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

MICIE Project

Ing. Paolo Capodieci

Selex Communications S.p.A.

Critical Infrastructure Protection

A Real Time Alerting System: Tools & Models

28th February, Rome

www.micie.eu

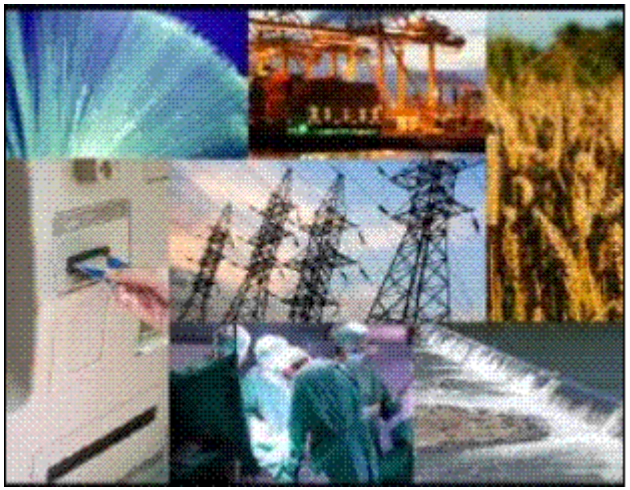
ICT-SEC 225353

Summary

- *MICIE Project Presentation*
  - *Scope, Objectives*
  - *WBS*
  - *Consortium composition*
  - *Project data*
  - *MICIE General architecture*
  - *Expected impacts and Added value at European level*

Before to start .....

la Repubblica.it



CRIMINALITA' INFORMATICA

"Night Dragon", cyber-attacco alle infrastrutture energetiche

Già colpite una dozzina di multinazionali del settore sparse in Europa, Cina e Stati Uniti.
L'operazione è simile a quella lanciata alla fine dello scorso anno contro le aziende nucleari iraniane.
Intanto, gli hacker di "Anonymous" annunciano per domenica una nuova offensiva

di CLAUDIO GERINO

ROMA - Nuova cyber-offensiva contro le infrastrutture energetiche mondiali.

(10 febbraio 2011

MICIE Project Presentation

Ing. Paolo Capodieci, MICIE Project Coordinator

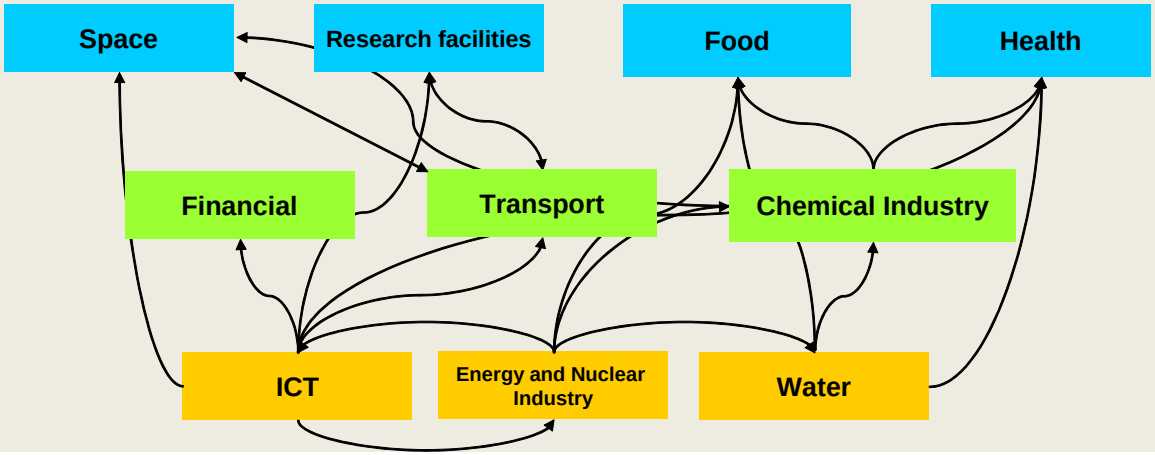
Selex Communications S.pA.

Italy

PROJECT SCOPE

SCOPE

The MICIE project, will design and implement a "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 any other interdependent Critical Infrastructure.



