Istituto di Scienza e Tecnologie dell'Informazione “A. Faedo”
Software Engineering and Dependable Computing Laboratory

Critical Infrastructures Resilience: Interdependencies and Assessment of Electric Power Grids

Felicita Di Giandomenico
ISTI-CNR, Pisa
http://sedc.isti.cnr. it

SERENE 2013 Autumn School
Kiev, 2 October 2013

What is this lecture about?

- Focus on **Critical Infrastructures**, specifically **Electric Power Systems**, with the aim of:
  - Pointing out the issues and challenges raised by the relationships (**dependencies**) existing among the infrastructures composing EPS
  - Discussing the need to **master such dependencies**, and hence the need to analyse their effects when failures occur
  - Presenting an approach to the **analysis and evaluation of the impact of (inter)dependencies** in EPS, developed by the presenter's group at ISTI-CNR in Pisa

Outline

- Introduction to Critical Infrastructures
- Dependability and resilience: basic concepts
- Interdependencies in Critical Infrastructures
- Overview of the Electrical Power Systems (EPS)
- Discussion on Model-based approaches to System Validation
- An approach to model EPS, accounting for interdependencies
  - Transmission system – single region
  - Transmission system – multiple regions
  - Distribution System

Definition of Critical Infrastructure:

Examples from Member States, Regional groups

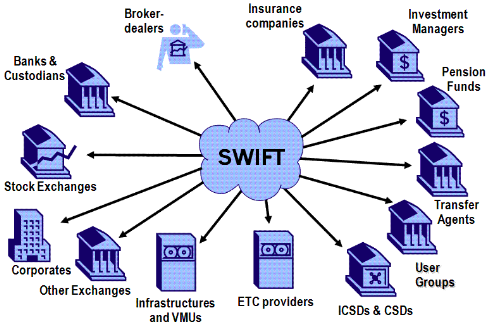
Australia	Those physical facilities, supply chains, information technologies and communication networks which, **if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation**, or affect Australia’s ability to conduct national defense and ensure national security.
Canada	Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or **interconnected and interdependent** within and across provinces, territories and national borders. **Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence**.
European Union	‘Critical infrastructure’ means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and **the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions**
United Kingdom	“The [Critical National Infrastructure] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that **loss could**: 1) **cause large-scale loss of life; 2) have a serious impact on the national economy; 3) have other grave social consequences for the community; or 3) be of immediate concern to the national government.”**
United States	Systems and assets, whether physical or virtual, so vital to the United States that **the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.**

Critical Infrastructure Sectors

- Electricity generation, transmission and distribution;
- Gas production, transport and distribution;
- Oil and oil products production, transport and distribution;
- Telecommunication;
- Water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
- Agriculture, food production and distribution;
- Heating (e.g. natural gas, fuel oil, district heating);
- Public health (hospitals, ambulances);
- Transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- Financial services (banking, clearing);
- Security services (police, military);
- Others

Critical Infrastructures

Some examples…



SWIFT

Broker-dealers

Insurance companies

Investment Managers

Banks & Custodians

Pension Funds

Stock Exchanges

Transfer Agents

User Groups

Corporates

Other Exchanges

Infrastructures and VMUs

ETC providers

ICSDs & CSDs

Evolution of Framework Conditions

- ❑ **PAST**
  - ✧ Infrastructures could only be impaired locally
  - ✧ Limited interdependencies, at national level only
- ❑ **CURRENTLY**
  - ✧ Strong networking within and between sectors through ICT
  - ✧ National and transnational relations
  - ✧ Cooperation in the provision of services
- ❑ **FUTURE**
  - ✧ Increase of Large-area disturbances and variety of threats
  - ✧ Incidents abroad may become a problem for internal security
  - ✧ ……

Critical Infrastructure Protection (CIP)

- **CIP** has become a priority for many Countries
- Many initiatives triggered at National and International level
  - **Research projects**
    - EU: IRRIIS, CRUTIAL, GRID, MIA, …
    - NSF: TCIP, …
  - **Development of Standards and Recommendations**
    - US: NERC (North American Reliability Corporation), Electric Power Research Institute, NIPC (National Infrastructure Research Centre), NIAC (National Infrastructure Advisory Council), ...
    - Australia: CIPMA (Critical Infrastructure Protection Modeling and Analysis Program), …
    - EU Directive 2008/114/EC - on the Energy and Transport sectors, …
  - **International Associations and Agencies**
    - CRIS (International Institute for Critical Infrastructures) Institute
    - IFIP WG 11.10 on Critical Infrastructure Protection
    - The Institute for Information Infrastructure Protection I3P
    - EU ENISA (European Network and Information Security Agency)

Critical Information Infrastructure (CII)

- ❑ Since most of the **critical infrastructures** are either built upon or monitored and controlled by ICT systems, *the* ***"cyber" infrastructure*****,** which is essential for the continuity of critical infrastructure services, has become the new focal point

- ❑ **Protection of the CII** has become especially important due to two reasons:
  - ✧ their invaluable and growing role in the economic sector;
  - ✧ their interlinking role between various infrastructure sectors and the essential requirement that other infrastructures function at all times

What is needed

- ❑ **Build CI following sound engineering design principles**
  - ✧ Especially, the ICT components are requested to be developed following rigorous software engineering principles
- ❑ **Protect them against accidental and malicious faults**
  - ✧ To mitigate consequences of vulnerabilities and malfunctions
- ❑ **Evaluate them to assess their degree of trustworthiness/ resilience**
  - ✧ To understand their adequacy and get guidance towards critical components that need improvements
  - ✧ Especially, sensitivity analysis to variations of internal and/or external conditions is highly helpful

Dependability and Resilience

(Mostly extracted from:

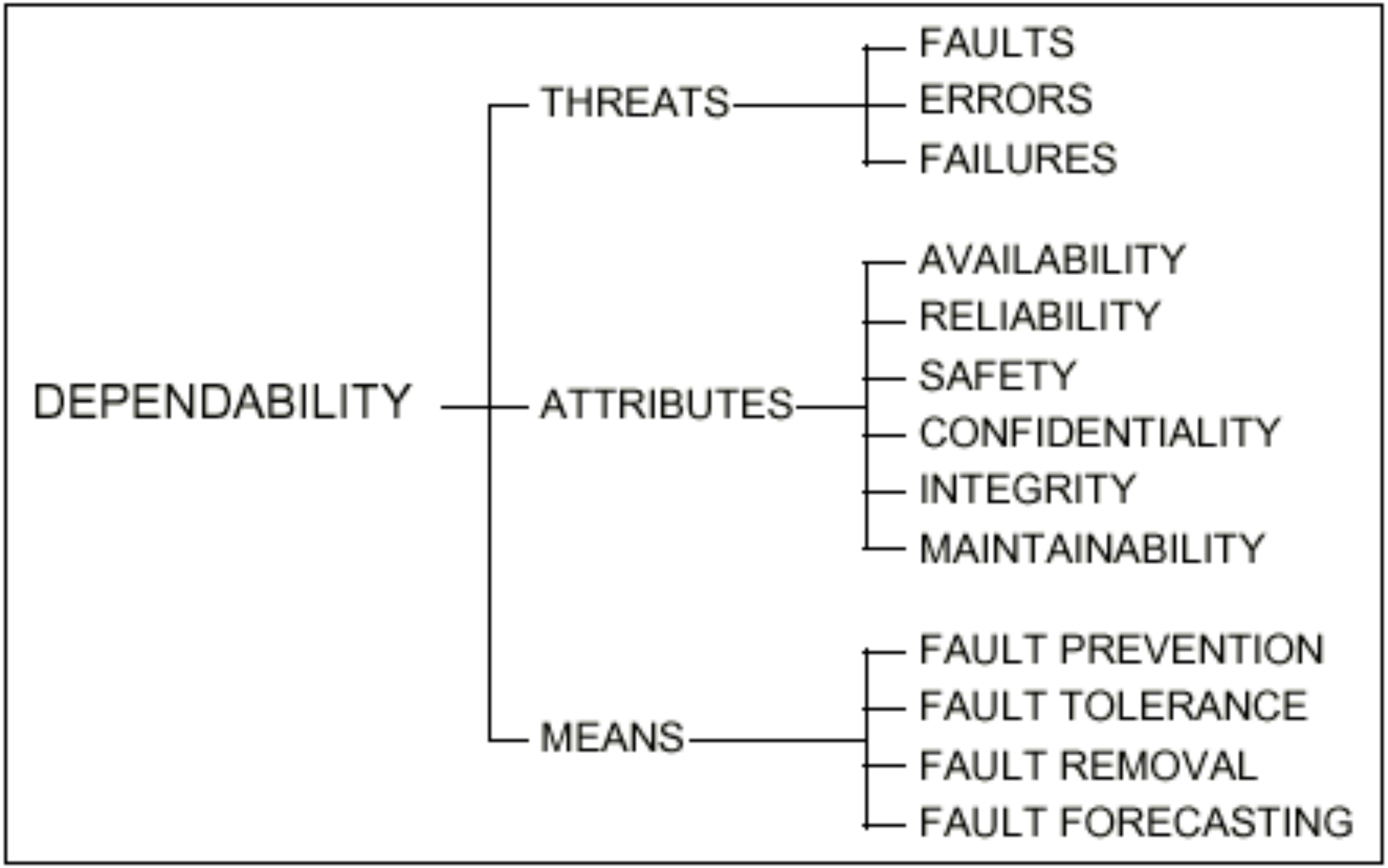
- *A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, Vol. 1:1, pp. 11-33, January-March 2004*
- National Infrastructure Advisory Council, "Critical Infrastructure Resilience - Final Report and Recommendations", September 2009, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf)

Dependability: basic concepts

Computing systems are characterized by 5 fundamental properties: functionality, usability, performance, cost, and **dependability**.

*“**Dependability** of a computing system is the ability to deliver service that can justifiably be trusted”*

Dependability		
Attributes	**Means**	**Threats**
Properties expected from the system and according to which assessment of service quality resulting from threats and means opposing to them is conducted	**Methods and techniques enabling 1) to provide service on which reliance can be placed and 2) to have confidence in its ability**	**Undesired (not unexpected) circumstances causing or resulting from undependability (reliance cannot or will not any longer be placed on the service**



