DELIVERABLE D3.3

The Operational Procedures, Guidelines and Recommendations FINAL

Project	Free Secure Interoperable Communication
Acronym	FREESIC
Contract Number	FP7-SEC-285205
Start date of the project	1st February 2012
Duration	30 months, until 31st July 2014

Date of preparation	2014/06/30
Author(s)	Saioa Ros
Responsible of the deliverable	Saioa Ros
Email	sros@nextel.es
Reviewed by	Mikel Uriarte, Oscar López, Shaun O'Neill, Joanna Modlawska, Stefan Vanya
Status of the Document	Final
Version	1.0
Dissemination level (select one)	PU Public

Control changes

Date	Version	Authors	Description
2012/10/31	0.0		D3.1 Interim Version Submission
2013/09/03	0.1	NEX	Reordering and update of inherited contents from D3.1
2013/11/08	0.2	NEX	Contribution to Recommendations section
2014/02/14	0.3	NEX	Contributions and updates to Procedures section General corrections and comments
2014/03/05	0.31	ITTI	Document review
2014/03/08	0.32	BAPCO	Document review
2014/04/02	0.33	NEX	Merge of comments provided by ITTI and BAPCO
2014/05/09	0.4	NEX	FREESIC Security Policy with WCT support Update on Operational Procedures section Creation of ANNEX A - Detailed Operational Procedures, as a separate document
2014/06/13	0.41	BAPCO	B-APCO Final Business and User review
2014/06/30	1.0	NEX	Final version release

Executive Summary

Previous major crisis incidents have demonstrated the need for co-ordinated national and sometimes international responses from a wide range of different agencies. Inherently these agencies have differing legal and regulatory frameworks, information security requirements, business processes and procedures, cultures, and roles & responsibilities. This diversity across agencies can often impact on effective collaboration between them and in particular can negatively affect communication and information exchanges. FREESIC has recognised these risks to inter-agency communications and proposes in WP3 a solution with two approaches; the technical solution (D3.4) and the organisational (non-technical) solution (D3.3).

The technical approach provides a cost-effective solution based on a universal distributed gateway formed by a set of communication servers, interfaces and data exchange services and operated from a web front-end which, with the appropriate configuration, allows interested Agencies to interconnect in a transparent manner with partner organizations and exchange information as required. This is supported by the organisational approach - the focus of this document - which provides the essential principals and good practises for agencies to effectively use the FREESIC system.

The organisational approach first incorporates the recommendations of experienced practitioners drawn from end-user consultation, which provide support to the design of operational guidelines and procedures.

Guidelines define 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. They are described in different communication categories in the field of emergency situations.

Procedures define mandatory protocols to support the application of interoperability guidelines. D3.3 is supported by an ANNEX document that includes a detailed set of operational procedures that provide step-by-step guidance on how to integrate into the FREESIC system, to set up interoperability attributes and to regulate the information exchange. These procedures follow a common template and apply to all phases of a major crisis incident.

A strategic level Security Policy defines the requirements and principles for the operation of FREESIC and thus providing the framework for the definition of the aforementioned guidelines and procedures.

Table of contents

Table of figures

1 Deliverable context

1.1 Deliverable purpose

WP3 aims to provide solutions to the interoperability barriers identified in WP2. *D3.3 – The operational procedures, guidelines and recommendations (Final)* is focused on defining the organisational solution for FREESIC by means of a set of recommendations, guidelines and procedures aimed at enhancing interoperability in emergency communications between different first responders during major incidents.

The main objectives of the deliverable are as follows:

- Utilise the expertise and knowledge gathered from consultation with end users in Europe for shaping the organisational solutions and recommendations for FREESIC.
- Define a set of operational communication procedures and guidelines for the use of the FREESIC system.

1.2 Related documents

- *D3.1 – The operational procedures, guidelines and recommendations (Interim)* [1]: D3.3 builds upon the preliminary work undertaken in D3.1 and updates it with further research results and developmental work conducted in the project.
- *D3.02 – Report on consultation with public authorities* [3]: This internal deliverable resulting from T3.2 – '*Consultation with public authorities, other EU member states'*, provides informed input to D3.3 to support the definition of recommendations.
- *D3.4 – The system architecture document (Final)* [2]: This deliverable provides the operational procedural inputs to D3.3 based upon the designed FREESIC system.
- *D4.1 & D4.2 – FREESIC system release notes* [4]: These two deliverables provide system components release notes so that related procedures can be defined in D3.3.

