

# PROJECT FINAL REPORT

**Grant Agreement number:** 225353

**Project acronym:** MICIE

**Project title:** Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures

**Funding Scheme:** STREP

**Period covered:** from 1-9-2008 to 28-2-2011

**Name of the scientific representative of the project's co-ordinator<sup>1</sup>, Title and Organisation:**

Paolo Capodiecì – Selex Communications S.p.A.

**Tel:**+ 3906 9185 2631

**Fax:**+ 3906 9185 23 89

**E-mail:** paolo.capodiecì@selex-comms.com

**Project website address:** www.micie.eu

---

<sup>1</sup> Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

## CONTENTS

<b>1</b>	<b>PUBLISHABLE SUMMARY .....</b>	<b>3</b>
1.1	EXECUTIVE SUMMARY .....	3
1.2	PROJECT CONTEXT AND OBJECTIVES.....	4
1.3	MAIN S&T RESULTS/FOREGROUNDS.....	6
1.4	THE POTENTIAL IMPACT .....	21
1.4.1	<i>Socio-economic impact and the wider societal.....</i>	<i>21</i>
1.4.2	<i>Dissemination activities and exploitation .....</i>	<i>22</i>
1.5	PROJECT DATA.....	33
<b>2</b>	<b>USE AND DISSEMINATION OF FOREGROUND .....</b>	<b>34</b>
2.1	SECTION A (PUBLIC).....	34
2.2	SECTION B (CONFIDENTIAL OR PUBLIC: CONFIDENTIAL INFORMATION TO BE MARKED CLEARLY) .....	44
2.2.1	<i>Part B1 .....</i>	<i>44</i>
2.2.2	<i>Part B2 .....</i>	<i>46</i>
<b>3</b>	<b>REPORT ON SOCIETAL IMPLICATIONS.....</b>	<b>47</b>

## 1 PUBLISHABLE SUMMARY

### 1.1 Executive summary

The MICIE project has developed and validated a so-called "*MICIE alerting system*" able to identify, 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, and yellow, orange and red).

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

The CI model make use of hierarchical modeling in order to evaluate the "level of interdependency" existing among the different CIs, which are characterized through proper "thresholds" values. The CI model also includes the identification and the formalization of proper "metadata" suitable for describing the CI status, according to a "CI independent" approach which, as far as possible, leaves out of consideration the CI peculiarities.

The MICIE alerting system also includes a proper discovery, communication and composition infrastructure able to operate in an heterogeneous CI framework, aiming at discovering the "useful" data in the different CIs, at translating them in CI-independent metadata, at transporting them via a secure and available communication network and at aggregating them by means of properly defined composition rules.

The main activities of MICIE project have been:

1. Design and analysis of qualitative and quantitative interdependency metrics and indicators accounting the service continuity and data integrity of the ICT infrastructure of the CIs;
2. Design and analysis of a hierarchical modeling framework for interdependency analysis based on the integration of heterogeneous modeling techniques;
3. Development of an on-line (real-time) "cascade failure induced" alarm level predictor able to provide a qualitative indication of the actual level of exposure to cascade failure;
4. Design of a suitable communication system able to assure availability, authenticity, integrity, of metadata exchanged;
5. Validation of the interdependency alarm -predictor system on the infrastructure of an Electric Company, Israel Electric Corp.

## 1.2 Project Context and Objectives

The term “Critical Infrastructures” (CI) relates to “*those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, and security, economic or social well-being of people*”.

CI can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activities and malicious behaviors. To save the lives and property of people at risk in the EU from terrorism, natural disasters and accidents, any disruptions or manipulations of CI should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union.

The damage or loss of a piece of infrastructure in one EU State may have negative effects on several others and on the European economy as a whole. This is becoming increasingly likely as new technologies diffusion (e.g. the Internet) implies that much of infrastructure’s controlling CIs are part of a larger network. In this sense Critical infrastructure sectors do not exist alone but interact each other. Such a situation means that CI protection must be addressed in cross sector (and cross border) view. Interdependencies between CIs imply that an impact (e.g. an undesired event) occurring on one infrastructure results also in an impact on one or more other interdependent infrastructures.

Improving the security of European CIs has become a top priority. Significant actions are underway to assess and reduce vulnerabilities to potential terrorist attacks or weather disasters, to plan for and practice response to emergencies and incidents and to develop new security technologies to detect security breaches.

In normal working condition each CI provides a set of services with a target Quality of Service (target QoS) (e.g. expressed in terms of continuity/readiness of service, integrity of data, etc), i.e. the QoS matching the requirements of the CI users. In a given CI the provision of such target QoS can be threatened by the occurrence of undesired events (e.g. failures, incidents, terrorist attacks) happening either in the reference CI, or in other CIs which are interdependent with the reference one.

In this respect, MICIE project aims to improve the CI Protection capability (in Europe) through the design and implementation of a MICIE alerting system that identifies, in real time, the level of possible threats induced on a given CI by undesired events happened in the reference CI and/or in other CIs which are interdependent with the reference CI.

MICIE solution is in line with the initiative to establish EU level framework (EPCIP) for the protection of Critical Infrastructure in Europe, and with the set-up of a Critical Infrastructure Warning Information Network (CIWIN in response to the need to increase the Critical Infrastructure Protection capability in Europe).

The above-mentioned threats will be expressed in terms of risk level for a given CI of being no more able of providing its services with its target QoS in consequence of some events happening in other CIs; such a risk level will be hereinafter referred to as CI risk level. So, the MICIE alerting system will be able to provide, in real time, each CI operator with a CI risk level measuring the probability that, in the near future, he will no more be 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.

The MICIE alerting system will compute, in real time, the CI risk levels on the basis of designed CI models (taking into account indicators of the mutual interdependency among CIs, as well as threshold values for such indicators) and of a suitable set of metadata (reporting in a properly aggregated way the status of the interdependent CIs) which are used as inputs of the above-mentioned CI models.

The MICIE alerting system is based on the following subsystems:

1. The **off-line design of CI models** able to "catch" the dominant dynamics deriving from the occurrence of undesired events. The definition of such CI models will include:
  - I. the identification of key semantics elements for the description of the CI status which are common to heterogeneous CIs; these common semantic elements will be organized in metadata, hereinafter referred to as CI independent metadata, described through ontology based formal languages. These elements will include qualitative and quantitative metrics and indicators accounting for the QoS (e.g. expressed in terms of service continuity and data integrity) experienced in the CIs;
  - II. the definition of a hierarchical modeling framework for off-line interdependency analysis based on the integration of heterogeneous modeling techniques (i.e. continuous versus discrete, stochastic versus deterministic, simulation versus analytical approach). This framework will be used in order to identify the level of interdependency existing among the different CIs; such level of interdependency will be characterized by mean of proper "thresholds" values.
2. The **MICIE Secure Mediation Gateways** having the following roles:
  - I. collecting of the "sensible" CI-specific data in the various CIs (i.e. the alarms data of undesired event happening in the CIs),
  - II. "translation" of such CI-specific data in CI independent metadata according to the selected ontology based formal language,
  - III. mutual exchange of these metadata on secure ICT links,
  - IV. composition of the metadata received by different MICIE Gateways in aggregated metadata by means of properly defined composition rules.
3. The **MICIE on-line risk prediction tool** which, on the grounds of the CI models mentioned in the issue (1) and of the aggregated metadata mentioned in the issue (2) (these last are used as inputs of the CI models), is able to predict, in real time, the CI risk levels.

To achieve the general objectives, the MICIE project has pursued the following three innovative specific scientific and technological objectives:

1. Designing CI modeling techniques in order to model the effects of undesired events happening in a given CI on the QoS of the services provided both by the CI in question and by the interdependent CIs. In particular, CI modeling includes the identification of key CI interdependency indicators accounting for the mutual interdependencies among CIs.
2. Designing and implementing an infrastructure for Secure Cross CIs' Information sharing and mediation. Such infrastructure includes the design and prototype of proper MICIE Secure Mediation Gateways able to collect sensible CI-specific data in the associated CIs, to translate them in CI independent metadata, to exchange these metadata on secure ICT links and to aggregate such metadata according to proper composition rules.
3. Designing and implementing a MICIE on-line risk prediction tool which encompasses the CI modeling techniques mentioned in issue (1) and makes use, as key inputs, of the metadata mentioned in issue (2).

### 1.3 Main S&T results/foregrounds

The MICIE project has achieved all the Scientific & Technological target objectives established at begin of the activities.

As main results, based on the test and validation activities carried out at IEC facilities we can state that MICIE system is a powerful tools able to assist the CI operator to reduce considerably the risk of failure in the network associate to events induced by interconnected CIs.

In quantitative terms we can estimate that the use of MICIE tool reduces the outage time on a electric distribution network of about the 2%. It will be possible to estimate some economic values after analyzing the communication faults events and their influence on the QoS of the electric energy supply, but it is clear now that the use of MICIE tool could increase the QoS of supplying of the electrical energy and improve the Service Level Agreement (SLA) between the energy producers and customers. The first results of the duration of the power unsupplied period without MICIE tool and using the MICIE tool are provided in the table xx. The table presents the comparison of outage duration ( $t_n$ ) in case of communication failure, where  $t_n = \sum(\text{Unsupplied KVA} * \text{Duration}) / \text{Installed KVA}$ .

STEP	Unsupplied KVA	Duration [min]		MICIE Tool	
		Communication O.K.	Communication failure	Unsupplied KVA	Duration
0	39000	5	90	39000	5
1	36800	1	20	36800	1
2	19300	1	30	19300	1
3	15700	1	10	Not counted	1
4	13700	1	10	17300	1
5	13200	1	5	16800	1
6	Not counted - less than 1 minutes				
7	6400	148	148	10000	148
8	1300	176	176	4900	176
$t_n$		37.7	163.1	3600	67.4

Table. Comparison of outage duration ( $t_n$ ) in case of communication failure

The Table demonstrates that in presence of the same communication failure, the use of MICIE tool provides to the operator the possibility to disconnect the energy source that has a risk of communication failure and to provide power supply (from step1) from the alternative energy source. This decision significantly reduces the outage duration ( $t_n$ ) for most of the customers, leaving unsupplied just a small part of them (in our case only one). This operation permits to increase the QoS of energy supply to the customers.

The use of the MICIE tool could improve the following procedures:

- Protect Energy and Communication CIs
- Decrease uncertainty while operating the CI
- Reduce time of service restoration
- Support on-line decision making to predict cascade failure
- SLA improvement based on analysis of highly risk potential outages of the CIs

With regards to the S&T objectives of the project, in line with the target objectives of the ICT-SEC Call, the main results are indicated in the following.

***1. Addressing technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures;***

*MICIE project developed a communication framework based on a number of Secure Mediation Gateways linking different Critical Infrastructures. Such a communication framework has been designed on the basis of a set of security requirements identified applying a risk analysis approach. Thus, we can state that the Secure Mediation Gateway developed in the MICIE project can be used*

in order to enable CIs to share information among them in a secure way. For more information, please refer to MICIE Deliverable D4.2.2 “Secure Mediation Gateway architecture – final version”.

## **2. Guarantee integrity of data and continuous provision of responsive and trustworthy services, and support dynamically varying trust requirements;**

MICIE infrastructure has been designed considering all the security aspects required by the CI communication system (i.e., integrity and non-repudiation of data, continuity of the service, etc.). A specific task (Task 4001) has been dedicated to analyse security requirements that the MICIE system has to guarantee, and security requirements have been identified using a risk analysis approach, on the basis of Common Criteria defined in ISO/IEC 15408. In particular, the communication system developed in the MICIE system to interconnect different CIs provides data availability (A), integrity (I) and confidentiality (C). For more information, please refer to MICIE Deliverable D4.1.2 “ICT system requirements – final version” containing a complete protection profile and Deliverable D4.2.2 “Secure Mediation Gateway architecture – final version” containing the updated security requirement, and the poster session of the conference SRC’2010 byitrust.

## **3. Understanding and managing the interactions and complexity of interdependent critical infrastructures;**

MICIE has developed a framework for interdependency modelling based on the integration of heterogeneous modelling techniques. In deliverable D2.1.1 a reference scenario has been identified. It consists in the identification of services, sequences of adverse events that could impair the quality of such services (in terms of continuity, readiness, performances, time response) and interconnected networks supporting such services (in terms of topologies, essential systems (i.e. Telco emergency power supply, cooling systems), interconnections among networks and systems. A first set of services supplied from the CI, under consideration, has been identified, trying to reveal interdependencies, and thus opening the way to cascading failures and escalation effects.

