables interoperability; separate networks are wasting of resources. This paper focuses on future broadband data communication needs of PPDR actors and presents a new fully redundant data communications network structure for Public Safety Communications (PSC). The architecture is decentralized and all critical communication paths have fully redundancy. Although having common physical connections, all network actors and elements (multichannel routers, nodes) are identified as well as every organisation's all user levels and their rights to different data sources are known. The network architecture based on the Distributed Systems intercommunication Protocol (DSiP) is highly fault-tolerant in normal conditions as well as in crises. The software-based approach is independent from different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables to build a practical and timeless cyber-secure data network for PPDR environment, which being fully decentralized is hard to injure. The networks of different organizations are virtually fully separated, but if wanted they can exchange messages and other information which makes them interoperable.

Key-Words: - Cyber security, Disaster relief, Distributed Systems intercommunication Protocol, Multi organizational environment, Public protection, Public safety, Public safety communications

1 Introduction

In recent years, the capabilities of Public Protection and Disaster Relief (PPDR) organizations across Europe have been considerably improved with the deployment of new technologies including dedicated TETRA and TETRAPOL networks. Nevertheless, a number of events like the London bombing of 7th July 2005, the Schiphol airport disaster and the flooding disasters in 2010 and 2011 have highlighted a number of challenges that PPDR organizations face in their day-to-day work. Secure and reliable wireless communication between first responders and between first responders and their Emergency Control Centre is vital for the successful handling of any emergency situation, whichever service (Police, Fire, Medical or Civil Protection) is involved.

Security organisations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organisations. Not only assets and standards must be shared across Europe to empower joint responses to threats and crisis in an increasingly interconnected network, but also security organisations have to benefit from interoperability functionality in their day-to-day work.

On the one hand Europe is a patchwork of languages, laws, diverse cultures and habits that can change abruptly across borders. On the other hand, even in a same country, each security organisation develops its own operational procedures. For efficient operations, many significant challenges need to be addressed, including public safety communication systems (not compatible even when they use the same technology), differing procedures as well as inadequate language skills in cross-border co operations. This paper addresses not only the technical security and interoperability issue, but also the complete procedure to build a cyber-secure Public Safety Communication (PSC) system for a multi organisational environment enabling foreign

ISBN: 978-1-61804-086-2

users to cooperate keeping the intrinsic and vital cyber security mechanisms of such networks.

2 Requirements for Public Safety Communication

This chapter identifies the generic requirements for Public Safety Communication (PSC). It addressed specifically the communication requirements that impact first responders.

PPDR field operations are increasingly dependent on ICT systems, especially on wireless and mobile communications. The generic PSC requirements are essentially the need for secure, bi-directional wireless voice communication, but with certain special features not available from the commercial mobile telecommunication network, such as the flexible formation of talk groups, broadcasting, fast call setup, the capability for team leaders to interrupt conversations, and direct-mode communication for cases where network service is either unavailable or disturbed due to the nature of the disaster. [1]

The TETRA system satisfies a large extent of these requirements, as evidenced by its popularity for PSC in Europe and Asia and recent large sales to police forces in the UK and Germany. The equivalent system in the US is Project 25. Details of the TETRA services can be summarised as [2]:

- Secure communications: not only to protect any personal data, but also to prevent eavesdropping or malicious intervention. This is provided through the use of private frequencies and end-to-end encryption
- Creation of teams (group call) and control hierarchy
- Prioritisation (emergency call)
- Broadcasting (e.g. evacuation signal)
- Fast call setup (Push-To-Talk)
- Direct mode communication (no base station)
- Open channel
- Listen-in
- Access to the public network
- Short Data Service

However, today's immediate missing requirement is interoperability, not only between different services, but also within the same service if different systems are in operation between regions. This situation has arisen due to the fact that the different emergency services in each region, in each country had historically much autonomy in the way they developed their networks and the terminal devices they purchased. [2]

Regarding the next generation of services for first responders, the ETSI MESA [3] has examined what would be possible if wireless broadband capacity was available; i.e. if some of the technologies that have revolutionised the commercial transport of information (both wired and wireless) in recent years were applied in the PSC market. From the full list from [3], the ones selected below are considered as being common to all PPDR services:

