Security research in Italy

Security Research in Italy 2014

VOL. 4

Preface

In these latest two years, the National Technological Platform SERIT (Security Research in Italy) has carried on a set of activities addressing the preparation of Horizon 2020 Research Programme, officially launched by the European Commission in December 2013.

Since the 2013, SERIT has been working out a list of Priorities in Security Research, starting from those themes proposed in the previous SERIT Roadmap. SERIT has also engaged a dialogue with the European Commission, by proposing these National priorities as possible contribution to the topics' content for the first two calls of Horizon 2020. As a main achievement, several of the proposed topics have been successfully integrated and are now part of the official Work-Programmes of Horizon 2020.

For the current 2014, with this document, SERIT objective will be to diffuse a greater knowledge about those funded FP7-Security Projects, that have been leaded by Italian organizations, by widely disseminating the main results reached throughout the research activities. SERIT plans also to strengthen the dialogue with the stakeholders and end-users' arena, in order to focus their emerging needs and to maximize the impact and the exploitation of achieved results.

Through these success' stories and after more than three years of official activities, SERIT aims, as the ultimate goal, at strongly providing National Institutions Representatives in charge of the National Research planning with a comprehensive set of recommendations about the Italian Security needs, in order to align the future Italian Research Agenda on Security with the identified SERIT priorities.

A wide set of research opportunities will be also generated at Regional level, stemming from the Smart Specialisation Strategy process.

We would like to sincerely thank all those have been working to achieve this important goal, which represents an important step towards the National Technological Excellence in Security, which will be also reflected at European Level.

Cristina Leone and Fabio Martinelli, *SERIT Chairmen*

SEcurity Research in ITaly vol. 4 has been partially funded by

Summary

Preface ..... p. 1
What is SERIT? ..... p. 4
ADVISE ..... p. 7
AFTER ..... p. 11
ARGUS 3D ..... p. 16
BONAS ..... p. 20
CockpitCI ..... p. 22
CoMiFin ..... p. 24
CUSTOM ..... p. 27
DIRAC ..... p. 30
INSPIRE ..... p. 32
ISTIMES ..... p. 34
MICIE ..... p. 38
MODES_SNM ..... p. 41
NI2S3 ..... p. 44
OSMOSIS ..... p. 47
PLANTFOODSEC ..... p. 51
PROACTIVE ..... p. 54
PROTECTRAIL ..... p. 57
SeaBILLA ..... p. 60
SECONOMICS ..... p. 63
SESAME ..... p. 66
SICMA ..... p. 69
STRUCTURES ..... p. 72
Progetti 5 call Security (FP7-SEC-2012) ..... p. 75
DESTRIERO ..... p. 77
ESENET ..... p. 78
GAMMA ..... p. 79
ISITEP ..... p. 81
SAWSOC ..... p. 83
SNOOPY ..... p. 84
SPARTACUS ..... p. 85
TAWARA_RTM ..... p. 86
TRITON ..... p. 87
NESSoS ..... p. 88

What is SERIT?

SERIT is the Italian Technological Platform, jointly launched by the National Research Council - CNR and Finmeccanica, which engage Italian industries (both large industries and SMEs) together with academia, research centers, national stakeholders and end-users, in order to develop and promote a National Research Agenda driving the future technological developments, while answering to a list of National Security needs.

SERIT competences had been organized according to a **Matrix** structure, composed by **8 Missions** (so called **Settori Guida- SG**-), representing those different areas that mainly characterize the Security aspects and needs in Italy, and **7 Technological Areas (TA)** , regrouping technologies by "family" and where have been identified a list of technological priorities.

Missions:

- SG 1 – Transportation Security;
- SG 2 – Energy Supply System Security;
- SG 3 – Borders Security;
- SG 4 – Cyber security;
- SG 5 – Agrifood Security;
- SG 6 – Health Security;
- SG 7 – Integrated Safety and Security of Cultural heritage and Built Environment;
- SG 8 – Smart Cities Security.

Technological Areas:

- TA 1 – Surveillance and Situation Awareness;
- TA 2 – Communications;
- TA 3 – Detection & Identification Systems;
- TA 4 – Technologies for Crisis Management & People, Assets and Infrastructures Protection;
- TA 5 – Information Processing & Management;

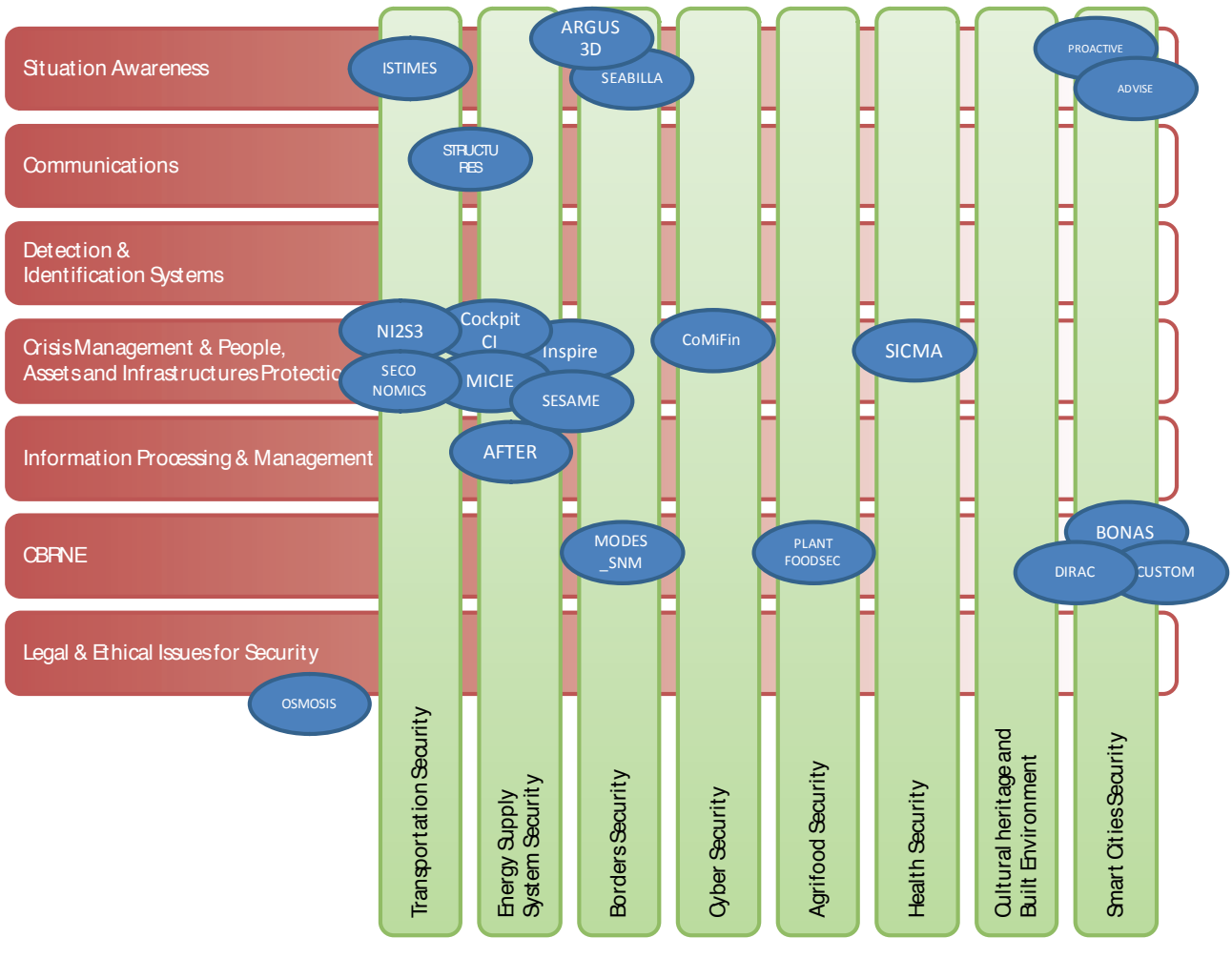
- TA 6 – CBRNE;
- TA 7 – Legal & Ethical Issues for Security.

SERIT set up several ambitious high-level objectives:

- To Reinforce the National and International Cooperation and competitiveness:
  - SERIT aggregates a number of experts and competencies under different domains, stimulating a fruitful network among stakeholders, users , technologies experts and national institutions;
  - SERIT promotes a dialogue with end-users and national stakeholders to bridge the industrial and academic research with the real needs and requirements expressed by users;
  - SERIT acts as a catalyst, in order to give members to access to national and European funds for research.
- To Promote the development of Human resources in Security research:
  - SERIT aims to promote and to develop the human capital in security, by promoting and supporting PhD. in collaboration with industries and academic members of the platform, in order to maintain the national excellences and the know-how in security research.
- To Develop a research agenda of the security community in Italy that is also coherent with the European vision.
  - SERIT already prepared two volumes with the identified research topics (for 2011 and for 2012) and a third volume that represents a contribution in terms of research priority topics for Horizon 2020 work programmes.

This volume aims to present an overview of FP7- Security research projects, leaded by Italian organization.

In this publication, SERIT will describe those projects for whose the European Commission have already signed the grant by end of last 2013, proposing a detailed description of those projects on- running for one year at least. In the following picture, the mapping of these projects on SERIT TA/SG Matrix is shown.



The detailed description of the projects follows.

ADVISE / *Advanced Video Surveillance archives search Engine for security applications*

Info

Call:	FP7-SEC-2011-1
Total Cost:	4,237,304.80 €
EU Funding:	2,989,761.60 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total Cost for Italy:	1,470,259.20 €
Eu Funding for Italy:	969,572.40 €
Website:	http://www.advise-project.eu

Abstract

In contemporary societies, video surveillance forms an integral part of incident investigation. Trails of delinquent activities may be left behind and captured/recorded by various surveillance systems. In many cases the investigation of a crime incident involves collecting and analysing video surveillance data from the crime scene.

In order for such an investigation to be successful, it is important to effectively uncover the trails and the association between suspects that can lead to the identification of accurate incriminating evidence. In this case, the investigators should be in a position of having access to a plethora of video surveillance information and the appropriate tools to perform sophisticated searches on the video archives, so as to pinpoint those video frames that reveal the evidence of criminal activities.

ADVISE aims at designing and developing an extensible framework that after negotiating all relevant legal, ethical and privacy constraints, is able to help the law enforcement authorities to fight against criminal activities, via efficient evidence mining into multiple, heterogeneous video archives. More in particular, ADVISE analyses and geo-registers surveillance video archives of different agencies, extracts statistical patterns of activity and searches (context-based and content-based) for specific events, people and objects through ontologies and semantic representations.

Main technological and scientific outcomes

In a context where surveillance systems are continuously growing in scale, heterogeneity and capabilities, two major obstacles have to be overcome. On one hand, the variety of technical components of surveillance systems, producing video repositories with different compression formats, indexing systems, data storage formats, sources, has to be addressed. On the other hand, the legal, ethical and privacy rules that govern surveillance and the produced content have to be taken into account.

To address these two major issues, the ADVISE system is composed by three major components:

- The first one performing the semantically enriched, event based video analysis which offers efficient search capabilities of video archives and sophisticated result visualization: ADVISE is able to extract statistical patterns of activity from video archives and search for specific events, people and objects through ontologies and semantic representations;

- The second one enforcing the legal, ethical and privacy constraints that apply to the exchange and processing of surveillance data: ADVISE takes into careful consideration the legal, ethical and privacy rules that govern surveillance and the produced content;
- Moreover, in order to support interoperability, the exchanged content and the associated metadata are transformed into a common format, while a dedicated ADVISE Engine efficiently deals with each surveillance and collaborating authority's technical and legal/ethical/privacy specificities.

Products/Operational Prototypes validated by End-users

An operational prototype has been designed and developed by the ADVISE consortium, providing three main features to help investigators' tasks, in the context of an investigation based on video material:

- Video Analysis: the Video Analysis feature processes the set of videos and identifies a set of predefined events. To accomplish this purpose, a list of objects and their respective actions (if applicable) are identified in the processed videos.
- Video Search: all extracted information are used by the Video Search feature, thus supporting searches on the information by law enforcement authorities.
- Video Access: it enables access to the video fragments matching the search query, after anonymising the personal and sensitive data that are not related to the search.

A workshop target to ADVISE users has been arranged in London, on the 19th of December 2013. During the workshop, the invited users had the possibility of playing with the current system, testing all the provided functionalities and providing their feedback.

The first operative prototype has been developed and tested by the Madrid Police agency. A final prototype is currently under development.

Main users of the ADVISE system are the ones using intelligent video surveillance systems for video pre-processing and search engine solutions, in particular, all organisations which have to manage CCTV footage. ADVISE users can belong to both the public and private sector, across a range of areas such as national defence and security, critical infrastructure, banking, employment, energy and utilities, entertainment, finance, government, healthcare, policing and justice, retail, telecommunications, travel and transport.

- Public sector (Homeland Security, law enforcement agency, Prisons, Public transports): national and local governmental agencies are increasingly turning to video surveillance solutions utilizing high-resolution image acquisition and behaviour pattern analysis software to detect and flag suspicious individuals.
- Private sector (Banking/Finance, Casinos/Gaming Retail/Commercial Corporate Hotels): they typically use surveillance systems with a considerable number of cameras which cover large areas and big amount of footage to be storage and processed in case of necessary. As a consequence, they mainly need video search as a service in the case something happens and they have to investigate analysing the stored video footage.

Follow-up

The Consortium is currently discussing the exploitation of project results at Consortium and partner level.

New technological, scientific or application perspective opened by the project

One of the main innovation of ADVISE system is the identification and tracking of suspects in video content performed by automatic extraction and semantic correlation of low-level events, taking into account legal and ethical constraints.

The project is closely integrated with other ENGINEERING initiatives on security intelligence, such as: SINTESYS (Security Intelligence System), an italian research project (PON) coordinated by ENGINEERING; LASIE (LArge Scale Information Exploitation of Forensic Data), an Integration Project in the topic SEC-2013.1.6-1 Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes of the Security Programme.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

The project is related to interesting topics of the Horizon 2020 Secure Societies 2014-2015 Work Programme. This Work Programme is focused on protecting citizens, society and economy, infrastructures and services, political stability and well-being taking into account the respect of privacy and civil liberties.

Specifically the reference area for the topics addressed by the project is “FCT - Fight against crime and terrorism”, which includes the following related topics:

- FCT-1-2015: Forensics topic 1: Tools and infrastructure for the fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation
- FCT-4-2015: Forensics topic 4: Internet Forensics to combat organized crime
- FCT-6-2015: Law Enforcement capabilities 2: Detection and analysis of terrorist-related content on the Internet
- FCT-10-2014: Urban security topic 1: Innovative solutions to counter security challenges connected with large urban environment.

Etichal aspects to be developed

A Private Impact Assessment has been conducted on the whole system i.e. the assessment of the impacts of the ADVISE system and of its components thereof on ethics, privacy and data protection. The whole system has been designed and developed following the recommendations deriving from such Privacy Impact Assessment. The ADVISE system offers the highest possible level of observance of ethical and legal principles provided that

It is used exactly as specified within the project.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	Engineering – Ingegneria Informatica Spa	ENG	Italy
2	Neuropublic A.E. – Pliroforikis & Epikoinonion	NPE	Greece
3	Centre for Research and Technology Hellas	CERTH	Greece
4	Quenn Mary and Westfield College – University of London	QMUL	UK
5	Singularlogic Anonymos Etairia Pliroforiakon Systimaton & Efarmogon Pliroforikis	SL	Greece
6	Vrije Universiteit Brussel	VUB	Belgium
7	Ingeniera de Sistemas parla la Defensa de Espana SA	ISDEFE	Spain
8	Almaviva – The Italian Innovation Company Spa	ALMAVIVA	Italy
9	Innovation Engineering Srl	IE	Italy
10	Ayuntamiento de Madrid	MADRID	Spain

AFTER / *A Framework for electrical power sysTems vulnerability identification, dEfense and Restoration*

Info

Call:	FP7-ICT-SEC-2007-1 Joint Call ICT & Security 1
Total Cost:	5,050,456 €
EU Funding:	3,473,803 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total Cost for Italy:	1,451,337 €
Eu Funding for Italy:	1,088,915 €
Website:	http://www.after-project.eu

Abstract

This project addresses the challenges posed by the need for vulnerability evaluation and contingency planning of the *energy grids and energy plants* considering also the relevant ICT systems used in protection and control. Our emphasis is on cascading events that can cause catastrophic outages of the electric power systems

The main addressed problems are related to high impact wide spread multiple contingencies, the most significant wide area criticality. This kid of contingencies and the following cascading effects can be caused by deliberate acts of terrorism, sabotage, criminal activity, malicious behaviour etc or they can simply be caused by a combination of accidents, natural disasters, negligence.

Both risk analysis and risk mitigation will be pursued.

In particular, two major objectives are addressed.

1. To ***develop a methodology and tool for the integrated, global vulnerability analysis and risk assessment*** of the interconnected Electrical Power Systems considering their interdependencies. This objective meets the TSO (Transmission System Operator) need to overcome current approaches based on separate evaluations of either power system or ICT system. Further, the adoption of risk concepts allows a more in-depth, quantitative evaluation of the security of the electrical power system.

2. To ***develop algorithms and tools supporting contingency planning*** in a two-fold approach:

   - preventing or limiting system disruption, by means of physical security techniques and defence plans; and

   - re-establishing the system after a major disruption, by means of restoration plans.

