ISICOM Mission Requirements - draft

FISI - WP3

Deliverable D3.1.1

Reference:	FISI_WP3_D3.1.1_V1.0
Number of pages:	
File:	FISI_WP3_D3.1.1_ V1.0
Classification:	Public
Contract:	EU FP7 Grant Agreement n° 257118

Prepared by:	TPZ
Version:	V1.0
Date:	14/09/2011
Signature:	

List of Authors

Company	Authors
TPZ TPZ	Vincenzo Fogliati Antonella Catucci

Change Records

Issue	Date	Changes	Authors
V0.0	06/05/2011	Table of Content	Vincenzo Fogliati Antonella Catucci
V0.1	02/09/2011	First version of deliverable	Vincenzo Fogliati Antonella Catucci
V1.0	14/09/2011	Second version of deliverable	Vincenzo Fogliati Antonella Catucci


Table of Contents

1. FORWARD

ISICOM is an initiative of the ISI European Technology Platform on Satellite Communications, aiming at defining the basic foundations and the building blocks for a future European Satellite Communication Infrastructure addressed to meet the needs and requirements of European and National Institutions in the Security, Emergency Management and Civil Protection domains. FISI Work Package 3 is aimed at supporting the ISI ETP in the definition and implementation of this ISICOM Initiative. This document illustrates activities performed by WP3 in the project period from January 1st and August 31st, 2011, focusing on the identification of the ISICOM Missions, the definition of related Scenarios and the main Actors involved, and then preliminarily illustrating some needed functionalities/capabilities and the rationale for the use of Satcom in the identified scenarios. WP3 activities aimed at defining user/stakeholders requirements in the subject domains are also summarised in this document.

2. INSTITUTIONAL MISSIONS/SCENARIOS AND PRELIMINARY IDENTIFICATION OF REQUIRED FUNCTIONALTIES AND CAPABILITIES

Security is, today, one of the main priorities for European Union. The following analysis has been implemented with the purpose to identify the main security related missions potentially benefitting from satellite communications functionalities. The main missions are listed hereafter, and will be described in the following paragraphs of this chapter:

- Security of citizens
- Security of infrastructure and utilities
- Surveillance and Border control
- Crisis Management in case of natural or man made disaster
- Transport Security

- EU External actions and Humanitarian relief activities

The analysis starts with the definition of main scenarios relevant for each mission and then identifies the security involved functionalities that each scenario requires, the main actors involved and the technological capabilities to meet the user requirements typical of each scenario. This logic work flow (summarized in the Figure 1) derives from the observation that capabilities are the principal building blocks for the technological and market assessments, as they represent the smallest complete assembly of technologies and processes that together lead to an ability to perform a specific security function, task or operation.

The preliminary identification of the rationale justifying the use of SatCom as powerful means to meet user expectations and needs in the various use cases and scenarios is also summarised.

The identified missions and, for each of them, the description of related analysis are described in the following paragraphs. To illustrate the analysis elements and related obtained results, for each identified mission a table summarizing the main elements of the analysis and the related results has been produced.

As anticipated above, the mentioned ISICOM mission analysis logical steps are summarized in the following figure:

