http://www.micie.eu/

SEVENTH FRAMEWORK PROGRAMME

Information Society

ROME, ITALY

28 FEB, 2011

RESCI-MONITOR

Real Time Security Monitoring of Interdependent Services in CIs

Jocelyn AUBERT

Centre de Recherche Public Henri Tudor, Luxembourg

jocelyn.aubert@tudor.lu

ICT-SEC 225353 MICIE

RESCI-MONITOR

• Real-time security monitoring of interdependent services in Critical Infrastructures (CI)

• Tool and a risk-based method, service oriented, dedicated to monitoring security risks of interdependent CI services

• Use of generic risks and security assurance levels

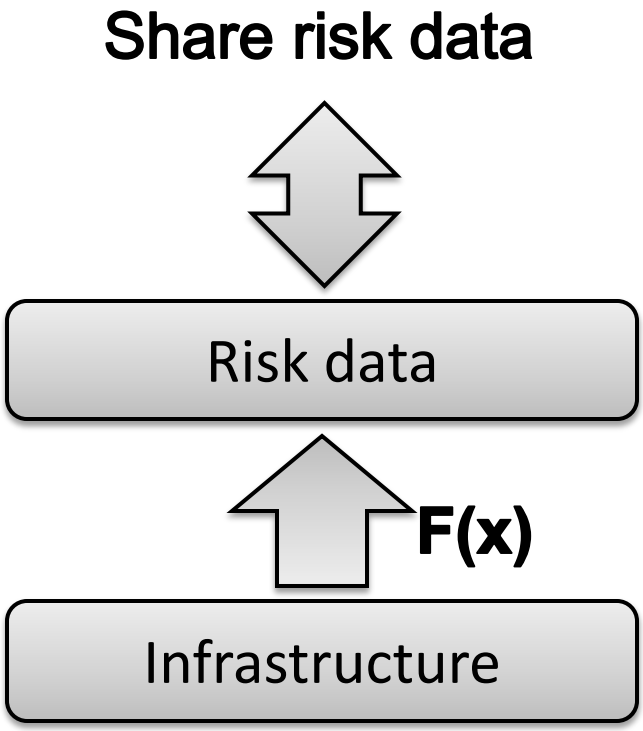
• Exploiting known security properties:
    • Confidentiality (C)
    • Integrity (I)
    • Availability (A)

OBJECTIVES

- Approach to enable real-time (on-line) monitoring of CI states
  - Gather information from the infrastructure and transform it to risk related information

- Abstract the data and express this information in terms of CIA

- Enable sharing with interdependent services/infrastructures



A THREE-STEP APPROACH

- **Off-line risk assessment**: Identification of the interdependency functional model based on a complete risk assessment

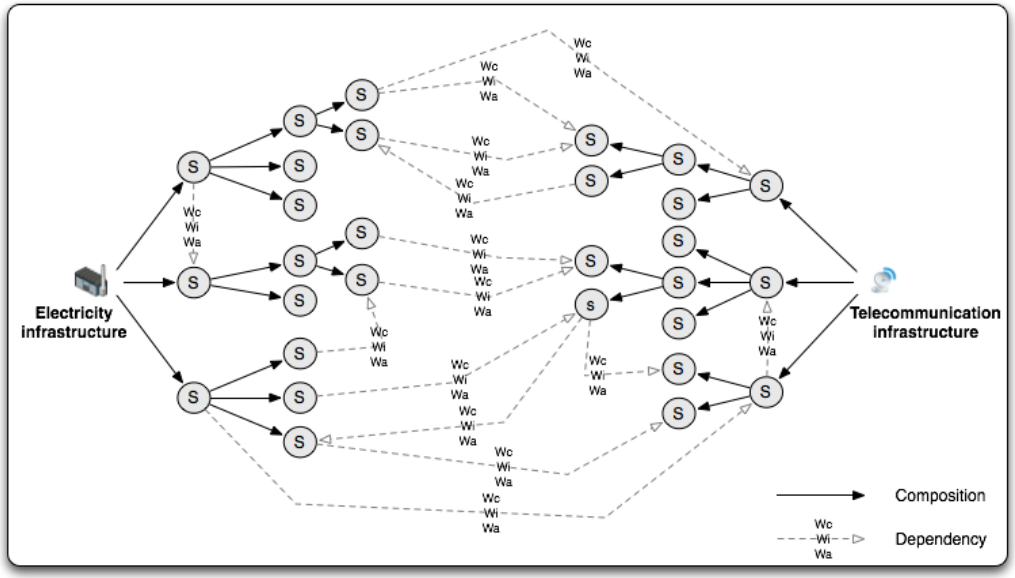
- **Measurement aggregation**: Aggregating real measurements into abstract service risk-related security properties

