Deliverable No. 3.3

Strategic Research and Engineering Roadmap

in the domain of Emergency and Crisis Management

Grant Agreement No.: 288274

Deliverable No.: D3.3

Deliverable Name: Strategic Research and Engineering Roadmap in the domain of Emergency and Crisis Management

Contractual Submission Date: 2013-10-31

Actual Submission Date: 2013-10-31

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	ROAD 2 SOS
Project Full Name:	Development of strategic research and engineering roadmaps in System-of-Systems Engineering and related case studies
Programme	FP7 – ICT – 2011.7, Challenge 3.3
Instrument:	Coordination and support action
Start date of project:	01.10.2011
Duration:	27 months
Deliverable No.:	D3.3
Document name:	Strategic Research and Engineering Roadmap in the domain of Emergency and Crisis Management
Work Package	WP 3
Associated Task	T 3.3
Nature[1]	R
Dissimilar nation Level[2]	PU
Version:	1.0
Actual Submission Date:	2013-10-31
Editor: Institution: E-mail:	Eusebio Bernabeu, Dolores Ordoñez, Maite Irigoyen UCM, Prodigy maiteirigoyen@pas.ucm.es, dordonyez@prodigyconsultores.com

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 – ICT – 2011.7, Challenge 3.3) under grant agreement n° 288274.

[1] **R**=Report, **P**=Prototype, **D**=Demonstrator, **O**=Other
[2] **PU**=Public, **PP**=Restricted to other programme participants (including the Commission Services), **RE**=Restricted to a group specified by the consortium (including the Commission Services), **CO**=Confidential, only for members of the consortium (including the Commission Services)

Change Control

Document History

Version	Date	Change History	Author(s)	Organisation
0.1	2013-02-05	Document drafted	Simon Ford, Nicky Athanassapoulou Ursula Rauschecker	IfM ECS Fraunhofer IPA
0.2	2013-02-19	Second draft	Maite Irigoyen	UCM
0.2-1	2013-02-20	Third Draft	Dolores Ordóñez	Prodigy
0.3	2013-03-13	Four Draft	Maite Irigoyen	UCM
0.3-2	2013-03-14	Fifth Draft	Dolores Ordóñez	Prodigy
0.3-3	2013-03-19	Sixth Draft	Maite Irigoyen	UCM
0.4	2013-05-20	Seventh Draft	Maite Irigoyen	UCM
0.5	2013-07-26	Eighth Draft	Maite & Dolores	UCM, Prodigy
0.6	2013-08-06	Ninth Draft	Dolores Ordoñez	Prodigy
0.7	2013-09-03	Tenth draft	Maite Irigoyen	UCM
0.8	2013-10-17	Eleventh draft	Maite Irigoyen, Dolores Ordoñez	UCM, Prodigy
0.9	2013-10-22	Twelfth draft	Dolores Ordoñez	Prodigy
1.0	2013-10-30	Final version	Nicky Athanassapoulou	IfM ECS

Distribution List

Date	Issue	Group
2013-05-20	Review	Consortium
2013-08-06	Review	Consortium
2013-10-22	Finalisation	IfM / SEZ

Table of Contents

Executive Summary

The efficient management of emergency situations requires fast detection and control of a vast amount of parameters. To deal with the complexity of this scenario, a systems-of-systems approach is considered promising. It is expected to support the response to critical situations by providing the possibility of sharing data and information among all constituent systems and with emergency responders.

Catastrophic situations are hardly predictable and the different types and categories imply the need for different emergency responders. There are three stages in emergency situations: the pre-event stage, the emergency stage and the restoration stage. In the pre-event stage, the task of an SoS would be to control different types of device networks (sensors, cameras, etc.) that monitor the status of several critical parameters. In case of the emergency situation, the second stage is reached with the goal to resolve the danger as soon as possible while avoiding as much damage of involved people and buildings as possible. Depending on the situation, the corresponding emergency bodies have to be able to minimize danger and human losses. Finally, the restoration stage is reached which focuses on reestablishing the original state in the crisis area. Different tasks might necessarily be done, such as restoring traffic, offering public services and infrastructures (public lighting, mailboxes, parking meters, etc.), reopening businesses, clearing streets, etc.

One of the main tasks for an efficient emergency management through an SoS is to develop a method to determine an optimal chain of command. In emergency bodies such as police or the army, there are strong hierarchies to be respected. Thus, it is necessary to decide who will be the most appropriate person that takes the responsibility to lead others. In the same way, a better organisational management between agencies has to be achieved through, for example, the elimination of institutional issues like the radius of action of emergency or government agencies.

Although the human factor is the most important one during the resolution of an emergency, software and hardware tools significantly facilitate the work of emergency responders and greatly contribute to improve the efficiency managing the situation. Simulation and modeling tools which allow reliable forecasts and decision support tools are crucial to identify optimal solutions to each specific emergency situation. These and other aspects are reflected in the roadmap (Figure 1), and explained in more detail along this report.

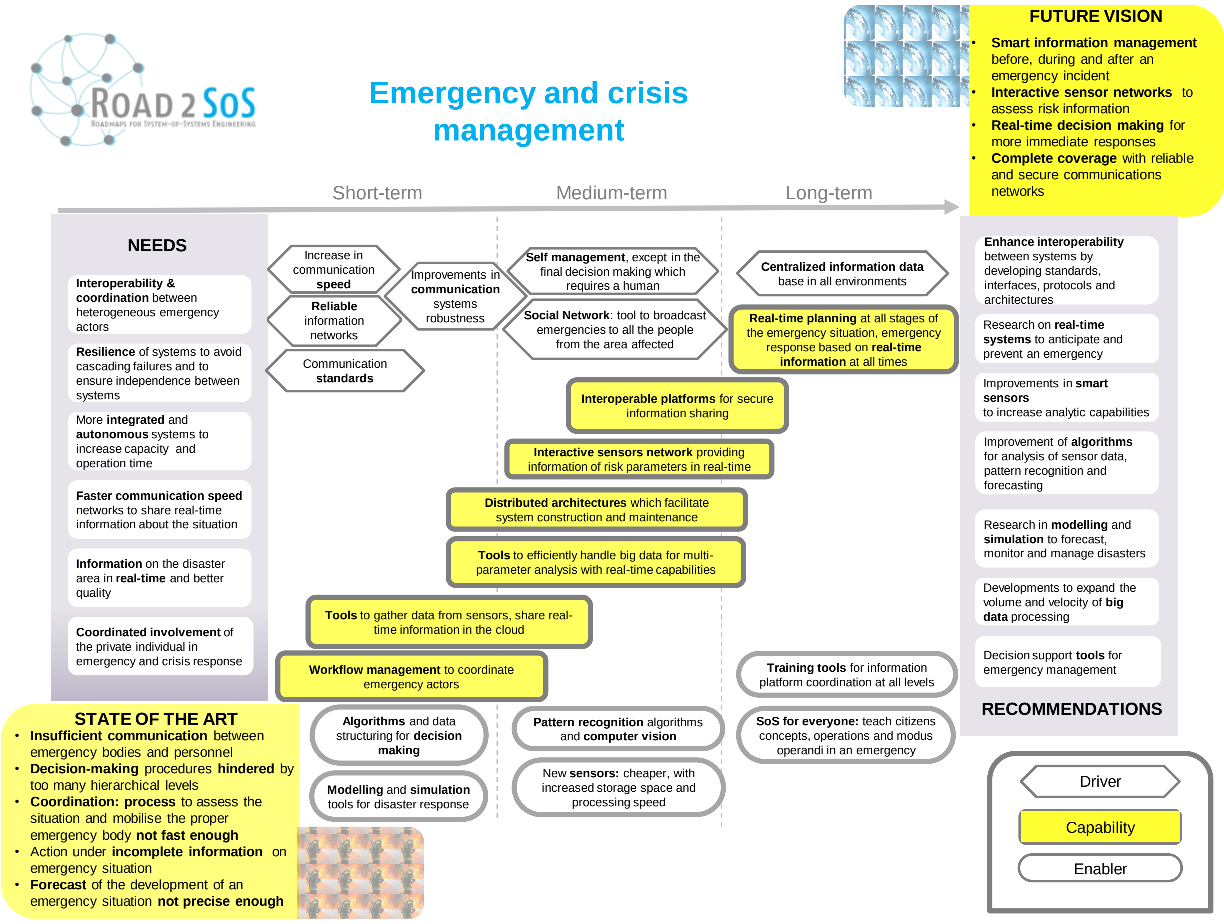

Figure 1 - Simplified SoS roadmap for the domain of Emergency and Crisis Management.

