INSPIRE: INcreasing Security and Protection through Infrastructure REsilience

Salvatore D'Antonio
Consorzio Interuniversitario Nazionale per l'Informatica
saldanto@unina.it

SEVENTH FRAMEWORK PROGRAMME

EC Grant Agreement n. 225553

Project summary

- INSPIRE is a two-year small or medium-scale focused research project (STREP)
- Start date: November 1st 2008
- End date: October 31st 2010
- Call for proposals: **Joint Call FP7-ICT-SEC-2007-1 (Critical Infrastructure Protection)**

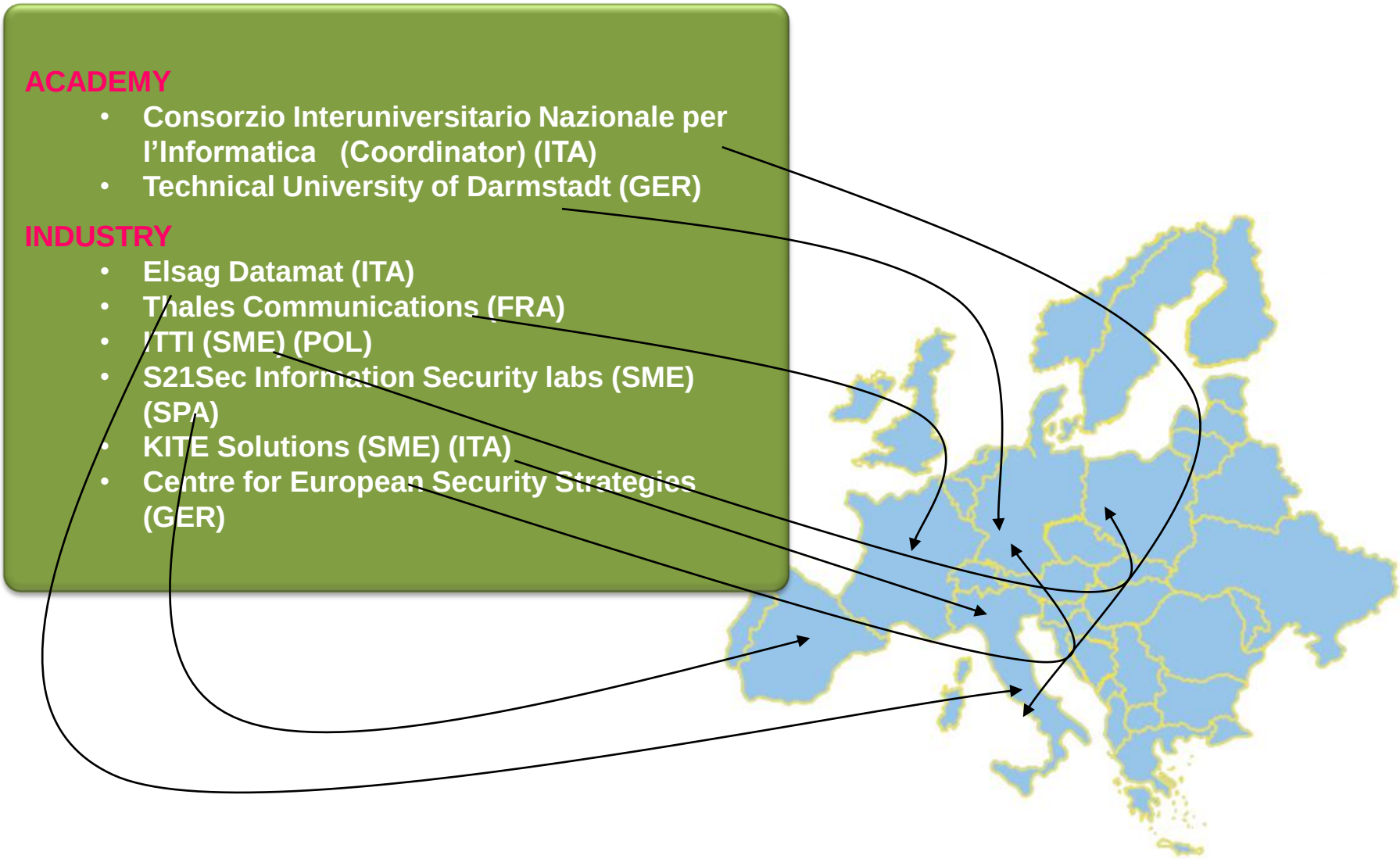
The Consortium

ACADEMY

- **Consorzio Interuniversitario Nazionale per l'Informatica (Coordinator) (ITA)**
- **Technical University of Darmstadt (GER)**