- Interoperability
- Communication inside buildings
- Improvement in spectrum efficiencies (e.g. reducing channel spacing, using Software Defined Radio, or Cognitive Radio)
- Migration path from existing systems (TETRA, Project 25)
- The ability to remotely partition the network system or bandwidth at a particular site
- Simultaneous access to multiple networks or host computers by a single device, and simultaneous access from multiple user devices to a single host
- Pre-emption: the prioritisation of access and routing and the ability to pre-empt non PPDR users (which implies the use of public or open (non-licensed) networks)
- A transaction and audit trail of the use of the network
- High-speed, error free transmission: at least 1.5 -> 2Mbps, end-to-end transmit time for data <400ms, end-to-end transmit time for voice <150ms (duplex), <250ms (half duplex) and <400ms if over satellite
- Seamless transparent transfer of devices across networks
- Inherent redundancy
- Typical data to be transported is identified as being:
    - Voice
    - Text
    - Detailed graphical information (e.g. maps)
    - Images
    - Video
- Connectivity to local, national and international PPDR databases, and the dynamic updating of database entries from in-vehicle equipment and personal handheld devices
- Remote control of robotic devices

ISBN: 978-1-61804-086-2

- Geographical position-locating capability

Lack of broadband connectivity of wireless communications for existing and future PPDR applications is a real problem [4]. The rationale behind many of the new services for PPDR actors is that having access to more information at the scene of the emergency, rather than having to request and retrieve it from the Emergency Control Centres, will improve the decision-making process at the scene of a crisis. Every first responder does not need a broadband terminal, but the commander of the mobile rescue team at the scene should have the broadband capability inside a fire engine, police car or ambulance. [2]

Some new features can be deployed using the narrowband capabilities of the existing Private Mobile Radio (PMR) spectrum allocated for PSC. Examples are [2]: exploiting the use of sensors in tunnels (or sent into tunnels) to detect temperature, air quality, traffic flow, or built into the clothing of firemen (e.g. location detection, health monitoring), and the electronic tagging of accident victims at the scene and informing the hospital of his/her condition during the ambulance journey. However, such solutions as the visualisation of current traffic congestion on the route to an incident, or enabling remote access to critical information resources such as building plans, satellite photographs, crime databases, etc., depend upon the incorporation of multimedia services that are not feasible over today's PSC networks [2]. For example, descriptions of potential new services from the ETSI MESA group assume bandwidths of at least 1.5 -> 2 Mbps, which would require network infrastructure such as 2.5/3G (EDGE, WCDMA), IEEE802.x (WLAN, WiMAX, LTE) or satellite [3].

A Finnish study [5] notes that all PPDR actors have the same basic needs for the system, voice and data communication but they also have own distinct requirements. For finding mutual solutions and operation models, system integration is needed. This also enables coherent system design including improved activities, cost savings and improved multi-authority co-operation at the scene.

The roles of complementary technologies in the future are as follow [5]:

- 2G/GPRS technologies are reaching the end of their life cycle.
- 3G technology has good coverage with U900 (better than 2G). However, there are problems on the availability/capacity of commercial networks during major accidents in crowded areas.
- The first 4G/LTE networks will be at 2.6 GHz, which is not suitable for rural coverage. In future, 800MHz LTE systems are anticipated.
- Wireless local area network (WLAN) technology has three user cases for data transfer: 1) from a vehicle to command and control room at the garage, 2) a local wireless network around the PPDR vehicle at the scene, and 3) from a vehicle to the Internet via a public WLAN; "WLAN fire plug".
- Satellite technology has a complementary role when there is no terrestrial communications system coverage. This includes long term usage when no other systems are available and communication need for temporary sites. The telecommunication operator TeliaSonera has announced a start of EutelSat KA-SAT services in June 2011. The service may however be of limited use in PPDR communication applications due to the requirement of a relatively large-size satellite dish antenna, limiting the usability of the service in moving vehicles.

