Semantically Enhanced Resilient and Secure Critical Infrastructure Services

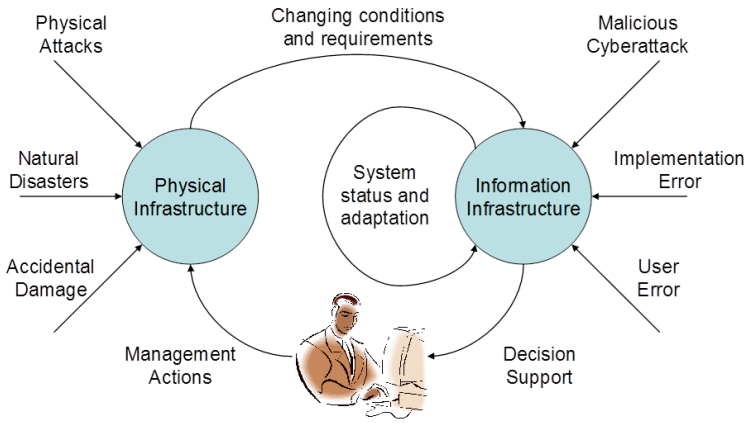
ICT and Security

Critical infrastructure ICT is increasingly interconnected

- information sharing → greater operational efficiency, but also reduced slack and flexibility
- interconnections → new risks from ICT failure cascade effects
- overall → more vulnerable to natural, accidental or malicious disruption

SERSCIS approach: use agile SOA to offset these threats

- adapt ICT components and networks to meet changing security needs
- adapt ICT connections to prevent cascades and contain security threats



Approach

- Model critical infrastructure at design time including ICT interconnections between stakeholders
  - from the perspective of an individual stakeholder
- Use the model to detect system vulnerabilities and controls
  - especially caused or amplified by ICT interconnections
- Use service-oriented adaptation to implement controls
  - service management: manage customer commitments and resource provisioning and regulate customer access to services
  - service composition: manage use of resources and adapt to failures
- Use run-time models to interpret system monitoring data
  - use machine reasoning to determine run-time threats and status
  - use design-time models to suggest responses to system operators

Case Study

Airport Collaborative Decision Making (A-CDM)

- CDM within an airport to better manage aircraft turnaround
- provide predictions about aircraft take-off time (critical inputs to the ATC network)
- creates interdependencies between systems of different levels of security and trustworthiness

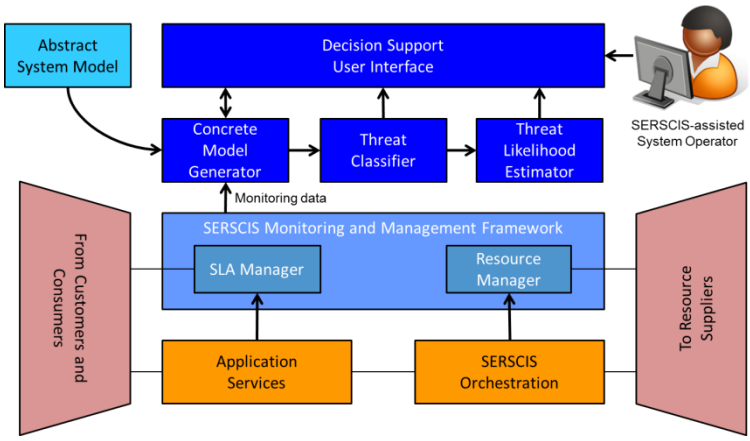
Quality of information is key for:

- accuracy of service scheduling information
- trustworthiness of information sources

Has impact on European-wide air traffic network planning

Technologies

- Semantic system models for critical infrastructure
  - design-time and run-time system
- Autonomic run-time system management framework
  - define and control customer/supplier relationships
- Autonomic run-time system composition tools
  - implement dynamic controls, such as failover
- Semantic decision support tools and user interfaces
  - machine reasoning to determine threat status and possible responses



Email: info@serscis.eu

http://www.serscis.eu

The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement n° 225336, SERSCIS