# The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication

John Holmström, Jyri Rajamäki and Taina Hult

***Abstract*—** Importance of reliable telecommunication is constantly increasing. A new multichannel data communication concept presented in this paper, provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, uninterruptable, secure and reliable communication link between communicating peers. The solution named DSiP (Distributed Systems intercommunication Protocol) makes it possible to distribute all telecommunication among several operators and methods, resulting in a true multichannel communication system. The DSiP-multichannel routing solution increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems. This is achieved by splitting risks between operators and communication channels; better routing and priority capabilities; taking security and intrusion risks into account; and adding modularity.

***Keywords*—**Data communications, Data security, Data traffic engineering, IP networks, Public safety, Security communications

## I. INTRODUCTION

Two persons who contributed big time to the existence of the Internet are Robert E. Kahn and Vinton Cerf. The Internet was developed in the early 70's. The Internet Protocol (IP) developed by Kahn and Cerf with their team, is generally a "good" protocol, but no one could foresee the need and amount of communication we have today. Some email applications came in the 80's. Tim Berners Lee specified HTML and wrote a browser in 1990.

Today, the most cost-efficient way to globally transport data is by using networks based on the IP-protocol. Multi-path routing for IP networks has been explored for many years in order to mitigate the effect of congestion in networks. Today, many IP-based solutions have been developed for business critical applications. They are used globally for helping companies ensuring business critical Internet connections and VPN-tunnels are always online. Sophisticated multichannel systems are constantly monitoring critical traffic having capabilities for using alternative routes if data traffic problems are encountered in the network. [1]

Operational tasks and working methods in organizations have evolved and changed over the years. Various communication devices, software, services and databases operating via Internet and via other connections have an increasingly greater role. It is important that all valuable data in the processes is uninterruptedly and reliable available anywhere at any time without problems.

There are many aspects that affect the overall security and reliability of information systems. Security and reliability risks should be taken into account when creating new, or when integrating existing systems. The aforementioned is imperative for example among critical control systems and when selecting the means for communication.

Communication has a critical role in many organizations. Especially among Fire, Search and Rescue (SAR) and Law Enforcement Authorities' (LEA), systems communication methods and channels play a key role, not to forget communication related to critical infrastructure of a society.

Cyber-, reliability- and security risks and threats related to communication systems and channels should be known and identified before making any decisions of procurement, for example. [2]

Risks, reliability and threats can be analyzed and identified from many different angles. The nature of secure and reliable critical communication depends on who you ask. With regard to business organizations and Civilian Authorities, their critical communication must typically use regular telecommunication operator capacity and stay "on-line" as much as possible. However, when considering for example Military tactical communication, regular telecommunication operators can't be used and tactical communication systems stay "on-line" as little time as possible. Both user groups need however to ensure that communications reliability, security,

Manuscript received April 21, 2011. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 40350/10 Mobile Object Bus Interaction (MOBI).

J. Holmström is with Ajeco Ltd., Arinatie 10, FI-00370 Helsinki, Finland (corresponding author to provide phone: +358-9-4770 470; fax: +358-9-4770 4799; e-mail: john.holmstrom@ajeco.fi).

J. Rajamäki is with the Laurea SID Leppävaara, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: jyri.rajamaki@laurea.fi).

T. Hult is a student at Business Information Technology, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: taina.hult@laurea.fi).