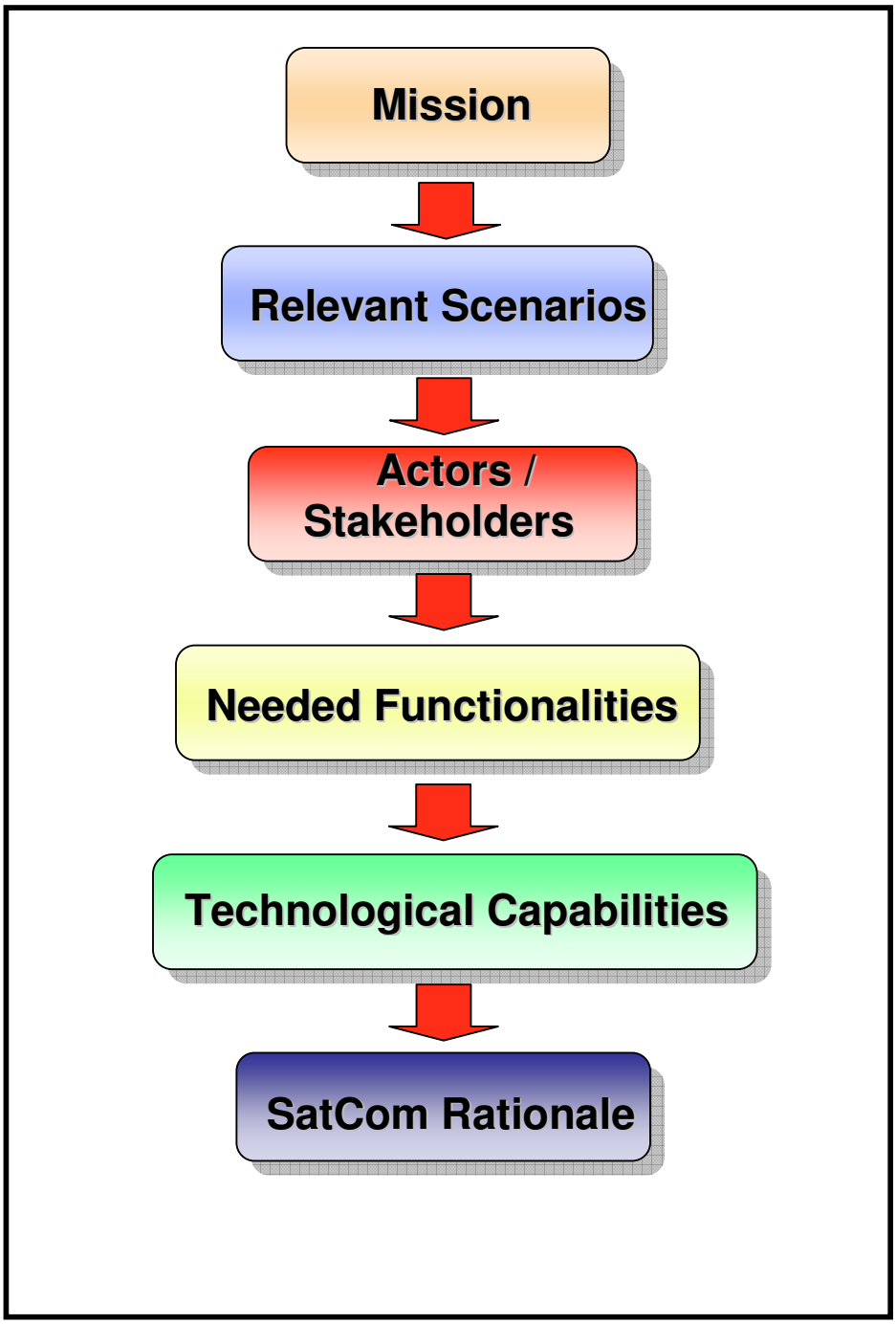

Figure 1: Logic Work Flow

2.1. SECURITY OF CITIZEN

For this Mission, potential risks related to security of citizens are connected with places and situations in which large and heterogeneous groups of people are involved and that can be characterized by a high potential risk of damage to people and assets. Starting from this concept, the following table summarises the main considered factors for this mission analysis together with the main resulting elements:

Mission: Security of Citizens				
Scenarios	**Main needed Security Functionalities**	**Main Technological Capabilities**	**Actors/Stakeholders involved**	**SatCom Rationale**
Protection of citizens in public places	- Surveillance and Control - Prevention - Decision making	- Wide coverage - Interoperability - Information Confidentiality and Access Authentication - Mobile - Fast Deployment - High Transfer rate	- Local administrations representatives - Law enforcement Authorities - Civil protection Agencies - Fire brigades - Defence Special Departments - Ministry of Interior - Medical Bodies and Institutions - National Institute for safety	- Wide Coverage - Interoperability - Confidentiality and Control Access to information - Fast Deployment - Mobile - Back-up to terrestrial connections - High Data rate
Security of the food chain and water sources	- Surveillance and Control - Prevention - Decision making	- Wide coverage - Interoperability - High access rate - High Data rate	- Local administrations representatives - Civil Protection Agencies - Medical Bodies and Institutions - National Institute for safety	- Backup to terrestrial connections - Interoperability - Wide coverage - High access rate - High Data rate

Fight against organized crime and terrorism	- Surveillance and Control - Prevention - Decision making	- Wide coverage - Interoperability - Information Confidentiality and Access Authentication - High Data rate	- Law enforcement Authorities - Defence Special Departments - Ministry of Interior	- Wide coverage - Interoperability - Confidentiality and Control Access to information - High Data Rate

Table 1: Security of Citizen

2.2. SECURITY OF INFRASTRUCTURE AND UTILITIES

In general terms, critical infrastructures are the physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of Institutions in the Member States. The scenarios, the main involved security functionalities, capabilities and related SatCom rationale for this Mission, are summarized in the following table:

Mission: Security of Infrastructure and Utilities				
Scenarios	**Main needed Security Functionalities**	**Main Technological Capabilities**	**Actors/Stakeholders involved**	**SatCom Rationale**
Energy, Water	- Monitoring and Risk assessment - Real time evaluation of infrastructure conditions - Post disaster activities	- High Transfer rate -Interoperability - Support monitoring and robot instruments - Robustness and Resilience - Wide Coverage - Interoperability with other Satellite Based Systems	- Law Enforcement Authorities - Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Water Distribution authorities (only for Water) - Medical Bodies and Organisations - Defence Special Departments	- Wide coverage - Interoperability - High Data rate - Data Fusion capability - Robustness and Resilience

			- Tax and customs authorities - Ministry of Interior - Ministry of Infrastructures - Private Bodies managing Critical Infrastructures	
Fixed Infrastructure Nodes	- Monitoring and Risk assessment - Real time evaluation of infrastructure conditions - Post disaster activities	- High Transfer rate -Interoperability - Support monitoring and robot instruments - Support Real-time modes - Robustness and Resilience - Wide Coverage - Interoperability with other Satellite Based Systems - Robustness and Urban environment Communication Capability	- Law Enforcement Authorities - Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Medical Bodies and Organisations - Defence Special Departments - Tax and customs authorities - Ministry of Interior - Ministry of Infrastructures - Private Bodies managing Critical Areas	- Wide coverage - Interoperability - High Data rate - Data Fusion Capabilities - Robustness - Resilience
Bridges/Tunnels	- Monitoring and Risk assessment - Real time evaluation of infrastructure conditions - Post disaster activities	- High Transfer rate -Interoperability - Support monitoring and robot instruments - Robustness and Resilience - Wide Coverage - Interoperability with other	- Law Enforcement Authorities - Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Water Distribution authorities - Medical Bodies and	- High Data rate - Interoperability - Data Fusion Capabilities - Robustness - Resilience

		Satellite Based Systems - Robustness and Urban environment Communication Capability	Organisations - Defence Special Departments - Tax and customs authorities - Ministry of Interior - Private Bodies managing Critical Infrastructures	
Industrial Plants	- Monitoring and Risk assessment - Real time evaluation of infrastructure conditions - Post disaster activities	- High Transfer rate -Interoperability - Support monitoring and robot instruments - Robustness and Resilience - Wide Coverage - Interoperability with other Satellite Based Systems	- Law Enforcement Authorities - Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Water Distribution authorities - Medical Bodies and Organisations - Defence Special Departments - Tax and customs authorities - Ministry of Interior - Private Bodies managing Industrial Infrastructures	- High Data rate - Interoperability - Data Fusion Capabilities - Robustness - Resilience

Table 2: Security of Infrastructure and Utilities

2.3. SURVEILLANCE AND BORDER CONTROL

Prevention of illegal cross-borders activities and fight against criminal organisations at land and maritime borders imply the implementation of thorough and comprehensive surveillance and control systems. In fact, the threat generated by illegal trafficking of people, weapons, drugs and contraband has progressively increased over the last years.

