Gathering End-user Requirements for the MACICO Public Safety Communications Project

Pasi Kämppi, Jaakko Tyni and Jyri Rajamäki

***Abstract*—**The Multi-Agency Cooperation In Cross-border Operations (MACICO) project will develop a concept for interworking for security organizations in their daily activity. It deals with cooperation of security organizations that do not use (in their day-to-day job) the same radio network, but in some missions could take benefit from a sharing of their respective infrastructure. Use cases such as pursuit of criminals across a border, close support of vehicles going through a border, and disaster relief operations require security organizations from both countries to communicate together and to continue to communicate with their control room. This paper comprises a useful reference on the standards and requirements identification related to interoperability of public safety communication systems, on the existing technological status and the immediate future activities.

***Keywords*—**Cross-border operations, Emergency communications, End user requirements, Interoperability, Next generation emergency service, Public safety

I. Introduction

PUBLIC safety communications (PSC) comprise the primary condition and requirement for the effective intervention of the public protection and disaster relief (PPDR) sectors. The Multi-Agency Cooperation In Cross-border Operations (MACICO) project develops a concept for interworking for PPDR organizations in their daily activity [1]. The main objective of MACICO is to reply on a short term to the Public safety organization needs on radio communication systems for cross-border operations and for cooperative crisis missions. The organizations will communicate without functional perturbation and corrupting the security of the network. MACICO will also study interoperability issues that rise for the transition period between the existing networks and next broad band generation. This paper provides user requirements specification (URS) for terrestrial trunked radio (TETRA) and Tetrapol communication systems in cross-border operations. The document describes functional and non-functional requirements.

In almost all cases the response time of the PPDR sectors and their degree of preparation to handle the emergency situation are the basic factors that determine the effective provision of PPDR services to individuals in danger. Both conditions can be met through efficient PSC infrastructure and intelligent PSC services that can inform the PPDR responders immediately as soon as an emergency situation occurs and over which as much detailed information on the incident as possible can be transmitted. Therefore, in every country national authorities as well as international organizations are focusing their efforts on the efficient support of PSC services over evolved network infrastructures [2].

TETRA is an open standard developed by European Telecommunications Standards Institute (ETSI). The target of standardization work was to define open interfaces to enable seamless interoperability between different networks and equipment manufacturers. The TETRA standard contains features to allow interoperability between deployed national networks but TETRA has been used in cross border operations only in pilots.

The first remarkable pilot was deployed in 2003. The Three Country Pilot was a project among The Netherlands, Belgium and Germany. The target was to connect the TETRA networks of all three countries using an Inter-System Interface (ISI phase 0). In a simulated crisis the specified group of civil protection authorities was able to communicate to each other on the Aachen – Limburg – Liège border area. The pilot was a success and many great lessons were learnt.

The second pilot was organized in 2010. Cassidian, an EADS Company, deployed another pilot project with ISI phase 1 where Swedish and German TETRA networks were connected to each other. This time the pilot was organized on maritime area. Again, the pilot was successful and many new things were found out.

II. Methodology

A. End Users Requirements Capture

This study focuses on the acquisition of use cases and system requirements. This study gathers all work related to the interaction with operators and end-users [3, 4]. It is organized around a framework for gathering operational scenarios and

The authors would like to acknowledge all the participants of the MACICO project [1], EUREKA and Tekes—the Finnish Funding Agency for Technology.

P. Kämppi, J. Tyni and J. Rajamäki are with SID (Service Innovations and Design) Leppävaara, Laurea University of Applied Sciences, FI-02650 Espoo, Finland; phone: +358 9 8868 7400, e-mail: {Pasi.Kamppi, Jaakko.Tyni, Jyri.Rajamaki}@laurea.fi.

requirements, as well as systematic methodology for harmonization of needs at European level.

The requirements are produced by existing operational users/operators from (several) already deployed networks. It shall address issues such as:

- Capability and conditions for the use of radio terminal by foreign users in their networks
- Use cases for Voice Communications including foreign terminals in a network
- Uses case for inter network communications
- Management conditions for gateways deployment and interoperability configuration
- Requirements on the interoperability backbone.

End user requirements are generally captured through iterative phases process [5]. The phases of analysis are:

- Data gathering
- Data analysis activities
- Expression as requirements.

Figure 1 describes the different layers of this study. In the process of capturing user requirements we need to study users, operational procedures, TETRA services, operators and technology. Research team must be able to gather information from different sources and actors, but at the same time act as an intermediator and interpreter between different actors. The researches should be able to understand and speak the language used by technological actors and end users.