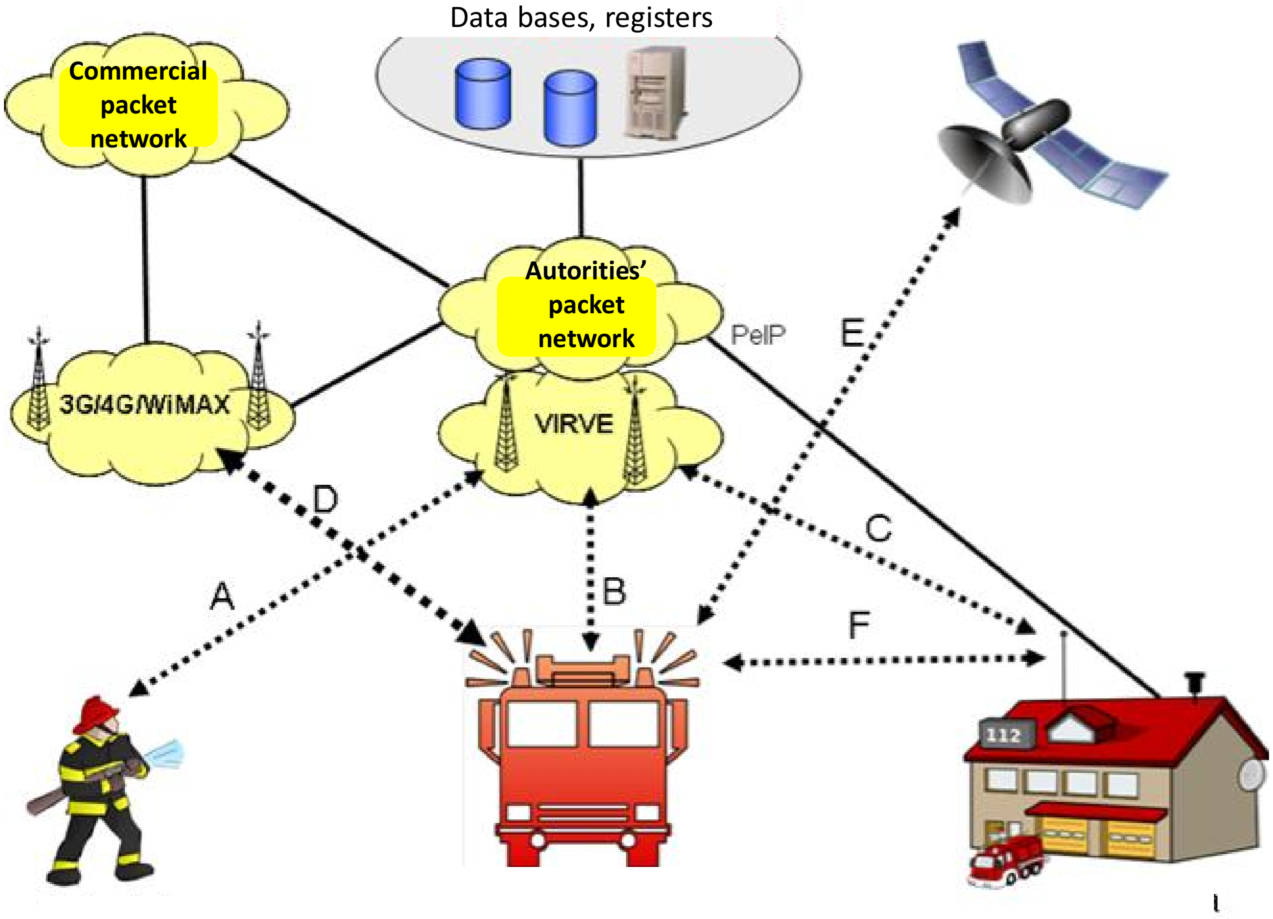
performance, interoperability, integrity, etc. are taken into account.

Integration of information systems is a current trend in all businesses and organizations [3]. The trend is towards larger more mobility and the Web plays a major role in providing critical business data, applications and services for mobile users. In this respect, service-level requirements play an important role in the process. However, service-level requirements are difficult to quantify during the project planning phase. The following intangible values could be used as guide lines for drawing up the operational constraints and goals required: 1) usability, 2) performance, 3) scalability, 4) reliability, 5 availability, 6) extensibility, 7) maintainability, 8) manageability, and 9) trustworthiness and security. Only after deployment, these attributes can be quantified. To meet pertinence requirements, the production (communication) system needs changing and tuning; if not possible, service-level requirements should be readjusted to conform the operational environment. The reason for the existence of any Web system is to support business and organizational needs. A shift of focus may be needed in any new project and Web architecting activities should be given more effort, attention and seriousness. [4]

### *A. The Communication Needs of Public Safety Authorities*

According to [5], the Communication Needs of Public Safety Authorities are: 1) reliable and robust voice communication everywhere, 2) allowing for co-operation and easy communication between all organizations, 3) short messaging for alarming, field task delivery and to secure the validity of the information, 4) file transfer from the place of incident to support sites as the command or 112 centers, and 5) offering of communication from the field for daily office work.

Urban societies need communications to maintain essential services, even during emergencies. Citizens demand safety and security, which can only be delivered by efficient public agencies with access to reliable and secure group (one-to-many) communication. Professionals rely on mission-critical communications to help working together, optimizing



A: TETRA air interface of handheld radio
B: TETRA air interface of vehicle radio/modem
C: TETRA air interface of station radio/modem
D: Air interface for commercial networks
E: SATCOM
F: WLAN Interface between Rescue vehicle and Fire station LAN/Intranet

Fig. 1 Interfaces of wireless communications in the field of fire and rescue services [7]

situational awareness, response time and control when facing challenging situations. Taskforces need the support of secure, uninterrupted voice and data services. Professional mobile radio (PMR) is field radio communications using portable, mobile phones, base stations, and dispatch console radios. Analog PMR systems are regularly not protected against eavesdropping and offer limited voice quality. The operation of digital PMR radio equipment is typically based on standards such as TETRA and TETRAPOL. Key features of professional mobile radio systems can include [6]: 1) point to multi-point communication, 2) push-to-talk, release to listen, 3) large coverage areas, 4) closed user groups, and 5) use of VHF or UHF frequency bands. Fig. 1 shows the interfaces of wireless communications in the field of fire and rescue services.