DEPENDABILITY

THREATS

- FAULTS
- ERRORS
- FAILURES

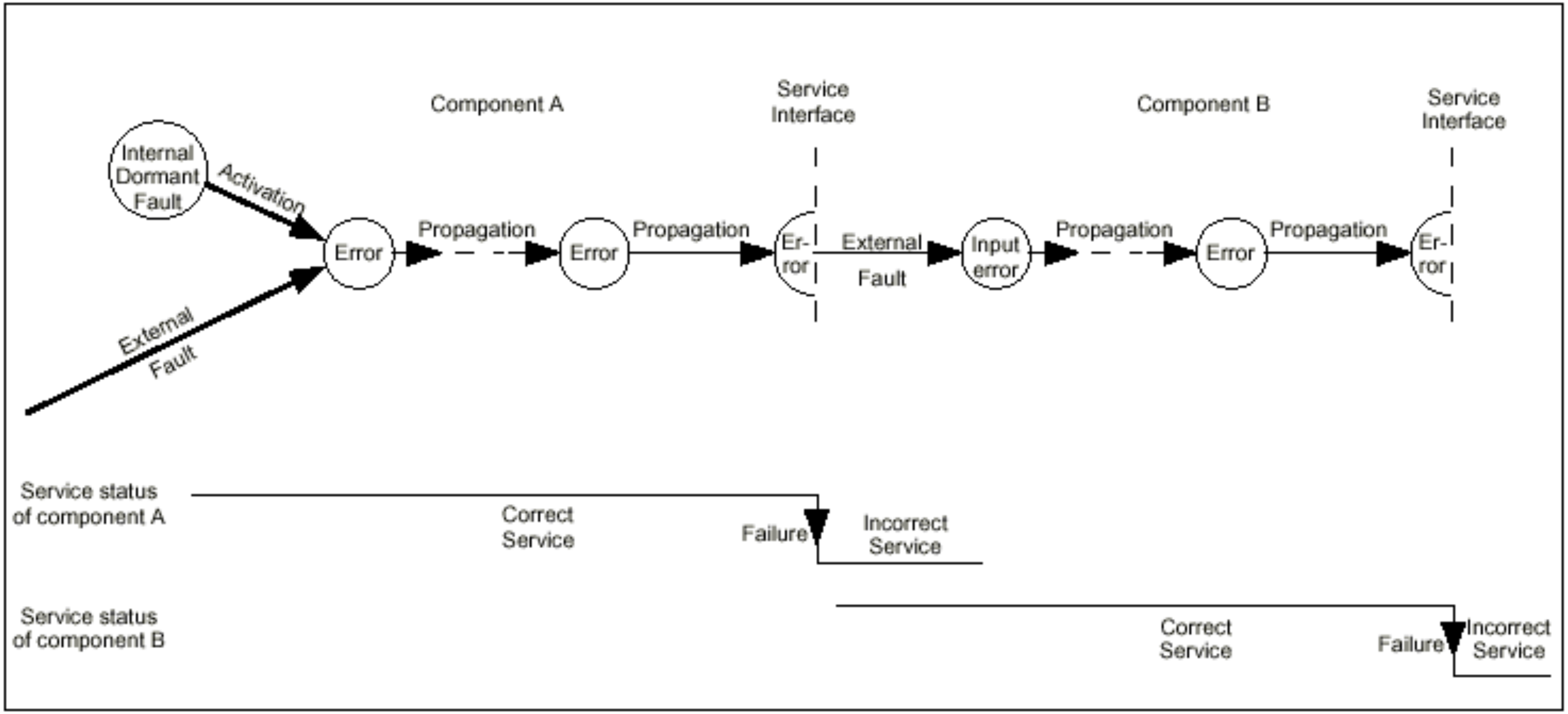
ATTRIBUTES

- AVAILABILITY
- RELIABILITY
- SAFETY
- CONFIDENTIALITY
- INTEGRITY
- MAINTAINABILITY

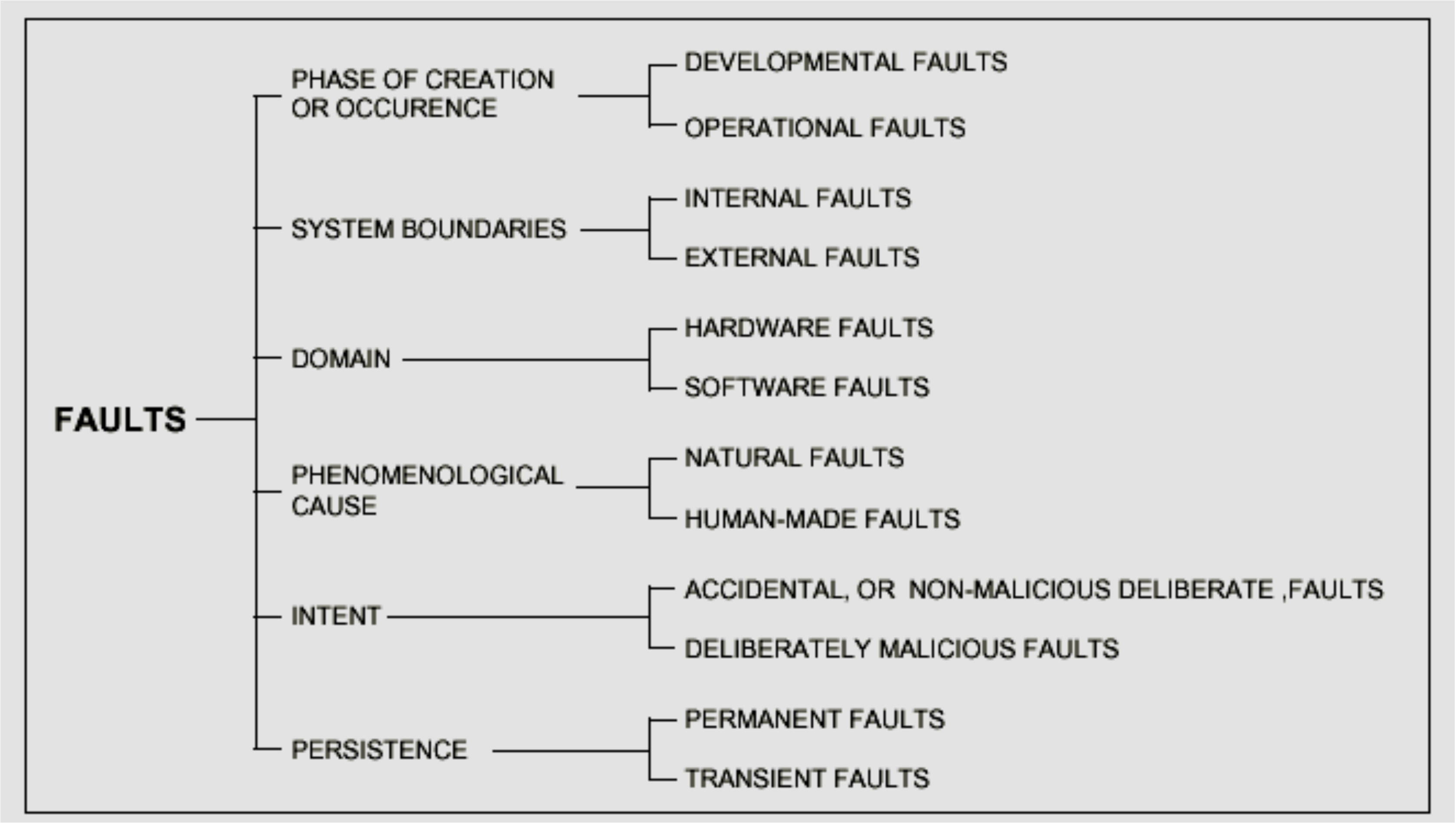
MEANS

- FAULT PREVENTION
- FAULT TOLERANCE
- FAULT REMOVAL
- FAULT FORECASTING

Fault – error - failure chain

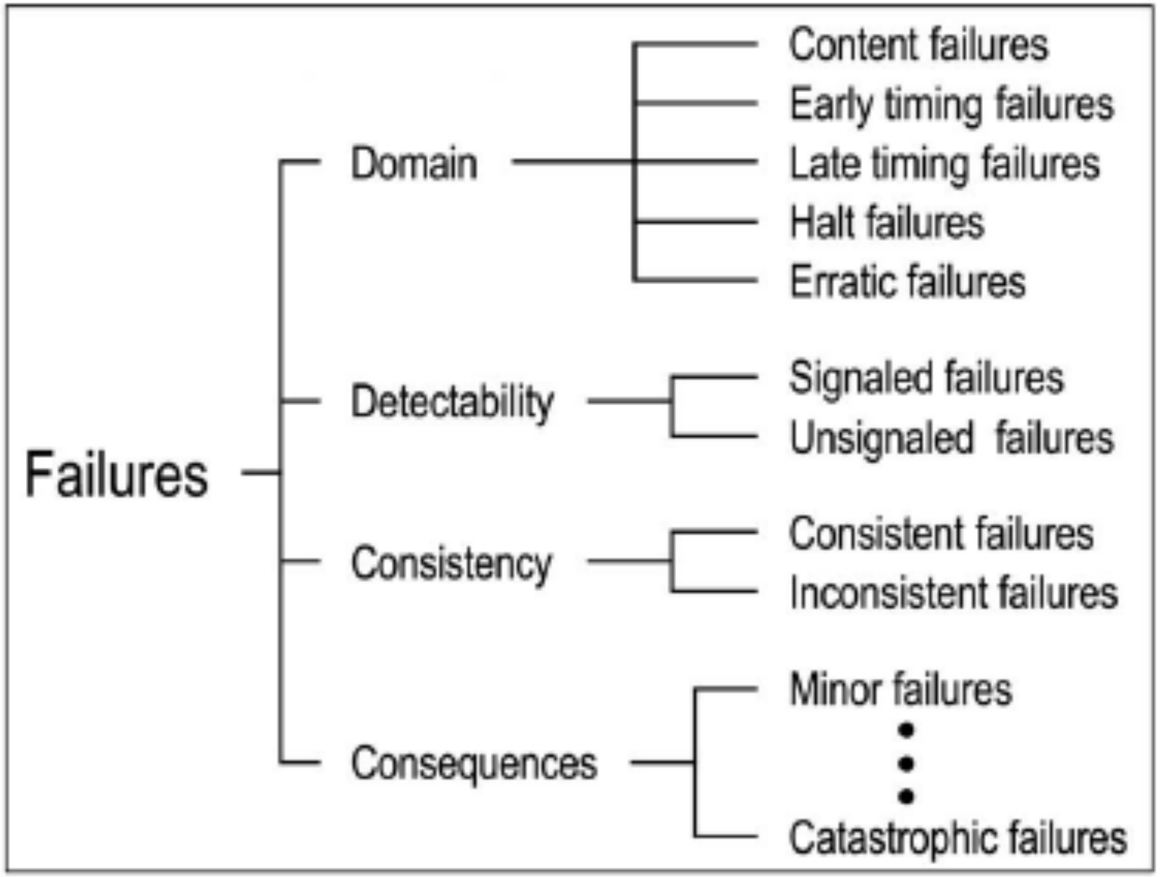


Service Threats



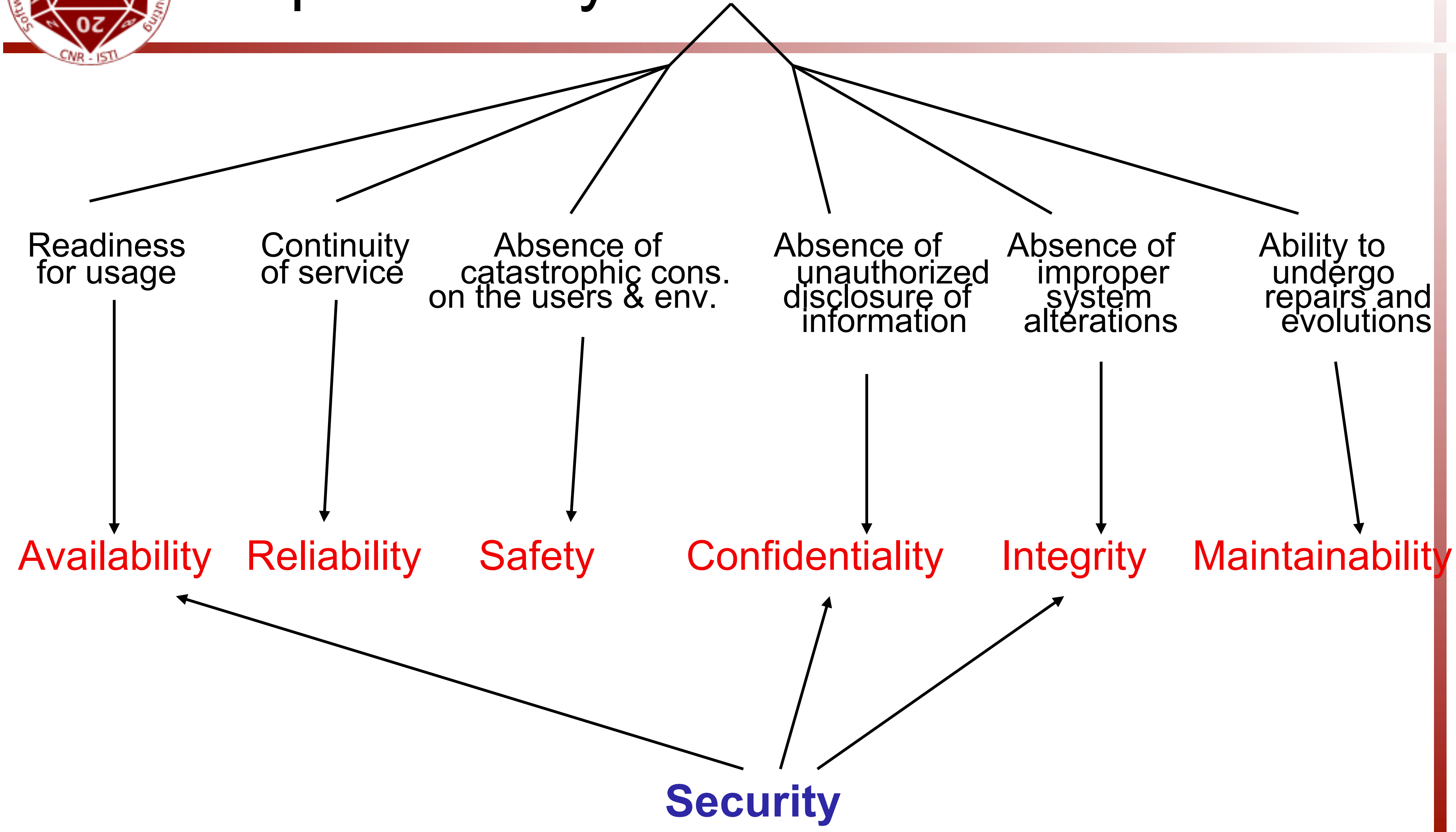
Elementary fault classes

Failure modes



Service Failure Modes

Dependability attributes



Readiness for usage

Continuity of service

Absence of catastrophic cons. on the users & env.

