



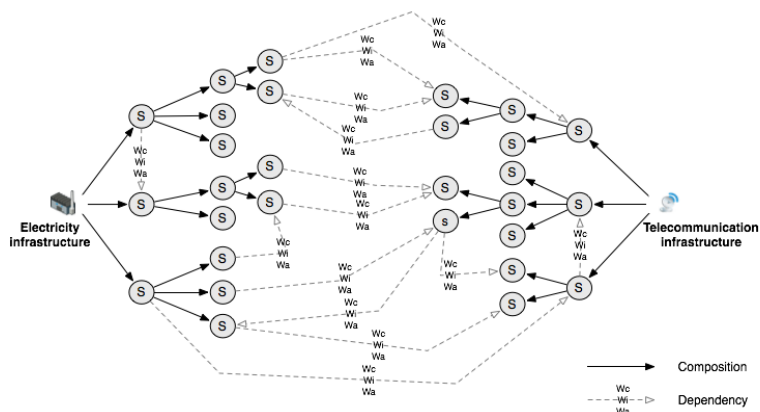
# RESCI-MONITOR REAL-TIME SECURITY MONITORING OF INTERDEPENDENT SERVICES IN CRITICAL INFRASTRUCTURES

**MICIE**  
Tools for Real Time Service Level  
Risk Analyses for Interdependent  
Critical Infrastructures

**RESCI-MONITOR**  
Is a tool and a risk-based method,  
service oriented, dedicated  
to monitoring security risks of  
interdependent critical infrastructure  
(CI) services using generic risks and  
security assurance levels.  
Exploiting known security properties,  
that are: confidentiality, integrity and  
availability (CIA), RESCI-MONITOR  
allows evaluating the security risk  
level of a CI service, taking into account  
it's dependencies with regard to its  
internal or external related services.

## STEP 1 - IDENTIFICATION OF THE INTERDEPENDENCY FUNCTIONAL MODEL BASED ON A COMPLETE RISK ASSESSMENT

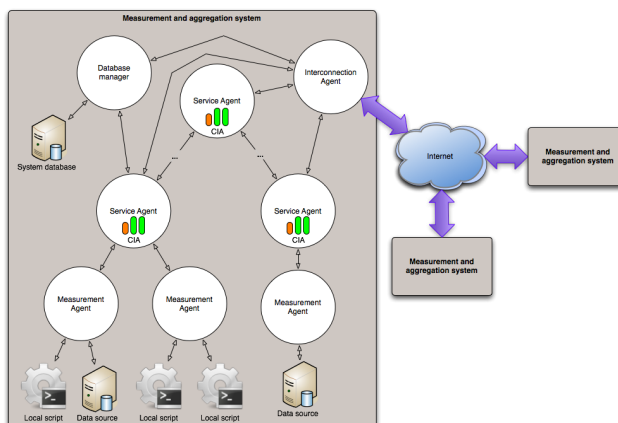
The off-line risk assessment step deals with an analysis of the infrastructure. CIs are seen as service providers which provide services to customers. Those customers can in turn be other dependent or interdependent CIs or CI services which need the service in order to provide their own service(s). In order to be able to observe the CI state we need to identify observable entities in the infrastructure (base measurements). Furthermore, to quantify the contribution of a base measurement to the confidentiality, integrity and availability of a service, a weight is associated to each base measurement. The same applies to each identified dependency.



Tree-like modelling of CIs

## STEP 2 - AGGREGATING REAL MEASUREMENTS INTO ABSTRACT SERVICE RISK-RELATED SECURITY PROPERTIES

Using interdependency functional model, the system is able to continually perform measurements on the various observable entities of the CI. Measurements are normalized and aggregated in the form of security risk levels (Confidentiality, Integrity, Availability).



## MORE INFORMATION

### Project Website:

www.micie.eu

### Coordinator contact:

Paolo Capodiecì  
Selex Communications Sp.A., Italy  
paolo.capodiecì@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

## STEP 3 - MONITORING SECURITY RISKS OF SERVICES

In the on-line risk monitoring step, each CI service receives risk indicators from interdependent CI services and can, after applying the associated interdependency weight for confidentiality, integrity and availability, use this information to adjust the overall service risk by including the interdependencies.

This monitoring helps to determine the security risk level of services and allows each CI provider to react and adopt the best behaviour (e.g. service degradation, service switch, etc.) corresponding to the security state of its different services.