The main results, for this Mission, are summarized in the following table:

Mission: Surveillance and Border Control				
Scenarios	**Main needed Security Functionalities**	**Main Technological Capabilities**	**Actors/Stakeholders involved**	**SatCom Rationale**
Land Border Control	- Wide Area Surveillance and Monitoring - Proactive detection, identification and authentication - Situation awareness and Info-sharing - Decision making	-Interoperability - Overlay Communication Network - Interworking with other Satellite Based Systems - Self Configurability - Global Coverage - Resilience - Robustness	- Medical Bodies and Organisations - Tax and customs authorities - Air Traffic Control and Aviation Authorities - Police Departments Medical Bodies and Organisations - Tax and customs authorities - Defence Special Corps - Ministry of Interior - Ministry for Foreign Affairs	- Global coverage - Interoperability - Interworking with EO and localization satellite systems - Resilience - Overlay Communication Network
Sea Border Control		-Interoperability - Overlay Communication Network - Interworking with other Satellite Based Systems - Self Configurability - Global Coverage - Resilience - Robustness	- National Coastguards Authority - Ports Authority - Police Departments - Defence Special Corps - Ministry of Interior - Ministry for Foreign Affairs	- Resilience - Global Coverage - Backup to terrestrial connections - Interworking with EO and localization satellite systems - Overlay Communication Network

Table 3: Surveillance and Border Control

2.4. CRISIS MANAGEMENT IN CASE OF NATURAL OR MAN MADE DISASTERS

Crisis situations are progressively increasing their potential negative impact on the modern society and on the human beings. Consequently, the crisis management activities are becoming more and more complex in terms of needed capabilities and technological means able to counteract them: in this evolving context, governments and first responders require new innovative and affordable solutions. Furthermore, increased population densities, growing mega-cities, environmental degradation, and the impact of Climate Change adding to poverty make the impact of natural hazards even worse.

Progress with regard to status of the art shall be at least two-fold: ensuring governments, first responders and societies are better prepared for a critical event, and, in parallel, improving the tools, infrastructures, procedures and organisational frameworks to respond and recover more efficiently and effectively both during, and after, the event. Taking into account these fundamental concepts, the results for this Mission case are summarized in the following table:

Mission: Crisis management in case of natural or man made disasters				
Scenarios	**Main needed Security Functionalities**	**Main Technological Capabilities**	**Actors/Stakeholders Involved**	**SatCom Rationale**
Fire Hazard	-Surveillance and early warning - Crisis management - Post-crisis management	- Overlay Communication Network -Interoperability - Resilience - User friendliness - High availability and high reliability Rapid Deployment- - Interworking with satellite based systems - Net-centric approach	- Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Defence Special Departments - Forest Rangers - Ministry of Interior - Medical bodies and organisations - Law Enforcement Authorities	- Overlay communications Network - Wide Coverage - Interoperability - Resilience - Rapid Deployment - Inter-operability with EO and localization satellite systems

Earthquake	-Surveillance and early warning - Crisis management - Post-crisis management	- Wide coverage -Interoperability - Resilience - User friendliness - High availability and high reliability - Rapid Deployment - Interworking with satellite based systems - Supporting Robot communications - Supporting Net-centric approach	-Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Defence Special Departments - Regional Environment Agencies - National Institutes of monitoring and study of climatology and geo-physical systems - Ministry of Interior - Medical bodies and organisations - Law Enforcement Authorities	- Overlay communications Network - Wide Coverage - Interoperability - Resilience - Rapid Deployment - Interworking with EO and Localization Systems
Land Slides	-Surveillance and early warning - Crisis management - Post-crisis management	-Interoperability - Resilience - User friendliness - High availability and high reliability - Rapid Deployment - Interworking with satellite based systems - Supporting Robot communications - Supporting Net-centric approach	- Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Defence Special Departments - Regional Environment Agencies - Nationals Institute of monitoring and study of climatology and geo-physical systems - Ministry of Interior - Medical bodies and organisations - Law Enforcement Authorities	- Overlay communications Network - Wide Coverage - Interoperability - Resilience - Rapid Deployment capability - Interworking with EO and Localization Systems

Floods	-Surveillance and early warning -Crisis management -Post-crisis management	-Interoperability - Resilience - User friendliness - High availability and high reliability - Rapid Deployment - Interworking with satellite based systems - Supporting Robot communications - Supporting Net-centric approach	-Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Defence Special Departments - Ministry of Interior - Medical bodies and organisations - Law Enforcement Authorities	- Overlay communications Network - Wide Coverage - Interoperability - Resilience - Rapid Deployment - Interworking with EO and Localization Systems
Hurricane	- Surveillance and early warning - Crisis management - Post-crisis management	- Wide coverage - Interoperability - Resilience - User Friendliness - High availability and high reliability - Rapid Deployment - Interworking with EO and Localization Systems - Supporting Robot communications - Supporting Net-centric approach	-Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Defence Special Departments - Forest Rangers - Ministry of Interior - Medical bodies and organisations - Law Enforcement Authorities	- Overlay communications Network - Wide Coverage - Interoperability - Resilience - Rapid Deployment - Interworking with EO and Localization Systems

Major Industrial Accidents/Technological Disasters	- Surveillance and early warning - Crisis management - Post-crisis management	Interoperability - Resilience - User Friendliness - High availability and high reliability - Rapid Deployment - Interworking with EO and Localization Systems - Supporting Robot communications - Supporting Net-centric approach	- Civil Protection Agencies - Local Administrations Representatives - Fire Brigades - Defence Special Departments - Ministry of Interior - Medical bodies and organisations - Law Enforcement Authorities - Private Bodies managing Critical Infrastructures	- Overlay communications Network - Wide Coverage - Interoperability - Resilience - Rapid Deployment - Interworking with EO and Localization Systems

Table 4: Crisis management in case of natural or man made disasters

2.5. TRANSPORT SECURITY

The problem of assuring security in the transport sector represents, without doubt, one of the main challenges for Europe.

In this respect, an effort to define some main elements of this very wide and varied European challenge has been performed. The following table summarises the main results obtained from this analysis.