Figure 2 shows that user requirements are based on literature review, end user interviews and discussions with technical experts. The results from different sources were cross-checked. This method, triangulation, were used to increase the validity of results.

B. LbD as a Background Model

This study has its theoretical background in Learning by Developing (LbD) model, which is used in Laurea University of Applied Sciences. Learning by Developing (LbD) is a pedagogical and communal approach which links learning to applied research, development projects and culture [6,7]. Students carry out their studies in real-world development projects, in which the phenomena and problems are approached through research.

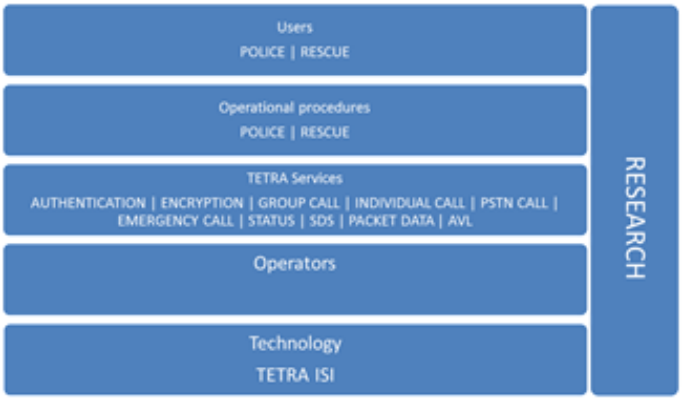

Fig. 1 The layers of research

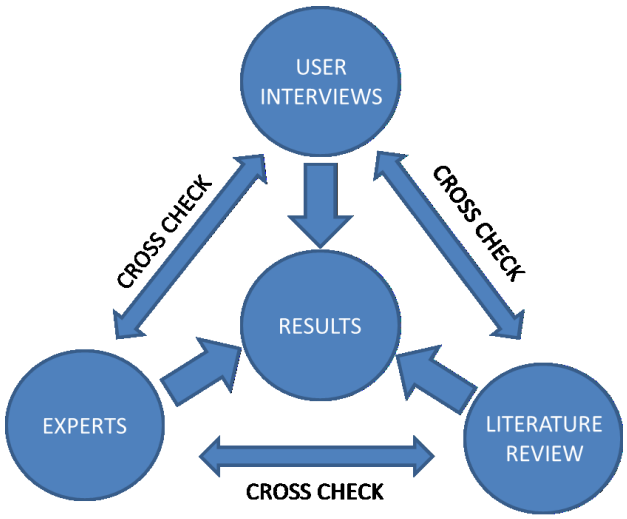

Fig. 2 MACICO Information Gathering Method

III. STANDARDIZATION

ETSI TETRA standards (TC TETRA) include the interface between two TETRA network infrastructures: TETRA Inter-System interface (ISI) standards.

The first set of TETRA ISI standard was available already in year 2000 in ETSI. First set of ISI interoperability TIP profiles (ISI ph1) was ready in 2001 in TETRA Association (TA). Since then there has been development/updates of the ISI standard, as well as completion of further ISI TIP ph2 and ph3 profiles. It can be said that a full set of ISI standards and TCCE TIP profiles have been available for over 5 years.

In TCCE (Former TA) TETRA IOP work continues also in the context of ISI standards, currently defining the so called ISI ph4, complementing the interoperability functionality in some aspects.

Fig. 3 shows the timetable of TETRA ISI milestones, including also some Cassidian and Motorola certification achievements. Cassidian has certified ISI ph2 in its TETRA infrastructure release in 2012.

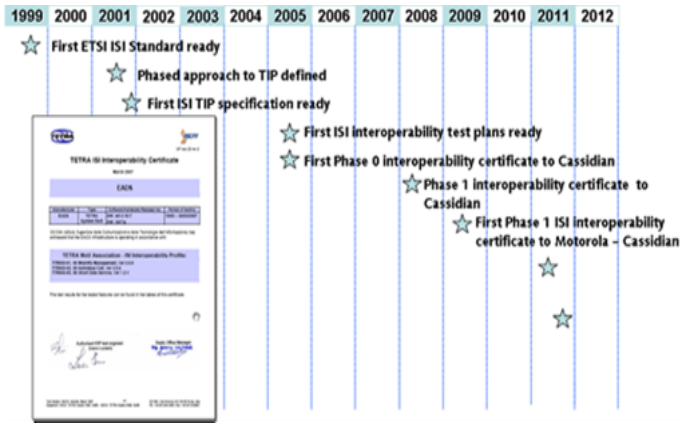

Fig. 3 TETRA standard and IOP milestones

The TETRA Inter-System Interface (ISI) standards are available and published by ETSI, the following lists the standards:

