On a framework for modeling and analyzing interdependencies in Electrical Power Systems

Felicita di Giandomenico
CNR-ISTI
felicita.digiandomenico@isti.cnr.it
Joint work with Silvano Chiaradonna (CNR-ISTI) and Paolo Lollini (Univ. of Florence)

Workshop on Critical Infrastructure Protection
51st Meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance
Guadeloupe, January 10-14, 2007

CRUTIAL CRitical UTility InfrastructurAL resilience

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

Outline

- Context and objectives
- Description of the Electrical Power System
    - The electrical infrastructure
    - The Information technology based control system
- Failure model of EPS
- State definition for EI and ITCS
- The Interdependencies between EI and ITCS
- Relevant aspects of the EPS modeling framework
- Feasibility study
- Conclusions and next steps

The context - 1

- Economy, security and quality of life increasingly depend on the resiliency of a number of **critical infrastructures**
- **Critical infrastructures** are complex collections of interacting systems and components, communicating through multiple heterogeneous networks
- **Interdependencies** increase vulnerability, as they give rise to multiple error propagation channels from one infrastructure to another
- Therefore, the **impact of infrastructure components failures** and their **severity** can becomes much higher and more difficult to foresee compared to failures confined to single infrastructures

➔ **Analysis of infrastructures components interactions is crucial to understand and characterize interdependencies**

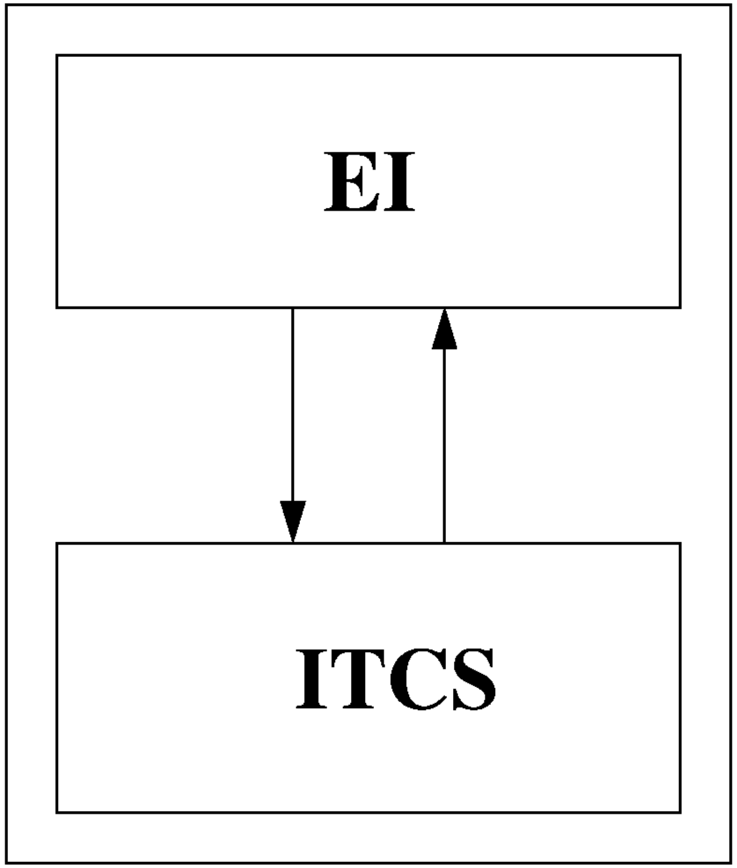
The context - 2

- **Electrical Power Systems** are prominent representatives of CI
- Interdependencies between the electrical power grid (**EI**) and the control system infrastructure (**ITCS**) have been responsible of major power grid blackouts
- The Consortium for Electric Reliability Technology Solutions (**CERTS**) is particularly active in studying cascading failures
- However, existing models **do not explicitly account for** the complex interactions between EI and ITCS
- The EU STREP 027513 **CRUTIAL** project is addressing the analysis and management of interdependencies and of the resulting operational risk

Objective

- Define a conceptual **modeling framework** well suited to characterize and analyze the **interdependencies** between
  - the information infrastructure
  - the controlled power infrastructure
- The focus is on **interdependence-related failure**:
  - Cascading failures
  - Escalating failures
  - Common-cause failures
- The goal is to **quantitatively assess** their impact on the resilience of these infrastructures

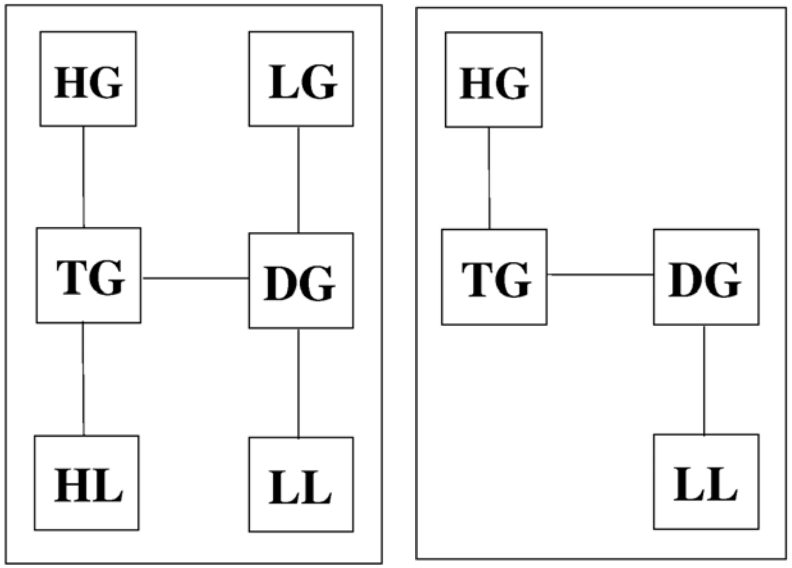
Electrical Power System (EPS) characterization



- The EPS system can be seen as composed of two interacting sub-systems:
  - The **Electric Infrastructure** (EI);
  - The **Information Technology Based Control System** (ITCS).
- An event (e.g. failure or recovery) that occurs in one sub-system can “affect” the behavior of the other sub-system (**interdependencies**).