Mission: Transport Security				
Scenarios	**Main needed Security Functionalities**	**Main Technological Capabilities**	**Actors/Stakeholders involved**	**SatCom Rationale**
Maritime	- Vehicle security monitoring and control - Travellers safety and security management - Traffic Monitoring and control - Proactive Detection and Authentication	- Information and system Integration capability - Interworking with EO and localization satellite systems - Broadband and high communication performance - Delay Tolerant networking - Wide Coverage - Supporting Intelligent Traffic Systems - Integration of regional level solutions	- Directorate General for Energy and Transport of European Commission - Ministry of Transport - Ministry of Infrastructures - Maritime Administration Organization - Port Authorities - Police Departments - Civil Protection - Medical Emergency Bodies and Institutions - National Coastguards	- Usability in areas not covered by terrestrial networks - Support communications within large areas, with high-speed vehicles and within turbulent environments - Global Coverage - Supporting integration with systems functioning indoor
Road	- Vehicle security monitoring and control - Travellers safety and security management - Traffic Monitoring and control - Proactive Detection and Authentication	- Information and system Integration capability - Interworking with EO and localization satellite systems - Broadband and high communication performance - Delay Tolerant networking - Wide Coverage - Supporting Intelligent traffic Systems	- Directorate General for Energy and Transport of European Commission - Ministry of Transport - Ministry of Infrastructures - Highways Administration Organization - Local Administrative Authorities - Police Departments - Civil Protection - Medical Emergency Bodies and Institutions	- Usable in areas not covered by terrestrial networks - Supporting communications large ranges, high-speed, over turbulent environments - Global Coverage - Supporting integration with systems functioning in closed environments

		- Integration of regional level solutions	- Fire Brigades - Road Administration Organization	
Rail	- Vehicle security monitoring and control - Travellers safety and security management - Traffic Monitoring and control - Proactive Detection and Authentication	- Information and system Integration capability - Interworking with EO and localization satellite systems - Broadband and high communication performance - Delay Tolerant networking - Wide Coverage - Supporting Intelligent traffic Systems - Integration of regional level solutions	Directorate General for Energy and Transport of European Commission - Ministry of Transport - Ministry of Infrastructures - Rail Administration Organization - Police Departments - Civil Protection - Medical Emergency Bodies and Institutions	- Usable in areas not covered by terrestrial networks - Supporting communications large ranges, high-speed, over turbulent environments - Global Coverage - Supporting integration with systems functioning in closed environments
Aviation	- Vehicle security monitoring and control - Travellers safety and security management - Traffic Monitoring and control - Proactive Detection and Authentication	- Information and system Integration capability - Interworking with EO and localization satellite systems - Broadband and high communication performance - Delay Tolerant networking - Wide Coverage - Supporting Intelligent traffic Systems - Integration of regional level solutions	- Directorate General for Energy and Transport of European Commission - Ministry of Transport - Ministry of Infrastructures - Aviation Administration Organization - Airports Authorities - Police Departments - Civil Protection - Medical Emergency Bodies and Institutions	- Usable in areas not covered by terrestrial networks - Supporting communications large ranges, high-speed, over turbulent environments - Global Coverage - Supporting integration with systems functioning in closed environments

Intermodal	-Vehicle security monitoring and control - Travellers safety and security management - Traffic Monitoring and control - Proactive Detection and Authentication	- Information and system Integration capability - Interworking with EO and localization satellite systems - Broadband and high communication performance - Delay Tolerant networking - Wide Coverage - Supporting Intelligent traffic Systems - Integration of regional level solutions	- Directorate General for Energy and Transport of European Commission - Ministry of Transport - Ministry of Infrastructures - Police Departments - Civil Protection - Medical Emergency Bodies and Institutions	- Usable in areas not covered by terrestrial networks - Supporting communications large ranges, high-speed, over turbulent environments - Global Coverage - Supporting integration with systems functioning in closed environments

Table 5: Transport Security

2.6. EU EXTERNAL ACTIONS AND HUMANITARIAN RELIEF ACTIVITIES

External action services and Humanitarian Relief activities provide rapid and effective support to the victims of disasters beyond the European Union's borders. European humanitarian mandate prescribes a focus on saving lives, assisting the most vulnerable groups, providing emergency assistance and relief to the victims of natural disasters or armed conflicts outside the European Union, thus permitting the EU to play a key role in the operational coordination in crisis situations.

The results of this mission analysis are summarized in the following table:

Mission: External actions and Humanitarian Relief				
Scenarios	**Main needed Security Functionalities**	**Main Technological Capabilities**	**Actors/Stakeholders involved**	**SatCom Rationale**
External Actions	- Emergency preparedness activities - Emergency Response - Environmental Emergencies - Humanitarian Civil-Military Coordination -Logistics Support - Needs Assessment -Surge Capacity	-Interoperability - Overlay Communication Network - Interworking with other Satellite Based Systems - Global Coverage - Resilience and Robustness - Authenticated Access to Information	- Sending and receiving States; - Governmental and non-governmental organizations; - Aid agencies and civil protection units; - Military and civil defence organizations; - EC agencies and organizations (EEAS " European External Action Services", ECHO "European Commission's Humanitarian Aid" - Non-Governmental Organizations - Private sector in relation to providing adequate emergency and crisis equipment - Medical Bodies and Organizations	- Global coverage - Interoperability - Interworking with EO and localization satellite systems - Resilience - Overlay Communication Network
	- Emergency preparedness activities - Emergency Response - Environmental Emergencies	-Interoperability - Overlay Communication Network - Interworking with other Satellite Based Systems	- Sending and receiving States; - Governmental and non-governmental organizations; - Aid agencies and civil protection	- Resilience and Robustness - Global Coverage - Backup to terrestrial connections - Interworking with other Satellite Systems

Humanitarian Aid	- Humanitarian Civil-Military Coordination -Logistics Support - Needs Assessment -Surge Capacity	- Global Coverage - Resilience and Robustness	units; - Military and civil defence organizations; - EC agencies and organizations (EEAS " European External Action Services", ECHO "European Commission's Humanitarian Aid" - Non-Governmental Organizations - Private sector in relation to providing adequate emergency and crisis equipment - Medical Bodies and Organizations	- Overlay Communication Network

Table 6: External actions and Humanitarian Relief

3. REVIEW AND ANALYSIS OF STAKEHOLDERS VISION AND USERS REQUIREMENTS

3.1. SUMMARY OF RESULTS OF PREVIOUS REVIEW/ANALYSIS

Relevant results coming from activities implemented by a previous Satellite Communications related project (sISI) and referring to the User Requirements identification have been here taken into account and considered/incorporated as a starting point by the FISI WP3 activities. The User Requirement List (resulting from the previously performed review) is as follows:

UR*-01: ALWAYS-ON AVAILABILITY OF COMMUNICATIONS CHANNEL
UR-02: RELIABILITY OF TRANSMITTED INFORMATION
UR-03: COMMUNICATIONS FLOW HIERARCHY
UR-04: INFORMATION DELIVERY TIME
UR-05: MOBILE SERVICES ON THE FIELD THROUGH ROBUST USER TERMINALS
UR-06: NETWORKS AND TERMINALS INTEROPERABILITY
UR-07: SYSTEM COVERAGE AREA
UR-08: CONFIDENTIALTY AND AUTHENTICATION
UR-09: AUTONOMOUS MANAGEMENT OF THE NETWORK BY INSTITUTIONAL DEPARTMENTS
UR-10: EASY USE OF SYSTEM / RELATED SERVICES
UR-11: COMMUNICATION SERVICES PORTFOLIO
UR-12: PROTECTION AGAINST ELECTROMAGNETIC INTERFERENCE

* UR : User Requirement

Table 7: List of User Requirements

For each of the above listed User Requirements, a description is provided in the following pages:

UR-01: ALWAYS-ON AVAILABILITY OF COMMUNICATIONS CHANNEL

Requirement Code	01–UR
Requirement Name	ALWAYS-ON AVAILABILITY OF COMMUNICATIONS CHANNEL
Brief Description	Availability of a communications channel fit for the criticality of the information to transmit in the different phases of emergency management.
Description: The Satellite Communication System for Emergencies must assure the availability of a communications channel and continuity in service supply, fit for the criticality of the information to transmit in the different phases of emergency management. This availability should be assured also without any operative terrestrial network (i.e. because damaged or unavailable terrestrial network in critical scenarios. The Satellite Communication System for Emergencies must also be able not to suffer any service disruption in presence of damages in critical points of the net ("fault-tolerance").	

UR-02: RELIABILITY OF TRANSMITTED INFORMATION

Requirement Code	02–UR
Requirement Name	RELIABILITY OF TRANSMITTED INFORMATION
Brief Description	Capability of the Satellite Communication System for Emergencies to assure the information transfer with an appropriate high quality level service, in terms of reliability of the information.

Description: The Satellite Communication System for Emergencies must be able to assure the information transfer with an appropriate high level service, supplying: ➢ The high integrity of the information (strong error correction codes / optimized communication protocols) ➢ High level of services continuity (provided end-to-end service shall survive any emergency situation, assuring the needed quality of service level).

UR-03: COMMUNICATIONS FLOW HIERARCHY

Requirement Code	03–UR
Requirement Name	COMMUNICATIONS FLOW HIERARCHY
Brief Description	Capability of the Satellite Communication System for Emergencies to allow the information transport from the required authorised sources to the required authorised recipients according to their roles in the User organisation and to the identified scenario.
Description: The Satellite Communication System for Emergencies should be able to allow the information transfer from sources to required recipients, through the establishment of appropriate links and connections between different knots of the networks. The information exchange must be controlled and flexible, in compliance with the communications hierarchy and the operational procedures. Sources and recipients of the information according to the importance that the users have indicated can be mainly: ➢ Professionals/individuals (e.g. crew chief, team member, liaison officer, decision maker, etc.)	

- Central Offices/ Departments (e.g. Civil Protection Agency, MIC – Monitoring Information Centre for Mechanism monitoring, etc...)
- Operational Structures (Regional Control Room, Centre of Local Coordination, etc.)
- On board (for vehicles) or by hand apparatus (e.g. camcorder for video-streaming, video surveillance, sensors)
- Same information could be contemporaneously transmitted to one or more recipients, where required.

UR-04: INFORMATION DELIVERY TIME

Requirement Code	04–UR
Requirement Name	INFORMATION DELIVERY TIME
Brief Description	Capability of the Satellite Communication System for Emergencies to assure the information transfer respecting the delivery time.

Description:

The Satellite Communication System for Emergencies must be able to assure the information transfer supplying the delivery time required.

The real time transmission is the required time of sending/exchange/reception to transmit voice, streaming and video information also about the context of the emergency.

Quasi real time or transmission of information/messages in a few minutes are time periods suitable to send/exchange/receive short data (“SMS”), database inquiries and large amounts of data (images, video, maps).

UR-05: MOBILE SERVICES ON THE FIELD THROUGH ROBUST USER TERMINALS

Requirement Code	05–UR
Requirement Name	MOBILE SERVICES ON THE FIELD THROUGH ROBUST USER TERMINALS
Brief Description	Capability of the Satellite Communication System terminals (deployed in field to expand the network) to resist to particular and foreseeable operating conditions, so as to guarantee the availability of the information and the communications channel required.

Description:

The Satellite Communication System for Emergencies must be able to assure the fast deployment of “ad-hoc networks”, able to operate in field through mobile terminals under critical conditions, anywhere and anytime..

Through mobile terminals the users can utilise communication services in full mobility, assuring connectivity while moving within the critical situation affected territory..

The Satellite Communication System terminals deployed in field must be able to resist to particular foreseeable operational conditions, so as to guarantee the availability of the information and the communications channel, with particular reference to the capability to assure the system operation under unfavourable climatic and difficult operational situations.

In this logic the requirement of a mobile device should be characterized by factors of robustness having reference to temperature, humidity, rain, snow, altitude, mechanic solicitations resistance and power life parameters depending on the emergency environmental conditions.

Every user category has specified different parameters.

UR-06: NETWORKS AND TERMINALS INTEROPERABILITY

Requirement Code	06- UR
Requirement Name	NETWORKS AND TERMINALS INTEROPERABILITY
Brief Description	Capability to operate on the field through terminals that could cooperate in synergy with local operating centres, swapping data and mission information.
Description: The interoperability requirement refers to a communication platform whose devices, terminals are able to operate together with other networks devices and terminals (even if the different networks are using different technologies and frequencies bands). In order to facilitate the synergic use of different networks, the use of appropriate communication standards is recommended. In such a way, the communication services and applications can be used in a synergic way too, thus supporting the communication messages interchange among people, organisation and control centres.	