• EN 300 392-3-1 Interworking at the ISI; Sub-part 1: General design

• EN 300 392-3-2 Interworking at the ISI; Sub-part 2: Individual Call ANF-ISIIC

• EN 300 392-3-3 Interworking at the ISI; Sub-part 3: Group Call ANF-ISIGC

• EN 300 392-3-4 Interworking at the ISI; Sub-part 4: Short Data Service ANF-ISISDS

• EN 300 392-3-5 Interworking at the ISI; Sub-part 5: Mobility Management ANF-ISIMM

• TS 300 392-3-6 Interworking at the ISI; Sub-part 6: Speech format implementation for circuit mode transmission

• TS 300 392-3-7 Interworking at the ISI; Sub-part 7: Speech format implementation for packet mode transmission.

• The following ISI related TIP specifications are available (in TCCE)

• TETRA MoU Technical Report 001 Part 6: Air Interface Migration

• TETRA MoU Technical Report 003 Part 01; Inter Systems Interface (ISI) Mobility Management ANF-ISIMM Implementation

• TETRA MoU Technical Report 003 Part 02; Inter Systems Interface (ISI) Individual Call ANF-ISIIC Implementation

• TETRA MoU Technical Report 003 Part 03; Inter Systems Interface (ISI) Short Data Service ANF-ISISD Implementation

• TETRA MoU Technical Report 003 Part 04; Inter Systems Interface (ISI) Lower Layers Implementation

• TETRA MoU technical report 003 Part 5-1; Inter Systems Interface (ISI) Speech Format Implementation for Circuit Mode Transmission

• TETRA MoU technical report 003 Part 5-2; Inter Systems Interface (ISI) Speech Format Implementation for Packet Mode Transmission

• TETRA MoU Technical Report 003 Part 06; Inter Systems Interface (ISI) Group Call ANF-ISIGC

• 3. IOP Test Plans: By today the following IOP Test Plans related to ISI have been approved (the TTR-001-06 actually belongs to the Voice + Data TIP suite):

• TIP Compliance test plan for testing of TIP Part 6: Air Interface migration Phase 2 (TTR001-06); IOP001-06

• TETRA MoU Technical Report 003 Part 01; Inter Systems Interface (ISI) Mobility Management

• TETRA MoU Technical Report 003 Part 02; Inter Systems Interface (ISI) Individual Call

• TETRA MoU Technical Report 003 Part 03; Inter Systems Interface (ISI) Short Data Service

The following IOP Test plan for TETRA ISI is pending in the specification process:

• TETRA MoU Technical Report 003 Part 06; Inter Systems Interface (ISI) Group Call

A set of ISI interoperability test profiles has also been defined by the TETRA MoU (which name is currently TETRA and Critical Communications Association (TCCA).

IV. Pilots and Related Projects

A. Three Country Pilot (2003)

The Schengen three-country pilot was a project among The Netherlands, Belgium and Germany. Its aim was to connect the TETRA networks of all three countries using an Inter System Interface (ISI) phase 0 [8]. The target was that a specified group of civil protection authorities could communicate in a simulated cross-border crisis on the Aachen – Limburg – Liège border area. By connecting three national sub-networks emergency professionals were able to test their ability to work together and evaluate TETRA technology on a simulated crisis.

The whole project was based on article 44 of the Schengen Agreement:

(1) In accordance with the relevant international agreements and accounts being taken of local circumstances and the technical possibilities, the Contracting Parties shall set up, in particular in border areas, telephone, radio, and telex lines and other direct links to facilitate police and customs co-operation, in particular for the transmission of information in good time for the purposes of cross-border observation and pursuit.

(2) In addition to these short-term measures, they will in particular examine the following possibilities: (a) the exchange of equipment or the assignment of liaison officials provided with appropriate radio equipment; (b) the widening of the frequency bands used in border areas; (c) the establishment of a common link for police and customs services operating in these same areas; (d) co-ordination of their programmes for the procurement of communications equipment, with a view to achieving the introduction of standardized compatible communications systems.

As stated in the final report, the Schengen Agreement's "mandate was confirmed by the Working Group on "Police co-operation" of the Council of the European Union with document 9865/2/96 ENFOPOL 139." The aim was to investigate whether TETRA meets the standards for cross-border communication in practice set by the security organizations working on border areas:

• Does the TETRA standard meet the tactical and operational requirements of the organizations involved?

• Do the mobile communication applications enabled by TETRA meet the needs of the cross-border co-operation officials, which include various security agencies, organizations and their dispatch centers?