- **On-line risk monitoring**: Monitoring security risks of services

Off-line risk assessment

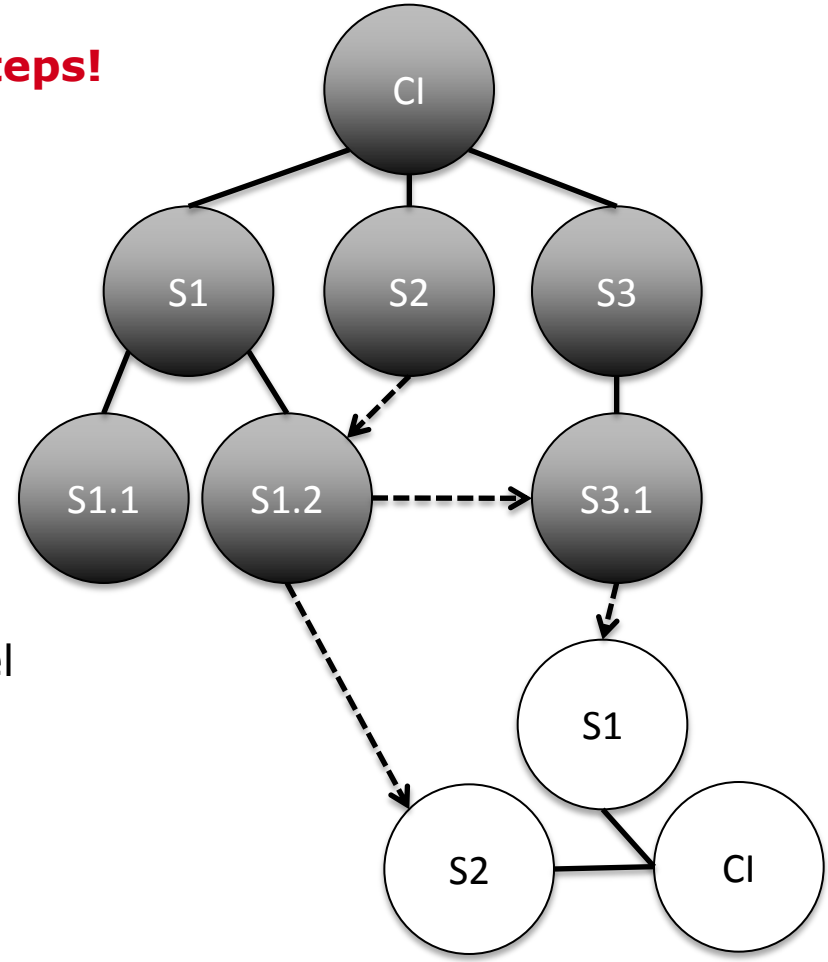
OFF-LINE RISK ASSESSMENT

- Crucial for success of security model
  - Good risk assessment is essential for capturing the state of the CI
- Aims to produce service oriented interdependency functional model



OFF-LINE RISK ASSESSMENT in 5 steps!