Critical Infrastructure are highly dependent on each other

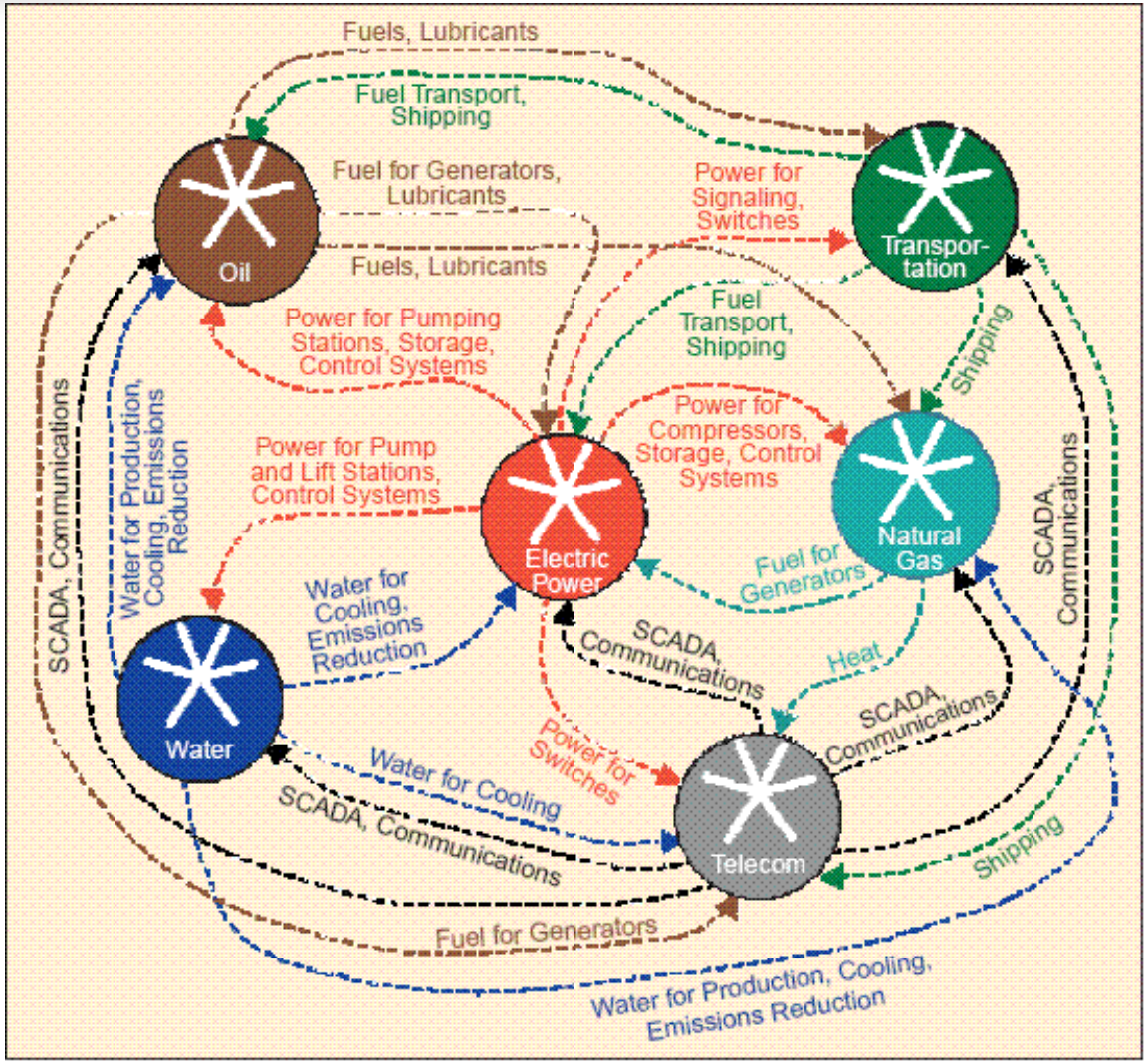
Typical Critical Infrastructures 1/2

Sector	Sub-sector
Energy	-*Oil* and *gas production*, refining, treatment, storage -*Distribution* by pipelines -*Electricity generation* and *transmission*
Nuclear industry	-*Production* and *storage*/processing of nuclear substances
Information, Communication Technologies, ICT	-Information system and *network protection* -Instrumentation automation and control systems (*SCADA* etc.) -Internet -Provision of *fixed telecommunications* -Provision of *mobile telecommunications* -*Radio communication* and navigation -*Satellite* communication -*Broadcasting*
Water	-*Provision* of drinking water -*Control* of water *quality* -*Control* of water *quantity*
Food	-*Provision* of food and safeguarding *food safety and security*