The Schengen Three Country pilot was divided into two phases, but the agreement to conduct this kind of project was already agreed upon in 1996, seven years before the field tests began. During those seven years each attending country needed to build up the technical solutions to enable the tests to take place. In practice, all countries had to upgrade their TETRA based radio communication networks and equipment.

The first phase of the test included the preparation of the network, equipment and the field test scenario. The

preparation phase lasted one year. During this phase all needed features were tested: (1) group call, (2) individual call, (3) telephone call, and (4) emergency call.

Air interface encryption and authentication from the foreign network were left out of the scope. As there was no ISI per se available, the connection between different networks was made possible by a modem. The test phase was a success. All tested features worked very well and all participants were able to communicate with each other.

The pilot project helped to identify several issues that need to be addressed before the cross-border co-operation in this mode could be taken into everyday use:

(1) Operational aspects

- integration of intervention teams in foreign networks
- common training and language courses
- agreements on common basic principles on radio procedures
- terminal numbering takes account the international radio communication needs

(2) Legislative

- protection of privacy
- proposals to improve the radio communication possibilities in the border regions

(3) Technical

- limited air interface encryption
- authentication and encryption can only be done by exchanging very important keys
- end-to-end encryption not possible
- use of modems and leased lines (costs) necessary
- multiple conversions from digital to analogue and back to digital reduce the audio quality
- terminal numbering for international communication (GSSI/ISSI) have to be aligned manually
- dispatcher cannot see when and to which network the radios are migrating
- exchange of status and SDS-messages is not possible
- exchange of emergency calls is not possible
- individual calls between countries are not possible

The end result in short was that recommendations for international cooperation should be made. The most needed mutual agreements were in technical, legislative and operational issues. Because of these recommendations, the board of this project urged to continue to phase two, which never happened.

B. Rakel-Bosnet (2009)

The Rakel - Bosnet project demonstrated the usability of TETRA networks in international and multi-authority operations in 2009-2010. The participants were Cassidian, BDBOS and MSB, the Swedish Coastguard, the German Federal Police Sea and the Swedish Police. Cassidian was the technology provider for both the German operational network BDBOS (Bosnet) and the Swedish MSB (Rakel).

This project was the first in the world to succeed in enabling two nationwide TETRA networks to be connected in a cross-border operation with the use of ISI phase 1. It was shown that roaming between two secure TETRA networks was possible and it was possible to control the outside connections within a network.

This project proved that TETRA networks worked well in an international incident management scenario although it was played at the Baltic Sea. It also showed that a dispatcher connection to visited network was possible and that it could control the DSW user rights.

Both countries gave positive feedback on the security and functionality of the network. An EU council agenda on cross-border communications was also raised. This is where the MACICO-project and the possible spinoffs come forward, as the purpose of the project is to connect different countries' and different officials' TETRA networks on cross-border areas within the EU.

V. User Interviews

Interviews were conducted with the help of Finnish end users with significant expertise on TETRA technology. The interviewees came from different organizations throughout the Finnish Officials' field which had been using the devices as fieldworkers and managers. The first round of interviews was organized by email but the response rate was very low. The second round of interviews was made face to face or in remote meetings. The second round indicated to interviewers that the questionnaire form was too technical and plenty of discussion was needed to get satisfying results.

The collective opinion is that the Finnish authorities' nationwide TETRA network Virve is secure and good but its coverage over sea areas and scarce areas in Lapland could be better. The most important feature is group calls. With the long experience about TETRA they pointed out that not only the technical issues make the cooperation between different authorities hard. A maritime rescue expert explained how the protocols on radio use and talk groups make cooperation very difficult. Representatives of different departments in the police force, rescue services (8 districts) and health care districts (7 in all) could all benefit from the same information. It would be tremendously helpful to harmonize the standards and protocols.

An issue that almost all interviewees pointed out was the crowdedness of the talk groups due to lack of training among the end users. However, features of multi-official talk groups were still longed for. A specialist from the rescue field in Finland pointed out, that a temporary management center placed in an aerial vehicle, or alternatively with an access to a view from an aircraft would help in natural hazards, such as forest fires and over the sea.

VI. Specific Requirements

This section presents functional requirements for TETRA and Tetrapol technologies in cross border environment. Requirements are based on user interviews, results of previous projects and discussions with project partners, especially with Cassidian Finland. Many of the needed features are transparent for end users but still necessary to guarantee system reliability and security.

A. External Interface Requirement

Air interface is used for communication between mobile terminal and network. Used networks and terminals have to be implemented according to TETRA/Tetrapol standards.

TETRA ISI (Inter System Interface) represents a set of basic services necessary to support communication between home and visited network. Used networks have to be implemented according to TETRA standards.