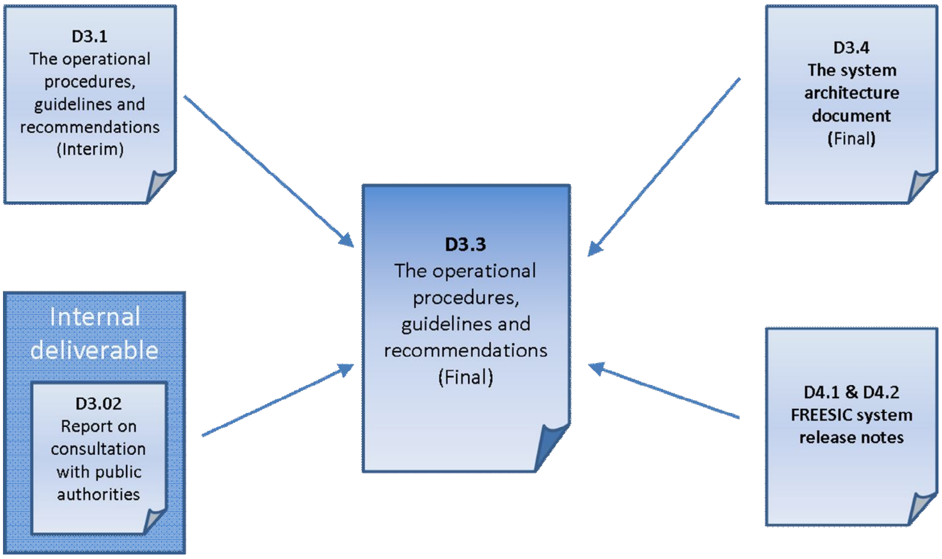
D3.1
The operational procedures, guidelines and recommendations (Interim)
D3.4
The system architecture document (Final)
D3.3
The operational procedures, guidelines and recommendations (Final)
Internal deliverable
D3.02
Report on consultation with public authorities
D4.1 & D4.2
FREESIC system release notes

Figure 1 D3.3 related documents

2 Introduction

Major crisis incidents can cause large scale devastation that inevitably affects the safety of very large numbers of people. Previous events have demonstrated the need for co-ordinated national or even international responses from a wide range of different agencies. These agencies can have differing legal and regulatory frameworks, information security requirements, business processes and procedures, cultures, and roles & responsibilities, all of which can impact on effective collaboration between agencies and in particular affect efficient communication and information exchange.

FREESIC has recognised this and proposes a solution with two approaches; the technical solution and the organisational (non-technical) solution.

The **technical approach** provides a cost-effective solution using existing communication infrastructures already deployed by organisations. It is based on a universal gateway with customisable adapters that enable third party infrastructures to be integrated to the FREESIC Unified Communication Network with minor implementation efforts using the sample implementations provided. From the user perspective network management tasks would be facilitated through the Collaboration Site based on WEB 2.0 components that allow end-users to configure their own interoperability attributes.

This technical approach is supported by the **organisational approach** that provides the essential principals and good practises for agencies to effectively use the FREESIC system. It is based on a set of guidelines and operational procedures that provide a unified framework to interoperate in multi-agency incidents.

However, it is important to note that FREESIC will not interfere with or aim to replace the usual work processes and practices of each agency, it only intends to enhance and complement inter-agency interoperability.

2.1 Organisational Approach Outcomes

The organisational approach consists of defining a set of guidelines and procedures to enhance operational interoperability for PPDR organisations when utilising FREESIC capability. Analogous to ISMS (Information Security Management System) [6], documentation is formally organized as shown in Figure 2, but applied on the emergency interoperability framework.