Typical Critical Infrastructures 2/2

Sector	Sub-sector
Health	-*Medical* and *hospital* care -Medicines, vaccines and pharmaceuticals -Bio-laboratories and bio-agents
Financial	-*Payment* and *securities* clearing and settlement infrastructures -Regulated markets Security
Transport	-*Road* transport -*Rail* transport -*Air* transport -Inland *waterways* transport -Ocean and short-sea shipping
Chemical industry	-*Production* and *storage*/processing of chemical substances -*Pipelines* of dangerous goods (chemical substances)
Space	-Space
Research facilities	-Research facilities

Typical Critical Infrastructures Interdependency



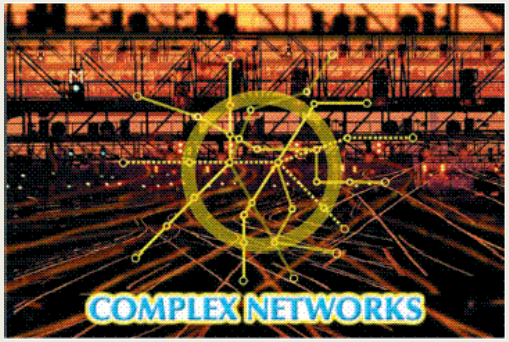
PROJECT SCOPE

1. *Analysis and Design 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. *Validation of the interdependency alarm predictor system on the infrastructure of an Electric Company, Israel Electric Corp, partner in the project.*

PROJECT SCOPE

HOW TO DO IT

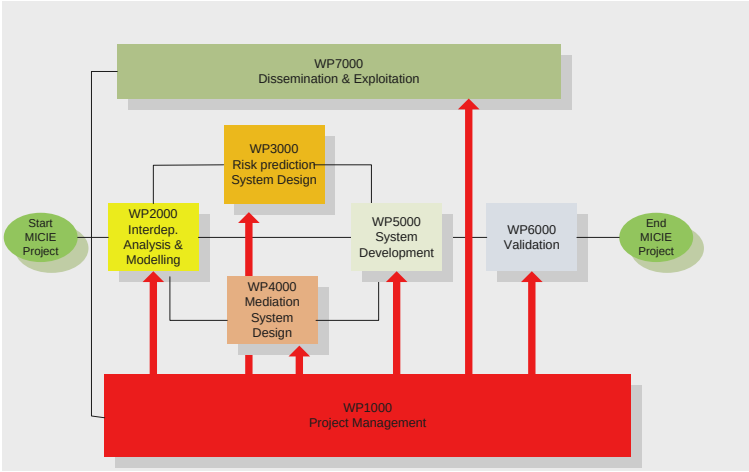
1. *The design and implementation of MICIE Secure Mediation Gateways*
2. *The design and implementation of a MICIE on-line risk prediction tool*
3. *Validation on the real (IEC) Critical Infrastructures*



Work Breakdown Structure

MICIE Project

- **WP1000 Management (Selex Comms)**
- **WP2000 Interdependency Analysis & Modelling (Enea)**
  - T. 2001 Reference Scenarios
  - T.2002 Service Oriented Approach
  - T.2003 Interdependency Metric and Indicators
  - T. 2004 Modelling Framework and Interdependency Analysis
  - T. 2004 Dynamic Bayesian Network approach
- **WP3000 Risk prediction System Design (Roma3)**
  - T. 3001 From Interdependecy metrics to Risk Prediction formulation
  - T. 3002 Metadata aggregation and Risk Prediction algorithms
- **WP4000 Mediation System Design (CRAT)**
  - T. 4001 ICT System Requirements
  - T. 4002 Cross CI's domain data mediation
  - T. 4003 Cross CI's domain data security
- **WP5000 System Development (Selex Comms)**
  - T. 5001 On-line risk prediction system
  - T. 5002 Secure Mediation Gateway
- **WP6000 Validation (IEC)**
  - T.6001 Demo system Integration
  - T. 6002 Validation Activities
- **WP7000 Dissemination & Exploitation (FCTUC)**
  - T. 7002 Exploitation
  - T. 7001 Dissemination