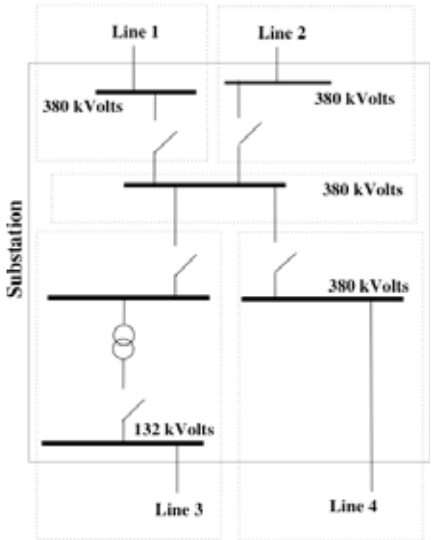
The Electrical Infrastructure

The **EI** produces and transports the electric power to the final users

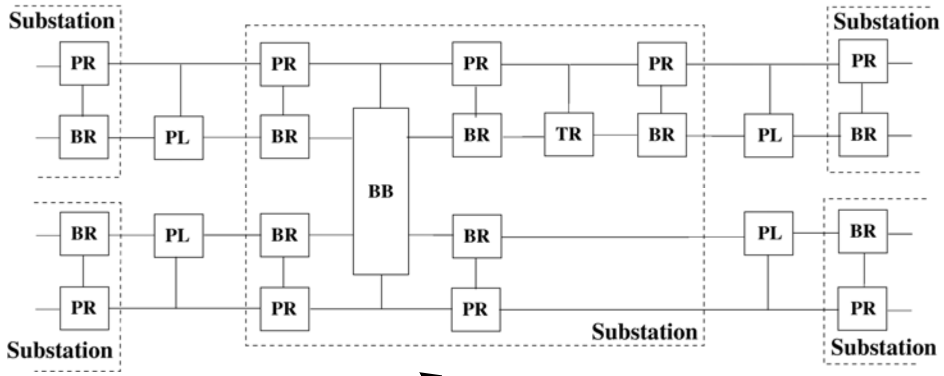


- **HG**: high voltage generation plant
- **LG**: medium/low voltage generation plant
- **TG**: transmission grid
- **DG**: distribution grid
- **HL**: huge voltage load
- **LL**: medium and low voltage load