Absence of unauthorized disclosure of information

Absence of improper system alterations

Ability to undergo repairs and evolutions

Availability

Reliability

Safety

Confidentiality

Integrity

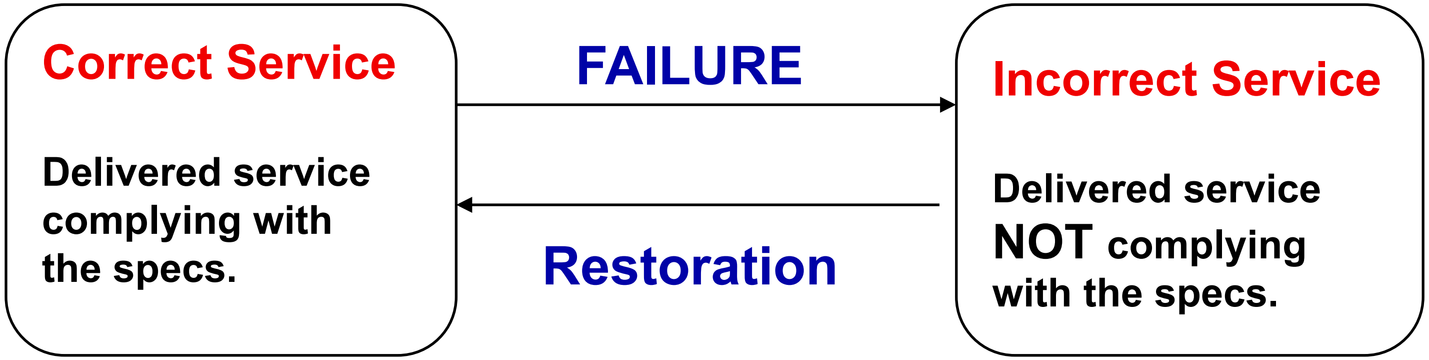
Maintainability

Security

Absence of unauthorized access to, or handling of, system state

Dependability Measures

The alternation of correct-incorrect service delivery is quantified to **define the measures** of dependability:



Correct Service

Delivered service complying with the specs.

FAILURE

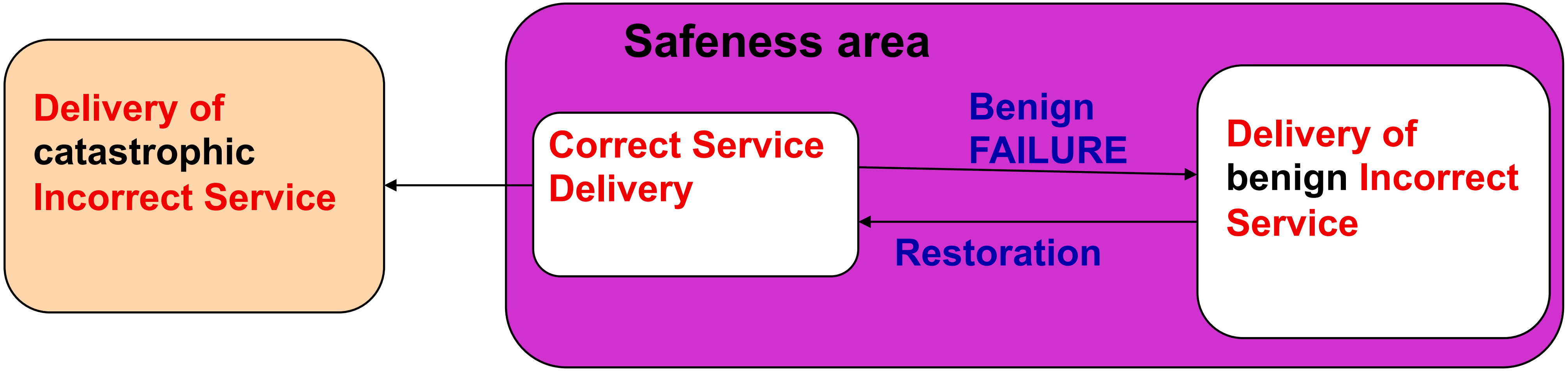
Restoration

Incorrect Service

Delivered service NOT complying with the specs.

- **reliability**: a measure of the continuous delivery of correct service — or the time to failure,
- **availability**: a measure of the delivery of correct service with respect to the alternation of correct and incorrect service,
- **maintainability**: a measure of the time to service restoration since the last failure occurrence.

Safety and Reliability


Delivery of catastrophic Incorrect Service
Safeness area
Correct Service Delivery
Benign FAILURE
Delivery of benign Incorrect Service
Restoration

- **safety** is an extension of **reliability**: the state of correct service and the states of incorrect service due to non-catastrophic failure are grouped into a safe state,
- **safety** is a measure of continuous **safeness**, or equivalently, of the time to catastrophic failure;
- **safety** is thus **reliability** with respect to catastrophic failures.

More Specific Measures

A system may deliver various services or levels of service

✧ from **full** capacity to **emergency** service - *degradable systems*

and have different **failure modes**.

E.g.: a telephone switch:

- may lose half its lines,
- may lose every other call,
- may carry all calls with low quality

Performability : measures of the value of service provided, taking into account failures (combined *performance and dependability* measure)

Considerations on dependability attributes

- Dependability attributes may be emphasized to a different extent depending on the application: always availability (more or less) while reliability, safety, confidentiality may or may not be required
- This variation in emphasis directly affects the appropriate balance of the techniques to be employed for making the resulting system dependable.
- Some of the attributes are in conflict (e.g. availability and safety, availability and security), necessitating design trade-offs.
- The dependability attributes of a system should be interpreted in a probabilistic sense: due to the unavoidable presence of faults, systems are never totally available, reliable, safe…..

The Means to Attain Dependability

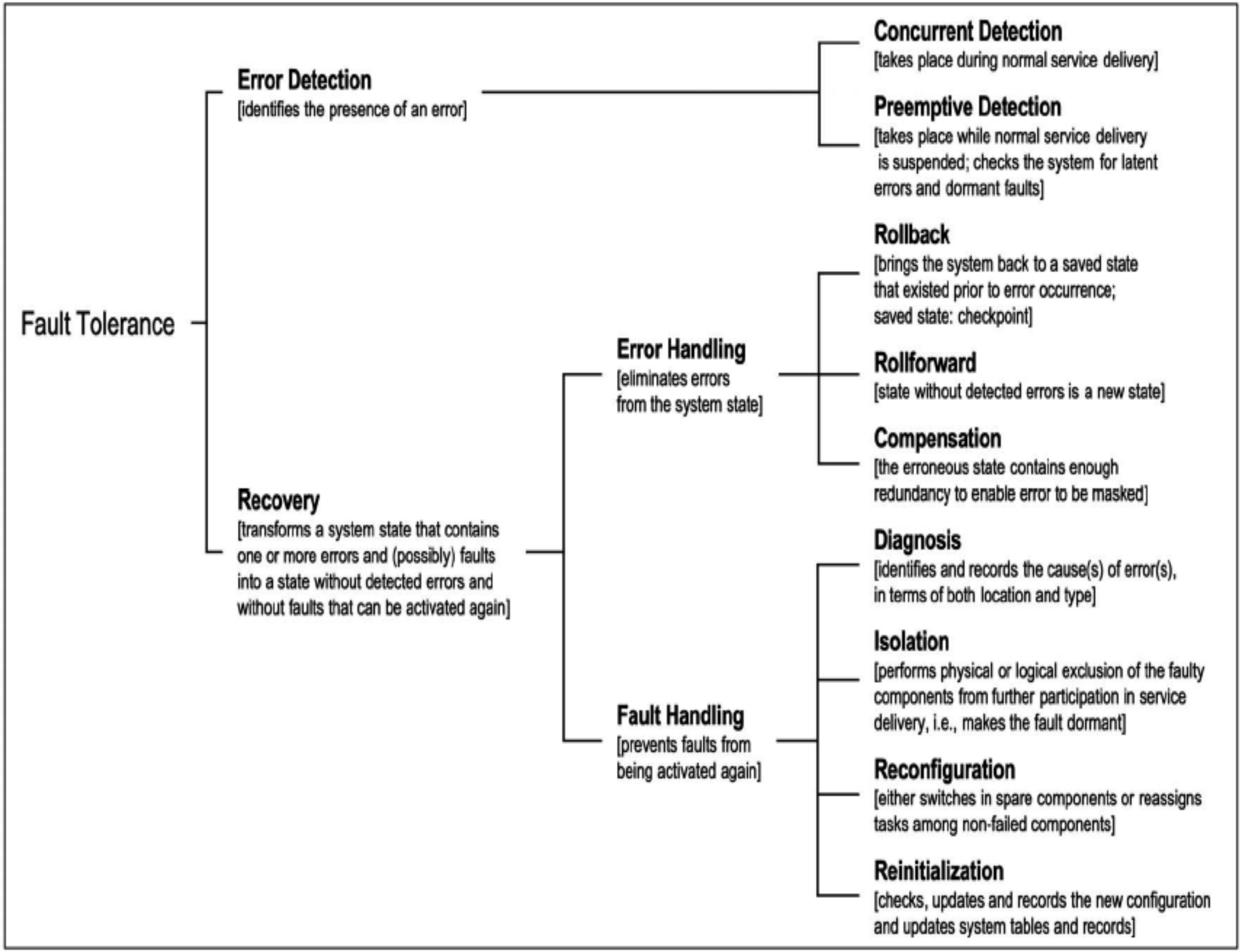
The development of a dependable computing system calls for the combined utilization of a set of four techniques:

- **fault prevention**: how to prevent the occurrence or introduction of faults,
- **fault tolerance**: how to deliver correct service in the presence of faults,
- **fault removal**: how to reduce the number or severity of faults,
- **fault forecasting**: how to estimate the present number, the future incidence, and the likely consequences of faults.

Fault Prevention

Fault prevention is attained by:

- ***quality control techniques*** employed during the design and manufacturing of hardware and software, including *structured programming, information hiding, modularization, etc*., for software, and *rigorous design rules and selection of high-quality, mass-manufactured hardware components* for hardware
- ***simple design***, possibly at the cost of constraining functionality or increasing cost
- ***formal proof*** of important properties of the design
- provision of ***appropriate operating environment*** (air conditioning, protection against mechanical damage), to prevent operational physical faults, and ***training, rigorous procedures for maintenance, 'foolproof' packages***, intend to prevent interaction faults
- ***firewalls and similar defenses*** to prevent malicious faults



Fault Tolerance

- **Error Detection** [identifies the presence of an error]
  - **Concurrent Detection** [takes place during normal service delivery]
  - **Preemptive Detection** [takes place while normal service delivery is suspended; checks the system for latent errors and dormant faults]
- **Recovery** [transforms a system state that contains one or more errors and (possibly) faults into a state without detected errors and without faults that can be activated again]
  - **Error Handling** [eliminates errors from the system state]
    - **Rollback** [brings the system back to a saved state that existed prior to error occurrence; saved state: checkpoint]
    - **Rollforward** [state without detected errors is a new state]
    - **Compensation** [the erroneous state contains enough redundancy to enable error to be masked]
  - **Fault Handling** [prevents faults from being activated again]
    - **Diagnosis** [identifies and records the cause(s) of error(s), in terms of both location and type]
    - **Isolation** [performs physical or logical exclusion of the faulty components from further participation in service delivery, i.e., makes the fault dormant]
    - **Reconfiguration** [either switches in spare components or reassigns tasks among non-failed components]
    - **Reinitialization** [checks, updates and records the new configuration and updates system tables and records]

Fault Removal during development

It consists of three steps: **verification, diagnosis, correction**

Verification techniques can be:

- ✧ Without actual execution (**static verification**): static analysis (e.g., inspections or walk-through), model-checking, theorem proving.
- ✧ Exercising the system (**dynamic verification**): either with symbolic inputs in the case of symbolic execution, or actual inputs in the case of testing.

Important is **the verification of fault tolerance mechanisms**, especially through:

- ✧ formal static verification,
- ✧ testing that includes faults or errors in the test patterns: fault injection.

As well as **verifying that the system cannot do more than what is specified**, important to **safety and security**.

Fault Removal during the operational life

- Fault removal during the operational life of a system is **corrective or preventive maintenance**
  - ✧ **Corrective maintenance** is aimed at removing faults that have produced one or more errors and have been reported
  - ✧ **Preventive maintenance** is aimed to uncover and remove faults before they might cause errors during normal operation. a) physical faults that have occurred since the last preventive maintenance actions, and b) design faults that have led to errors in other similar systems.

Fault Forecasting

Fault forecasting is conducted by performing an evaluation of the system behavior with respect to fault occurrence or activation.