Deliverable D2.2.1 describes the formalisms of the heterogeneous modelling framework, the modelling process to build models representing the reference scenario and the interdependency indicators. Heterogeneous (stochastic versus deterministic, agent based, dynamic simulation) models are under development to perform short term predictions of the QoS of the CIs according to the services, the interconnected networks and the undesired events identified in the reference Scenario. We refer to the Power Grid Isolation and Reconfiguration Service (FISR) that is performed by SCADA operator, by means of SCADA system and depends upon SCADA dependability, security and performances. FISR detects and isolates outages then restores the grid in order to power again its customers. The aim is to investigate quantitative relationships between the Quality of Services provided by SCADA operator and the quality of power supply provided by the power grid operator to power grid customers. The deliverable describes the first heterogeneous models on which predict short term indicators of the QoS of FISR (ie. service connectivity, reliability, rerouting, time response, operability level).

Within D2.2.2, Reliability indicators of the power grid, indicators of Quality of power supply to customers, performance and dependability indicators of FISR service (time response, dynamical path, connectivity, reliability and availability) have been investigated. The on line version of FISR model implemented by RAO simulator has been implemented. A model to compute security attributes (in terms of confidentiality, integrity and availability) of services is presented according to a high level view of infrastructures’ services. Probability of loss of a service on occurrence of specific

events have been investigated by Bayesian belief networks. Comparison criteria of modelling methodologies versus the on line risk prediction tool and hints to its development have been individuated

The deliverable D2.1.2 “ CI Reference Scenario and service oriented approach – final report ” completes the gathering and understanding of information, data, interconnected networks, interconnections among networks and procedures described in previous deliverable D2.1.1 “ CI Reference Scenario and service oriented approach – interim report ” . Here, the major effort has been spent on the Telco network and procedures to be performed by the operator of the Telco Control Centre in normal service operation, incident, emergency and crisis situations.

The deliverable D2.2.2 regards heterogeneous models refinement. Several aspects have been taken into account: a) demonstration of traceability of models against the reference scenario and reference networks currently available; b) careful identification of actual model inputs and outputs; c) clear identification of model expected outputs; d) real time capability of models to assist on line SCADA and NMS operators. Particularly, models afford the quality of the service to grid customers related to the risk of loss/degradation of Fault Isolation and System Restoration (FISR) service, including security aspects, as a benchmark for the various modelling approaches.

In deliverable D2.2.3 the refinement of models has mainly consisted: a) in implementing Dynamic Bayesian Belief Networks (DBNs) to take time into account; b) in “Deterministic and agent based simulation”. A specific test has been run. Demonstrations of running on line model have been performed; c) RESCI-MONITOR (Real-time Evaluation of Security – MONITOR) has been improved. Demonstrations of running on line model have been performed; d) Refinements of NS2 models to performs QoS computation of FISR service, in terms of reliability indexes (S-T connectivity: minpaths, mincuts and reliability), performances indexes (time response, % of affected customers, RTT and dynamical paths). Demonstrations of running model have been performed. Cf. paper at CRITIS 2010.

#### **4. Preventing against cascading effects;**

MICIE addressed the problem of cascading effects defining an on line tool for their prediction based on cross sector exchange of CIs’ status metadata.(cfr document deliverable D 3.2.2 D6.3)

#### **5. Providing recovery and continuity in critical scenarios (including research towards designing and building self-adapted and self-healing complex systems)**

MICIE addressed this topic providing a tool to increase situation awareness. This has been used as building block for the implementation of a complete autonomic control system able to detect crisis situations, plan and enforce countermeasures. (cfr document deliverable D3.2.2 , D 6.3.)

#### **6. Security and dependability metrics and assurance methods for quantifying infrastructure interdependencies;**

MICIE investigated qualitative and quantitative interdependency indicators. They take into account the service continuity and data integrity of the ICT infrastructure of the CIs and the impact of such attributes on the delivery of service of any other cross-domain infrastructure. Within D2.2.1, D2.2.2, D2.2.3, Reliability indicators of the power grid, indicators of Quality of power supply to customers, performance and dependability indicators of FISR service (time response, dynamical path, connectivity, reliability and availability) have been investigated. Such indicators have been

computed within the different heterogeneous modelling approaches of WP2000: Dynamic Bayesian Belief Networks which take time into account, Deterministic and agent based simulation, RESCI-MONITOR for real-time evaluation of security, Performance and rerouting NS2 models, Network reliability models. Such models perform, even in real time, QoS computation of FISR service, in terms of reliability indexes (S-T connectivity: minpaths, mincuts and reliability), performances indexes (time response, % of affected customers, RTT and dynamical paths), security attributes (in terms of confidentiality, integrity and availability) of services and the probability of loss of a service on occurrence of specific events.

### **7. Designing and developing secure and resilient networked and distributed information system**

MICIE designed a secure and resilient infrastructure for the mediation and the exchange of metadata among different Critical Infrastructures. All the CIs had the possibility to be interconnected to that infrastructure thanks to the MICIE Secure Mediation Gateway. Moreover the common semantic designed to describe metadata foster the cooperation between different CI security systems. For more information, please refer to MICIE Deliverable D4.2.2 “Secure Mediation Gateway architecture – final version”.

### **8. Provide automatic mechanisms for automatic risk detection;**

The MICIE on-line prediction tool provides pre-emptive evaluations about the possible effects of dangerous interdependencies in order to alert CI operators. Specifically, the 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.(cfr document deliverable D3.2.2 D 6.3)

More specifically the results on the three main project's activities are explained in the following

1. Modeling techniques and Interdependency Indicators
2. On-line risk prediction tool
3. Secure Cross CIs' Information sharing and mediation

#### **ACTIVITY 1: Modeling techniques and Interdependency Indicators**

Heterogeneous (stochastic versus deterministic, agent based, dynamic simulation, etc.) models are under development, with the aim of investigating the short term prediction of the Quality of Services (QoS) delivered by different Critical Infrastructures. Models are based on the underlying interconnected networks that cooperate for service delivery and on possible undesired events ( i.e. attacks to the most critical elements, sequences of realistic failures, and congestions and consequences of rerouting policies of communication networks). We investigated how a possible degradation of the QoS of SCADA (expressed in

terms service connectivity, reliability, rerouting, time response, operability level) affects the quality of power supply provided by the power grid operator to power grid customers (expressed in terms of duration and number of interruptions). Within this aim, the Power Grid Fault Isolation and Reconfiguration Service (FISR), performed by SCADA, throughout its operator, is a particularly critical service. FISR detects and isolates grid outages, then restores the grid in order to re-energize grid customers. The interconnected networks, which underline the delivery of FISR service (SCADA system, Telecommunication network and power distribution grid) have been identified (in terms of topologies, functionalities, performances, rerouting and failure behaviors, interconnections at physical, geographic and logical layers) and represented with multiple techniques, tools and models: Dynamic Bayesian Belief Networks which take time into account (GENIE tool), Deterministic and agent based simulation (RAO simulator), real-time evaluation of security (RESCI-MONITOR), Discrete event simulation for performance and rerouting techniques (NS2open source platform), Network reliability analysis (NRA,WNRA). Such models perform, even in real time, QoS computation of FISR service, in terms of reliability indexes (S-T connectivity: minpaths, mincuts and reliability), performances indexes (time response, % of affected customers, RTT and dynamical paths), security attributes (in terms of confidentiality, integrity and availability) of services and the probability of loss of a service on occurrence of specific events. The aim is the short term prediction of QoS of FISR by means of its static and dynamic indicators, computed under normal and critical operation (when possible undesired events occur). Static QoS indicators, such as connectivity and availability, depend upon failure and repair behavior of networks elements. They are computed by means of analytical methods (we resort to the Weighted Network Reliability Analyzer, an Academic tool) and by the integration of the different topologies in a simulative perspective; a close cooperation with the stakeholders and experts has been required in order to provide a unitary vision of the overall System of Systems. Dynamic QoS indicators, such as packet round trip time, node throughput and packet dynamical paths, node operability level, depend upon network congestion and routing policies other than on failure and repair activities. They are computed by simulation schemas (we adopted, among the others, RAO and NS2 network simulators).

SCADA system, MV power grid and Telco network constitute a single heterogeneous network that supports FISR service, as shown in figure.

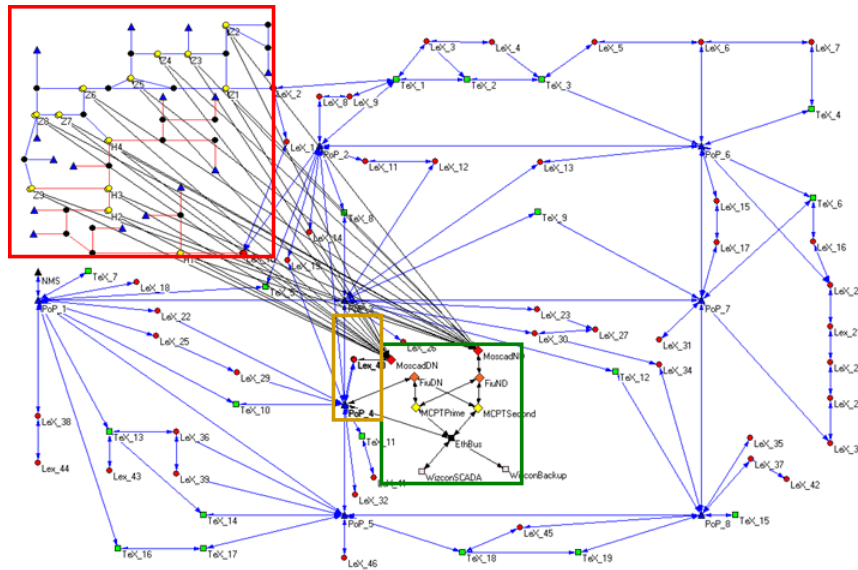
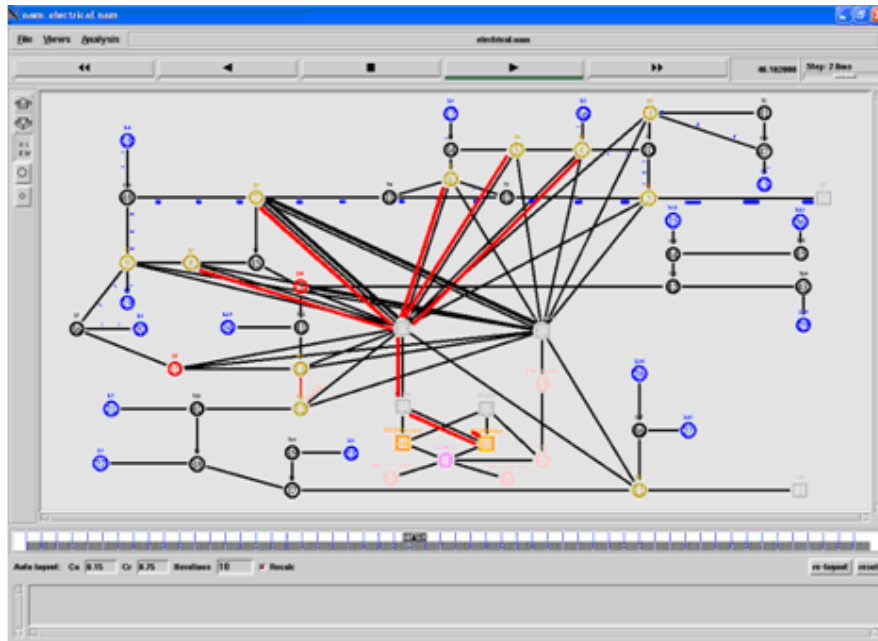


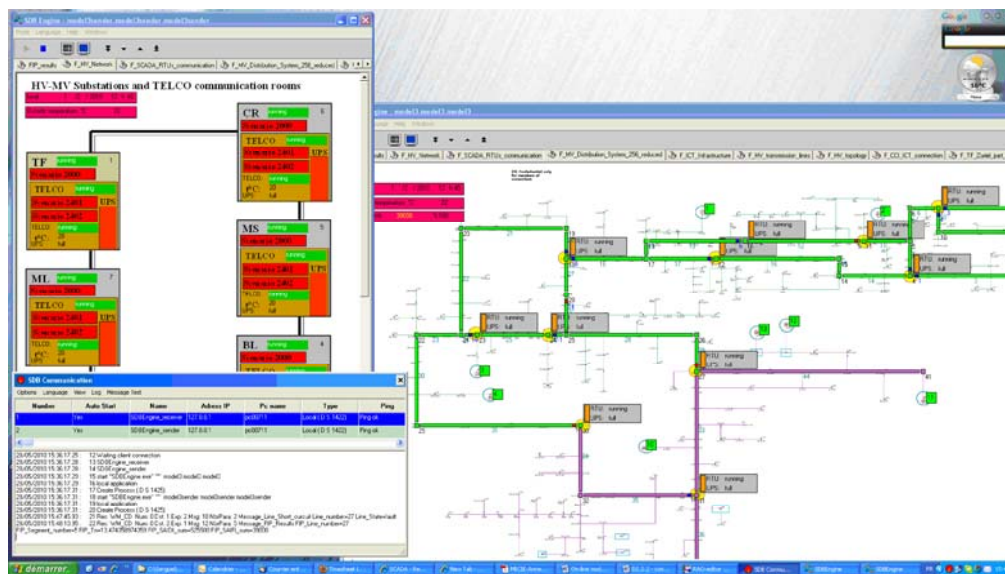
Figure below shows a snapshot of the NS2 model of interconnected networks used to investigate rerouting and performance indicators of FISR.



