PROJECT FINAL REPORT

Grant Agreement number: 285 205

Project acronym: FREESIC

Project title: Free Secure Interoperable Communications

Funding Scheme: FP7-CP-FP

Period covered: from 01/02/2012 to 31/07/2014

Name of the scientific representative of the project's co-ordinator[1], Title and Organisation: Mr. Stefan Vanya, Ardaco, a.s.

Tel: +421 2 3221 2311

Fax:

E-mail: stefan.vanya@ardaco.com

Project website address: www.freesic.eu

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

4.1 Final publishable summary report

- **An executive summary**

The principal motivation for the FREESIC project arises from issues identified during the work on the SECRICOM Project where the majority of FREESIC partners were involved. The SECRICOM Project identified legal, organizational and operational barriers that negatively impacted on effective multi-agency interoperability during crisis events. Even when an efficient technical solution such as SECRICOM was being used, these barriers were never overcome totally.
To break through these barriers the FREESIC project proposes a solution with several innovative aspects such as a network of networks concept as well as a generic WEB 2.0 (do it yourself) approach. The solution is based on a universal gateway with customizable adapters that enable third party infrastructures to be connected to the FREESIC Unified Communication Network. From the user perspective network management tasks will be facilitated through the Collaboration Site based on WEB 2.0 components that allow end-users to configure their own interoperability attributes. Another aspect of the FREESIC project is the focus on potential end-user expectations, habits and constraints. These features make the FREESIC solution unique and suggest it has high exploitation potential.
Emergency responder organizations are facing challenges with increasing levels of complexity; this greater complexity in turn leads to responding agencies and their actors adopting greater specializations, and the greater the specialization, the more the structure of responders is segmented. This then, inevitably leads to the need for more effective intra and inter agency interoperability. However, at the same time these agencies are facing budgetary limitations inhibiting the implementation of one-purpose solutions. The FREESIC has recognized this and proposed a cost-effective solution using existing communication infrastructures already deployed by organizations. These infrastructures can be integrated to FREESIC Unified Communication Network with minor implementation effort using the sample implementations provided.
Because of the generic WEB 2.0 (do it yourself) approach the FREESIC provides a system built-in democracy of the interoperability organization. This, together with the user focuses and cost effectiveness, provides a solid base for the concept to become one of the major interoperability tools in Europe and beyond.

- **A summary description of project context and objectives**

FREESIC context:

The basic idea of the FREESIC is a kind of unification of a telephone exchange system with socio-professional networking. Interested professional organisations are then able to interconnect their professional communication systems while the links among the different organisations are created in a way similar to well-known social networking systems.

©John Cooper 1937 Telephone Exchange

See Figure 1: FREESIC idea is based on the unification of telephone exchange systems with the socio-professional networking systems

The organisations connected to the FREESIC are still using their own existing communication systems. It should also be stated that FREESIC has no intentions of modifying an agency's internal processes and procedures nor of replacing existing communication infrastructures deployed in an organisation. FREESIC demonstrates it worth when agencies need to interoperate. When this need to work together arise **the FREESIC system provides an interoperability platform with transparent interoperability rules** enabling interconnection of organizations' communication systems and thus facilitating the required information exchange

The overall visions of the FREESIC project can be summarized in the following ideas:

- The building of a collaboration network of emergency responder agencies across borders prior to major event activation
- Systematic mapping of constraints (cultural, legal, technical) that currently hinder the close cooperation of different responder agencies and tracking of improvements as they are implemented.
- Interconnection of responder agency communication systems without major investment and close to zero operational costs
- Agencies being able to join FREESIC and to stay connected without major investments

FREESIC objectives:

The chapter repeats the objectives from FREESIC DoW document

Objective 1: Solve the legal, security, reliability and operational issues

The interoperability is not only about a technical solution, the legal, security and operational issues might stop the initiative even if the best technical solution exists. We plan to address these issues soon in the project life. The communication systems of emergency responders are critical for their work and that is why such systems are being adequately protected either by security mechanisms, organizational procedures or by law, e.g. in Slovak Republic the systems are part of national critical infrastructure, certified for transmission of classified information and the technical details are classified. The interoperability between such systems is not just a question of technical feasibility of such integration but more about demonstrating that the other systems will not threaten the operational readiness, security or reliability of the emergency communication system.

The success criteria are:

- The concerns, legal limitations, reliability attributes and risks are documented in a single document, containing the inputs from multiple EU member states
- The solution for each of those issues is documented in a report and its annexes (the solution does not have to be technical, could be organizational etc.)

Objective 2: Bring the interoperability communication platform to life

The communication services should be based on data types not technology (service oriented architecture). For example if one system publishes its capabilities (e.g.: text, call, PTT) it should not matter what is the source technology. It must be possible to send the text to the system (e.g. to a Tetra handset) even if the source is from e-mail, SMS or web form. The transcoding and technical restrictions (e.g. the maximum text length of 160characters) should be handled by the gateway.

