

**SERSCIS** will use a service-oriented architecture to make interconnected **ICT systems** more manageable, allowing dynamic adaptation to manage changing situations, and counter the **risk amplification effect of interconnectedness**.

To control the resulting ICT components, the project will develop:

- tools and ontologies for modelling critical infrastructure, including ICT components, in order to capture their requirements, behaviour and compositional nature
- system dependability metrics and agreements, and dynamic governance mechanisms, including dynamic trust management
- system composition mechanisms, allowing dynamic discovery and interconnection of component services
- decision support tools that exploit underlying semantic models to provide situational awareness of system status and threats



# Semantically Enhanced Resilient and Secure Critical Infrastructure Services

## Application Areas and Exploitation

SERSCIS will be validated in an information-intensive critical transport infrastructures using highly interconnected ICT networks in two **Application Areas**:

**AIR TRANSPORT** in air traffic flow control and airport services process optimization.

A second scenario to ensure that the technology developed is generic enough to be used in multiple sectors:

**SEA TRANSPORT** in intermodal port community operations

Results Exploitation will cover academic and university technologists as well as critical transport infrastructure end-users and relevant regulatory and standardization bodies.



European Commission  
Information Society and Media



This project has received funding from the European Community's Seventh Framework Programme (FP7/2007–2013)

<http://www.serscis.eu>



The aim of SERSCIS is to develop **adaptive service-oriented technologies** for creating, monitoring and managing secure, resilient and **highly available information systems** underpinning **critical infrastructures**.

The ambition is to develop technologies for such information systems to enable them to **survive faults**, mismanagement and **cyber-attack**, and automatically adapt to **dynamically changing requirements** arising from the direct impact from natural events, accidents and malicious attacks.

## Case Study

Project results will be measured through Case Studies to measure the impact of SERSCIS technology in controlling infrastructure vulnerabilities:

Vulnerabilities caused by external events:

- affecting the critical infrastructure that demand a change in requirements from ICT systems
- compromising the availability of ICT systems

Vulnerabilities caused by the ICT system:

- faults or underperformance
- security breaches making interconnected system components untrustworthy

## System Modelling

Modelling provides a **structured method** for capturing information about systems to provide a **unified understanding**. This can then help successfully deploy a dynamic SOA for CNI.

SERSCIS will generate a methodology that **integrates modelling and management** of services. Modelling frameworks will be developed covering **requirements** and **vulnerabilities**, including failures and cascading effects through interconnected ICT systems.

Human and machine interpretable models will support **Governance** and **Decision Support** for **dependability and trust** as well as reliability in service agreements.

## System Governance

System Governance helps critical infrastructure developers, integrators and operators to define the behaviour of services and systems and to **automatically manage** them such that they remain within the specified limits.

SERSCIS will develop **service dependability agreements**. Component behaviour is monitored with respect to these agreements.

Mechanisms are employed to ensure component behaviour remains within the terms of a service dependability agreement. These mechanisms include **dynamic trust relationships** and **policy-based management**.

## System Composition

SERSCIS will provide innovative **service composition models** capable of mapping overall system dependability and **QoS requirements** onto the workflows it must support.

This workflow can then be **dynamically composed**, configured and **orchestrated** at run-time using the most appropriate ICT services to achieve the required **end-to-end dependability**.

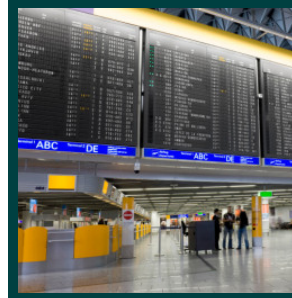
SERSCIS will use a hybrid approach for automatic service composition by combining **semantic reasoning** and applicable **optimization** strategies.

## Decision Support

Decision Support Tools (DSTs) provide **through-life information** to users ranging from designers to auditors to operators. DSTs must **inform** users of **status** to show current system **behaviour** and provide **guidance** on **dealing with failures and threats**.

DSTs in SERSCIS will exploit **semantic models** of ICT systems within CNI to improve users' **situational awareness** and support **Governance**.

DSTs will use the modelled **business, infrastructure and security critical** focused information to develop dashboards for displaying relevant information and prior reasoning.



Mike SurrIDGE  
**Project Coordinator**  
IT Innovation Centre  
2 Venture Road  
Southampton  
SO16 7NP  
UK  
Tel.: +44 23 8076 0834

For more information  
please email:  
[info@serscis.eu](mailto:info@serscis.eu)