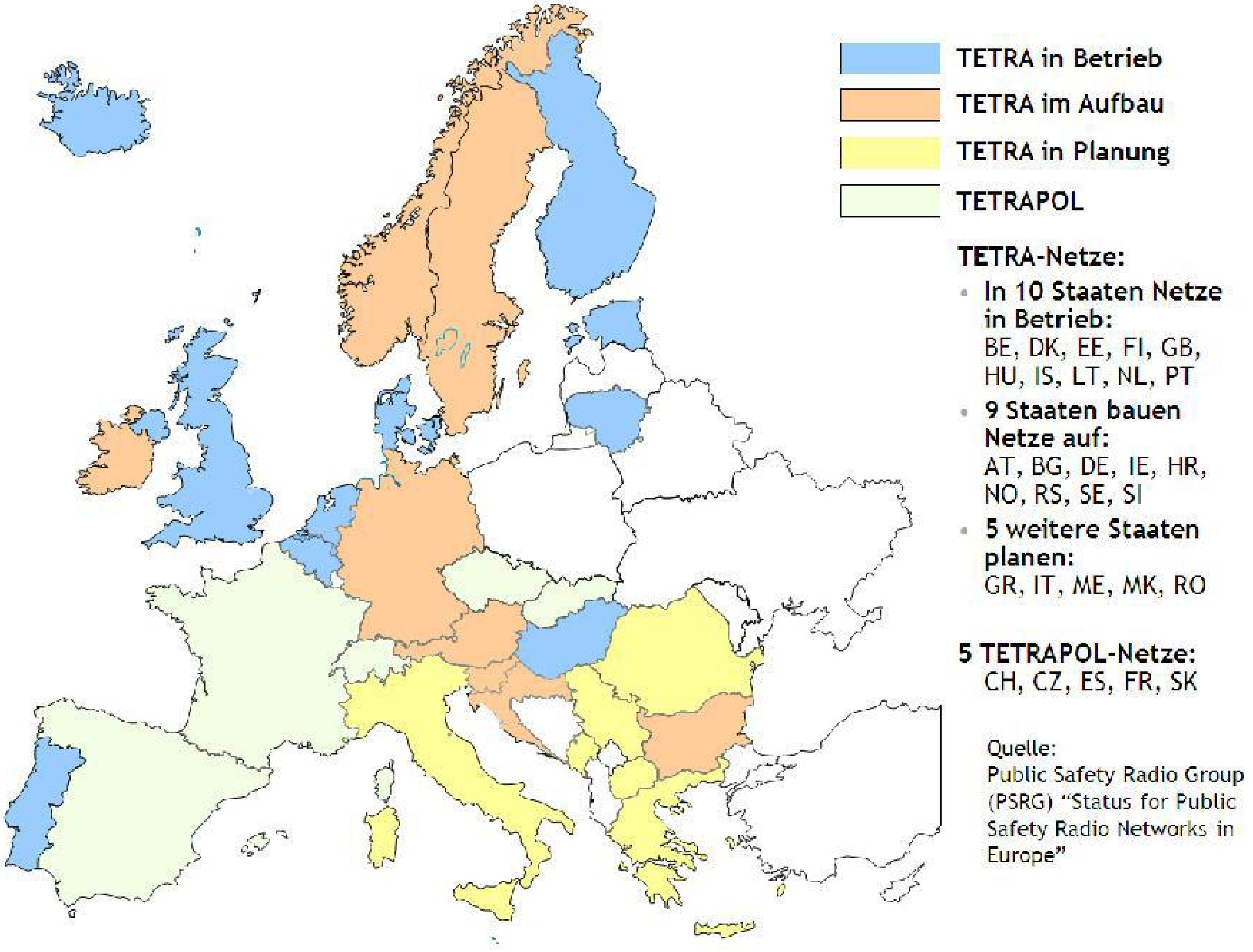
### *B. TETRA and TETRAPOL*

The Terrestrial Trunked Radio (TETRA) standard has been implemented and developed by the European Telecommunications Standards Institute (ETSI). The TETRA standard can be described as a suite of standards. In practice, these standards cover different technology aspects such as for example air interfaces, network interfaces and services and facilities.

TETRA is a worldwide standard and there exist hundreds of TETRA networks across the world. TETRA systems have many advantages. One advantage is its Interoperability Certification requirement. TETRA can be used and shared by all public safety organizations hence being an economic solution. It offers secure communication channels during emergency situations and disasters. TETRA is a fully digital system, which offers high-quality voice in addition to a wide range of possibilities for data transfer. TETRA also supports voice and circuit switched and packet-switched data transmission with different bit rates and error-correction levels.

A TETRA system is based on virtual private network technology. It offers one physical network which can be shared among different organizations. In practice, each user group is able to utilize a TETRA based network as it would only be available to the group.