To this aim, AFTER propose the use of the global risk assessment methodologies as a support to defence plan design. A language to model defence plans functionalities and ICT architecture is developed. New defence plan concepts are also introduced to cope with emergency situations.

Restoration is dealt with by dedicated methodologies and support tool to identify efficient optimal restoration plans requiring intelligent reconfiguration of the electric grid.

An evaluation phase will demonstrate the benefits of the proposed techniques in terms of overall risk monitoring and emergency situation management.

All the major developments of the Project will be discussed with the TSOs/Electricity Plant owners partners of the Consortium and with an external **TSO Reference Group (TRG),** with the aim to keep adherence with the real operating needs.

Main technological and scientific outcomes

As an essential critical infrastructure of our society, electric power systems must be protected against failures due to natural and man-induced outages.

Although the level of vulnerabilities has increased significantly over time, current generation of Energy Management Systems, that served the power grids well with powerful computational tools for system security assessment, are very weak in dealing with cascading effects.

Furthermore, power dispatchers are left with essentially no support for risk assessment of the system vulnerability or wide area protection, control and restoration.

The state-of-the-art in power system engineering does not provide a systematic method to predict vulnerable operating scenarios and determine automatic or supervised reconfiguration and control actions.

Although a massive amount of data is being collected from new technologies such as PMUs, there is no widely adopted method on how the new data will be used for wide area vulnerability assessment, protection and control.

As a matter of fact it is a stringent need to achieve high availability of electrical power supply to the users and, only in case of extremely critical events, actually resulting in blackouts, limit the amount and duration of affected users and restore full service in a short time. This goal requires diverse and complex activities both in planning and in operation stages. In particular, to a greater extent than in the past for the motivations presented above, it is generally agreed that the effects of interdependencies between the electrical power system and other systems (primarily the ICT systems), as well as of the electrical power system interconnections with neighbouring electrical power systems have to be considered.

AFTER *project aims at* increasing the TSO capabilities in *creating*, *monitoring* and *managing* secure interconnected electrical power system infrastructures, able to survive to *major failures* and to efficiently *restore* service supply after major disruptions.

These objectives are pursued with the definition of a framework, methodologies and tools to enhance the security and resilience of complex energy systems, in particular for:

1. risk assessment (*hazard, vulnerability* and *impact analysis*) of the interconnected and integrated electrical power and ICT systems;
2. design and assess of global defence and restoration plans.

We propose to develop analytical methods for the interconnected energy grids and provide tools to mitigate the impact of accidents and attacks on these networks.

AFTER project, will end in 2014, September 30rd, will achieve several results:

- To develop the concepts and techniques for physical security: *intelligent*, *distributed monitoring* and *early warning* of physical intrusions;
- To develop tools to *protect* the critical infrastructures *against cascading events*, including those caused by *natural disasters* and *sabotage;*
- To perform contingency analysis of the transmission and distribution networks/grids and *determine automatic restoration* and *intelligent reconfiguration;*
- To develop *sensing*, *monitoring*, *communications*, and *software agent technologies* for *security monitoring* and *early warning;*
- To provide a *structure for integration* of the results.

All the outcomes of the research phase and methodology construction were put in actual implementation focusing on the relationship with SCADA systems which due to the evolution of the embedded systems and the ability to integrate and interconnect low level controlling systems in distributed architectures will reserve a special care on protection of the infrastructures which should enable this type of scenarios.The first result of AFTER is a **methodology**, supported by a **tool,** for ***global risk*** assessment, vulnerability identification and risk analysis, of the electrical power system considering the relevant wide area ICT system used for control and protection.

The second major result is the definition of algorithm and tools for the identification of ***global defence plan*** to prevent system disruption. A necessary step consists in the definition of modelling techniques of defence plan functionalities and architecture, including new wide area fast acting defence plans schemes for power and ICT criticalities, in order to integrate them into the overall system model.

Concerning **contingency planning** to **restore service after disruption**, the major outcome of AFTER will be is a decision support **methodology** and prototype **tool**, based on optimization techniques, for the efficient power and ICT systems ***restoration***.

Application scenarios

The table below summarises the main outputs of AFTER and the possible **application scenarios**.

(1) Global vulnerability and risk assessment of electrical power system considering the relevant ICT systems

- *operations*: support operators in power system monitoring and supervision to identify high risk system operating conditions, thus allowing to take preventive actions (e.g. generation redispatching)
- *operational planning*: support operators in power system operational planning (day ahead to some days ahead); identify forecasted system operating conditions (also resulting from market rules) presenting high risk, thus allowing to call for preventive actions (e.g. generation rescheduling)
- *planning*: support planners in analysing the risk level associated to forecasted development scenarios.

(2) New defence plan concepts and defence plan design support

- *planning*: support engineers in global defence plan design. By means of the risk assessment tool, planners can assess: the new defence plan concepts proposed within the Project and the effectiveness of different defence plan solutions (architectures, settings, etc.) in reducing operational risk.

(3) Restoration support

- *planning*: planners can assess the effectiveness of different restoration solutions
- *operations* (*restoration*): operators can be supported in the restoration process in identifying the best restoration actions.

Products/Operational Prototypes validated by End-users

Prototype tools will be developed and assessed by end users in 2014.

Follow-up

New technological, scientific or application perspective opened by the project

Approciation of risk assessment method in operation and operational planning of transmission network .

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

- Methodology application in demo;
- Operational planning methods and tools taking into account risks;
- Risk based planning of power system;
- Methodology extension to cover several kind of threats;
- Integration of big data.

Etichal aspects to be developed

- Integration with current operational practice;
- Tools efficiency.

Socio-economic aspects to be developed

Cost benefit analysis of risk based methods.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Enea - Ricerca sul Sistema Elettrico**	**ERSE**	Italy
2	Agenzia nazionale per l'energia, le nuove tecnologie e lo sviluppo economico sostenibile	ENEA	Italy
3	SINTEF EN	SINTEF-EN	Norway
4	SINTEF ICT	SINTEF-ICT	Norway
5	Genoa University	UNIGE	Italy
6	University College Dublin	UCD	Ireland
7	City University - London	CU	UK
8	ALSTOM	ALSTOM	France
9	SIEMENS	SIEMENS	Germany
10	Commission of the European Communities - Joint Research Centre	JRC	Belgium
11	ELIA	ELIA	(TSO) Belgium
12	Terna Rete Elettrica Nazionale SpA	TERNA	(TSO) Italy
13	CEPS, a.s.	CEPS	(TSO) Czech Republic

ARGUS 3D / *AiR GUidance and Surveillance 3*

Info

Call: FP7-SEC-2007-1 - SEC-2007-3.3-01 – Air 3D detection of manned and unmanned platforms

Total cost: 4.943.520 €

EU funding: 3.262.050 €

Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:

Total cost for Italy: 2.843.908 (57,63% of Total cost)

EU funding for Italy: 1.820.226 (55,80% of Total Funding)

Website: http://www.argus3d.eu

Abstract

The project aims to improve the detection of manned and unmanned platforms by exploiting the treatment of more accurate information of cooperative as well as non-cooperative flying objects, in order to identify potentially threats.

The scope will be reached by managing the 3D position data in region including extended border lines and large areas, 24 hours a day and in all weather conditions, derived from enhanced existing Primary Surveillance Radar (PSR), together whit conventional data and information coming via various passive radar technique in order to extend the airspace coverage and to enhance the target recognition capability of the surveillance systems.

Thus, the security could be enhanced in large areas, at sustainable costs, by improving the recognition of non-cooperative target through more accurate information on it's characteristics and/or more accurate positioning.

The final objective of the research consists of study, design and realization of a simple demonstrator of a low cost, interoperable, radar based, system able to identify, all kinds of non-cooperative threat with the contribution of data coming from:

- an innovative three-dimensional PSR;

- conventional sensors (Primary radar, Secondary radar, ADBS, etc…);

- a network composed by a multitude of multi-operational passive, bistatic and high resolution radar.

The system core will performs mainly an opportune Fusion of the such data and an accurate control of Consistency enhancing the early warning alerts capacities of final user based on a detailed 3D map of the area under surveillance with additional information on the nature of the target and on the alert level selected considering the track, the direction and a trajectory prediction of the target performed by the included Decision Support module.

Main technological and scientific outcomes

The scientific and technical objectives of ARGUS 3D project are:

- Studying, designing and implementing an innovative, low-cost, multi-sensor, radar-based system for 3D air guidance and that integrates conventional surveillance systems currently used for civil applications and two classes of non-conventional radar systems;
- Showing the possibility to use Passive radars, which are a special form of radar receiver that detect and track objects by processing reflections from non-cooperative sources of illumination already available in the environment (e.g. commercial broadcast and communications signals), as gap filler of the conventional ATM system in order to increase the visibility and the coverage at low cost;
- Developing of an innovative data fusion algorithm able to manage data from heterogeneous sensors based on JPDA (Joint Probabilistic Data Association) and IMM (Interacting Multiple Model) filter approach;
- developing a PSR with monopulse estimation capability in the vertical plane and therefore able to return the altitude information for any detected target;
- developing an innovative data management function able to provide a valid support to decision, suggesting the operator the countermeasures to defend, against the incoming threat, the area under surveillance.

Products/Operational Prototypes validated by End-users

A reduced version of the ARGUS 3D system composed by the a PSR with altitude extraction and a Passive Radar based on FM radio signals. During the test phase was made tests on both targets of opportunity (flight landing and taking off by the Fiumicino airport) and a cooperative target, provided by ENAV, that flight following a flight path agreed with the technicians. The demo was not made in real time, but the data on real targets was collected, stores, analyzed and showed to the final users in a different moment.

In ARGUS 3D project, during the validation phase an analysis, based on results coming from simulation analysis from an operative demonstrator that uses real data, was shown to the Final user (ENAV – Italian Air National Service Provider) involved in the project. In a second phase the same results were shown to a user group that involved operative users coming from different companies, such as Eurocontrol, Armed Forces Communications & Electronics Association (AFCEA), NATS UK (UK Air National Service Provider), UK Department of Transport (DFT), Elettronica, Vitrociset, etc.

During the demo the passive radar used for the test was developed by the university of Rome Sapienza. During the project life, SELEX Sistemi Integrati (now Selex ES) developed, with the support of the University of Rome Sapienza, a new product (AULOS) that is a passive radar based on FM/DVB-T radio signals that was tested both for air traffic control that for vessel control (this possible application of passive radar raised also during ARGUS 3D validation phase).

Follow-up

ARGUS 3D approach, with further developments, could be applicable at different contests, including Air Traffic Control and Air Defence. The presence, during the validation session, of people coming from different fields (military or civil) shows that the security is an issue both for military and civil application. Moreover, passive radar could be used also for different applications, such as coastal border control, vessel traffic control, but also to monitor cars and people in open space (e.g. vehicle in war field, or vehicle on airport landside/airside, etc.). These new applications could be further investigated in the future with new similar projects.

New technological, scientific or application perspective opened by the project

- New further analysis on passive radar could be focussed on innovative transmitter of opportunity that could increase the performance of the system.
- Some of the further transmissions of opportunity that could be used are related to new communication protocols such WiMax, etc.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

New themes on different applications of passive radar for surveillance of sea or land areas with a small environmental impact, low cost solution.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**SELEX ES**	**SELEX-ES**	Italy
2	SESM Scarl	SESM	Italy
3	Università “La Sapienza” di Roma - Dip. di Scienza e Tecnica dell’Informazione e della Comunicazione	UNIROMA1	Italy
4	BUMAR	BUMAR	Poland
5	University College of London	UCL	UK
6	Fraunhofer FHR	FHR	Germany
7	ENAV S.p.A.	ENAV	Italy
8	ECONET S.L.	ECONET	Spain
9	Dependable Real Time Systems Ltd.	DRTS	UK
10	ISO Software Systeme GmbH	ISO-GMBH	Germany
11	REDHADA S.L.	REDHADA	Spain
12	CiaoTech Srl	CIAOTECH	Italy

BONAS / *BOmb factory detection by Networks of Advanced Sensors*

Info

Call:	FP7-SEC-2010-1
Total cost:	3,488,360.01 €
EU funding:	3,488,360.01 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	794,827 €
EU funding for Italy:	794,827 €
Website:	http://bonas.tekever.com

Abstract

The aim of BONAS is to design, develop and test a novel wireless sensors network for increasing citizen protection and homeland security against terrorist attacks, in particular against the threat posed by IED devices.

The sensor network will focus on the detection of traces of precursors used in IED production (particulates, gases and/or waterborne) present in the environment surrounding the vicinity of a "bomb factory". The different sensors are specifically designed to be deployed in sensitive locations and easily camouflaged. This network will support the "factory's location", allowing an early threat thwart. A feasibility study will assess the usefulness and potential advantages that the BONAS concept will bring about in the future and the costs of mass production of sensor networks integrating COTS components.

BONAS intends also to investigate and prepare the potential future deployment of key sensors aboard a flying platform with a view towards increasing the BONAS network detection capabilities.

The wireless sensor network will feature a variety of sensing devices (in-situ and remote), that will jointly provide broad chemical spread and low false alarm rates through an expert system management of the data collected. In particular, BONAS will develop: Lidar/Dial system; QEPAS sensor; SERS sensor; an Immunosensor.

BONAS includes a multidisciplinary team of leading European research groups (ENEA, QUB, CSEM, ONE, UCBL, UNIL, KCL) together with industrial organizations (CREO, LDI, SAB, TEK, EADS) and end-users (NBI) with previous experience and activity in the field of specific local and remote sensors development and with experience on Security projects. The consortium represents the complete supply chain of the proposed product, which sets good perspectives for exploitation and commercialization of the generated innovations.

The consortium will be supported by an already established Advisory Board formed by experts from the main European and Israeli police corps.

Main technological and scientific outcomes

The scientific and technical objectives of BONAS project are:

- Lidar/Dial apparatus
- QPAS apparatus
- SERS minispectrometer
- Electrochemical sensor
- Vapour and particle Sampler

Products/Operational Prototypes validated by End-users

Two demo are foreseen next

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**ENEA - Agenzia Nazionale per le Nuove Tecnologie, l'Energia e lo Sviluppo Economico Sostenibile**	**ENEA**	Italy
2	Consorzio CREO - Centro Ricerche Elettro Ottiche	CREO	Italy
3	SERSTECH AB	SAB	Sweden
4	TEKEVER - TECNOLOGIAS DE INFORMACAO, S.A	TEK	Portugal
5	Laser Diagnostic Instruments AS	LDI	Estonia
6	CSEM – Centre Suisse d'Electronique et de Microtechnique SA – Recherche et Developpement	CSEM	Switzerland
7	EADS DEUTSCHLAND GMBH	EADS	Germany
8	Université Claude Bernard Lyon 1	UCBL	France
9	Office National d' Études Nationale et de Recherches Aérospatiales	ONE	France
10	University of Lausanne	UNIL	Switzerland
11	National Bureau of Investigation	NBI	Finland
12	King's College London	KCL	UK
13	Commissariat à l' énergie atomique et aux énergies alternatives	CEA	France
14	Queen's University Belfast	QUB	UK

CockpitCI / *Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures*

Info

Call:	FP7-SEC-2011.2.5-1 Cyber attacks against critical infrastructures – Capability Project
Total cost:	4,388,000 €
EU funding:	2,987,000 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,978,000 €
EU funding for Italy:	1,393,000 €
Website:	http://www.cockpitci.eu

Abstract

The protection of the national infrastructures is one of the main issues for national and international security. While FP7 MICIE project has proved that increasing cooperation among infrastructures increases their level of service and predictive capability, it is not enough to effectively counteract threats such as cyber attacks. Such attacks could be performed blocking communication from central SCADA to local equipments or inserting fake commands/measurements in the SCADA-field equipment communications (as happened with STUXNET worm). The paradox is that critical infrastructures massively rely on the newest interconnected (and vulnerable) ICT technologies, while the control equipment is typically old, legacy software/hardware. Such a combination of factors may lead to very dangerous situations, exposing systems to a wide variety of attacks. To overcome such threats, the CockpitCI project aims on one hand to continue the work done in MICIE by refining and updating the on-line Risk Predictor deployed in the SCADA centre, on the other hand to provide some kind of intelligence to field equipment, allowing them to perform local decisions in order to self-identify and self-react to abnormal situations induced by cyber attacks. It is mandatory to operate both at SCADA control centre and at field equipment because it is very dangerous to let field components operate autonomously. To address this issue an hybrid validation system will be implemented: at the Control Centre level an "Integrated On-line Risk Predictor" will provide the operator with qualitative/quantitative measurements of near future level of risk integrating data coming from the field, from other infrastructures, and from smart detection agents monitoring possible cyber attacks; at field level, the system is complemented with a smart software layer for field equipment and a detection system for the TLC network. The system will be validated on real equipment and scenarios provided by Israel Electric Corp.

Main technological and scientific outcomes

The main objectives of the project (the project is still running) are:

- To improve the resilience and dependability of Critical Infrastructures (CIs) through the automatic detection of cyber threats and the sharing of near real-time information about events, including cyber attacks, among CI owners, extending the capabilities developed in the previous MICIE project. Automatic detection of cyber threats will be based on classical techniques as well as innovative SCADA specific and machine learning devices and techniques;
- To identify, in near real time, the CI functionalities impacted by cyber-attacks and assess the degradation of CI delivered services. Novel modeling and simulation capabilities are under investigation to model an interdependent set of CI under cyber attacks and the influence on CI QoS.
- To translate awareness into risk, classify the associated risk level, broadcast alerts at different security levels and activate a strategy of containment of the possible consequences of cyber-attacks.