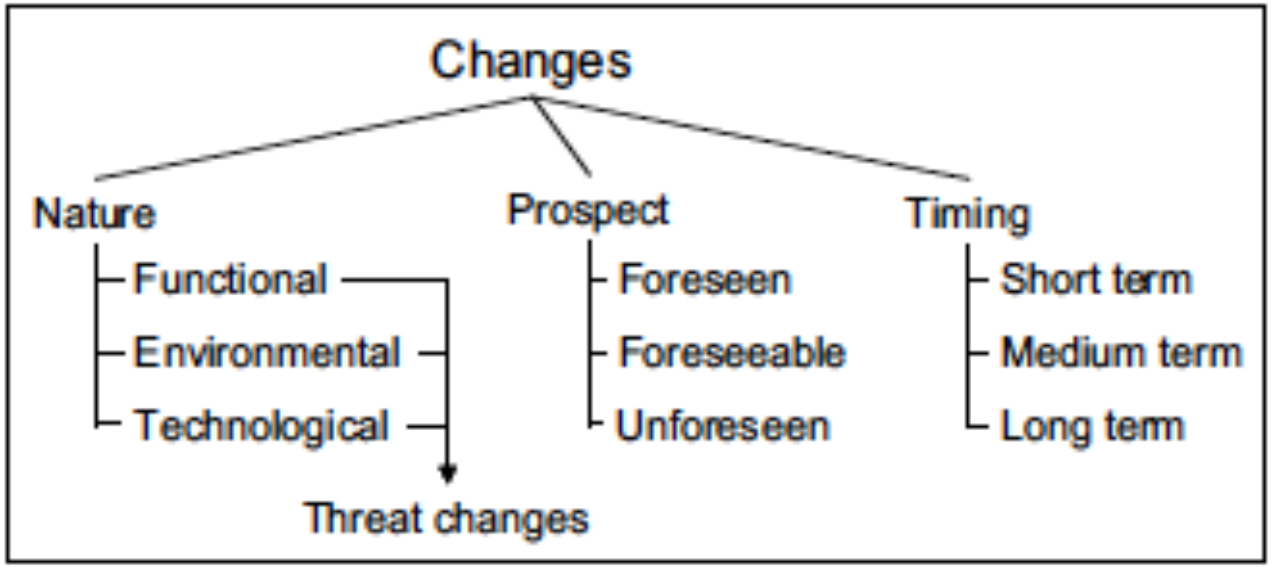
- **Qualitative Evaluation**: aims to identify, classify, rank the failure modes, or the event combinations (component failures or environmental conditions) that would lead to system failures
- **Quantitative Evaluation**: which aims to evaluate in terms of probabilities the extent to which the relevant attributes of dependability are satisfied, through
  - either specific methods (e.g., *FMEA* for qualitative evaluation, or *Markov chains* and *stochastic Petri nets* for quantitative evaluation)
  - or methods applicable to both forms of evaluation (e.g., *reliability block diagrams*, *fault-trees*)

Resilience

Definition (from Laprie 2008):

The persistence of service delivery that can justifiably be trusted, when facing changes

The changes can be classified according to three dimensions:



Infrastructure Resilience - 1

Definition (from NIAC 2009)

*"**Infrastructure resilience** is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to **anticipate**, **absorb**, **adapt** to, and/or **rapidly recover** from a potentially disruptive event",*

Where:

- **Absorptive capacity** is the ability of the system to endure a disruption without significant deviation from normal operating performance. For example, fire-proofing foam increases the capacity of a building system to absorb the shock of a fire

Infrastructure Resilience - 2

- **Adaptive capacity** is the ability of the system to adapt to a shock to normal operating conditions. For example, the extra transformers that the U.S. electric power companies keep on store and share increases the ability of the grid to adapt quickly to regional power losses.

- **Recoverability** is the ability of the system to recover quickly – and at low cost – from potential disruptive events

- **Anticipation** capacity is the ability to predict behavior and impact of potential disruptive events, in order to identify weak points and vulnerabilities, for which mitigation measures need to be devised.

Infrastructure Resilience - 3

According to NIAC, three features characterize Infrastructure Resilience:

- **Robustness:** the ability to maintain critical operations and functions in the face of crisis.
- **Resourcefulness:** the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds.
- **Rapid recovery**: the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption.

Some directions to Infrastructure Resilience

- ✧ Increase the system’s **robustness** through redundancy and intrusion tolerance techniques

- ✧ Increase the **recoverability** of the system through minimizing the time to recovery by adopting smart repair schedules, also leading to higher availability and survivability

- ✧ Increase the **anticipation** ability through early evaluation of the impact of disruption/attack events

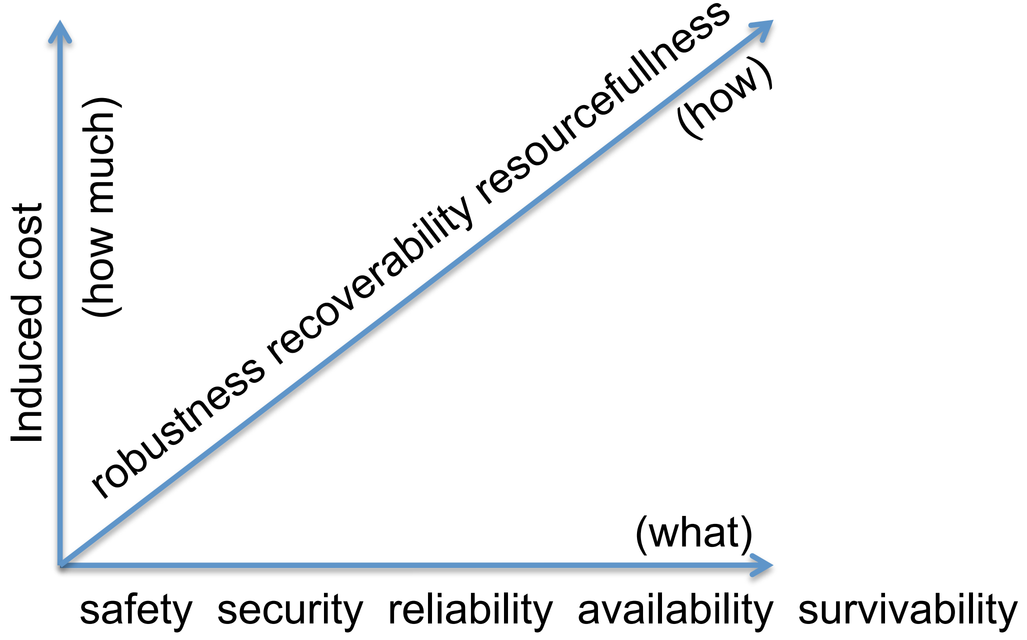
- ✧ Comparing infrastructure designs alternatives with respect to their survivability and dependability will lead to more informed design decisions and hence, to more **resourceful** infrastructures

Resilience-Cost tradeoff

The relationship between

- a system's extra-functional requirements/properties, i.e., (**what**),
- the architecture features that are constructed to make the system more resilient, i.e., (**how**),
- the associated costs to build a resilient system, i.e., (**how much**).

needs to be carefully considered


Induced cost
(how much)
robustness recoverability resourcefullness
(how)
(what)
safety security reliability availability survivability

Interdependencies

Definitions – from Rinaldi et a. 2001

Dependency: A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.

Interdependency: A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.

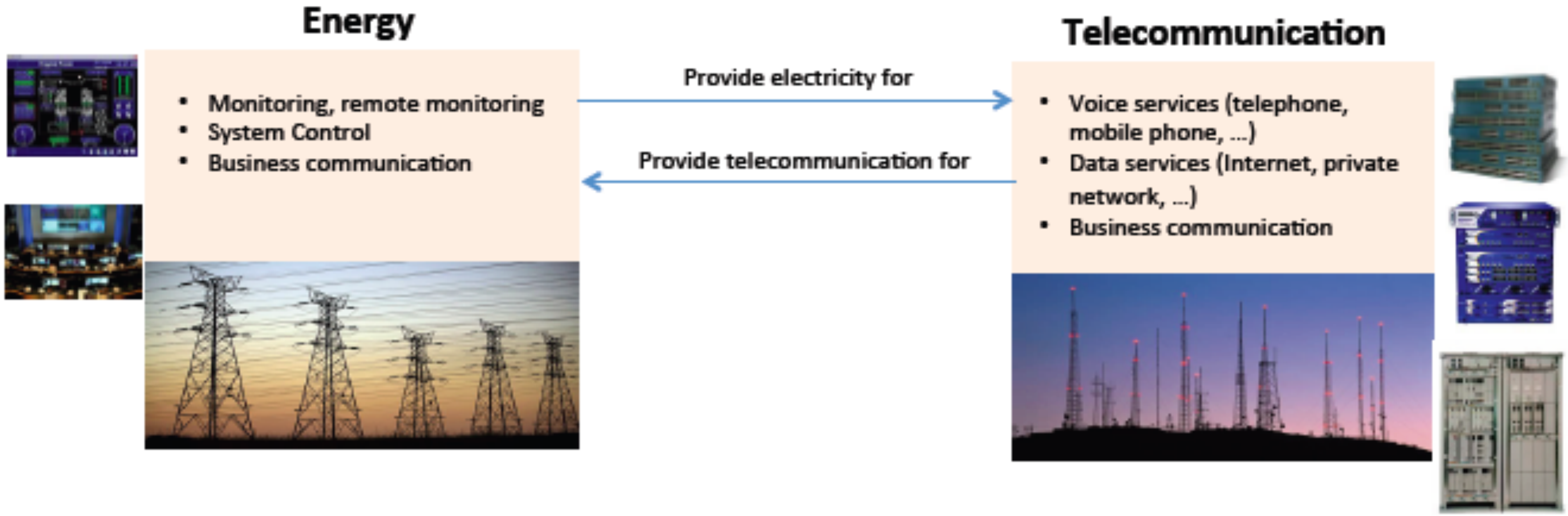
In practice, **interdependencies** among infrastructures dramatically increase the overall complexity of the "system of systems."

Examples of interdependencies

Telecommunications and **Energy** sectors are among the most interdependent CI

Examples:

- No electricity means telecom services are highly impacted
- No telecom services means the energy sector loses some monitoring capability



Energy

- Monitoring, remote monitoring
- System Control
- Business communication

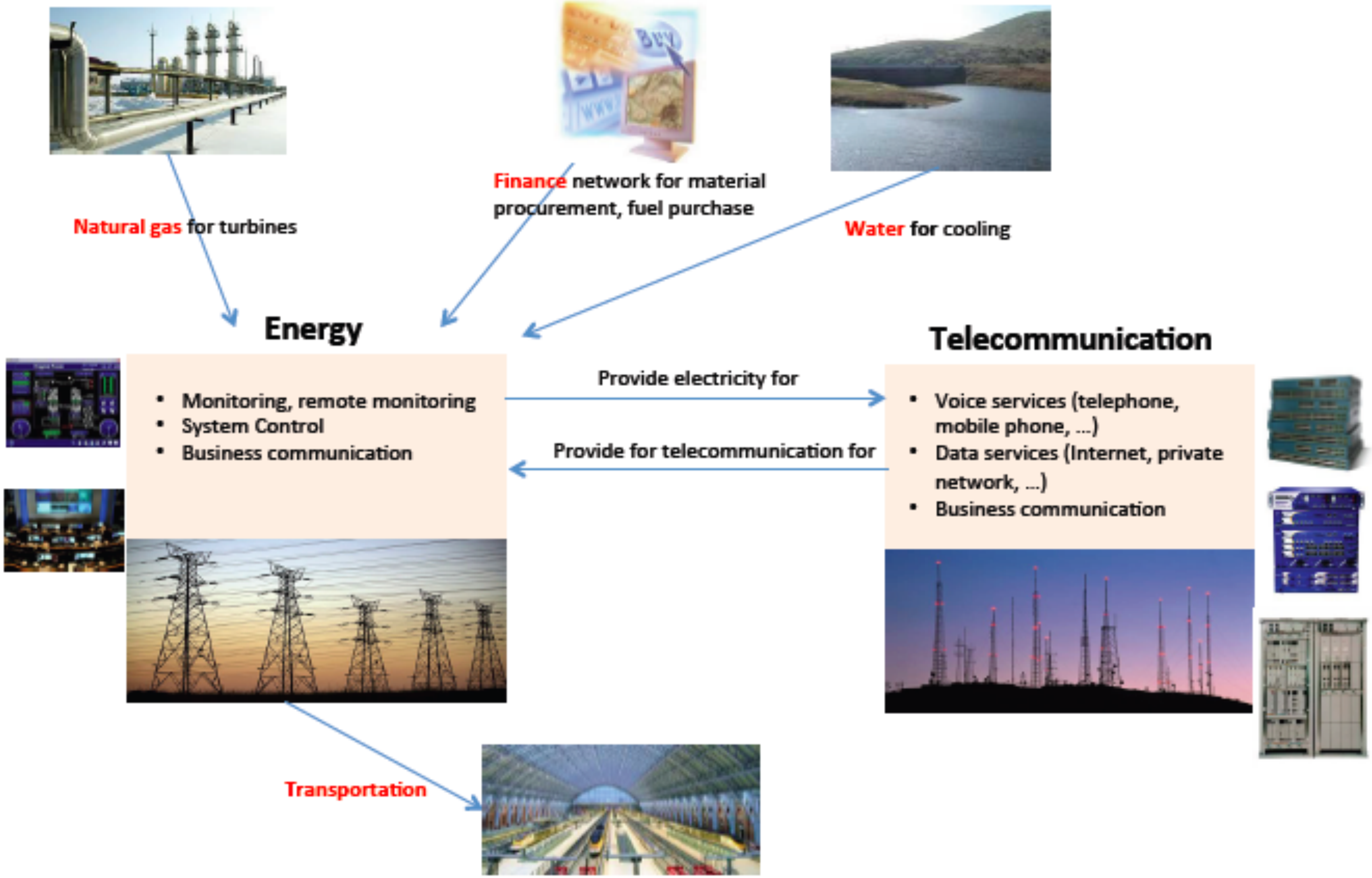
Provide electricity for

Provide telecommunication for

Telecommunication

- Voice services (telephone, mobile phone, …)
- Data services (Internet, private network, …)
- Business communication