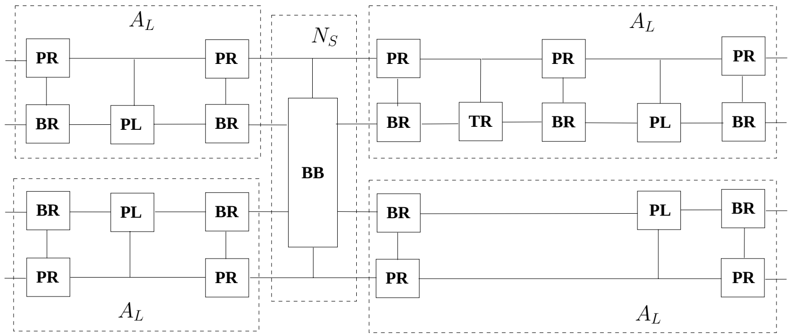
Focusing on substation and power lines

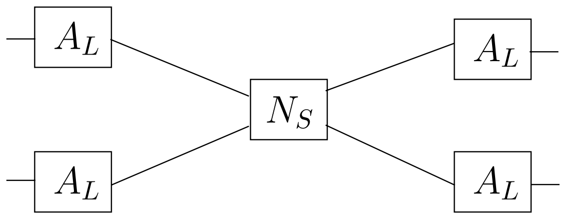


Physical view

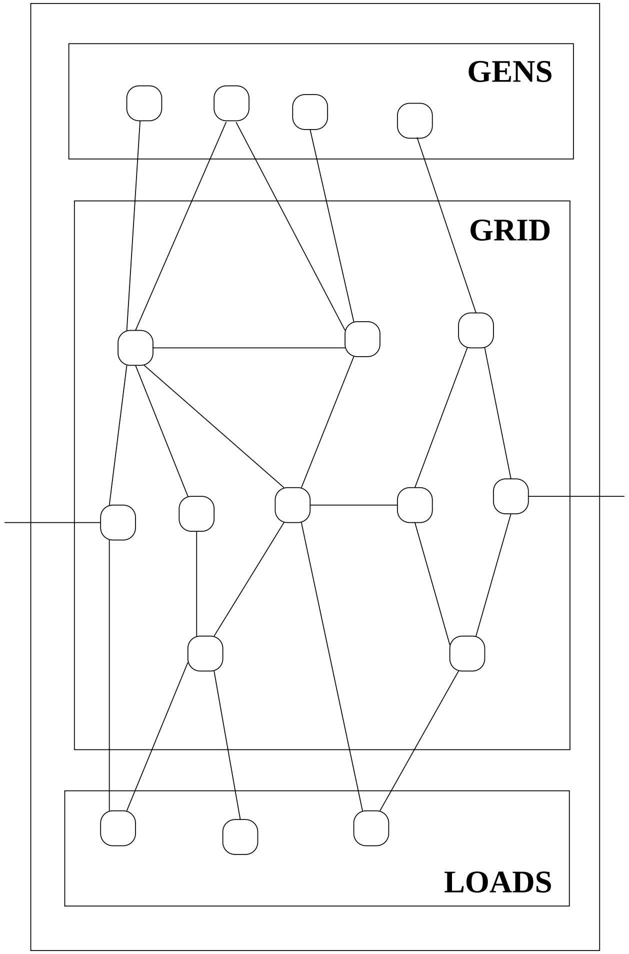


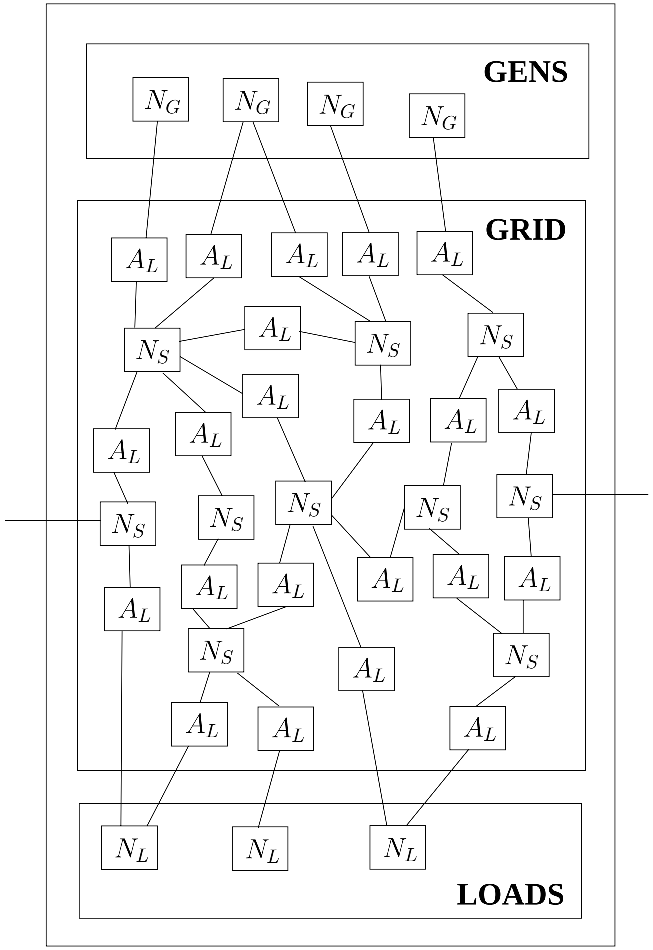
Logical views





Example of Topology for a TG





meshed graph

Logical scheme

The ITCS system

ITCS is in charge of:

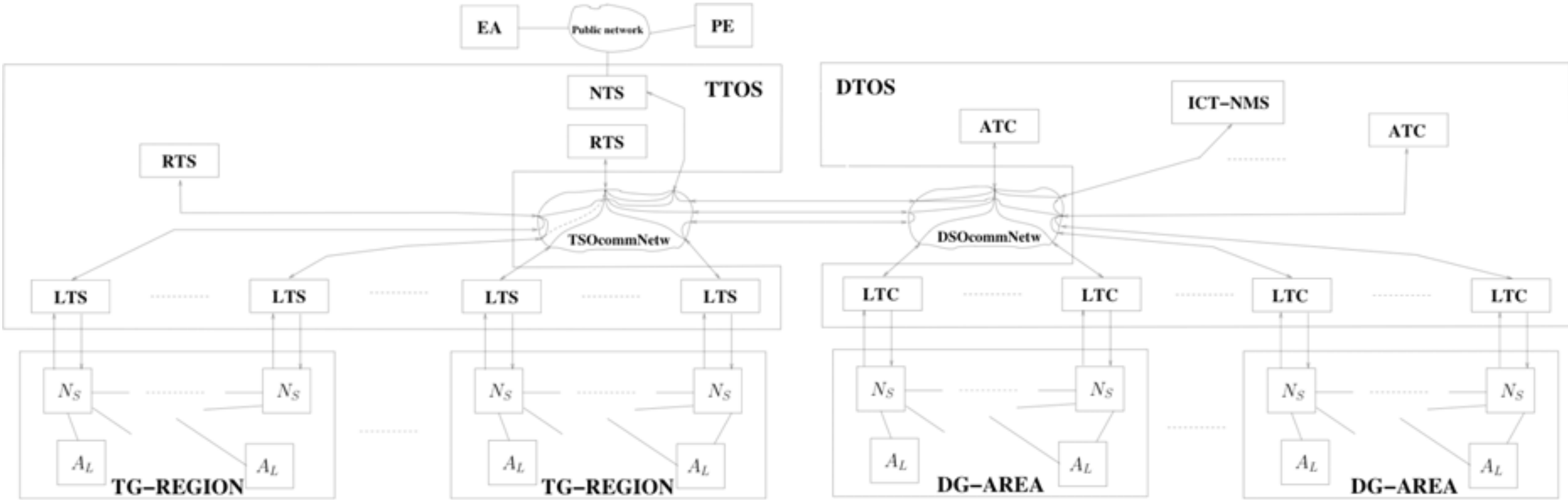
- Assuring availability of EI
- Enhancing QoS (frequency and voltage regulation)
- Optimizing generators and substations management

Logical components of ITCS:

- Protection system;
- Frequency and voltage regulation systems;
- Tele-operation systems (DTOS for the DG and TTOS for the TG)

The logical ITCS components interact through a hierarchical structure, using public and/or private networks to exchange exchange grid status information and control data

Logical structure of TTOS and DTOS



LTS (Local Tele-control System), **RTS** (Regional Tele-control System) and **NTS** (National TelecontrolSystem) of TTOS,
LTC (LocalTele-control System) and **ATC** (AreaTele-control System) of DTOS

These components differ for their criticality and for the locality of their decisions.