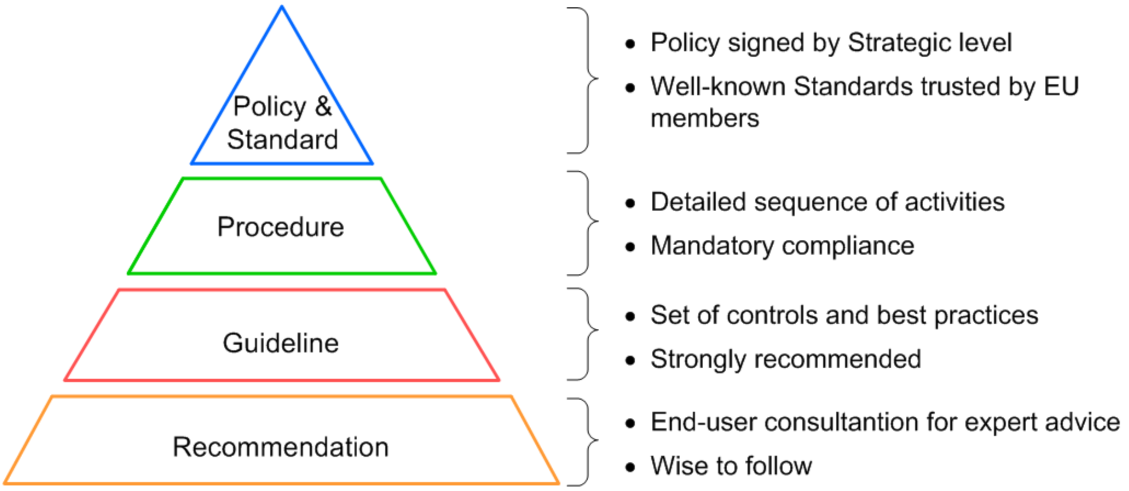
Policy & Standard
Policy signed by Strategic level
Well-known Standards trusted by EU members
Procedure
Detailed sequence of activities
Mandatory compliance
Guideline
Set of controls and best practices
Strongly recommended
Recommendation
End-user consultantion for expert advice
Wise to follow

Figure 2 Interoperability guidelines and procedures framework

Recommendations incorporate the advice of experienced practitioners to enhance interoperability, this advice being the knowledge gathered from end-user consultation. Their non-fulfilment or lack of implementation is viewed as not critical for success but it is wise to follow them. These recommendations should direct the design of operational guidelines and procedures.

Guidelines define 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 define mandatory protocols to support the application of interoperability guidelines and maximise operational capabilities and resources provided by FREESIC. Procedures have to cover the entire lifecycle of a crisis in terms of previous preparation & configuration, interoperability invocation, operation during the crisis and incident debriefing.

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

3 FREESIC Security Policy

FREESIC security policy is the document defined by high strategic level to provide the requirements and principles for a secure and efficient operation of ICT information and infrastructure of FREESIC.

The main objective is to provide the foundation for the creation of required documentation for secure operation of interoperable communications among first responders, such as guidelines, procedures and principles of behavior of users and components of the FREESIC System.

3.1 Scope

This FREESIC Security Policy applies to:

- ICT infrastructure belonging to the FREESIC system
- Information stored or in use by the FREESIC System

3.2 Responsibilities

The Security policy defines the responsibilities of staff and users having access to the FREESIC ICT systems and information.

- The FREESIC security manager: S/he is responsible for defining the security mechanisms that are to be applied and ensuring that they are in place.
- The FREESIC administrator: S/he is responsible information security management through the application of an internal security information management framework.
- The FREESIC user: S/he is responsible for using the FREESIC ICT in compliance with the FREESIC security policy and related guidelines and procedures.

3.3 Principles

The FREESIC Security Policy has the following principles:

- Authorised use

Access to FREESIC ICT resources and information is supported by a user/password access control mechanism. Authorised users are validated by the FREESIC administrator.

- Confidentiality of data

Confidentiality of data is supported by secure SSL connections to information access resources for which FREESIC is responsible.

- Monitoring and reporting

FREESIC reserves the right to monitor the use of ICT systems and information, to ensure compliance with the security policy and may report security incidents when required to the FREESIC Security Manager, so that s/he can decide on the actions to be applied. FREESIC also ensures that information security requirements are communicated to all relevant parties when needed.

- Abuse and misuse

Failure by FREESIC staff and users to comply with the security policy and related documentation may lead to disciplinary actions. Such failures by FREESIC users may lead to the termination of the registration of the user or agency to the FREESIC system.