Service interworking with legacy networks (TETRA/Tetrapol or Tetrapol/Tetrapol); current preferred solutions for service interworking with legacy networks consist of developing a gateway between the existing PMR network and the guest network and a dedicated application in order to export the features / services from the existing network.

The PSTN interface provides access to Public Switched Telephone Network (PSTN). PSTN is used to communicate with e.g. commercial mobile networks (2G, 3G). PSTN interface has to be implemented according to standards.

A Remote dispatcher interface provides connections for control rooms. This interface is not standardized and it allows vendor specific interface specifications.

B. Functional Requirements for Network

1) Numbering and addressing

When networks are connected to each other for interworking it is essential that each network element and subscriber has a unique address or subscriber number to avoid possible number collisions. Migrated subscribers can be identified by using full ITSI (MCC+MNC+SSI) in TETRA or RFSI in Tetrapol. The home and visited network should be able to handle traffic with MNI identifiers.

2) Pre-provisioning

It is not considered safe for any subscriber to be allowed to migrate to visited network without specific authorization. It is possible to grant access only for certain subscribers by pre-provisioning subscribers. The visited network checks if the visiting subscriber fulfils basic migration requirements before fetching authentication parameters from the home network (ETSI TR 101 448 V1.1.1). There are also defined migration profiles in the visited network that define what services are allowed to visiting subscribers. Migration profiles, to allow/deny use of visited TETRA or Tetrapol network, should include at least the following services (ETSI TR 101 448 V1.1.1): group call, individual call, telephone call, emergency call, status, SDS and packet data.

3) Authentication

The TETRA standard supports the mutual authentication of a Mobile Station (MS) and the network, which is in TETRA normally referred to as the Switching and Management Infrastructure (SwMI). This makes it possible for a TETRA system to control the access to it and for an MS to check if a network can be trusted (TETRA Security). If a TETRA MS roams to a TETRA network other than its "home" network, this "visited" TETRA network will need to obtain authentication information from the "home" network of this MS in order to be able to perform mutual authentication and generate and/or distribute encryption keys. The transfer of authentication information between networks is in principle supported in three ways (TETRA Security): (1) the most straightforward method is to simply transfer the authentication key K to the visited network. Transfer of a data file of keys, even being encrypted, for security reasons is however not advisable. (2) A second option is to transfer certain information that can be used for one single authentication procedure. This is basically the same method as is applied in GSM and can be implemented in a very secure way. However this is only practical where the MS cannot mutually authenticate the SwMI – otherwise the visited SwMI would have to interrogate the home SwMI for a response each time the MS invoked this mutual authentication. (3) A third alternative is therefore supported. This allows a home network to transfer a set of session authentication keys for an MS, which can be used for repeated authentications to a visited network without revealing the original authentication key of the MS. This option combines security and efficiency and permits mutual authentication to take place at a realistic pace. The transfer of the session keys over ISI link should be secured making the use of home session keys safe. Current TETRA terminals, supporting authentication in home network support also authentication in visited network without HW/SW updates. In Tetrapol, a terminal cannot be used until authenticated by the network. Authentication consists of checking that the terminal parameters (serial number, individual address, etc.) match those recorded when the terminal was registered.

4) AIE Security

User traffic and signaling information can be encrypted over the air interface between the MS and the SwMI, both for individual and group communications. The Air interface encryption mechanism is available for Voice and Data in Trunked Mode Operation and in Direct Mode Operation. The use of several encryption algorithms, both standard and proprietary, is supported (TETRA Security). Traffic encryption protects user speech and data. Signaling encryption provides protection from traffic analysis, and prevents an eavesdropper from discovering who is operating in a particular area, or who is calling who (TETRA Security). There are several sorts of encryption keys. Some keys may be derived or transferred as part of the authentication procedure, some keys can be sent to MSs using Over The Air Re-keying (OTAR) or they may be preloaded in the MSs.

5) End to End (E2EE) Security

TETRA and Tetrapol support End to End encryption using a variety of encryption algorithms as deemed necessary by national security organizations. The TETRA Association Security and Fraud Prevention Group (SFPG) have extended the work carried out in the TETRA standard to define a general framework for the incorporation of End to End encryption. Recommended sample solutions have also been provided for the International Data Encryption Algorithm (IDEA) algorithm (IPR owned by Ascom) and the newer Advanced Encryption Standard (AES) algorithm (IPR free), which benefits from a larger cryptographic algorithm block size. Custom and indigenous algorithms are also possible with End to End encryption (E2EE), although these are not recommended for air interface encryption due to their need for

integration in signaling protocols and availability of standard compliant terminals (www.tetramou.com).

