INSPIRE: INcreasing Security and Protection through Infrastructure REsilience

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

CRITIS 2008 - Frascati (Italy) - October 14th, 2008

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)**

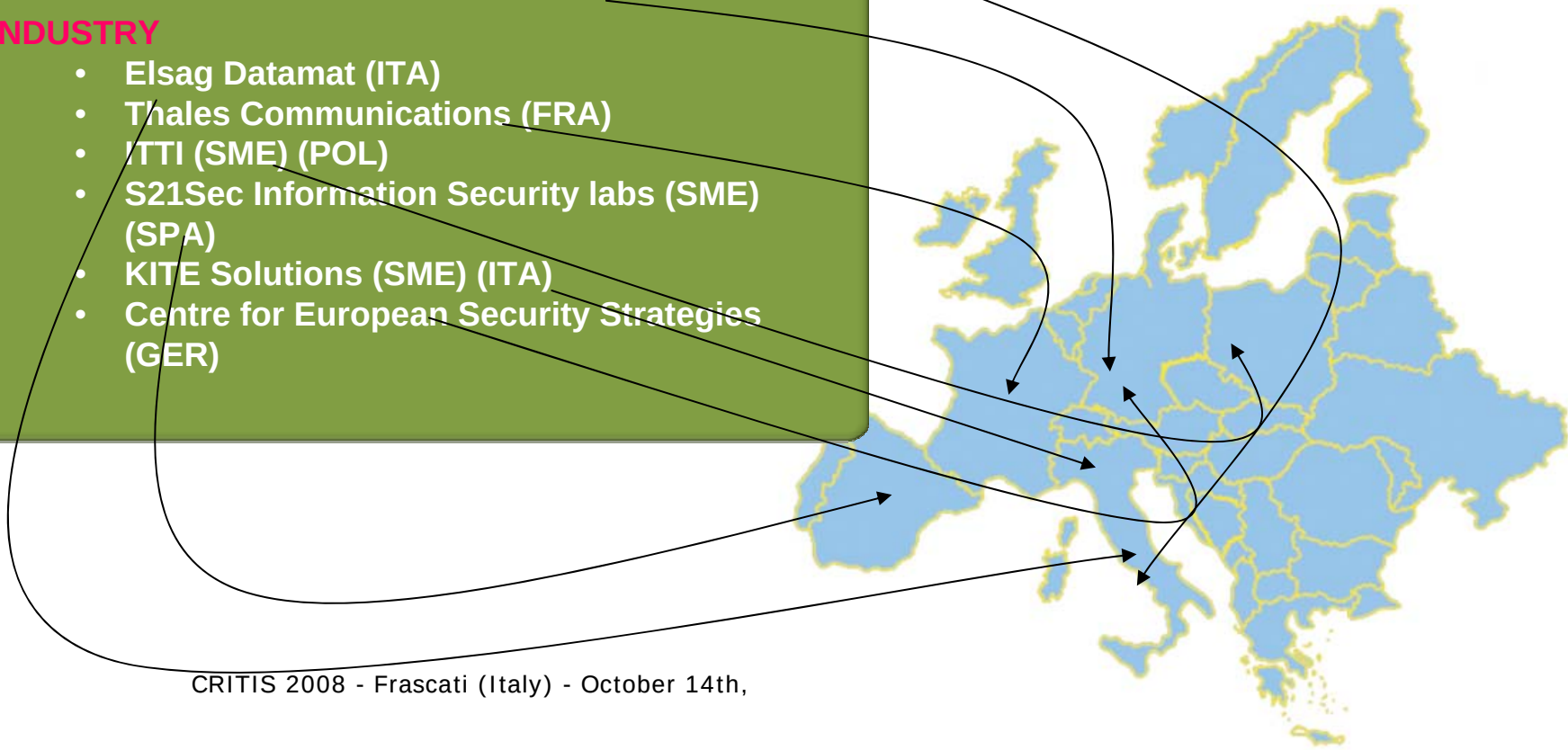
The Consortium

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 protect traffic flows produced by SCADAs and prevent cyber attacks against networked Process Control Systems
- Dissemination and contributions to standards
- Definition of a roadmap for improving the protection of critical information infrastructures