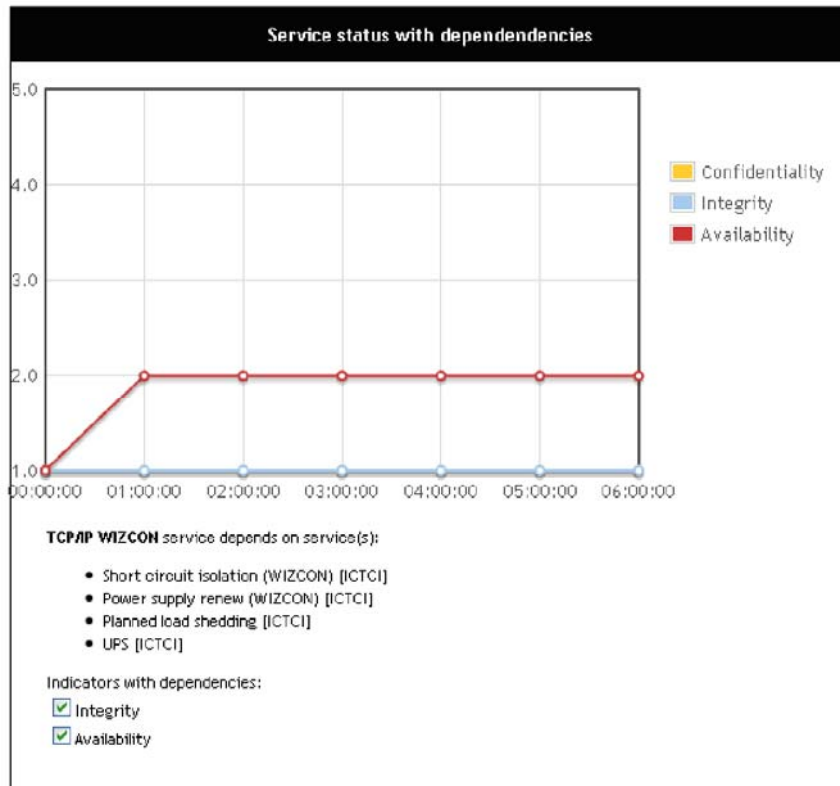
The Static and Dynamic indicators are then composed to compute the response time of Fault Isolation and System Restoration (FISR) service. Widely adopted reliability indices for power distribution grids, such as CAIDI

(Customer Average Interruption Duration), SAIDI (System Average Interruption Duration) and SAIFI (System Average frequency Interruption), are used to quantify the impact of the QoS of FISR on the Quality of Service of the Power grid supply to utility customers.

A model of the three interdependent CIs using RAO simulator (presented in D2.2.1) has been started in a way to get at the end a unique model with interdependencies included. The model will reproduce the behavior of each CI (electricity distribution, communication and SCADA) as well as behavior arising from the CIs interdependencies. So the model will be able to simulate various reference scenarios and to estimate the influence of CIs parameters and interdependency factors on the important indicators of quality of service for customers, contributing to estimate risks.



In security models, for each service, their dependencies are expressed in terms of confidentiality, integrity and availability. Metrics and underlined measures for each attribute are identified.



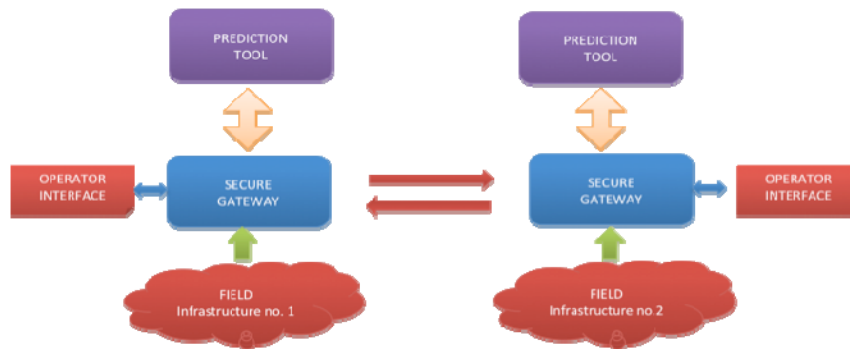
## ACTIVITY 2: On-line risk prediction tool

One of the outputs of MICIE project is a prototyped tool able to predict, in a distributed way, the state of some services related to two or more interconnected infrastructures. Such forecast will have a deep impact on the management of each infrastructure due to the new capabilities available to the operators of each control room. Capabilities related to a better real-time understanding of crisis scenarios in which will be clear, to all involved people, what is going to happen and what is possible to do with available systems. It is clear that, to have a reasonable emergency management improvement, a real enhancement with respect to a standard isolated scenario, some data has to be exchanged between control rooms.

Obviously, the tool inside each infrastructure directly receives only the data originated within its infrastructure. Fortunately, the different tools will be interconnected. Now, the main issue is the synchronization of such tools to guarantee a consistent global awareness.

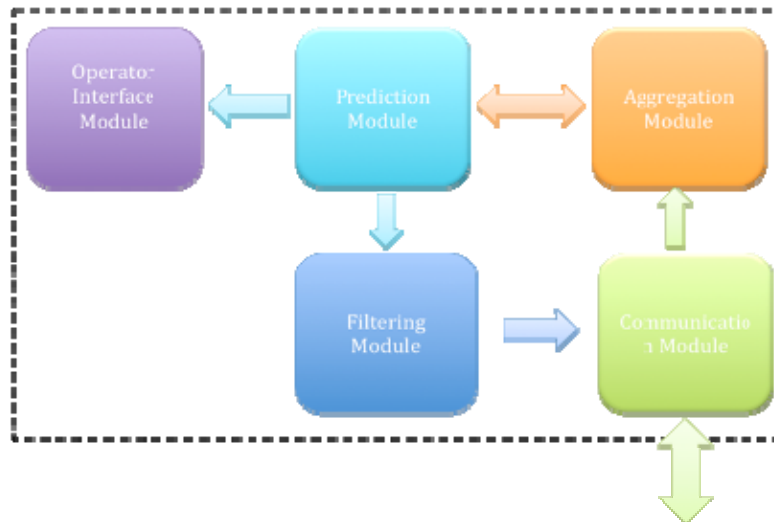
In our view, the easiest way to grant the consistency of the overall state estimated by the different distributed tools is to equip every system with a common general model, even if every specific domain receives only a subset of the inputs. Hence, we propose that each tool has exactly the same model of the overall system of systems (see Figure 1).

The more general problem that arises is, hence, the synchronization of multiple distributed tools, with a common model of the interdependencies existing among CIs and their elements, in presence of different inputs coming from the field and with the possibility of exchanging only a subset of the whole state.



**Figure 1 MICIE Online Tool Architecture**

The core of the whole system is the MHR Prediction Tool, whose architecture is presented on Fig.2.



**Fig. 2 Prediction Tool Architecture Overview**

The MHR Prediction Tool is composed of five interrelated modules, each devoted to a specific task:

- Prediction Module produces a new prediction;
- Aggregation Module aggregates the predictions coming from other tools, the data coming from the field and the last local prediction, in order to provide an updated input for the prediction module;
- Filtering Module filters the updated prediction provided by the prediction module, exposing to the Secure Mediation Gateway only the Quality of Services;
- Communication Module interfaces with the Secure mediation gateway;
- Operator Interface Module shows operators the prediction provided by the prediction module in an easily understandable view.

The Prediction Module is the core of the whole Prediction Tool. It is based on the MHR-CISIA simulator, which is able to provide a prediction on the future state of the whole system of systems. To this end the simulator requires an input XML file containing the initial condition of each entity and Service.

In order to use this simulator in an online framework, there is the need to update such an input file based on the data coming from other PTs and from the field.

The Aggregation Module is the software module devoted to merge the different data sets coming from different data sources (i.e., the other Prediction Tools and the field).

Moreover there is the need to take into account also the last output of MHR-CISIA simulator, in order to maintain a memory on the state of the entities.

The most relevant issue is how to aggregate data coming from multiple information sources; to this end two approaches can be adopted:

- Source Reliability Rating: the different information sources might be characterized by a parameter representing their reliability. This approach can be very useful to reduce the impact of unreliable data in the resulting aggregated state; however, in the case of the reference scenario analyzed, each infrastructure has an exact knowledge of negative phenomena occurring to its equipments and services, or, at least, each information provided by a Prediction Tool to the others has complete reliability if it is restricted to the subset of entities and services belonging to the infrastructure where it is attested, while in general, the information about services provided by other infrastructures is not exact, since it just represents the part of information extracted by the interdependency model when a partial set of inputs (i.e., sector specific inputs) is applied to it.
- Domain competence: each tool has maximum competence for what regards data related to such an infrastructure. In this case there is the need to provide an aggregation strategy able to privilege the sector specific information coming from local prediction module. A feasible approach, in this case, is a worst case approach, where the maximum failure and the minimum operativeness is chosen while aggregating different data sets. This criterion is not use for every parameter inside entities. Sometimes the criterion used was to give priority to the field value, such as the breaker status. Such a criterion has the property of not being dependent on the order of the aggregation.

The Filtering Module provides the data that will be forwarded to other Prediction Tools. To this end, given the updated prediction, only the quality of the services is selected.

There is also the possibility to introduce a tuning parameter in order to dynamically change the nature of the information exposed; for instance there is the possibility to exchange every piece of information in order to reconstruct exactly the state.

The Communication Module represents the actual interface of the Prediction Tool with the SMGW and then with the Adaptor and the other Prediction Tools.

The communication with other tools and the adaptor is performed by communicating with the local SMGW, which is demanded to retrieve information and provide it to the local Prediction Tool, as well as providing the updated prediction of local Prediction Tool to other remote SMGWs.

The whole communication architecture is based on the WSO2/Tomcat framework and uses web services to perform data exchange. Such an exchange can be performed both in pull and push mode.

More in detail, the communication module is composed of two software modules:

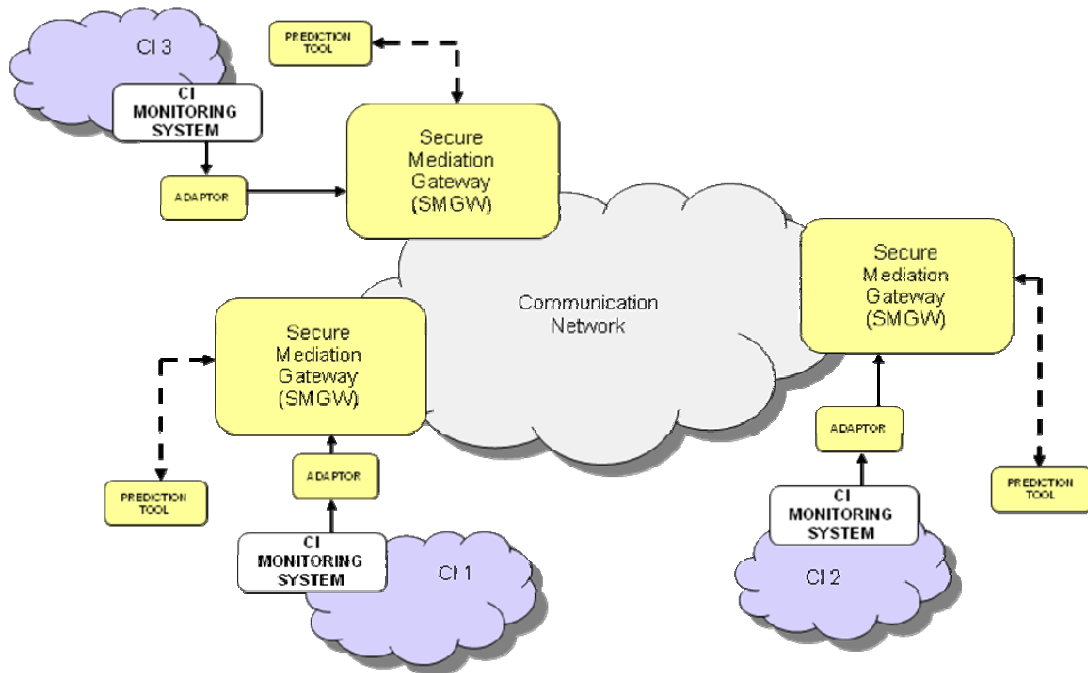
- Client: it is a Java application devoted to collect data coming from other Prediction Tools and from the adaptor. Since the SMGW is completely transparent to the Client, it can be configured as if it is directly connected to the remote Web services (in push mode).
- Output Web service: it is aimed to forward the filtered prediction to other Prediction Tools.