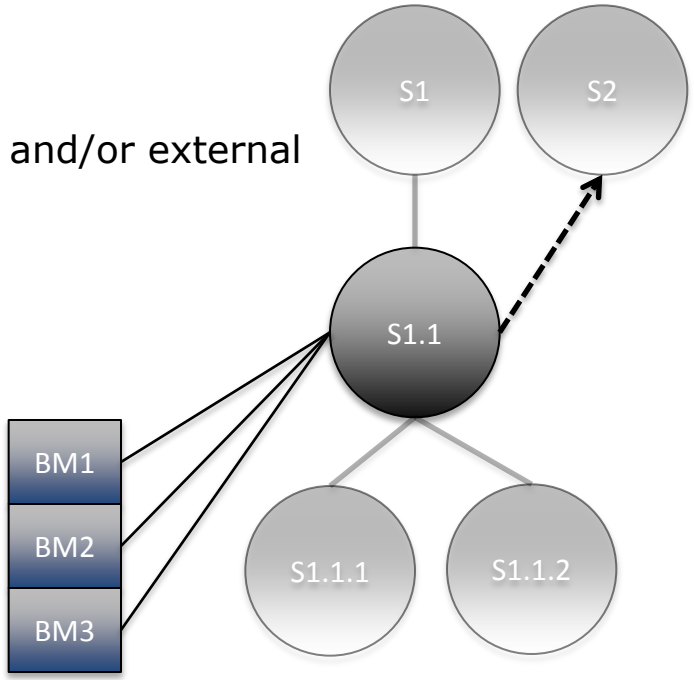
- Identify services
- Identify interdependencies
  - with internal services
  - with external services
- Weight interdependencies
  - contribution to CIA
- Identify base measures at service level
  - to capture service state
  - with confidence of measurement (AL)
- Weight base measures
  - contribution to CIA



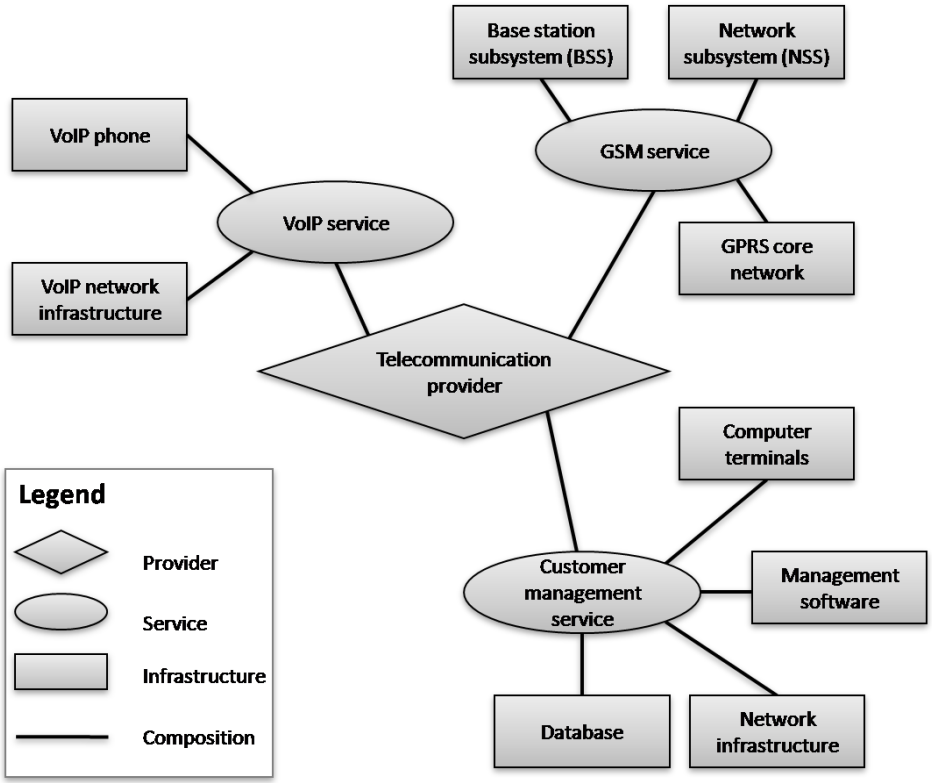
OUTPUTS

- Service oriented interdependency functional model
  - with CI services decomposition