The nature of a crisis event affects the usable media. For example in case of a sudden panic event, the public cellular technology is useless. A large crowd (rock concert, hockey game etc.) will load the public cellular net heavily due to the concentration of mobile phones under a limited number of


🟦 TETRA in Betrieb
🟧 TETRA im Aufbau
🟨 TETRA in Planung
🟩 TETRAPOL
TETRA-Netze:
In 10 Staaten Netze in Betrieb:
BE, DK, EE, FI, GB, HU, IS, LT, NL, PT
9 Staaten bauen Netze auf:
AT, BG, DE, IE, HR, NO, RS, SE, SI
5 weitere Staaten planen:
GR, IT, ME, MK, RO
5 TETRAPOL-Netze:
CH, CZ, ES, FR, SK

Quelle:
Public Safety Radio Group (PSRG) "Status for Public Safety Radio Networks in Europe"

Fig. 2 The nation-wide PMR networks in Europe [8]

base stations - a minor crisis event in this kind of situation may allow for using dispersed public communication channels. And, finally, public cellular technology will most probably remain useful and intact during, for example, an oil disaster due to the large geographic area of the latter.

Regardless of many inevitable advantages in TETRA based networks, being economic and working under all circumstances, it has a disadvantage which is: heavily limited data capacity.

TETRAPOL is another digital PMR technology standard for mission-critical public safety users. The main difference between TETRA and TETRAPOL is that TETRA makes use of the available frequency allocations using Time Division Multiple Access (TDMA) technology with four user channels on one radio carrier with 25 kHz spacing between carriers. TETRAPOL's air interface is based on Frequency Division Multiple Access (FDMA) radio access and Gaussian Minimum Shift Keying (GSMK) modulation.

Fig. 2 shows the nation-wide PMR networks in Europe. TETRA networks are in operational use in Finland, UK, The Netherlands, Belgium, Hungary, Eastland, Lithuanian, Denmark and Portugal.

### C. *Multichannel Communication*

The introduction of the VIRVE network in Finland has enabled a high level of multi-authority co-operation at the (incident) scene. All authority actors have the same basic needs for the system and data communication, but also have own distinct requirements. An intention for finding mutual solutions and operation models, facilitating system integration and enabling coherent system design, exist; improved activities, cost savings, improved multi-authority co-operation at the scene are of desire. [9]

The voice services of the VIRVE network are working well with high reliability, fast connection setup and good coverage. Customers are generally satisfied and in the near future, no major changes in the voice services are foreseen. Furthermore, data services are reliable and the coverage is good. However, the VIRVE data services are of low capacity with customers being unsatisfied with this performance in VIRVE. Improvements to the low data capacity are not visible in the near future that would fulfill the need. The possibility of TETRA Enhanced Data Service (TEDS) upgrade may bring partial solutions to the limited data capacity. [7]

According to [7], the roles of complementary technologies in the future are as follows:

1) Datame (@450/ WiMAX/CDMA,LTE) has good coverage and usability according to tests performed by Police authorities. However, there is uncertainty of the future existence of this radio technology.
2) 2G/EDGE/GPRS technologies are reaching the end of their life cycle.
3) 3G/HSPA technology has good coverage with U900 (better than 2G). However, there are problems on the availability/capacity of commercial networks during major accidents in crowed areas.
4) The first 4G/LTE networks will be at 2.6 GHz, which is not suitable for rural coverage. Future, 800MHz LTE/4G systems are anticipated.
5) WLAN technology has three user cases for data transfer: 1) Vehicle - Fire station at the garage, 2) Local wireless network around fire truck at the scene, and 3) Vehicle - public WLAN:"WLAN fire plug".
6) Satellite technology has a complementary role when there is no terrestrial coverage. This includes long term usage when not available other way, and satellite transmission for temporary site. 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 Authority communication applications due to the requirement of a relatively large-size satellite dish antenna, limiting the usability of the service in moving vehicles.

In Europe, the present state of public safety communications is that TETRA/TETRAPOL is the best choice for voice communication for authorities having virtually no competitors. On the other hand, the data communication capacity over TETRA does not fulfill growing future needs; however the slow data is robust and works well. Wideband data (=TEDS) is possible to implement in the future but does not solve all problems. The planned TETRA Rel. 3 is not available before 2020 and includes some degree of uncertainty regarding implementation. The aforementioned effectively means that in addition to TETRA, complementary data transfer technologies are needed; choices of today and near future include3G/HSPA, 4G/LTE, WLAN and Satellite Communication.

The 450 MHz band formerly used for cellular NMT technology is today used by Flash OFDM 450 technology in Finland. The 450 MHz bandwidth has a good penetration capability and the cell size of the @450 network is relatively large. There are however concerns about if the Flash OFDM technology will prevail. An alternative technology could be CDMA operating at the 450 MHz band. Regardless of the 450 MHz band with OFDM prevailing or not; there is presently a strong demand for dedicated broadband capacity among authorities. [7]

The solution to ensure quality of critical communication is to use several communication paths provided by several operators. Parallel use of communication channels data links, regardless of technology, solves many problems. The progress of technology is enabling alternative channels for communication.

The big questions are, how much should and could public safety responders rely on commercial broadband services? What is the availability of public networks during major accidents? The aforementioned means that a multichannel router or terminal must intelligently and constantly be aware of usable network resources and coverage (TETRA, 3G, 4G, WiMAX, WLAN, etc.) Furthermore "WLAN - fire plug" availability should also be taken into account.