UR-07: SYSTEM COVERAGE AREA

Requirement Code	07-UR
Requirement Name	SYSTEM COVERAGE AREA
Brief Description	Service coverage area, to be extended to the whole Territory involved in the emergency communication scenario, to allow the management of complex operations within a wide area.
Description: The Satellite Communication System for Emergencies must assure a full network performance and related service supply within of the whole Territory involved in the emergency communication scenario, to allow the management of complex operations.	

A global (worldwide) geographic coverage is required by almost all of the contacted user representatives

UR-8: CONFIDENTIALTY AND AUTHENTICATION

Requirement Code	08-UR
Requirement Name	CONFIDENTIALTY AND AUTHENTICATION
Brief Description	The confidentiality of the information to transmit in the different phases of emergency management and the authentication of people accessing the system shall be ensured.
Description: The Satellite Communication System for Emergencies shall ensure that unauthorised people are prevented from accessing the system and the transmitted information, under the different phases of the emergency management. The entire communication flow shall be managed through appropriate protocols and procedures, in order to guarantee: ➢ The authentication of the accessing users and the related authorizations ➢ The so-called “no-rejection” of the transmitted information (identifying surely the parts that contributed to the transmission of the information, also subsequently to the moment in which the transmission happened) ➢ Capacity to protect the transmitted information through cryptographic methods, thus enabling a high level of communication flow confidentiality.	

UR-9: AUTONOMOUS MANAGEMENT OF THE NETWORK BY INSTITUTIONAL DEPARTMENTS

Requirement Code	09–UR
Requirement Name	AUTONOMOUS MANAGEMENT OF THE NETWORK BY INSTITUTIONAL DEPARTMENTS
Brief Description	Capability of the Institutional Users to operate the Network autonomously and in an effective way, so as to guarantee the respect of their institutional role and operational procedures, also ensuring the needed flexibility in managing multiple critical emergency situations.

Description:

The Satellite Communication System for Emergencies must be managed effectively in an autonomous way by the Institutional Users, with regard to both the Network and the related Services, particularly referring to:

- The Network Management functionalities, in order to optimize the use of resources, fully respecting the Institutional Users organisations roles and procedures.
- The management of the Frequency Band (under the constraints imposed by the used technologies) and the provided Services
- The management of the interoperability functionalities among different networks and terminals constituting the complete emergency management system.
- The Satellite Communication System for Emergencies must also allow the Institutional Departments to manage simultaneously multiple critical emergency situations, allocating dynamically the resources to the different criticalities in progress, in a flexible and controlled way.

UR-10: EASY USE OF SYSTEM / RELATED SERVICES

Requirement Code	10–UR
Requirement Name	EASY USE OF SYSTEM / RELATED SERVICES
Brief Description	Usability of the services and the terminals by people without specific technical expertise.
Description: The Satellite Communication System for Emergencies must allow an easy use of its services and terminals by people without specific technical expertise. Proper and simple user interfaces and appropriate tools shall be considered, so as to facilitate the system use by Institutional departments	

UR-11: COMMUNICATION SERVICES PORTFOLIO

Requirement Code	11–UR
Requirement Name	COMMUNICATION SERVICES PORTFOLIO
Brief Description	The set of different communication services required within an emergency scenario.
Description: Within an emergency context, the voice communication is considered the most important service to be assured by the system. In addition to voice communications, other required services are hereafter reported (listed according to the importance and priority level assigned by the user): ➢ short messages transmission ➢ location/positioning service ➢ high/ very high data rate ➢ traditional video(+audio) transmission ➢ imaging ➢ data transmission at low-medium rate	

- videoconference applications.

UR-12: PROTECTION AGAINST ELECTROMAGNETIC INTERFERENCE

Requirement Code	12-UR
Requirement Name	PROTECTION AGAINST ELECTROMAGNETIC INTERFERENCE
Brief Description	The Emergency Communications system should be protected against both intentional electromagnetic interference/harm/attacks and unintentional interference
Description: The Emergency Communication system shall embed proper protocols, algorithms and devices in order to protect itself against both intentional electromagnetic interference/harm/attacks and unintentional interference.	

3.2. METHODOLOGICAL APPROACH TO REFINE STAKEHOLDERS VIEW AND CONSOLIDATE USER REQUIREMENTS

3.2.1 CONTACTED ORGANIZATIONS

The list of Institutional User Requirements reported in the Table 1 of the previous paragraph 3.1 was defined on the basis of contacts and interviews performed in the frame of the above mentioned previous project and involving a first set of Institutional Users (in line with the objectives set by the previous project). The enlargement of the previously defined set of Users representatives, the refinement of the scope of the analysis and the consolidation of related results are now considered to be necessary in order for these results to become the basis for the ISICOM mission requirements definition. These

activities have started in the reporting period and will be finalised in the first months of the second reporting period. Furthermore, these activities are implemented through a methodology involving the identification and subsequent contact with a new enlarged set of Institutional Users representatives and the elaboration and submission of an ad-hoc Questionnaire, in order to permit FISI WP3 to reach the before mentioned objectives (enlargement and refinement of the analysis and consolidation of results to make them applicable to the ISICOM definition phase). The list of Institutional Users representatives contacted during the reporting period is presented hereafter in Table 2, while the Questionnaire used for the interviews is reported and briefly described in the subsequent paragraph 3.2.2.