- To investigate and leverage the ability of field equipment to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety.

Products/Operational Prototypes validated by End-users

A demo is foreseen at the end of the project.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex ES**	**SELEX-ES**	Italy
2	Centre de Recherche Public Henri Tudor	CRP TUDOR	Luxembourg
3	Consorzio per la ricerca nell'automatica e nelle telecomunicazioni	CRAT	Italy
4	Università degli Studi Roma Tre	UNIROMA3	Italy
5	ENEA – Agenzia Nazionale per le nuove tecnologie, l'energia e lo sviluppo sostenibile	ENEA	Italy
6	The Israel Electric Corporation Limited	IEC	Israel
7	itrust consulting s. à r. l.	ITRUST	Luxembourg
8	Multitel asbl	MULTITEL	Belgium
9	Universidade de Coimbra	UC	Portugal
10	University of Surrey	SURREY	UK
11	Compania Nationala De Transport al energiei Electrice Transelectrica SA	TEL	Romania
12	Lyse Energi AS	LYSE	Norway

CoMiFin / *Communication Middleware for Monitoring Financial Critical Infrastructure*

Info

Call:	FP7-ICT-SEC-2007-1
Total cost:	3,571,385 €
EU funding:	2,350,000 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,645,852 €
EU funding for Italy:	1,098,725 €
Website:	http://www.comifin.eu

Abstract

As remarked in recent studies of the US Federal Reserve, a financial infrastructure is an unmanaged large scale networked system of interconnected financial markets and banking systems by which domestic and international financial institutions allocate capital and manage their risk exposures. This infrastructure is also characterized by rapid growth given the continually enhanced telco-based e-services offered by the financial institutions as well as the diversity of communication/financial networks and user level devices that interface with this infrastructure. Needless to add, the basis of the economic viability of modern society, the dependency of both the traditional and growing e-commerce economy implies the financial infrastructure's socio-economic role as a critical infrastructure.

The main purpose of the CoMiFin is strategically targeting the EU technological and institutional lag in financial infrastructure protection (FIP). Specifically, CoMIFin aims to provide "an infrastructure level monitoring, notification and mitigation" middleware as an essential element of FIP. CoMiFin aims at supporting business continuity of a financial actor on top of an unmanaged network of managed financial infrastructures under all foreseeable failure scenarios including the operational failures and deliberate breaches. This is a nontrivial task requiring a holistic and cooperative approach across multiple elements of a financial infrastructure, such as disparate financial and telco networks, various middleware platforms, and other interconnecting components.

Main technological and scientific outcomes

The primary outcome of the CoMiFin project is a novel middleware architecture that facilitates information sharing and processing among participating principals (e.g., financial institutions, utility providers, cloud providers, etc) for the sake of identifying threats (e.g., IT cyber attacks, money laundering, frauds) targeting their IT infrastructures and business. The information sharing and analysis is accomplished through the new Semantic Room (SR) abstraction allowing interested parties to be grouped into trusted and secure collaborative environments. The input data can be real time security events, historical attack data, logs, etc. Data can be generated by local monitoring subsystems (such as system management products, IDS, firewalls, etc.) installed within the IT of the participating principals as well as by external sources (e.g., CERTs).

Major project results include:

- Creation of a community of interest (including FAB members) that has cooperated in a highly positive way to exchange information and ideas on financial CIP;
- Creation of a common dictionary between financial experts and research people, in such a way they can understand each other and they can jointly address financial requirements to figure out the suitable models to be applied and to identify new models;
- Definition of Semantic Room model for controlled information exchange;
- Development of a working prototype of the CoMiFin middleware architecture that includes all the major technical features required for a commercial product;
- Implementation of 5 different semantic rooms, each one implementing an algorithm and using a technology suitable for a specific threat. These semantic rooms can communicate with each other exchanging alerts and other information in order to enhance their respective detection mechanisms;
- Information exchange overseas with US research laboratory (NISAC/SANDIA) in order to disseminate CoMiFin model and to gain their knowledge on simulation of CI behavior over time.

Products/Operational Prototypes validated by End-users

- Meeting with Italian financial institutions, Italian Central Bank (BKI), IntesaSanPaoloBank, Swift (BISP), April 2009 (MEF)
- Meetings with Budapest Bank (part of GE Money), Groupama-Garancia Insurance, Hungarian Financial Supervisory Authority
- Ministry of Interior (Italian), Sept 2009
- Video demonstrator of the CoMiFin platform (http://www.CoMiFin.eu/images/dashboard-screencast.swf)

One of the most important assets of CoMiFin has been the Financial Advisory Board (FAB), composed by financial experts:

- UBS (Mr. Kohler, chairman);
- Bank of Italy (Mr. Pagani);
- SWIFT (Mr. Hansen, Mr. Newman);
- Groupama (Mr. Fazekas);
- Bank of Budapest (Mr. Alföldi);
- Banca IntesaSanPaolo (Mr. Ferrero, Mrs Briano);
- SIA-SSB (Mr. Galeazzi);
- ABI-Lab (Mr. Lucchetti).

The role of FAB has been of most importance for identifying the real business needs and constraints of financial stakeholders. The FAB has really steered the project in the direction of existing gaps between what financial actors need and the offering of IT market.

After the end of the project a prototype activity has been implemented in Ministry of Finance system with a demo over real financial data.

Follow-up

Adoption of CoMiFin model in other Critical Infrastructure Protection areas.

New technological, scientific or application perspective opened by the project

CoMiFin has proposed a new model by applying the cooperation model to financial world. The financial world has many specific requirements, mainly related to security and privacy of exchanged information

and a model where cooperation can be established among trusted partners only. Semantic Room approach introduced by CoMiFin let address those new needs and open new research areas in Critical Infrastructure Protection.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

Adoption of CoMiFin model in other Critical Infrastructure Protection areas.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex ES**	**SELEX ES**	Italy
2	Technical Universitat of Darmstadt	TUD	Germany
3	IBM	IBM	Israel
4	Waterford Institute of Technology/TSSG	WIT	Ireland
5	Ministry of Economics and Finance	MEF	Italy
6	OptXware	OPT	Hungary
7	KreditTilsynet	KRD	Norway
8	University of Modena	UoM	Italy
9	Consorzio Interuniversitario Nazionale per l'Informatica	CINI	Italy

CUSTOM / *Drugs and precursor sensing by complementing low cost multiple techniques*

Info

Call:	SEC-2009-1.3-02
Total cost:	5,295,523 €
EU funding:	3,486,406 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	2,537,734 €
EU funding for Italy:	1,664,029 €
Website:	http://www.custom-project.eu

Abstract

A large number of techniques for drug precursors chemical sensing has been developed in the latest decades. These techniques are able to screen and identify specific molecules even at very low concentration in lab environment, nevertheless the objective to build up a system which proves to be easy to use, compact, able to provide screening over a large number of compounds and discriminate them with low false alarm rate (FA) and high probability of detection (POD) is still an open issue. The project CUSTOM, funded by the European Commission within the FP7, deals with stand alone portable sensing apparatus based on multiple techniques, integrated in a complex system with a complimentary approach. The objective of the project is to achieve an optimum trade-off between opposite requirements: compactness, simplicity, low cost, sensitivity, low false alarm rate and selectivity. The final goal is the realization of an optical sensing platform able to detect traces of drug precursors compounds, such as ephedrine, safrole, acetic anhydride and the Benzyl Methyl Ketone (BMK). This is reached by implementing two main sensing techniques: the fluorescence enhanced by the use of specially developed Organic macro-molecules, and a spectroscopic technique in Mid-IR optical range.

The fluorescence is highly selective with respect to the target compounds, because it is based on properly engineered fluorescent proteins which are able to bind the target analytes, as it happens in an 'immune-type' reaction. The spectroscopic technique is based on the Photo-Acoustic effect, enhanced by the use of a widely Tunable Quantum Cascade Laser.

Finally, the sensing platform is equipped with an air sampling system including a pre-concentrator module based on a sorption desorption cycles of a syndiotactic polystyrene polymer

Main technological and scientific outcomes

The main outcomes of the CUSTOM project are:

- The development and the assessment of two different a sensing techniques. The first is based on biochemical fluorescent proteins, the second relies on a LASER photoacoustic principle and a spectra pattern recognition algorithm;

- The realization of a stand alone portable technological demonstrator able to able to screen and identify specific molecules at low concentration over a large number of compounds and discriminate them with low false alarm rate (FA) and high probability of detection (POD);
- The development and the realization of a chemical preconcentrator based on syndiotactic Polystyrene;
- The set up of a focused community consisting on several industrial, academic and end user partners focusing on sensing applications for security.

Products/Operational Prototypes validated by End-users

- ✓ Protocol for biochemical Synthesis of the reagents for fluorescent sensing. The reagents are used in a competitive assay technique to detect two different drug precursors (ephedrine and BMK);
- ✓ Tunable Quantum cascade LASER operating in the 1100cm-1 with 80cm-1 of wavelength range;
- ✓ Algorithm for spectra pattern recognition used in the LPAS;
- ✓ Chemical preconcentrator used to feed the sensor;
- ✓ Complementary sensing operating mode based on High Probability of Detection and Low False Alarm Rate;
- ✓ Organization of conferences about specific thematic of interest and inviting key speakers to provide value information and keep up the attention of attendees.

The end users involved in CUSTOM are european law enforcement agencies related in the fight against *Illicit Traffic of Narcotic Drugs and Psychotropic Substances.*

Apart from the Direction Nationale du Renseignement et des Enquêtes Douanières - DNRED, which is a beneficiary of the project and has the task to carry out investigations on smuggling and customs fraud for the French custom, the following organizations take part to the advisory board of CUSTOM as end user:

- CARABINIERI RIS di ROMA (ITALY)
- Facoltà di medicina legale, SAPIENZA Universita' di Roma (ITALY)
- Spanish Police (SPAIN)
- The Narcotraffic department of the Basque Police (SPAIN)
- Agenzia delle Dogane Italiane (ITALY)
- Polizia Scientifica di Napoli (ITALY)
- Ministero dell'Interno Italiano (ITALY)

Other stakeholders relevant to the project's goals are part of a network community of Large Organizations, Research Centers/Universities, Public authorities and Clusters/Associations, such as dog handheld Police team, Intelligence Forces, civil protection, private companies etc. involved in the **Security Market chain.**

The demo of CUSTOM prototype took place in the SELEX-ES labs in Rome, in May 21th 2013. During the demo was present the end-user DNRED.

The end-user has shown interest in the demonstrator and has planned more demonstrations in difficult working: inside containers, trucks and cars.

Follow-up

New technological, scientific or application perspective opened by the project

From the scientific point of view the prospects are to extend the family of the analytes detected by the sensor (in the design phase were provided only precursors of drugs). The extension of the detection technique to substances such as compounds for chemical warfare agents and toxic industrial odors, allows the use of sensor CUSTOM even in military applications, for environmental monitoring and for control of the borders. From the technological point of view the perspective is that of increasing the demonstrator's TRL 5/6 to 6/7.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex-ES**	**SELEX-ES**	Italy
2	GASERA Ltd	GASERA	Finland
3	University of Turku	UTU	Finland
4	Alcatel-Thales III-V LAB	III-V LAB	France
5	CNR – Istituto di Biochimica delle Proteine	IBP-CNR	Italy
6	ENEA	ENEA	Italy
7	Consorzio Interuniversitario Nazionale per la Scienza e Tecnologia dei Materiali	INSTM	Italy
8	University of Aalto	AALTO	Finland
9	INAS – Tecnalia	INAS	Spain
10	Direction Nationale du Renseignement et des Enquêtes Douanières	DNRED	France

DIRAC / *Rapid screening and identification of illegal drugs by IR absorption spectroscopy and gas chromatography*

Info

Call:	SEC-2009-1.3-02
Total cost:	4,300,000 €
EU funding:	3,000,000 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	2,000,000 €
EU funding for Italy:	1,400,000 €
Website:	http://www.fp7-dirac.eu

Abstract

Detection of Amphetamine Type Stimulants (ATS), precursors, and derivatives, remains an open challenge if we move out of forensic labs, and consider field-sensors for daily use against the production, trafficking, and street distribution of illicit drugs. Although Gas Chromatography and InfaRed Absortpion Spectroscopy (GC-IRAS) together represent the most powerful tool for the identification of Amphetamines and the classification of designer drugs, GC-IRAS is currently available only as bench top instrumentation for bulk analysis. In DIRAC, an advanced GC-IRAS sensor of ATS is developed, that combines silicon micro-machined GC components and a hollow-fiber-based IRAS cell, to demonstrate hand-portability –for field operation–, together with trace sensitivity and fast response. Furthermore, the sensor integrates advanced solutions for sample separation and treatment, that allow to analyse substances in different physical state and with different chemical characteristics, as traces and as bulk.

Main technological and scientific outcomes

The DIRAC sensor is available and running. Integration of the sensor in its final demo case (hand-luggage) will be completed by the end of the year. The sensor essentially consists of :

- A sampling unit, with autonomous capacity to detect amphetamines at an early warning stage;
- An identification unit consisting of a vapour pre-concentration device, a GC separation module, an IRAS module, a Surface Ionization (SI) detector, and an Expert System that analyzes elution times, IR spectra, and SI signals, to identify targets, or (if direct matching fails) to establish similarities with classes of target compounds.

The sensor is capable to analyze a wide range of substances in different form and physical state:

- Precursors have been analyzed both as vapours pre-concentrated from the open air or from the head-space of a vessel, and as solid particles collected in a thermal desorber;
- ATS and ATS salts have been analyzed as solid particles collected in a thermal desorber.

The sensor has demonstrated nanogram sensitivity, fast response (from 10 s to 2-3 min depending on substance and sensing scheme), and effective rejection of interferents.

Products/Operational Prototypes validated by End-users

Validation of the prototype (ongoing) is undertaken by members of the DIRAC Consortium and by an external group of users:

Member of the Consortium:

- The National Institute of Criminalistics and Criminology (NICC), based in Brussels
- The Finnish National Bureau of Investigation (NBI), based in Vantaa
- The Dep. of Forensic Sciences of the University of Lausanne

External Group of Experts:

- Belgian Customs
- Swiss Customs
- Belgian Police
- German Police

A small demo is now planned for the first quarter of 2014. Location and demo plan currently under discussion. The demo will be most probably be arranged at one of the Belgian airports or harbours, in cooperation with the Belgian Customs.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Consorzio CREO - Centro Ricerche Elettro Ottiche**	**CREO**	Italy
2	CNR – Istituto per la Microelettronica e Microsistemi	CNR-IMM	Italy
3	Selex-ES	SELEX-ES	Italy
4	Consorzio Interuniversitario Nazionale per la Scienza e Tecnologia dei Materiali	INSTM	Italy
5	Fraunhofer IPM	IPM	Germany
6	EADS	EADS	Germany
7	University of Lausanne	UNIL	Switzerland
8	University of Galati	UGAL	Romania
9	Nationaal Instituut voor Criminalistiek en Criminologie	NICC	Belgium
10	National Bureau of Investigation	NBI	Finland

INSPIRE / *Increasing Security and Protection through Infrastructure Resilience*

Info

Call:	Joint Call ICT-SEC-2007.1.7: Critical Infrastructure Protection
Total cost:	3,697,402 €
EU funding:	2,400,000 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,491,200 €
EU funding for Italy:	946,200 €
Website:	http://www.inspire-inco.eu

Abstract

The main objective of the INSPIRE project was to enhance the European potential in the field of security by assuring the protection of Critical Infrastructures (CIs) through the identification of their vulnerabilities and the development of innovative techniques for securing networked process control systems.

To increase the resilience of such systems INSPIRE developed traffic engineering algorithms, self-reconfigurable architectures and diagnosis and recovery techniques.

The core idea of the INSPIRE project was to protect Critical Infrastructures by appropriately configuring, managing, and securing the communication network interconnecting the Supervisory Control And Data Acquisition (SCADA) systems that are used to monitor and control CIs.

Main technological and scientific outcomes

The main outcomes of the INSPIRE project can be summarized as follows:

- Security assessment of SCADA systems and creation of a database containing information about vulnerabilities affecting such systems;
- Design and development of traffic engineering techniques to increase resilience of the SCADA communication network;
- Development of detection and diagnosis techniques to protect SCADA systems against cyber-attacks;
- Development of remediation techniques to mitigate the effects of attacks/faults in SCADA systems.

Products/Operational Prototypes validated by End-users

At the moment there isn't made any demo.

Follow-up

As an ancillary project of INSPIRE, an international cooperation initiative had been established between INSPIRE and the US project GridStat, led by Washington State University. The goal of this cooperation action, named INSPIRE-INCO, was to promote exchange of experience and research results between the two ongoing projects in the field of power grid security and resilience. The INSPIRE research topics had been further investigated and validated in the framework of INSPIRE-INCO through the participation and the involvement of the INSPIRE-INCO researchers in the working groups of NASPI (North American SynchroPhasor Initiative).