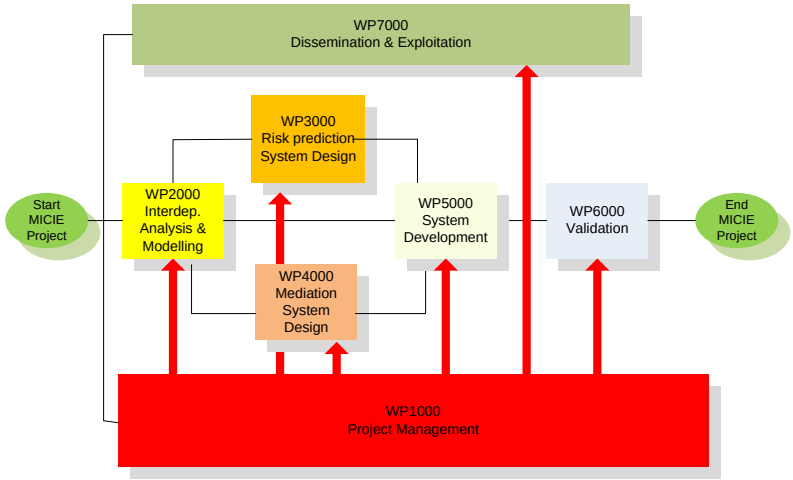


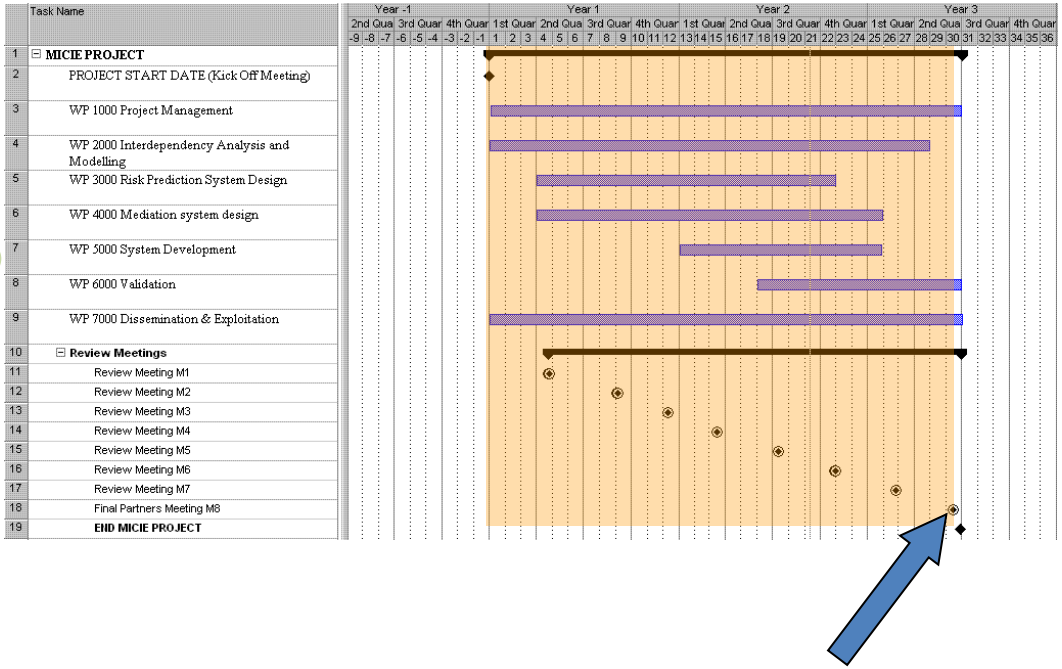
SCHEDULING

P1: from month1 (Sept 2008) to month 10 (June 2009) Completed !!!

P2: from month11 (July 2009) to month 20 (April 2010) Completed !!!

P3: from month 21 (May 2010) to month 30 (28th February 2011) Completed !!!