3 Multi Organisational Environment

According to [6] in major disasters no PPRD organisation can work alone, but co-operation is needed between actors. The operational parties should not merely trust on their own resources. Besides, a few organizations possess all the needed areas of expertise in a large-scale event, not to mention a large-scale disaster. Information sharing and training at organizational levels is required in order to achieve a working relationship between the actors. This means the actual and operational interoperability between the first responding organizations; also in reality and in the field – not only on 'a paper level' in the form of an official agreement. [6]

The military (MIL), public protection and disaster relief (PPDR) as well as critical infrastructure protection (CIP) actors have multiple similar needs. Similarities in disaster relief mission scenarios include 1) serious disruptions in expected functionalities of critical infrastructures, e.g. transport, supplies, infrastructures, 2) operations in remote areas without communication

ISBN: 978-1-61804-086-2

infrastructures, 3) cross border operations and multi-national teams, 4) high request for interoperability, 5) no remaining infrastructures after a serious disaster, 6) congestion or no use of commercial networks, and 7) utilizing both AdHoc networks and permanent infrastructures [7]. Similarities in command and control communications involve 1) need to receive information on the operational environment, 2) need for the decision maker to watch operation (live feed), 3) need to decide and emanate orders, and 4) need to assess the evolution of the operational situation after decision [7].

4 Cyber Secure Public Safety Communications

Fig. 1 presents a new cyber secure data communications network structure for a multi organizational PPDR environment. The architecture is fully decentralized and all critical communication paths have redundancy. Although having common physical connections, all network actors and elements (multichannel routers, nodes) are identified as well as every organisation's all user levels and their rights to different data sources are known. The decentralized architecture based on the Distributed Systems intercommunication Protocol – DSiP (see e.g. [7]-[9]) is highly fault-tolerant in normal conditions as well as in crises. The software-based approach is independent from different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables to build a practical and timeless cyber secure data network for multi organizational environment, which being fully decentralized is hard to injure. The networks of different organizations are virtually fully separated, but if wanted they can exchange messages and other information which makes them interoperable.

5 Discussion

The public safety communication and information management services market is small (in the year 2008 approximately 2 million users in the US, and similar amounts in Europe and Asia) compared with the 3.4 billion mobile phone users in the commercial telephone network [2]. The PSC and information management systems have different needs (reliability, robustness, security and simplicity) from the regular consumer ITC business. Furthermore, different PPDR services in each region had much autonomy, how they developed their networks. This has caused poor interoperability. PSC systems (networks, devices, services) also have a long lifespan; the systems being sold today have changed little over the past 25 years [2]. The aforementioned matters present the need for different business models than in the regular consumer ITC services.

The two main challenges in European PPDR field operations are the lack of interoperability and the lack of broadband connectivity [4]. Lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, and gaps in procurement or research. Lack of broadband connectivity of wireless communications limits especially the work of the commander of the mobile rescue team at the scene. At least inside every fire engine, police car and ambulance should have the broadband capability.

Today, all new cars have dual brake systems; if one fails, the brakes can still be used for stopping the car. Commercial passenger aircraft have two or more engines; if one engine fails, the plane still flies. How it is possible that critical communication systems are based only on a single communication channel? Distributed Systems intercommunication Protocol (DSiP) offers multichannel communication software forming multiple parallel communication paths between the remote end and the command and control room. Should one communication channel be down, other channels will continue.

References:

[1] ETSI EMTEL Technical Reports TS 102 181: Requirements for communication between authorities/ organisations during emergencies.
[2] Public Safety Communication Europe, WP1: Users requirements, Report on the definition of the generic users requirements, D1.2, 2009.
[3] ETSI Project MESA: Services and Applications SoR - TS 170.001 V3.3.1.
[4] G. Baldini, Report of the workshop on "Interoperable communications for Safety and Security", Publications Office of the European Union, 2010.
[5] M. Rantama, Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa, Pelastusopiston julkaisu, B-sarja. Tutkimusraportit 2/2011.