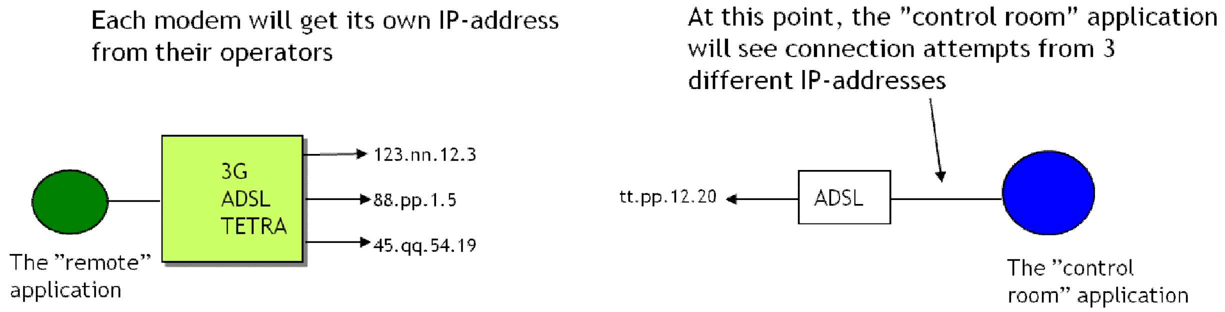

Each modem will get its own IP-address from their operators
At this point, the "control room" application will see connection attempts from 3 different IP-addresses
3G
ADSL
TETRA
123.nn.12.3
88.pp.1.5
45.qq.54.19
The "remote" application
tt.pp.12.20
ADSL
The "control room" application

Fig. 3 Typical Multi-modem System

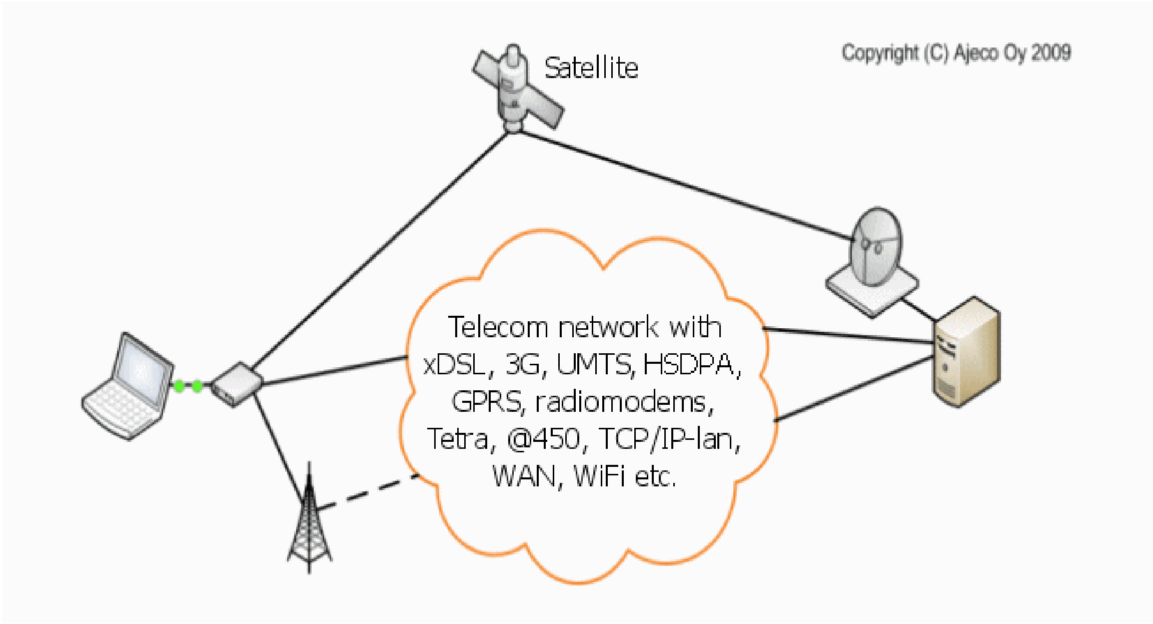

Satellite
Copyright (C) Ajeco Oy 2009
Telecom network with xDSL, 3G, UMTS, HSDPA, GPRS, radiomodems, Tetra, @450, TCP/IP-lan, WAN, WiFi etc.

Fig. 4 DSiP Telemetry System

## II. Problem Formulation

Fig. 3 shows how a typical multi-modem remote application works. All modems will get their own IP-address from their operators and the control room application(s) will see connection attempts from multiple IP-addresses. This kind of a multi-modem system cannot share communication between different physical media without rewriting the application software to do so, because IP does not support multichannel communications by maintaining simultaneous socket connections over multiple physical media. Rewriting an application software to support multichannel communications is a very challenging task.