The success criteria are:

- The servers are running and accessible from the internet
- The SECRICOM devices and software modules are able to connect to the platform and use its services to communicate between each other
- The web pages for configuration of access rights exist and allow each agency to configure which FREESIC users are allowed to communicate with the agency
- At least one sensor or non-human communication system is connected to demonstrate interoperability of equipment too
- The performance issues have been solved and the system is acceptable for end user's needs

Objective 3: Publish the open source gateway and documentation

Most agencies have already made significant investments to their communication infrastructure and their systems usually provide a good service for the users of the same organization. The generic open source gateway should provide easy means for them or their system integrators to integrate their current or future communication systems with other local agencies or foreign agencies. They

are the ones who know their communication system the best and the gateway should provide them all the necessary information, technology and source code to make the integration doable without additional knowledge. Every agency should only need to integrate once, to the FREESIC, they do not have to invest significant resources to develop ISIs[2] between every other system they might need today or in the future.

The success criteria are:

- A free libraries and open source code exist for Linux platform at least (other operating systems are optional)
- The gateway provides methods for establishing the full-duplex phone call, push-to-talk group communication and text message exchange at least (the CCTV or video conferencing is optional)
- The security modules that ensure information confidentiality, integrity and authenticity are open source so that the organization can review it to gain their trust
- The overall security mechanisms and modules have been evaluated by reputable institution (in case of our project it is the task of NSA)

Objective 4: Integrate the first users

The end users are not only the well known emergency responders such as police, fire brigade or ambulance. There are tens of other agencies that participate during major incidents. E.g.: Environment protection experts, civil protection, chemical labs, electrical distribution / power plant operators, gas distribution companies, national guard who help to respond to emergencies and disasters, such as hurricanes, floods, and earthquakes.

The success criteria are:

- At least 3 different agencies from 3 different countries integrated into the FREESIC communication network
- There should be at least two different types of communication systems integrated into the FREESIC platform (e.g.: telephony and radios - Tetrapol)

Objective 5: Establish Europe wide cooperation and awareness about FREESIC

To be truly successful we need to cooperate with other research activities, experts and spread Europe awareness about the free interoperability project. Our partners UL, BACPO and ITTI are institutional members of international forum Public Safety Communications Europe (PSCE) or local public bodies that provide recommendations to agencies (National Security Authority, British Association of Public Safety Officers). They are active in the Research Committee and will contribute to the bodies like Industrial Mission Group for Security.

The success criteria are:

- Participate on at least one other relevant research project event/meeting a year
- At least one presentation a year on an international conference dedicated to communication or crises management such as PSC Europe forum

[2] Interoperable System Interfaces

- Participate as an exhibitor on at least one international show a year (e.g.: BAPCO Show, MILIPOL Paris etc.)
- At least one workshop for a closed group of experts and end users
- Presence on the widely used social networks (Linked-In, Facebook)

- **A description of the main S&T results/foregrounds**

Getting closer to PPDR organisations:

The FREESIC consortium had as part of its overall strategy an intention - which it achieved - to engage meaningfully with Users on an ongoing basis throughout the duration of the Project. The Project was seeking genuine two-way discussions to obtain valued user contributions at all stages of its progress. The breadth, depth and variety of this User engagement - across several EU states, with a wide variety of agencies in different environments - contributed greatly to the overall Project deliverables and outcomes.

As regards breadth of User engagement the following 9 countries were involved in consultation and discussions at various stages throughout the Project's duration:-

- Czech Republic
- Germany
- Luxembourg
- Poland
- Slovakia
- Spain
- Sweden
- UK
- USA

Such is the nature of the public safety environment that occasions arose due to operational commitments when planned User engagement was not achieved e.g. a selected Dutch User representative being unable to attend the T3.1 International Validation Exercise in Manchester UK in April 2013 (M14) because of a Dutch royal wedding. In a similar vein the Project adopted a flexible and understanding approach when engaging with Users in Poland (during the Euro 2012 Football Championships) Slovakia, (General Election 2012) and the UK (London 2012 Olympics); this sympathetic Project approach reaped its benefits with good quality ongoing User inputs when they did become available as the Users appreciated our insight into their challenges and problems and our intention to work around them for the benefit of all parties concerned.

The project sought engagement with several types of agencies with a view to obtaining contributions and insights from a range of different emergency/first responder/security agencies at strategic management level through to field commander roles together with agency ICT specialists. This ensured we had a depth of engagement that represented different PPDR disciplines from across Europe, and indeed the USA that offered different operational command level perspectives yet resulted in re-assuringly similar themes that the project was able to draw together in the requirements identification phases.

The following types of organisations were involved as FREESIC end-users or influencers:

- Ambulance/Health,
- Armed Forces,
- Civil Protection,
- Fire.
- Police
- National Agency Security Specialists,
- Academics,

- National Agency/Government level engagement - Czech Republic, Luxembourg, Poland, Sweden, Slovakia, UK,
- Regional Agency/Government level engagement- Poland, Spain & UK,

In terms of the range and types of User focused events project partners conducted the following different activities:-

- 4 Field Test Demonstrations – Nitra-Slovakia M14 (FREESIC Nitra 2013 exercise), London M22 (B-APCO conference), Paris M22 (MiliPol exhibition) and Final field testing in Luxembourg in M29,
- 17 Formal Meetings,
- 14 Workshops,
- 13 1-2-1 meetings,
- 3 Trade Exhibitions,

The above shows how flexible the project was in engaging with PPDR professionals both in terms of 'best fit' with individuals' and agencies' availability and the needs of the project at any particular point in its life-cycle.