INDUSTRY

- **Elsag Datamat (ITA)**
- **Thales Communications (FRA)**
- **ITTI (SME) (POL)**
- **S21Sec Information Security labs (SME) (SPA)**
- **KITE Solutions (SME) (ITA)**
- **Centre for European Security Strategies (GER)**



Concept and objectives

- Design and development of innovative mechanisms capable to differentiate and prioritize SCADA and Process Control Systems traffic flows
- Design and development of novel techniques which allow network security frameworks to prevent, detect and react to cyber attacks against networked Process Control Systems
- Dissemination and contributions to standards
- Definition of a roadmap for improving the protection of critical information infrastructures

Research challenges

- Analysis and modelling of dependencies between critical infrastructures and underlying communication networks;
- Designing and implementing traffic engineering algorithms to provide SCADA traffic with quantitative guarantees;
- Exploiting peer-to-peer overlay routing mechanisms for improving the resilience of SCADA systems;
- Defining a self-reconfigurable architecture for SCADA systems;
- Development of diagnosis and recovery techniques for SCADA systems;

Expected project results and innovation

- Definition of a comprehensive framework which enables to provide per-flow QoS and resource optimization without using sophisticated scheduling mechanisms
  - While QoS architectures employ scheduling mechanisms to differentiate flows locally at each router, our approach will be to differentiate flows by routing them along different explicit paths (MPLS networks).
- Adoption of P2P architecture to SCADA systems to enhance their resilience
  - Mechanisms for multi-path P2P routing and for secure distributed storage of SCADA data allowing for fault-tolerant data transport
- Definition of an innovative approach to SCADA system diagnosis
  - A distributed framework capable to process in real-time the information produced by multiple data feeds which are scattered over the infrastructure

Peer-to-peer overlay routing for resilient SCADA systems

- P2P overlay networks create a fully decentralized architecture as in SCADA systems
- P2P overlays provide for self-organization and self-healing properties which emphasize the potentials that P2P can play in building resilient SCADA systems
- P2P architectures allow for masking strong heterogeneities in both communication nodes and links making them very attractive for the interconnected by-nature-heterogeneous SCADA critical infrastructures
- P2P overlays suit well for dynamic topologies that future SCADA systems may show as they may integrate dynamic ad hoc networks

P2P overlays in INSPIRE - 1

- The INSPIRE project aims at investigating the characteristics of P2P for the purpose of hardening SCADA systems against a cyber-attack
  - In case real-time message delivery constraints are not being met (due, for example, to a denial of service attack), a P2P overlay network is used to route message floods in an effort to ensure delivery
- Full or partial functionality (graceful degradation) after failures or attacks will be maintained by ensuring the timeliness and reliability of the delivery of sensor data
  - Path and data redundancy techniques will be implemented in order to maintain the required system responsiveness