1. Introduction

The trend of an increasing interconnection of formerly self-contained systems into Systems of Systems (SoS) is expected to yield – by synergy and emergence – unprecedented capabilities in many domains. SoS approaches can be expected to improve the competitive position of companies, especially SMEs, and help tackle a range of societal challenges.

To effectively design, develop, run, and maintain SoS, a range of technologies and capabilities are necessary. To provide a clear view of the required technologies/capabilities but also barriers and enabler relevant with regards to SoS, the Road2SoS project develops research and engineering roadmaps in four selected application domains: (1) integrated multi-site manufacturing, (2) multimodal traffic control, (3) smart grid and distributed energy generation, and (4) emergency and crisis management. The identification of common strands arising independently in several application domains leads to recommendations for research priorities and shall inform future SoS-related R&D in Europe.

This report provides an overview of the roadmap developed in the domain of emergency and crisis management. Following a description of the roadmapping methodology, the roadmap's main aspects will be presented, covering the range of socio-economic trends, drivers and needs, along with the technological challenges and the enablers that are facilitating SoS-approaches modes.

2. Methodology

There are two contrasting approaches to creating roadmaps. The first approach, a technology-push prospective roadmap, starts with existing research projects and fills in the remainder of the roadmap to identify the diversity of capabilities to which this research could lead. In contrast, the second approach, a requirements-pull prospective roadmap, begins by envisioning the desired technology, system or other end products, before working backwards to identify the critical research and development required to fill in the remainder of the roadmap to arrive at these products.

In the Road2SoS project, roadmaps have been created by combining the technology-push and requirements-pull perspectives. Starting with existing science and technology development programs which are more technology- or requirements-driven, research gaps were identified that obstruct forward progress and the diversity of end products to which successful development could lead (Figure2).

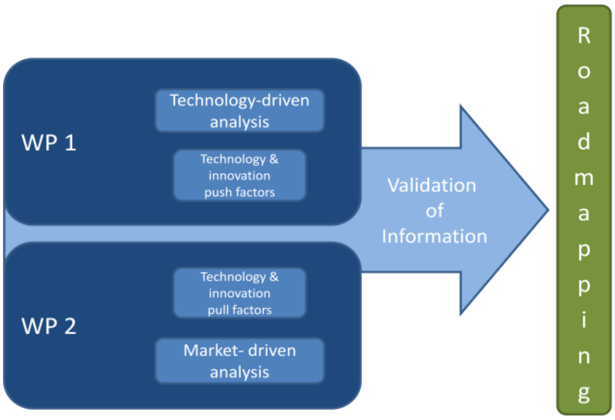

Figure 2 - Representation of the integration of the results coming from the technology-driven/push and the market-driven/pull analyses

Prospective analyses cover time frames from the present to typically a decade or more into the future. A time frame of 15 years into the future was selected due to the EC's planning horizons and objectives and the need to include SME participation. The roadmaps developed present information at a medium aggregation level.

2.1 *Common roadmap architecture and workshop process*

A common roadmap architecture and workshop process was developed and adopted in order to facilitate the collection and analysis of similar data across the four domains examined in Road2SoS, enabling the identification of key drivers, technologies and enablers that are relevant to make SoS approaches work in the selected application domains.

This common roadmap architecture (Figure 3) considers three time periods on its horizontal axis: the short-term (+5 years), the medium-term (+10 years), and the long-term (+15 years). On the vertical axis, four layers, each comprising a number of sub-layers, are included.

2.2 *Phases of development*

The roadmaps were developed through the following three phases.

Phase 1: Data collection and analysis
During this phase, the collection and analysis of RTD and innovation results (push perspective), domain needs and relevant trends/drivers (pull perspective) took place. This was conducted through literature

review, interviews and surveys with stakeholders from research institutions, companies and governmental organisations.

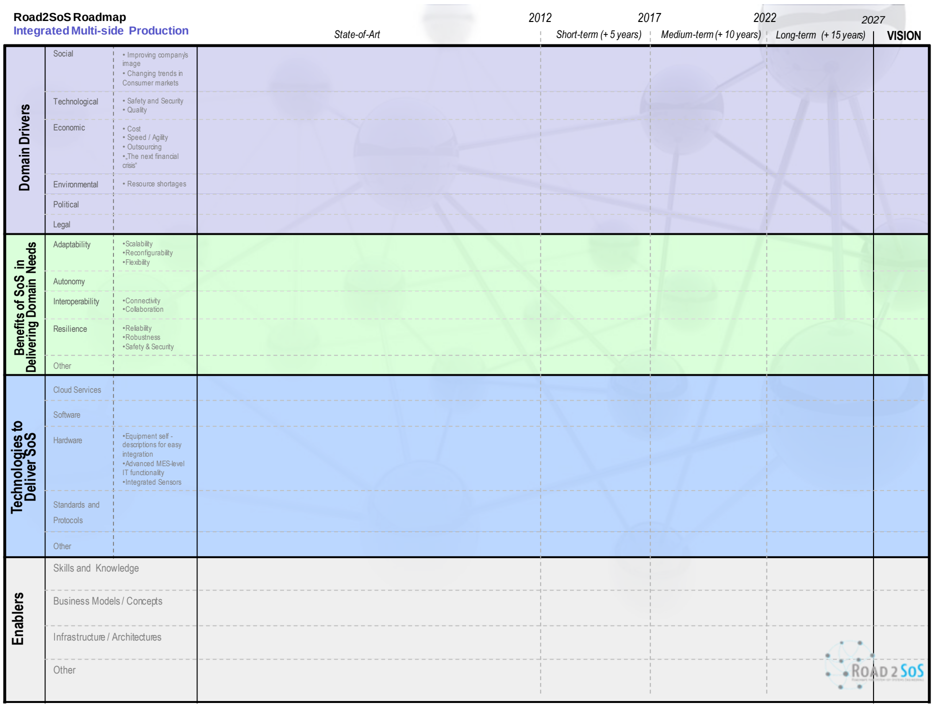

Figure 3 - Common roadmap architecture

Phase 2: Development of technology roadmaps

In this phase, a roadmapping workshop was used to validate the Phase 1 findings, complement them, and analyze them for mutual implications of push and pull perspective. Aspects captured in the roadmap furthermore underwent prioritization and in-depth discussions were devoted to top-priority aspects.

The full-day roadmapping workshop, held on 26th October 2012 in Madrid, involved a group of selected experts from industry, academia and governmental organisations.

Phase 3: Cross-sectoral approach

In this final phase of development of the roadmaps, cross-domain analysis for common drivers, technologies and enablers arising independently in two or more application domains was conducted. The results were validated by means of several case studies in each of the four domains.

3. Roadmap

The result of the roadmapping process is shown in (Figure 4). Each item is colour-coded to show its relative priority against other items within its layer. In the following sections, the highest priority items are explained in turn, beginning with the domain vision that was presented to participants at the roadmapping workshop.