EI Failure Model

1. **Transient or permanent disconnection** of a component **N_S, N_G, N_L and A_L** **with consequent disconnection** of one or more components from the grid. **Transient or permanent failed disconnection** of a component **N_S, N_G, N_L and A_L** **without isolation** from the grid.

2. **Transient or permanent overloads** of **N_S and A_L. Unexpected reduction of production** of **N_G**. **Unexpected increase or reduction of demand** of **N_L**. **Voltage collapse**. **Under-frequency and loss of synchronism**.

Disconnections imply changes in the topology T of the grid and consequent changes of V, F, I, A, P and Q.

The disruptions at point 2 represent changes of the electrical parameters of the components of the grid N_S, N_G, N_L and A_L and do not necessarily imply changes in T.

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

ITCS Failure Model

- **The failures of the ITCS components can be summarized in:**
  - omission failure,
  - time failure,
  - value failure and
  - byzantine failure.

Here the focus is on the failures and not on their causes (internal HW/SW faults, malicious attacks, etc.).

State definitions

- EI status is defined by an **hybrid state** S_{EI}:

  S_{EI}=(discrete part; continuous part)

  In particular: $S_{EI}=(T; V,F,I,A,P,Q)$,

  where

  T=Topology of the grid

  V,F,I,A,P,Q= Voltage, Frequency, Current flow, Angle, Active and Reactive Power

- ITCS status is defined by a **discrete state** S_{ITCS}:

  S_{ITCS}=(discrete part)

  E.g.: S_{ITCS}=(Working, Partially failed, Lessened, Recovery, …)

Why an hybrid state for EI?

- **The electrical values associated to an EI component** (e.g. voltage, current flow, …) **are important**, since they influence:
  - The time to disruption of the component
  - The correct application of a protection
  - The type of reconfiguration action to be applied (more or less "aggressive", timed-constrained, …)
  - …
- **The topology of the EI is important**, since it influences:
  - The propagation of a disruption from an EI component to its contiguous components
  - The type of reconfiguration action to be applied (local, regional, national, …)
  - …

Causes of state changes

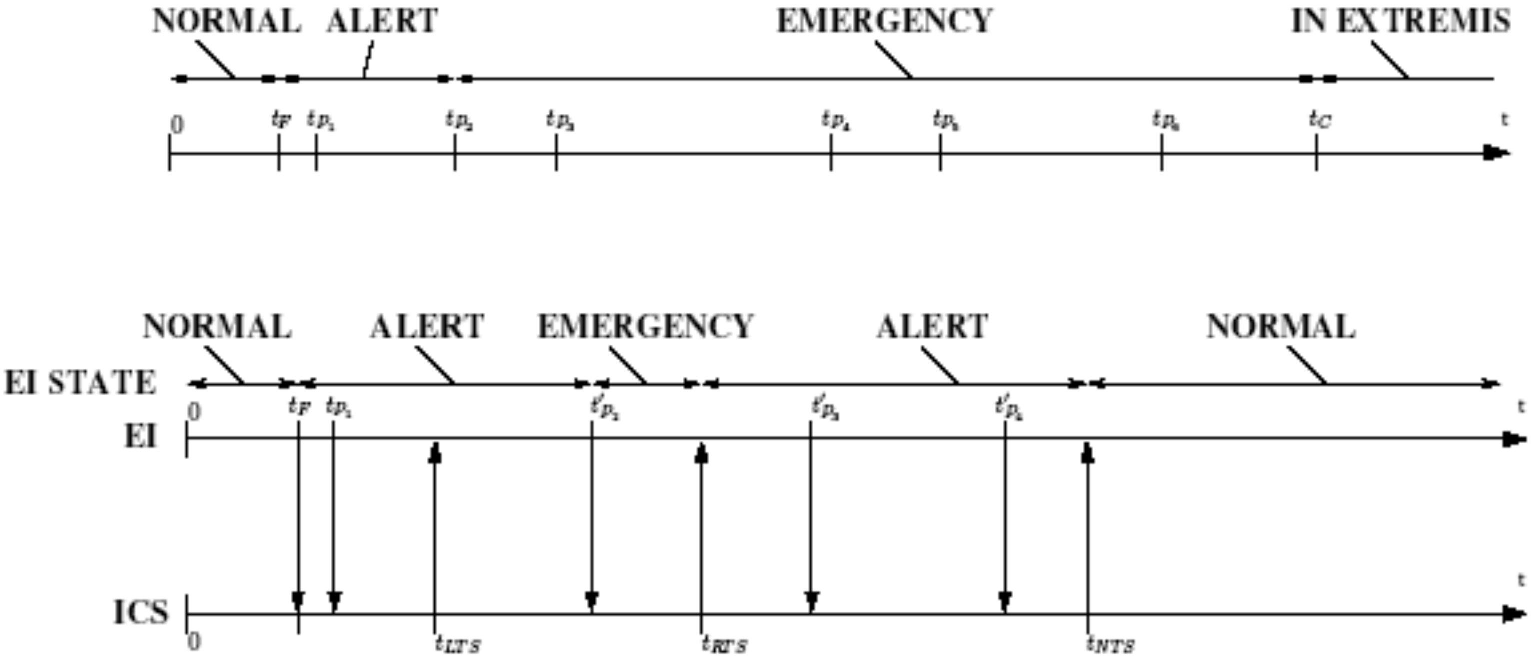
- **The state of EI changes in case of**:
  – Disruption of an EI component
  – Activation of a local protection
  – Reconfiguration action by ITCS (including erroneous, delayed or not required reconfiguration)
- **The state of ITCS changes in case of:**
  – Failure/recovery of an ITCS component
  – Disruption of the EI