A typical security problem many times preventing Virtual Private Networks (VPN) from being used in a multi-modem data communication environment, is that VPN solutions typically allow for creating a secure link over only one physical media at a time. If the media encounters problems, the VPN must be re-established over another media. These limitations are related to IP-addressing issues and how the IP-stack handles socket connections.

### A. Research Question

The IP-protocol is a great protocol for transporting data but it is not enough when considering mission critical or highly important systems. For that reason, the research question (RQ) of this study is formulated:

*RQ: Is there any solution that allows also regular communication methods to be used in mission critical telemetry systems?*

## III. Problem Solution

The new multichannel data communication concept provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, secure and reliable and unbreakable communication link between communicating peers.

Our proposed solution is based on the Distributed Systems intercommunication Protocol® (DSiP) [10] which handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication. It increases dramatically the reliability, security and controllability of communication systems being completely independent from operators. DSiP

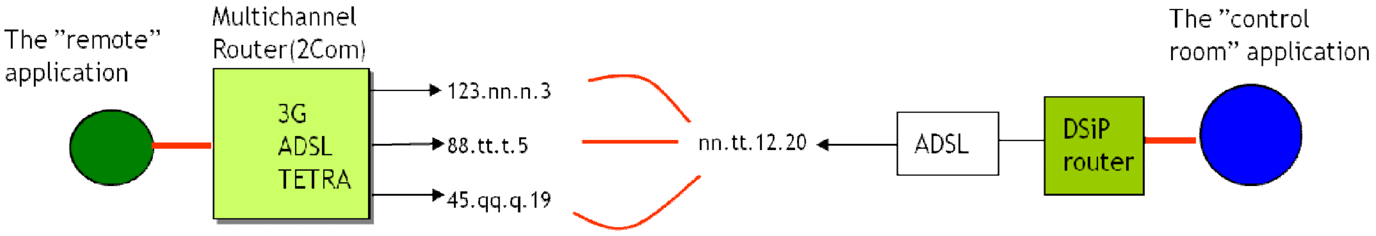


Fig. 5 DSiP Multichannel System

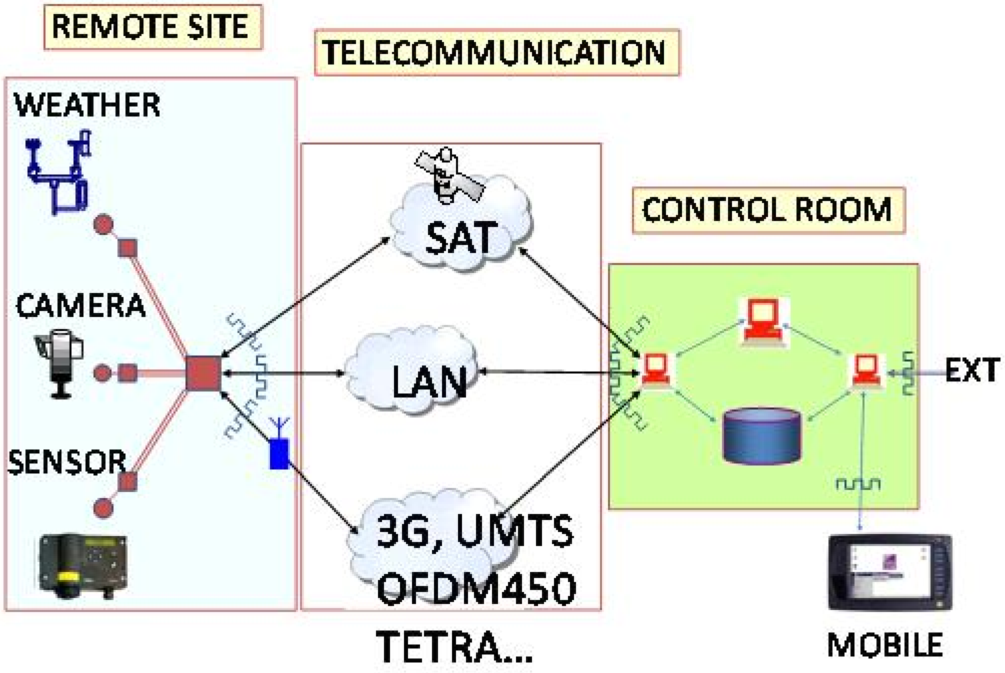


Fig. 6 Modularity of DSiP

can be regarded as a traffic engineering layer above the regular IP-layer – "the missing OSI layer".

DSiP allows for:

1) Combining and using telecommunication methods in parallel so that multiple connections appear like a single reliable and unbreakable connection. DSiP can route data over both IP- and non-IP connections.
2) DSiP is independent from operators. It allows the user to shop and combine telecommunication from any operator.
3) DSiP contains protocol translation methods making equipment, systems and software compatible.
4) DSiP implements security mechanisms as well as reduces risk for DOS attacks and virus-infusion.
5) DSiP has better control over data routing, priorities and services.