- Incident management

FREESIC ensures that ICT security breaches or incidents, which may result in loss or damage of FREESIC information and assets, are reported and investigated. FREESIC staff and users have the responsibility to report any security incident identified to the FREESIC administrator. FREESIC will take the appropriate corrective measures to amend the security issue.

- Service continuity

FREESIC envisages service continuity mechanisms, such as satellite connections, to be activated in the event of significant service disruptions.

- Security Policy review

FREESIC will perform periodic reviews of the security policy taking into account relevant security incidents and changes in EU legislation, thus ensuring continued good practices and protection against new threats. Any update on the FREESIC Security Policy will be communicated to all relevant parties.

3.4 Related documentation

FREESIC is committed to the development and review of operational guidelines and procedures on how to use the FREESIC system in an efficient and secure manner. Current supporting documentation is included in *sections 5 Operational Communication Guidelines*, *section 6 Operational Communication Procedures* and *ANNEX A Detailed Operational Procedures*.

4 Operational Communication procedures

This section describes the general process that an end-user has to follow to make use of the FREESIC platform; which is supported by a detailed set of operational procedures that provide a step-by-step guidance on how to integrate into the system, to set up interoperability attributes and to regulate the information exchange.

4.1 General overview

FREESIC is a universal distributed gateway formed by a set of communication servers, interfaces and data exchange services and operated from a web front-end; which, with the appropriate configuration, allows interested Agencies to interconnect in a transparent manner with partner organizations and exchange required information.

Figure 3 presents a simple scheme of the different FREESIC components that the user will have to address in different stages of the implementation and configuration process.

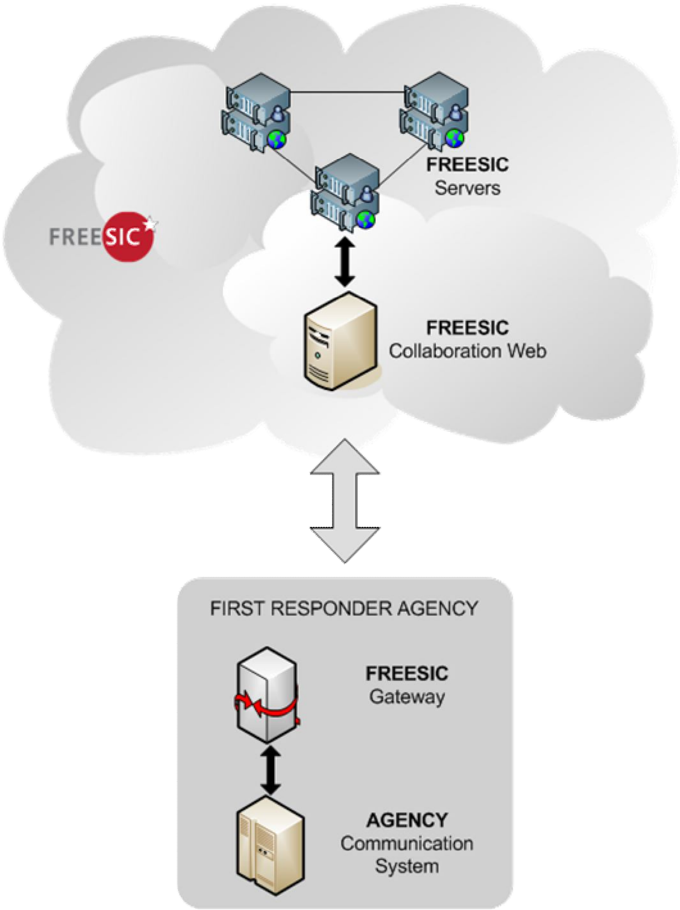

Figure 3 FREESIC Main Components

FREESIC also offers several online support mechanisms for the integration and configuration process, which will be accordingly addresses by operational procedures when needed:

- FREESIC Collaboration Web: http://collaboration.freesic.eu/Freesic/

- FREESIC Development Space: https://freesic.atlassian.net/wiki/display/FD/FREESIC+Development+Home
- FREESIC Source Code Repository: https://bitbucket.org

In order to cover the whole operational life of an incident, procedures are defined in three phases with different procedural requirements:

- **Preparation phase**: This is the phase prior to an incident. It includes integration of agency's communication systems with the FREESIC interfaces, definition of agency profiles, creation of preconfigured groups, etc.
- **Operation phase**: The incident is ongoing. This is the phase where communication systems are exploited during the incident. It includes interoperability activation, communications forwarding, etc.
- **Resolution phase**: It covers the incident closure and return to normality. This phase includes interoperability discontinue, reporting, etc.