A security assessment of power grid monitoring systems had been performed and the INSPIRE security framework had been adapted to the specific security issues concerning power grids thanks to the availability of real data provided by the GridStat researchers.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Consorzio Interuniversitario Nazionale per l'Informatica**	**CINI**	Italy
2	Selex ES	SELEX ES	Italy
3	KITE Solutions	KITE	Italy
4	Technische Universität Darmstadt	TUD	Germany
5	ITTI SP. Z.O.O.	ITTI	Poland
6	Thales Communications France S. A.	TCF	France
7	S21sec Information Security Labs S.L.	S21SEC	Spain
8	Centre for European Security Strategies	CESS	Germany

ISTIMES / *Integrated System for Transport Infrastructures surveillance and Monitoring by Electromagnetic Sensing*

Info

Call:	Joint Call FP7-ICT-SEC-2007-1
Total cost:	4,368,000 €
EU funding:	3,133,460 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	2,340,388 €
EU funding for Italy:	1,599,752 €
Website:	http://www.istimes.eu

Abstract

ISTIMES project has designed, assessed and promoted an ICT-based system, exploiting distributed and local sensors coupled with space observations for non-destructive electromagnetic monitoring of critical transport infrastructures. The integration of electromagnetic sensing technologies with new ICT systems enables remotely controlled monitoring and surveillance and real time data imaging of the infrastructures. The monitoring system allow get information about the state of the infrastructure detecting both slow and fast degradation (including ageing effects) and coupling current monitoring and quick damage assessment. The ICT architecture, which is fully federate and scalable, allows at adding new sensors or new measuring sites, to modify the monitoring strategy depending on the events and to provide alert to the stakeholders when anomalies occur. Protocols have been defined so that in situ techniques enter into the observational chain starting from the cheapest ones, depending on the status of the infrastructure. This approach allows support stakeholders both in defining ordinary/extraordinary maintenance strategies and in managing emergencies and disasters.

Main technological and scientific outcomes

The main outcomes of the ISTIMES project can be summarized as follows:

- Design, implementation and validation of a system able to couple long term monitoring and quick damage assessment for the critical transportation infrastructures. The integration of ICT system architecture with a large arena of electromagnetic non-invasive sensing techniques makes the system readily suitable for other kind of infrastructures;
- Design and implementation of a ICT system architecture for the control and data acquisition of a network (as well as network of networks) of heterogeneous sensors via WEB. The ICT system architecture is able to provide information via WEB to the stakeholders;
- Set-up and in laboratory assessment of several prototypes of instrumentations for non-invasive sensing and transition of sensing instrumentations from the laboratory conditions to on-field deployment;
- Development of data fusion/integration strategies for a synergic use of the different sensors;

- Demonstration of the effectiveness of the system via experiments both in controlled conditions, (but in real scale), and in really challenging test beds (directly on field).

Products/Operational Prototypes validated by End-users

The ISTIMES system has been validated at three challenging test beds as Sihlhochstrasse bridge in Zurich, Varco Izzo railway tunnels and Musmeci bridge in Potenza city area. The demonstration activities have shown the effectiveness of ISTIMES approach in operational conditions, also on the basis of the positive feedback of the owners/managers of the infrastructures.

Several demos have been performed during the project. They regarded the monitoring/diagnostics of: two motorway bridges, respectively in Zurich and Potenza; a railway tunnel affected by a landslide in an area close to Potenza city.

The end-users directly involved in the project and demo activities were: Federal Road Office of Switzerland; Municipality of Potenza; Dipartimento di Protezione Civile, IFSTTAR.

Italian Civil Protection and IFFSTAR (that is an intermediate user) are partners of the project, so that they participated to all the activities of the project, from strategies definition to validation and dissemination.

The success of the demonstration activities has stimulated the interest from end-users outside of the Consortium, which have requested specific monitoring services(in particular ESITF for dams monitoring and Provincia of Potenza for road system monitoring).

The applicative success of the project is testified by the fact that end-users outside of the ISTIMES Consortium have requested specific monitoring services as:

- Provincia di Potenza for the monitoring of the overall road network (2500 km long);
- Ente per lo Sviluppo dell'Irrigazione e la Trasformazione Fondiaria in Puglia, Basilicata, Irpinia" (ESITF), which has requested a monitoring service for the the Monte Cotugno dam on Sinni River, i.e., the largest European rock-filled one and 1.8 Km long.

Follow-up

The future developments aim both at further developing of ISTIMES and at deploying the ISTIMES system in operational conditions and developing user friendly outputs, which can improve the acceptance of this ISTIMES concept by the end-users. Therefore, the main actions are focussed on

- The improvement of the system both improving the use of space data for the large scale awareness and positioning tools;
- A better interfacing of non-invasive electromagnetic technologies with civil engineering sensing technologies and modelling in order to get information about the vulnerability of the infrastructure;
- The translation of the technological indicators provided by the system in user friendly information for the stakeholders;
- The design and implementation of observation/sensing measurements protocols accounting for the specificity of the monitored infrastructure and the economic viability;
- The embedding of the system in a more general frame of the crisis management, thanks to the integration of ISTIMES ICT architecture with interoperable Spatial Data Infrastructures, so to activate information exchange with mobile devices and web (citizens as sensors, social network,…);
-

The set-up of the novel concept of the embedded security, where the sensors are explicitly considered as one of the key elements in the design of an infrastructure.

New technological, scientific or application perspective opened by the project

The main scientific technological challenges can be listed as:

- The set-up of advanced data processing for the different sensors in order to obtain more accurate and easily interpretable information;
- The set-up of data integration approaches for a synergic use of the different sensors;
- The development of a new concept where both the results of the measurement/ monitoring chain and the structural (civil engineering) models of the infrastructures are used in a "positive feedback loop" mode. This means that the monitoring results are used to refine the structural models, which after are able to better drive the measurement chain;
- The coupling of current monitoring with quick damage assessment in order to exploit the impact on security of the development and integration of sensing techniques, which are also required for the current management;
- The sharing of costs.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

The thematic could be the design, implementation and validation of an integrated approach, where the wide area surveillance (by means of satellite and airborne platforms) is complemented by the ground based techniques for a detailed inspection/diagnostics of the single structures and with the involvement and the enhancement of the role of citizens.

Moreover it should be necessary to integrate electromagnetic sensing techniques with other sensing ones as these typically used in the framework of Civil Engineering and with structural modelling in order to be able to give a quantitative (and not only qualitative) information about the vulnerability status of the infrastructure.

More generally it is necessary that European Commission gives more attention to cross-cutting issues (e.g. resilience and crisis management are strongly linked), and to cost sharing, promoting a view in which security issues are currently part of the ordinary life of infrastructure

This approach is of interest not only for the critical infrastructures but more in general for the environment, territory, urban settlements, cultural heritage. This kind of thematic is very suitable for the development of Precommercial Public procurements, where the social needs are translated in scientific/ technological challenges.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Consorzio Tecnologie per le Osservazioni della Terra ed i Rischi Naturali**	**TERN**	Italy
2	Telespazio	TPZ	Italy
3	Dipartimento di Protezione Civile	DPC	Italy
4	Eidgenoessische Materialpruefungs- und Forschungsanstalt	EMPA	Switzerland
5	Institut Français des Sciences et Technologies des Transports, de l'Amenagement et des Reseaux	IFSTTAR	France
6	Lund University	ULUND	Sweden
7	Tel Aviv University	TEL AVIV	Israel
8	Territorial Data Elaboration SRL	TDE	Romania
9	Norsk Elektro Optikk	NEO	Norway

MICIE / *Tool for systeMIc risk analysis and secure mediation of data exchanged across linked CI information infrastructurEs.*

Info

Call:	ICT-SEC-2007.1.7
Total cost:	3,496,456 €
EU funding:	2,448,164 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,772,498 €
EU funding for Italy:	1,340,723 €
Website:	http://www.micie.eu

Abstract

The MICIE project, implemented a so-called "MICIE alerting system" that identifies, in real time, the level of possible threats induced on a given CI by "undesired" events happened in such CI and/or other interdependent CIs. In particular, whenever such events occur, the MICIE alerting system supports the CI operators providing them with a real time risk level (e.g. expressed in a chromatic scale such as white, green, yellow, orange, red).

The alarm conditions are evaluated by means of an on-line prediction tool making use of properly designed abstract CI models powered with aggregated metadata describing the CI status.

Main technological and scientific outcomes

The main outcomes of the MICIE project can be summarized as follows:

- Understanding and managing the interactions and complexity of interdependent critical infrastructures;
- Provide automatic mechanisms for automatic risk detection;
- Prevent against cascading effects;
- Provide recovery and continuity in critical scenarios.

Products/Operational Prototypes validated by End-users

The **Energy Sector Industry** might be considered a potential beneficiary for the infrastructural threats or SCADA systems. More generally all the Operator managing Critical Services and Infrastructures (e.g. Electrical, Water, Telecoms, and Gas providers).

MICIE tested some results at the Israel Electric Corporation (IEC) facilities, simulating a real piece of an Electrical grids.

The MICIE project has developed a tool that helps to increases the QoS in the supply of energy between the energy producers and customers. The validation activities of the project has demonstrated a considerable reduction in the time of unsupplied power when the MICIE tool is used, thus allowing to improve QoS to end customers. This is also made possible by the overall approach that allows to better predict events and consequences of cascade failures on the system state.

An independent study *(The Innovation Potential f FP7 Security and Trust Projects)* granted by the European Commission has ranked MICIE in 3^ position in a Top-Down Classification for the contribution to the Digital Agenda.

Follow-up

Follow-up and further developments are in progress with the EC-FP7 funded project *CockpitCI.*

New technological, scientific or application perspective opened by the project

The **modelling methodology** proposed in MICIE project, based on the integration of heterogeneous modelling techniques, oriented to the identification of the most suitable level of abstraction adopted to represent the inner architecture of the considered infrastructures.

The **MICIE on-line prediction tool** provides the CI operators with a real-time risk level indicating the probability that, in the near future, they will no more being able to provide the CI services with the desired QoS in consequence of certain undesired events happened in the reference CI and/or in other interdependent CIs.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

Policies and models related to the information exchanged by different CI. The CI Operators define policies using a policy specification language and/or using a graphical user interface (GUI). The policies are represented in a formal way using a policy standard-like specification language.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex ES**	**SELEX ES**	Italy
2	Israel Electric Corporation	IEC	Israel
3	Enea	ENEA	Italy
4	Centre de Recherché Public Henri Tudor	CRP TUDOR	Luxembourg
5	Consortium for the Research in Automation and Telecommunication University of Rome - “La Sapienza”	CRAT	Italy
6	University of Bradford	BRAD	UK
7	Dipartimento Informatica e Automazione –Università di Roma Tre	DIA-UNIRO-MA3	Italy
8	Universidade De Coimbra	FCTUC	Portugal
9	Przemyslowy Instytut Automatyki I Pomiarow	PIAP	Polska
10	Itrust Consulting SARL	ITRUST	Luxembourg
11	MULTITEL ASBL	MULT	Belgium

MODES_SNM / *Modular Detection System for Special Nuclear Material*

modes SNM

Info

Call:	FP7-SEC-2011.1.5-1
Total cost:	3,213,051.20 €
EU funding:	2,411,633.00 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,299,300.00 €
EU funding for Italy:	1,000,760.00 €
Website:	http://www.modes-snm.eu

Abstract

The MODES_SNM project aims to carry out technical research in order to develop a prototype for a mobile, modular detection system for radioactive and Special Nuclear Materials (SNM). To maximize the detection capability for SNM the project will develop new detectors for fast and thermal neutrons, as well as gamma-rays, based on the technology of high pressure scintillation cells using noble gases (as 4-He and Xe) recently developed by ARKTIS. The proof-of-principle of the new detectors has already been recently demonstrated. The project's goal is to deliver a tested prototype of a modular mobile system capable of passively detecting weak or shielded radioactive sources with accuracy higher than that of currently available systems. The identification of

the gamma-ray emitter is also possible by using the spectroscopic analysis performed by high pressure Xe cells whereas the ratio between fast and thermal neutrons will bring information about the eventual shielding around the source. The R&D aims at improve the current detectors (i.e. at designing, constructing and testing robust, safe, and lightweight high pressure cells with an advanced read-out system) so that they can be used as basic components of the modular mobile system. A suitable Information System will be also developed to manage the detectors, integrate and analyze the data, and provide to the user simple information derived by a decision tree utilizing the data from the three types of detectors. The prototype detection system is the major deliverable of the project. The project also includes the qualification of this detection system in laboratory condition to quantify its detection performance and ultimate limits, as well as a demonstration phase in which the detection system will be field-tested by the end-user group established within the project.

Main technological and scientific outcomes

The main outcomes of the ISTIMES project can be summarized as follows:

- Development of new detectors for thermal neutrons and gamma ray using high pressure noble gas ARKTIS;
- Development of new HV desktop system from CAEN SpA;
- Development of an optimized desktop digitizer for neutron/gamma discrimination CAEN SpA;

- Development of a new read-out system for scintillators based on Silicon Photomultipliers;
- Development of an Information system for automated search and identification of radioactive sources and special nuclear material;
- Van mounted demonstrator to be used essentially by Custom Agencies.

Products/Operational Prototypes validated by End-users

The MODES_SNM project started on January 2012 and will end on June 2014. A demonstration campaign is planned for March-May 2014. During the demonstration the MODES_SNM van-mounted prototype will be operated directly by end-users.

At this time the End-User that already agreed in the demonstration campaign are the Custom Agencies of UK, Ireland and Nederland. We are still waiting on the Italian Custom Agency. The demonstration will consist basically in two type of operations:

a) Search for radioactive/ nuclear materials in seaport patrolling the container places;

b) Search for radioactive/nuclear material by monitoring car/truck queues during the embarkation operation of ferries;

c) Monitoring passengers queue in seaport terminals.

All end-user will spend 1 week at the Padova University for training. After this, the MODES_SNM prototype will be transferred to Liverpool, Dublin and Rotterdam to be operated directly by end-users.

At this time certainly new detectors from ARKTIS and new front-end electronics from CAEN will represent new products for the market. The development of high pressure Xe detector for gamma ray is receiving a large interest.

Follow-up

We are looking to new projects in the Work-plan of HORIZON2020 in which the MODES_SNM experience and the developed hardware and software tools can be further developed or integrated with other sensors in view of a complete RNBC defense system.

New technological, scientific or application perspective opened by the project

The combined use of high sensitivity neutron (fast and thermal) and gamma-ray detector to identify the presence of radioactive/nuclear material and provide the identification of the suspect item. Such system can be useful in several applications in Civil Security as well as in environmental monitoring and in the decommissioning of military installations as well as power plans.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

The RNCB aspects are already in the security work-plan of HORIZON2020.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Università degli Studi di Padova**	**UNIPD**	Italy
2	C.A.E.N. Spa	CAEN	Italy
3	Università degli studi dell'Insubria	UNINSUBRIA	Italy
4	Arktis Radiation Detectors Ltd	ARD	Switzerland
5	ETH Zurich	ETH	Switzerland
6	National Centre for Nuclear Research	NCBJ	Poland
7	University of Liverpool	LIV	UK
8	The Revenue Commissioners	RC	Ireland

NI2S3 / *Net-centric Information & Integration Services for Security Systems*

Info

Call:	FP7-ICT-SEC-2007-1 Joint Call ICT & Security 1
Total cost:	4,325,728 €
EU funding:	2,711,640 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	2,297,250 €
EU funding for Italy:	1,394,370 €
Website:	

Abstract

Complex interactions between the elements of a critical infrastructure indicate, that there is a need to deploy a corresponding infrastructure protection system, which is capable to of extending security control to all elements of the protected system, and, at the same time, of maintaining a global view of the infrastructure.

The key objective of the NI2S3 project is to research and implement a reference methodology for developing security systems based on NEC Information and Integration Services (I2S) for Critical Infrastructures. The security systems must be capable to collect and process information from many heterogeneous sources in order to build up or improve the situation awareness of critical infrastructures and to enable the decision making.

More specifically, the NI2S3 Project aims:

- to provide a definition and a design of an NI2S3 critical infrastructure protection system regarding the security, resiliency and availability of the subject infrastructure,
- to define performance indicators and tools for system validation,
- to develop a technology for the evaluation of the performance, robustness and reliability of such protection system,
- to develop a NI2S3 application demo as a proof of concept.

The NI2S3 project is focused on the research and development of a reference methodology to guide the design and the implementation of security systems for critical infrastructure protection, basing on the philosophy and the concepts of the NEC-based systems approached with SOA techniques.

The refining and validation of this methodology is performed by an application demonstrator, realized in accordance with NEC and SOA concepts.

Therefore, the practical implementation and commercialization of a real NI2S3 will require a “step ahead” in this direction, not addressed by the project itself.

Main technological and scientific outcomes

Ni2S3 project, completed by 2011, September 30rd, achieved the following main results:

- Proposal of a reference architecture for CII (Critical Information Infrastructure). A new comprehensive architectural framework named CrAF (Critical Architecture Framework) was proposed starting from a base reference (TOGAF ADM specialized for CII) and extending it with contribution of other selected architecture frameworks (DoDAF, COBIT, SABSA);
- Improved techniques for situational awareness.in CII. Correlation of sensible events and infrastructure data and events were investigated and implemented in the demonstrator using temporal and logical correlation templates to enhance a proactive security mechanism mainly in distributed systems sensible to cyber attacks;
- Vulnerability Assessment methodology and tools. A demonstration tool for general application of stress and validation tests was also implemented to address a measurement of the robustness and reliability of a designed infrastructure;
- A demonstrator was developed with the objective to monitor and control an Highway analysing and protecting the information infrastructure which is underpinning such application environment.

All the outcomes of the research phase and methodology construction were put in actual implementation focusing on the relationship with SCADA systems which due to the evolution of the embedded systems and the ability to integrate and interconnect low level controlling systems in distributed architectures will reserve a special care on protection of the infrastructures which should enable this type of scenarios.