The operator interface module is based on IFIX SCADA system, since typically operators are confident with this kind of operator panels.

IFIX is much more than a simple graphical environment; it is a complex SCADA monitoring system able to retrieve data from the field by means of an OPC Adaptor (or other adaptors if required).

### ACTIVITY 3: Secure Cross CI's Information sharing and mediation

A communication infrastructure has been developed in the MICIE project in order to enable the information sharing among different and heterogeneous Critical Infrastructures.



In order to develop such communication infrastructure, two main technical challenges have been addressed:

1. Heterogeneity of data to be shared, related to heterogeneous CI's;
2. Security of the communication system due to the confidentiality of the information exchanged.

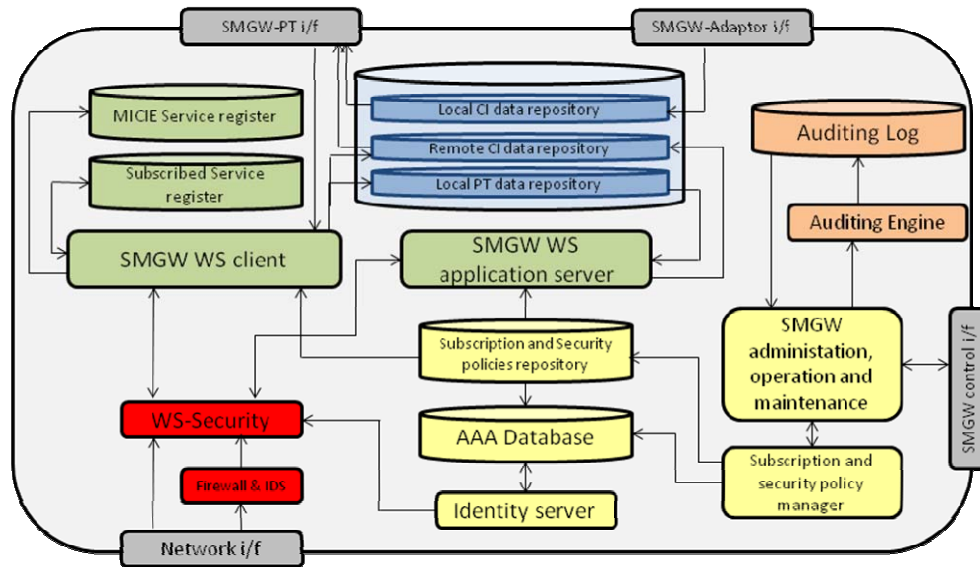
The heterogeneity of the data has been addressed by means of the introduction of an abstraction layer where a common semantic has been utilized to describe all the element and the services of the infrastructures using a uniform and common data format.

In particular, starting from the updated information about the modeling activities from WP3000, an ER schema has been designed and then translated into an OWL schema using the Protégé tool. Thus, all the data collected by each legacy CI monitoring system are translated using the defined common semantic by the so called "Adaptors", in charge also of performing data filtering.

Security of the communication system is assured by the Secure Communication Gateway, designed on the basis of security requirements identified by means of a risk analysis.

In particular, the communication system developed in the MICIE system to interconnect different CIs provides data availability (A), integrity (I) and confidentiality (C), and also non-repudiation (NR) and accountability (AC) of his origin.

The architecture of the SMGW is shown in the following figure.



Considering the importance of SMGW role in the whole system, specific attention has been devoted to how it is managed. More specifically, a Policy Based Management Architecture has been adopted. The SMGW manager graphical user interface (GUI) will allow the operator to browse through existent information and define actions that remote SMGWs can perform on them (e.g. write and/or read risk information). All data access controls are implemented with a high level of granularity thus maintaining simplicity and abstraction from equipment configuration details.

The use of policies supports definition, verification and deployment of security policies related to the information gathered by the MICIE system. For instance, those policies permit:

- the definition of how and to whom each particular piece of information can be sent;
- the definition of trust relations among different CI;
- the enforcement of different communications protocols/technologies in each particular context;
- the enforcement of service level agreements or service level specifications between CIs;
- the decision on how received events will be managed by the SMGW.

Policies are represented in a formal way and stored in a policy repository. SMGW manager interacts with other modules on the SMGW that implement policies acting as Policy Enforcement Points.

## 1.4 The potential impact

### 1.4.1 Socio-economic impact and the wider societal

MICIE has extensive innovation elements and significant potential to address a range of ambitious challenges relevant to the EU objectives on security and protection of critical infrastructures. Successful delivery of MICIE concept and objectives requires significant synergy among research organisations, industrial companies, and broadcasters across Europe. To this end, MICIE presents an excellent contribution with added value at the European level.

The need to approach at European level the protection of the Critical Infrastructures has been recognised by the Commission with the development of the EPCIP (European Program on Critical Infrastructure Protection).

One of the cornerstone elements of the EPCIP is the improvement of the cross-border cooperation among critical infrastructures of the different countries. This goal is achieved through the definition of a common framework and improving information sharing. Specifically, one of the elements foreseen by the EPCIP is the creation of an early warning network able to provide quickly information about vulnerabilities and threats that might affect the European Critical Infrastructure. This system, labelled CIWIN (Critical Infrastructure Warning Information Network), will operate as a fast response system able to improve the information sharing among Member States and with respect to the EU Commission

MICIE project will contribute to the EPCIP framework, and in particular provides a technological mean for CIP information sharing process and solutions to concretely use this information to improve their security. Indeed, MICIE is not limited to design how share information, but it emphasize an innovative use of this information that appears largely coherent with the actual requirements of CI stakeholder about information disclosure and use. However, MICIE goal is not concurrent or substitutive with respect to design of CIWIN, but it is complementary. Indeed, MICIE aims to create an on-line alarm and early warning system which provides predictive information about the potentially dangerous condition induced by an abnormal increment of interdependencies. In this way it provides information that are complementary with those delivered via CIWIN.

MICIE project shall contribute to:

- Reinforce European industry's potential to create important market opportunities and establish leadership.
- Establish, strengthen and preserve trust in the use of technologies for the protection of critical infrastructures. This includes creating sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding potential classification requirements, international co-operation needs, communication and implementation strategies etc.), in order to ensure acceptance of such technologies by relevant stakeholders.

- Significantly improve the security, performance, dependability and resilience of complex and interdependent critical infrastructures while considering as well organizational dynamics, human factors, societal issues and related legal aspects.
- Reduce pan-European damages and costs induced by cascade failure and, more in general, to failure in critical infrastructures allowing a better alerting and hence management of crisis events.
- Provide more effective protection through enhanced co-operation, coordination and focus across Europe, and contribution to the development and promotion of metrics, standards, evaluation and certification methods
- Improve the crisis management concerning the interdependent critical infrastructures by national authorities. More particularly, in the context of continuous evaluation of action plans related to national security concerns.

#### 1.4.2 Dissemination activities and exploitation

The MICIE partners have been fully committed to ensure the maximum possible exploitation of the project results. All the participating companies and organisations had the possibility to successfully carry out dissemination and exploitation activities, due to the wide networks of contacts and collaborating entities that each partner has, and due to the constant involvement in conferences, seminars, workshop, etc.

The consortium was built around a core group of industrial manufacturers, end-users and academic partners, leaders in research (modelling, nonlinear systems, simulations, network communications, networks), in services for civil protection and in commercial activities related to communication, also including not-EC partners (founded within the EC initiative).

**Dissemination work** begun at an early stage of MICIE project by building the project hallmarks — the logo, a flyer and the website. The logo was designed as suggesting the connection and interdependencies of different entities that represent a single Critical Infrastructure.

The **MICIE website** (<http://www.micie.eu>), through which general information on MICIE is made available, played a major role in the dissemination of the project activities and results. It was launched in November 2008 and continuously populated with content during the lifetime of the project. Practically every public result of the project is available at the website: the majority of peer-reviewed publications, public deliverables, brochures, MICIE workshops' programs and presentations, slides of invited talks at other events, videos, etc.

The MICIE website was also collaborative work tool: in addition to the public website, it featured a restricted access Intranet that supported collaborative work during the course of the project (documentation repositories, mailing/discussion lists, reporting tools, scheduling and registration for project meetings, etc.). In order to ensure medium/long term availability of the MICIE results, the website and its content will be kept operational until (at least) 2015.

**Peer-reviewed publications** also played an important role in the dissemination of MICIE results. A total of 26 peer-reviewed papers were already published or accepted for publication: 1 book chapter, 3 journal papers and 22 conference papers. In addition, 8 other papers are currently under review (3 journal papers, 5 conference papers) and several more papers are expected to follow in the next months. Overall, those publications cover the most relevant conferences in the area, as well as a significant part of the relevant journals (the detailed list of these publications is presented in Section 2.1). The MICIE Consortium is also evaluating the possibility of preparing a book based on the key results from the project, complemented with invited contributions from external authors.

**Exhibitions and demonstrations at large events** were also used to foster dissemination. MICIE Stands/Exhibitions were prepared for ICT'2010 (the largest ICT event during the course of the project, exceeding 5,000 participants) and the Future Internet Week 2010 (over 2,500 participants). These stands included large posters, brochures and live demonstrations of the MICIE system. A plenary presentation of the MICIE Project was made at EUTC'2010, the main networking event organized by the European Utilities Telecom Council (EUTC) and the only European event dedicated to energy & utility professionals from Europe's gas, water and electricity utilities. MICIE also participated in the 5th Edition of the European Security Research Conference (SRC'2010), a high-profile event, with two MICIE-related posters.

Three **MICIE Workshops** were organized in the course of the project (Haifa in November 2009, Luxembourg in May 2010 and Rome in February 2011). The programs for these workshops included presentations about the MICIE Project, presentations from related European projects, presentations from national and European organizations and presentations from the industry. Each workshop gathered more than 50 attendees – local industry and academia, researchers from European projects, national and European organizations – which actively participated in the discussions, providing precious feedback to the MICIE Project and valuable networking and exploitation paths that will be explored in the future. The program and the slides of the workshop presentations are available at the MICIE website.

In what concerns with **standardization activities**, MICIE partners participated in the ISO 27xxx workgroup on security, ISO 15408 workgroup on Common Criteria and the specific workgroup on ISMS applied to Critical Infrastructure and dependability concept. A number of comments were provided on the ISO 27010 standards, most of the accepted during the official ISO meeting in Redmond, November 2009.

MICIE partners also participated in the 1st Meeting of the ESCorTS Focus Group, sponsored by CEN-CENELEC and the ESCorTS Project. The objectives of this Focus Group include the survey of stakeholders' needs and best practices, in the area of SCADA security, and convergence stimulation of current standardization efforts. This meeting, as well as the discussion within the mailing list of this Focus Group, allowed MICIE to collect information and opinions on relevant standards under revision, e.g. the ISO-99.00.02 that will become IEC 62443.

The consortium also promoted greater understanding of/exposure to standardization activities, namely by contacts with entities directly or indirectly involved in standardization processes, such as CEN, CENELEC, ENISA and EUTC.

MICIE actively pursued **liaison activities** with European and national entities and working groups, such as EUTC, CEN-CENELEC, ESCorTS, ENISA, the IntelliCIS IC0806 COST Action and local initiatives on Critical Infrastructure Protection. Direct contacts were also established with many of the potential beneficiaries of MICIE outcomes, such as utilities and national bodies, as well as with other European research projects.

Broader audiences were also targeted, with a **few magazine publications** about the MICIE Project.

A detailed list of these above-mentioned dissemination activities is presented in Section 2.1. In order to support those activities, a number of **dissemination materials** were produced. Those materials included five brochures (MICIE Fact Sheet, SMGW Architecture, Risk Prediction Tool, Interdependency Modeling Tools, RESCI-MONITOR), folders to distribute documentation, three large sized posters (200x80 cm and 200x120 cm), flags with the project logo and website URL, graphical templates for MICIE presentations, etc. A CD-ROM is also being prepared, with the complete collection of public results of the project. Overall, those materials – that unified and reinforced the MICIE visual brand – helped in the dissemination of the project results.

Concerning **Exploitation** commercialisation and distribution in Europe and at world level is clearly the final intention of the consortium; this will be achieved through the involvement at different conditions of all the partners, considering that relevant technical background and know-how must be necessarily used.

Key players for exploitation will be the MICIE industrial organisations (SCOM, IEC); for both the project offspring matches the strategic business development plans, therefore it is expected that the activities of the project will directly impact on the enhancement of the core business of the industrial partners.