Interdependencies

- $S_{ITCS} \rightarrow S_{EI}$
  - Impact on T and/or the values of V,F,I,A,P,Q
    - E.g. a value failure of LTS (incorrect closing or opening of the power line A_L) - such failure can also impact on connected RTS components
- $S_{EI} \rightarrow S_{ITCS}$
  - E.g. a failure in the EI causes a partial black-out that could reduce the performance of the private or public networks used by ITCS, or isolate part of the ITCS.
- $(S_{EI}$ and $S_{ITCS}) \rightarrow (S_{EI}$ or $S_{ITCS})$
  - E.g. an ITCS component fails (omission failure) and does not isolate an EI component affected by a disruption

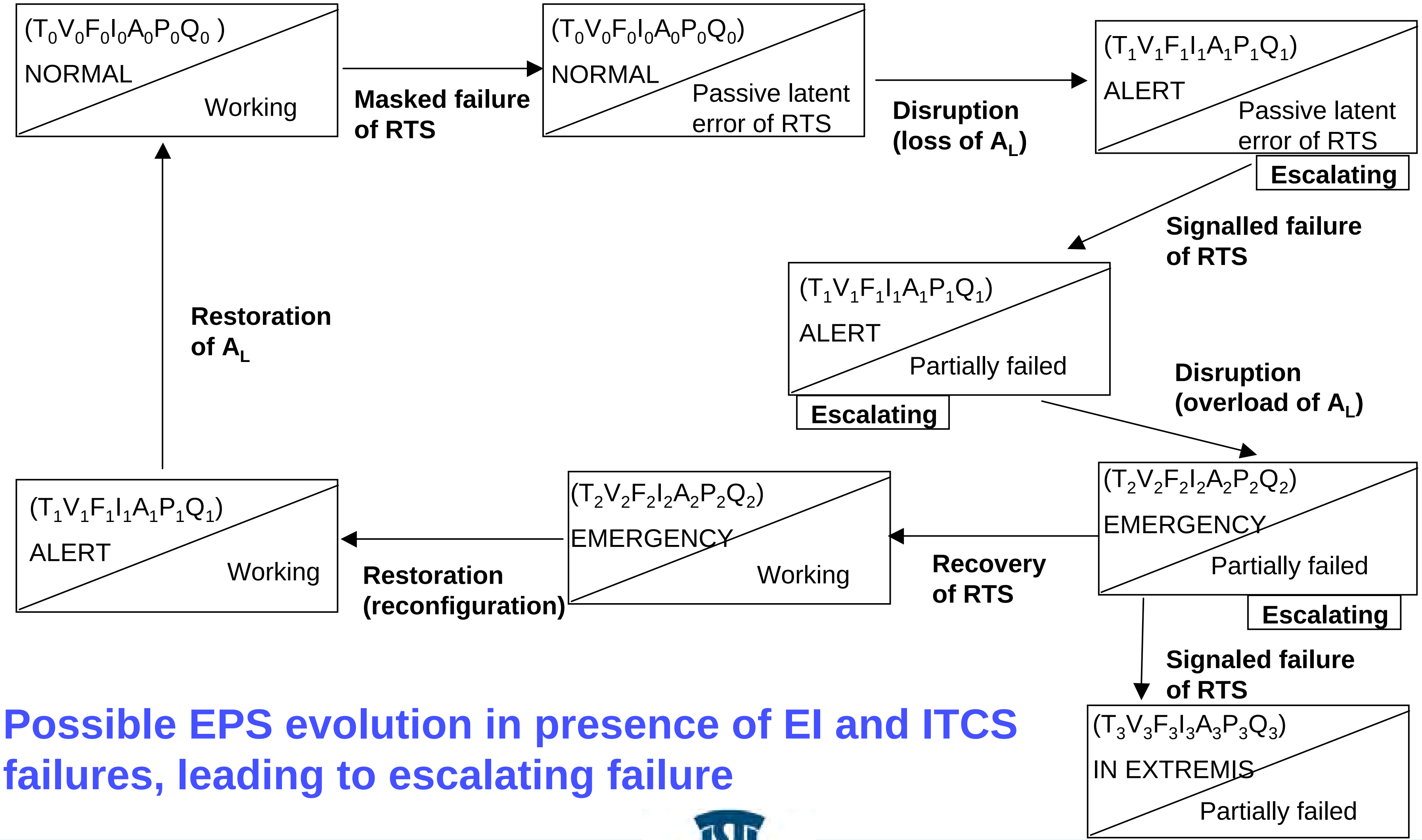
    ➔ the grid topology changes (the disruption propagates and a set of contiguous EI components becomes disrupted)

Dynamic behavior of EPS



Where **NORMAL**, **ALERT**, **EMERGENCY** and **IN EXTREMIS** are EI operative states with increasing criticality from NORMAL (all constraints are satisfied) to IN EXTREMIS (service partially or totally interrupted)

Dynamic behavior of EPS - 2



Possible EPS evolution in presence of EI and ITCS failures, leading to escalating failure

Focus on the modeling framework - 1

- It should be able to capture structural and behavioral aspects of EPS components
- Major identified characteristics, grouped in:
  - Modeling power aspects
  - Modeling efficiency aspects
  - Solution power aspects

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

Focus on the modeling framework - 2

Modeling power aspects

❖ **The framework should support:**

A1. Different formalisms for different sub-models

A2. Representation of continuous and discrete states

A3. Time and probability distributions and enabling conditions can depend on both the continuous and the discrete state

A4. Call to functions implementing the reconfiguration, regulation and auto-evolution algorithms