### *A. System Overview*

Fig. 4 shows an overview of the DSiP communication system, which is capable of routing data over any kind of connection, IP and non-IP, and works in multi-operator environments applying satellites, 3G, GPRS, UMTS, HDSPA, IP-network, TETRA, serial connections and radio modems.

### *B. Robust and Secure Data Communications*

The DSiP-protocol supports splitting on a VPN tunnel over several physical media simultaneously without the aforementioned constraints, as shown in Fig. 5. In addition, it solves incompatibility issues on both physical and logical levels in addition to providing modularity, data integrity, security and versatility to data communications systems ranging from small to very large size. By following a set of logical rules within the DSiP and by using IP or any bit transferring channel (e.g. radio modems) as means for transport, applications, equipment and software from different vendors may intercommunicate transparently i.e. applications may respond to, and ask for services without needing to know about physical implementations [10]. The DSiP protocol maintains a VPN link regardless of changes in the used physical media i.e. VPN works during channel switches.

### *C. Modularity*

A DSiP telemetry system always consists of three elements: the remote site or LAN segment, the telecommunication system and the command and control room or local LAN segment. If one of these element changes, it does not affect the others, as the DSiP solution is highly modular as Fig. 6 shows.

## IV. Applications

### A. SCADA Systems

DSiP is applied in the SCADA control of Finland's main power grid. Furthermore, a major part of Vattenfalls power distribution network in Finland is managed and controlled by DSiP, AM08M RTU's and AM06T communication bridges. Power grid breakers are monitored and controlled by a SCADA-system through the DSiP-system. Fig. 7 shows how an operative system works.

### B. Coast Guard Surveillance System

The Finnish Frontier & Coast Guard uses coastal surveillance cameras in order to continuously execute control and get telemetry information. The system is an important part of general surveillance and SAR, has an operative status as must remain working on a 365/24/7 basis. The DSiP-system allows for location independent operation i.e. control rooms can be placed at any desired location.

DSiP is also a central communications solution in the Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C) - integration project [11] and the Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) demonstration project [12] both funded by EU's FP7 security program.

### C. Outdoor Lighting Control

A pilot project has been conducted with Helsingin Energia regarding control of outdoor lighting using Mobile Television Broadcast (DVB-H) as transmission media for DSiP control packets and GPRS as return channel. The DVB-Gate-unit replaces ripple control receiver units in the power distribution network. It contains two communication interfaces: A DVB-T/H interface for receiving broadcasted commands and a GPRS interface for sensor- and energy meter feedback. The GPRS also acts as a backup channel. The DSiP-system provides the data communication infrastructure together with controller tasks and nodes.

## V. Discussion

With DSiP, customers can use multiple communication channels in parallel in such a way, that ending peers ”think” they are using one channel. DSiP shares communication resources between different hardware equipment and software modules; automatically routes data and uses secondary routes if primary connections are broken. It always knows the correct sender and correct receiver and uses strong encryption and timestamps. DSiP makes communication more robust and improves data security. The DSiP may be regarded as a secure and reliable multi-point to multi-point communication system with VPN characteristics.

IP traffic and its packets have methods for controlling priority, or perhaps better, quality. The IP QoS (Quality of Service) is however either not supported at all, or, supported in non-conforming ways in operator traffic. Customers using DSiP have enhanced controlling possibilities for controlling the data flow i.e. traffic: (1) control priorities – important information is routed first, less important later; (2) control over network timeouts – no undetermined delays or waits; (3) control the usage of communication and bandwidth – DSiP always ”knows” the condition of all routes; and (4) have better control over maintenance and configuration; and (5) the DSiP system has in-built congestion control and (6) routing services based on cost-factors enabling certain, less important traffic to be filtered should the used communication be of low capacity for example.

