CRUTIAL

CRitical UTility InfrastructurAL Resilience

An Overview

Felicita Di Giandomenico
ISTI-CNR, Pisa, Italy
felicita.digiandomenico@isti.cnr.it

CRUTIAL

CRitical Utility InfrastructurAL Resilience

Specific Targeted Research Project: FP6-2004-IST-4-027513

EU strategic objective: Towards a global dependability and security framework

Duration: January 2006 - December 2008

Coordinator: CESI RICERCA

CRUTIAL Consortium

CESIRICERCA

Network and Infrastructures Department

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DE LISBOA

Faculty of Sciences

University of Lisboa

LAAS

LAAS-CNRS
Centre National de la
Recherche Scientifique

ISTI
ISTITUTO DI SCIENZA E TECNOLOGIE
DELL'INFORMAZIONE "A. FAEDO"

Consiglio Nazionale delle Ricerche

KU LEUVEN

electa

Katholieke Universiteit Leuven

cnit

consorzio nazionale
interuniversitario
per le telecomunicazioni

Research Area: **Critical Information Infrastructure Protection - CIIP**

Focus on: **Infrastructures operated by Power Utilities**

- Power grids
- Control applications/Automation systems
- Information Systems
- Communication Systems

Vision: **Resilient distributed power control in spite of threats to the information and control infrastructures**

Objectives:

- Provide **modelling approaches** for understanding and mastering the various **interdependencies** among power, control, communication and information infrastructures
- Investigate **distributed architectures** enabling dependable control and management of the power grid

Motivations

Resilience of *critical utility infrastructures* needs to be improved.

- SCADA systems are **real-time** sys with some **fault-tolerance** concern classically **not** designed to be widely **distributed** or remotely accessed or **open**, and designed w/o **security** in mind
- Power utilities infrastructures are the target of **new threats vulnerabilities** emerging from tight coupling of power, control, communication and information infrastructures and from evolving control systems
- Risk is not well mastered
  - current configurations probably risk far more damaging **failure scenarios** than anticipated

Challenge

To make power control resilient in spite of threats to their information and communication infrastructures

Research Agenda

- **Analysis of critical scenarios**
  - in which faults in the information infrastructure provoke serious impacts on the controlled electric power infrastructure
- **Investigation of models**
  - that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures
- **Investigation of distributed architectures**
  - enabling trustworthy control and management of the power grid
- **Analysis and evaluation of control system scenarios**
  - to provide support for the quantitative and qualitative analysis of the devised solutions

Identification and description of Control System Scenarios

- **Identification of scenarios**
  - analysis of the **existing control** systems
    - existing vulnerabilities vs. emerging issues
  - investigation of **new control** applications
    - distributed generation and microgrids

- **Description of identified scenarios**
  - identification of **interdependencies**
  - definitions of appropriate **measures for resilience**

Interdependencies modelling

- **Methodologies and a conceptual modeling framework**
  - **Characterize and analyze interdependencies between the information infrastructures and the electric power infrastructure**
  - **Assess the impact of interdependencies on the resilience of these infrastructures wrt occurrence of critical outages**
- **Major challenges:**
  - **Model types of outages characteristic of interdependent critical infrastructures (*Cascading outages, Escalating outages and Common cause outages)***
  - **Develop an integrated modeling and evaluation approach taking into account accidental and malicious faults of the different infrastructures**

- **Model of individual infrastructures in isolation vs models combining multiple interdipendent infrastructures;**
- **Cope with complexity**
  - Hierarchical and compositional modeling approach
- **Analyze interdependences under different operation phases and regimes, with different configurations, behaviors and requirements**
  - Multi-phased modeling approach
- **Describe scenarios that involve variables with different orders of magnitude, or system parameters that are only partially defined**
  - Stiffness problem and aggregation techniques
- **Develop dynamic online modeling and evaluation methodologies to support adaptive reconfiguration strategies**
  - From off-line to on-line evaluation

Testbed development

Two testbeds, integrating the electric power system and the information infrastructure

Objectives of testbeds:

- implementation of control applications (hierarchical centralized and decentralized ones) in order to better identify them;
- usage for architectural patterns;
- assessment of interdependencies, complementary to the modelling

- The first platform will be based on **power electronic converters** that are controlled from PCs interconnected over an open communication network (at K.U.Leuven)
- The latter platform will consist of **power station controllers** on a real-time control network, interconnected to corporate and control centre networks (at CESI RICERCA)

Architectural solutions

- Definition of the overall architecture framework
  - Intrusion-tolerant architectures with and without trusted components
  - Architectural hybridization to enable trusted-trustworthy subsystem operation

- Middleware services and protocols
  - Fault and Intrusion tolerant services and protocols
  - Using distinct techniques that address different levels of criticality of the architecture
  - Able to support a diverse set of requirements from the applications

- **Protection mechanisms**
  - **Develop a framework to express a global security policy for the various organizations/departments involved in the infrastructure**
  - **Base this framework on the Organisation-Based Access Control (OrBAC) model**

- **Monitoring mechanisms**
  - **Devise monitoring mechanisms allowing on-line adaptation to situations not predicted.**

    Main tasks:
    - **Fault diagnosis**
    - **System reconfiguration**

Analysis and evaluation of Control System Scenarios

- **Set-up of the modelling environment**

  - **Selection of tools adequate to model critical infrastructure peculiarities**
  - **Inclusion of different formalisms and relative compositional rules (support for layer and/or hierarchies) and solution algorithms under an integrator tool (candidates: DrawNET and Möbius)**

- **Model based evaluation**

  - **Evaluation of defined services and protocols, in terms of metrics that capture the interdependence aspects**

- **Experimental validation of architectural solutions**

  - **Validate some of the trusted run-time components of the architecture against attacks prevention or intrusions tolerance**

More details at

http://crutial.cesiricerca.it