- For each service:
  - super service and sub-services
  - weighted interdependencies between internal and/or external services
  - base measurements to capture service state
    - contribution to CIA
    - confidence expressed as assurance level



ILLUSTRATIVE EXAMPLE



Base station subsystem (BSS)				
Base measure	WC	WI	WA	AL
Network coverage	0	0.2	0.5	3
Component failure	0	0.6	0	4
…	…	…	…	…

BSS Network coverage		
Value	Level	Interval
1	Not reached	[10% ; ∞[
2	Weak	[6% ; 10%[
3	Acceptable	[3% ; 6%[
4	Correct	[1% ; 3%[
5	Reached	[0% ; 1%[

Measurement aggregation

MEASUREMENT AGGREGATION

• Continuous step, using the service oriented interdependency functional model

• Transform real measurements into abstract risk related parameters at service level

• Aggregate sub-services risks levels into upper-service risks levels

Risk level	Interpretation	Value
RL 1	Small	1
RL 2	Medium	2
RL 3	Strong	3
RL 4	Very strong	4
RL 5	Unacceptable	5

MEASUREMENT AGGREGATION

- From base measurements to risk levels
  - Using deviation of measurement from an expected value
- Risk level aggregation at service level
  - From base measurements
  - From sub-services risks levels
- Assurance level aggregation at service level
- For each service:
  - Risk level for each attribute CIA [1..5]
  - Assurance level for each attribute CIA [1..5]

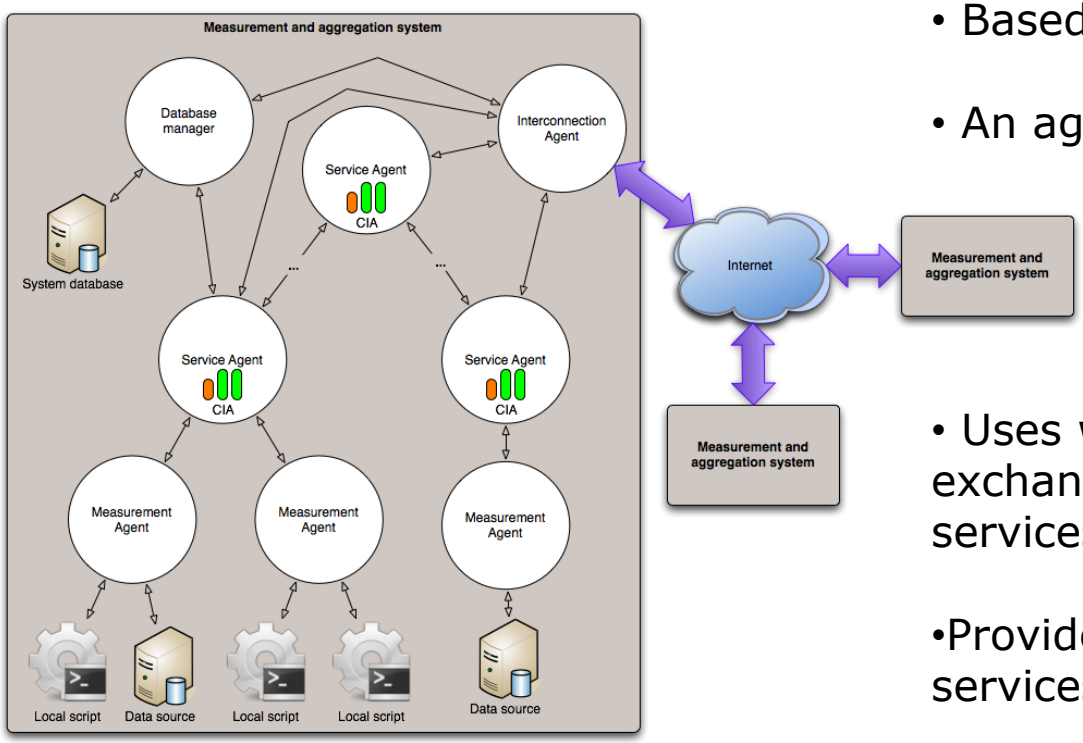
On-line risk monitoring

ON-LINE RISK MONITORING

- Send/receive risk data from interdependent services
- Integration at service level of interdependent service risks levels
  - Using interdependencies weights contribution in terms of CIA
- For each service:
  - Risk level for each attribute CIA [1..5]
  - Assurance level for each attribute CIA [1..5]