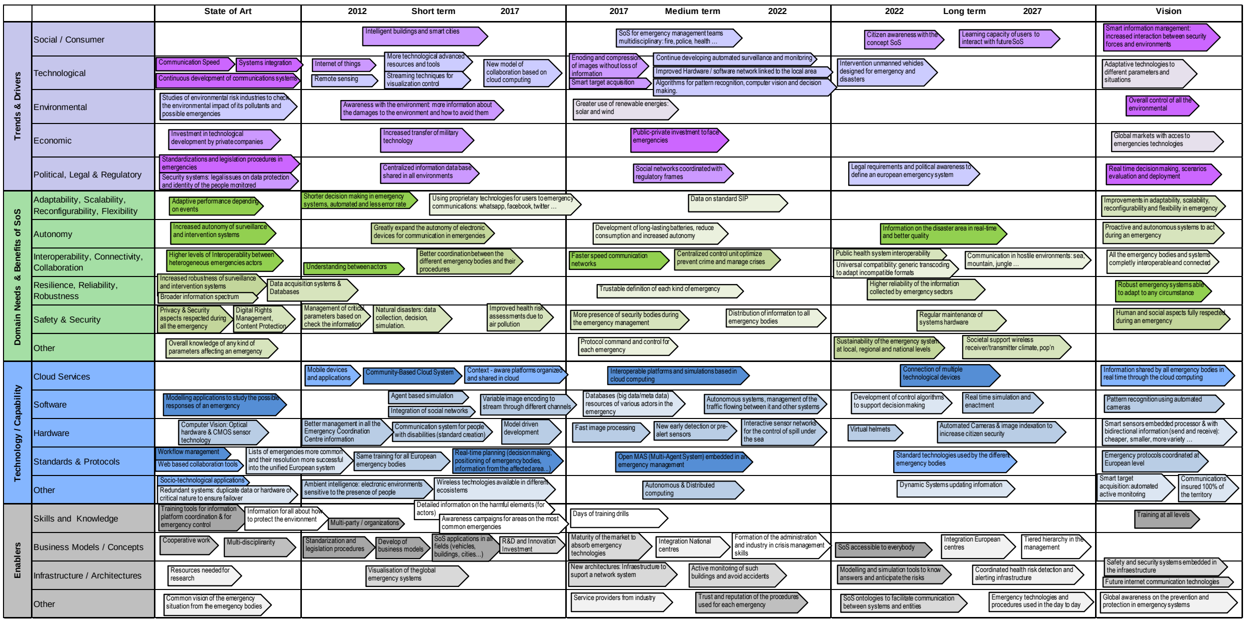

Figure 4 - Roadmap Landscape

3.1 *Possible future Vision for the domain*

The future vision for emergency and crisis management is an SoS which is able to meet the needs of all citizens of a city while controlling the risks in this area. This system should be able to control pre-alert situations in all corresponding areas and to avoid critical situations before they occur. In our future vision, there is a system which manages emergencies in a fast, orderly and effective way. The main objective is to resolve an emergency as soon as possible while minimising the damages as much as possible. Within a smart city's perspective, the occurrence of emergency and crisis situations (such as accidents, terrorist attacks, natural disasters, fires, etc.) should not disturb the normal order of things or hinder the everyday life of citizens.

The role of emergency and security responders is of vital importance in system of systems. By definition, smart cities and SoS consist of constituent systems with ability to work autonomously but where failover can occur. In an SoS focused on emergency management, some level of autonomous self-repairing behaviour can be achieved, but decision-making on how to operate in an emergency situation today remains the responsibility of human beings. Thus, the importance of emergency responders in SoS. However, SoS can support decision-making and greatly help to reduce the response time in a critical situation. Real-time information, pre-alert systems, visual surveillance and specific protocols will contribute to increase the speed of reaction in the affected areas.

A key part of SoS focused on emergency management is the pre-alert and monitoring of critical parameters that may indicate a dangerous situation. Sensors and sensor networks, as will be seen later in this roadmap, are the most suitable technology for this task. For example, a network of sensors installed in a building with smoke detectors, humidity, visibility, motion, etc. can detect fire or intrusion in forbidden areas and can also control actuators such as power-lights, emergency ventilation, irrigation fire systems, etc. A sensor network that is able to interact and feedback information is the best tool to monitor specific situations and control them under certain threshold of security. Additionally, as this technology continuously improves, many more tools will be available in order to implement an emergency management-oriented system.

Information obtained through sensor networks has to be treated and analysed in order to get as much valuable information as possible. Intelligent information management is not only bind to the exploitation of information when an incident occurs. Prior to an emergency, an intelligent information management system should ensure that a situation is less dangerous for involved civilians and buildings or even avoid the situation if anticipated well enough. Furthermore, once resolved the emergency, intelligent management has to contribute to the restoration of normal order of the affected area in the shortest time possible.

Therefore, in the future vision of SoS dedicated to emergencies and crisis management, prevention technologies (such as sensor networks), communication technologies (for fluid and efficient communication during an emergency) and intelligent management of information shall be fully taken into account.

3.2 *Trends and Drivers*

The top layer of the roadmap pertains to the wider social, technological, environmental, economic and political trends (STEEP), changes that are envisioned to affect the multimodal traffic control domain. A detailed view of this layer is depicted in Figure 5.

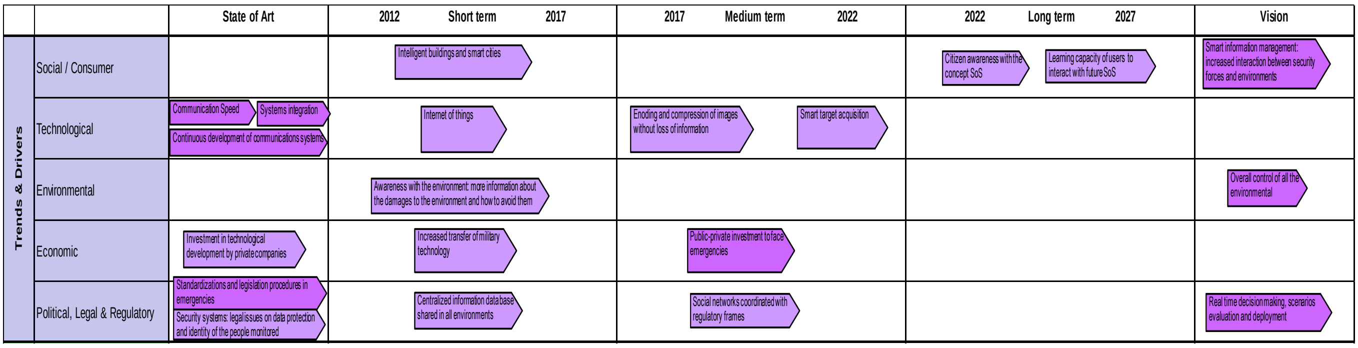

Figure 5 - Trends and drivers

As in Figure 4, the darker shades indicate those items that were identified by roadmapping workshop participants as being of higher significance. The ten most important trends and drivers are:

- Standardisation and legislation procedures in emergencies
- Communication speed
- Increased transfer of military technologies
- Overall control of environmental parameters
- Continuous development of communications systems
- Systems integration
- Public-private investment to face emergencies
- Real-time decision making, scenario evaluation and deployment
- Smart information management: increased interaction between security forces and environments
- Security systems: legal issues on data protection and identity of the people monitored.

The four most important drivers identified are described in the following sections.

3.2.1 Standardisation and legislation procedures in emergencies

Standardisation on national and international level of emergency procedures and legislation is necessary. National and international guidelines and directives will have to be developed by the main bodies related to emergency management. The standardisation of the procedures and the development of protocols will lead to a new concept of total quality in this type of services, improving cooperation between emergency stakeholders at national and international level. Each organisation is obliged to comply with state-based health and safety legislation and regulations, requiring the provision of a safe workplace for staff and visitors at any time. This extends to the prevention and management of unforeseen and potentially life threatening emergency situations. As a system of system the standards and legislation procedures have to be defined by each type of building and edification depending on their needs.