6) Group Call

Group call enables the users that have selected the same talk group in their mobile radios to communicate with each other on a half-duplex basis. Half-duplex means that one user is speaking while the others in the same group listen to the person that is transmitting.

7) Group Call Queuing

In TETRA and in Tetrapol a queue is provided in the trunking controller during network busy periods to store and handle calls on a First In, First Out (FIFO) basis in order of user priority level. The advantage is that a user only has to initiate a call request once, knowing that even in busy periods the call will be automatically established once a traffic channel becomes free, thus reducing user stress and frustration when contending with other users on a busy network (www.tetramou.com). It is known that all network vendors do not support call queuing.

8) Individual Call

Individual call is a one-to-one call between two mobile radios. The call can be full-duplex or half-duplex in TETRA and only half-duplex in Tetrapol. Individual calls should work over ISI or through the gateways as it works internally in home network.

9) Emergency Call / Emergency Call Routing

Emergency calls provide the highest uplink priority and highest priority access to network resources. If a network is busy, the lowest priority communication is dropped to handle the emergency call. Activating the emergency call automatically alerts the affiliated control room dispatcher and other terminal users in the talk group of that person. Interoperability enhancements should support emergency call of visited users in a similar way to work internally in home network.

10) Short Data Service

Short Data Service (SDS) is a data service that is comparable with the Short Data Message (SMS, short message service) of GSM. Many applications can use the SDS service to carry information. The most common use of SDS service is the sending of message that is entered via the keypad of the subscriber. Also the GPS location information is usually transported via SDS messages. The limit of data is 140 byte per message.

11) Status Messages

Status messages allow defining preconfigured status messages that are identified by unique number. The system interprets messages numbers to messages. There could be different associations for message numbers in different networks.

12) PSTN Call

A PSTN call provides full-duplex calls in TETRA and half-duplex calls in Tetrapol to Public Switched Telephone Network (PSTN) like to commercial mobile networks.

13) Packet Data

The packet data service can be supported on one TDMA time slot with a gross protected bit rate of 4800 bits/s or multiple TDMA time slots up to a maximum of four. The use of multiple TDMA time slots is often referred to as bandwidth on demand and can be used to increase gross protected data throughput up to 19.2 kbits/s (www.tetramou.com). In the core network data can be routed via a Gp- or Gi-interface and it should be considered what interface is used with interworking. There is an IPI standard in ETSI, supporting packet data over ISI. IPI is not supported in any TCCA TIP profiles and there are currently no suggestions to support IPI or packet data over ISI. Default is to route packet data out of the network, where the terminal is registered and to internetworking in IP networks. IP mobility can be used for migrating between TETRA networks. On the Tetrapol side and with a solution based on a gateway, the problem is simplest. The interface to the control rooms already contains all the elements necessary to the provision of the services in connected packet mode.

14) Dynamic Group Number Assignment

This service allows the creation of unique Groups of users to handle different communication needs and may also be used to group participants in an ongoing call. This service is considered by many public safety organisations to be extremely useful in setting up a common talk group for incident communications. For example, selected users from the Police, Fire and Ambulance could be brought together to manage a major emergency where close co-ordination between the three emergency services is required. Similarly, DGNA is also considered useful for managing incidents by other user organisations such as Utilities and Transportation (www.tetramou.com).

15) Automatic Vehicle Location

Automatic Vehicle Location (AVL) is used to track and trace persons or vehicles using TETRA/Tetrapol radios. Most TETRA radios are equipped with an integrated GPS receiver and Tetrapol radios need additional GPS receiver to be integrated with terminal. The TETRA/Tetrapol radio is able to determine its location and can send this information to the infrastructure were it can be forwarded to an end point which is in most cases a control room (www.tetra-consultancy.com).

The location is sent via a SDS or packet data to an AVL server. The AVL system may be a fixed host in the TETRA network, connected via control room API of the TETRA network or a server connected to the PEI of a radio terminal. The radio needs be have the destination address (ISSI) of the AVL system pre-programmed. It is common that the TETRA radio sends the location message as a LIP (Location Information Protocol) to the AVLS server. The LIP protocol is an ETSI standardised protocol for location information. The control room(s) connect to the AVL server to obtain the location information of the TETRA mobile radios and display their locations on a map. The connection between the control room(s) and AVL server is usually a proprietary protocol (www.tetra-consultancy.com).