Larger view of interdependencies



Natural gas for turbines

Finance network for material procurement, fuel purchase

Water for cooling

Energy

- Monitoring, remote monitoring
- System Control
- Business communication

Provide electricity for

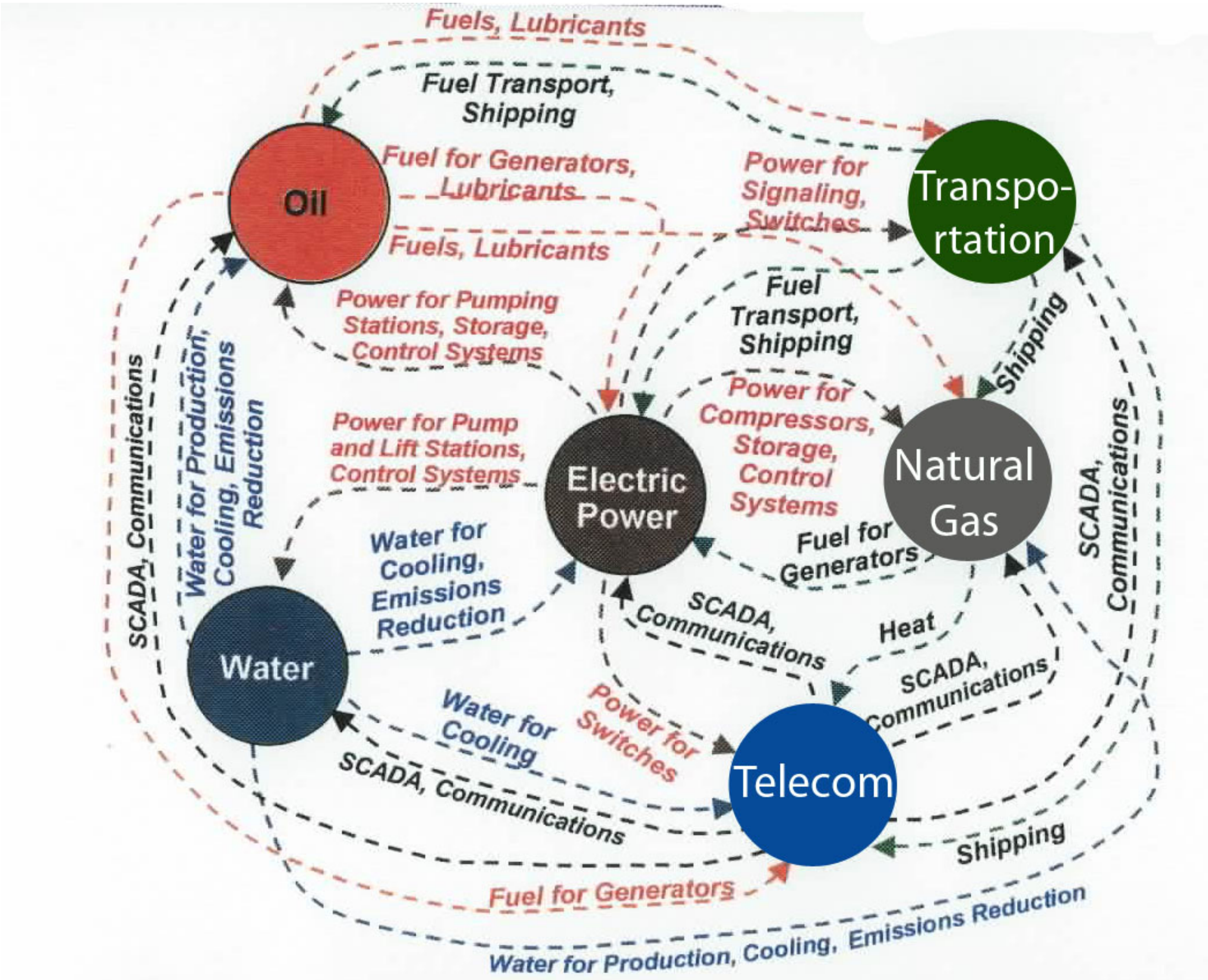
Provide for telecommunication for

Telecommunication

- Voice services (telephone, mobile phone, …)
- Data services (Internet, private network, …)
- Business communication

Transportation

A view of interdependencies among major Critical Infrastructures


Fuels, Lubricants
Fuel Transport, Shipping
Fuel for Generators, Lubricants
Oil
Power for Signaling, Switches
Transpo-rtation
Fuels, Lubricants
Fuel Transport, Shipping
Power for Pumping Stations, Storage, Control Systems
Shipping
SCADA, Communications
Water for Production, Cooling, Emissions Reduction
Power for Compressors, Storage, Control Systems
Power for Pump and Lift Stations, Control Systems
Electric Power
Natural Gas
SCADA, Communications
Fuel for Generators
Water for Cooling, Emissions Reduction
SCADA, Communications
Heat
Water
SCADA, Communications
Water for Cooling
Power for Switches
Telecom
SCADA, Communications
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

Types of Interdependencies

- □ **Physical**: when material output of one infrastructure is used by another infrastructure
- □ **Cyber:** when the state of one infrastructure depends on information transmitted through the information infrastructure
- □ **Geographic:** when a local environment event can affect all the infrastructures (interdependence is due to proximity)
- □ **Logical**: none of the previous, e.g., dependency through financial markets or human decisions and actions

Understanding Interdependencies

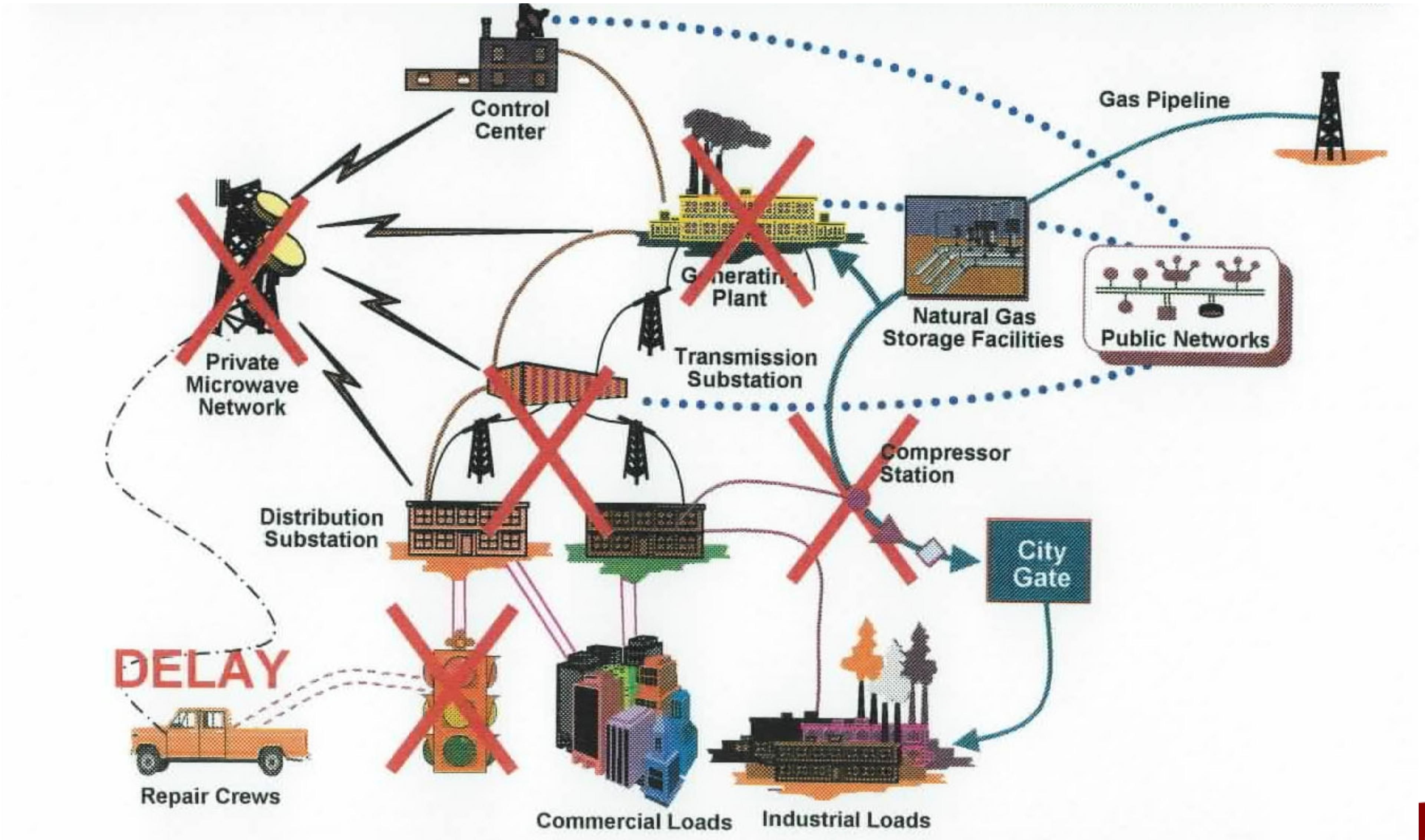
Interdependencies increase the risk of failure or disruptions in multiple infrastructures. Therefore it is crucial to understand them in terms of:

- Importance to the operation of the infrastructures
  - Normal operations
  - Disruptions
  - Repair and restoration
- How interdependencies change as a function of outage duration and other factors
- What linkages exist between critical infrastructures and community assets, in order to understand consequences of outages
- How backup or other mitigation mechanisms can reduce interdependence problems

Types of Interdependencies-related Disruptions

- **Cascading failure** – a disruption in one infrastructure causes a disruption in a second infrastructure
- **Escalating failure** – a disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g., the time for recovery or restoration of an infrastructure increases because another infrastructure is not available)
- **Common cause failure** – a disruption of two or more infrastructures at the same time because of a common cause (e.g., natural disaster, right-of-way corridor)

Examples of Cascading and Escalating failures



Example of cascading effect: Black-out in Italy, 28/09/2003

Sequence of events:

- a tree flashover caused tripping of a major tie-line between Italy and Switzerland (Mettlen-Lavorgo, loss of 1320 MW) at **03:01:22**
- Automatic and manual reclosure of line failed due to the large angle (42°) across the breaker resulted in an overload on a parallel path
- Attempts to mitigate the overload of a second line (Sils-Soazza), which tripped at 03:25:22, was not successful
- the cascading trend continued and the power deficit in Italy was such that the ties to France, Austria and Slovenia were tripped
- the frequency decay could not be controlled adequately by under-frequency load shedding
- the entire Italian System collapsed at **3:28:00**

Italian blackout – contd.

The blackout affected more than **56 million people**

- **worst blackout in the history of Italy**
- power was restored after 3 hours in the northern area and during the same day for most of Italy

Several studies undertaken to analyze and understand the causes of this failure:

- **technical vulnerabilities** (mainly originated from changes in the regulation and monitoring of energy transfers across Europe)
- **managerial and human factors** causes (these arguably included an over-reliance on computer-based decision support systems)
- **a strong interaction between power network and communication network** has been highlighted
  - the power grid unavailability put at stack the local backup facilities, leading to the unavailability of the supply to communication/control devices
  - This, in turn, caused strong delays in the restoration process (**Escalation effect**)

Example of cascading effect – Blackout in North America and Canada – 14/8/2003

Sequence of events:

- The Midwest ISO (MISO) state estimator and real-time contingency analysis (RTCA) software not functioning properly from 12:15 to 16:04
  - prevented MISO from performing proper "early warning" assessments as the events were unfolding
- At the First Energy (FE) Control Center, a number of computer software problems occurred on the Energy Management System (EMS) starting at 14:14
  - contributed to inadequate situation awareness at FE until 15:45
- Trip of East Lake 5 at 13:31:34 and lines in Ohio between 15:05:41 and 15:41:35
- Due to EMS failures at FE and MISO control centers, no proper actions (such as load shedding) taken
- Critical event leading to widespread cascading outages in Ohio and beyond was tripping of Sammis-Star 345 kV line at 16:05:57

- **Load shedding in northeast Ohio at this stage could have prevented cascading outages that following**

Blackout in North America and Canada – contd.