A5. Definition of (performability) measures, appropriate for EPS risk analysis

Focus on the modeling framework - 3

Modeling efficiency aspects

❖ **The framework should support:**

- **B1.** Hierarchical composition of different sub-models
- **B2.** Replication of (anonymous and non-anonymous) sub-models (sharing a common state)
- **B3.** Compact representation of the grid topology (e.g. using incidence matrix [nodes x arcs])
- **B4.** Compact representation of the electrical parameters (V,F,I,A,P,Q) (e.g. through arrays of real-values)

Focus on the modeling framework - 4

Solution power aspects

- **The framework should support:**
  - Analytical solution of the overall model (if feasible). Possible problems:
    - State-space explosion
    - Stiffness
    - Unavailable analytical methods for the considered class of models - more applicable to simpler sub-models
  - Simulation
    - by automatic tools
    - by ad-hoc simulation software
  - Separate evaluation of different sub-models and combination of the results

Feasibility study - 1

Feasibility of the modeling framework, aiming to show:

- **How some basic framework characteristics can be actually obtained**
- **Model construction of a simple EPS instance focusing on**
  - Substations
  - Protections
  - Local Tele-control systems
  - Regional Tele-control systems

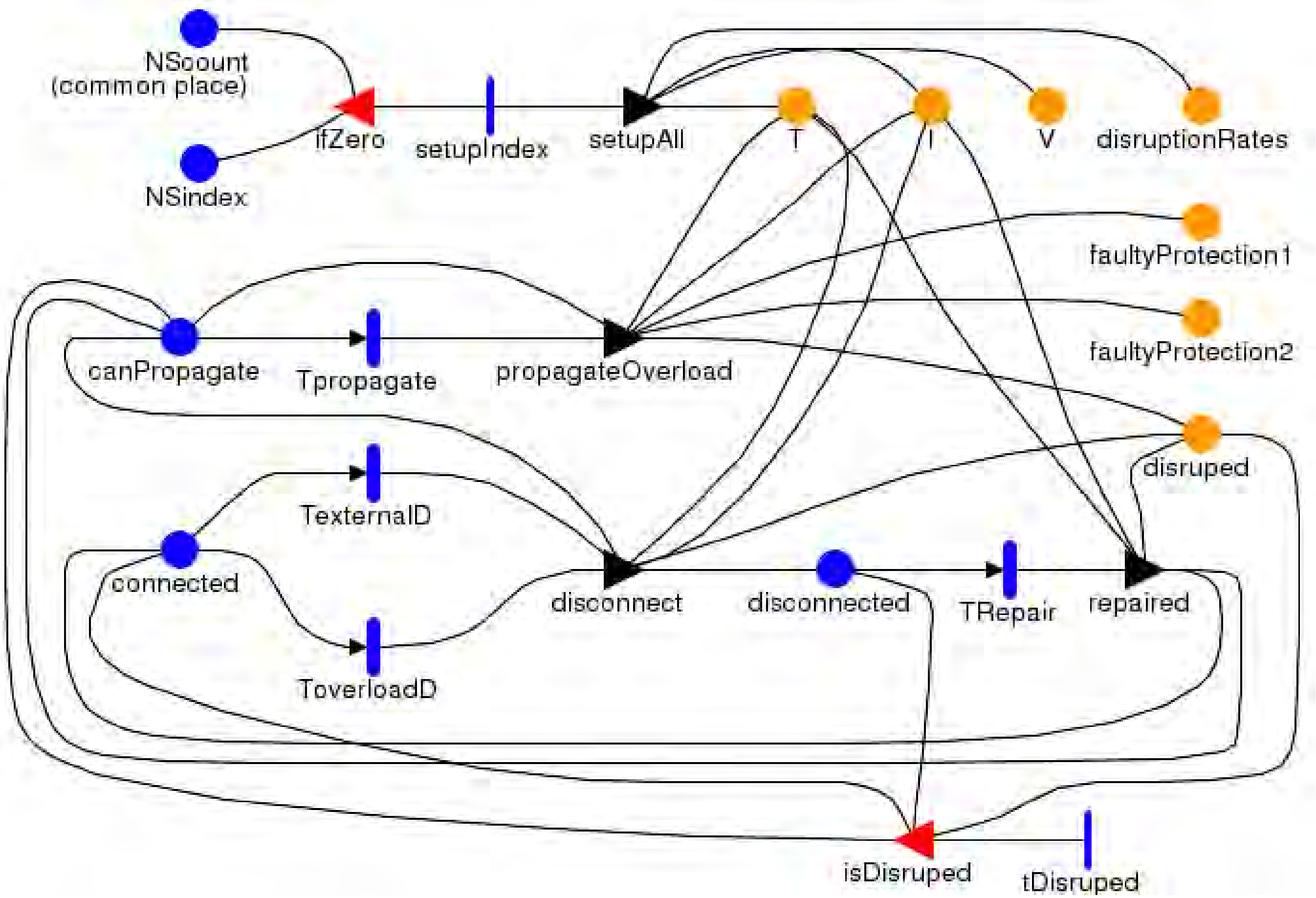
Feasibility study - 2

- Feasibility of the modeling framework using the multi-formalism/multi-solution tool Mobius

- Formalism for models representation: Stochastic Activity Networks (SAN)

- Motivations for this choice:
  - Mobius provides features to support the framework characteristics (points A1. - A5.; B1. - B4.)
  - It also supports multiple solution methods (analytic, simulation) and combination of solutions obtained through different methods.