In a Tetrapol the location is sent via Short Datagram to an AVL server. The AVL system may be a fixed host in the Tetrapol network identified by a functional IP address, connected to the Data Network Controller (DNC). In Tetrapol servers it is not recommended to use radio terminals to connect to the AVL Server due to collision of messages. The UDT (User Data Terminal) connected to the radio must have

configured the functional IP address of the AVL Server. There is no Tetrapol location protocol defined, so the messages use a proprietary protocol and it depends on the AVL Server integrator. The connections between the control room(s) and AVL server and between UDT and Radio Terminal are defined in Tetrapol Publicly Available Specification.

16) Integration with Control Rooms

Control room operation and connection is outside of ETSI ISI interface service. The default assumption is that a visiting user can be connected/under control of a local command center in the visited network or connected/under control of home control center. TETRA ISI is to support control room dispatcher workstation to join visiting terminals groups in visited network as well as joint (linked) groups, like joining the groups of home network. In the Tetrapol presupposed solution, the interface to the control room will be exploited to achieve the connection between the network and the gateway.

C. Functional Requirements for Terminal

1) Features for Migration

TETRA/Tetrapol terminals should include migration support, as defined in TETRA/Tetrapol standards, to visited network. It has to be ensured that the needed features are supported by the visited network and the terminals in the visited network. Considered features are: authentication, AI Encryption, E2E Encryption, group call, individual call, telephone call, emergency call, status, SDS, packet data and AVL.

2) Network Selection

The radios must have to the possibility to favour one network. A manual change must always be possible. This is made because of logging in automatically on the strongest network. The displays of the radios have to show the active network. Identification of a calling team has to be displayed on the radios.

3) Direct Mode

In direct mode of simplex operation, mobile subscriber radio units may communicate to each other by using radio frequencies which may be monitored by but which are outside the control of the TETRA/Tetrapol Trunked network.

In case of different standard (TETRA/Tetrapol) and even in case of different frequency plans inside the same standard, this raises the question of the dual mode terminal. Interoperability between handsets of different standards can only be provided by overlapping, bridged networks or locally through direct mode. More general interoperability, for example roaming, can only be achieved through dual standard appliances. Many recent Public Safety radios use a similar internal architecture for both standards, the differing technical protocols being implemented in firmware. It may therefore be feasible for manufactures to produce a dual standard option at an affordable price, or even upgrade existing appliances with new firmware. This task will consist in a feasibility study to assess options for bringing dual standard handsets to the market, and resolve any licensing issue this might imply.

4) Phonebook Associations

It is supposed that cross border operations are not performed as daily basis (except concerning customs personals) so fixed phonebook associations are needed for seamless communications (SDS, talk) between different parties.

D. Non-Functional Requirements

Non-functional requirement focus on how the system should perform the specific operation instead of what the system can do. Performance, reliability, availability, security, maintainability and portability are some of non-functional requirement approach discussed in the following chapter. Although non-functional requirement are stated below, measurement of the requirements should be declared in order to analyze, verify, and to meet the needed non-functional requirements.

1) Performance

The system should meet the following performance parameters (ETSI TR 101 448 V1.1.1); the group call setup delay should be less than 1,0 seconds, 95 % of the setups should be within the specified time, the end-to-end audio delay experienced by the users for calls without end-to-end encryption over the ISI should not be higher than 0,7 seconds and the initial migration registration procedure (including authentication) to a foreign network should not take more than a few seconds longer than the first registration (including authentication) on the home network radio

2) Reliability and availability

Physical connections for ISI-interfaces should be provided by reliable and secure service provider (same as in home network).

3) Security

The link of the ISI-interface between SwMIs should be encrypted. The visited network should fulfill the same security standards as home network.

VII. CONCLUSIONS

The MACICO project implements the latest version of ISI interface (ISI phase 2) on top of TETRA architecture. MACICO also creates scenarios and user requirements for implementation and demonstrations. The research process of capturing the end user requirements showed that the role of the researcher may differ depending on the context. User requirements are based on results of previous projects, end user interviews and discussions with technical experts.

The MACICO project is innovative because it addresses not only the interoperability issue, but also the complete procedure that accepts foreign users on a security radio network (which is a priori forbidden for them) and looks for a solution that keeps the intrinsic security mechanisms of such networks. Moreover MACICO paves the way towards the development of strong and meaningful interactions between narrowband public safety and LTE broad band networks.

However, the operational procedures of first responders vary a lot within each country. Before it is possible to standardize these procedures, much interdisciplinary research and development work is needed.