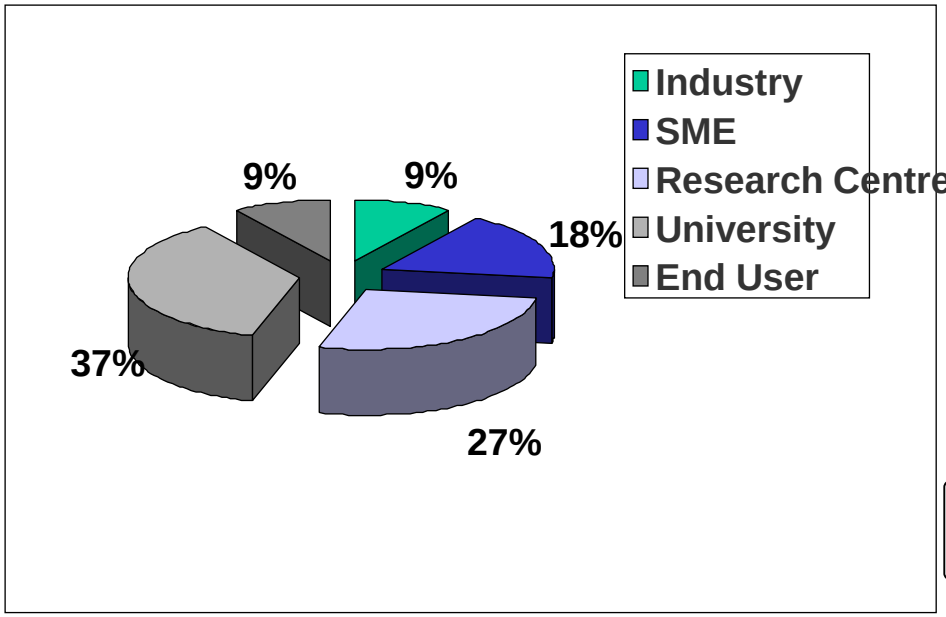


Final workshop – End of Project

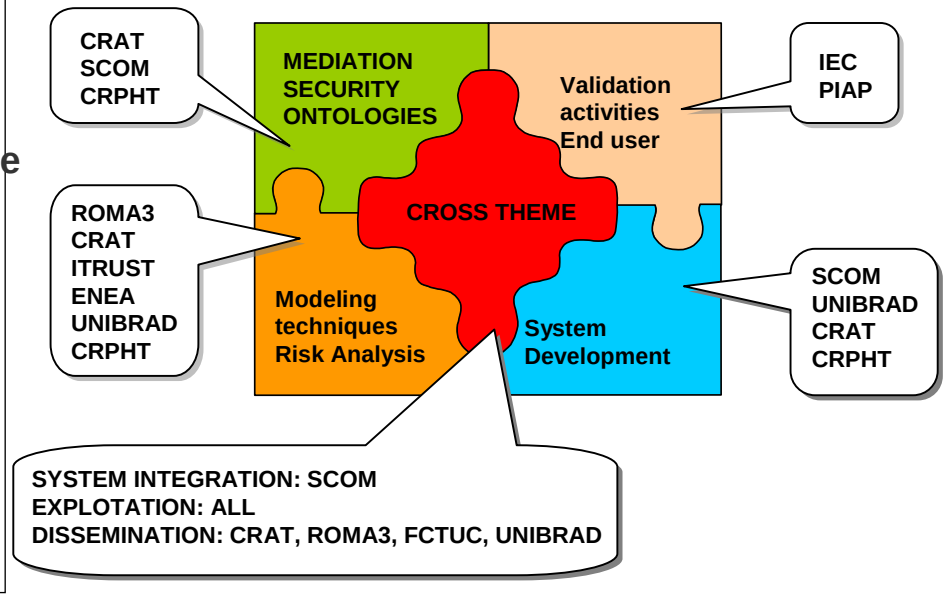
CONSORTIUM COMPOSITION

no.	Participant name	Country		Type
1	Selex Communications S.p.A.	IT		Industrial
2	Centre de Recherché Public Henri Tudor	LU		Research Centre
3	Consortium for the Research in Automation and Telecommunication University of Rome - "La Sapienza"	IT		University
4	Dipartimento Informatica e Automazione –Università di Roma Tre	IT		University
5	Enea	IT		Research Centre
6	Industrial Research Institute for Automation and Measurements	PL		Research Centre
7	Israel Electric Corp.	IL		Industrial – End User
8	itrust consulting s. à r. l.	LU		SME
9	Multitel asbl	BE		SME
10	University of Coimbra Faculdade de Ciências e Tecnologia	PT		University
11	University of Bradford	UK		University