Modeling a Substation



SAN of a single N_S

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

Major SAN elements - 1

- The extended place **T** (common place among the replicas) is an array of array of short type and represents the topology: **T[i,j]=1** means component *i* is connected to component *j*, otherwise its value is **0** (**A2., B3.**)

- The extended places **I** and **V** (common places among the replicas) are arrays of struct type and describe the characteristics of the electrical parameters (only current and voltage, for simplicity): e.g., **I[j]** represents the current flow associated to component **j**, and relative threshold values for overloads and breakdown (**A2., B4.**)

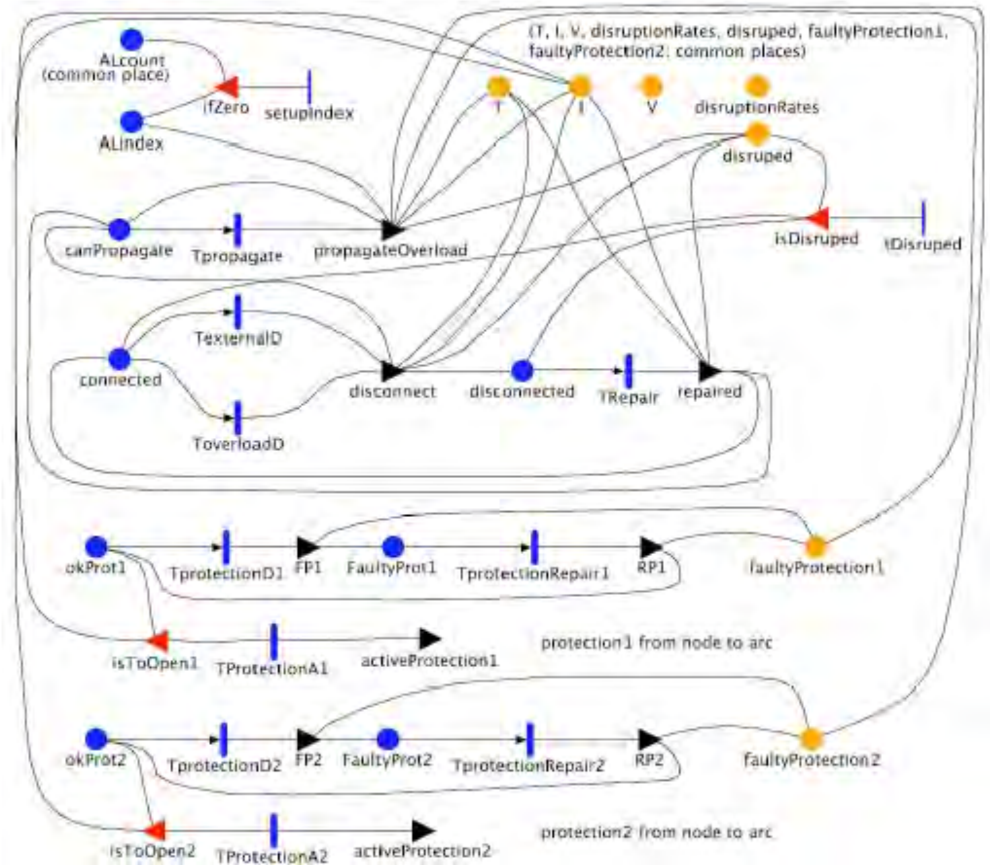
Major SAN elements - 2

- The input gate **ifZero** enables to distinguish each replica when the N_S model is replicated (**B2.**)

- The function **propagateOverload()** is in charge of determining the new values of T and of the electrical parameters, following an event of overload of the current flow (it calls external functions, **A4.**)

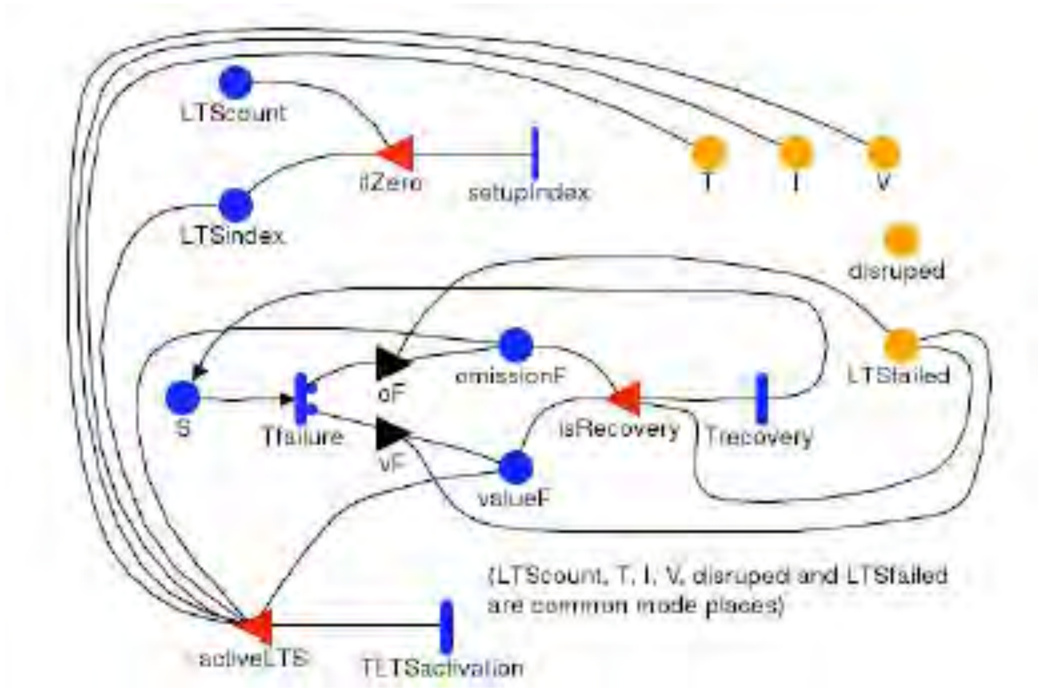
- The rate of the activity **ToverloadD** (time to the occurrence of an internal disruption) depends on the current flow of the component (**A3.**)