Country	Insitution
France	*Secrétariat général de la défense et de la sécurité nationale.*
	Ministere de l'Economie, des Finances et de l'Industrie
Romanie	*Ministry of Administration and Interior*
Sweden	*Karolinska Institutet - Health issues - Experimental traumatology*
Germany	*Bundesministerium Für Wirtschaft und Technologie*
	Bundeskanzleramt (The German Chancellery)
	Federal Ministry of Transport
Netherlands	*Ministry of Security and Justice*
Poland	*Government Centre for Security*
Italy	*Joint Research Centre ISPRA*
	Presidency Council Ministers
United Kingdom	*UK Home Office*
Greece	*Centre for Security Studies - KEMEA*
	Kmea - Center for Security Studies
Czech Rep	*Ministry of Transport*

	Ministry of Interior
Ireland	*Department of Energy*
Lithuania	*Office of the Prime Minister*
Slovakia	*Ministry of Transport, Construction and Regional Development of the Slovak Republic*
	Ministry of Interior
Slovenia	*Ministry of Defence of the Republic of Slovenia*
	Republic of Slovenia Ministry of Defence
	Ministry of Interior of the Rep. Slovenia
Latvia	*Ministry of Internal Affairs of Latvia*
Denmark	*Danish Emergency Management Agency*
Hungary	*National Directorate General for Disaster Management (NDGDM)*
Luxembourg	*Haut-Commissariat a la Protection Nationale*
Belgium	*Federal Public Service Home Affairs*

Table 2: Users/Stakeholders to be contacted

3.2.2 QUESTIONNAIRE USED FOR THE CONTACTS/INTERVIEWS

The contact phase performed by FISI WP3 in the first reporting period has involved the first list of identified users/stakeholders representatives (in a number of EU Countries) reported in the above paragraph and has been implemented through the elaboration and submission of a specific Questionnaire (aiming at obtaining direct information about users/stakeholders requirements). The elaboration of answers by the User representatives and reception of them by the WP3 team is in progress during the elaboration of this Deliverable. Other Users representatives will also be contacted, through the same Questionnaire, during the first months of the second project reporting period. The whole contact phase will be finalised by December 2011: a report on the obtained results (including the complete analysis and resulting synthesis of all of the received answers) will

be produced by WP3, thus permitting to finally consolidate the ISICOM Mission Requirements.

The Questionnaire, elaborated by FISI WP3, is asking each of the contacted User representative to indicate:

- whether the previously defined Requirements (listed in Table 1 of Paragraph 3.1) are consider as relevant for the contacted User Representative too;
- which is the priority level of each of the Requirements according to the User perception;
- Whether the User Organisation is already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement;
- Whether the User Organisation has additional Requirements, not included in the preliminary List;
- A brief description of the possible additional Requirements.

The Questionnaire is reported in the following pages.

Questionnaire
"User Requirements"

Activity performed within the EU "FISI" Project
VII R&D Framework Programme of the European Union

Information about the replying Organisation:

Organisation Name: ……

Address: … ……..

City/Country: ……

Post Code: ……

Interviewed Person information:

Name: … ……..

Telephone: ……

Fax: … ……

E-mail: … ……

Role in the Organisation: ……

Dear Madam/Sir,

the preparation and submission of this questionnaire is part of the activities of the FISI ("Future integral satellite communications initiative") Project, which is funded by the European Commission (within the Seventh Framework Program for Research & Development of the European Union) and aims at consolidating the institutional users' requirements for emergency management and security applications (with specific reference to the communication functionalities which could be provided by a satellite communication system for emergency and security applications). In this regard, previous analyses performed in the frame of past EU Projects allowed to define the following set of 12 User requirements related to communications functionalities:

R-01: Always-on availability of communications channel
R-02: Reliability of transmitted information
R-03: Communications flow hierarchy
R-04: Information delivery time
R-05: Provision of mobile services on the field through robust user terminals
R-06: Networks and terminals interoperability
R-07: Coverage area
R-08: Confidentiality and authentication
R-09: Autonomous use and management of the system by institutional departments
R-10: Easy use of system / related services
R-11: Protection against electromagnetic interference
R-12: Communication services portfolio

In order to have the possibility to refine and consolidate the previously performed analysis (that resulted in the above reported list of 12 Requirements and the related description), it is very important for the FISI current project activities to receive your kind feedback about the possible relevance and importance of these 12 Requirements for your Organisation.

Consequently, in the following you will find some Forms (each one referring to a single Requirement inserted in the above List) which include a number of questions posed to your kind attention.

We thank you very much in advance for your kind support and attention!

FORM 1 - Requirement R-01	***ALWAYS-ON AVAILABILITY OF COMMUNICATIONS CHANNEL***
Brief Description	Always-on availability of a communication channel (fit for the criticality of the information to be transmitted in the different phases/scenarios of the emergency management and security applications).
Is this Requirement R-01 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-01 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-01? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially meeting the Requirement) [ ] yes (totally meeting the Requirement) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 2 - Requirement R-02	*RELIABILITY OF TRANSMITTED INFORMATION*
Brief Description	Capability (of the Satellite Communication System for Emergencies) to assure the information transfer with an appropriate high quality of service level, in terms of reliability of the information transmitted.
Is this Requirement R-02 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-02 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-02? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 3 - Requirement R-03	*COMMUNICATIONS FLOW HIERARCHY*
Brief Description	Capability (of the Satellite Communication System for Emergencies) to allow the information transport from the required authorised sources to the required authorised recipients only, according to their roles in the User organisation and in the identified scenario.
Is this Requirement R-03 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-03 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-03? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 4 - Requirement R-04	*INFORMATION DELIVERY TIME*
Brief Description	Capability (of the Satellite Communication System for Emergencies) to assure the information transfer, fully respecting the needed delivery time.
Is this Requirement R-04 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-04 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
According to your organization operational experience, which should be the sending/exchange/reception time of the transmitted information during emergency operations?* *Please answer by putting "X" in the relevant items (in the column here on the right)*	[ ] Real time transmission ▪ *please specify which information typologies/operational scenarios need real time transmissions:* ……..……... …….. [ ] Quasi real time transmission ▪ *please specify which information typologies/operational scenarios need a quasi real time transmission* …… …… [ ] Transmission of information/messages in a few minutes ▪ *please specify which information typologies/operational scenarios need transmission of related data in a few minutes* …… …… …….. [ ] Transmission of information within 1 hour

	▪ *please specify which information typologies/operational scenarios need transmission of related information within 1 hour* ……..…….. …….. …… [ ] Transmission of information within a few hours ▪ *please specify which information typologies/operational scenarios need transmission of related information within a few hours* ..……. . …… [ ] Other (*please specify*) ……..…… …….. ……

FORM 5 - Requirement R-05	*PROVISION OF MOBILE SERVICES ON THE FIELD THROUGH ROBUST USER TERMINALS*
Brief Description	Capability of the Satellite Communication System terminals (deployed in the field to expand the network) to perform mobile communications functionalities and resist to particular/critical operating conditions, so as to guarantee the availability of the information and of the communications channel required under any condition.