The project, both through demonstrator and in the research analysis exploited SOA as a way of communication and integration adopting OASIS Standards. In particular a gateway from SCADA Systems and a standard ESB was developed demonstrating the suitable adaptation of SOA architecture to distributed data acquisition and control environments.

NI2S3 confimed to be a cross-border project, which will give the chance of develop technology and reference methodology for developing Critical Infrastructures security systems that can be better accepted by the potential stakeholders, being them designed under the guidelines of each of the participant's country needs.

NI2S3 outcomes address scenarios which are emerging in all the distributed systems architecture able to collect data from remote sites, collect them to analyse the resulting information and (this is the new and important stage in the next future) to correlate in temporal and spatial. These systems are typically Net Centric and are becoming a significant part of the services delivery so becoming more and more critical just in the sense this project intends to address the proposed solutions.

Products/Operational Prototypes validated by End-users

The project is not applicable.

Follow-up

New technological, scientific or application perspective opened by the project

NI2S3 introduces the concept to face security issues of the Critical Infrastructure joining the analysis of the physical behaviour and the communication protocol inspection in deep. This approach improves the Cyber Situational Awareness increasing the chance to detect Zero day attacks. The first results achieved during NI2S3, are the starting point of the EC FP7 PREEMPTIVE Project (FP7-SEC-2013-1). PREEMPTIVE (PREVENTIVE METHODOLOGY AND TOOLS TO PROTECT UTILITIES) extends that concept and aims to develop a tools to face zero day cyber-attacks against the utility networks.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Vitrociset Spa**	**VITROCI-SET**	Italy
2	Università degli Studi di Firenze	UNIFI	Italy
3	HW Communications	HWCOMMS	UK
4	Center for TeleInFrastruktur	CTIF	Denmark
5	AGH University of Science and Technology	AGH	Poland
6	Comarch	CMR	Poland

OSMOSIS / *Overcoming security market obstacles for SMEs' involvement in the technological supply chain*

Info

Call:	FP7-SEC-2009-1
Total cost:	580,888 €
EU funding:	580,888 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	315,468 €
EU funding for Italy:	315,468 €
Website:	http://www.osmosisecurity.eu

Abstract

The focus of the OSMOSIS project is to provide a framework to support European organizations in being involved in the security market, by increasing their capabilities to understand the security market trends and untapped market potentials, and facilitate their involvement in the technological supply chain.

To achieve those objectives, the following activities/services have been realised:

- Identification of market opportunities in the Security technology supply chain, through the involvement of key stakeholders such as Large Organizations and RTD performers;
- The creation of a taxonomy for the Security Technological market, which started from the taxonomy created in the STACCATO project and provided a new taxonomy able to facilitate the search and retrieve of information related to the Security Technology market supply chain;
- Setting up of meta-clusters of organizations around the defined taxonomy (specific interest of categories of stakeholders in the security domain) to facilitate technology transfer and collaboration;
- Realisation of networking actions (workshops, webinars) that favor the entrance of organizations (mainly SMEs) in the security technological supply chain;
- Intermediate for the setting up of RTD and Take Up action in the security sector where SMEs and other identified organizations could join stakeholders and integrators of security supply chain.

Main technological and scientific outcomes

The main outcomes of the OSMOSIS project have been:

- A report with the identification of untapped market potentials in the technology security market supply chain;
- A taxonomy of the Security Technological market and related supply chain;
- The set up of a Information Technology platform which favour the match among organizations involved in the security supply chain, R&D projects, and financing opportunities for R&D projects. The platform makes use of the developed taxonomy to create clusters of organizations with similar interests, and provide open innovation features to allow organizations to search for competences and projects outside of their current internal knowledge and network;
- The support provided during the project allowed to establish several commercial agreements among organizations of the network, as well as more than 30 R&D projects.

Products/Operational Prototypes validated by End-users

- ✓ Taxonomy of security technology market supply chain;
- ✓ IT platform to access a database of hundreds of stakeholders, RTD project ideas, and a database of grants (European and national) favouring research and innovation in the security supply chain. The database are searchable through several parameters, and is continuously updated via XML from the database of CIAOTECH (www.innovationplace.eu);
- ✓ The platform includes interactive communication tools, as: participation in three specific Security Interest Group (SIG), creation and visualization of eBusiness Cards, possibility to create the own meta-cluster based on the developed taxonomy;
- ✓ Organisation of webinars about specific thematic of interest and inviting key speakers to provide value information and keep up the attention of attendees.

OSMOSIS has been able to become a centre of reference for more than 600 organisations involved in the **Security Market** chain.

In the OSMOSIS Database there is a total of 220 registered users: 143 are stakeholders, from which 108 SMEs, from different categories. With regard to the geographical distribution of the 108 registered SMEs, most of the companies in the OSMOSIS community come from Italy, Spain and France, due to the presence of partners' organizations in those countries with a balanced distribution among different Business Activities (R&D Services, Knowledge services, Products, Solutions). The most populated technology areas are the Electronics and the Engineering groups.

Other stakeholders relevant to the project's goals are Large Organizations, Research Centers/ Universities, Public authorities and Clusters/Associations, such as Police, Intelligence Forces, Airports, civil protection, private companies etc.

OSMOSIS organised two International workshop: one in Rome (Italy) the 15th June 2011, and one in Madrid (Spain) the 28th February 2012.

- 1st International workshop held in Rome (Italy): 46 attendees to the plenary session, about 10 project ideas shared in the round table, link to other interesting initiatives.
- 2nd International workshop held in Madrid (Spain), 101 attendees coming from organisations outside the consortium, 12 speakers held presentations in the event, 25 bilateral meetings were held: 11 between the REA project officer and organisations, and 14 between OSMOSIS partners and organisations, Link to other interesting initiatives: PESI (Spanish Technology Platform on Industry Safety) and the enterprise TECNALIA, expressed their interest to be linked to OSMOSIS activities.

OSMOSIS platform is still available and offers the following services:

- Access to a DB of organisations, classified following a specific taxonomy and including only relevant organizations operating in security related engineering and/or research activities;
- A list of security research opportunities that could be exploited by SMEs to collaborate with Large Organizations;
- Information on security-related grants ate European level, and at national level (six countries included: Italy, Germany, UK, France, Belgium, Netherlands);
- Interactive communication tools to allow the communication of the identified opportunities and the transfer of specific knowledge to SMEs of the different meta-clusters.

Follow-up

The project had a follow up, financed by the Region Lazio and is still on-going, planned to end in December 2013. The follow up is the PROGRESS-IT project, which aims to design, implement and validate an IT tool based on advanced information extraction and retrieval techniques, able to support end-users such as SMEs, Large Organisation, Research centers and Universities in identifying and filtering useful information related to the Security research and innovation Domain. PROGRESS IT makes use of the taxonomy developed in OSMOSIS to categorize and organise information retrieved. The final result will be a information retrieval and extraction tool able to find relevant information in the Security domain related to Papers, Patents, technical documentation and the Web in general. PROGRESS IT is realised by CIAOTECH and INNOVATION ENGINEERING (two SMEs of the Lazio Region), and the research centre SESM (part of Finmeccanica), is also involved as subcontractor to provide the Security Domain knowledge needed to develop the Information Retrieval and Extraction tool.

New technological, scientific or application perspective opened by the project

OSMOSIS was a support action, therefore no specific research was performer. Nevertheless, the taxonomy developed and the application of the Open Innovation principle in the developed IT platform, allowed to foresee new technological perspectives in the information retrieval and extraction techniques applied to the security sector.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**CIAOTECH Srl**	**CTECH**	Italy
2	SESM Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l.	SESM	Italy
3	GMVIS Skysoft, S.A.	GMVIS	Portugal
4	Consorzio Interuniversitario Nazionale per l'Informatica	CINI	Italy
5	Technische Universitaet Muenchen	TUM	Germany
6	INNOSTART Nemzeti Uzleti es Innovacios Kozpont Alapítvany	INNOSTART	Hungary
7	Honeywell, spol. s r.o.	HTS	Czech Republic
8	Instituto Nacional de Tecnica Aeroespacia	INTA	Spain
9	Fundación para el Conocimiento Madrimasd	FCM	Spain
10	Selex ES	SELEX ES	Italy
11	PNO Consultants S.A.S.	PNO	Spain

PLANTFOODSEC / *Plant and Food Biosecurity*

PLANT AND FOOD BIOSECURITY

Info

Call: 7TH Framework Programme, Theme: Security, Topic: SEC-2010.7.0-1 Networking of researchers for a high level multi-organisational and cross-border collaboration

Total cost: 5,609,529.69 €

EU funding: 4,624,499.00 €

Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:

Total cost for Italy: 1,235,024 €

EU funding for Italy: 1,116,424 €

Website: http://www.plantfoodsec.eu

Abstract

This project focuses on biological threats having the capacity to affect and damage agriculture, infect plants and ultimately affect the food and feed at any stage in the food supply chain. The European Network of Excellence PLANTFOODSEC aims to establish a virtual Centre of Competence in plant and food biosecurity to enhance preparedness and response capabilities to prevent, to respond and to recover from a biological incident or deliberate criminal activity threatening the European agrifood system.

Main technological and scientific outcomes

Halfway through the project implementation period, PLANTFOODSEC has:

- Identified regulatory threats;
- Prioritised target crops (including food, feed and timber crops);
- Prioritised target pathogens using a new tool for assessment based on risk scenarios;
- Characterised the early development of a plant disease epidemic;
- set up a tool for the prioritization of target human pathogens on plants (HPOP) and mycotoxins; and designed a virtual diagnostic network.

Main future expected outcomes:

- A decision-making tool for use by law enforcement officers to allow discrimination between deliberate and accidental outbreaks;
- Risk assessment tools for plant pathogens and HPOP.
- A database of EU and international expertise in relation to contingency plans, capabilities for tracking pathogen outbreaks, models of management systems for bioterrorism threats;
- Strategies in risk communication.

Products/Operational Prototypes validated by End-users

End users of this work are expected to be the national and European level authorities responsible for plant health and for security; For conventional plant health risks there are national regulatory authorities in each EU Member State, and there are higher level cooperative actions within EFSA, EPPO and the IPPC that parallel security issues covered in this project.

Current EU capabilities to detect and respond to agroterrorism or biocriminal acts are very modest and are divided among many organisations that lack coordination. Although they are normally handled by regional or national bodies, biosecurity risks transcend national and regional boundaries and must be monitored, assessed and managed in a coordinated way across the EU.

Coordination within the EU as well as among agencies is very much needed. The EU should coordinate activities aimed at preparing European agricultural systems at large to withstand a deliberate release of pathogens. In addition, such coordination would multiply the benefits to be derived from reinforcing existing links between various EC directorate generals, making it possible to adopt a multisectoral approach to the issue and to include biosecurity as a priority in future work programmes. Cooperation with relevant authorities and agencies will also be extremely important.

Follow-up

New technological, scientific or application perspective opened by the project

Forensics tools to be applied to discriminate between an accidental and an intentional outbreak threatening plant health and food biosecurity (mycotoxins, HPOP-human pathogens on plants like *E.coli*, *Salmonella* spp.).

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

At the moment there are gaps between biosecurity, trade, biodiversity and food safety legal regimes at international and European level. Future research and action on plant and food biosecurity should include:

- Implementing a stakeholder forum (possible coordination and support action);
- Harmonising and integrating biosecurity systems: “one health” paradigm strengthening the links between plant, animal and human health; enhancing networking with other EU-funded projects in the field of biosecurity in order to take advantage of the synergies that exist across sectors;
- Ensuring the sustainability of the virtual diagnostic network and widening its user base throughout the EU in order to increase the ability to log disease outbreaks and to enable early warning systems;
- Ensuring the durability of the PLANTFOODSEC network, which will require more resources for training and staff exchange, and for external organisations and end users (COM services), taking into account risks related to dual-use research;
- Creating a robust programme (including infrastructure) for protecting EU crops and other plant resources, which will require significantly more trained personnel at all levels; preparing appropriate educational materials; increasing education programmes for extension services, the potential first-line responders; and further
- Developing microbial forensics to help determine the geographic origin of introduced pathogens and distinguish between the accidental and intentional introduction of pathogens.

Etichal aspects to be developed

Dual use of research for students and scientists involved in plant and food biosecurity.

Soco-economic aspects to be developed

- Economic impact of plant and food biosecurity outbreaks;
- Strategies for risk communication.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Center of Competence for the innovation in the agro-environmental field** of University of Torino	**AGROINNOVA**	Italy
2	National Institute of Agricultural Botany	NIAB	UK
3	Food and Environment Research Agency	FERA	UK
4	London Imperial College	IMPERIAL	UK
5	Institute for crop sciences and resource conservation - University of Bonn	UNIBONN	Germany
6	Institut National de la Recherche Agronomique	INRA	France
7	Regional Environmental Center	REC	Hungary
8	Middle East Technical University	MITU	Turkey
9	Justice Research Institute	UNICRI	Italy
10	Agricultural Research Organisation	ARO	Israel
11	National Institute for Microbial Forensics & Food and Agricultural biosecurity	NIMFFAB	USA

PROACTIVE / *PRedictive reasOning and multi-source fusion empowering AntiCipation of attacks and Terrorist actions In urban enVironmEnts*

Info

Call:	FP7-SEC-2011-1- Capability Project Topic: SEC-2011.1.2-1 Strategies for countering a terrorist attack in an urban environment.
Total cost:	4,679,412.00 €
EU funding:	3,371,799.60 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,746,112.00 €
EU funding for Italy:	1,219,294.00 €
Website:	http://www.fp7-proactive.eu

Abstract

During the last decade the world has witnessed major terrorist attacks in urban environments, such as the collapse of New York's Twin Towers on 11th September 2001, the bombing of packed commuter trains in Madrid on 11th March 2004, as well as the London bombings in July 2005. These incidents have manifested that modern cities are very susceptible to terrorist attacks. This weakness is directly related to the special characteristics of urban areas, which comprise a number of man-made structures (buildings, infrastructure and facilities), along with variable and complex dynamics of economic, political and cultural interactions. Broadly definable as "social variables" of the urban context, these interactions need to be addressed: an example is the concepts of "community" and "familiarity": the strength of community is familiarity. The communities of urban-based migrant populations, left unassimilated within the larger scope of established metropolitan areas, often become inward focused and ethnocentric havens for undocumented travellers, criminal activity focused on immigration/documentation, and a base for material support to terrorists. Terrorists actively seek out the familiarity of communities sympathetic to their cause to solicit funding, support, documentation, jobs, and recruits.

Combating terrorists in an urban environment is a very challenging task, given the complex social inter-relationships and interactions of the various groups engaged in a terrorist incident, the high degree of uncertainty associated with the location and origin of potential attacks, the need to protect several infrastructural facilities (such as telecommunications, energy, and transportation hubs), as well as the more general cultural, political and social conditions of an urban environment. In response to these challenges, security forces, counter-terrorism units, police authorities and intelligence agencies are increasingly looking into novel processes and tools that could help them to perceive indications of terrorist attacks, while also predicting potential incidents in order to adapt their operations accordingly

The main goal of PROACTIVE is to research a holistic citizen-friendly multi sensor fusion and intelligent reasoning framework enabling the prediction, detection, understanding and efficient response to terrorist interests, goals and courses of actions in an urban environment.

To this end, PROACTIVE will rely on the fusion of both static knowledge (i.e. intelligence information) and dynamic information (i.e. data observed from sensors deployed in the urban environment). The framework will be user-driven, given that the project is supported by a rich set of end-users, which are

either members of the consortium or members of a special end-user advisory board.

From a technological perspective, PROACTIVE will integrate a host of novel technologies enabling the fusion of multi-sensor data with contextual information (notably 3D digital terrain data), while also resolving the ambiguities of the fusion process. Moreover, the PROACTIVE framework will incorporate advanced reasoning techniques (such as adversarial reasoning) in order to intelligently process and derive high level terroristic semantics from a multitude of source streams. The later techniques will be adapted to the terrorist domain, in order to facilitate prediction and anticipation of actions and goals of the terroristic entities.

Overall, PROACTIVE will leverage cutting-edge technologies such as the Net-centric Enable Capability (NEC) approach and the emerging "Internet-of-Things" concept, which are key enablers of new capabilities associated with real-time awareness of the physical environment, as well as with tracking and analyzing human behaviour. PROACTIVE will address the technological challenges that inhibit the wider deployment of NEC/ IoT in anti-terrorist applications.

Following the deployment and evaluation of the framework, PROACTIVE will produce a set of best practices and blueprints, which will contribute to a common EU approach to terrorist prevention in an urban environments.

Main technological and scientific outcomes

The main objectives of the PROACTIVE project are the following:

- To research and develop a scalable information fusion grid and accompanying TR and CA algorithms that can short-term anticipate and prevent terroristic activities and asymmetric attacks in large scale urban environments. The fusion grid will be autonomic, self-organizing and adaptive to specific urban environments, terrorist profiles and protection goals;

- To implement, validate and evaluate the concept and associated methods, tools and techniques in a controlled (yet realistic) urban environment (which may include simulated components), in strict cooperation with several security agencies (i.e. police) and antiterrorism/criminology centres;

- To ensure the privacy friendly nature of the PROACTIVE framework, while also creating a privacy certification suite for benchmarking and measuring the privacy friendliness of the framework.

The proposed framework in the project will facilitate security forces both in automatically acquiring, assessing and preventing to situations that might relate to terrorist attacks. The pervasive and autonomic nature of the framework will facilitate the security forces to leverage information by multiple-sensors, since it will obviate the need for manual surveillance and processing of the sensor streams (e.g., watching hundreds of cameras).