Use of results:

The relationships that the members of the FREESIC consortium established with these agencies represent an important foreground for further exploitation for the aims of further R&D or scientific activities as well as are opening the doors for commercial exploitation by the SMEs, partners in the FREESIC consortia.

Non-technical foregrounds of the FREESIC research:

The principal goal of the FREESIC project was the definition and implementation of a technical infrastructure that seamlessly resolved different non-technical barriers inhibiting effective interoperability between PPDR agencies - such barriers can be cultural, procedural, legal, security related, commercially based as well as technical. Consequently the consortium conducted a detailed mapping of these barriers. This research included:

- Activities organised with end-users, as listed above, ,
- 20 crisis events from across the EU were reviewed,
- 20 relevant projects were researched.

By undertaking this approach of user engagement and overlaying it with some academic research and intellectual findings the project was able to obtain sufficient relevant material to inform the project's User requirements needs and issues; this despite very real concerns from several agency individuals about releasing information to the project that might negatively impact on public safety and security, public confidence in PPDR organisations and on occasion commercial confidentialities as regards current agency communication systems suppliers.
.

Based on the aforementioned material a set of operational procedures, guidelines and recommendations were elaborated for the FREESIC system consisting of the following parts:

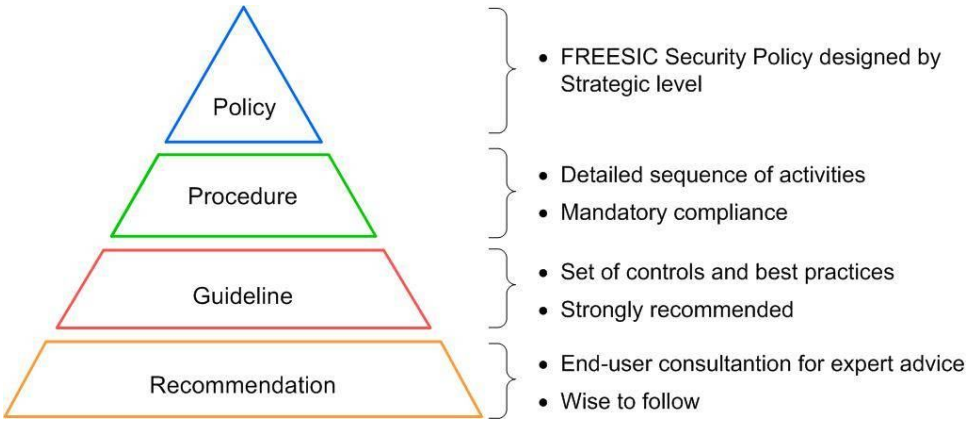


Figure 2 FREESIC Non-Technical Approach

Recommendations incorporating the advice from end user consultation of experienced practitioners to enhance interoperability. Their non-compliance or lack of implementation being viewed as not critically affecting the success of FREESIC but nevertheless it is considered wise to follow them. These recommendations shaped the operational guidelines and procedure design.

Guidelines defining a set of strongly recommended best practices on when and how to employ interoperability aspects. They aim to provide a unified framework for working together in crisis situations that enhances communications and coordination in multi-agency incidents.

Procedures defining mandatory protocols to support the application of interoperability guidelines and maximise operational capabilities and resources provided by FREESIC. These procedures are relevant for the entire lifecycle of a crisis in terms of previous preparation configuration activities, interoperability invocation, and operation during a crisis and incident debriefing.

Policy being defined at strategic level as the mission and general principles for the operation of FREESIC, providing the framework for the aforementioned guidelines and procedures to be defined.

The project is particularly proud of the achievement that the set of operational procedures provides a step-by-step guidance on how to use the FREESIC platform during a live incident through to event closure. They specify how to integrate into the system; to configure interoperability preferences and to regulate the information exchange.

PREPARATION PHASE
OP-01: Register an agency in the FREESIC system
OP-01.1: Register on FREESIC collaboration web
OP-01.2: Create agency profile
OP-01.3: Register communication system
OP-01.4: Edit communication system
OP-01.5: Remove communication system
OP-01.6: Define role
OP-01.7: Edit role
OP-01.8: Remove role

OP-02: Configure communication preferences
OP-02.1: Request partnership
OP-02.2: Accept / reject partnership
OP-02.3: Remove partnership
OP-02.4: Create talk group
OP-02.5: Edit talk group
OP-02.6: Remove talk group
OP-02.7: Create scenario
OP-02.8: Edit scenario
OP-02.9: Remove scenario
OP-02.10: Configure individual call permissions
OP-02.11: Edit individual call permissions

OP-03: Deploy FREESIC Local Gateway
OP-03.1: Request access to FREESIC development space
OP-03.2: Connect to FREESIC development space
OP-03.3: Prepare local development environment
OP-03.4: Adapt FREESIC source code (if necessary)
OP-03.5: Configure FREESIC local gateway

OPERATION PHASE
OP-04: Invoke Interoperability
OP-04.1: Start gateway
OP-04.2: Start preconfigured talk groups

OP-05: Operation during ongoing incident
OP-05.1: Create talk group
OP-05.2: Edit talk group
OP-05.3: Remove talk group
OP-05.4: Configure individual call permissions
OP-05.5: Remove individual call permissions