Modeling protections



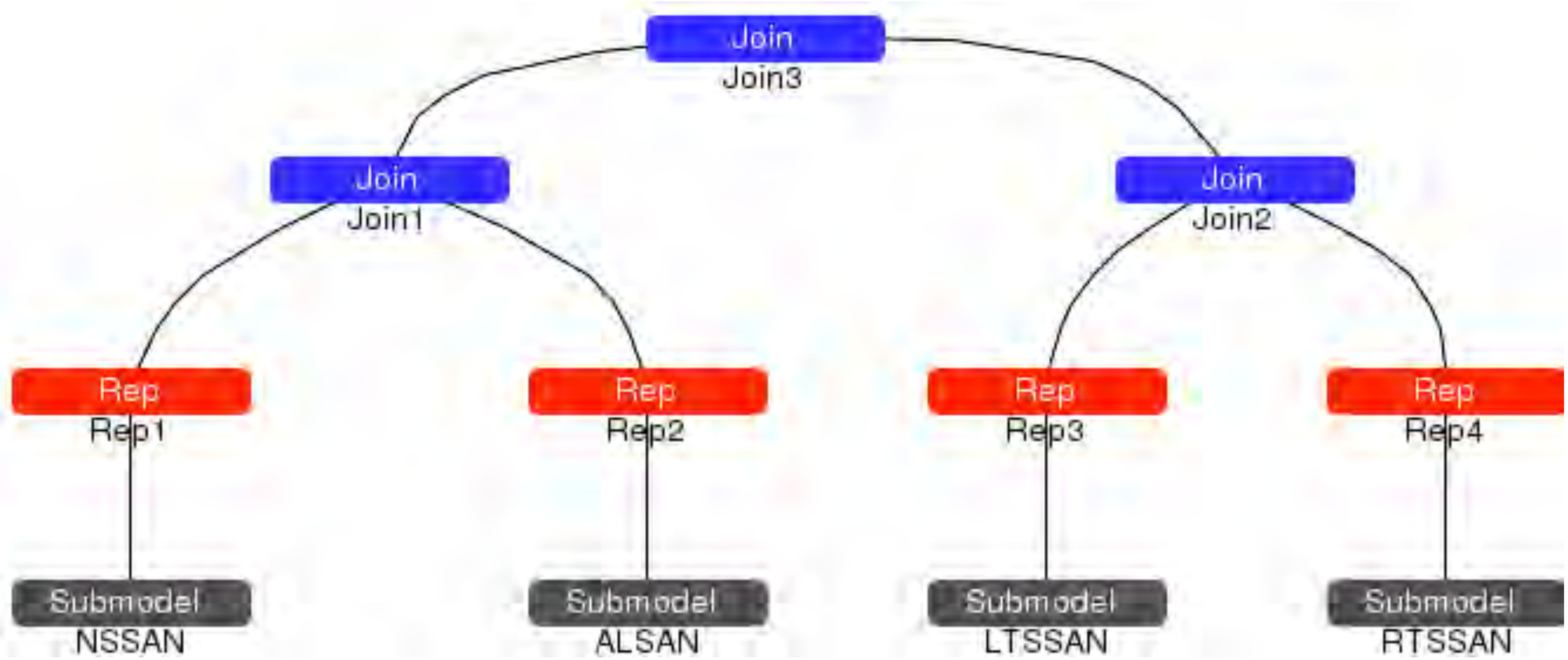
SAN for protections inside AL

Modeling a local Tele-operation system



SAN for LTS

Building part of an instance of EPS



- Replication and composition of the template models is performed through the **Rep** and **Join** operators (B1.)
- The replicas interact through common places (B2.)

Conclusions

- Definition of a modeling framework to analyze the interdependencies between the electrical infrastructure EI and the control information system ITCS
- Still preliminary studies, but relevant contributions to
  - The analysis of the structure and behavior of the EI and ITCS subsystems, including their failure models and states definitions;
  - The identification of the major challenges the modeling framework has to deal with, and discussion of possible approaches to cope with them;
  - The implementation of a few basic modeling mechanisms inside the Mobius modeling and evaluation environment, to support the feasibility of the proposed approach through an existing tool.

Next steps

- Further investigations on the appropriate level of model’s details for EI and ITCS
- Extension and refinements of the modeling mechanisms
- Verification of the applicability of the approach on a simple but complete EPS example
- Study of the solution aspects
- ….

Main references

1. L. Ferrarini and E. Ciapessoni. Indagine sulla sicurezza funzionale dei sistemi di automazione delle reti elettriche. NORME / AUTOMAZIONE /Workpackage 1 /Milestone 1.2 Rapporto 1/1 della milestone A5-052457, CESI - FIA Informatica e Automazione, Dicembre 2005. http://www.ricercadisistema.it/Documenti/SintesiDoc.aspx?idN=1360&idD=312616

2. J-C. Laprie, K. Kanoun, and M. Kaaniche. Modeling cascading and escalating outages in interdependent critical infrastructures. In IEEE Int. Conference on Dependable Systems and Networks (DSN-2006), pages 226–227, Philadelphie (USA), June 2006. Fast abstract.

3. S. Chiaradonna, P. Lollini, and F. Di Giandomenico. On the modeling of an instance of the electric power system. Technical Report rcl061201, University of Florence, Dip. Sistemi Informatica, RCL group - http://dcl.isti.cnr.it/Documentation/Papers/Techreports.html,December 2006.

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