3.2.2 Increasing communication speed

During a critical situation, the share of information between bodies in charge of managing and solving this situation has a direct impact in the number of damages caused, both materialistic and human. Thus, it is critically important for any emergency communication to be timely and quickly disseminated. The best way to gather information is through a sensor network. Sensor networks deal with real-world parameters and often experience real-time constraints in their communication. In surveillance systems for example, communication delays between sensing and actuating loops directly affect the quality of tracking. Another fact to take into account is the need for a communication platform that is able to work in hostile environments during an emergency like a hurricane, an earthquake, a tsunami, a flood (where the emergency communication systems could be completely destroyed, including power stations, internet servers, mobile phone towers, and 911 services). In such situations, it is necessary to share all available information with all service bodies immediately.

3.2.3 Increased transfer of military technology

Military engages in high volume investments into research which yields technologies of high relevance to the domain of emergency and crisis management. Dedicated efforts should be undertaken to transfer solutions and technologies to the civil world.
Many inventions which have been developed for military use first have later been successfully transferred to the civil world. Examples are GPS, unmanned vehicles and drones. This highlights the need to promote cooperation between public and private industry and military institutions. Meetings between stakeholders of civil and security markets should be encouraged. A symbiotic link already exists between military and civilian sectors with transfer of staff and technologies from one to another, enriching the knowledge and technologies of each sector. In the domain of emergency management, this transfer of knowledge and technologies from the military industry to civilian sector has to be increased in order to further improve the monitoring, control and response in the pre-event stage of emergency situations.

3.2.4 Overall control of environmental parameters

With the continuous increase of technological and industrial development, the risk and potential collateral damage associated with these new developments have also increased. The worst damages are the ones with direct impact on the environment, resulting for example in deforestation and the pollution of nature. The pollution from leaking or spills of chemical substances, excessive pollution of the air, forest fires, etc. are emergencies that endanger both the environment and the safety of citizens. The key for the management of these situations is the pre-event stage. In order to reach this goal it is necessary to monitor environmentally critical parameters. This task could be performed with the help of technologies like sensor networks consisting of temperature, chemical, smoke or visibility sensors. This will provide real-time monitoring of critical parameters status enabling anticipation and control of potentially dangerous situations. This prevention and monitoring approach greatly contributes to avoid emergencies and/or reduce the damages caused.

3.3 *Domain Needs*

The second layer of the roadmap addresses the needs of the multi-modal traffic control domain that are related to SoS. These needs are classified as: resilience, safety and security, adaptability, autonomy and interoperability. A detailed view of this layer is depicted in Figure 6.

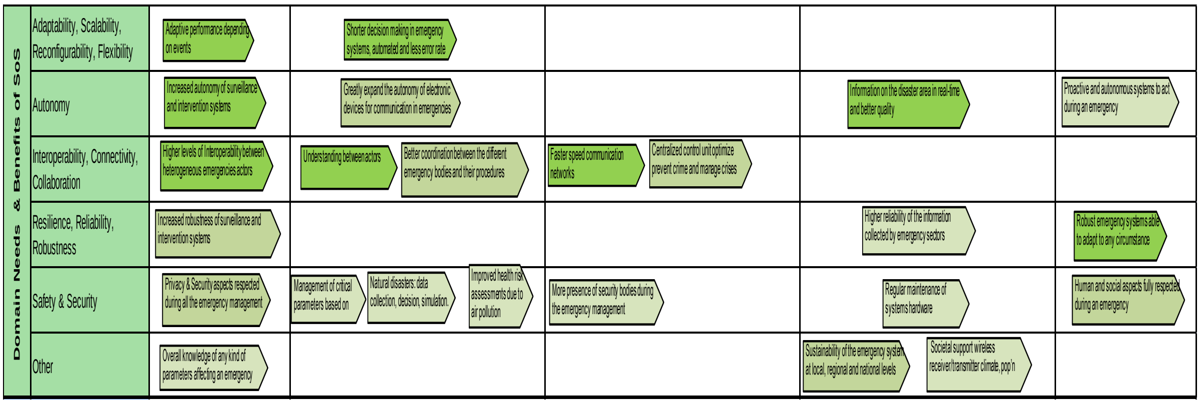

Figure 6 - Domain needs

The darker shades indicate those items that were identified by roadmapping workshop participants as being of higher significance. The ten most important needs and benefits are:

- With the aim to ensure security and safety of the citizens, the following ten factors have been identified as important: Robust emergency systems able to adapt to any circumstance.
- Adaptive performance depending on events.
- Shorter decision making in emergency systems, automated with less error rate.
- Faster speed communication networks.

- Higher levels of interoperability between heterogeneous emergencies actors.
- Increased autonomy of surveillance and intervention systems.
- Information on the disaster area in real-time and better quality.
- Greatly expand the autonomy of electronic devices for communication in emergencies.
- Better coordination between the different emergency bodies and their procedures.
- Centralized control unit optimize prevent crime and manage crises.

The aspects ranked highest are further described in the following sections.

3.3.1 Robust emergency systems able to adapt to any circumstance

Robust systems have the ability to maintain their performance despite receiving shocks. To ensure that a system is robust, it must have a number of features and qualities such as redundancy, which consists in duplication of its critical components. If a failure occurs in the system, which might endanger a task or the system itself, redundancy will offer alternatives to ensure that operation is maintained.. The resilience of a system is characterized by two important aspects; the resistance to change or flexibility that is expressed as the ability of a system to resist disturbance without suffering an irreversible change and the ability of a system to recover after a failure or a change in working conditions. If a system is robust and fulfills these qualities it will be capable of adapting itself and keep working correctly with any external perturbation.. In a crisis management incident it is necessary that all the security and safety systems keep working and adapt themselves to the new situation with higher workflow and different circumstances to manage or control.

3.3.2 Adaptive performance depending on events

Depending on the nature of an emergency and the events that take place, the performance of the systems involved must adapt to that emergency situation. Existence of good synergy between different systems will allow them to work well together for a common purpose. When an emergency occurs the target is to obtain better information and quick resolution of the situation of danger. The systems entrusted to control the critical parameters, the platforms of information, the communication systems between the emergency services, the emergency transport etc. need to work together with all the other systems that support them. Thus, if necessary, a system will work synergistically with other systems or vary its workflow depending on the conditions to which it should adapt himself.

3.3.3 Shorter decision making in emergency systems, automated and less error rate

In a crisis, the crisis management support system (CMSS) is expected to help its users to prepare, analyze, and resolve conflict. A CMSS can be designed to help decision makers to: (i) access large on-line databases to cope with information overload and analyze data reliably, (ii) consult distributed knowledge bases using case-based reasoning to learn lessons from past crisis, and (iii) use group decision support system (DSS) to alleviate problems related to group pathologies, improve decision quality, and enhance an organization's readiness to deal with catastrophe.

3.3.4 Faster speed communication networks

High-speed communication networks are characterized by large bandwidth-delay products. Communication networks are among the fastest growing engineering areas and are driving extraordinary developments in communication industry. An increasing amount of research is devoted to the deployment of new communication networks that merge the capabilities of telephone and computer networks in order to transmit multimedia traffic over a fully integrated universal network. Continuous development of existing and new data models to increase the speed communication network is essential

3.4 *Key Innovation opportunities identified in the Domain*

In order to address the drivers and needs described in sections 3.2 and 3.3, technologies and enablers were identified and assigned. In the following subsections, it is explained why and how those technologies and enablers help to support the drivers and needs by means of the four priority innovation opportunities (Figure 7).