RESOLUTION PHASE
OP-06: Discontinue communications
OP-06.1: Stop active talk groups
OP-06.2: Stop gateway

Figure 3 Operational Procedures covering the whole life of an incident

PROCEDURE PHASE	
Procedure ID:	OP-01.1
Procedure Name:	Register on FREESIC collaboration web
Owner:	Nextel S.A.
Procedure Version number:	1.0
Date issued:	2014/04/30
Description:	This procedure describes the process of requesting authorization to access to the FREESIC Collaboration Web
Objectives:	To confirm that the Agency is a valid user of the FREESIC Collaboration Web and validate access to it.
Actors:	Agency LEAR FREESIC admin
Note:	NA
Conditions for procedure initiation:	NA
Events triggering the use of this procedure:	NA
Procedure steps:	1. Go to the FREESIC Collaboration Web 2. Click on "Register New Account" 3. Fill in the form with the Agency information 4. Click on "Send" 5. A mail will be received on the specified address with the FREESIC admin approval
Expected result:	The Agency gets authorization to login on the FREESIC Collaboration Web.
Attachments:	FREESIC Collaboration Web: http://collaboration2.freesic.eu/Freesic/

Figure 4 Example of an Operational Procedure - How to register on the FREESIC Collaboration Web

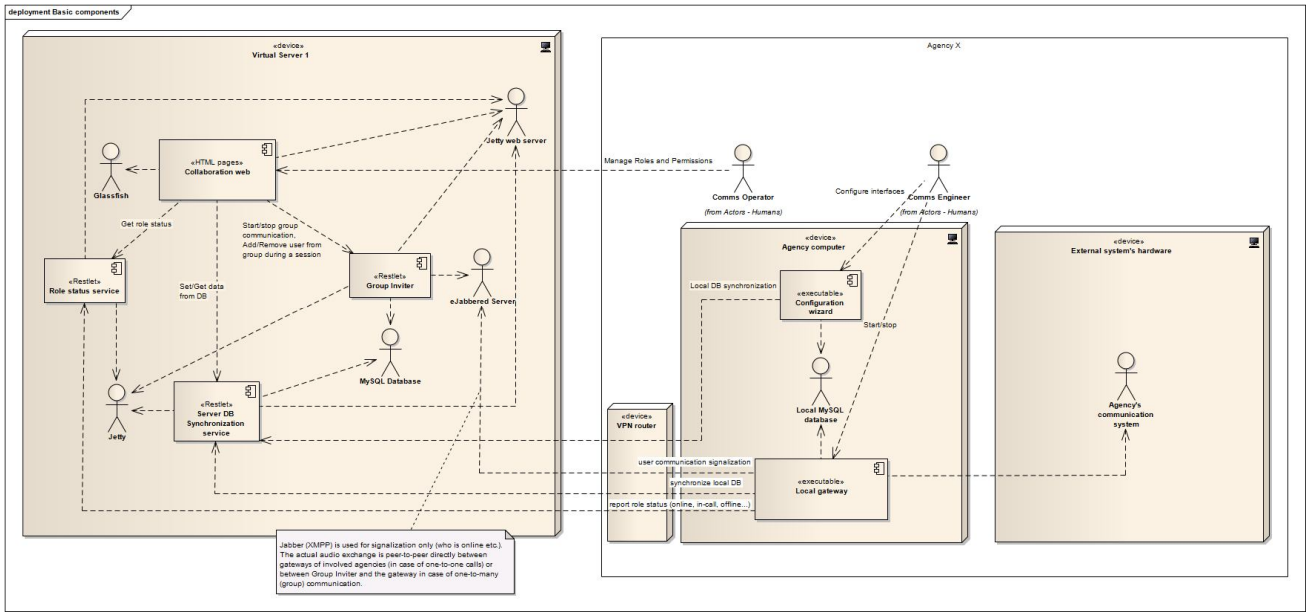
Use of results:
The developed procedures, guidelines and recommendations manual together with the identified and researched interoperability barriers provided an excellent knowledge base for the project to draw upon as it undertook its planned technical research and development

Technical achievements:

The FREESIC architecture was significantly modified for the resolution of findings observed at the field test in NITRA. As a result of these modifications ejabberd XMPP platform was used as FREESIC core communication server. The choice of ejabberd brought several advantages such as:

- fully open source system,
- protocols based on well established standards (XMPP),
- fully scalable solution,
- preparedness for data other than voice.

The audio communication was implemented using open jitsi libraries. The audio channels are established peer-to-peer which means no communication overload on the communication server which processes only the signalling messages. The choice of ejabberd also enables the deployment of the FREESIC core in the cloud. The high level architecture of the final deployment is indicated in the figure bellow.



See Figure 5 FREESIC final deployment

The solution consists of:

1. COTS[3] jabber server (ejabberd) acting as communication core for FREESIC signalling messages,
2. COTS database (MySQL) that is used to store system configurations,
3. COTS web server (jetty) to host the FREESIC collaboration web,
4. COTS Java application server (Glassfish) executing the FREESIC collaboration web services,

   Note: All the COTS components are open source and freeware.

