Research Partnership Proposal
Partner Search for R&D project

PS FP7/H2020 - Security - Reference Model for Standardizatio of Industrial System Trustworthiness (Privacy, Safety, Security

Own reference: ASQF - Jan DeMeer Deadline: 21/01/2013

Abstract

A compound research and industrial network for software competence based in the German Capital Region is looking for project partners for a FP7/H2020 project.
The project aims at developing a Stakeholder-based Reference Model for implementing trustworthy system architectures.
Project partners in the fields of Software Security and Privacy, Software Engineering with the competences in Model-based Testing, SW Development/Design Methods for Large Systems, Sensor Technology etc, are sought for.

Description

The basic objective of this project is to provide a Reference Model (RM) that makes Eternal Systems (Ultra-large Scaled Systems or, for short the Grid) “stable” against failures and tampering attacks.
This is achieved by keeping control of eternal system processing by authorized Stakeholders, e.g. a Grid Control Centre. The managed eternal system - even being a target of tampering or malfunctioned system behavior must be kept in an acceptable operative "stable" state.
It is planned to develop the RM in tight cooperation with national (DIN) and International (ISO/IEC, ETSI) standardization bodies, especially in the areas SC27 (Security), SC38 (Cloud) ETSI ISI/R2GS (System/Organization Security) and others not able to be mentioned here.
The coordinator is active in Security Architecture Research for Standardization. We need competences in practical Engineering of Ultra-Large Scaled Systems, such as Grids, Clouds, Traffic or Logistics Systems, IT Security Technologies, Cross-Domain operating (Publish-Subscribe) Middlewares, Sensor Networking and Control Technologies.

Technical specifications

The assumption of co-existence of malfunctioning with normative operation presupposes that the stakeholder authorized to control the grid must itself be free from tampering attacks, whic is achieved by securing the control stakeholder's domain by the invented safe & secure Perimeter Technology. This technology is implemented according to the requirements of the Common Criteria [ISO/IEC 15408]. (Notice: all stakeholder behavior of a perimeterized Doma is called “inside” whereas everything that happens elsewhere in the grid is called “outside”, i.e inside behaviour is opaque == private - thus secure, and outside behaviour is open == public thus vulnerable.)
From the secured control domain, observations and measurements are achieved by appropriat testing or sensoring technology which are interconnected to critical grid components to be observed. The observed information is fed back to some controlling stakeholder that is entitled to make decisions – with respect to given business or quality goals and finally will generate

controlling commands to the grid or to some (Cloud) Service Computation Provider.

Technology keywords

- Communications Protocols, Interoperability
- IT and Telematics Applications
- Process control and logistics
- Quality Standards
- Rational use of energy

Collaboration details

- Type of partners sought: SME, Industry, Research Organization

- Specific area of activity of the partner: Security, SoA, SW Design & Testing, System Control, Formal Methods, Middleware, Enterprise & System Management

- Task to be performed by the partner sought: Project, Work Package Management, Technical Expert from all fields mentioned above, plus Field Testers, Demonstrators, Developers, Designers

- Size: SME-, Industry-, Research- seized

- Experience: Regional/National/International Stakeholderships in the area of Large-scaled Systems such as Grid or Cloud Architectures.

Targeted countries

- All

Profile owner: Other , 11 - 50 employees

EEN Contact

Alexandra Pohl
Phone: +49-331/6603232 , Fax: +49-331/6603235
E-mail: alexandra.pohl@zab-brandenburg.de