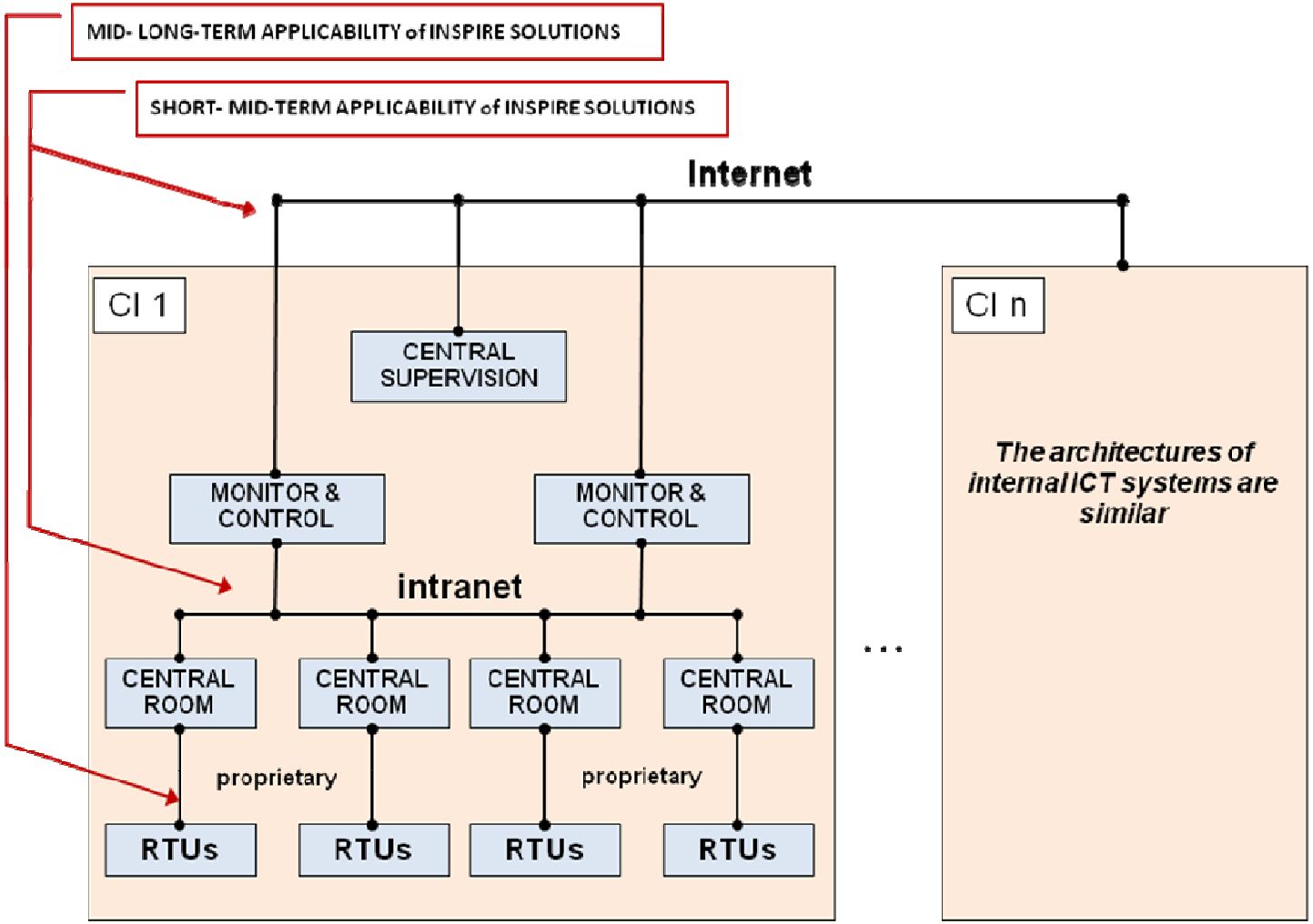
Research challenges

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

Critical Information Infrastructures

- ***Complexity*** - Characterizing the structural properties of the networks is of paramount importance for understanding the complex dynamics of the systems built upon them.
- ***Mobility*** - New kinds of links requiring a proper protection are used to connect critical infrastructures and this protection seems to be even more difficult due to their highly distributed nature, possibility of break away and wireless technology inherent characteristics
- ***Interdependency*** - Protection of a critical infrastructure requires a detailed and comprehensive knowledge of the intradependencies within and interdependencies between the critical systems and the communication network.
- ***Adaptability*** - Communication networks consist of complex collections of non-linear, highly interactive components. To a great extent, they do not have any centralized control, located in a “master centre” and can therefore be understood as a set of complex adaptive systems (CAS).

