Subject:
Designing and developing industrial automation systems are undergoing rapid transformation from being islands of automation to large networks of distributed and reconfigurable cyber-physical systems. Cyber-physical systems are usually composed of a set of networked agents, consisting of sensors, actuators, control processing units, communication devices and physical entities as well as their interactions. Monitoring and control of cyber-physical systems, in many cases spread out over small or large geographical areas, are achieved with supervisory control and data acquisition (SCADA). SCADA systems are now particularly being exposed to threats and vulnerabilities they have never been exposed to before. As consequence, cyber-physical systems raise a number of security problems. Most of research for securing SCADA has focused on basic security mechanisms for prevention (authentication, access controls, etc.), detection, and response to security breaches. Despite these efforts, security of cyber-physical systems does not account for considering security concerns in their distributed software architectures at the design time, neither assessing security risks targeting cyber-components, physical entities and their interactions at runtime. The goal of this thesis is to bridge this gap by focusing on: 1) Security-by-design for developing cyber-physical Service Oriented Architecure (SOA) based systems, 2) Vulnerabilities assessment and risk treatment at design and runtime, and 3) Resilient control to enable end-to-end security policies in distributed and dynamic environments.

Keywords:
industrial control systems, SCADA, cyber-physical systems, service oriented architectures (SOA), risk managements, attack diagnosis, security analysis, system resilience, security policies

Expected collaborations:
the work on security will be conducted in collaboration with the Cloud and Autonomic Computing (CAC) Center at the University of Arizona (USA). The work on cyber-physical systems is conducted in collaboration with PERSYVAL-Lab, Grenoble, France

Background required from the applicant:
Master degree in information security is highly recommended. A master degree in Information System is required with a strong motivation to learn foundation of information security

Existence of a PDF file detailing the proposal ("yes" or "no") : yes