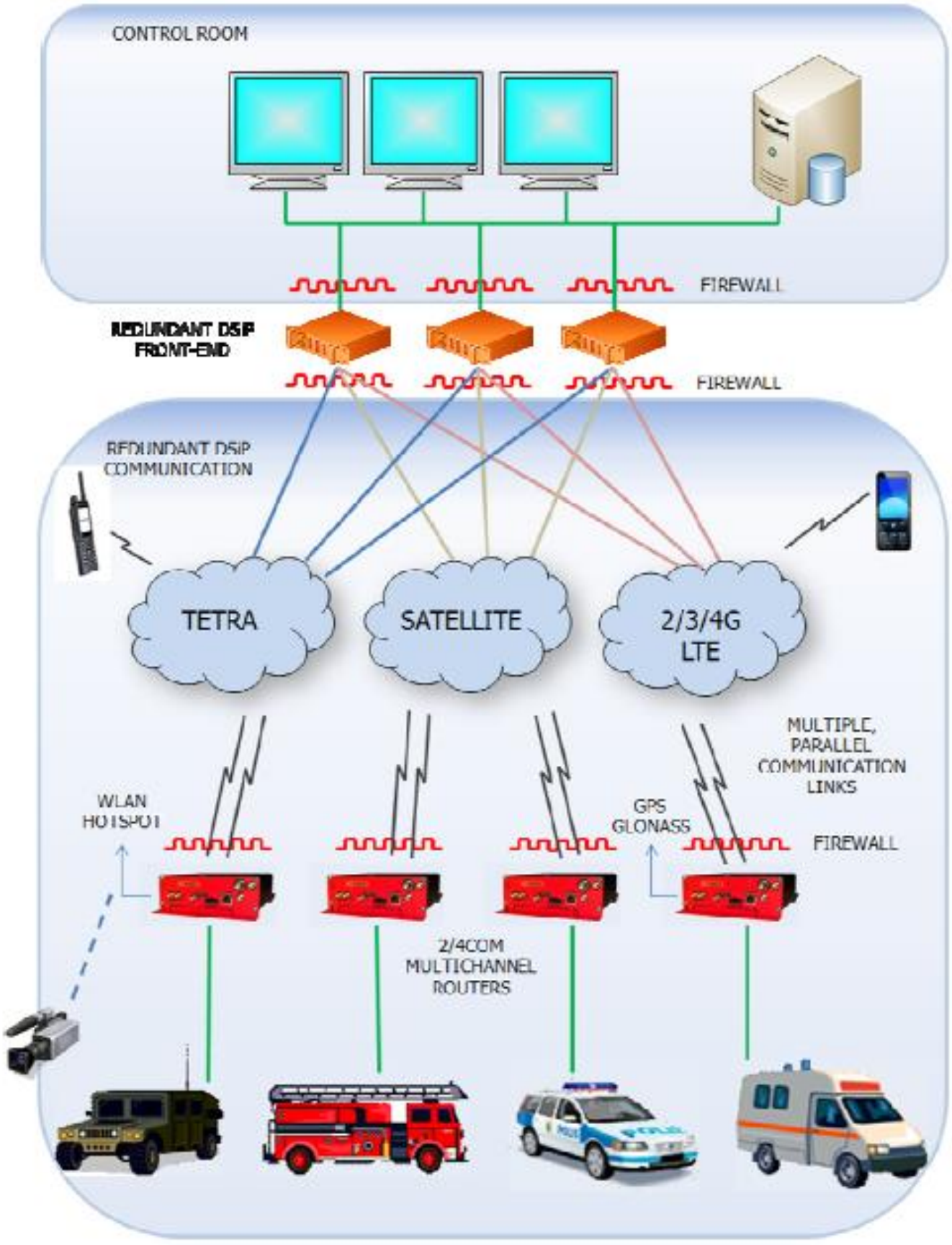

Fig. 1 Fully redundant multichannel Public Safety Communication network

ISBN: 978-1-61804-086-2

[6] Investigation Commission of Jokela School Shootings, Ministry of Justice Publications 2009:2, Helsinki. G. Lapierre, "Synergies and challenges between Defence and Security (PPDR) applications. What implication for the EU?", PSC Europe Conference, 7-8 June 2011, Brussels.

[7] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, "A TCP/IP communication architecture for distribution network operation and control", in Proc. of the 17th Internal Conference on Electricity Distribution, Barcelona, Spain, May 12-15, 2003.

[8] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, Twente, The Netherlands, 2010. IEEE Xplore.

[9] J. Holmstrom, J. Rajamaki and T. Hult, "The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication", International Journal of Communications, Issue 3, Volume 5, 2011, pp.115-122.