Regarding these three phases, the following process has to be followed by First Responder Agencies to operate with the FREESIC system.

Preparation Phase:

1. Register in the FREESIC Collaboration Web
    a. Request an account to the FREESIC system admin and wait for the approval.
    b. Once logged in, register Agency's communication system and users/roles that will be public for other agencies.
2. Configure interoperability and communication preferences.
    a. Ask for partnership to other Agencies registered in the web.
    b. Once partnerships request accepted, configure communication capabilities in terms of talk groups and individual call permissions.
3. Implement a FREESIC Gateway locally on the Agency's premises to interconnect their communication system to the FREESIC platform (FREESIC Servers) through the Internet.
    a. Prepare the development environment that will host the Gateway.
    b. Some precompiled version of the gateway for the most popular IT communication environments are available for download (Asterisk VoIP, Xmpp Jabber, Secricom and Tetrapol). If this is the case just download the corresponding gateway code.
    c. If it is not the case, the gateway source code will have to be adapted to the Agency's communication environment.
    d. Once the Gateway is deployed, configure the interfaces according to the communication preferences defined previously in the Collaboration Web.

Operation Phase:

1. When interconnection among different agencies in a major incident is needed, interoperable communication will be activated in the FREESIC platform according to the communication settings of each organization.
    - e. Start the FREESIC Gateway.
    - f. Start the preconfigured talk-groups.
2. If during the incident the need for new communication requirements is identified, new settings can be configured in the Collaboration Web.
    - a. Define required scenarios, talk-groups and individual calls.
    - b. Start these new elements.

Resolution Phase:

1. When interconnection among different agencies in a major incident is not needed anymore, interoperable communication will be deactivated in the FREESIC platform.
    - c. Stop active talk-groups.
    - d. Stop the FREESIC gateway.

4.2 Procedures overview

Bellow is the detail on the procedures necessary to successfully use the FREESIC system and its components from the initial set-up steps for registration and configuration, through operational use during a live incident, until the event closure.

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

The aforementioned operational procedures are further developed in ANNEX A – Detailed Operational Procedures [14].

5 Operational Communication Guidelines

Guidelines provide a set of strongly recommended controls and best practices that agencies should follow to achieve effective interoperable communications. This section is arranged in several relevant categories aimed at enhancing interoperability for emergency agencies [9][10][12].

5.1 Communication plan

Communication plans are envisaged to support the overall response to an event. When an incident leads to a multi-agency response, each agency has to work towards a common aim and understand each other’s roles, capacity and capabilities in order to operate effectively within their own agency and in partnership with other agencies.

The following considerations should be taken into account when defining communication plans:

- Communication plans are to be defined and agreed between agencies in advance to any operation having been tested in a contingency planning environment whenever possible.
- When developing communication plans, agencies should share with their counterparts the resources and capabilities to be used for their individual command and management structures.
- When developing communication plans, all agencies should have a common understanding of the language used so as to avoid misunderstandings.
- A SLA or memorandum of understanding between partner agencies should be formulated.
- Communication plans must take into account each agency’s limitation and constraints, and assumptions should not be made without confirming capabilities beforehand with each agency involved.
- Communication plans must ensure that optimal use of available talk groups is made, for all types of required communication services.
- Communication plans used in daily operation should allow to be scaled up when required to an inter-agency scale, so that first responders will continue to work as per daily routine.
- During the course of an incident it is essential that a review of the communication plan is carried out at regular intervals or when any change of circumstances arises. Therefore, such plans must be flexible.

5.2 Communication centre

Each responder agency is supported in its response to a major crisis incident by a communication or control centre. These centres are responsible for the management and coordination of communications for their agency and its response and resource deployment to incidents and events.