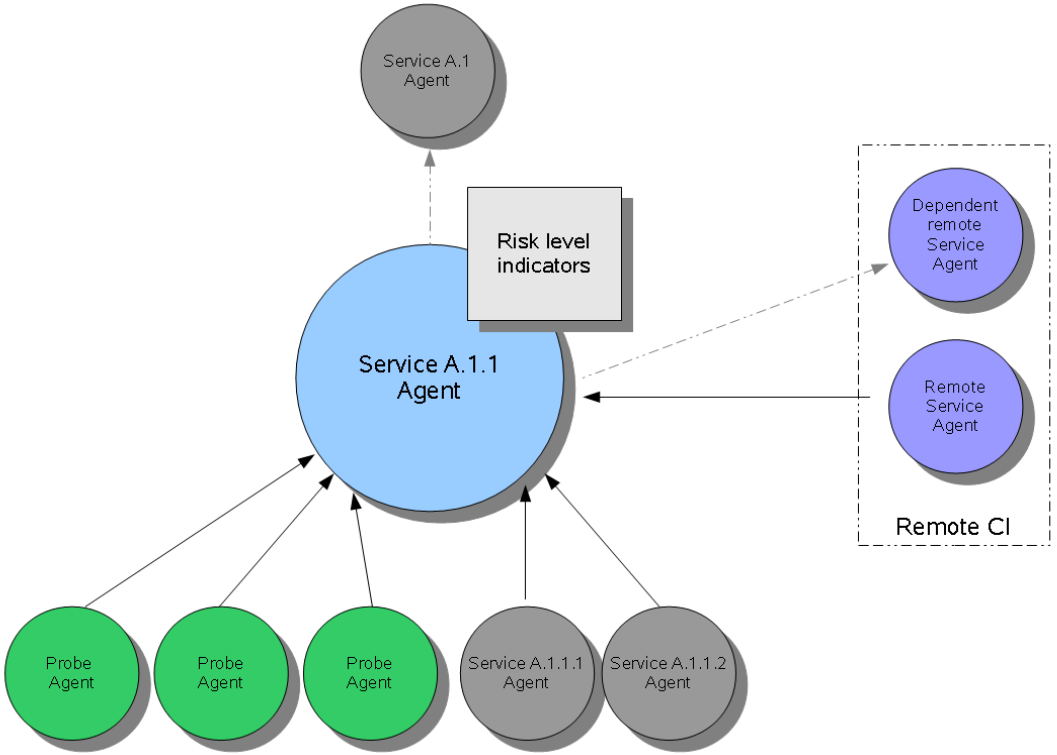
RESCI-MONITOR: a tool

RESCI-MONITOR: a tool

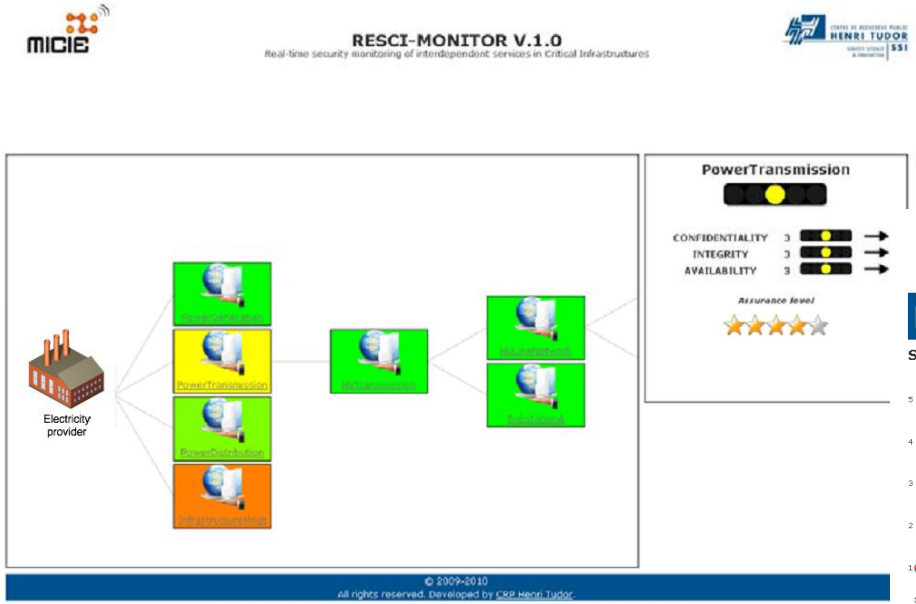


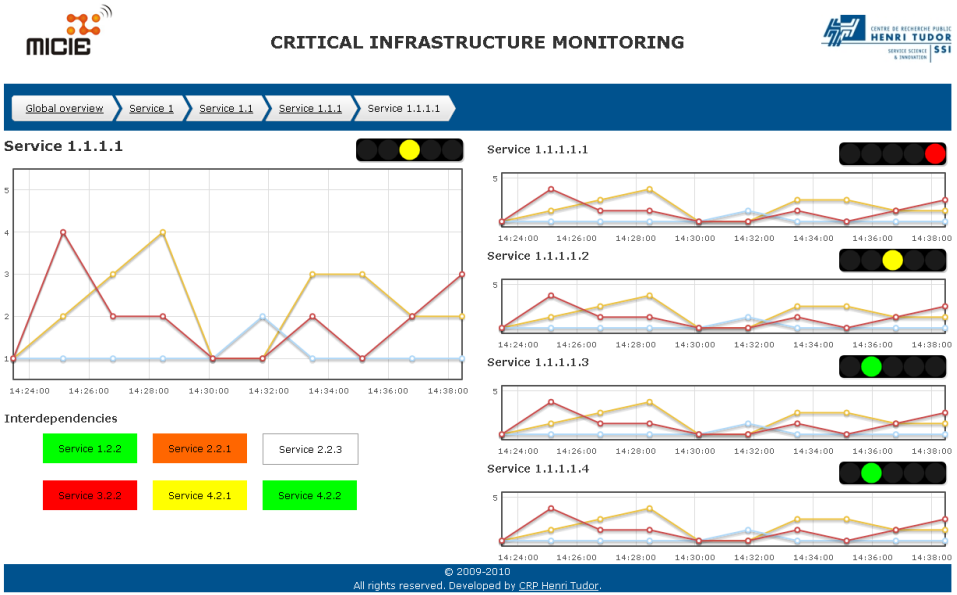
- Based on multi-agent system
- An agent per service
- Uses web-services to exchange interdependent services risk levels
- Provides on-line status of CI services

RESCI-MONITOR: at service level



RESCI-MONITOR: operator GUI





CONCLUSION

Advantages

- Risk-based model
  - Taking into account other parameters than availability
  - Monitor risk related system parameters
- Different nature of infrastructures
  - Small, common set of parameters
  - Make infrastructure comparable
- Information sharing
  - Hide complexity of infrastructure
  - Confidential internal parameters do not need to be shared

Critical evaluation

- Why CIA?
  - Well suited for capturing security system state
  - Easily extendable to include other parameters
- Will providers be willing to share data?
  - Minimum amount of shared data
  - Supporting measures (contracts, SLA, etc.)
- Is too much expert knowledge demanded?
  - Yes (for now)!
  - Find ways to reduce expert knowledge
    - Pattern recognition
    - Self-adapting weights

THANKS FOR YOUR ATTENTION!

Any questions?

jocelyn.aubert@tudor.lu