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Vitrociset S.p.A.**	**VITROCISET**	Italy
2	AGH University of Science and Technology.	AGH	Poland
3	Research and Education Laboratory in Information Technology	RELIT	Greece
4	Consorzio Milano Ricerche	CMR	Italy
5	HW Communications Ltd	HW-COMMS	UK
6	Center for Security Studies (KEMEA) - Ministry of Citizen Protection	KEMEA	Greece
7	Kingston University	KINGSTON	UK
8	Istituto di Sociologia Internazionale di Gorizia	ISI	Italy
9	MTA SZTAKI Computer and Automation Research Institute	MTA SZTAKI	Hungary
10	Universität der Bundeswehr München	UNIBW	Germany

PROTECTRAIL / *The railway industry partnership for integrated security of rail transport*

Info

Call:	DG Enterprise - Security Call FP7-SEC-2009-1, topic SEC-2009.2.2.1: Integrated protection of rail transportation
Total cost:	21,600,000 €
EU funding:	13,100,000 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,746,112.00 €
EU funding for Italy:	1,219,294.00 €
Website:	http://protectrail.eu

Abstract

Facing the problem of enhancing the railway security with a systematic top-down approach (i.e. to search for an all-inclusive solution valid for all the conceivable threat scenarios) is judged by PROTECTRAIL members too ambitious even if it could generate potential economies of scale and effort rationalisation. The proposed PROTECTRAIL approach is therefore to split the problem of making the railway more secure into smaller asset-specific security problems (missions) for which it is easier to reach satisfactory solutions applicable and usable in different threat scenarios. Each sub-mission could be therefore better oriented to particularly significant areas of interest, resulting from risk analysis or from rail operator priorities. In a clear view of scope and performance goals, for each sub mission it will be easier to define, research and develop solutions in terms of architectures, technology deployment, as well as the necessary procedures, organizations to manage the specific issue. The PROTECTRAIL challenge is therefore to make interoperable the single asset-specific solutions and to conceive and design a modular architectural framework where each asset-specific solution can be “plugged”, that is the basis to assure a streamlined process of federation, integration and interoperability of respective solutions. The PROTECTRAIL project will address the following security sub-missions: protection of signal and power distribution systems against any terrorism act, track clearance, clearance of trains before and after daily use, staff clearance, luggage clearance control, passenger clearance control, freight clearance control, tracking and monitoring of rolling stock carrying dangerous goods, protection of communication and information systems, stations, buildings and infrastructure protection.

Main technological and scientific outcomes

The main objectives of the PROTECTRAIL project are the following:

- SOA integration of railway security capacities with a definition of a common event model representing in a standardised way time, geo-location, available resources and ancillary information and implementation and demonstration of the feature and discovery mechanisms;
- Improved railway security solutions with operator in the loop.

Products/Operational Prototypes validated by End-users

The first demo took place on from 8th an 11th October 2013 in Zmigrod (Poland).

At the demo were present rail operators (SNCF - France, RFI - Italy, PKP PLK - Poland, Litrail - Lithuania, ZSSK- Slovakia, ProRail - Netherland, LDZ -Latvia) – and railway stakeholders (UIC -International Union

of Railways, UNIFE - Professional association for the railway supply industry, CER - The Community of European Railway and Infrastructure Companies, UK Transport Ministry, Polish Transport Ministry, SOK Polish Railway Police).

The following scenarios have been demonstrated and validated by end users during the demo week:

- "Stations and passengers" covering passenger tracking and left luggage neutralization;
- "Intrusion in railway depot and unauthorised areas" covering CCTV analytics, biometric systems cyberprotection of signalling and onboard low power sensors;
- "On-board with passengers" covering crisis management systems, ISO 22311 based NVR systems, on-board tools for the train managers, CBRNE devices and passengers and luggage reconciliation systems;
- "Dangerous goods in freight trains" covering hand-held CBRNE scanners and gantry X-Ray scanning;
- "Track protection" covering CCCTV based change detection.

Moreover it has been tested the 4G LTE transmission from on-board to wayside.

The feedback is not yet available.

It is planned to have another demo in Villecresnes (near Paris) in the period November 2013 - January 2014 and a final demo event for low impact high probability events in May 2014.

Follow-up

New technological, scientific or application perspective opened by the project

SOA integration in railway security domain.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

- Protection from high probability low impact events (vandalism, copper theft, etc.);
- Cybersecurity of railway infrastructures.

Etichal aspects to be developed

Usability of some of the proposed solutions dealing with privacy of travelers (e.g. face recognition and people tracking)

Socio-economic aspects to be developed

Cost and benefits of railway security solutions.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	Ansaldo STS S.p.A.	STS	Italy
2	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek	TNO	Netherlands
3	Union Internationale Des Chemins De Fer	UIC	France
4	SELEX-ES Spa	SELEX-ES	Italy
5	Bombardier Transportation GMBH	BT	Germany
6	Alstom Transport SA	ALS	France
7	Thales Transportation Systems SA	TTS	France
8	Sarad GmbH	SARAD	Germany
9	UNIFE – The European Rail Industry	UNIFE	Belgium
10	Sagem Sécurité SA	SAG	France
11	Ductis GmbH	DUCTIS	Germany
12	Železnicná spolocnost Slovensko a.s.	ZSSK	Slovakia
13	Joint Stock Company Lithuanian Railways	LITRAIL	Lituania
14	ItalCertifer S.c.p.a.	ITCF	Italy
15	PKP Polskie Linie Kolejowe SA	PKPPLK	Poland
16	D'Appolonia S.p.A.	DAPP	Italy
17	Elbit Systems Ltd.	ESL	Israel
18	Facultés Universitaires Notre-Dame de la Paix	FUNDP	Belgium
19	EPPRA	EPPRA	France
20	Kingston University Higher Education Corporation	KU	UK
21	Société d'Etude et de Réalisation Nucléaire	SODERN	France
22	Smiths Heimann S.A.S.	SMITHS	France
23	Rail Cargo Austria	RCA	Austria
24	CEA Commissariat à l'Énergie Atomique	CEA	France
25	Canberra nv/sa (Areva Group)	CB	Belgium
26	Institut Franco-Allemand de Recherches de Saint-Louis	ISL	France
27	Turkish State Railways	TCDD	Turkey
28	MER MEC S.p.A.	MERMEC	Italy
29	Société Nationale des Chemins de Fer	SNCF	France

SeaBILLA / *Sea border surveillance*

Info

Call:	SEC-2009.3.2.2
Total cost:	15,438,918 €
EU funding:	9,841,610 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	4,372,591 €
EU funding for Italy:	2,828,163 €
Website:	http://www.seabilla.eu

Abstract

The SeaBILLA proposal aims to 1) define the architecture for cost-effective European Sea Border Surveillance systems, integrating space, land, sea and air assets, including legacy systems; 2) apply advanced technological solutions to increase performances of surveillance functions; 3) develop and demonstrate significant improvements in detection, tracking, identification and automated behaviour analysis of all vessels, including hard to detect vessels, in open waters as well as close to coast.

SeaBILLA is based on requirements for Sea Border Surveillance defined by experienced operational users. These requirements have been transformed into Scenarios, included in Annex to this proposal, representative of gaps and opportunities for fruitful cooperative information exchange between Members States a) for fighting drug trafficking in the English Channel; b) for addressing illegal immigration in the South Mediterranean; c) for struggling illicit activities in open-sea in the Atlantic waters from Canary Islands to the Azores; in coherence with the EU Integrated Maritime Policy, EUROSUR and Integrated Border Management, and in compliance with Member States sovereign prerogatives.

The project will provide concrete added value and benefits for users, by providing a solution that can be implemented at national and EU level to increase effectiveness, pool resources and address Maritime Security and Safety challenges; for world competitiveness of EU industries, by increasing knowledge and reducing risks for future product investments; for European citizens, by providing effectively deployable solutions for law enforcement along the European sea borders. SeaBILLA will be carried out by a reliable team of major European system integrators, technology providers and leading research organizations, establishing strong links with several EU and national projects and assuring worldwide exploitation of project results.

Main technological and scientific outcomes

The project provides insights on sensor networking configuration with specific focus on updated threats in significant European scenario. Quantitative benefits expressed in terms of MoP and MoE of the selected technologies / solution have been computed also using simulation environments provided by the partners. Tight interaction with end user communities have been guaranteed by regional demonstration and end user workshops. Technology qualifications have been supported by Seabilla trial campains.

Products/Operational Prototypes validated by End-users

Passive Radar was tested in Lampedusa, Civitavecchia and Livorno (Italy). At this demo were present Italian Navy and Italian Coast Guard.

Passive Radar was tested also in Cherbourg (France). At this demo were present French Navy and DGA.

UAV Flight was tested in the English Channel. At this demo were present French Navy and DGA.

The project is still running to date

Follow-up

New technological, scientific or application perspective opened by the project

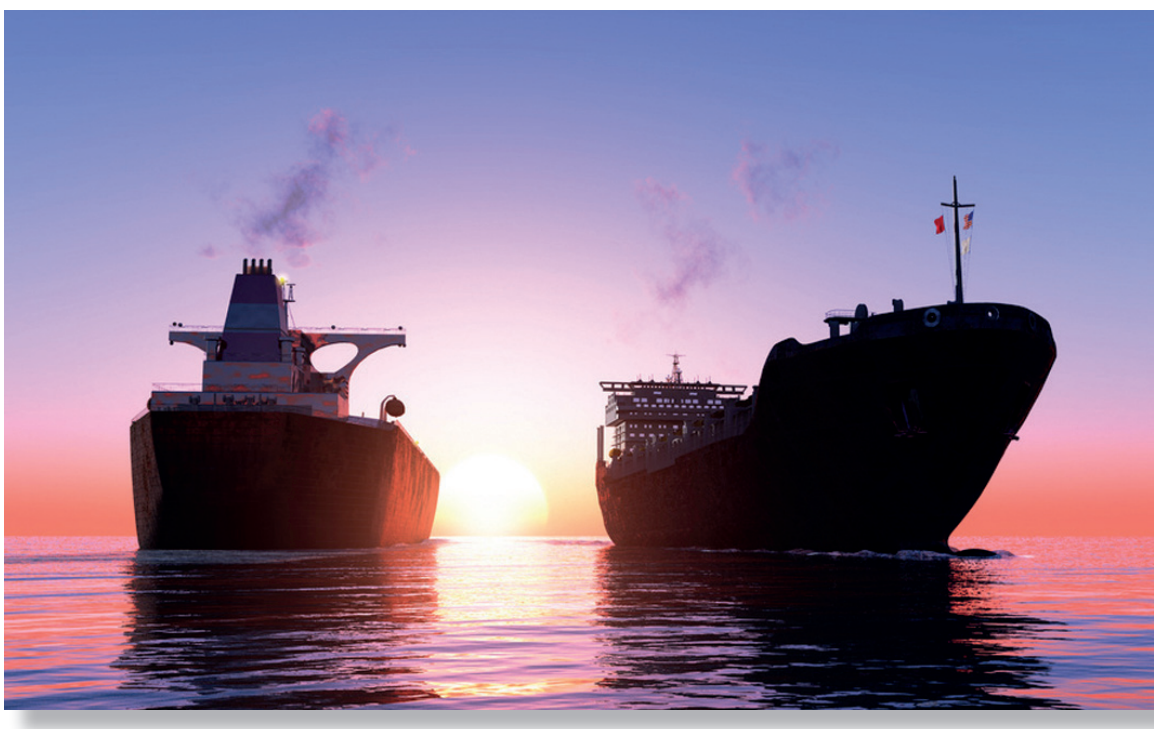
- Cooperative data (AIS, Radar Plot, Observations) provided by commercial fleets to a regional command and control centre to increase maritime situational awareness;
- Passive means as gap filler in coastal surveillance network.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

Passive radars as enabling technologies to monitor either small boat and low altitude flying objects.

Socio-economic aspects to be developed

Perform structured value for money analysis combining engineering studies, field evidences and commercial aspects.



Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex ES**	**SELEX ES**	Italy
2	Alenia Aermacchi	ALA	Italy
3	BAE Systems	BAES	UK
4	Consorzio Nazionale Interuniversitario Telecomunicazioni	CNIT	Italy
5	Correlation Systems	CorrSys	Israel
6	EADS Defence & Security	EADS DS	France
7	Eurocopter Espana	ECE	Spain
8	Edisoft	EDISOFT	Portugal
9	Swedish Defence Research Agency	FOI	Sweden
10	HITT	HITT	Netherlands
11	Indra Espacio	IE	Spain
12	Indra Sistemas	INDRA	Spain
13	Joint Research Center	JRC	EU
14	MONDECA	MONDECA	France
15	SAGEM Défense Sécurité	SAGEM	France
16	Space Application Service	SpaceApps	Belge
17	Thales Alenia Space Italia	TASI	Italy
18	Thales Netherlands	TNNL	Netherlands
19	Nederlandse Organisatie Voor Toegepast – Natuurwetenschappelijk Onderzoek	TNO	Netherlands
20	Telespazio	TPZ	Italy
21	Thales Systemes Aeroportes	TSA	France
22	TTI Norte	TTI	Spain
23	University College London	UCL	UK
24	Universidad de Murcia	UMU	Spain
25	University of Portsmouth	UoP	UK

SECONOMICS / *Socio-Economics meets Security*

SECONOMICS

Info

Call:	FP7-SEC-2011-1
Total cost:	4,720,656.77 €
EU funding:	3.451.096,14 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,280,000 €
EU funding for Italy:	979,000 €
Website:	http://seconomicsproject.eu

Abstract

SECONOMICS goal is synthesizing sociological, economic and security science into a usable, concrete, actionable knowledge for policy makers and social planners responsible for citizen's security. The project is driven by industry case studies and will specifically identify security threats in transport (air and urban and super urban metro) and critical infrastructure. The research focus places social science and political science at the heart of the modeling framework. In particular the project seeks to explore the challenges of pan European coordination in security outcomes for transport and critical infrastructure.

The contribution of the project will be in developing and furthering the state of the art in modelling security problems in a technological and socio economic context and then applying state of the art risk assessments and analysis of the social context to develop optimal policies. The outputs are twofold: first assessment of the future and emerging threats in the identified areas with rigorous modeling of the optimal mechanisms for mitigation within the policy domain. Second, and more crucially, a generalized policy "toolkit" that will assist decision makers in identifying and reacting coherently (within the appropriate social context) to future and emerging threats that may arrive long after the project has been completed.

The lasting impact of SECONOMICS will be a methodological revolution driven by a common, but diverse set, of modelling tools and utilizing recent advances in modelling technology that seamlessly transverses the social, economic and technological domains.

Main technological and scientific outcomes

The main objectives of the SECONOMICS project are the following:

- To provide a general socio-economic methodology for security resource allocation which is relevant across various domains;
- To provide a tool that facilitates such process to policy makers;
- To showcase such methodologies and tools in relevant case studies, which may serve as best practice analysis that may replicated in other European (and global) critical infrastructures;
- To include within the global risk governance process issues in relation with social perceptions and attitudes towards risk as key drivers;

- To improve the process of identifying and assessing risks from an economical point of view, the process of balancing security with policy, economics and other relevant constraints and the process of quantifying positive and negative externalities.

Products/Operational Prototypes validated by End-users

Until present, models were presented to stakeholders. Not sill validated, the process is ongoing.

Our technical partners have developed several risk and economics models. They presented their models to stakeholders

Since the SECONOMICS project is in the middle years, models/protypes are still primitive. However, we presented the draft models/prototypes to stakeholders, particularly airport operators, critical infrastructure operators and urban transport operators (Not national or supranational policy makers yet).

The potential users are quite diverse, including:

- Ministries of defence
- Homeland security ministries
- Insurance companies
- Private security companies
- Owners of critical infrastructure (electrical companies, banks,…)
- Airport authorities, National Grid authorities, Transportation network authorities
- City townhalls
- Regulators: CPNI (UK), ENTSO (EU), ENISA (EU)
- EUROCONTROL
- Community of critical national infrastructure suppliers
- National government and wider EU institutions
- Research Community.

Follow-up

New technological, scientific or application perspective opened by the project

SECONOMICS focuses not only a techological aspect but also sociological and economic aspects in investigating security. Furthermore, SECONOMICS explores the issues of new and emerging security threats as well as current security threats.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

Most of security regulations/compliances affect the general public. Security project should take into account the impact of security regulations on the public and explore a way to investigating it.