Considerations regarding communication centres are as follows:

- An overarching coordinating communication centre has to be designated during an incident.
- The overarching coordinating communication centre has to monitor user demand of communications network resources and take corrective action if needed. The coordinating communication centre should prioritize communication and suspend less important usage in order to free resources for more critical communications, if necessary.
- When staff from different responder agencies' communication centres is working together, it is essential that common standards are adopted, such as plain English, the use of readily understood call-signs and common symbols for mapping.
- When possible, at least one communication centre belonging to one of the participating agencies should record communications for audit purposes. These recordings should be available to all agencies if required for subsequent reviews, court proceedings and training purposes.

5.3 Talk groups

A talk group can be described as a communication channel that permits all users using it to exchange information. In terms of communication capabilities, transmission to an open talk group (an interoperability or common talk group) is the most efficient method to communicate with a large group of users responding to an incident. When responding to a major crisis event, interoperability talk groups enable multiple agencies to have dedicated channels for decision making, coordinating tasks and reporting.

Considerations in terms of talk groups are as follows:

- Communication plans should state clearly which interoperability talk groups can be used, who can activate them, who can use them and under which circumstances and how to access and use them. It must be also specified what information (sensitive information) could be communicated over each talk group.
- Appropriate talk groups should be pre-loaded on the terminals available to responders. Without the common talk groups listed in the respective terminal, a user will be unable to establish interoperable communications with partner agencies.
- Consistency in talk group naming/tags should be ensured across all involved Agencies.
- Any talk group should be able to be monitored and recorded as appropriate by the corresponding communication centre, provided that previous authority has been granted.
- Interoperability talk groups should permit new users to join seamlessly by selecting the talk group on their terminal, provided that previous authority has been granted.
- Consideration should always be given to capacity levels; if congestion issues are likely to arise alternative options should be considered.
- Correct management of talk groups is essential to avoid network congestion. Only the necessary users should be set to a talk group, to avoid unnecessary usage of valuable network capacity.
- In situations where capacity of the system is limited, interoperability talk groups should allow users to request a prioritization of their own transmissions.

5.4 Communication and information exchange

Several considerations should be taken into account in the inter-agency communication and information exchange process:

- Communication between end users during an incident should only take place when a need for such communication exists and it provides added value.
- Information sharing agreements should be formalised with partner agencies.
- The sender should format the message in a way that is appropriate to the communication medium, such as voice and text.
- Agency specific jargon shall be avoided. Common and agreed terminology should be used.
- In order to avoid ambiguous call-signs, a common naming convention should be adopted for all responder agencies to identify users.
- Communication is complete when the recipient receives the message and confirms that it has been correctly understood.
- When mission critical information is broadcast the message should be prefixed with an agreed priority word to indicate the importance of the message that follows.
- Communication must follow the principles of Accuracy, Brevity, Clarity and Discipline.

5.5 Communication capacity

Communication capacity refers to the number of communication lines that can be effectively operated during an event. This depends on factors such as the capacity of the individuals, the capacity of technology, information complexity or working environment.

In terms of capacity, all communication systems are finite. Consequently the following considerations are necessary:

- In the planning process of the capacity of communication centres, the number of users and amount of traffic that communication systems can handle need to be calculated.
- The number of talk groups that is appropriate for a communication operator to manage should be agreed. This may vary depending on the predicted volumes for a particular interoperability talk group.
- Consideration should also be given to users' capacity to process the received information coming from different sources (voice, textual, graphical, etc).

5.6 Communication resilience

Resilient communications can be defined as reliable and accurate information that must be passed correctly and without delay between those who need it.

In terms of communication resilience, the following considerations should be made:

- Communication contingency plans must be defined in advance, shared with partner agencies, tested in exercises and updated.
- Diverse communication options need to be available, so that agencies have redundant communication systems that can be activated if needed.

- Communications plans should ensure that there are resilient options for maintaining interoperability if communication system coverage cannot be assured at all times.
- Working in special coverage areas, such as rural or underground environments and highly damaged areas, requires special protocols for the use of talk groups due to the limitation of network capacity in these areas.

5.7 Command and control structure

The scale of major incidents usually requires the adoption of formal command and control structures that generally across EU can be described as strategic, tactical and operational levels.

Considerations in terms of roles and routes for communication in the operation structure are as follows:

- Roles and responsibilities for each agency should be shared, so that collaborating agencies recognise and understand the separate roles, capabilities and responsibilities of partner agencies during the incident.
- The use of the interoperability talk groups should not bypass agency's chain of command.
- Should the need arise; strategic, tactical and operational commanders appointed by each responder agency must have the ability to communicate and coordinate with each other.