Trends & Drivers

Priority Technologies		1 Standardizations and legislation procedures	2 Communication Speed	3 Increased transfer of military technology	4 Overall control of all the environmental parameters	5 Continuous development of communications systems	6 Systems integration	7 Public-private investment to face emergencies	8 Real time decision making, scenarios evaluation and deployment	9 Smart information management: increased interaction between security forces a	10 Security systems: legal issues on data protection and identity of users	11 Centralized information data base shared in all environments	12 Enoding and compression of images without loss of information
A	Real time simulation and enactment + Predictive modeling		1		1			1		1	1		
B	Interactive sensor network		1	1					1	1	1		
C	Autonomous technology		1		1			1		1	1		
		0	3	1	2	0	0	2	1	3	3	0	0

Domain Needs

Priority Technologies		1 Robust emergency systems able to adapt to any circumstance	2 Adaptive performance depending on events	3 Shorter decision making in emergency systems, automated and less error rate	4 Faster speed communication networks	5 Higher levels of Interoperability between heterogeneous emergencies actors	6 Increased autonomy of surveillance and intervention systems	7 Information on the disaster area in real-time and better quality	8 Greatly expand the autonomy of electronic devices for communication in emerg	9 Better coordination between the different emergency bodies and their procedur	10 Centralized control unit optimize prevent crime and manage cr	11 Increased robustness of surveillance and intervention systems	12 Human and social aspects fully respected during an emergency
A	Real time simulation and enactment + Predictive modeling	1	1	1	1		1	1		1			
B	Interactive sensor network		1		1		1	1	1	1			
C	Autonomous technology	1	1	1	1		1		1				
		2	3	2	3	0	3	2	2	2	0	0	0

Related Technologies

Priority Technologies			1 Interoperable platforms and simulations	2 Real-time planning	3 Modelling applications	4 Workflow management	5 Connection of multiple technological devices	6 Open MAS	7 Context-aware platforms	8 Web based collaboration tools	9 Standard technologies used by the different emergency bodies	10 Mobile devices and applications	11 Socio-technological extensions	12 Information shared by all emergency bodies in cloud computing	13 Agent based simulation	14 Ambient intelligence	15 Real time simulation and enactment	16 Autonomous systems	17 Emergency protocols coordinated at European level	18 Automated Cameras & image indexation to inicrease citizen security	19 Computer Vision: Optical hardware & CMOS sensor technology	20 Virtual helmets
A	Real time simulation and enactment + Predictive modeling	7	1				1		1			1					1					
B	Interactive sensor network	6			1	1			1				1								1	
C	Autonomous technology	6						1		1		1		1			1		1			1
			1	0	1	1	1	1	2	1	0	2	1	1	0	0	2	0	1	0	1	1

Enablers

Priority Technologies		1 Standarization and legislation procedures	2 Develop of business models	3 Multi-party / organizations	4 SoS applications in all fields (vehicles, buildings, cities…)	5 SoS accessible to everybody	6 Training tools for information platform coordination & for emergency control	7 Training at all levels	8 Modelling and simulation tools	9 Cooperative work	10 Multi-disciplinarity	11 Virtual emergency training	12 Maturity of the market to absorb emergency technologies	R&D and Innovation Investment	
A	Real time simulation and enactment + Predictive modeling	1					1	1							8
B	Interactive sensor network	1		1	1		1				1				10
C	Autonomous technology	1			1			1		1					11
		3													

Figure 7 - Priority Technologies

During the workshop the various technologies identified were prioritized. The key innovation opportunities were identified for the domain of Emergency and Crisis management; 'Real time simulation and enactment and predictive modeling', 'Interactive sensor network' and 'Autonomous technology'. These were explored in detail within three small groups in the afternoon session. Each group developed a mini-roadmap for its selected innovation opportunity, which are discussed in the next sections.

3.4.1 Real time simulation and enactment and predictive modeling

Predictive modeling systems can provide the information needed about possible directions that can be taken for resolving an emergency or crisis situation Simulation systems are necessary to explore uncertainties about possible developments of emergency situations. Simulation and modeling tasks can be implemented for multidisciplinary teams and users. The mini-roadmap for this opportunity was focused on some characteristics needed in the development of simulation and modeling systems.

3.4.2 Interactive sensor networks

Sensor networks normally have a tight interaction with the physical environment and hence tend to be very data-centric. Current distributed computing platforms required to support these networks face many constraints, including limited CPU speed, memory size, power, and bandwidth. Individual nodes in sensor networks are typically unreliable as the network topology dynamically changes frequently. Due to all of these issues, many solutions developed for general distributed computing platforms and for ad-hoc networks cannot be applied to sensor networks and new innovative solutions are required.

3.4.3 Autonomous technology

Autonomous technologies are required to enable individual systems within an SoS to perform their own traffic management. The main characteristics that emergency management SoS must have are situation awareness, self-diagnosis, response to changes and adaptive reasoning to different conditions.

3.5 *Technologies and Capabilities*

Figure 8 shows the technologies and capabilities layer of the roadmap, including sub-layers for hardware, software, standards and protocols and cloud services. These technologies are necessary to apply SoS approaches in the emergency and crisis management domain.

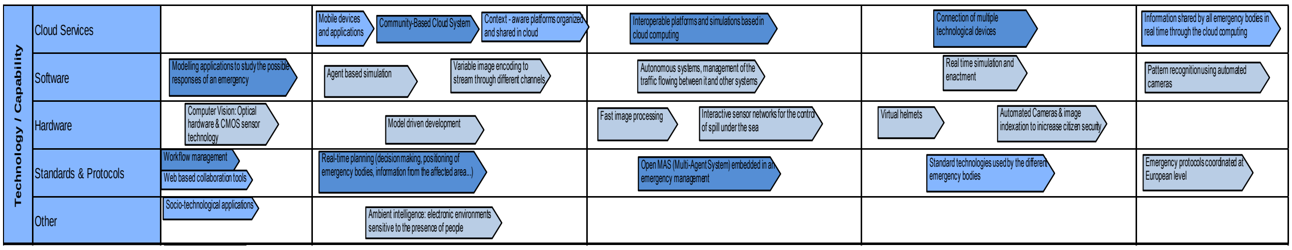

Figure 8 - Technologies and capabilities

From the list of important technologies in the domain the connection and the flow of information and development of enabling technologies needed to achieve it score very high. The most ten important technologies are:

- Interoperable platforms and simulations based in cloud computing.
- Real-time planning.
- Modelling applications to study the possible responses of an emergency.
- Workflow management.
- Connection of multiple technological devices.
- Open MAS (Multi-Agent System) embedded in an emergency management.
- Context - aware platforms organized and shared in cloud.
- Web based collaboration tools.
- Standard technologies used by the different emergency bodies.
- Mobile devices and applications.
- The aspects ranked highest are further described in the following sections.

The aspects ranked highest are further described in the following sections.

3.5.1 Interoperable platforms and simulations

In a system of systems, security of information and maintaining confidentiality while sharing information is essential. It is vital that personnel dealing with an emergency and crisis situation can be fully identified and be granted access to necessary information. The ultimate goal is to enable all different security forces, i.e. different security police departments, military units etc, to share all the information they have. A security policy describes the process of how, when and with whom information can be shared. It also specifies under which conditions, what actions can be taken when discovering threats or vulnerabilities. To do this it is necessary to have interoperable instant messaging across multiple systems. This can further speed the communication exchange between systems or components of a SoS and improved decision making in an emergency situation enabling greater efficiency and speed in its resolution.

3.5.2 Real time planning

The best definition for real time is "*Of or relating to computer systems that update information at the same rate as they receive data, enabling them to direct or control a process such as an automatic pilot*" [1]. Considering real-time computation issues, the path planning algorithms provide safety guarantees as it provides intermediate milestones with guaranteed buffer time before a catastrophe occurs.