CONSORTIUM COMPOSITION



MICIE consortium composition by type

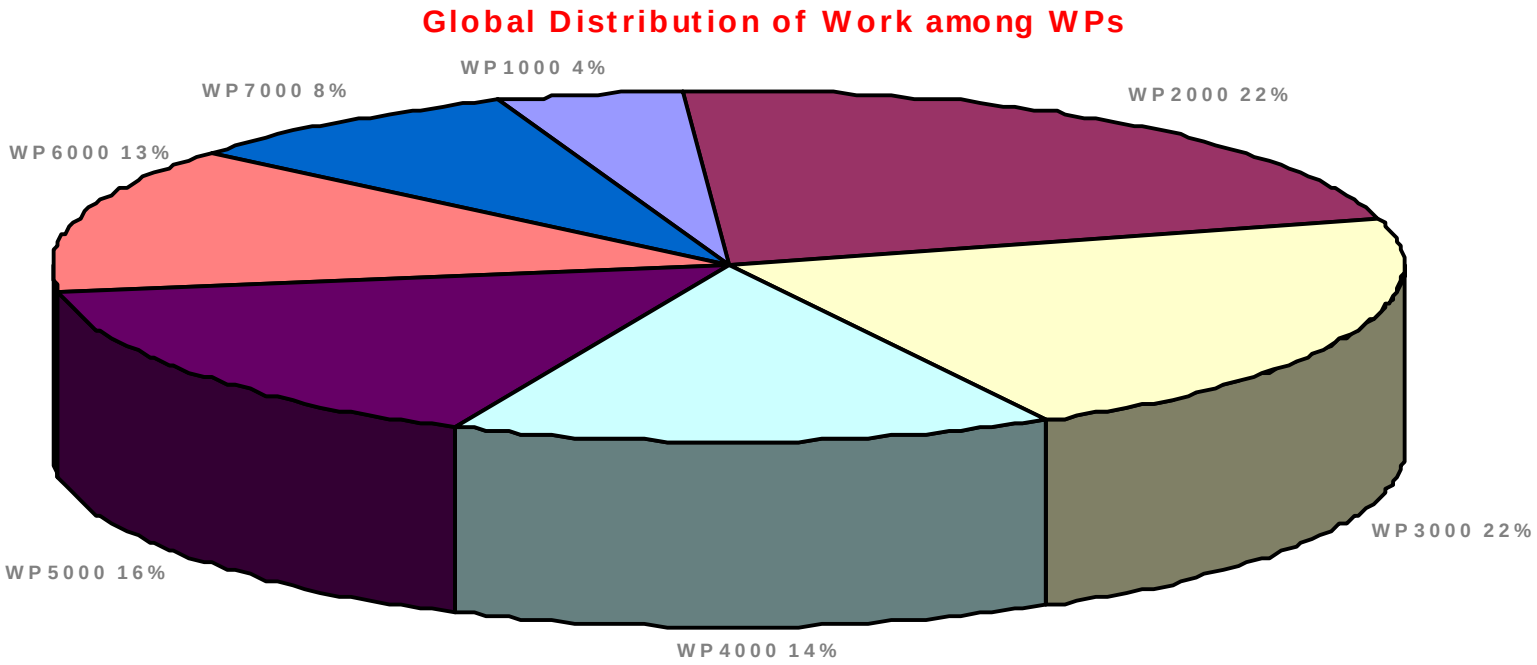


MICIE consortium complementarities vs competence domain

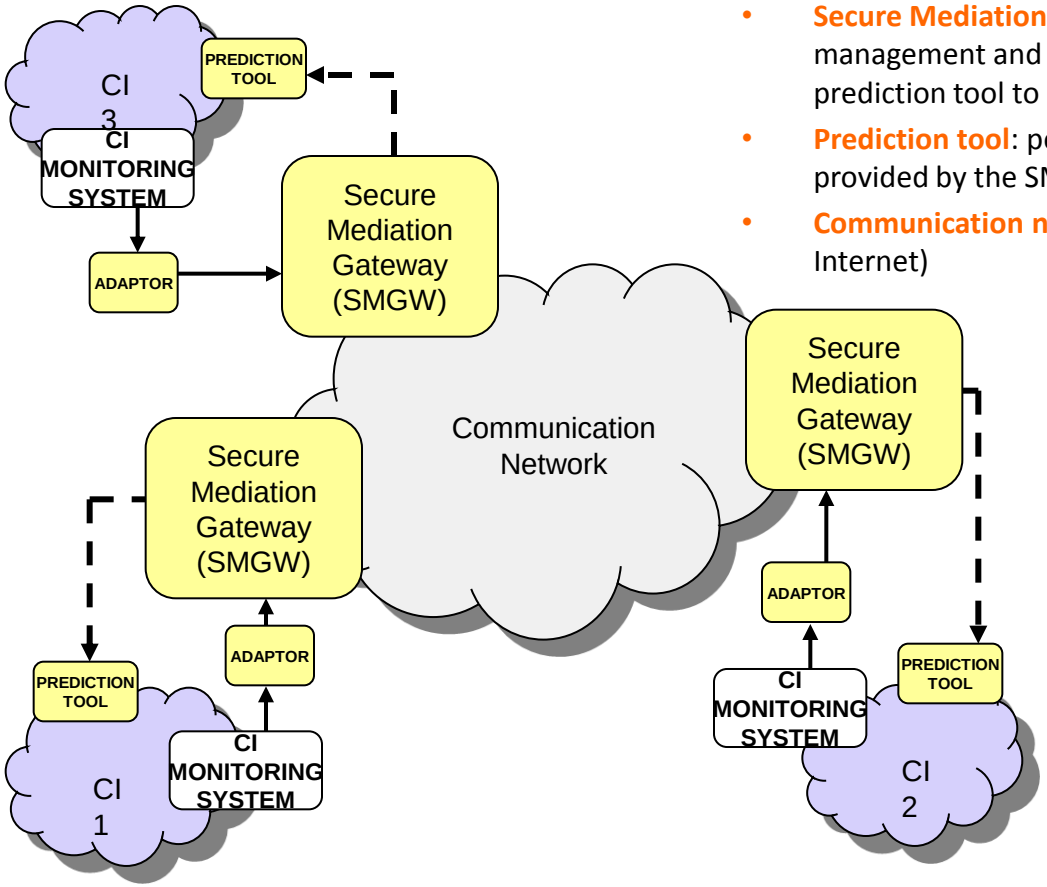
PROJECT MAIN DATA

- Project duration 30 months
- Start 1st September 2008
- End 28th February 2011
- Total effort 314 man / months
- Total cost 3.496.456,00 Euro
- EC Contribution 2.488.164,00 Euro