Applicability of INSPIRE



Expected project results and innovation

- Analysis of dependencies between critical infrastructures and communication networks
  - Models and tools for representing and simulating Large Complex Critical Infrastructures (LCCI)
- 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

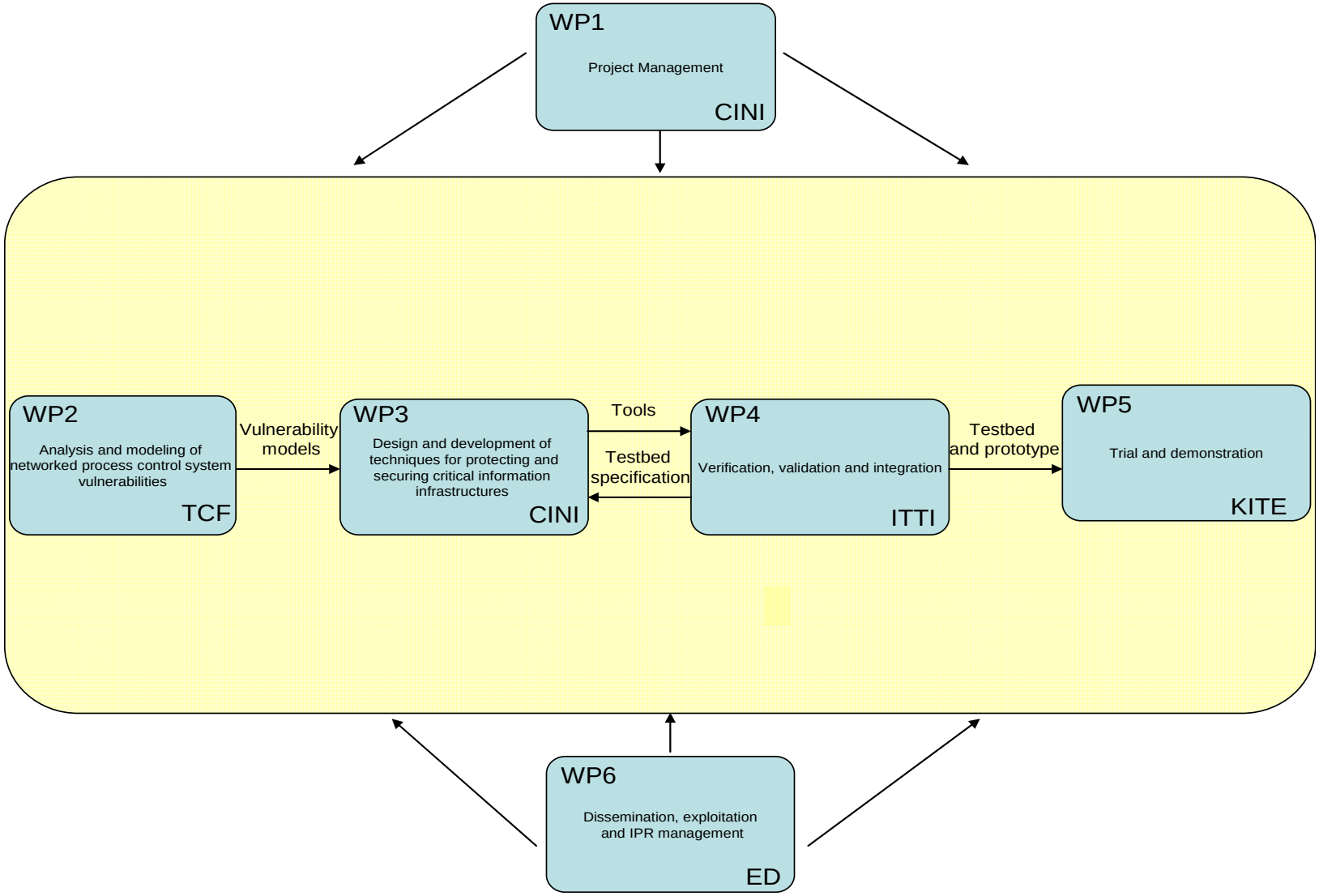
P2P overlays in INSPIRE - 1

- 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

P2P overlays in INSPIRE - 2

- We propose an on-demand use of the P2P overlay network, e.g., upon intrusion detection, otherwise the P2P service is passive
- P2P deployment will not introduce new vulnerabilities to the system
  - This can be preventively achieved through selection of closed P2P systems that enable attack detection and recovery. A closed P2P overlay is characterized by the fact that peers are authorized and known a priori, and that only authorized entities can add/remove peers explicitly/manually if needed.
- We aims at deriving a threat model for P2P-enabled SCADA systems identifying potential vulnerabilities and designing counter-measures for them

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

Dissemination

- Clustering activity
  - IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems)
  - VIKING (Vital Infrastructure, networKs, INformation and control systems management)
  - SERSCIS (Semantically Enhanced Resilient and Secure Critical Infrastructure Services)
  - MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures)
- Participation to standardization bodies (IETF, ETSI)
- Group of Experts: Federutility, ACEA, Telespazio, RFI, AIIC, ENISA

Questions ?

saldanto@unina.it