3.5.3 Modeling applications

A system may consist of software and / or hardware components, and connections and interfaces between these components. System modeling is a technique used to express, visualise, analyse and transform the architecture of a system. . A system model can be thought as a skeletal model of the system. System modeling is intended to assist in the development and maintenance of large systems with more emphasis during the construction phase. The idea is to encapsulate complex or changeable aspects of a design inside separate components with well-defined interfaces, indicating how each component interacts with its environment. Complete systems are then developed by synthesising these components. System modeling can increase the reliability and reduce the development costs by making it easier to build systems, to reuse previous built components within new systems, to change systems to suit changing requirements such as functional enhancement and platform changes, and to better understand system operations. In this way, a system model can satisfy different requirements such as documenting the system or providing a notation for tools such as consistency checkers. It can also be used in the design stage of system development. Thus, system modeling is used to ensure that a developing piece of software evolves in a consistent manner and that the task of integrating software components is simplified.

3.5.4 Workflow management

Workflow management deals with the automation of business processes. A workflow could be a one-time-only process or an ad hoc workflow, a collaborative process that coordinates a team working together to achieve a goal (e.g., designing systems specifications), or a mission-critical, transaction-oriented production workflow. A workflow management application defines all the business processes, from start to end, including all exception conditions, tracks process-related information and the status of each process step as it gets executed. Workflow management technology provides a mechanism for planning and controlling how people work together in business environments. It acts as the connectivity tool to manage, monitor, organize and distribute specific business tasks and the associated required information. A principal concept in workflow management is the coordination of tasks in the business process. The way through which these are conducted might include verbal information, human gesture, documents, images, graphics, sounds and/or any type of `information'.

3.6 *Enablers*

Certain enablers for SoS in emergency and crisis management have been identified in the roadmapping process and are depicted in Figure 9. They are non-technical and include the sublayers: “skills and knowledge”, “business models and concepts” and “infrastructures and architectures”.

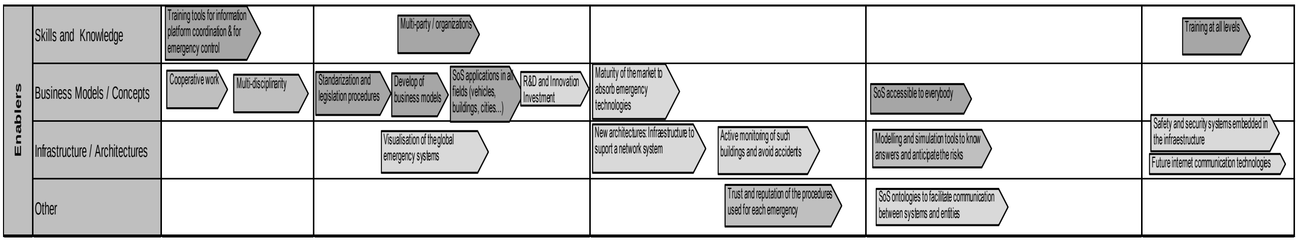

Figure 9 - Enablers landscape in the summary roadmap.

The darker shades indicate those items that were identified by roadmapping workshop participants as being of higher significance. The ten most important enablers are:

- Standardization and legislation procedures.
- Development of business models.
- Multi-party / organizations.
- SoS applications in all fields (vehicles, buildings, cities…).
- SoS accessible to everybody.
- Training tools for information platform coordination & for emergency control.
- Training at all levels.
- Modeling and simulation tools to know answers and anticipate the risks.
- Cooperative work.
- Multi-disciplinarity.

The four most relevant enablers are detailed below.

3.6.1 Standardization and legislation procedures.

There is a need to develop appropriate legislations and design standardized basic procedures for emergency responders to reduce risk and speed up the resolution of an emergency. These should contain information on possible difficulties that may be encountered that could affect the normal functioning of the area which is intended to be secured and monitored. It involves the development and improvement of procedures for the evaluation of risks, assessment of damages, analysis of needs, and protocols for specialized actions inherent to emergency care. It should include guidelines such as the management of humanitarian aid, or the management of population’s participation in the context of the emergency care.

3.6.2 Development of business models

Government organizations could become their own SoS integrators, and attain advantages through leveraging of information technology resources and systems.
At a top level, a public organization can design and maintain a strategic development plan in a flexible framework that accommodates the changes expected over a long period of time. The information maintained in this framework allows the organization to know where it is going, how and when it is going to get there, the required capabilities and interfaces of each SoS component, and the impact of changes to system requirements, budgets, schedules, etc., on the overall SoS. The middle level processes allow the organization to perform studies among alternative solutions to implement required capabilities based on what is the best for the wide SoS rather than just local considerations. The final result of the middle level processes is a selected and approved solution and its associated cost, schedule, benefits, and technical baselines. The third level processes implement the approved solutions in accordance with the approved baselines.

3.6.3 Multi-party / organizations

A multi-organizational project management system has to provide full lifecycle tracking of business activities of a complex mix of governmental entities and business organizations. It can be provided by maintaining a secure database of data or records to track such activities. The system provides secure sharing of information among governments and organizations by controlling access to data based on organizational membership and assigned role of system users. The system provides flexible structural relationship among the various data. A graphic web-based user interface of the system enables efficient access to data entities for the input and update of specific data. A multi-organizational project management method must manage and process both structured and unstructured data. It uses data oriented design concepts and document management core functionalities to solve problems associated with managing multi-jurisdictional activities for governance organizations, or for managing other projects, programs, events, actions, incidents, contracts, bids, funds or exercises that involve multiple unrelated organizations. Multiple people, from multiple organizations, can enter and update information and data, allowing information to be entered at its source. This would create a way to manage, arrange and control the information of a system of systems effectively, clearly and easily to all users involved.

3.6.4 SoS applications in all fields

There are a variety of SoS applications that can be applied in the management of emergencies and crisis, both in the short-term and long term.
Implementations of new technologies already provide a more comprehensive, reliable and functional service. A clear example is the implementation of systems of systems and distributed systems that

automate the process of crisis management and provide a degree of interoperability unknown so far. Short-term strategies can be summarized in the following points:

- Training and expertise.
- Implantation of nano-technology in SoS field. An example of this technology is the nano-transducers applied to a sensor network. Some of the applications of this sensors network in a SoS are environmental management, fire management, management of robberies and intrusions, presence control and control of lighting.
- Improved algorithms for pattern recognition, computer vision and decision making.
- New information and communications platforms such as "Cloud Computing". This offers information services and computing resources over the network, enables the collaboration between different actors in the emergency management and ensures automated updated information fast due to the large amount of computing resources provided.

In the long term, the following technology application can facilitate the management of crisis and emergency situations:

- Intelligent buildings and smart cities. Improvements and price reduction of new sensors, has enabled a wide range of parameters to be precisely measured such as the temperature of each brick outside a building, the oxygen and CO_2 levels inside each office, etc… The monitoring of these parameters greatly contributes to managing emergency situations more efficiently. It also allows active monitoring of buildings and helps avoid accidents, such as leaving open a gas spigot. Further into the future intelligent cities are expected to gain prominence. Development and application of nano-technology and miniaturized surveillance networks will be a big step forward. The integration of electronic components in 3D wafers will allow the improvement of existing sensors and integrate them into everyday objects such as clothing items, urban infrastructure and power grids. This degree of integration will allow the monitoring of large areas, at a lower cost and with higher efficiency and reliability.

4. Recommendations

Important points to emerged through the roadmapping workshop were:

- Consider the emergency as a whole: pre, during and post.
- Information collection is very important for prevention.
- External factors like energy supply are important and need to be taken into account.
- Emergencies are managed by people; therefore people should be informed and trained.
- Health risks should be also considered, as well as the crisis caused by virus/bacteria.
- Current technologies are not mature enough.