- At 16:10:38, cascading loss of major lines in Ohio and Michigan affected also power transfer from Canada (Ontario) to the US on the Michigan border
- Voltage collapsed due to extremely heavy loadings on transmission lines
- **Cascading outages of several hundred lines and generators leading to blackout of the region**
- Approximately **50 million people** in 8 states in the US and 2 Canadian provinces affected
- During this disturbance, over 400 transmission lines and 531 generating units at 261 power plants tripped

➢ Failure of critical apparatus of the control system did not allow prompt reaction to the electrical problem, causing the **cascade effect** (again , an interdependence problem)

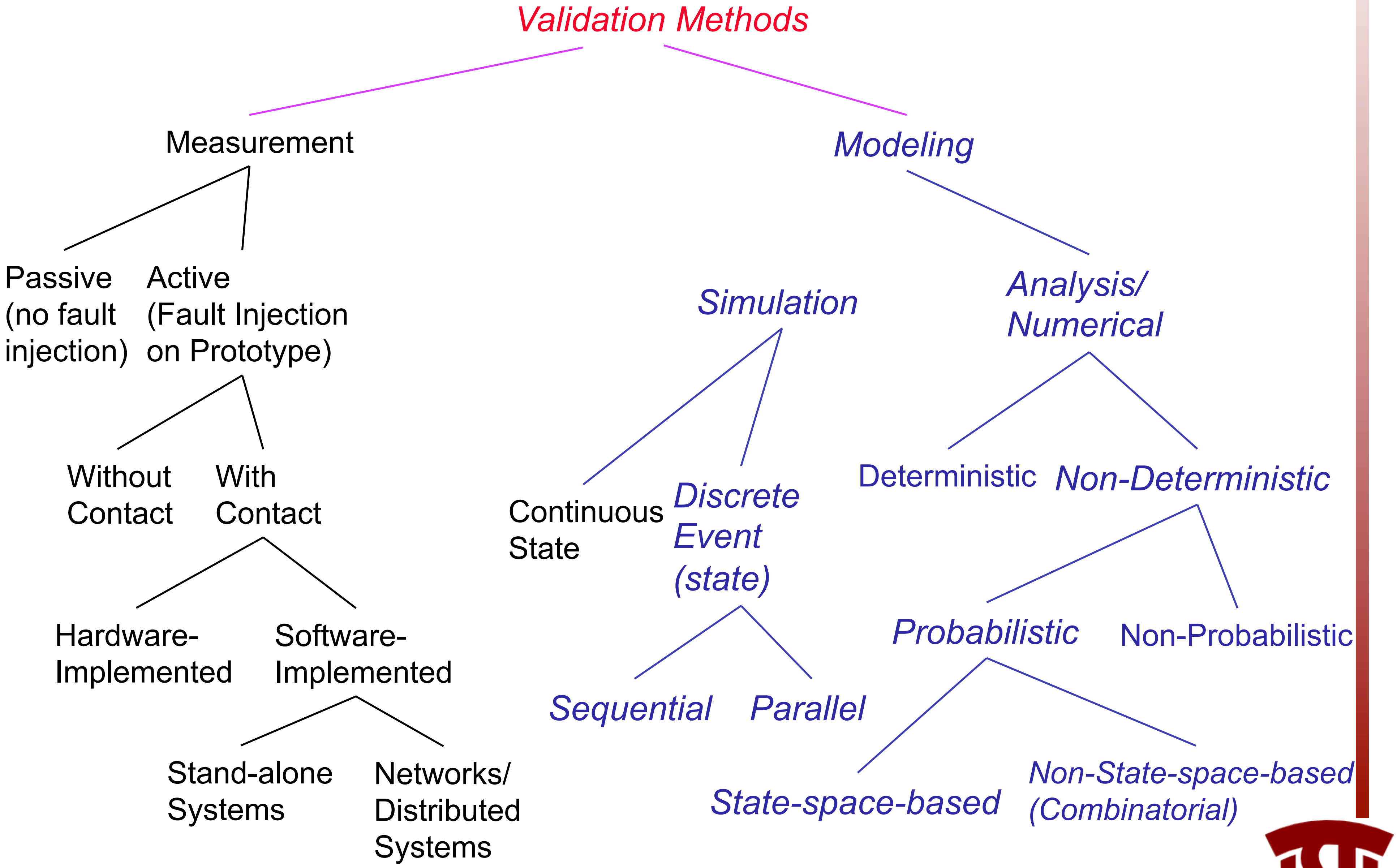
Summarizing some considerations

- An **analysis and evaluation process** is required to identify vulnerabilities, interdependencies and inter-operability between systems,
  - to understand what specific assets of the addressed CI are utmost critical and need to be protected the most
- Following this analysis, steps can be taken to **mitigate the identified vulnerabilities**, in an order that reflects the assessed level of criticality.
- Including also aspects related to **interdependencies** intra- and inter- critical infrastructures allows a greater understanding of the **cascading effects** caused by damage to a particular asset and protect that asset accordingly.
- **Evaluating that an asset may be more critical than another**, due to its effects on other infrastructures and essential services, plays a very important role when looking at CI:
  - For example, if an electric substation is damaged leading to a blackout, complications are experienced by a number of other systems/infrastructures and by the services they provide, like railroad operations causing a decreased movement of commodities and potential complications for emergency services.
  - Thus, that electric substation must be protected not only for the Energy Sector, but also for the safeguarding of other sectors infrastructure.

Validation through the Model-based approach

(from Bill Sanders teaching material)

Validation: the process of determining whether a **realization** meets its **specification**



Validation Methods

Measurement

Modeling

Passive (no fault injection)

Active (Fault Injection on Prototype)

Simulation

Analysis/ Numerical

Without Contact

With Contact

Continuous State

Discrete Event (state)

Deterministic

Non-Deterministic

Hardware-Implemented

Software-Implemented

Sequential

Parallel

Probabilistic

Non-Probabilistic

Stand-alone Systems

Networks/ Distributed Systems

State-space-based

Non-State-space-based (Combinatorial)

Choosing Validation Techniques

There are several choices:

- ❑ **Combinatorial** modeling
- ❑ **Analytic/numerical** modeling
- ❑ **Simulation** (including fault injection on a simulated system)
- ❑ **Measurement** (including performance benchmarking and fault injection on a prototype system)

Each with differing advantages and disadvantages

Choice of a validation method depends on:

- ❑ **Stage of design** (is it a proposed or existing system?)
- ❑ **Time** (how long until results are required)
- ❑ **Tools** available
- ❑ **Accuracy**
- ❑ **Ability to compare** alternatives
- ❑ **Cost**
- ❑ **Scalability**

When does Validation take place?

In all the stages of the system development process:

➢**Specification** - Combinatorial modeling, Analytic/Numerical modeling

➢**Design** - Analytic/Numerical modeling, Simulation modeling

➢**Implementation** - Detailed Simulation modeling, Measurement, including Fault Injection

➢**Operation** - Combinatorial modeling, Analytic/Numerical modeling, Detailed Simulation modeling, Measurement, including Fault Injection

Specification and Realization evolve throughout the lifecycle of a system

Choosing Validation Techniques cont.

Criterion	Combinatorial	State-based space	Simulation	Measurement
Stage	Any	Any	Any	Post-prototype
Time	Small	Medium	Medium	Varies
Tools	Formulae, spreadsheets	Languages & Tools	Languages & Tools	Instrumentation
Accuracy	Low	Moderate	Moderate	High
Comparison	Easy	Moderate	Moderate	Difficult
Cost	Low	Low/Medium	Medium	High
Scalability	High	Low/Medium	Medium	Low

Some guidelines to system validation

In general, always be suspicious of validation results...

- **Guidelines**:
  - Validate simulations with analytic models and measured data
  - Validate analytic models with simulations and measured data
  - Validate measured data with analytic models and simulations
- **And, in particular, always**
  - Evaluate “boundary cases” to which you know the answers
  - Make sure trends are as you expect, or understand why they are not

The “Art” of Performance and Dependability Validation

- **Performance and Dependability validation is an art because**:
  - There is no recipe for producing a good analysis,
  - The key is knowing how to abstract away unimportant details, while retaining important components and relationships,
  - This intuition only comes from experience,
  - Experience comes from making mistakes.
- **There are many ways to make mistakes.**

Doing it Right

- Understand the desired **measure before you build the model** or design a measurement or fault-injection experiment.
- The desired **measure determines the type of model**, **performance benchmark, or fault-injection experiment** and the level of detail required.
  - **No model or measurement technique is universal.**
- First step: choose the desired measures:
  - Choice of measures form a basis for comparison.
  - It's easy to choose wrong measure and see patterns where none exist.
  - Measures should be refined during the design and validation process.
- Understand the meaning of the obtained measures:
  - Numbers are not insights.
  - Understand the accuracy of the obtained measures, e.g., confidence intervals for simulation.

More Doing it Right

- **Include all critical aspects in a model of a system:**
  - Once measures are chosen, you must choose what system aspects to include in the model.
  - It is almost never possible or practical to include all system aspects.
- **Use representative input values:**
  - The results of a model solution, performance benchmark, or fault injection experiment are only as good as the inputs.
  - Inputs will never be perfect.
  - Understand how uncertainty in inputs affects measures.
  - Do sensitivity analysis.
- **Include important points in the design/parameter space:**
  - Parameterize choices when design or input values are not fixed.
  - A complete parametric study is usually not possible.
  - Some parameters will have to be fixed at “nominal” values.
  - Make sure you vary the important ones.

More Doing it Right

- **Make all your assumptions explicit**:
  - Results from models, benchmarks, or fault-injection experiments are only as good as the assumptions that were made in obtaining them.
  - It's easy to forget assumptions if they are not recorded explicitly.
- **Use the appropriate model solution or measurement technique:**
  - Just because you have a hammer doesn't mean the world is a nail.
  - Fault injection and simulation, numerical/analytic, and combinatorial solutions all have their places.
- **Keep social aspects in mind:**
  - Dependability analysts almost always bring bad news.
  - Bearers of bad news are rarely welcomed.
  - In presentations, concentrate on results, more than on the process.

Model Validation

- Model validation is the process of making sure that the **model** you build is **correct**.

Correctness means two things:

1) The model **accurately represents** the system,
2) The **model specified is the model intended**.

Models may be validated using a number of methods:

- **Modular design**: test modules separately; interchange functionally similar modules,
- **N-version models**: high-level and detailed models should give similar results,
- **Run simplified cases**: e.g., one packet in the network,
- **Tracing**: examine one trajectory,
- **Understand trends**: understand the direction of the trends, and any discontinuities.

More on Model Validation

- Models are frequently validated by three methods:
  - **Measurements**: measures on the model should match measures on the real system,
  - **Theoretical results**:
    - measure something to which you already know the answer, e.g., throughput cannot exceed capacity,
  - **Insight of experts**:
    - Modeler expertise comes with experience,
    - Consult with people who understand the system.

- Validating a model is similar to validating software
  - **Design review**: present the model design to a small committee that will critically review it.
  - **"Code" review**: someone else critically examines the model in detail.
  - **Assertions**: place assertions in the model to warn when things go wrong.
  - **Black box/White box testing**.

What is a Model

A **Model** is an **abstraction** of a system

> "that highlights the important features of the system organization and provides ways of quantifying its properties neglecting all those details that are relevant for the actual implementation, but that are marginal for the objective of the study"(*)

Therefore:

- Making the **right assumptions** on system components and environment is a crucial issue
- **Assumptions** depend on the **indicator** under analysis

(*)*Definition from G. Balbo, "Introduction to stochastic petri nets", Lectures on Formal Methods and Performance Analysis, volume 2090 of Lecture Notes in Computer Science, pages 84-155. Springer Verlag, 2001*

Power Grid Systems: logical structure

Part I: focus on the Transmission segment

The Context

Activity carried on in the context of the EU STREP 027513 **CRUTIAL** project (Critical Utility Infrastructural Resilience), which has addressed the **analysis and management of interdependencies** and of the resulting operational risk in Electric Power Systems. The innovative approach resides in modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks.