As concerns **Selex Communications** has identified in the international panorama the emergence of an innovative concept of Network Centric, with the goal of providing a new line of products. The interest of Selex Communications is triggered both from the market side, where there are some potential interesting

applications also in the military field, and from the technological side. The concept at the base of this new line is the development of a integrated communication system called PERSEUS (*Professional and Emergency Resilient System Enabling Ubiquitous Services*). The Secure Mediation Gateway developed in the project will be integrated as adds-on and industrialized in the PERSEUS Professional Router system, which is a Selex communication proprietary product. Then the complete MICIE tools will be proposed as a new product / system to the CI stakeholder as well as dual use in the Defence domain, after an appropriate customization.

The PERSEUS Professional Router series is a versatile and reliable IP networking solution suitable for professional applications; it is designed so as to be seamlessly deployed in any scenario to fulfill professional or infrastructural network requirements.

PERSEUS arise a complete communication system, but at the same time a modular and scalable one depending on the required applications. PERSEUS answers to the needs of who has necessity of a private network, but at the same time they must be able to get connection with public networks and services.

Selex Communication's experience in communication network for Public Safety, Defence, and Transportation allowed the creation of a solution based on international standards and an interoperable one, but at the same time characterized by specific features that make it unique.

PERSEUS main features are:

- integration of different access technology for voice and data communications, which guarantee the availability of suitable communication means for any situation
- available of broadband, fixed and wireless connections
- extreme attention to the user mobility
- secure communications and access to the network
- use of several transport technologies (backbone), integrable with already existent transport networks
- network reconfigurability, resistance of the system and its parts to problems caused by unavailability of transmission means (e.g. as when catastrophes or interferences occur, etc.)
- adaptability of the network, which automatically employs the most suitable communication technologies depending on their availability, user profile and required services
- availability of mobile infrastructures of the access networks (transportable radio base-stations) allowing a fast intervention and operation even in uncovered areas or where the traffic capacity should be increased

Distinctive system feature – making it suitable for “mission critical” applications – is the extreme resilience, that is the ability to still offer the required services (or a subset) even in emergency condition, when the public systems go down and only remain active those networks properly studied. Nevertheless the system allows using and interoperating with COTS terminals, so that its usability results extended and the cost for low-valuable users limited.

As far as Public Administration and Public Safety are concerned, PERSEUS is appropriate for applications as land control, emergency, borders control, monitoring of environmental data and traffic. In particular it is suited for mission critical / emergency operations where first responders and Emergency Medical Services are involved.

Also Defence Administration can take advantage of using PERSEUS both in the national area and abroad missions. PERSEUS subset architectures can easily be employed by companies - as extension of their private networks in order to add innovative applications and services – and in Transport environments.

On the base of internal market analysis, Selex Communications has identified in the field of CI networks, new opportunities of business, both in the civil market and in the military market, deciding therefore to start an activity of Research and Development with the purpose to widen its own portfolio products and to acquire new markets segment. Concluding, the opportunities for search, development and production of Tools for CI Protection both for the civil sector that to serve in the military is meaningful and in growth. For a manufacturing industry as Selex Communications, this represents an opportunity of growth both in economic terms and as opportunity to create new occupation in the field of high technology.

**IEC** has made significance efforts to improve the QoS in energy supply for the customers. During the last 10 years the average time of unsupplied energy to the customers was reduced from 800 minutes to 150 minutes (without LV grid). This was reached by implementation of the energy management systems on the different levels of electrical grid. The wide installation of the ICT systems causes the significant interdependencies of the Electrical CI and Communication CI.

The operator of the CI should make decision in very short period based on understanding of the current status of the CI and working procedures. This decision making process is based on the operating of the different ICT systems. The modern ICT systems are very complex and are based on different communication systems that are also based on the complex power supply infrastructure. So the failure in one of the infrastructures could dramatically influence on the quality and even on mistakes in the decision making process and on the QoS of the infrastructure.

From the other hand, the IEC communication infrastructure provides different services to the multiple applications of the company like phones, videoconferences, information systems and so on. The QoS of the Communication infrastructure depends of proactive maintenance and management while Electrical infrastructure failure. The on-line prediction tool could provide additional information of the availability of the Electrical infrastructure and could improve the decision making process of the operator of the Communication infrastructure.

IEC estimates that the on-line prediction tool like MICIE Tool could provide additional information to the electrical grid operator that could improve the quality of the decision making process and could prevent decision making mistakes during uncertain situation and in this way could increase the QoS.of power supply.

**ENEA** is mainly called upon:

- to promote and carry out basic and applied research and innovation technology activities, also through prototypes and product industrialization;
- to disseminate and transfer technologies, encouraging their use in productive and social sectors;
- to provide high-tech services, studies, tests and evaluations to both public and private bodies and enterprises;
- to collaborate with national and local administration to define research programs and manage research activities.

To these aims and in the sectors falling within its areas of competence, ENEA:

- carries out complex research, development and demonstration projects, mainly technology and engineering — based, sets up and operates major scientific apparatus;
- assesses the level of advanced technologies development, as well as their economic and social impacts, also on demand by public administrations;
- promotes collaboration with foreign bodies and institutions, also for defining technical regulations and participation to major research programs and international organizations, providing its (specific)expertise;

The Computation and Modelling unit (UTMEA-CAL) inside ENEA is in charge to carry out R&D activities on the new frontiers of modelling methods and tools for reliability/dependability evaluation, with current emphasis on modelling and analysis of large complex interconnected systems. The focus is on the investigation of risk based methodologies, qualitative and quantitative indicators, multi formalism and multi solution methods and tools for Quality of Service measures (in terms of performances, reliability and dependability) of large interconnected technological networks, including power grids and Telco networks at regional/national level. UTMEA-CAL takes part in many European Commission initiatives focused on ICT applications on energy and telecommunication sectors within the framework of Critical Information Infrastructure Protection (CIIP).

In detail, in MICIE project, the following additional results have been reached:

- raised awareness and gained knowledge on Telco network and Power grid interdependencies and on the consequent causes of possible outages
  - to be used for improving network analysis and/or developing new tools to help in an early detection of interdependency problems to limit future black-outs
  - to be used for training opportunities for researchers, utilities' technicians as well a for industry
  - for further research
- Development of advanced simulation tools that allow quantification of impact of interdependencies:

- Scenarios identified enable to demonstrate interdependencies and effectiveness of remedial actions
- High-skilled consultancy to detect interdependencies
- Training opportunities for researchers, utilities' technicians as well a for industry
- Perspectives of commercialising this software as add-on in network analysis software.

Results gained within MICIE project are very valuable for promoting and carrying out applied research and innovation technology activities. Particularly, the demonstrator of MICIE alerting system (Adaptors, secure mediation gateway and Risk prediction tool) and the demonstrators of the main models developed inside WP2000 modelling activities (Network Simulation 2 (NS2), Network analyzer (NRA, WNRA, TNRA), Deterministic and Agent Based simulation (RAO), Security Monitoring (RT-SM) models) are hosted within ENEA-UTMEA labs. The first activities to be performed are to submit the demonstrators to a deeper testing process in order to better focus on their current characteristics and possibly enhance the robustness of their behaviour. The resulted ENEA environment will be a leverage for the Italian stakeholders in electrical field (i.e. TERNA, ACEA, ENEL) and telecommunication field (i.e. Telecom Italia, Telecom Italia Mobile) for approaching the complex aspect of interdependency among such sectors, in terms of better comprehension, representation and investigation on how they can impact on service delivery.

MICIE results will also be disseminated and the used technologies will be transferred, encouraging their use in other productive and social sectors.

For **ROMA TRE** the project was the opportunity to acquire more practical experience with a real scenario and to master the CISIA Simulator and MHR modelling methodology. The increased interest on the topic of Critical Infrastructure Protection is expected to foster the demand for better simulation and real time estimation software, and CISIA/MHR are expected to play a crucial role in this field.

Moreover thanks to the experience obtained by MICIE project, new fields of research are now open and seem very promising; among the others:

- **Using SCADA systems to represent Risk levels:** one of the key aspects of the MICIE Prediction Tool was the adoption of a SCADA software such as IFIX to present to the operators the informations obtained by the exchange of data among infrastructures. For instance it was possible to show, besides the actual level of failure, some indicators on the expected failure in the future, as well as some indicators on the risk of a failure in the future (i.e., due to the impossibility to reconfigure the power grid, which is actually working). The challenge will be to find innovative ways to represent risks and previsions in a convenient and operator-oriented way.
- **Synchronization of systems with uncertainty:** During the project the need to define algorithms for the synchronization of distributed systems with partial information sharing was highlighted. Moreover, since the models are typically affected by uncertainty there is the need to provide a framework for the synchronization of uncertain systems (e.g., CISIA which is base don fuzzy numbers). The study of this problem from both the theoretical and practical point of view has been addressed in this project, however

such a field of research continues to be almost unexplored. For instance it is possible to study more realistic cases, to consider delays due to the communication channel, to consider time varying topologies and to provide algorithms to optimize the convergence while reducing the exchange of data.

For **CRPHT** the exploitation strategy is articulated on the following targets:

- Public sector

In this case, particular focus is more towards the public administration and services acting at the level of national security, where MICIE tools (RESCI-MONITOR<sup>2</sup> in our case) are specifically exploitable in the business of crisis management activities.

CRPHT intends to use the results produced in the framework of MICIE project, more particularly RESCI-MONITOR – a tool and a risk-based method, service oriented, dedicated to monitoring security risks of interdependent critical infrastructure services using generic risks and security assurance levels – to produce and transfer to Luxembourg public authorities tools to facilitate crisis management.

The various actors, resources, sectors and assets involved in a crisis being seen as infrastructures with interdependent relationships.

To date, several tools are being considered. First, a simulation tool to not only plan and implement crisis management actions but also evaluate crisis management, and secondly, a management tool providing valuable assistance in managing a crisis in real time.

Work mentioned above, including the production of tools has already received the interest of governmental authorities, aware that the adoption of tools enabling business decision will enable in medium term the continuous improvement of crisis management at national level, or in the specific case of Luxembourg across borders.

- Industrial sector:

In this case, MICIE tools (RESCI-MONITOR in our case) are considered as tools at the operational level of security risk based monitoring considering IT infrastructures. The specific industrial sectors of interest are: energy, transport, particularly in the context of transport of dangerous goods, as well as in finance, particularly in the case of monitoring real-time transactional based financial systems.

The exploitation is based on the generalization possibilities of the results from MICIE in the before mentioned sectors, specifically with the main industrial actors based in Luxembourg, namely: CETREL and ABBL for the financial sector, CREOS and ENOVOS for the energy sector and with the National Transport Authorities (targeting security governmental institutions such as army, police, customs, emergency services).

---

<sup>2</sup> RESCI-MONITOR for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures.

- Scientific world:

As part of a PhD work in progress at CRP Henri Tudor, in cooperation with the University of Luxembourg and with the University of Oulu in Finland, research is currently under development in the improvement and formalization of the modelling activities considered as part of the developed methodology.

Additionally to this, the subject of Critical Infrastructure Protection is one of the thematic considered as scientific and technological priorities at the CRP Henri Tudor. Therefore, MICIE framework will be exploited as much as possible as an instrument that will guide future research projects seen from the academic but also from the R&D side.

For **PIAP**, as a leader in the field of mobile robots (SCADA systems) studies for safety and security purposes, the results of the project will have a key importance in developing strategies for the development of new products, which contribute to improving both safety and comfort of their users. Exploitation of the results of the project in PIAP will be focused on two main aspects: exploitation of the results in the industrial SCADA systems and exploitation of the results in safety/industrial security systems.

From the point of view of industrial SCADA systems results of the project will be exploited during the development of novel systems for cognitive control and management of wastewater systems and energy-management systems developed intensively in PIAP. Especially part of reliable data integration and reliable interfacing will play significant role in these systems. Knowledge gained during MICIE project will enable development of unique functionalities for critical infrastructure management systems developed in PIAP.

Exploitation of the results of MICIE in security/industrial safety systems will be focused on further development of interfacing sub-systems especially for FRONTEX agency, which are recently intensively developed in PIAP. As a result knowledge gained in MICIE project will enable step forward in system development in PIAP.