4.1. Technological recommendations

The following **technological recommendations** could be in consideration in future European researches in the emergency and crisis management domain:

4.1.1 Interoperability of heterogeneous systems: Standards, interfaces, protocols

Communication and information exchange standards, interfaces and protocols should be developed that facilitate different systems or networks to communicate and exchange information in real time. This will enable the timely resolution or prevention of a dangerous situation.

4.1.2 Real-time systems, real-time communication, data acquisition

The concept in the information management to anticipate or prevent a catastrophe is the same in all emergencies. To be able to correctly solve a hazardous situation it is of vital importance to have all the necessary information in order to know the cause of the situation, handling thus all parameters that contribute to find a solution. This acquired information must be available in real time for all the parties involved in resolving the crisis: fire-fighters, police, emergency units, military, etc.

4.1.3 Smart sensors

The development and implementation of interconnected smart sensor networks that can carry and make available important information to a system itself as well as other systems is important for a timely resolution of a crisis or an emergency.

4.1.4 Networking capabilities, sufficient data rate, communication channel speeds

There are many capabilities able to be solved by a system network. There are many situations in which a smart grid of sensors can help to resolve an emergency situation. The combination of a high number of sensors makes this task easier due to the large amount of information able to be managed.

4.1.5 Big Data including increased complexity

The three main characteristics of big data are: volume, speed and variety. Big data provides knowledge to institutions, improving as such the service offered to citizens and contributing to solve problems. Systems that allow the management and real time access to big data can provide a real benefit in a crisis and emergency situation.

4.1.6 Improved algorithms (automated reasoning, autonomous decision making, etc.)

An improved system for pattern recognition and identification of objects will allow the use of automated systems in direct intervention and crisis resolution catastrophes with a lower rate of errors in decision-making. Decision Making
In the management of emergencies and crisis decision-making cannot be automated and still involves human participation. Visualisation systems for real time information processing can assist the resolution of a crisis to be faster and more effective.

4.1.7 Modeling and simulation tools for SoS

In the field of emergency situations, modeling and simulation tools are very important as they enable the forecast and prevention of undesirable outcomes to specific situations. They greatly contribute to identify the best solutions available for each situation. These modeled and simulated systems will be useful to create warning and monitoring systems to avoid hazards and predict disasters.

4.1.8 Architectures

The combined and coordinated actions of the different parts of a system can achieve more results than all the parts acting independently. This concept known as “synergy” is critical in the field of emergency management. These systems have three main tasks to address: (i) communication between actors involved; (ii) data processing; and (iii) decision making unit. Designing and developing suitable architectures and / or frameworks for different emergency situations can result to better, faster and more efficient use of available resources and prevention of loss of human lives.

4.1.9 Governance, Emergence, Life-cycle-issues

The emergency domain directly involves people, either rby impacting human's life or by being managed directly by people (operating in the field or taking decisions on how to act). Current governance models should be reviewed or new models developed to be concise and clear to all different actors involved.

Stability, reliability, resilience and dependability are the main characteristics of a system of systems, independently of its field of application. However, these have a special significance in the management of emergencies. There is a great need to increase the stability of an emergency-oriented SoS, ensuring that it is robust and safe when a catastrophe occurs. It should also be reliable and functional in order to ensure that it will still work when one of its parameters become unstable or fail. The SoS also must be flexible in order to adapt its various systems to a variable workflow. or to allow each of its systems to be adaptive and complement the functions of another system.

4.2 Social recommendations

The following **social recommendations** should be taken into consideration in future European research programmes in this domain:

4.2.1 Establish business model demonstrators

Emergency is a domain that affects directly people and goods, therefore the socio-economical needs of SoS in the emergency domain are mostly addressed to:

-increase people capacity and qualifications in order to offer a better service and response when dealing with an emergency;

-develop new business models that allow many different private companies to develop and provide the required equipment, technologies and materials to public organisations dealing with an emergency or crisis situation. Or develop appropriate models for private enterprises to participate in the resolution of an emergency or crisis. Identify means of resolving problems related with multiple ownership in SoS

In SoS oriented to emergency and crisis management, the problem of multiple ownership is quite important as:

- There are incompatibilities between public and private agencies responsible for the safety of an area
- There is lack of protocols and clear hierarchies established between different territorial governments
- There is lack of clarity as to the organization and control of various security entities such as the national police, municipal police, civil guard, military, etc.

4.2.2 Demonstration

In the emergency domain, the risk-benefit is normally unclear, since the major goal of any operation is to secure human lives. In this context, all potential resources must be used and mobilized. Demonstrators will play a major role to define situations and analyze better ways to act.

4.2.3 High upfront investment

Despite the high investment required to implement technological systems related to security, this investment is amortized over the medium term.

4.2.4 Education is not sufficient among decision-makers

In the emergency field, final decision should be taken by the person in charge of each emergency. In many cases, different persons are involved to support the decision maker. The lack of knowledge about SoS could be a problem when dealing with different systems that should be interconnected and well-coordinated, since some important information can be missed. The resistance to change and learn about SoS and NT is one of the barriers of SoS.

4.2.5 Human machine interface (HMI)

Emergency human–machine interfaces (HMIs) could be used to avoid or minimize losses. These interfaces should be designed to accommodate the human capabilities that have been altered by danger-induced emotional responses. In a modern socio-technical or human–machine system, when an emergency arises, it invariably involves interaction with technology and appropriateHMIs need to be developed to communicate, neutralize or eliminate the imminent dangers posed by such an emergency.

4.2.6 Security and privacy, IP-issues

In managing a hazard, emergency bodies are responsible for analyzing all the information available and controlling a situation and acting in the most optimal way in order to best resolve or prevent an emergency. Advanced access to information like, emergency location, terrain, buildings, internal building layouts in the affected area, existence of hazardous substances, number of people with special needs such as handicapped, elderly, children, etc. can be critical. They should also receive information about individuals involved in the emergency (health reports, nationality, home location, etc.). This information should be treated in confidence and only be accessible during the emergency situation. Clear protocols and procedures need to be established and follow on check up mechanisms to ensure that any information is not misused or accidentally released into the public domain.

References

This deliverable is based on inputs from Road2SoS deliverables D1.1 (Report on data collection and analysis of relevant European and international RTD projects/ initiatives), D1.2 (Interviews summary report), D2.2 (Market survey summary report) and D2.3 (Socio-economic summary report), which built the basis for the "pre-populated" roadmap (see 2.2 Phase 1: Data collection and analysis). References can be found in the respective deliverables.

To build the roadmaps, various Road2SoS workshops have been held, namely the "Road2SoS Expert Panel" May 22nd 2012 in Karlsruhe, "Road2SoS-Roadmapping Workshops" September 2012 – October 2012 in Paris, Brussels, Madrid. More information on these workshops can be found in the deliverables D1.3 (Expert Panel meeting minutes) and D3.2 (Minutes of the Roadmapping Workshops).

To mature and validate the roadmaps, 12 "case studies in industry" and 8 "dissemination workshops" have been conducted. Detailed information can be found in the deliverables D4.1 (Case Studies) and D6.2 (Dissemination Workshops Report).