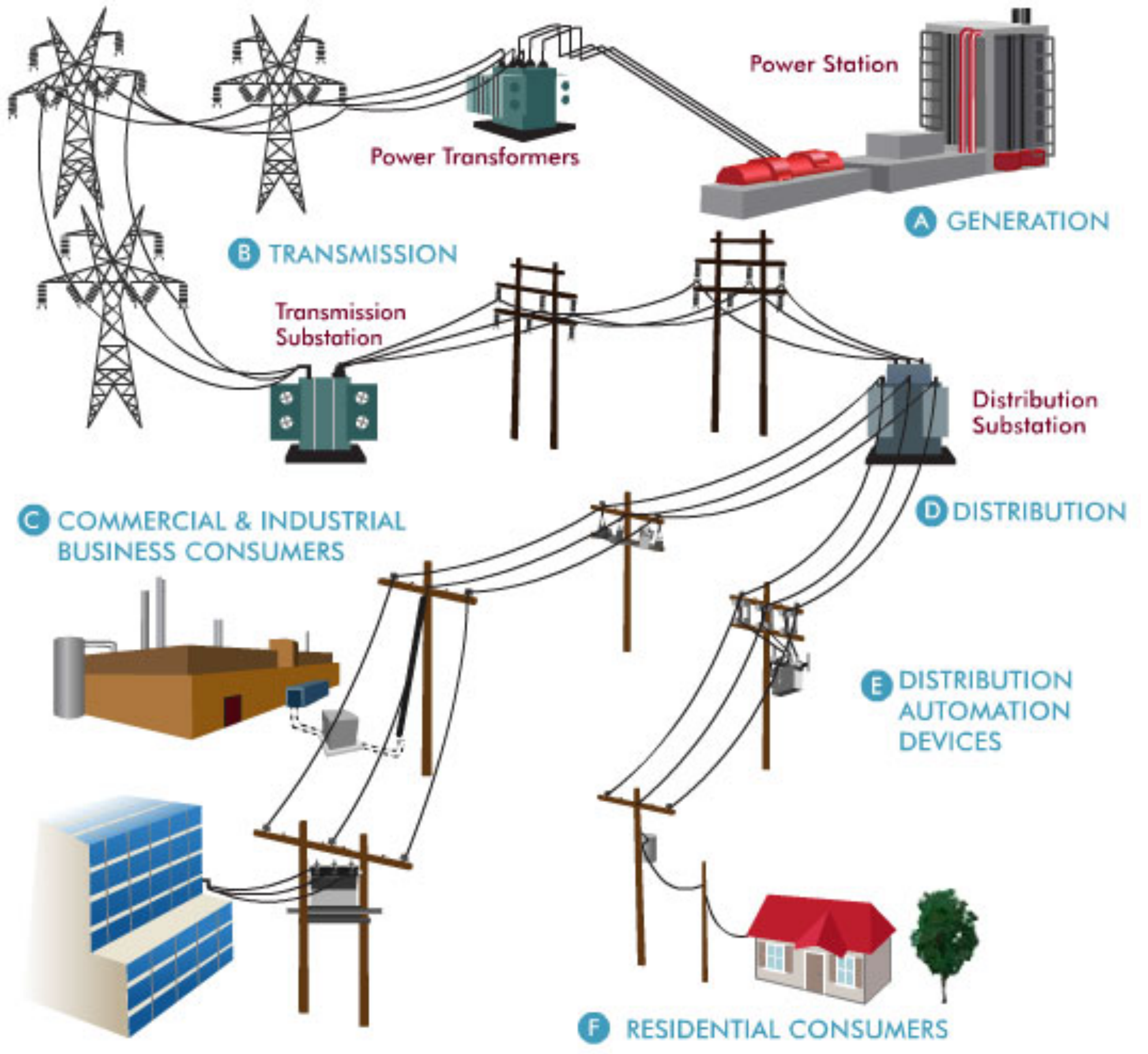
The objectives of the project were:

- investigation of **models and architectures** that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures;
  - **analysis of critical scenarios** in which faults in the information infrastructure provoke serious impacts on the controlled electric power infrastructure;
  - investigation of **distributed architectures** enabling dependable control and management of the power grid.

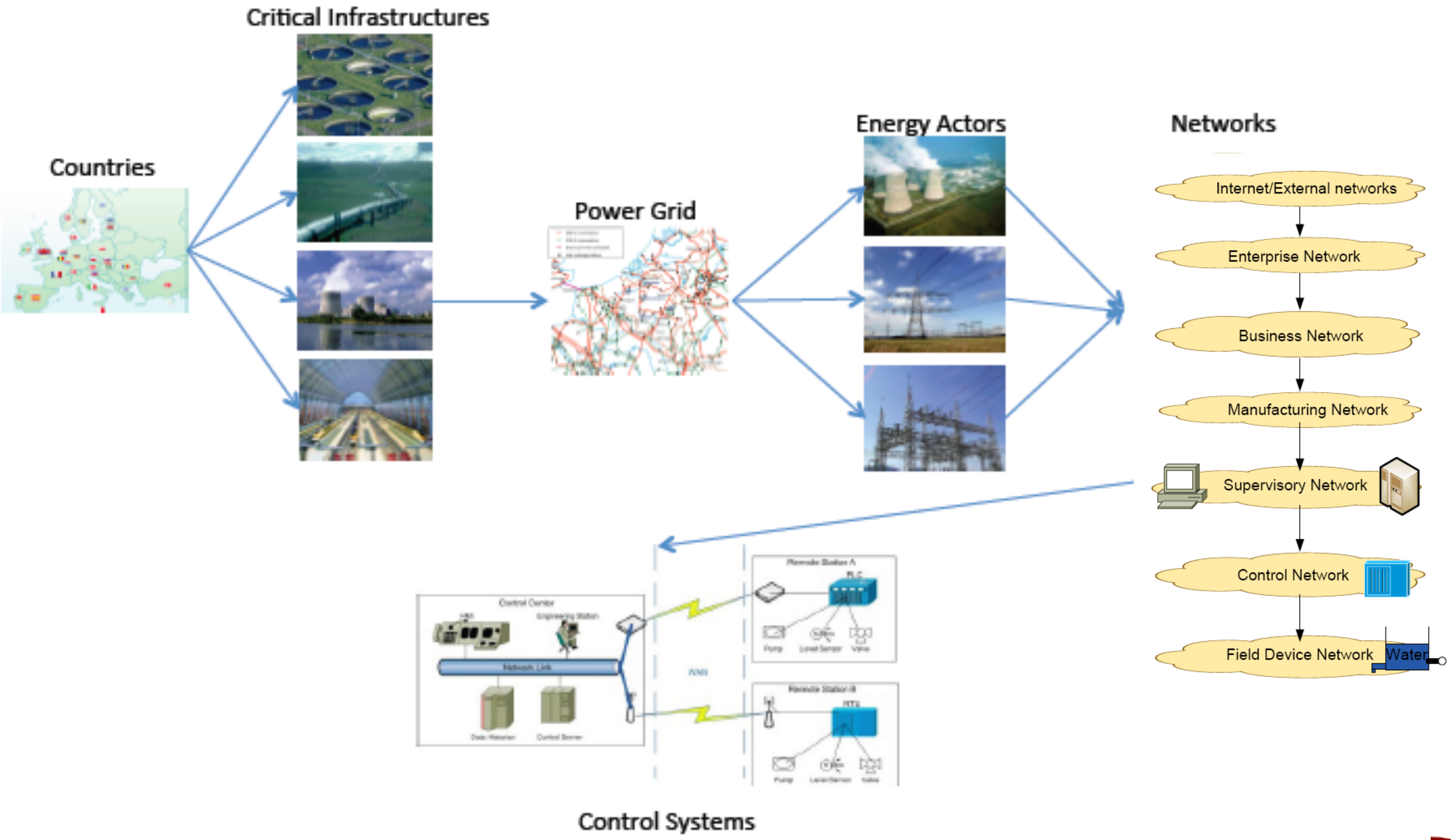
The project run from February 2006 to April 2009

6 Partners involved: Cesi Ricerca, Italy; University of Lisbon, Portugal**; CNR-ISTI, Italy**; CNRS-LAAS, France; K.U. Leuven, Belgium; CNIT – Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Italy
http://crutial.rse-web.it

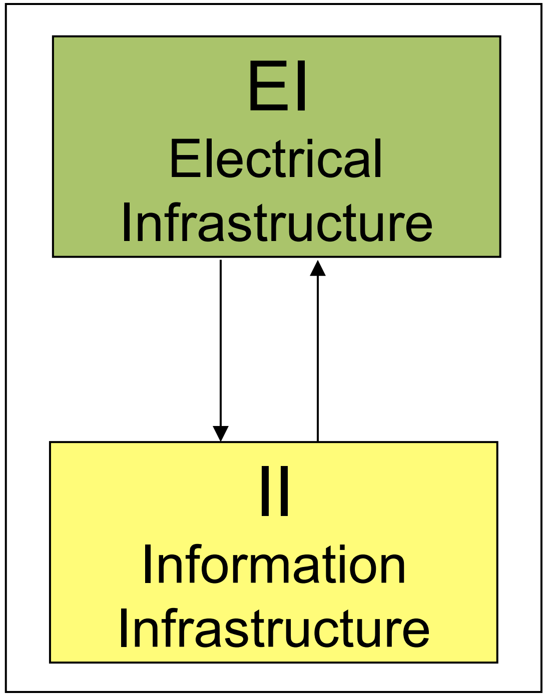
The power/electricity sector



Wider view of the Electricity Sector



High-level view of the Power Grid System



Two interacting Infrastructures:

- **Electrical Infrastructure (EI)**, which produces and transports the electric power to the final users
- **Information Infrastructure (II)**, which controls the EI, mainly with the objectives of:

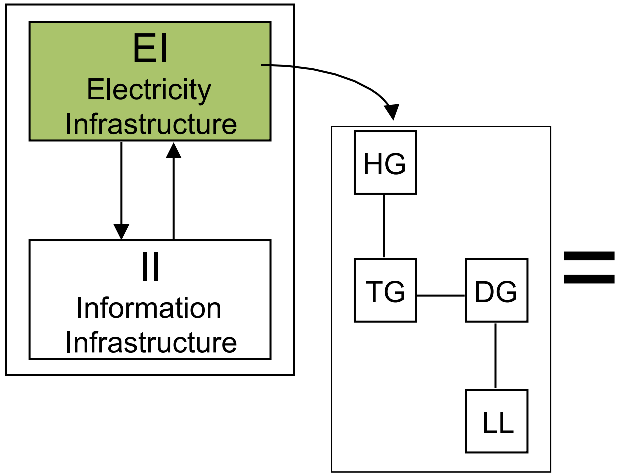
  i) reducing out of service time of generators, power lines and substations (availability);

  ii) enhancing quality of service (through frequency and voltage regulation);

  iii) optimizing generators and substations management.

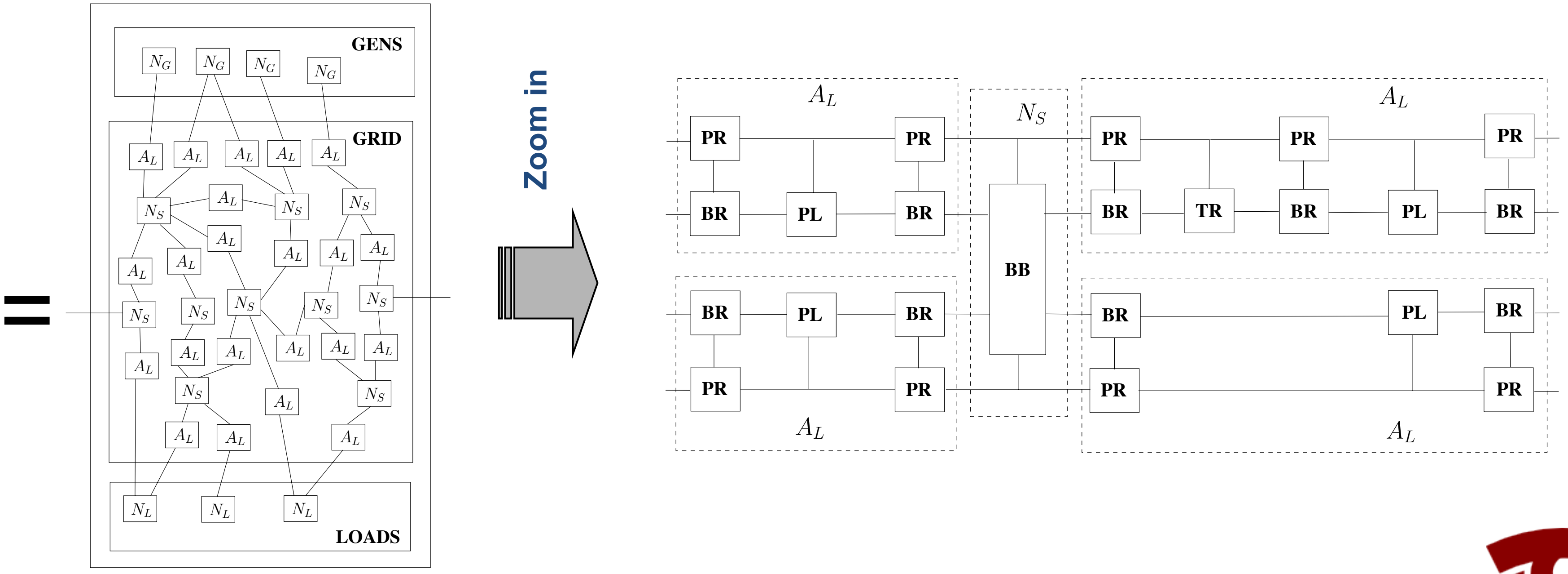
- An **event** (e.g. failure or recovery) that occurs in one sub-system can “affect” the behavior of the other sub-system (**interdependencies**).

