

MODEL TOOLS FOR MANAGING INTERACTION BETWEEN CRITICAL INFRASTRUCTURES AND RELATED DEPENDABILITY AND VULNERABILITIES



MORE INFORMATION

Project Website:

www.micie.eu

Coordinator contact:

Paolo Capodieci
Selex Communications Sp.A., Italy
paolo.capodieci@selex-comms.com

PARTICIPANTS

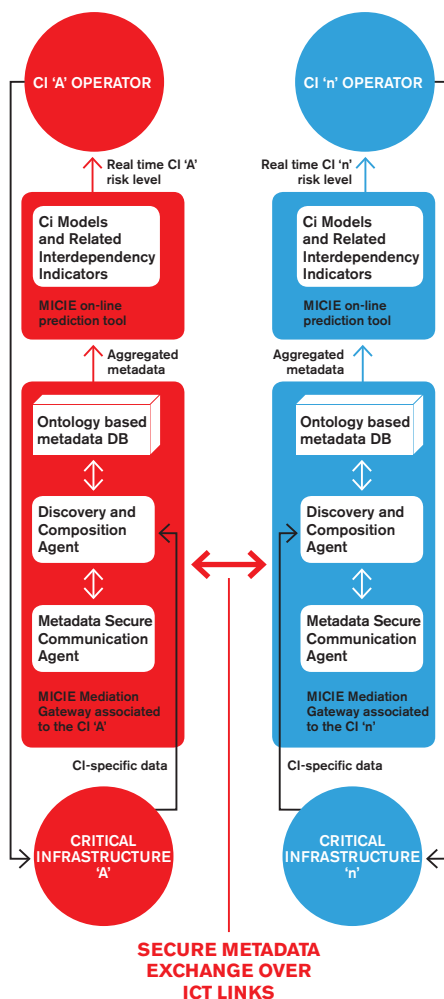
- › Selex Communications S.p.A., IT
- › Centre de Recherche Public Henri Tudor, LU
- › CRAT – “Sapienza” University of Rome, IT
- › Dipartimento Informatica e Automazione, Università di Roma Tre, IT
- › ENEA, IT
- › Industrial Research Institute for Automation and Measurements, PL
- › Israel Electric Corp, IL
- ›itrust consulting s.à r.l., LU
- › Multitel asbl, BE
- › University of Coimbra, PT
- › University of Bradford, UK

MICIE project, being in line with EU initiative to establish a Critical Infrastructure Warning Information Network (CIWIN), will design and implement a so-called “MICIE alerting system” that identifies, in real time, the level of possible threats induced on a given CI by “undesired” events happened in such CI and/or other interdependent CIs. In particular, whenever such events occur, the MICIE alerting system will support the CI operators providing them with a real time risk level (e.g. expressed in a chromatic scale such as white, green, yellow, orange, red.

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

PROJECT OBJECTIVES

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 and the impact of such attributes on the delivery of service of any other cross-domain infrastructure.
2. Design and analysis of a hierarchical modelling framework for interdependency analysis based on the integration of heterogeneous modelling 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 commutation network able to assure availability, authenticity, integrity, confidentiality and non-repudiation of metadata exchanged.
5. Validation of the interdependency alarm -predictor system on the infrastructure of an Electric Company, Israel Electric Corp, partner in the project.



GENERAL CONCEPT

Improving the security of European CIs has become a top priority. Significant actions are underway to assess and reduce vulnerabilities to potential terrorist attacks, 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.

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.

SCIENTIFIC AND TECHNOLOGICAL OBJECTIVES

MICIE project will pursue the following three innovative specific scientific and technological objectives which will be detailed in the following three main points:

1. Designing CI modelling 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 modelling 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 will include 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 modelling techniques mentioned in issue (1) and makes use, as key inputs, of the metadata mentioned in issue (2).