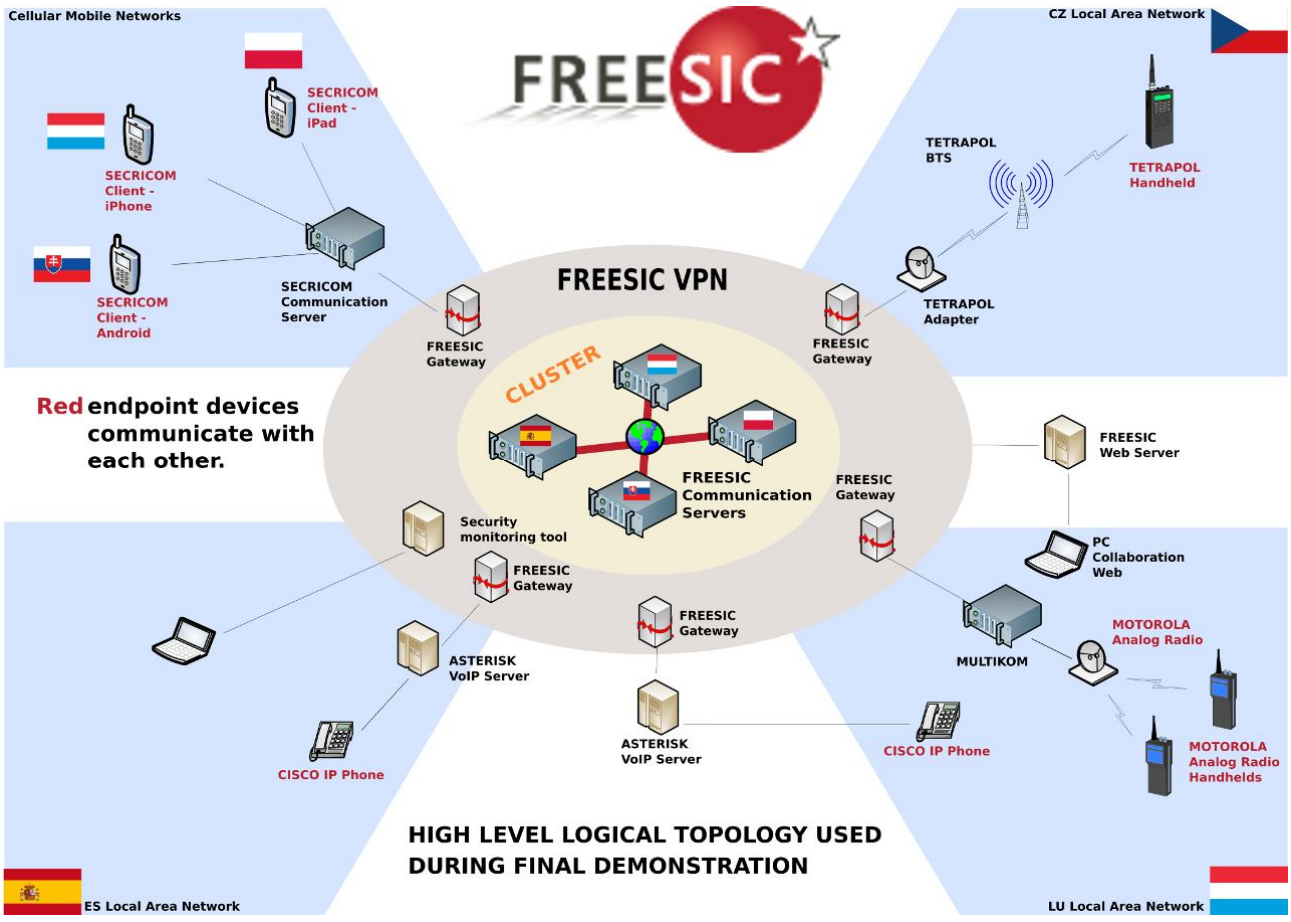
5. FREESIC Collaboration Web (on JSP technology) that is used for decentralised management of the inter-agency communications,
6. FREESIC Group inviter connected to collaboration web to manage the inter-agency talk groups,
7. Role status service accounting the status of different roles registered in the FREESIC (online, offline, unknown);
8. Server DB synchronization service to synchronise the configurations of the gateways with the central configuration DB.

[3] COTS - Commercial of the shelf

Upon successful implementation of the core components the interoperability of the following technologies has been proven using the XMPP core:

- Secricom,
- VoIP (Asterisk),
- Tetrapol,
- Motorola radio

The following schema shows the final deployment of FREESIC interoperability system (the one used at field test in Luxembourg).



See Figure 6 FREESIC final deployment

We have successfully prepared and thoroughly tested complete framework for implementation of gateways to various communication systems. As a product of implementation and testing process have been created detailed step by step guides leading any implementing party to the succesfull result.

Some functionalities proprietary in one communication infrastructure may be missing and not be easy to implement in other – e.g. full duplex communication shall not be available at all; and ex post implementation in half duplex networks may be extremely complicated.

Freesic general and fully open architecture allows incorporate communication network with partial support of whole Freesic functionality range. Freesic offers partial integration of it functionality, too. There is no imperative to implement whole Freesic functionality spectrum to newly added communication systems. It's necessary to concern to basic communication functionality (e.g. PTT signalization, half duplex voice transmission and etc.), mainly in early implementation phases.