**ITRUST** exploits the results of MICIE in current and upcoming several projects:

- Consulting activities: Thanks to MICIE,itrust has acquired in-depth knowledge on security aspects specific to the electricity sectors. Therefore,itrust could make several audit and consultancy projects in 2010 already for electricity operators, like defining an information security policy, performing a SCADA penetration test, developing a SCADA security improvement plan. Itrust will continue this consulting and audit activity targeted to the energy sector in the next years.
- Exploitation in other current R&D projects: the Proof-of-concept based on anitrust demonstrator and a protection profile for secure information sharing will be reused in several other R&D projects atitrust:

- an internal R&D project ISIS (for Information Security Improvement System), developing a CMS tool dedicated to share security related information (based on xml technologies) with peers;
  - BUGYO-Beyond to add agents for measuring security assurance, which can be used in real-time in the risk prediction and which aims at defining a real-time risk prediction and visualisation based on all information stored inside ISIS;
  - DIAMONDS, an ITEA2 project to design and automate security test, in whichitrust intends to enhance the ISIS information with information related to security tests;
  - Location Assurance Service Provider (LASP), an ESA project developing a demonstrator for a service provider validation the trustworthiness of a Galileo Localisation, in which the common criteria design of security requirement and the communication gateway of MICIE will be reused.
- Exploitation in further R&D studies: ITRUST intends to apply the data format describing service risk predictions, which has been presented at CRITIS 2010, in an upcoming project to share such information among several EU operators. Therefore,itrust has an agreement with the national grid operator to use their data for validation,itrust has initiate a collaboration with SMILE GIE, operator of a CERT infrastructure, anditrust intends to adapt its own risk assessment methodology called TRICK-Light to the need of CIP operators, in particular for SCADA security.

**MULTITEL** exploitation strategy is centred on the following issues.

**Internal use:** Working experience obtained during the project as well as simulation models will significantly contribute to the development of the Multitel Discrete Complex Systems Modelling, Simulation and Decision Making Lab, including its growing, experience and dissemination. The goal is to become a reference in Europe in Interdependent Critical Infrastructures modelling and simulation, operating scenarios analysis, on-line simulation and validation.

**External use:** Sales of derived products - on the basis of models developed, we project to develop specific monitoring/decision making modules in the field of risk prediction and reduction for electrical infrastructure operators in Belgium and beyond. Enriched with the experience of MICIE project, Multitel also becomes an active partner of Belgian workgroup "Coordination of Energy Research", especially its "Smart Grids" subdivision.

From scientific point of view, new understanding in many actual issues is and discussed with scientific community, namely in necessary granularity level of simulation models used for reference scenarios analysis and Quality of Service Indicators estimation, adequacy of used simulation tools and their further enhancement, etc.

For **FCTUC**, the benefits of participating in the MICIE Project are manifold.

First, the direct cooperation with top-level academic and industry partners provided a stimulating and fertile environment for the FCTUC team which – by means of collaborative research – was able to extensively complement and expand its core set of security-related competencies. Achieved results are quite valuable per se – resulting in a number of scientific papers authored or co-authored by FCTUC researchers – and follow-up research activities with some members of the MICIE consortium are also expected in the near future. Joint research with CPRHT on Trust and Security Models for CIP, for instance, is already under way.

Second, the MICIE Project became a key component of FCTUC portfolio on security-related research, complementing its previous experience (focused on communication networks and telecommunications) with novel application fields, such as power utilities, industrial control networks and critical infrastructures in general. This allowed FCTUC to reinforce its position in a number of initiatives – such as the IntelliCIS COST Action and national-level forums – and to seed new joint research and innovation partnerships based on the scientific outcomes of MICIE – two new FP7 ICT project proposals were already prepared.

Furthermore, this allowed FCTUC to increase its cooperation with national and international industrial players in the energy management field, such as EDP (the largest electric utility), PT Inovação (the research unit of the largest Portuguese telecommunications company), Galp Energia (oil and gas extracting, refining, distribution and retail) and ISA (an award-winning SME specialized in Telemetry and Machine-to-Machine communications), resulting in a number of new collaborative projects that are now starting to develop. FCTUC plans to further exploit potential opportunities for applied research and for the direct provision of innovation and consultancy services to the industry.

Last but not least, the MICIE Project contributed to the FCTUC post-graduate teaching activities, strengthening its expertise in the areas of monitoring and security management in industrial networks, with a number of benefiting M.Sc. and Ph.D. students. Filipe Caldeira, a member of the FCTUC team, is expected to conclude its PhD in Q3/2011, with a Thesis that is partially based on MICIE-related research.

## 1.5 Project data



### **Project Coordinator**

*Ing. Paolo Capodiecì*  
*Selex Communications*  
*Viale dell'Industria 4*  
*00040, Pomezia (Rome) - Italy*  
*Tel: +39 91091631*  
*Fax: +39 01091 604*  
*[paolo.capodiecì@selex-comms.com](mailto:paolo.capodiecì@selex-comms.com)*  
*<http://www.selex-comms.com>*

### **Scientific Coordinator**

*Prof. Stefano Panzieri*  
*Università degli Studi "Roma Tre"*  
*Via della Vasca Navale, 79*  
*00146 Rome (Italy)*  
*Tel. +39 06 5733 3376*  
*[panzieri@uniroma3.it](mailto:panzieri@uniroma3.it)*

### **Partners**

*Centre de Recherche Public Henri Tudor (LU), Consortium for the Research in Automation and Telecommunication University of Rome - "La Sapienza" (IT), Dipartimento Informatica e Automazione – Università di Roma Tre (IT), Enea (IT), Industrial Research Institute for Automation and Measurements (PL), Israel Electric Corp (IL), Itrust consulting s. à r. l. (LU), Multitel asbl (BE), University of Coimbra Faculdade de Ciências e Tecnologia (PT), University of Bradford (PT)*

**Project duration** 01/09/2008 – 28/02/2011

**Total Cost** : 3,496,456.00 Euro

**EC Contribution** : 2,448,164.00 Euro

## **2 USE AND DISSEMINATION OF FOREGROUND**

### **2.1 Section A (public)**

The following public dissemination measures were taken during the course of the MICIE Project:

- Preparation of the MICIE public portal and progressive update of its content and design. This website contains most of the results of the project (deliverables, papers, technical documentation, workshops, exhibitions, etc.) and will remain online at least until February 2015 (4 years past the end of the project).
- Publication and/or submission of journals papers and peer-reviewed conference papers, based on MICIE research work. So far 26 peer-reviewed papers were published or accepted for publication, and 8 additional papers have been submitted (with pending reviews). More papers will be prepared in the next months, and the possibility of preparing a MICIE-based book is also being considered.
- Organization of three MICIE Workshops (Haifa, Luxembourg, Rome). Each of these workshops gathered more than 50 attendees – local industry and academia, European projects, national and European organizations – which actively participated in the discussions, providing precious feedback to the MICIE Project and valuable networking and exploitation paths that will be explored in the future.
- Presentation of the MICIE Project in seminars, workshops, invited talks and other meetings involving potential stakeholders and exploitation opportunities.
- Participation at ICT'2010 (exceeding 5,000 participants) and Future Internet Week 2010 (over 2,500 participants), with a MICIE Stand/Exhibition composed of dissemination materials (posters, brochures...) and live demonstrations.
- Participation in other high-profile events, such as the EUTC Annual Conference 2010 (plenary presentation) and SRC'2010 (2 MICIE posters).
- Publication of dissemination papers in broader scope IT magazines (IT.Nation 2010, IT-News 2010, ERCIM News...).
- Participation in standardization activities such as the ISO 27xxx workgroup on security, the ISO 15408 workgroup on Common Criteria, the workgroup on ISMS applied to Critical Infrastructure and dependability concept, and the CEN-CENELEC ESCorTS Focus Group.

In addition to those activities, each of the project partners pursued and will continue to seek exploitation opportunities that, altogether, will ensure that the outcomes of the MICIE Project will have a positive and long lasting impact in the field, directly and indirectly seeding novel technological products, new business opportunities and additional research activities.

**TEMPLATE A1: LIST OF SCIENTIFIC (PEER REVIEWED) PUBLICATIONS, STARTING BY CHRONOLOGICAL ORDER**

No.	Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers <sup>3</sup> (if available)	Is/Will open access <sup>4</sup> provided to this publication?
1	A Holistic-Reductionistic Approach for Modeling Interdependencies	S. De Porcellinis et al.	Critical Infrastructure Protection III	Springer AICT, Vol. 311, 2009	Springer Verlag	N/A	2009	pp. 215-227	doi:10.1007/978-3-642-04798-5_15 ISBN: 978-3-642-04797-8	Yes (1)
2	Modelling Interdependency among Physical, Cyber and Human Behaviour via a MHR approach	S. De Porcellinis et al.	Workshop "Modelling interdependency between Technological and Human Systems under Crisis Scenarios" held within COST'09	-	-	ETH, Zurich	2009	-	-	Yes (1)
3	On the distributed synchronization of on-line IIM Interdependency Models	Gasparri et al.	7th IEEE Int. Conf. on Industrial Informatics (INDIN 2009)	June 24-26, 2009		Cardiff (UK)	2009	pp. 795-800	doi:10.1109/INDIN.2009.5195904	Yes (1)
4	A SVM based behaviour monitoring algorithm towards detection of un-desired events in critical infrastructures	Jiang et al.	Proc. Of CISIS'09	Springer AISC 63 (23-26 September)	Springer Verlag	Spain	2009	pp. 61-68	doi: 10.1007/978-3-642-04091-7_8	Yes (1)
5	Risk Analysis of SCADA Systems Interconnecting Power Grids and Telco Networks via	Bobbio et al.	4th International Conf. on Risks and Security of	19-22 October 2009	IEEE (IEEEExplore)	Toulouse, France	2009	pp- 90-97	ISBN: 978-1-4244-4498-4 doi:10.1109/CRISIS.2009.5411974	Yes (1)

<sup>3</sup> A permanent identifier should be a persistent link to the published version full text if open access or abstract if article is pay per view) or to the final manuscript accepted for publication (link to article in repository).

<sup>4</sup> Open Access is defined as free of charge access for anyone via Internet. Please answer "yes" if the open access to the publication is already established and also if the embargo period for open access is not yet over but you intend to establish open access afterwards.

	Heterogeneous Models and Tools		Internet and Systems (CRISIS'09)							
6	From heterogeneous modeling and analysis to an on line prediction tool to improve QoS of interdependent networks	Capodieciet al.	Proceedings of Electricity 2009	1 November 2009	SEEEI	Telaviv, Israel	2009	-	-	Yes (1)
7	Agent Based Input-Output Interdependency Model	Oliva et al.	Int. J. on Critical Infrastructure Protection	Number 3 (2010)	Elsevier	-	2010	pp. 76-82	doi:10.1016/j.ijcip.2010.05.001	Yes (1)
8	Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures	Aubert et al.	5 <sup>th</sup> Int. Conf. on Availability, Reliability and Security (ARES 2010)	February 15-18, 2010	IEEE Computer Society	Krakow, Poland	2010	pp. 262-267	doi: 10.1109/ARES.2010.102	Yes (1)
9	Online Distributed Interdependency Estimation with Partial Information Sharing	Gasparriet al.	Proc. of COMPENG 2010 - Complexity in Engineering	22-24 February 2010	IEEE Computer Society	Rome, Italy	2010	pp. 82-84	ISBN: 978-0-7695-3974-4 doi: 10.1109/COMPENG.2010.30	Yes (1)
10	Improving Resilience of Interdependent Critical Infrastructures via an On-Line Alerting System	Capodieciet al.	Proc. of COMPENG 2010 - Complexity in Engineering	22-24 February 2010	IEEE Computer Society	Rome, Italy	2010	pp. 88-90	Doi: 10.1109/COMPENG.2010.28 ISBN: 978-0-7695-3974-4	Yes (1)
11	QoS of a SCADA system interconnecting a Power grid and a Telco network	Ciancamerla et al.	4 <sup>th</sup> Conf. of the Italian Association of Energy Management (AIGE),	26-27 May 2010	AIGE	Rome, Italy	2010	-	-	Yes (1)
12	QoS of a SCADA system versus QoS of a Power Distribution Grid	Ciancamerla et al.	Proc. of PSAM'10 Conference	7-11 June 2010		Seattle, USA	2010	N/A (CD Proceedings)	-	Yes (1)
13	Secure Mediation Gateway Architecture Enabling the Communication Among Critical Infrastructures	Caldeira et al.	Proc. of the Future Network & Mobile Summit 2010	16-18 June 2010		Florence, Italy	2010	N/A (CD Proceedings)	-	Yes (1)
14	A Dynamic Bayesian Network Based Structural Learning towards Automated Handwritten Digit Recognition	Pauplin et al.	5 <sup>th</sup> Int. Conf. on Hybrid Artificial Intelligence Systems (HAIS'10)	Springer LNAIS 60676 23-25 June 2010	Springer	San Sebastian, Spain	2010	pp. 120-127	-	Yes (1)