Socio-economic aspects to be developed

Most of security regulations/compliances affect the general public. Security project should take into account the impact of security regulations on the public and explore a way to investigating it.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Università degli studi di Trento**	**UNITN**	Italy
2	Deep Blue Srl	DBLUE	Italy
3	Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V.	FHG	Germany
4	Universidad Rey Juan Carlos	URJC	Spain
5	The University Court of the University of Aberdeen	ABDN	UK
6	Ferrocarril Metropolita de Barcelona SA	TMB	Spain
7	ATOS Spain SA	ATOS	Spain
8	SecureNOK AS	SNOK	Norway
9	Institute of Sociology of the Academy of Sciences of the Czech Republic Public Research Institution	IS AS CR	Czech Republic
10	National Grid Electricity Transmission PLC	NGET	UK
11	Anadolu University	ANADOLU	Turkey

SESAME / *Securing the European Electricity Supply Against Malicious and accidental thrEats*

Info

Call:	FP7-SEC-2010-1
Total cost:	3,993,481.28 €
EU funding:	2,753,789.76 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	926,053.28 €
EU funding for Italy:	732,159.96 €
Website:	https://www.sesame-project.eu

Abstract

Threats for the supply of electricity have changed dramatically throughout the last decade: additional to the natural and accidental ones, the new threat of malicious attacks needs to be considered. Such attacks might be jointly imparted so as to affect large portions of the European grid, make repair difficult and cause huge societal impact. The outstanding importance and the far more complex level of interconnectivity of electricity distribution / transmission / generation – compared to the supply through other energy carriers - makes the development of a highly focused toolkit for its protection an essential and urgent task. SESAME develops a Decision Support System (DSS) for the protection of the European power system and applies it to two regional electricity grids, Austria and Romania. This DSS enables to:

- identify the vulnerabilities and to detect their origins;
- estimate the damage / impact of real or simulated network failures;
- identify the possible measures for prevention of outages and acceleration of automatic restoration;
- rank these measures according to their effectiveness and their cost-benefit ratios;
- carry out contingency analyses of the transmission / distribution network and generation facilities;
- detect long-term erroneous trends in the security of energy supply and counteract against them by adjusting the market mechanisms.

There do not exist State-of-the-Art approaches incorporating all of these core dimensions of the problem: the increase in complexity of the security of energy supply requires a comprehensive and multi-disciplinary solution. SESAME brings together the most distinguished experts in the fields of power network security, technology policy and regulatory economics, impact assessment of disasters, network simulation software and knowledge engineering. All partners have proven their excellence in complex security research in earlier cooperative projects and most of them have already worked together successfully.

Main technological and scientific outcomes

Objective 1: The main output of SESAME is a prototype software package, which enables the user to undertake all necessary analyses of the 4 steps explained above. As output of the tool, the (a) vulnerabilities of the analyzed grid and production plants are fully detected, their origins are given, the (b) impact / damage of real or simulated network failures are precisely estimated, the possible countermeasures are identified and the most appropriate of these (c) measures for prevention of outages and acceleration of automatic restoration are suggested, which are derived from (d) precise contingency analyses of the transmission and distribution network.

Objective 2: The development of a comprehensive regulatory framework for the security of electricity systems, which is based around three main dimensions – i.e. economic analysis, technology and innovation policy, and regulatory schemes at both national and the EU level. The presence of regulatory authorities in the core project consortium as well as in the Stakeholder Advisory Board ensures the incorporation of these analyses in future European regulation.

Products/Operational Prototypes validated by End-users

The prototype software package implementing the DSS will be tested by 2 end-users.

The 2 end users will be :

- Romanian TSO – Transelectrica ;
- Austrian regulator – Energie – control.

Two demos are undergoing thanks to 2 end users partners.

The project is not finished yet.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Politecnico di Torino**	**POLITO**	Italy
2	Energieinstitut an der Johannes Kepler Universität Linz	EIL	Austria
3	INDRA SISTEMAS S.A. - Spain	INDRA	Spain
4	University of Durham	DUR	UK
5	ENERGIE-CONTROL GMBH	E-CONTROL	Austria
6	Deloitte SL	DTT	Spain
7	Technische Universiteit Delft	TUD	Netherlands
8	Compania Nationala de Transport al Energiei Electrice Transelectrica SA	TEEL	Romania
9	RS Consulting Limited	RS	UK
10	Joint Research Centre – European Commission IET	JRC	Belgium

SICMA / *Simulation of Crisis Management Activities*

Info

Call:	FP7-SEC-2007-1
Total cost:	3,902,600 €
EU funding:	2,566,330 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	1,483,970 €
EU funding for Italy:	970,260 €
Website:	http://www.sicmaproject.eu

Abstract

SICMA focuses on computer assisted decision making for Health Service crisis managers. The research is targeted to the evaluation of decision-support enhancement potential achievable by integrating a suite of models and analysis tools able to provide insights into the collective behaviour of the whole system in response to different crisis situations and decision implementations.

The operational objectives are aimed at providing decision support during the crisis response:

- Preparation phase: assisting in the identification of the best way to employ available assets, the limits of the achievable response and the effectiveness of different inter/intra-services cooperation procedures;
- Implementation phase: providing a forecast of the situation evolution, proposing doctrine/procedures based solutions and presenting the effects of alternative decisions (to test mitigation measures before they are implemented).

The scientific and technological objectives are aimed at:

- Studying the effects of unpredictable factors (like human behaviour, size/specifics of the incident) to present the user with a “distribution” of the effectiveness of a certain “decision” rather than the effectiveness of that solution deterministically dependant on the preconceived scenario;
- Modelling human behaviour to represent individuals and groups as realistically as possible;
- Developing an integration infrastructure allowing for efficient integration of simulation models/supporting-tools developed or provided by different organisations.

The combined effects of the:

- “Bottom-up” modelling approach (i.e. build independent model components and then combine them);
- Unpredictable factors modelling (e.g. human behaviour);
- Analysis of decision-effectiveness distribution has the advantage of documenting both the unexpected bad and good things in the organization(s) thus leading to better responses, fewer unintended consequences and greater consensus on important decisions.

Main technological and scientific outcomes

Main Outcomes in terms of technological/scientific advances:

- M&S tools able to simulate:
  - The scenario evolution;
  - The activities and interactions of the Health Service components;
  - The effects of the interactions of the Health Service with the other Organizations;
  - The effects of international cooperation (e.g. availability of additional resources).
- Analysis Tools able to:
  - Present decision makers with the measures of effectiveness required to identify the bottleneck and the possible improvements;
  - Compute the "distribution" of the effectiveness of a "decision" rather than the effectiveness of that solution deterministically dependant on the scenario
- Training & Support tools able to:
  - train the crisis manager in the execution of the agreed procedures;
  - provide the user with the correct procedures to solve the problem.

Products/Operational Prototypes validated by End-users

The SICMA prototype has been designed and developed with the continuous support of end-users:

- Consiglio Nazionale delle Ricerche, Italy – scientific advisor;
- Università Cattolica del Sacro Cuore – end-user.

Tests are being performed using data recorded during real crisis.

At the moment there isn't made any demo.

Follow-up

SICMA has addressed only the "traditional" type of injures ("trauma").

Extension to the CBRN case is being performed in the scope of the PRACTICE and EDEN FP7 projects.

New technological, scientific or application perspective opened by the project

SICMA is being proposed as a tool to support the planning of medical logistics in military out-of-area operations.

A similar approach can be used to support other organisations involved in Crisis Management Operations.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex ES**	**SELEX ES**	Italy
2	ITTI Sp. z o.o.	ITTI	Poland
3	Consiglio Nazionale delle Ricerche	CNR	Italy
4	SKYTEK	SKYTEK	Ireland
5	Industrieanlagen Betriebsgesellschaft mbH	IB	Germany
6	Elbit Systems Ltd	ES	Israel
7	Centre for European Security Strategies	CESS	Germany
8	IFAD TS A/S	IFAD	Denmark
9	Università Cattolica del Sacro Cuore	UNICATT	Italy

STRUCTURES / *Strategies for the improvement of critical infrastructures resilience to electromagnetic attacks*

Info

Call:	SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic Attacks - Capability Project
Total cost:	4,797,731.63 €
EU funding:	3,497,673.54 €
Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:	
Total cost for Italy:	991,186 €
EU funding for Italy:	729,811 €
Website:	http://www.structures-project.eu

Abstract

The aim of the STRUCTURES project is to analyze the possible effects of intentional electromagnetic interference (IEMI) on civilian infrastructures (power plants, communication systems, computer networks, etc.) and assess the related impact for defense and economic security. Innovative awareness and protection strategies will be identified and an outline of the actual threats and consequences of an electromagnetic attack will be provided to policy makers.

The Project is part of the more general theme of “Critical Infrastructures Protection”, focusing in particular on the “Intentional Electro Magnetic Interference” (IEMI) threat.

Such a threat is going to become in the next future more and more dangerous due to the largest availability of low/medium cost electromagnetic sources and to the increasing technical level of terrorism and organized crime.

The project will go through a number of steps to develop new capabilities and technologies and acquire information on IEMI effects in order to help civil society and policy makers to fight such a threat.

A first step will be the assessment of the scenarios of interest and the identification, preparation and validation of analytical/numerical and experimental methodologies for risk assessment and design of protection devices.

An investigation on IEMI effects on the critical infrastructures and sub-systems will follow, as well as the identification and testing of cost-effective technologies able to improve the infrastructure resilience.

Finally Guidelines and methodologies for IEMI protection will be developed and organised in pre-regulatory documentation.

The Project is expected first of all to provide improved comprehension of the problems and risks related to IEMI attacks to Critical Infrastructures. Further, viable (e.g. not only technically but also economically sustainable) solutions to estimate and reduce the risk will be made available to be provided to policy makers and Critical Infrastructure managers.

Main technological and scientific outcomes

Main Outcomes in terms of technological/scientific advances:

- Classification of e.m. susceptibility levels of equipment, systems and infrastructures;
- Optimal design criteria to make infrastructures more robust against IEMI; IEMI shielding for structures, systems, sub-systems etc.;
- Design of components and strategies for protection (with preference given at first to low cost solutions);
- Design of components and strategies for protection (with preference given at first to low cost solutions);
- Simulations tools for analysis (risk assessment) and design (protection improvement).

Products/Operational Prototypes validated by End-users

Not applicable at the moment. The project started on July 2012.

Follow-up

Based on the results of study of the project, future developments are identified in the definition and verification of methodologies for the risk assessment on existing infrastructure and the development of non-invasive protection methods (active methods).

New technological, scientific or application perspective opened by the project

- Use of modeling methods for the risk analysis of Intentional Electromagnetic Interference to Critical Infrastructures;
- Active systems for the protection of Critical Infrastructures against Intentional Electromagnetic Interference;
- New standards for the protection of Critical Infrastructures against Intentional Electromagnetic Attacks.

Suggestions for eventual new themes related to the project and its evolution that can be proposed in H2020

Development of prototyping and testing of active protection system against Intentional Electromagnetic Interference.

Ethical aspects to be developed

Analysis of dual use issues.

Socio-economic aspects to be developed

Economic impact on Critical Infrastructures design, realization and maintenance of the protection systems.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Ingegneria Dei Sistemi S.p.A**	**IDS**	Italy
2	Ecole Polytechnique Fédérale de Lausanne	EPFL	Switzerland
3	Haute Ecole Spécialisée de Suisse Occidentale	HES-SO	Switzerland
4	The University of York	UoY	UK
5	MONTENA technology sa	MONTENA	Switzerland
6	Helmut-Schmidt- Universität	HSU	Germany
7	Bergische Universität Wupperta	BUW	Germany
8	University of Twente	UT	Netherlands
9	Istituto Superiore Mario Boella	ISMB	Italy
10	Navigate Consortium	NAVI	Italy

Progetti 5 call Security

(FP7-SEC-2012)

DESTRIERO / *A DEcision Support Tool for Reconstruction and recovery and for the IntEroperability of international Relief units in case Of complex crises situations, including CBRN contamination risks*

Objective

Today more people than ever are threatened by disasters, with no regards if natural or man-made. Furthermore, CBRN tamination risks can occur as a sequence of these events. Regions affected are wider and wider and restruction and recovery operations are longer-lasting, costly and complex, especially when detamination is necessary.

DESTRIERO aims at developing a next generation post-crisis needs assessment tool for restruction and recovery planning, including structural damage assessment through advanced remote sensing enriched by in-field data collection by mobile devices (buildings, bridges, dams) and related data integration and analysis, based on international standards, novel (automated) data and information interoperability across organisations and systems, in combination with an advanced multi-criteria decision analysis tool and methodology for multi-stakeholder information analyses, priority setting, decision making and recovery planning.

Earth observation images will tribute to fast damage assessment and monitoring of the areas, together with data acquired by relief units on the field using novel smart-phone apps. Identified needs will be recorded, stored and made available to all organisations involved. Coordination and collaborative work at all levels of the organisations and among different ones will be possible through a network centric approach for the interoperability of information and service and the decision support tool.

Critical infrastructure recovery will be sidered with priority, as essential for the recovery of social and eomic aspects (roads, bridges, schools, hospitals, plants, etc.), CBRN tamination and humanitarian aspects will be taken into sideration, as aggravating circumstances, while support to accountability of humanitarian aid tributions will be facilitated.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**E-GEOS Spa**	**E-GEOS**	Italy
2	Consorzio Interuniversitario Nazionale per l'Informatica	CINI	Italy
3	ITTI Sp Zoo	ITTI	Poland
4	Saadian Technologies Limited	SAADIAN	Ireland
5	Amper Programas de Electronica y Comuni-caciones Sa	AMPER	Spain
6	Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V.	FRAUNHOFER	Germany
7	Szkola Glowna Zluzby Pozarniczej	SGSP	Poland
8	Hoge Gezondheidsraad	HGR	Belgium
9	Asociacion de Empresas Tecnologica Inno-valia	INNOVALIA	Spain
10	Universitat Politecnica de Valencia	UPV	Spain
11	Police Service of Northern Ireland	PSNI	UK
12	Thales Sa	THALES	France
13	SESM Soluzioni Evolute per la Sistemistica e I Modelli Scarl	SESM	Italy

ESENET / *Emergency Services Europe Network*

Objective

The improvement of the European capability to respond to everyday emergencies and guarantee the safety and security of citizens in case of major emergencies and disasters requires a significant step forward in the integration of existing systems at several levels.

The ESENet initiative aims at establishing a network of stakeholders in the Emergency Management domain that will identify, discuss and agree on needs, requirements, new technologies and best practices in responding to everyday as well as to major emergencies.

The project plans to organize a total of 8 web-meetings and 4 workshop, with all the network members invited to attend and contribute to working documents prepared by the project partners on several topics, including interoperability at all levels (from technical level to organizational) and in all types of safety and security missions (daily/ordinary and/or large scale missions as well as local or cross-border missions).

The ultimate goals of ESENet are:

- The identification of gaps in the emergency service provision chain and the collection of user requirements; the results of such activity will be a living document that will be made available to all stakeholders;
- The selection of available and/or promising technologies for tackling the identified challenges, also identifying areas where further research is needed; the project will deliver a public report;
- The analysis of organizational gaps, with suggestions and best practices at EU level about procedures, framework agreements and reorganizing suggested tasks; the results of such work will be reported in a public deliverable in form of suggestion of a roadmap to improve Emergency Services;
- The identification of available standards or areas where standards will be needed.

The project is built around the members and the ESSN (Emergency Services Staff Network) currently organised by the project partner EENA. 22 members have already confirmed in writings their interest in being part of the ESENet project.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Intelligence for Environment and Security Srl – Ies Solutions**	**IES**	Italy
2	ERUPSI Sro	ERUPSI	Slovakia
3	European Emergency Number Association Asbl	EENA	Belgium

GAMMA / *Global ATM security management*

Objective

The GAMMA project stems from the recognition that while the SESAR initiative is effectively addressing some security issues in the new global ATM scenarios, there is a need to extend this scope to ensure a comprehensive assessment of the full set of security threats and vulnerabilities affecting ATM, considered as a system of systems and covering operational as well as technological aspects. In addition, there is a need, not completely met by SESAR, to establish a comprehensive framework for managing ATM security once SESAR deployment is engaged to minimise the effects of ATM crises brought about by security incidents. The GAMMA vision is to adopt a holistic approach for assessing ATM security, maintaining alignment with SESAR and reaching the following main objectives:

- Extend the scope of threat assessment performed within SESAR to a more comprehensive system of systems level, inclusive of all ATM assets and all forms of threats.
- Develop a Global ATM Security Management framework, representing a concrete proposal for the day-to-day operation of ATM Security and the management of crises at European level.
- Define the architecture of an ATM security solution, suitable to support the security management of the global ATM system.
- Design and implement prototype components of the ATM solution so as to demonstrate the functionalities and operations proposed for the future European ATM.
- Set up a realistic validation environment, representative of the target ATM solution, through which to perform validation exercises aimed at validating the feasibility and assessing the adequateness of the procedures, technologies, and human resources issues proposed.

GAMMA is strongly driven by the End Users present in the consortium supporting the project activities from the threat and vulnerability analysis to the validation of the developed concepts. The international dimension will also be considered with special reference to interoperability with US systems.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Selex ES Spa**	**SELEX-ES**	Italy
2	Lancaster University	LANCASTER	UK
3	Thales Alenia Space Espana SA	TAS	Spain
4	Thales Avionic Sas	TA	France
5	USTAV Informatiky Slovenska Akademia Vied	UISAV	Slovakia
6	Deutsches Zentrum Fuer Luft	DLR	Germany
7	Boeing Research & Technology Europe SLU	BRTE	Spain
8	Cassidian Sas	CASSIDIAN	France
9	Administratia Romana a Serviciilor de Trafic Aerian	ROMATSA	Romania
10	ENAV Spa	ENAV	Italy
11	Thales Research & Technology Limited	TRT	UK
12	Ingeniera de Sistemas para la defense de Espana SA	ISDEFE	Spain
13	Ciaotech Srl	CIAOTECH	Italy
14	Airbus Prosky Sas	APS	France
15	European Aeronautic Defence and Space Company – Eads France SAS	EADS	France
16	RNC Avionics Limited	RNC	UK
17	Società per Azioni Esercizi Aeroportuali – SEA Spa	SEA	Italy
18	Cassidian Cybersecurity Sas	CASSIDIAN CS	France
19	42 Solutions BV	42 Solutions	Netherlands

ISITEP / *Inter System Interoperability for Tetra-TetraPol Networks*

Objective

A European network where forces share communications, processes and a legal framework would greatly enforce response to disaster recovery and security against crime. Until now, uncertainty on costs, timescale and functionalities has slowed down integration of national Public Protection & Disaster Relief (PPDR) networks. The lack of interoperable communication systems has impeded the cooperation of PPDR forces, although a strong European commitment has been established through Schengen and Lisbon treaties. ISITEP will develop procedures, technology and legal agreements to achieve a cost effective solution for PPDR interoperability. ISITEP will demonstrate full radio interface migration for PPDR resources. ISITEP end users will drive requirements to guarantee legal, operational and technical coherence. In addition, a legal agreement template will be proposed for approval between Norway and Sweden within the project timeframe.