5.8 Training and exercising

One of the key factors in determining the success of the emergency services interoperating effectively is to hold regular joint training and exercising events to understand and be familiar with the capabilities, cultures and working practices of each responder agencies.

Considerations in terms of training are as follows:

- At the strategic level there is a responsibility for testing each agency's own communication plans and for arranging and delivering multi-agency training programs.
- Training exercises should include interoperability at strategic, tactical and operational levels.
- All personnel who are expected to authorise the activation of interoperability talk groups, those who monitor or coordinate their use in communication centres and those who will use them at an incident must be trained and exercised beforehand in the necessary procedures.
- An assessment of the training should be undertaken so that the identified problems can be addressed.

5.9 Debriefing

At the conclusion of a multi-agency exercise or incident, each of the agencies involved in the incident should hold a series of operational debriefs. Initially these will be confined to each particular agency, but later a multi-agency debrief, and lessons learnt will be analysed and incorporated into future plans. These debriefs will cover many aspects of the overall multi-agency response and will include the effectiveness of communications.

Considerations in terms of incident debriefing are as follows:

- The debriefing process should involve a discussion among all the participating responder agencies about the effectiveness of inter-agency communication, in order to validate the communication plans and to identify where improvements are necessary.
- Results should be available for all the participating agencies.
- Multi-agency debriefs should consider also the contribution provided by other, non-emergency service agencies to expand the knowledge and learning process.
- The aim of these debriefs should be to honestly and openly examine problems and mishaps to identify areas for improvement in procedures, equipment and systems and to reinforce what worked well in the crisis response. Debriefs should not be a forum for criticising.
- Debriefing should address the capabilities of the communication system and provide comments for further improvements.
- Debriefing shall cover both positive and negative aspects of exercise/incident.

5.10 Security

When different agencies interoperate for information exchange, each agency must be aware of the potential risk that information disclosure could lead to a breach of security. Some information may be sensitive and, therefore, not suitable for sharing it in an open forum.

Considerations that should be taken into account for interoperability in information exchange:

- Responder agencies are most likely to communicate mainly unclassified information. FREESIC system should stay at unclassified level.
- For protection of unclassified information, availability, integrity, authenticity and confidentiality should be ensured.
- Nevertheless, in crisis situations classified information could be sent, in the case that the impact of unavailability of this information is higher than the impact of its disclosure.
- For protection of classified information, availability, integrity, authenticity, confidentiality and non-repudiation should be ensured.
- Information sharing agreements should be agreed and disseminated among agencies, defining roles and security policies.
- Documentation should be accessible to users and should consist of an interoperability description, procedures description, security concepts, design & system documentation, implementation documentation and a manual for secure operation.
- Exchanged information logs and records should be protected.

6 Operational Communication Recommendations

This section highlights some of the key recommendations for the FREESIC system to achieve effective multi-agency interoperability that emerged from the internal report *D3.02 Report on consultation with public authorities* [3], which involved research with and engagement of users across several EU states.

Recommendations drawn from D3.02 included technical aspects towards the FREESIC system implementation and non-technical aspects towards the FREESIC user operational communication guidelines and procedures definition. This section deals with the non-technical elements of the recommendations, while the technical ones are addressed by the system architecture and implementation.

FREESIC guidelines and procedures should emphasize and encourage the definition of unified and agreed contingency plans, communication plans and Service Level Agreements (SLAs). Adoption of such arrangements will facilitate the appointment and acceptance, between all involved agencies at a multi-agency crisis event, of an overall incident command structure with agreed roles and responsibilities, identification of inter-agency and inter-role information exchange needs and where required direct communications between different agencies communication/control centres.

Linked to the need for effective contingency plans is the requirement that FREESIC guidelines and procedures should also support the definition of a common lexicon and terminology and the adoption of agreed data standards across EU states.

Consideration should also be given to the development of guidelines and procedures for agencies that do not regularly respond to major incidents; this will enable such agencies, when required to contribute to multi-agency events, to be informed about best practices and procedures when deployed in such operations.

Guidelines and procedures should also encourage agencies to schedule and perform periodic unified training exercises in order to practise multi-agency operations, familiarise personnel at all levels with required procedures and identify areas for improvement.