15	An Alerting System for Interdependent Critical Infrastructures	Simões et al.	Proc. of the 9th European Conference on Information Warfare and Security (ECIW 2010)	1-2 July 2010	Academic Conferences International	Thessaloniki, Greece	2010	pp. 275-283	-	Yes( 1)
16	Trust and Reputation Management for Critical Infrastructure Protection	Caldeira et al.	Proc. of the 6th Int. Conf. on Global Security, Safety & Sustainability (ICGS3'10)	Springer CCIS V.92 1-3 Sept. 2010	Springer	Lisbon, Portugal	2010	pp. 39-47	doi: 10.1007/978-3-642-15717-2_5	Yes (1)
17	Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures. Case study of a Risk-Based Approach	Aubert et. al	Proc. of ESREL 2010	Sept. 5-9, 2010	ESRA	Rhodes, Greece	2010	-	-	Yes (1)
18	Discrete event simulation of QoS of a SCADA system interconnecting a Power grid and a Telco network	Ciancamerla et al.	1st IFIP Int. Conf. on CIP - IFIP WCC 2010	Springer IFIP Series 20-23 Sept. 2010	IFIP, Springer	Brisbane, Australia	2010	-	-	Yes (1)
19	Risk ontology and Service Risk Descriptor shared among interdependent CI	Aubigny et al.	Proc. of the 5th Int. Conf. on CI Information Security (CRITIS 2010)	Springer LNCS September 2010	Springer	Athens, Greece	2010	-	-	Yes (1)
20	Trust and Reputation for Information Exchange in Critical Infrastructures	Caldeira et al.	Proc. of the 5th Int. Conf. on CI Information Security (CRITIS 2010)	Springer LNCS September 2010	Springer	Athens, Greece	2010	-	-	Yes (1)
21	Trust and reputation management for critical infrastructure protection	Caldeira et al.	Int. Journal on Electronic Security and Digital Forensic	Vol. 3, No. 3, 2010	Indescience Publishers	-	2010	pp. 187-203	Doi: 10.1504/IJESDF.2010.038282	Yes (1)
22	Support tool development for real-time risk prediction in interdependent critical infrastructures	Schaberreiter et al.	Int. Workshop on Risk and Trust in Extended Enterprises	November 1-4, 2010	IEEE	San Jose, USA	2010	-	ISSN 0929-0672	Yes (1)

			(RTEE'2010)							
23	MICIE: An Alerting Framework for Interdependent Critical Infrastructures	Capodiecici et al.	Towards a Service-Based Internet – 3 <sup>rd</sup> European Conf. ServiceWave 2010	Springer LNCS 6481 13-15 Dec. 2010	Springer	Ghent, Belgium	2010	pp. 207-208	Doi: 10.1007/978-3-642-17694-4_26	Yes (1)
24	Risk level estimation in interdependent critical infrastructures using intelligent RAO simulator	Iassinovski	Prof. of the Congress on Intelligent Systems and Information Technologies (AIS-IT 2010)	Physmathlit:2010	Physmathlit	Moscow, Russia	2010	pp. 8-14	-	Yes (1)
25	Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network, Reliability Engineering & System Safety	Bobbio et al.	Reliability Engineering & System Safety (Journal)	Vol. 95, Issue 12, December 2010	Elsevier	-	2010	pp. 1345-1357	doi:10.1016/j.res.2010.06.011	Yes (1)
26	Critical Infrastructure Security Modelling and RESCI-MONITOR: A Risk Based Critical Infrastructure Model	Schaberreiter et al.	IST-Africa 2011 Conference	May 11-13 2010	-	Gaborone – Botswana	2010	-	-	Yes (1)

(1) In general the mentioned publications are not published in open-access journals. Nevertheless, they are made available at the project website ([www.micie.eu](http://www.micie.eu)), either in their final format or in pre-print format (according to the publishers agreements).

TEMPLATE A2: LIST OF DISSEMINATION ACTIVITIES								
No.	Type of activities <sup>5</sup>	Main leader	Title	Date	Place	Type of audience <sup>6</sup>	Size of audience	Countries addressed
N/A	Participation in 19 Conferences and Workshops, to present the peer-reviewed papers already mentioned in Template A1: COST'09, INDIN'09, CISIS'09, CRISIS'09, CRITIS'09, Electricity'09, ARES'2010, COMPENG'2010, AIGE'2010, PSAM'10, CIP-WCC 2010, ECIW'2010, CRITIS'2010, HAIS'2010, Future Network & Mobile Summit 2010, ICGS3'10, ESREL'2010, RTEE'2010, IST-Africa 2011.							
1	MICIE Website	FCTUC	-	Since September 2008	-	Scientific Community, Industry, Policy Makers, Media	N/A	Global
2	Organization of Workshop	IEC	First MICIE Workshop	25 November 2009	Haifa, IL	Scientific Community, Industry, Policy Makers	Over 50 attendees	Israel
3	Organization of Workshop	ITRUST, TUDOR	Second MICIE Workshop	20 May 2010	Luxembourg	Scientific Community, Industry, Policy Makers	Over 60 attendees	Luxembourg, Belgium, European
4	Organization of Workshop	ROMA3	Third MICIE Workshop	28 February 2011	Rome, IT	Scientific Community, Industry, Policy Makers	Over 50 attendees	Italy, European
5	Exhibition	MICIE	ICT'2010	27-29 September	Brussels	Scientific	Over 5,000	European

<sup>5</sup> A drop down list allows choosing the dissemination activity: publications, conferences, workshops, web, press releases, flyers, articles published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters, Other.

<sup>6</sup> A drop down list allows choosing the type of public: Scientific Community (higher education, Research), Industry, Civil Society, Policy makers, Medias ('multiple choices' is possible).

	(stand+demonstration)	(all)		2010	BE	Community, Industry, Policy Makers		
6	Exhibition (stand+demonstration)	FCTUC	Future Internet Week'2010	15-17 December 2010	Ghent BE	Scientific Community, Industry, Policy Makers	Over 2,500	European
7	Exhibition (2 Posters)	ITRUST, PIAP	5th European Security Research Conf. SRC'2010	23 September 2010	Brussels, BE	Scientific Community, Industry, Policy Makers	Not disclosed	European
8	Invited seminar	FCTUC	EDP S.A. <i>portuguese utility</i>	18 February 2009	Coimbra, PT	Industry	15	Portuguese
9	Invited presentation	ITRUST	CREOS <i>utility</i>	February 2009	Luxembourg	Industry	10	Luxembourg, Germany, Belgium
10	Invited presentation	ITRUST	Haut Commissariat à la Protection national (HCPN)	14 July 2009	Luxembourg	Policy Makers	15	Luxembourg
11	Invited participation	ITRUST	1st Meeting of the ESCoRTS Focus Group	27 January 2010	CEN- CENELEC Brussels	Policy Makers	20	European
12	Organization and presentation	FCTUC	Innovation Forum on Security and CIP (NET-SCIP)	22 February 2010	Coimbra, PT	Scientific Community, Industry, Government	50	Portuguese
13	Invited Presentation	FCTUC	Ciência 2010	5 July 2010	Lisbon, PT	Scientific Community, Industry	70 (event: 500)	Portuguese
14	Plenary Presentation	IEC, SCOM	EUTC 2010 Annual Conference	29 October 2010	London, PT	Industry	70	European
15	Presentation	FCTUC	NET-SCIP Workshop	13 October 2010	Porto, PT	Scientific Community, Industry, Policy Makers	50	Portuguese

16	Presentation	FCTUC	4th Workshop of the COST Action IC0806	June 13-14 2011	Barcelona, ES	Scientific Community	-	European
17	Flyer/Brochure	MICIE	MICIE Fact Sheet	2009	N/A	Scientific Community, Industry, Policy Makers	N/A	N/A
18	Flyer/Brochure	CRAT	SMGW Architecture	2010	N/A	Scientific Community, Industry, Policy Makers	N/A	N/A
19	Flyer/Brochure	ROMA3	Risk Prediction Tool	2010	N/A	Scientific Community, Industry, Policy Makers	N/A	N/A
20	Flyer/Brochure	ENEA	Modeling Tools	2010	N/A	Scientific Community, Industry, Policy Makers	N/A	N/A
21	Flyer/Brochure	CPRHT	RESCI-MONITOR	2010	N/A	Scientific Community, Industry, Policy Makers	N/A	N/A
22	Stand Posters, folders, flags (4 large posters, 1 folder, flags)	MICIE	N/A	2010	N/A	Scientific Community, Industry, Policy Makers	N/A	N/A
23	Magazine Publication ( <i>L'IT du Futur sur des rails européens</i> )	ITRUST	ITNews 2.0	March/April 2009	N/A	Scientific Community, Industry, Policy Makers	N/A	Luxembourg
24	Magazine Publication ( <i>MICIE: Prévention des Risques de</i> )	CPRHT	ITNation 2.0	2010 (N. 4)	N/A	Scientific Community,	N/A	Luxembourg

	<i>Dépendances entre Infrastructures Critiques)</i>					Industry, Policy Makers		
25	Newsletter Publication ( <i>IT Security: Risk-Based Prediction Tool and Method for Critical Infrastructures</i> )	CPRHT	ERCIM News 81	April 2010	N/A	Scientific Community, Industry, Policy Makers	N/A	European
26	Magazine publication ( <i>Scambio di informazioni tra infrastrutture critiche</i> )	SCOM, CRAT	Safety and Security Italian Magazine	To be published (2011)	N/A	Scientific Community, Industry, Policy Makers	N/A	Italian
27	Press Releases (several)	SCOM, ENEA, Roma3 ITRUST, IEC	<i>media</i>	Several dates (Project start, MICIE Workshops)	N/A	Medias	N/A	Local and European

## 2.2 Section B (Confidential<sup>7</sup> or public: confidential information to be marked clearly)

### 2.2.1 Part B1

No applications for patents, trademarks, registered designs, have been submitted

---

<sup>7</sup> Note to be confused with the "EU CONFIDENTIAL" classification for some security research projects.

<b>TEMPLATE B1: LIST OF APPLICATIONS FOR PATENTS, TRADEMARKS, REGISTERED DESIGNS, ETC.</b>					
Type of IP Rights <sup>8</sup> :	Confidential Click on YES/NO	Foreseen embargo date dd/mm/yyyy	Application reference(s) (e.g. EP123456)	Subject or title of application	Applicant (s) (as on the application)
<i>Not Applicable</i>	<i>Not Applicable</i>	<i>Not Applicable</i>	<i>Not Applicable</i>	<i>Not Applicable</i>	<i>Not Applicable</i>

<sup>8</sup> A drop down list allows choosing the type of IP rights: Patents, Trademarks, Registered designs, Utility models, Others.

## 2.2.2 Part B2

Type of Exploitable Foreground <sup>9</sup>	Description of exploitable foreground	Confidential Click on YES/NO	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application <sup>10</sup>	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
<i>Not Applicable</i>								

<sup>9</sup> A drop down list allows choosing the type of foreground: General advancement of knowledge, Commercial exploitation of R&D results, Exploitation of R&D results via standards, exploitation of results through EU policies, exploitation of results through (social) innovation.

<sup>10</sup> A drop down list allows choosing the type sector (NACE nomenclature) : [http://ec.europa.eu/competition/mergers/cases/index/nace\\_all.html](http://ec.europa.eu/competition/mergers/cases/index/nace_all.html)

### 3 REPORT ON SOCIETAL IMPLICATIONS

#### A General Information *(completed automatically when Grant Agreement number is entered.)*

Grant Agreement Number:

225353

Title of Project:

Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures

Name and Title of Coordinator:

Paolo Capodiecici - Research &amp; Innovation Financing Manager

#### B Ethics

##### 1. Did your project undergo an Ethics Review (and/or Screening)?

- If Yes: have you described the progress of compliance with the relevant Ethics Review/Screening Requirements in the frame of the periodic/final project reports?