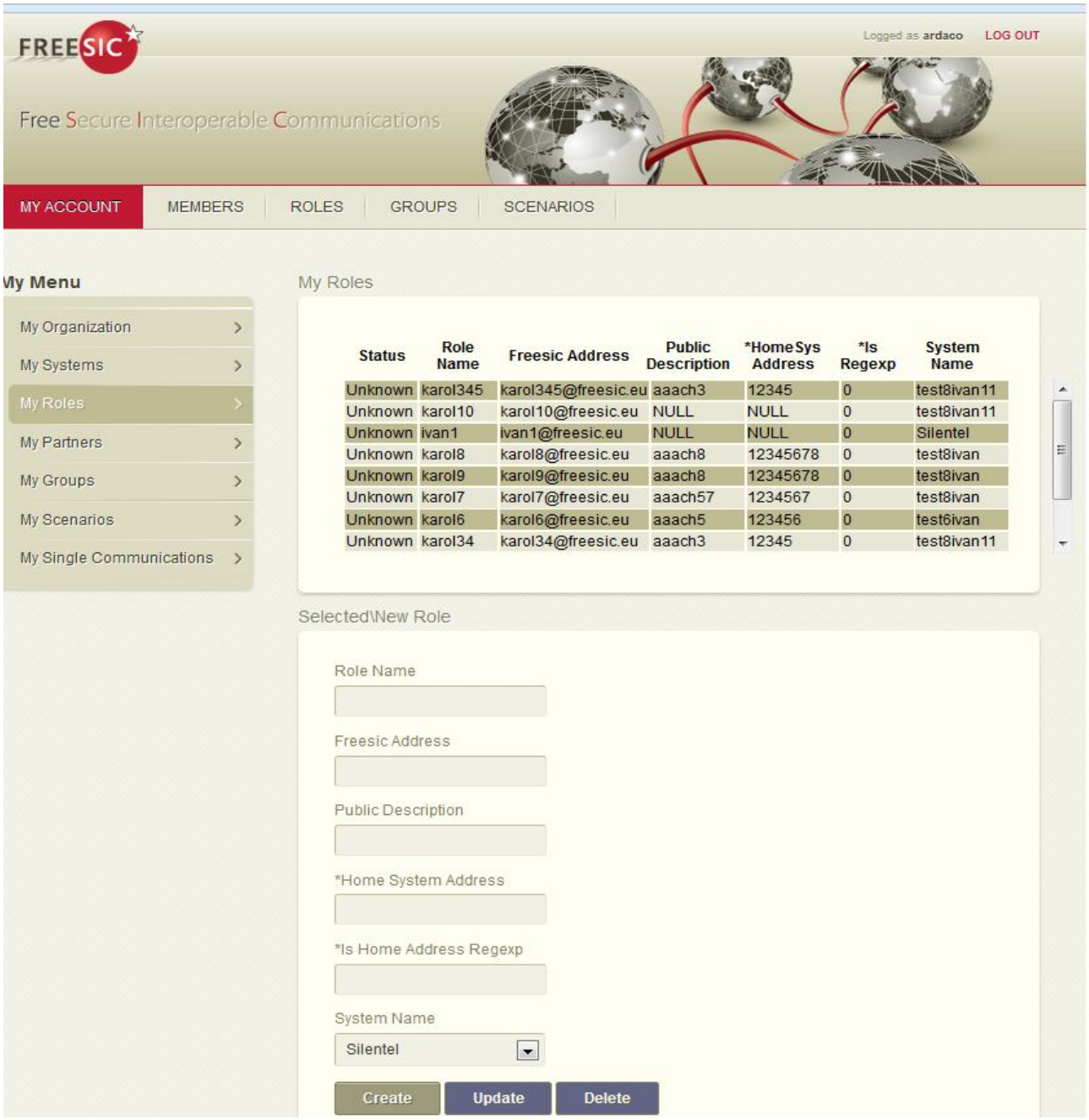
The respect for non blocking operation and thread safe programming are other key points which shall value every Freesic gateway programmer. All gateway functions marked as non blocking must be carefully verified and tested to accomplish this.

Same kind of attention requires multi thread operations which may be required by programming language nature e.g. Java or general non blocking operation request (e.g. TCP or serial link communication handling).

Lot of potential problems may be induced by different hardware difficulties which are hard to detect especially when they generate pseudo software problems. We met with many broken devices, cable and connector disconnections and closed communication ports during gateways implementation and testing. In many cases we are trying to find software error without result when solution was in hardware part. It is crucial to test whole chain from network (internet) connection, over software implementation to last hardware device when any mysterious problems occur.

The collaboration web

Collaboration web is running under page http://collaboration.freesic.eu:8080/Freesic/ . (for testing purposes the following credentials can be used - user: YA1, password: adg12). The picture bellow shows a screenshot of the FREESIC collaboration web:



See Figure 7 - The adding of further roles to a PTT talk group using the FREESIC collaboration web. Among the available roles there are also the ones of partner entities