Additional References

[1] The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company.
[2] Road2SoS Project. "Cross-Domain Commonalities" (2012)
[3] T-AREA-SoS Project, Deliverable D2.1, "State of the Art on Systems of Systems Management and Engineering" (2013). https://www.tareasos.eu/docs/pb/SoA_V3.pdf
[5] Renu Sinha,"Impact of experience on decision making in emergency situation", Lulea University of technology (2005)

ANNEX I. GLOSSARY OF TERMS

- ✓ Trends and drivers

Term	Explanation
Systems integration	Process of linking together different computing systems and software applications physically or functionally, to act as a coordinated whole.
Internet of things	A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability
Unmanned Vehicle	Vehicle without a person ("man") on board. Unmanned vehicles can either be remote controlled or remote guided vehicles, or they can be autonomous vehicles which are capable of sensing their environment and navigating on their own.
Unmanned Aerial Vehicles (UAV)	Aircraft without a human pilot on board. Its flight is controlled either autonomously by computers in the vehicle or under the remote control of a pilot on the ground or in another vehicle.
Smart city	A city can be defined as 'smart' when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic development and a high quality of life, with a wise management of natural resources, through participatory action and engagement. Implies a new kind of governance, genuine citizen involvement in public policy.
Streaming	It is the distribution of multimedia through a network of computers so that the user consumes the product at the same time that you download. The streaming Word applies to a direct current (without interruption). These kinds of technology works via a data buffer that will store what is going low at the user station then show you the stuff. This is opposed to mechanism of downloading files, requiring the user to download full files to gain access to your content. The term is usually applied to the dissemination of audio or video. Streaming requires a connection by the less than equal bandwidth service transmission rate.

Cloud Computing	General term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). It is a new model of business services and technology that even allows the user to access a catalog of standardized services with them and respond to the needs of your business, in a flexible and adaptive, if not predictable or demands peak workloads, paying only for the consumption made, or even free if providers are funded by advertising or nonprofit organizations.

✓ Needs and benefits

Term	Explanation
Decision making	Decision making can be regarded as the cognitive process resulting in the selection of a course of action among several alternative scenarios. Every decision making process produces a final choice. The output can be an action or an opinion of choice.
Real-time	A system in real time (STR) is that digital system that actively interacts with an environment with dynamic known in relation to their inputs, outputs and time constraints, to give you a proper functioning in accordance with the concepts of predictability, stability, controllability and reachability. Real-time systems are present in our everyday life, practically in everything that surrounds us; in planes, trains and automobiles; in the television, washing machine or microwave, cell phones and the digital telephone exchanges. They are an essential element to ensure the generation, transmission and distribution of electric power and to ensure the quality and safety of countless industrial processes.
Database	A database is an organized collection of data. The data are typically organized to model relevant aspects of reality in a way that supports processes requiring this information. For example, modeling the availability of rooms in hotels in a way that supports finding a hotel with vacancies. Database management systems (DBMSs) are specially designed applications that interact with the user, other applications, and the database itself to capture and analyze data. A general-purpose database management system (DBMS) is a software system designed to allow the definition, creation, querying, update, and administration of databases.
Digital Right Management	DRM is a generic term that refers to access control technologies used by publishers and copyright holders to limit usage of digital media or devices. It is also used to refer to restrictions associated with specific instances of

	digital works or devices. The DRM overlap to some extent, with software copy protection.
SIP standard	Session Initiation Protocol (SIP) is a protocol developed by the Working Group MMUSIC of the IETF with the intention of being the standard for initiation, modification, and termination of interactive user sessions where involves multimedia elements such as video, voice, instant messaging, online gaming and virtual reality. The syntax of operations is similar to HTTP and SMTP protocols used in Web pages and e-mail distribution services respectively. This similarity is natural since SIP was designed to provide telephony to become one service on the Internet.

- ✓ Technologies and capabilities

Term	Explanation
Computer simulation	A computer simulation runs on a single computer, or a network of computers, to reproduce behavior of a system. The simulation uses an abstract model (a computer model, or a computational model) to simulate the system. Computer simulations have become a useful part of mathematical modeling of many natural systems in physics (computational physics), astrophysics, chemistry and biology, human systems in economics, psychology, social science, and engineering. Simulation of a system is represented as the running of the system's model. It can be used to explore and gain new insights into new technology and to estimate the performance of systems too complex for analytical solutions
Modeling and simulation	Get information about how something will behave without actually testing it in real life. It includes emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making managerial or technical decisions. The terms "modeling" and "simulation" are often used interchangeably.
MAS (Multi-agent systems)	It is a computerized system composed of multiple interacting intelligent agents within an environment. Multi-agent systems can be used to solve problems that are difficult or impossible for an individual agent or a monolithic system to solve. Intelligence may include some methodic, functional, procedural or algorithmic search, find and processing approach.
Image indexation	An indexed image stores an image as two matrices. The first array has the same size as the image and a number for each pixel. The second array is called a color map may differ from the size of the image. The numbers of the first matrix is an instruction on what color to use as the color map. So all indexed images have a color map associate that you cannot leave.

CMOS	Complementary Metal Oxide Semiconductor is a logic families used in the manufacture of integrated circuits. Its main feature consists in the combined use type P-MOS transistor and N-MOS type configured such that, at rest, the power consumption is only due to eddy currents. The majority of integrated circuits manufactured using CMOS technology. This includes microprocessors, memories, digital signal processors and many other types of digital integrated circuits whose consumption is considerably low. In a CMOS circuit, synthesize logic function is implemented in duplicate by two circuits: one based exclusively on P-MOS transistors (pull-up circuit), and another based solely on N-MOS transistors (pull- down circuit). The P-MOS circuit is used to propagate the binary value 1 (pull-up), and the N-MOS circuit to propagate the binary value 0 (pull -down).
Redundant systems	In computer engineering, are those that repeat those hardware data or critical character you want to insure against possible failures that may arise from continued use. It is presented as a solution to the problems of protection and reliability. This type of system is responsible for performing the same process in more than one season, because if for some reason one stops working or collapse, immediately another would have to take his place and perform the above tasks. Redundancy techniques have been used by the military and aerospace industry for many years to achieve high reliability. A replicated database is a distributed system such as redundant. Apart from the existing servers that have multiple CPUs and memory modules, redundant devices on a server usually hard drives, network cards and power supplies.
Big data / Meta data	Big data is the term for a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications. The challenges include capture, duration, storage, search, sharing, transfer, analysis, and visualization. The trend to larger data sets is due to the additional information derivable from analysis of a single large set of related data, as compared to separate smaller sets with the same total amount of data, allowing correlations to be found to "spot business trends, determine quality of research, prevent diseases, link legal citations, combat crime, and determine real-time roadway traffic conditions.
Meta data	The term metadata refers to "data about data". The term is ambiguous, as it is used for two fundamentally different concepts (types). Structural metadata is about the design and specification of data structures and is more properly called "data about the containers of data"; descriptive metadata, on the other hand, is about individual instances of application

	data, the data content. In this case, a useful description would be "data about data content" or "content about content" thus metacontent. Descriptive, Guide and the National Information Standards Organization concept of administrative metadata are all subtypes of metacontent
Distributed computing	Distributed computing is a field of computer science that studies distributed systems. A distributed system is a software system in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal. There are many alternatives for the message passing mechanism, including RPC-like connectors and message queues. Three significant characteristics of distributed systems are: concurrency of components, lack of a global clock, and independent failure of components. An important goal and challenge of distributed systems is location transparency. Examples of distributed systems vary from SOA-based systems to massively multiplayer online games to peer-to-peer applications.

- ✓ Enablers

Term	Explanation
Multi-party	It is a recent trend in public and private interorganizational policy that multiple actors get involved to collaborate around issues of water and soil management, nature preservation, land use, farming practices, introduction of new technologies in life sciences and related problem domains.
Virtual training	Virtual training is a training method in which a simulated virtual environment is used. In this environment an instructor is able to explain, show or test certain abilities that can contribute to the learning process.
Embedded systems	An embedded or embedded system is a computer system designed to perform one or a few dedicated functions often in a computer system in real time. Contrary to what happens with general purpose computers (such as a personal computer or PC) that are designed to cover a wide range of needs, embedded systems are designed to meet specific needs. In an embedded system the majority of components are included in the motherboard (video card, audio, modem, etc.) And often the resulting devices did not have the appearance of what is usually associated with a computer. Examples of embedded systems may be devices such as a taximeter, a system access control, and the electronics controlling a

	vending machine or the control system of a photocopier including multiple applications.