Global Distribution of Work among WPs

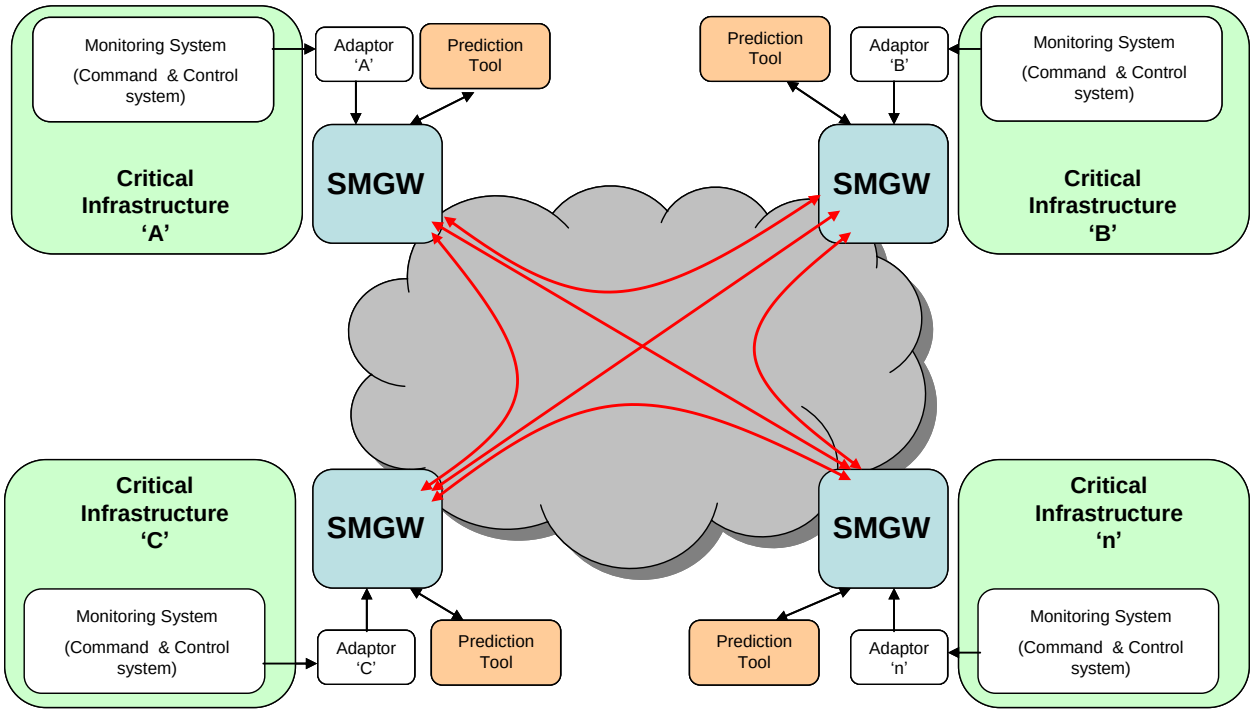


MICIE overall system



- **CI monitoring system**: Critical Infrastructure legacy monitoring system
- **Adaptor**: translates CI-dependent information coming from the CI's monitoring system into CI-independent data
- **Secure Mediation Gateway (SMGW)**: includes the functionalities for the management and the exchange of the information needed by the prediction tool to perform its operations
- **Prediction tool**: performs risk prediction on the basis of the information provided by the SMGW
- **Communication network**: It can be a private or public network (i.e., Internet)

MICIE overall system architecture



Project Expected Impacts

- *Reinforce European industry's potential to create important market opportunities and establish leadership*
- *Contribution to establishing, strengthening and preserving trust in the use of technologies for the protection of critical infrastructures*
- *Significant improvement in the security, performance, dependability and resilience of complex and interdependent critical infrastructures*
- *Reduction of pan-European damages and costs induced by cascade failure in critical infrastructures allowing a better alerting and management of crisis events*
- *Improvement of the cross-border cooperation among critical infrastructures of the different countries according to EPCIP (European Program on Critical Infrastructure Protection)*

Added value in carrying out the work at European level

- *MICIE objectives required the mobilisation of high-level specific technical and scientific competences, as well as the contributions of End-User infrastructures;*
- *The project required the combination of the adequate skills from large industries, academia, operators and end-users, which are difficult to find in any of the individual Organization;*
- *One of the added-value carrying the work at European level, therefore, is the opportunity to join high-level competences of partners coming from different Countries, thus gathering the skills in all the disciplines involved in the research such as algorithms and mathematical problem, communications technologies, security and complex modelling frameworks, software development.*

Relevance to European Union policies

- *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*
- *As defined in the framework of EPCIP "The CIP information sharing process among relevant stakeholders requires a relationship of trust, such that the proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected"*
- *MICIE project will provide support in solving the outlined security issues concerning CIP information sharing through the definition of the secure gateway implementing security (authenticity, confidentiality, availability) of metadata exchanged across CIs'.*

Relevance from Industry point of view

- *On the basis of market analysis, Selex Communications has identified new opportunities of business in the field of data mediation and secure communications, for Homeland Security market*
- *The development of the Secure Mediation Gateway represents a chance in terms of industrial strategy for Homeland Security products and to acquire new markets segment*
- *For a manufacturing industry as Selex Communications, this represents an opportunity of growth both in economic terms and as opportunity to create new knowledge in the field of Critical Information Protection*

END OF MICIE PRESENTATION

Paolo Capodieci

www.micie.eu