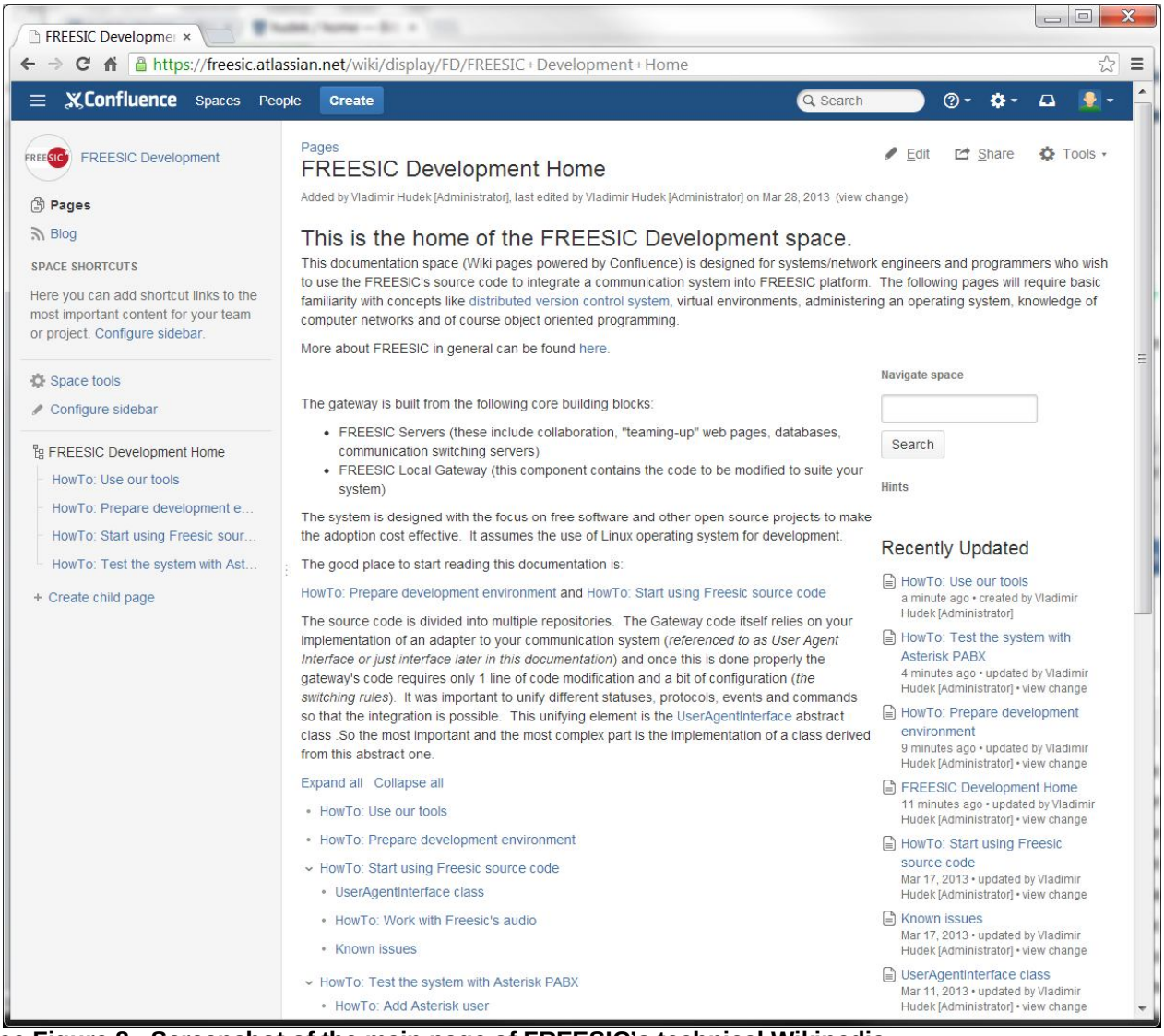
The FREESIC collaboration web represents one of the core components of the FREESIC concept of decentralised interoperability platform. Using the FREESIC collaboration web the users can create their FREESIC roles that can potentially interoperate with the roles of other agencies.

The FREESIC Gateway

Upon creation of roles the participating agencies can ask their system integrators to develop adapters to the open FREESIC gateway that is available for them with sample implementations on the corresponding FREESIC Development Space Wiki pages with all the corresponding technical documentation. They are written in technical language and expect that the users are familiar with

FREESIC and have good knowledge of computer networks, system administration and object oriented programming.

Source: https://freesic.atlassian.net/wiki/display/FD/FREESIC+Development+Home



See Figure 8 - Screenshot of the main page of FREESIC's technical Wikipedia
(The credentials to the web have been provided to project partners, REA and reviewers)

Once the agency implemented the gateway configured the right way, it gained the interoperability with any other agency connected to the FREESIC.

<u>The FREESIC security features:</u>

The FREESIC security concept is based on a distributed VPN network between the participating agencies using Cisco VPN routers and Open VPN clients installed on the servers. The overall security attributes of the FREESIC interoperability platform were documented (in document "D5.3 The system security evaluation report") and reviewed by Slovak National Security Agency for compliance with the technical standards required for restricted level. In the earlier phases of the project it was recognized that stricter classification levels are practically unrealistic to be achieved for such international multi-agency system.

Note: Higher classification levels could be achieved with a completely decentralised interoperability platform consisting of a unified interface between agencies. Such interoperability system would work without any or with very basic central parts (databases, servers) and all the communications would be resolved in a decentralized way. Although, the implementation of such system was out of the FREESIC project scope, it can be the base for a further R&D project.

The NSA stated that system can be used for the processing of non-classified information and provided recommendation for eventual certification of the system on level RESTRICTED.