Is this Requirement R-05 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-05 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-05? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 6 - Requirement R-06	*NETWORKS AND TERMINALS INTEROPERABILITY*
Brief Description	Capability to operate on the field through terminals able to inter-operate/cooperate with other networks' terminals and local operating centres, properly exchanging data and mission information.
Is this Requirement R-06 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-06 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-06? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 7 - Requirement R-07	*COVERAGE AREA*
Brief Description	Service geographic coverage area, to be extended to the whole Territory involved in the emergency communication scenario, thus allowing the management of complex operations within a wide area.
Is this Requirement R-07 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-07 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority

According to your Organisation needs, which is the best suited geographic coverage area for an emergency communication system?*

[ ] Global (worldwide)

[ ] European

[ ] Multi-National

[ ] National

[ ] Regional

[ ] Local

*Please answer with an "X"

FORM 8 - Requirement R-08	*CONFIDENTIALITY AND AUTHENTICATION*
Brief Description	To assure the confidentiality of the information to be transmitted in the different phases of emergency management and the authentication of authorised people who are accessing the system.
Is this Requirement R-08 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-08 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-08? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 9 - Requirement R-09	*AUTONOMOUS USE AND MANAGEMENT OF THE SYSTEM BY INSTITUTIONAL DEPARTMENTS*
Brief Description	Capability of the Institutional Users to operate the System autonomously (without external interventions) and in an effective way, so as to guarantee the respect of their institutional role and operational procedures, also ensuring the needed flexibility in managing multiple critical emergency situations.
Is this Requirement R-09 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-09 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority

Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-09? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 10 - Requirement R-10	***EASY USE OF SYSTEM / RELATED SERVICES***
Brief Description	Easy use of the system and the user terminals by people without specific technical expertise.
Is this Requirement R-10 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-10 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-10? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 11 - Requirement R-11	*PROTECTION AGAINST ELECTROMAGNETIC INTERFERENCE*
Brief Description	The Emergency Communications system should be protected against both intentional electromagnetic interference/harm/attacks and unintentional interference

Is this Requirement R-11 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-11 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Is your Organisation already using (at present) any technological asset/system/device able to meet (partially or totally) this Requirement R-11? *If you replied "yes", please also indicate the type of technological asset/system/device your Organisation is using.*	[ ] yes (partially) [ ] yes (totally) [ ] no *Type of technological asset/system/device:* …… ……..

FORM 12 - Requirement R-12	*COMMUNICATION SERVICES PORTFOLIO*
Brief Description	The set of different communication services required within an emergency scenario.
Is this Requirement R-12 relevant for your Organisation?* * Please answer with an "X"	[ ] yes [ ] no
Please indicate a priority level for this Requirement R-12 *(according to your Organisation needs and specific mission).*	[ ] High level of priority [ ] Medium level of priority [ ] Low level of priority
Which typologies of communication services does your organization require to correctly perform its operational activities in an emergency context?* * *Please answer by putting "X" in the relevant items (in the column here on the right)*	[ ] Voice communication [ ] Short Messages transmission [ ] Traditional Video (+Audio) transmission [ ] High definition Video (+Audio) transmission [ ] 3D Video(+Audio) communication [ ] Imaging (*e.g.* Cartography, geo-referenced data and remote sensed data) transmission [ ] Location/Positioning (*e.g.* GPS) service [ ] Data transmission at low-medium rate [ ] Data transmission at high/very high data rate [ ] Videoconference applications [ ] Remote video surveillance applications [ ] SCADA (Supervisory Control And Data Acquisition) applications (*e.g.* survey system/ landslide alert)

Thanks for your kind collaboration on the previous section of the Questionnaire!

To finalise the FISI project analysis, we need now one last contribution from your side: as a matter of fact, it is very likely that some communications requirements of importance to your Organisation could be NOT included in the list of 12 Requirements illustrated in the previous section of this questionnaire. For this reason, in the following section you are kindly asked to indicate possible ADDITIONAL REQUIREMENTS of importance to your Organisation.

Additional Requirements	
According to your Organisation experience and mission, are there any other Requirements relevant for your Organisation and NOT included in the previous list of 12 Requirements?	[ ] yes [ ] no
If you replied "yes" to the previous Question, could you please illustrate the additional requirements relevant to your Organisation?	"Title" of Additional Requirement AR-01: …… Brief description of Additional Requirement AR-01: …… …… …… "Title" of Additional Requirement AR-02: …… Brief description of Additional Requirement AR-02: …… ……

	…… "Title" of Additional Requirement AR-03: …… Brief description of Additional Requirement AR-03: …… …… …… . . . "Title" of Additional Requirement AR-N: …… Brief description of Additional Requirement AR-0N: …… …… ……


4. CONCLUDING CONSIDERATIONS AND WORK TO BE DONE IN THE NEXT PROJECT PERIOD

This document has illustrated activities performed by WP3 in the project period from January 1st to August 31st, 2011, including the identification of the ISICOM Missions, the definition of related Scenarios and the main Actors involved, and then preliminarily illustrating some needed functionalities/capabilities and the rationale for the use of Satcom in the identified scenarios.

A direct contact phase with User Representatives has also started during the first project reporting period. Relevant results coming from activities implemented by a previous Satellite Communications related project and referring to the User Requirements identification have been taken into account in the FISI WP3 direct contact phase with Users Representatives.

These direct contact phase activities, started in the first reporting period, will be finalised in the first months of the second reporting period. These activities are being implemented through a methodology involving the identification of User Representatives to be interviewed and subsequent contact through an ad-hoc Questionnaire.

The contact phase performed by FISI WP3 in the first reporting period has involved a first list of identified users/stakeholders representatives (in a number of EU Countries). The elaboration of answers by the User representatives and reception of them by the WP3 team is in progress during the elaboration of this Deliverable. Other Users representatives will also be contacted, through the same Questionnaire, during the first months of the second project reporting period. The whole contact phase will then be finalised by December 2011: a report on the obtained results (including the complete analysis and resulting synthesis of all of the received answers) will be produced by WP3, thus permitting to finally consolidate the ISICOM Mission Requirements.