References:

[1] CELTIC-Plus, MACICO Project Information [online] Available: http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp
[2] G. Lyberopoulos, K. Filis, I. Mesogiti, E. Theodoropoulou, G. Korinthios, E. Nikolitsa, F. Liberal, J.O. Fajado, M. Ramos, "Emergency Communications: Current State and Users' Requirements", GERYON_DR_D2.1_v1.0.docx, 2012.
[3] P. Kämppi, J. Tyni, Jyri Rajamäki. (2014) Uses Cases of the Multi-Agency Cooperation in Cross-border Operations (MACICO) project. 8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST14)
[4] P. Kämppi, M. Aro, J. Rajamäki. (2014) End-User Requirements for Multi-Agency Cooperation in Cross-border Operations (MACICO) Project. 8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST14)
[5] C. Patriakis, D. Salama et al. (2012) SARACEN-project. D2.1e End – User Requirements with respect to 3D services. Available: http://ec.europa.eu/information_society/apps/projects/logos/4/248474/080/deliverables/001_D21eEndUserrequirementswithrespectto3Dservicesv60pdf1.pdf
[6] R. Pirinen & M. Fränti (2008) Framework and Culture of Proactive Competencies Learning. Learning by Developing (LbD) Proceedings of the 7th WSEAS International Conference on EDUCATION and EDUCATIONAL TECHNOLOGY (EDU'08) Available:http://www.wseas.us/e-library/conferences/2008/venice/edu/edu14.pdf
[7] R. Pirinen (2009) *Thematic Curriculum.* Proceedings of the 8th WSEAS International Conference on EDUCATION and EDUCATIONAL TECHNOLOGY
[8] Three-Country Pilot. *Final report Three-Country Pilot 'first phase'* November 2003. Available: http://www.iwi.uni-hannover.de/lv/seminar_ss04/www/Martin_Bretschneider/bibliography/BMIThreeCountry03.pdf

Pasi P. Kämppi was born in Varkaus, Finland on 11th December 1973. His educational background is presented in chronological order: B.Sc. in telecommunications, University of Applied Sciences, Kotka, Finland, 1996; Sergeant in signal corps, The Finnish Defense Forces, 1997; MBA (BIT), Laurea University of Applied Sciences, Espoo, Finland, 2011. Currently he is studying in HAMK University of Applied Sciences in Professional Teacher Education Unit. He also holds Juniper JNCIA-EX certification on year 2009.

He has been working with telecommunications since 1997. He started his career on 1997 in Nokia Networks as Testing Engineer and he had several positions like Senior Testing Engineer, System Specialist and Senior System Specialist in Nokia Siemens Networks. His responsibility was packet switched mobile networks and IP networking. He has deployed many technologies for field testing including 3G, UMA, WiMAX and LTE. On 2011-2012 he worked as network consultant in Qentinel. Since 2012 he has been working as project manager, researcher and lecturer in Laurea University of Applied Sciences. Currently he is in active role in MOBI- and MACICO-projects. He has also authored many ICT, telecommunications and public safety related scientific publications.

Jaakko Tyni was born in Veteli, Finland on 14th of November 1974. He graduated from University of Helsinki in 2004, with Social Ethics as a major subject. Last four years he has worked in Laurea University of Applied Sciences in different positions. He has been a researcher in several projects in the field of safety and security, for example RIESCA (Rescuing of Intelligence and Electronic Security Core Applications) 2009-2010, SATERISK (Satellite Tracking Risks) 2009-2011, PERSEUS 2010-2014 and MACICO-project (2011-2014). Mr. Tyni acts currently as a Chief Research and Development Officer in Laurea.

Jyri Rajamäki received his M.Sc. (Tech.) degree in electrical engineering from Helsinki University of Technology, Finland in 1991, and Lic.Sc. (Tech.) and D.Sc. (Tech.) degrees in electrical and communications engineering from Helsinki University of Technology in 2000 and 2002, respectively.

From 1986 to 1996 he works for Telecom Finland being Development Manager since 1995. From 1996 to 2006 he acted as Senior Safety Engineer and Chief Engineer for the Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006 he has been a Principal Lecturer at Laurea University of Applied Sciences, Espoo, Finland, where he also serves as a Head of Laurea's Data Networks Laboratory ´SIDLabs Networks´. His research interests are electromagnetic compatibility (EMC) as well as ICT systems for private and public safety and security services. He has authored about 90 scientific publications.

Dr. Rajamäki has been an active actor in the field of electro technical standardization. He was 17 years the secretary or a member of Finnish national committee NC 77 on EMC, ten years a member of NC CISPR and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was also the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Dr. Rajamäki has been the scientist in charge for several research projects funded by Tekes – the Finnish Funding Agency for Technology and Innovation, industry and EURESCOM. He is currently the scientific supervisor and director of one CELTIC Plus and one Tekes project.