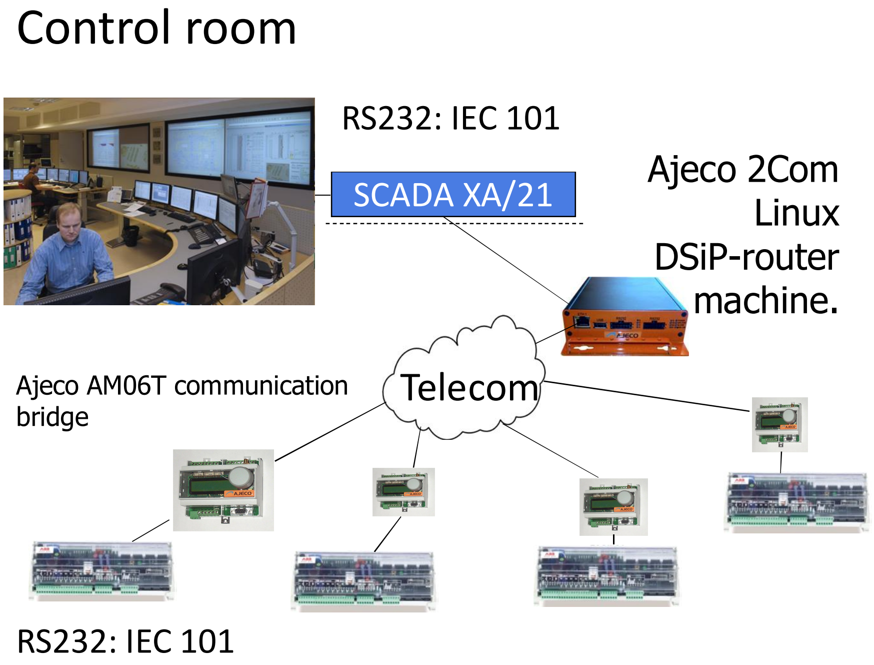

Control room
RS232: IEC 101
SCADA XA/21
Ajeco 2Com Linux DSiP-router machine.
Telecom
Ajeco AM06T communication bridge
RS232: IEC 101

Fig. 7 DSiP-encapsulated IEC-messaging to electrical substations

DSiP can combine and use IP and non-IP communication links and also tunnel IP traffic through non IP connections. DSiP allows for tunneling of other protocols through itself and can make equipment and software compatible via intelligent interface mechanisms.

Being independent from every single telecommunication operator, and virtually any physical method, end-users could distribute the operator risk by using multi-operator network topology.

DSiP is not a heavy or difficult protocol to embed into various equipment and platforms. However, DSiP contains features like:

- Solutions for data-integrity and security and authentication
- Automatic re-routing of information via backup channels – redundancy
- A controllable method for multi & broadcasting – bandwidth control
- A uniform interface to software & equipment – solving incompatibility issues
- Scalability – the system is very flexible – easily add new and old equipment & swr
- Complete independency of physical communication methods – any means for transmitting a bit is good
- Real-time online knowledge of the network topology – NO unwanted connection delays.
- Centralized authentication-, Network management- and Configuration server software – tools for maintaining the system.

A DSiP test environment is set up in Laurea University of Applied Sciences, with the purpose of testing and demonstrating the functions of the multichannel routing solution exploiting multiple communication paths in practice. By creating different problem situations, we are able to test the reliability and robustness of the communication system. So far, the results from the testing environment have been encouraging. Multiple connections over all tested types of media appear like a single ultra-robust communications channel. When one connection fails, DSiP easily finds another working route. The way how the new connections are created can be read from log files. However, this is not very illustrative and for that reason, we are developing new visualizing tools. [13]

## VI. Conclusion

With regard to European mission-critical public safety communications, TETRA/TETRAPOL is the best choice for voice communication and in the near future, it has no competitors. Data communication over TETRA is rather slow and does not fulfill future needs even though the low capacity communication can be considered very reliable. Wideband data “enhanced TETRA” (=TEDS) is potentially attractive but does not solve all problems. TERA Rel. 3 is not available before 2020 and has some degree of uncertainty regarding. The conclusion is that in addition to TETRA, complementary technologies are needed and multichannel communications is the answer.

The need for secure multichannel communication is global and exploding. DSiP is a solution allowing also regular communication methods to be used in mission critical communication systems. It also enables a combination of all kinds of telecommunication resources: IP traffic and non-IP traffic over TETRA, radio links, satellite communications, serial connections etc. can all co-exist forming a single uniform and maintainable system.

## References

[1] J. Holmstrom, J. Rajamäki and T. Hult, “DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication” in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.57-60.

[2] T. Hult and J. Rajamäki, “ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project”, in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.143-148.

[3] D. Litan, A.-M. Mocanu, “Information systems integration, a new trend in business”, ”, in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.250-256.

[4] S. Tumin, S. Encheva, “A brief look at Web architecting”, in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.245-249.

[5] J. Koivukoski, “What are the future solutions and technologies of national security communications?” VIRVE Day -seminar, Helsinki, Finland, March 2011.

[6] Professional mobile radio – Wikipedia, http://en.wikipedia.org/wiki/Professional_Mobile_Radio

[7] M. Rantama, Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa, Pelastusopiston julkaisu, B-sarja: Tutkimusraportit 2/2011. http://www.pelastusopisto.fi/pelastus/images.nsf/files/A1933B8977CDAE26C22578570025B300/$file/Pelti%20loppuraportti%20liitteineen.pdf

[8] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, htpp://www.bdbos.bund.de

[9] K. Junttila, “What are the future needs of mission critical communications at rescue services?” VIRVE Day -seminar, Helsinki, Finland, March 2011.

[10] 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.

[11] M. Morel and S. Claisse, “Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C)” in Proc. of the Ocean and Coastal Observation: sensors and observing systems, numerical models and information systems, Brest, France, June 21-23, 2010.

[12] Demonstration project on the Surveillance of the EU Sea Borders, by Europolice on 22. January2011, Available: http://europolice.noblogs.org/2011/01/demonstration-project-on-the-surveillance-of-the-eu-sea-borders/

[13] 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 Nov. 24-25, 2010.