Security was highlighted as an important aspect of the FREESIC guidelines and procedures. Security requirements will vary depending on the information classification level. In addition, the development of guidelines and procedures for the security of the FREESIC system should ensure that only agencies subscribing to FREESIC should have access to it.

One of the most important recommendations that apply to both technical and non-technical aspects is that FREESIC should not impact upon or try to replace an Agency’s current communication system or ways of working, but it should enhance and complement existing systems and procedures for more effective multi-agency interoperability.

At the administrative level a well-based business case should be developed with a view to better persuading agencies and stakeholders to adopt and make use of the FREESIC system.

The incorporation of the aforementioned recommendations will ensure that the bellow defined FREESIC operational guidelines and procedures are in line with the stakeholders’ needs and requirements.

7 Conclusions

Deliverable *D3.3 – The operational procedures, guidelines and recommendations* has covered the non-technical approach of the solution aimed in WP3.

The set of guidelines, procedures and recommendations defined in the document are designed to enhance operational interoperability for emergency service and civil protection agencies when utilising FREEESIC system in crisis situations. Indeed, it is important to highlight that these guidelines and procedures do not intend to replace, nor bypass, the daily arrangements of each Responder Agency's operation, but to improve and strengthen inter-agency collaboration.

First, the document defines the FREESIC security policy including the scope, responsibilities and main statements to be recognised and taken into account by FREESIC staff and users when accessing and utilising the FREESIC system and its information. This security policy also sets out the requirement for developing FREESIC documentation in terms of a set of operational guidelines and procedures on how to use the FREESIC system and enhance interoperability in multi-agency crisis communications.

The input for the definition of this documentation has been the recommendations extracted from end-user consultation, which involved research with and engagement of users across several EU states.

Utilising this knowledge and expertise, a set of operational guidelines have been produced to provide Responder Agencies with a common framework for working together in crisis situations and best practices on how to operate the main components of command and control, such as the communication plan, communication centre operations, talk groups, training exercises, and so on.

Finally a set of operational procedures have been developed to guide the user on all the steps to deploy, configure, activate and use the FREESIC system. FREESIC is a distributed platform formed by a set of communication servers, interfaces and data exchange services and operated from a web front-end; to which end users interconnect and configure their appropriate communication preferences allowing transparent exchange of information. Detailed procedures are provided in a separate document called *ANNEX A – Detailed Operational Procedures*.

8 Acronyms

	- C -
CISA	Certified Information System Auditor
	- E -
EU	European Union
	- H -
HW	Hardware
	- I -
ICT	Information and Communication Technology
	- O -
OP	Operational Procedure
	- P -
PPDR	Public Protection Disaster Relief
	- S -
SLA	Service Level Agreement
SW	Software

9 References

[1] D3.1 – The operational procedures, guidelines and recommendations

[2] D3.4 – The system architecture document (Final)

[3] D3.02 – Report on consultation with public authorities

[4] D4.1 & D4.2 – FRRESIC system release notes

[5] D2.1 – The formal requirements specification document

[6] CISA Certified Information Systems Auditor – Study Guide. David L. Cannon

[7] Major Incident – Procedure Manual. London Emergency Services Liaison Panel (LESLP)

[8] Common Criteria Class ADG – Guidance Documents

[9] Crisis and Emergency Risk Communication – CDC (Centres for Disease Control and Prevention); http://www.au.af.mil/au/awc/awcgate/cdc/cerc_book.pdf

[10] Behaviour change communication in emergencies. UNICEF; http://www.unicef.org/ceecis/BCC_full_pdf.pdf

[11] Standard operating procedure guide on multi-agency airwave interoperability; National Policing Improvement Agent (NIPA); 2010

[12] Guidance on multi-agency interoperability; National Policing Improvement Agent (NIPA); 2009

[13] UNIVERSITY OF WARMIA AND MAZURY IN OLSZTYN. Technical Sciences. S. O'Neill, J. Strother, J. Zych, W. Wojciechowicz – User Requirements for Mission-Critical Application – the SECRICOM Case; http://www.uwm.edu.pl/stas/wydawnictwo/09.23/tech.pdf

[14] D3.3 – ANNEX A Detailed Operational Procedures