Although, the use of XMPP core allows the application of end-to-end encryption from gateway to gateway, we decided for VPN option at the demonstration and operation to avoid problems with firewall settings at the participating organisations. Nevertheless, according NSA recommendation **for the certification of the system on level RESTRICTED, the agency firewalls shall be set enabling point-to-point communication between the agencies and then XMPP end-to-end encryption shall be applied**.

Regarding Security Monitoring aspects, a "Security Monitoring Tool" was deployed by Nextel on the demo architecture during the Final Filed Test that took place in Luxemburg the 5th June 2014.

The Security Monitoring tool is structured in a distributed architecture, with several sensors gathering security information from different segments of the network and providing it to a central server that analyses, correlates and displays the security status to the user. This is achieved through the following capabilities:

- Discovery and inventory of network assets
- Host and service detail and availability monitoring
- Network Monitoring
  - Usage
  - Latency tracking
- Vulnerability Discovery
- Anomaly and Intrusion detection
- Security events management
  - Security policies
  - Correlation rules
- Alarm generation

The security monitoring tool being deployed in the Spanish site, the scope of the surveillance included the Spanish demo site and the VPN connections to remote sites in Luxemburg, Poland, Slovakia, Czech Republic and some devices in the cloud.

There is a "Final Field Test Security Report" that provides the security analysis performed with the data gathered by the Security Monitoring tool during the Final Field Test.

Verification of system performance:

The full description and the detailed description of performance tests can be found in "D6.2 - The final test report ANNEX E– FREESIC Performance and Load".

As results of the load tests we can estimate that current system configuration would be able to handle approx. 10 concurrent talk-groups with 15 members each (150 users talking) and would consume 350MB of system memory.

- **Highlight clearly significant results;**

- The FREESIC collaboration web was and continues to be interconnected with the communication core and available on the internet (http://collaboration.freesic.eu:8080/Freesic/).

- FREESIC with its XMPP core was implemented and demonstrated at exhibitions during BAPCO 2013 in UK and MILIPOL 2013 in France. Moreover the solution was also successfully demonstrated in Luxembourg at the final field demonstration test in June 2014 to an international end-user audience. The new solution has shown the potential to remove the principal bottlenecks that were present in the SECRICOM based solution (E.g. the ejabberd based solution is fully scalable, can be implemented in the cloud and the system to system voice delay is reduced to less than 0,5 second),

The most significant result is the demonstration of the decentralized interoperability concept that enables bilateral agreements among agencies on interoperability, resolving the majority of organisational barriers linked with the existing centralised interoperability solutions (E.g. the adhesion to large governmental frame agreements).

* **One of the biggest achievements is successful implementation of fully featured gateway to the PMR TETRAPOL network.**

The implementation have been made with respect to the all communication modes of PMR network as well as security needs of professional emergency forces such as police, fire brigades, health services and others.
Implementation of TETRAPOL technology is particularly very important because this technology is used in more than 80 networks in more than 70 countries all over the world. Some deployments are also used as temporarily installation by special forces.

* **The potential impact (including the socio-economic impact and the wider societal implications of the project so far) and the main dissemination activities and exploitation of results.**

The significant and on-going involvement of end-users, from a wide number of different nationalities, throughout the Project's duration contributed to an internationally accepted resolution of many PPDR interoperability issues. This included engagement with and inputs from the USA during the International Requirement gathering and validation process which extended the European knowledge base in this field - where differing perspectives were offered but also re-assuringly similar resolutions proposed from the transatlantic region. Identification and greater insight of project constraints around: culture, funding & procurement cycles and governance & training limitations brought benefits exceeding the project itself e.g. Elements of the FREESIC documentation regarding interoperability issues and proposed solutions have been used to support a business case for a UK regional multi-agency messaging switching trial.

The concept presented by the FREESIC project-creating fold for modification of the governing centralistic paradigms to decentralised one that can be the future of the approaches for interoperability in further domains. Following the end of the project the majority of the partners continue to further develop the FREESIC concept through cooperation on a recently commenced new project – REDIRNET - which is dedicated to decentralized interoperability of access for sensors, cameras and databases.

Numerous events as listed in part A offered the opportunity to raise the awareness of FREESIC and its capabilities; key events are listed as follows:-

- Presentations to Luxembourg Government,
- Presentation to UK Home Office,
- Presentation at NATO,
- Presentation at Security Essen and Milipol Paris exhibitions

Because of the unique, decentralised WEB 2.0 (do it yourself) approach, the FREESIC provides a system built-in democracy of interoperability organisation. This, together with a user focus and an emphasis on cost effectiveness, provides a solid base for the concept to become one of the major interoperability tools in Europe and beyond.

Further details on exploitation of project results can be found in document "D7.5 - Exploitation Plan Final Update".

Items with exploitation potential are listed in PartB.

* **The address of the project public website, if applicable as well as relevant contact details.**

The project website can be accessed on: http://www.freesic.eu

Contacts:
Project coordinator: Stefan Vanya, email: Stefan.vanya@ardaco.com
Deputy coordinator: Daniela Macakova, email: Daniela.Macakova@ardaco.com

Attached documents: Furthermore, project logo, diagrams or photographs illustrating and promoting the work of the project (including videos, etc…), as well as the list of all beneficiaries with the corresponding contact names can be submitted without any restriction as attachment.