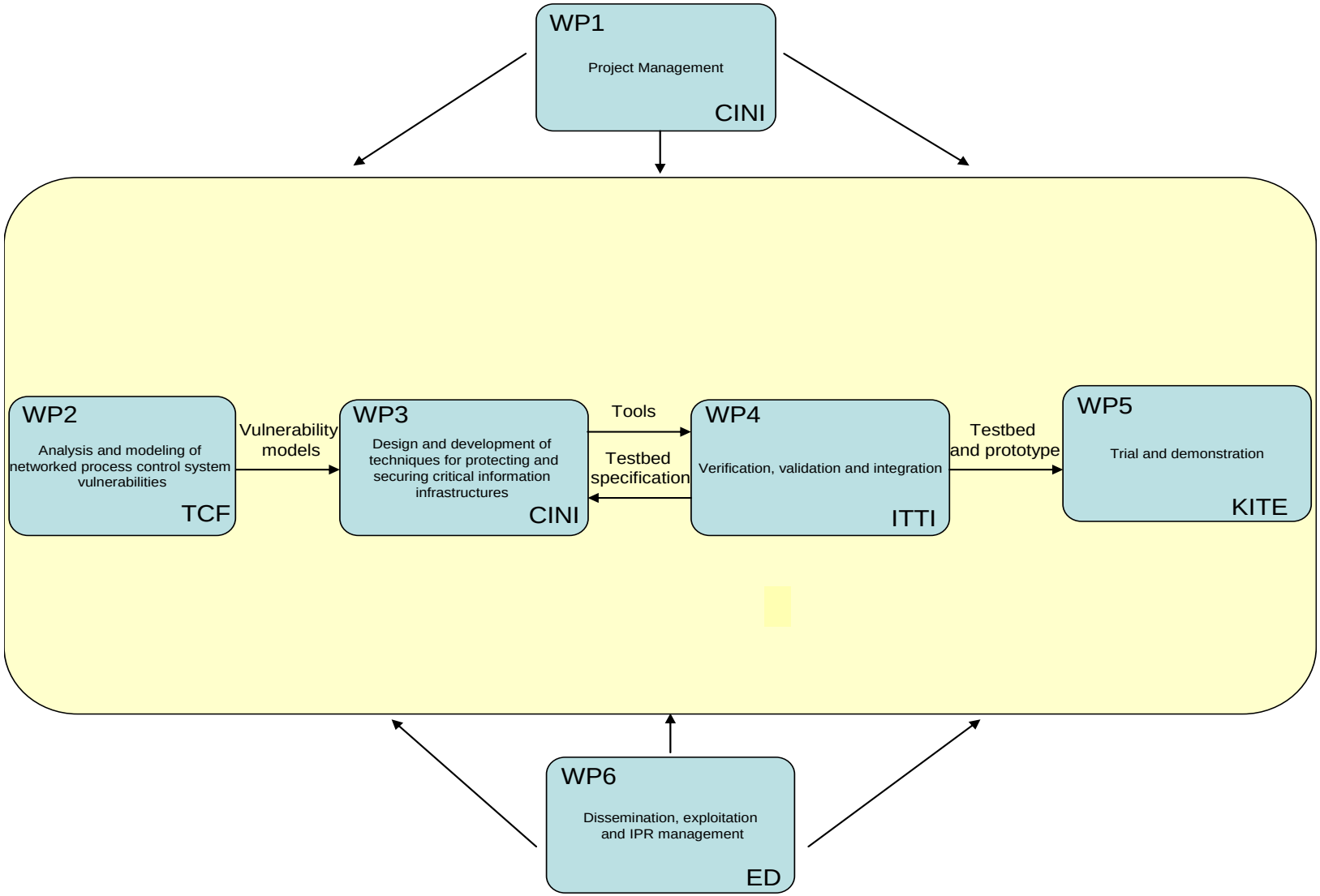
Definition of a self-reconfigurable architecture for SCADA systems

- A list of activities which are key to assure system resiliency includes:
  - error/intrusion detection,
  - fault diagnosis,
  - system degradation,
  - error processing,
  - fault treatment,
  - component re-integration
- INSPIRE aims at designing an architectural framework for handling multiple classes of faults/attacks in a SCADA system
- Use of adaptable parsers that can convert external event formats to an internal flexible structure enabling analysis and processing of collected data
- A Complex Event Processor (CEP) engine looks for patterns of events in a stream of data in order to detect faults/intrusions and to handle them

Development of diagnosis and recovery techniques for SCADA systems

- Evidence is showing that, for complex systems such as SCADA systems, diagnostic activities must collect and filter out data on component behaviour over time
- INSPIRE aims at making advancements in the definition of a distributed diagnosis/reconfiguration framework
- A diagnostic system based on the concept of threshold must be able to:
  - understand the nature of errors occurring in the system
  - judge whether and when some action is necessary
  - trigger the recovery/reconfiguration/repair mechanisms to perform the adequate actions

Project WPs


WP1
Project Management
CINI
WP2
Analysis and modeling of networked process control system vulnerabilities
TCF
Vulnerability models
WP3
Design and development of techniques for protecting and securing critical information infrastructures
CINI
Tools
Testbed specification
WP4
Verification, validation and integration
ITTI
Testbed and prototype
WP5
Trial and demonstration
KITE
WP6
Dissemination, exploitation and IPR management
ED

Questions ?

saldanto@unina.it