No

Special Reminder: the progress of compliance with the Ethics Review/Screening Requirements should be described in the Period/Final Project Reports under the Section 3.2.2 'Work Progress and Achievements'

##### 2. Please indicate whether your project involved any of the following issues (tick box) :

###### RESEARCH ON HUMANS

- |   |    |
|---|----|
| • Did the project involve children?                         | No |
| • Did the project involve patients?                         | No |
| • Did the project involve persons not able to give consent? | No |
| • Did the project involve adult healthy volunteers?         | No |
| • Did the project involve Human genetic material?           | No |
| • Did the project involve Human biological samples?         | No |
| • Did the project involve Human data collection?            | No |

###### RESEARCH ON HUMAN EMBRYO/FOETUS

- |   |    |
|---|----|
| • Did the project involve Human Embryos?  | No |
| • Did the project involve Human Foetal Tissue / Cells?  | No |
| • Did the project involve Human Embryonic Stem Cells (hESCs)?                                 | No |
| • Did the project on human Embryonic Stem Cells involve cells in culture?                     | No |
| • Did the project on human Embryonic Stem Cells involve the derivation of cells from Embryos? | No |

###### PRIVACY

- |   |    |
|---|----|
| • Did the project involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)? | No |
| • Did the project involve tracking the location or observation of people?   |    |

###### RESEARCH ON ANIMALS

- |  |    |
|--|----|
| • Did the project involve research on animals? | No |
|--|----|

• Were those animals transgenic small laboratory animals?	<i>No</i>	
• Were those animals transgenic farm animals?	<i>No</i>	
• Were those animals cloned farm animals?	<i>No</i>	
• Were those animals non-human primates?	<i>No</i>	
<b>RESEARCH INVOLVING DEVELOPING COUNTRIES</b>		
• Did the project involve the use of local resources (genetic, animal, plant etc)?	<i>No</i>	
• Was the project of benefit to local community (capacity building, access to healthcare, education etc)?	<i>No</i>	
<b>DUAL USE</b>		
• Research having direct military use	<i>No</i>	
• Research having the potential for terrorist abuse	<i>No</i>	
<b>C Workforce Statistics</b>		
<b>3. Workforce statistics for the project: Please indicate in the table below the number of people who worked on the project (on a headcount basis).</b>		
<b>Type of Position</b>	<b>Number of Women</b>	<b>Number of Men</b>
Scientific Coordinator		1
Work package leaders		7
Experienced researchers (i.e. PhD holders)		5
PhD Students	1	5
Other		
<b>4. How many additional researchers (in companies and universities) were recruited specifically for this project?</b>		<b>4</b>
Of which, indicate the number of men:		1

<b>D Gender Aspects</b>		
<b>5. Did you carry out specific Gender Equality Actions under the project?</b>	<input type="radio"/> √ <input type="radio"/>	Yes No
<b>6. Which of the following actions did you carry out and how effective were they?</b>		
<input type="checkbox"/>	Design and implement an equal opportunity policy	Not at all effective <input type="radio"/> √ <input type="radio"/> <input type="radio"/> <input type="radio"/>
<input type="checkbox"/>	Set targets to achieve a gender balance in the workforce	<input type="radio"/> √ <input type="radio"/> <input type="radio"/> <input type="radio"/>
<input type="checkbox"/>	Organise conferences and workshops on gender	<input type="radio"/> √ <input type="radio"/> <input type="radio"/> <input type="radio"/>
<input type="checkbox"/>	Actions to improve work-life balance	<input type="radio"/> √ <input type="radio"/> <input type="radio"/> <input type="radio"/>
<input type="radio"/>	Other: <input style="width: 150px;" type="text"/>	
<b>7. Was there a gender dimension associated with the research content – i.e. wherever people were the focus of the research as, for example, consumers, users, patients or in trials, was the issue of gender considered and addressed?</b>		
<input type="radio"/>	Yes- please specify <input style="width: 150px;" type="text"/>	
<input checked="" type="radio"/>	No	
<b>E Synergies with Science Education</b>		
<b>8. Did your project involve working with students and/or school pupils (e.g. open days, participation in science festivals and events, prizes/competitions or joint projects)?</b>		
<input checked="" type="radio"/>	Yes- please specify <input style="width: 150px;" type="text"/>	Stand to ICT2010 Event
<input type="radio"/>	No	
<b>9. Did the project generate any science education material (e.g. kits, websites, explanatory booklets, DVDs)?</b>		
<input checked="" type="radio"/>	Yes- please specify <input style="width: 150px;" type="text"/>	Web site ( <a href="http://www.micie.eu">www.micie.eu</a> ) – Papers, Brochures.
<input type="radio"/>	No	
<b>F Interdisciplinarity</b>		
<b>10. Which disciplines (see list below) are involved in your project?</b>		
<input checked="" type="radio"/>	Main discipline <sup>11</sup> : Mathematics and computer sciences [mathematics and software development]	
<input type="radio"/>	Associated discipline <sup>11</sup> : <input style="width: 100px;" type="text"/>	<input type="radio"/> Associated discipline <sup>11</sup> : <input style="width: 100px;" type="text"/>
<b>G Engaging with Civil society and policy makers</b>		
<b>11a Did your project engage with societal actors beyond the research community? (if 'No', go to Question 14)</b>	<input type="radio"/> √ <input type="radio"/>	Yes No
<b>11b If yes, did you engage with citizens (citizens' panels / juries) or organised civil society (NGOs, patients' groups etc.)?</b>		
<input type="radio"/>	No	
<input type="radio"/>	Yes- in determining what research should be performed	
<input type="radio"/>	Yes - in implementing the research	
<input type="radio"/>	Yes, in communicating /disseminating / using the results of the project	

<sup>11</sup> Insert number from list below (Frascati Manual).

<b>11c In doing so, did your project involve actors whose role is mainly to organise the dialogue with citizens and organised civil society (e.g. professional mediator; communication company, science museums)?</b>	<input type="radio"/> <input type="radio"/>	Yes No	
<b>12. Did you engage with government / public bodies or policy makers (including international organisations)</b>			
<input type="radio"/> No <input type="radio"/> Yes- in framing the research agenda <input type="radio"/> Yes - in implementing the research agenda <input type="radio"/> Yes, in communicating /disseminating / using the results of the project			
<b>13a Will the project generate outputs (expertise or scientific advice) which could be used by policy makers?</b> <input type="radio"/> Yes – as a <b>primary</b> objective (please indicate areas below- multiple answers possible) <input type="radio"/> Yes – as a <b>secondary</b> objective (please indicate areas below - multiple answer possible) <input type="radio"/> No			
<b>13b If Yes, in which fields?</b>			
Agriculture Audiovisual and Media Budget Competition Consumers Culture Customs Development Economic and Monetary Affairs Education, Training, Youth Employment and Social Affairs		Energy Enlargement Enterprise Environment External Relations External Trade Fisheries and Maritime Affairs Food Safety Foreign and Security Policy Fraud Humanitarian aid	Human rights Information Society Institutional affairs Internal Market Justice, freedom and security Public Health Regional Policy Research and Innovation Space Taxation Transport

<b>13c If Yes, at which level?</b> <input type="radio"/> Local / regional levels <input type="radio"/> National level <input type="radio"/> European level <input type="radio"/> International level		
<b>H Use and dissemination</b>		
<b>14. How many Articles were published/accepted for publication in peer-reviewed journals?</b>	<b>26</b>	
<b>To how many of these is open access<sup>12</sup> provided?</b>	26	
<b>How many of these are published in open access journals?</b>	0	
<b>How many of these are published in open repositories?</b>	26	
<b>To how many of these is open access not provided?</b>	0	
<b>Please check all applicable reasons for not providing open access:</b>		
<input type="checkbox"/> publisher's licensing agreement would not permit publishing in a repository <input type="checkbox"/> no suitable repository available <input type="checkbox"/> no suitable open access journal available <input type="checkbox"/> no funds available to publish in an open access journal <input type="checkbox"/> lack of time and resources <input type="checkbox"/> lack of information on open access <input type="checkbox"/> other <sup>13</sup> : .....		
<b>15. How many new patent applications ('priority filings') have been made?</b> <i>("Technologically unique": multiple applications for the same invention in different jurisdictions should be counted as just one application of grant).</i>	<b>None</b>	
<b>16. Indicate how many of the following Intellectual Property Rights were applied for (give number in each box).</b>	Trademark	<b>None</b>
	Registered design	<b>None</b>
	Other	<b>None</b>
<b>17. How many spin-off companies were created / are planned as a direct result of the project?</b>	<b>None</b>	
<i>Indicate the approximate number of additional jobs in these companies:</i>		
<b>18. Please indicate whether your project has a potential impact on employment, in comparison with the situation before your project:</b>		
<input type="checkbox"/> Increase in employment, or <input checked="" type="checkbox"/> Safeguard employment, or <input type="checkbox"/> Decrease in employment, <input type="checkbox"/> Difficult to estimate / not possible to quantify	<input type="checkbox"/> In small & medium-sized enterprises <input type="checkbox"/> In large companies <input type="checkbox"/> None of the above / not relevant to the project	
<b>19. For your project partnership please estimate the employment effect resulting directly from your participation in Full Time Equivalent (FTE = one person working fulltime for a year) jobs:</b>	<i>Indicate figure:</i> 4	

<sup>12</sup> Open Access is defined as free of charge access for anyone via Internet.

<sup>13</sup> For instance: classification for security project.

Difficult to estimate / not possible to quantify	<input type="checkbox"/>
<b>I Media and Communication to the general public</b>	
<b>20. As part of the project, were any of the beneficiaries professionals in communication or media relations?</b>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<b>21. As part of the project, have any beneficiaries received professional media / communication training / advice to improve communication with the general public?</b>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<b>22 Which of the following have been used to communicate information about your project to the general public, or have resulted from your project?</b>	
<input type="checkbox"/> Press Release	<input checked="" type="checkbox"/> Coverage in specialist press
<input type="checkbox"/> Media briefing	<input type="checkbox"/> Coverage in general (non-specialist) press
<input type="checkbox"/> TV coverage / report	<input type="checkbox"/> Coverage in national press
<input type="checkbox"/> Radio coverage / report	<input checked="" type="checkbox"/> Coverage in international press
<input checked="" type="checkbox"/> Brochures /posters / flyers	<input checked="" type="checkbox"/> Website for the general public / internet
<input type="checkbox"/> DVD /Film /Multimedia	<input checked="" type="checkbox"/> Event targeting general public (festival, conference, exhibition, science café)
<b>23 In which languages are the information products for the general public produced?</b>	
<input type="checkbox"/> Language of the coordinator	<input checked="" type="checkbox"/> English
<input type="checkbox"/> Other language(s)	

**Question F-10:** Classification of Scientific Disciplines according to the Frascati Manual 2002 (Proposed Standard Practice for Surveys on Research and Experimental Development, OECD 2002):

## FIELDS OF SCIENCE AND TECHNOLOGY

### 1. NATURAL SCIENCES

- 1.1 Mathematics and computer sciences [mathematics and other allied fields: computer sciences and other allied subjects (software development only; hardware development should be classified in the engineering fields)]
- 1.2 Physical sciences (astronomy and space sciences, physics and other allied subjects)
- 1.3 Chemical sciences (chemistry, other allied subjects)
- 1.4 Earth and related environmental sciences (geology, geophysics, mineralogy, physical geography and other geosciences, meteorology and other atmospheric sciences including climatic research, oceanography, vulcanology, palaeoecology, other allied sciences)
- 1.5 Biological sciences (biology, botany, bacteriology, microbiology, zoology, entomology, genetics, biochemistry, biophysics, other allied sciences, excluding clinical and veterinary sciences)

### 2. ENGINEERING AND TECHNOLOGY

- 2.1 Civil engineering (architecture engineering, building science and engineering, construction engineering, municipal and structural engineering and other allied subjects)
- 2.2 Electrical engineering, electronics [electrical engineering, electronics, communication engineering and systems, computer engineering (hardware only) and other allied subjects]
- 2.3. Other engineering sciences (such as chemical, aeronautical and space, mechanical, metallurgical and materials engineering, and their specialised subdivisions; forest products; applied sciences such as

geodesy, industrial chemistry, etc.; the science and technology of food production; specialised technologies of interdisciplinary fields, e.g. systems analysis, metallurgy, mining, textile technology and other applied subjects)

### 3. MEDICAL SCIENCES

- 3.1 Basic medicine (anatomy, cytology, physiology, genetics, pharmacy, pharmacology, toxicology, immunology and immunohaematology, clinical chemistry, clinical microbiology, pathology)
- 3.2 Clinical medicine (anaesthesiology, paediatrics, obstetrics and gynaecology, internal medicine, surgery, dentistry, neurology, psychiatry, radiology, therapeutics, otorhinolaryngology, ophthalmology)
- 3.3 Health sciences (public health services, social medicine, hygiene, nursing, epidemiology)

### 4. AGRICULTURAL SCIENCES

- 4.1 Agriculture, forestry, fisheries and allied sciences (agronomy, animal husbandry, fisheries, forestry, horticulture, other allied subjects)
- 4.2 Veterinary medicine

### 5. SOCIAL SCIENCES

- 5.1 Psychology
- 5.2 Economics
- 5.3 Educational sciences (education and training and other allied subjects)
- 5.4 Other social sciences [anthropology (social and cultural) and ethnology, demography, geography (human, economic and social), town and country planning, management, law, linguistics, political sciences, sociology, organisation and methods, miscellaneous social sciences and interdisciplinary, methodological and historical SIT activities relating to subjects in this group. Physical anthropology, physical geography and psychophysiology should normally be classified with the natural sciences].

### 6. HUMANITIES

- 6.1 History (history, prehistory and history, together with auxiliary historical disciplines such as archaeology, numismatics, palaeography, genealogy, etc.)
- 6.2 Languages and literature (ancient and modern)
- 6.3 Other humanities [philosophy (including the history of science and technology) arts, history of art, art criticism, painting, sculpture, musicology, dramatic art excluding artistic "research" of any kind, religion, theology, other fields and subjects pertaining to the humanities, methodological, historical and other SIT activities relating to the subjects in this group]