The project goals will be obtained through the delivery of the ISITEP framework, which will be based on:

- Mission oriented procedures, functional models and legal agreements
- An European network solution integrating all types of European national PPDR networks through a novel Inter System Interface (ISI) over IP protocol encompassing:
  - ETSI standardized ISI among TETRA national networks
  - ISI over IP gateways among national TETRAPOL networks
  - ISI over IP gateways among TETRAPOL - TETRA networks
- Bi-technology terminals based on smartphones/tablets with PPDR applications
- Supporting tools to assess business sustainability, technology needs and improve training.

Through ISITEP, European end users will leverage enhanced terminals in operations abroad within an agreed framework of procedures. This will improve cooperation among European PPDR resources for the benefit of all citizens. European stakeholders will have an economically sustainable solution for sharing national PPDR services. ISITEP's results will be disseminated by a proper plan leveraging the Consortium, which includes all the manufacturers of national European networks and the main PPDR stakeholders.

Furthermore, through ISITEP technology, the European security industry will have new market opportunities.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**SELEX-ES**	**SELEX ES**	Italy
2	Istituto Superiore delle Comunicazione e delle Tecnologie dell'Informazione	ISCOM	Italy
3	Nederlandse Organisatie Voor Toegepast Natturwetenschappeljk Onderzoek	TNO	Netherlands
4	Universitat Politecnica de Catalunya	UPC	Spain
5	Net Technologies Etaireia Periorismenis Efthynis	NETTECHN	Greece
6	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	MBZK	Netherlands
7	Service Public Federal Interieur	SPF	Belgium
8	Devoteam Fringes SA	DEVOTEAM	Spain
9	Cassidian Finland Oy	CASSIDIAN	Finland
10	Università degli Studi Roma Tre	UNIROMA3	Italy
11	Cassidian Sas	CASSIDIAN	France
12	Myndigethen for Samhallsskydd och Beredskap	MSB	Sweden
13	Norwegian Ministy of Justice and Public Safety	NMJPS	Norway
14	Amper Sistemas S.A.	AMPER	Spain
15	Motorola Solutions Danmark AS	MOTOROLA	Denmark

SAWSOC / *Situation AWare Security Operations Center*

Objective

SAWSOC aims at bringing a significant advancement in the convergence of physical and logical security, meaning effective cooperation (i.e. a coordinated and results-oriented effort to work together) among previously disjointed functions. Recently some achievements have been made (e.g. SEM and SIM have merged into SIEM, and LACS and PACS have merged into IM), Security Operations Center (SOC) technology has improved significantly, but much is yet to be done. SAWSOC holistic approach and enhanced awareness technology will allow dependable (i.e. accurate, timely, and trustworthy) detection and diagnosis of attacks. This will ultimately result in the achievement of two goals of paramount importance, and precisely: 1) Guaranteeing the protection of citizens and assets, and 2) Improving the perception of security by citizens. Goal 1 is in line with the objectives of the Security Work Programme in general, and goal 2 perfectly matches the expected impact as listed in the Work Programme for Topic SEC-2012.2.5-1. SAWSOC's design will be driven by three real use cases, with highly diverse requirements. Such use cases collectively form an experimental test-bed perfectly suited for driving the design as well as for validating the development of a platform such as SAWSOC that will support true convergence of physical and logical security technologies, and overcome the fragmentation of security approaches. The first use case deals with the protection of a Critical Infrastructure for Air Traffic Management. The second deals with the protection of a Critical Infrastructure for Energy Production and Distribution. The third deals with the protection of a public place, specifically a stadium, during an event. The project will take stock of associated initiatives, which have a direct or indirect link with the topic (e.g.: topic SEC-2011.2.5-1 Cyber attacks against critical infrastructures, ESRAB and ESRIF), and will benefit of an enhanced SME participation in the Consortium, with three hi-tech SMEs from three different countries, playing relevant as well as complementary roles.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**SELEX-ES Spa**	**SELEX-ES**	Italy
2	Consorzio Interuniversitario Nazionale per l'Informatica	CINI	Italy
3	Comarch SA	COMARCH	Poland
4	Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V.	FRAUNHOFER	Germany
5	Intercede Limited	INTERCEDE	UK
6	Esaprojekt SP z oo	ESAPROJEKT	Poland
7	The Israel Electric Corporation Limited	IEC	Israel
8	ENAV Spa	ENAV	Italy
9	Lonix Oy	LONIX	Finland
10	Espion Limited	ESPION	Ireland
11	Bergische Universitaet Wuppertal	BUW	Germany

SNOOPY / *Sniffer for concealed people discovery*

Objective

Integration of a handheld artificial sniffer system for customs/police inspection purposes e.g. the control of freight containers. The artificial system should be able to seek first hidden persons and second also controlled goods, illicit drugs and safety and security hazards.

The instrument consists of a gas- and vapour sampling pump unit, an enrichment unit, a desorption unit, a detection unit (sensor array) and an alarm indicator unit. The air sampling modus needs a high air flow in order to sample and enrich a lot of target gases and the detection modus needs a low air flow modus for transporting the targets after the desorption process as low diluted as possible to the detector. The target gases cover human perspirations like carbonic acids, aldehydes, thiolic compounds and nitrogen compounds and the human breathing product CO2. Different kinds of sensors will be used so that each target can be detected as selective as possible.

For providing an estimation of the probability of the presence of humans inside the inspected area pattern recognition will be used.

The sniffer instrument will be benchmarked towards dogs and towards ion mobility spectrometry.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Università degli Studi di Brescia**	**UNIBS**	Italy
2	Consiglio Nazionale delle Ricerche	CNR	Italy
3	C-TECH Innovation Limited	C-TECH	UK
4	EADS Deutschland Gmbh	EADS	Germany
5	Università degli Studi di Roma Tor Vergata	UNIROMA2	Italy
6	Centre for Security Studies	KEMEA	Greece

SPARTACUS / *Satellite Based Asset Tracking for Supporting Emergency Management in Crisis Operations*

Objective

Motivated by the opportunity to develop industry pull applications and services for the European EGNOS and GALILEO satellite systems, SPARTACUS will design, realise, test and validate in simulated and real world scenarios GALILEO-ready tracking/positioning solutions for critical asset tracking and crisis management. Integrating, adapting, and improving hardware, software, communication, and tracking algorithm areas of expertise from consortium members strategically committed to GNSS business expansion, SPARTACUS will develop services dedicated to three application areas. They are 1) to track, trace, and localise critical transport assets especially in times of crisis and in case of major failure of existing networks, 2) to track the flow of relief support goods from the sending side to the receiving/end place, and 3) to support and ensure the safety of first responders in crisis management operations. The project will employ a deliberate methodology that leads progression through Identification, Development, Implementation and Exploitation. SPARTACUS innovation areas include hardware adaptations, algorithms for precision improvement, integration of the receivers with inertial platforms to provide dead reckoning functionalities, and communication availability in emergency by restoring local existing network over satellite backhauling. In addition, modular and scalable platforms will be made appropriate for each application area. Consortium networks, marketing channels, and end users from the rail, disaster relief, and first responder sectors will prepare these new EU-specific services for market uptake.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**D'Appolonia Spa**	**DAPP**	Italy
2	University of Newcastle Upon Tyne	NCL	UK
3	Università degli Studi di Pavia	UNIPV	Italy
4	Alma Mater Studiorum – Università di Bologna	UNIBO	Italy
5	Triagnosys Gmbh	TGS	Germany
6	Institut Mihajlo Pupin	PUPIN	Serbia
7	Akkon Hochschule Fur Humanwissenschaften	AHS	Germany
8	Globalgps Bh Doo Sarajevo	GGPS	Bosnia and Herzegovina
9	D.M.A.T. Consulting KG	DMAT	Austria
10	Autoritatea Feroviara Romana	AFER	Romania
11	Imoss Ag	IMSS	Switzerland
12	Ansur Technologies AS	ART	Norway

TAWARA_RTM / *TAp WAter RAdioactivity Real Time Monitor*

Objective

The TAWARA_RTM project aims at developing a complete platform to control the quality of the tap water with respect to the radioactivity content. The platform will provide a real time measurement of the activity in the water (measuring the gross alpha and beta activity) to verify whether the distributed water is far from the limits set by the EU legislation (see Directive 98/83/CE of the European Council) reaching thresholds that require rapid actions. In case of an alarm due to an activity in the water lager than the defined thresholds, a warning message is sent to the water plant management to verify the need of stopping the water distribution. At the same time, a second part of the system is activated, to determine the nature of the contamination by gamma ray spectroscopy, defining the nature of the contamination and the corresponding counter-measures. Moreover, the determination of the contaminants is needed to establish the effects on the population and produce a full information report to the Civil Security Authorities. The prototypes of a real time monitoring system and spectroscopy analyser will be designed, built, tested under laboratory condition and finally installed at the water plant in the North Waterworks Plant [Zakład Wodociągu Północnego] of Warsaw managed by the Warsaw Waterwork Company (Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A. – MPWIK), for the demonstration campaign. The site selected for the demonstration is particularly problematic for possible radioactivity contamination being communicating through the network of rivers and canals with the Chernobyl region and being close to a Polish National Nuclear Waste storage site. The TAWARA_RTM project will include the development of the complete platform including the fast Real-Time Monitor system (RTM), the Spectroscopic system (SPEC) as well as the Information and Communication System that will be designed to include in future also chemical and biological sensors.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Università degli Studi di Padova**	**UNIPD**	Italy
2	Università degli Studi di Pisa	UNIPI	Italy
3	Naradowe Centrum Badan Jadrowich	NCBJ	Poland
4	Miejskie Przedsiebiorstwo Wodociagow i Kanalizacji W M. St. Warszawie Spolka Akcyjna	NPWIK	Poland
5	Wardynski i Wspolnicy Spk	WARDYNSKI	Poland
6	Scionix Holland Bv	SCIONIX	Netherlands
7	Costruzioni Apparecchiature Elettroniche Nucleari – C.A.E.N. Spa	CAEN	Italy
8	Agenzia Nazionale per le Nuove Tecnologie, l'Energia e lo Sviluppo Economico Sostenibile	ENEA	Italy

TRITON / *Trusted Vessel Information from Trusted On-board Instrumentation*

Objective

A new consciousness has arisen in the scenario of civilian and commercial maritime control: surveillance and safety systems may be under the attack of intentional or unintentional or malevolent players, whose aim (or effect) is to bypass or mystify the control system to obtain economic gain. The advances of mass-price technology, easily sold over the Internet, make this kind of potential events a serious threat that the maritime control has to cope with.

TRITON (TRusted vessel Information from Trusted On-board iNstrumentation) is an R&D project that gives some of the possible answers to the threats above, focusing on increasing the trustworthiness of on-board instrumentation used to report vessel information to the control organisms. Today's maritime surveillance operations rely on ship reporting systems such as AIS (Automatic Identification System), LRIT (Long Range Identification and Tracking) and VMS (Vessel Monitoring System), whose reported data (such as vessel ID, accurate position and time, course over ground, speed over ground, heading, rate of turn, etc.) are typically not verified nor validated in any way.

Acknowledging the primary role of GNSS to support these reporting systems, a first objective of the TRITON project is to provide to the on-board unit a "trusted" GNSS-based source of positioning and timing information, robust to some intentional jamming and spoofing attacks. A second objective is to provide to the on-board unit a robust communication transceiver, featuring methods for overcoming the present limitations of the communication standards in maritime field, exploiting UHF "white spaces".

At the end of the project, a proof of concept of the proposed technological solutions will be given in a prototype and appropriate test suites. On top of this, a clear understanding of residual threats will result, based on a comprehensive analysis pursued under different viewpoints: technological, cost-benefits and regulatory.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Istituto Superiore Mario Boella sulle Tecnologie dell'Informazione e delle Telecomunicazioni**	**ISMB**	Italy
2	71 Group Ab	71 GROUP	Sweden
3	Granturco and Partners Sprl	GRANTURCO	Belgium
4	Kongsberg Norcontrol It As	KONGSBERG	Norway
5	Alpha Consultants Srl	ALPHA STUDIO	Italy
6	Acorde Technologies SA	ACORDE	Spain

NESSoS / *The Network of Excellence on Engineering Secure Future Internet Software Services and Systems*

Info

Call:	FP7 ICT Call 5
Total cost:	5,000,000 €
EU funding:	3,800,000 €

Total cost of the project and co-financing from the EU to the Italian partnership involved in this project:

Total cost for Italy:	1,300,000 €
EU funding for Italy:	1,000,000 €
Website:	http://www.nessos-project.eu

Abstract

"The **N**etwork of **E**xcellence on Engineering **S**ecure Future Internet **So**ftware **S**ervices and Systems (NESSoS) aims at constituting and integrating a **long lasting research community on engineering secure software-based services and systems**.

The NESSoS engineering of secure software services is based on the principle of addressing security concerns from the very beginning in system analysis and design, thus contributing to reduce the amount of system and service vulnerabilities and enabling the systematic treatment of security needs through the engineering process. In light of the unique security requirements the Future Internet will expose, new results will be achieved by means of an integrated research, as to improve the necessary assurance level and to address risk and cost during the software development cycle in order to prioritize and manage investments. NESSoS will integrate the research labs involved; NESSoS will re-address, integrate, harmonize and foster the research activities in the necessary areas, and will increase and spread the research excellence. NESSoS will also impact training and education activities in Europe to grow a new generation of skilled researchers and practitioners in the area. NESSoS will collaborate with industrial stakeholders to improve the industry best practices and support a rapid growth of software based service systems in the Future Internet.

The research excellence of NESSoS will contribute to increase the trustworthiness of the Future Internet by improving the overall security of software services and systems. This will support European competitiveness in this vital area.

Main technological and scientific outcomes

The scientific and technical objectives of NESSoS project are:

1. The creation of a long lasting research community on engineering secure software based service systems with more than 300 researchers;
2. The creation of a common body of knowledge with more than 170 Knowledge objects (www.nessos-project.eu/cbk):
3. The integration of research agendas and the creation of the NESSoS research Roadmap on Secure Future Internet, that has been considered as the basis of the coming EU Public/Private Cooperation on Network and Information Security (NIS);
4. The integration of infrastructures, tools and methodologies in a common Service Development Environment (www.nessos-project.eu/sde) with more than 20 tools integrated and open to the community;
5. The contribution to education, dissemination and spreading of excellence with the publication of more than 300 research papers in 3 years.

Products/Operational Prototypes validated by End-users

One of the main products of a Network of Excellence as NESSoS is the creation of the research roadmap in the area that the network is addressing. Thus, one of the main products of NESSoS is its research Roadmap. The end-users of this roadmap include at least researchers and policy makers.

The topics identified in the NESSoS research roadmap have been also useful to drive some of the topics of the next calls in H2020, in particular in the Challenge 7 and the NESSoS research community increased from 50 researchers to 300. Thus we believe we were able to attract the interest and attention of both classes of end-users.

Follow-up

The NESSoS research community already created a world-wide WG on Secure Service Engineering as Technical WG (11.14) of the International Federation of Information Processing (IFIP). We do plan to foster all the NESSoS initiatives as community.

New technological, scientific or application perspective opened by the project

The research topics and the research community are perfectly aligned with the new challenges identified by the research community, as risk management and assurance as well as security and privacy by design. The research partners are committed to increase the research activities/results/products in these areas and related.

Socio-economic aspects to be developed

One of the main elements of the NESSoS proposal was to reduce the gap between industry best-practices and academic research. The project partially achieved this goal and the community plans to increase the efforts, in particular in relation to the proposed EU cybersecurity directive that will increase the attention on cybersecurity aspects in industries/organizations and in the society at large in general.

Partners

Part. no.	Beneficiary name	Part. short name	Country
1 (Coordinator)	**Istituto di Informatica e Telematica – CNR**	**IIT-CNR**	Italy
2	ATOS S.A.E	ATOS	Spain
3	Eidgenössische Technische Hochschule Zürich	ETHZ	Switzerland
4	Fundacion IMDEA Software	IMDEA	Spain
5	Institut National de Recherche en Informatique et en Automatique	INRIA	France
6	Katholieke Universiteit Leuven	KU Leuven	Belgium
7	Ludwig-Maximilians-Universität München	LMU	Germany
8	Siemens AG	Siemens AG	Germany
9	Stiftelsen Sintef	SINTEF	Norway
10	University Duisburg-Essen	UNI-DUE	Germany
11	Universidad de Malaga	UMA	Spain
12	Università degli studi di Trento	UNITN	Italy

NOTES

SEcurity Research in ITaly vol. 4 has been partially funded by

The book cover has been created for SERIT by Francesco Gianetti.

All the pictures in this book have been bought from the image archive

www.fotolia.com

Finito di stampare a febbraio 2014 a Cascina presso Stylgrafica Cascinese

ISBN 9788890547058