Electric infrastructure

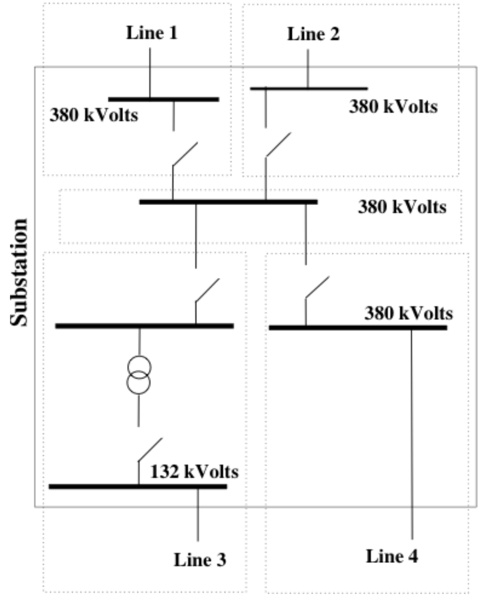


The **EI** produces and transports the electric power to the final users

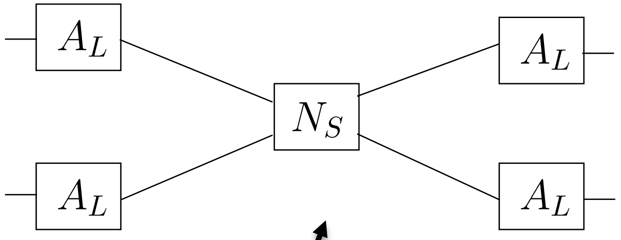
- **HG**: high voltage generation plant
- **TG**: transmission grid
- **DG**: distribution grid
- **LL**: medium and low voltage load



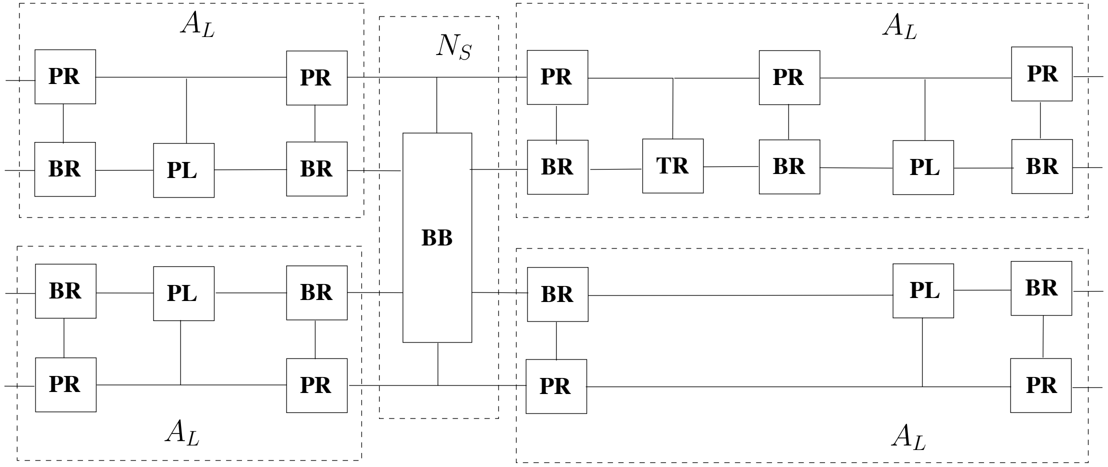
Focusing on substation and power lines



Physical view



High-level Logical views



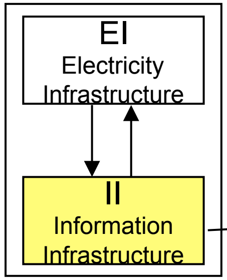
Low-level Logical views

Information Infrastructure

Logical components of II:

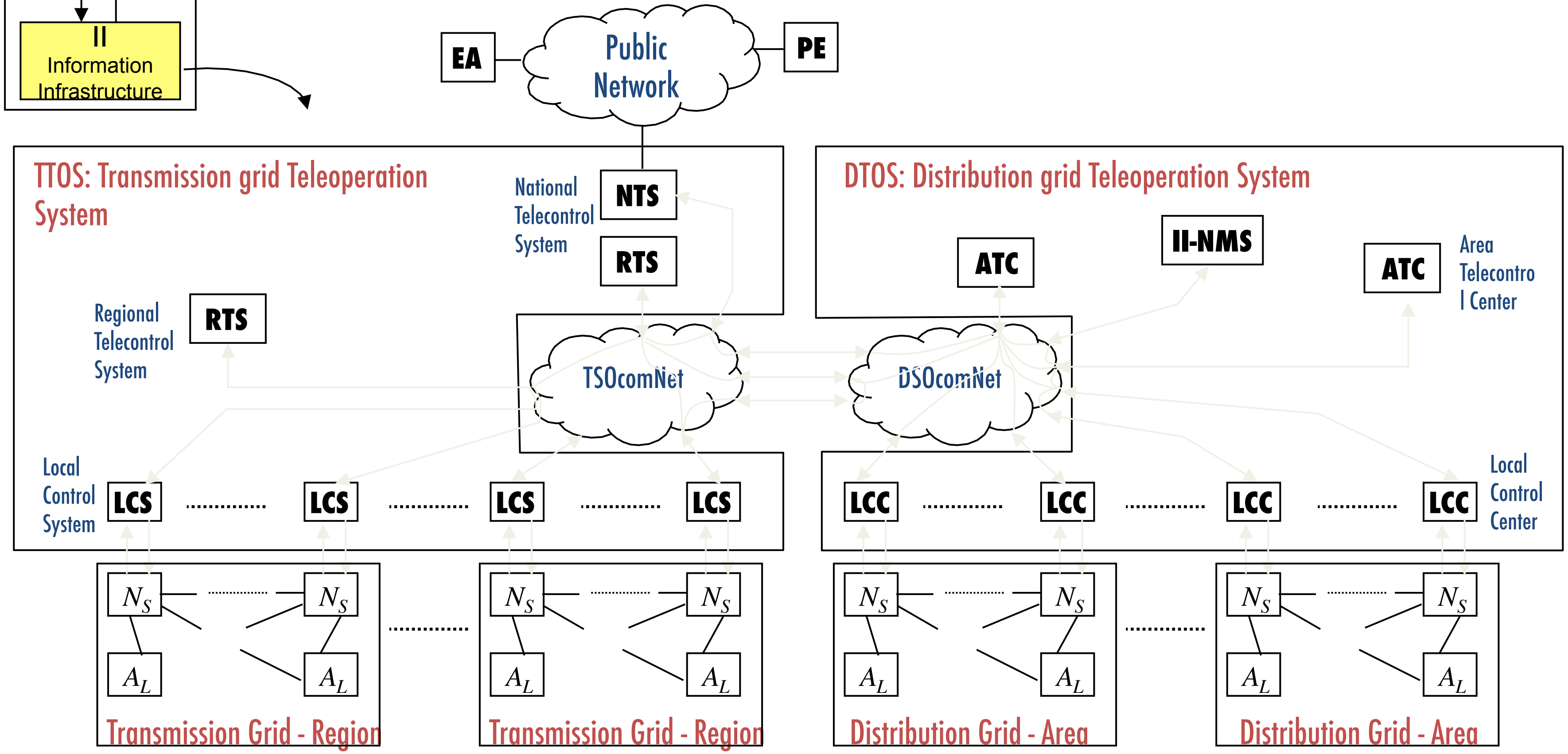
- Protection system;
- Frequency and voltage regulation systems;
- Tele-operation systems (DTOS for the DG and TTOS for the TG)

They interact through a **hierarchical structure,** using public and/or private networks to exchange information and control data. They differ for their **criticality** and for the **locality** of their decisions



EI
Electricity Infrastructure

II
Information Infrastructure



EA

Public Network

PE

TTOS: Transmission grid Teleoperation System

National Telecontrol System

NTS

RTS

Regional Telecontrol System

RTS

TSOcomNet

Local Control System

LCS .... LCS .... LCS .... LCS

DTOS: Distribution grid Teleoperation System

ATC

II-NMS

ATC

Area Telecontrol Center

DSOcomNet

Local Control Center

LCC .... LCC .... LCC LCC

N_S .... N_S

A_L A_L

Transmission Grid - Region

Transmission Grid - Region

Distribution Grid - Area

Distribution Grid - Area

EI Failure Model

- 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.

- 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.

II Failure Model

The failures of the II components can be summarized in:

- omission failure,
- time failure,
- value failure, and
- byzantine failure.

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

State definitions

- The 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

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

S_{II}=(discrete part)

E.g.: S_{II}=(Working, Partially failed, Lessened, Passive latent error, Active latent error, …)

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 II (including erroneous, delayed or not required reconfiguration)

The state of II changes in case of:

- Failure/recovery of an II component
- Disruption of the EI

Interdependencies

S_{II} ➔ 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} ➔ S_{II}

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 II, or isolate part of the II

(S_{EI} and S_{II}) ➔ (S_{EI} or S_{II})

E.g. an II 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)

Major assumptions

- The EI state is determined by the equations for the DC (direct current) power flow approximation (derived from the standard alternate current AC circuit equations), which give a linear relationship between:
  - the power at the nodes and
  - the power flow on the lines
- Abstraction level of infrastructures representation to trade between
  - Sufficient accuracy
  - Manageable complexity of the modelling process and model solution, in particular, about the **control infrastructure**:
    - Represent the **effect of the application of the control functions/ actions** on the grid topology (in terms of grid reconfiguration), instead of modelling in detail the control itself
    - Model the **effect of faults** (errors/failures of infrastructures components), which could be of accidental nature as well as intentional attacks

Focus on the modelling framework - 1

- Definition of a **conceptual modelling fram**ework, based on a **modular approach** by **composing template atomic models**, to allow representation of a variety of EPS configurations
- 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

Focus on the modelling framework - 2

Modelling power aspects

- **The framework should support:**
  - Different formalisms for different sub-models
  - Representation of continuous and discrete states
  - Time and probability distributions, as well as enabling conditions can depend on both the continuous and the discrete state
  - Call to functions implementing the reconfiguration, regulation and auto-evolution algorithms
  - Definition of measures, appropriate for EPS risk analysis

Focus on the modeling framework - 3

Modelling efficiency aspects

- **The framework should support:**
  - Hierarchical composition of different sub-models
  - Replication of (anonymous and non-anonymous) sub-models (sharing a common state)
  - Compact representation of the grid topology (e.g. using incidence matrix [nodes x arcs])
  - 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

Measures of Interest

- Measures representative of the resilience/QoS of the service delivered by the EPS
- of interest to operators, service providers, as well as final customers, e.g. :
  - The expected **percentage of undelivered power** (the undelivered power divided by the power demand) at time t and in the interval [0, t]
  - The expected **numbers of components affected by a disruption** at time t and in the interval [0, t]
  - The expected **reward** at time t and in the interval [0, t], based on a reward structure where costs are associated to generators, rewards are associated to satisfied loads and a cost is associated to each interruption of service
  - …

The defined measures of interest can be evaluated in terms of **mean, variance or distribution**

Framework's implementation

The basic modeling mechanisms have been implemented using **Stochastic Activity Networks** and **Möbius** tool, focusing on:

Electrical Infrastructure components:

- **Nodes** (Substations, Generators and Loads)
- **Power Lines**, with their **Protections**

Information Infrastructure components:

Local operations $RS_1()$ (performed by LCS), and

Global operations $RS_2()$ (performed by RTS)

TSOcomNetw: public or private network

The definition of **$RS_1()$** and **$RS_2()$** depends on the policies and algorithms adopted by II. They are obtained by solving a linear programming problem **to minimize the change in generation or load shedding, subject to the system constraints.**

The new state determined by **$RS_1()$** is suboptimal wrt **$RS_2()$** (being based on local information);

$RS_1()$ completes in time **$T_1=0$**, while **$RS_2()$** in time **$T_2>0$**

And accounting for both **EI components and II components failures**

Incremental approach to the EPS study

EPS study carried on **incrementally**, to gradually master complexity and gain confidence in the modeling and analysis results:

1. **Transmission segment** of the electrical grid, considering only **one region** from the control point of view
2. **Transmission segment** of the electrical grid, accounting for **multiple regions** from the control point of view
3. **Distribution segment** of the electrical grid, including **renewable energy resources** and accounting for more sophisticated control towards the smart grid management

Adopted Formalism and Tool

- Formalism adopted in the power grid modeling framework:

  Stochastic Activity Networks – SAN

W. H. Sanders and J. F. Meyer. Stochastic Activity Networks: Formal Definitions and Concepts. In European Educational Forum: School on Formal Methods and Performance Analysis, pages 315{343, 2000.

- Tool for development and solution of models:

  Möbius

D. Daly, D. D. Deavours, J. M. Doyle, P. G. Webster, and W. H. Sanders. Möbius: An extensible tool for performance and dependability modeling. In B. R. Haverkort, H. C. Bohnenkamp, and C. U. Smith, editors, 11th Int. Conf., TOOLS 2000, volume 1786 of LNCS, pages 332–336. Springer Verlag, 2000.

https://www.mobius.illinois.edu/

Stochastic Activity Networks

(from Bill Sanders teaching material)

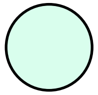
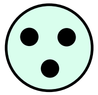
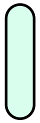
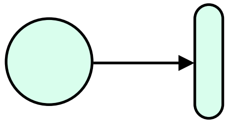
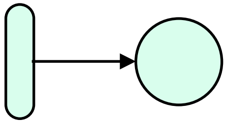
Introduction on SAN

Stochastic activity networks, or SANs, are a convenient, graphical, high-level language for describing system behavior.
SANs are useful in capturing the stochastic (or random) behavior of a system.
They extend stochastic Petri Nets and have the following properties:

- A general way to specify that an activity (transition) is enabled
- A general way to specify a completion (firing) rule
- A way to represent zero-timed events
- A way to represent probabilistic choices upon activity completion
- State-dependent parameter values
- General delay distributions on activities

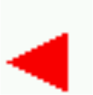
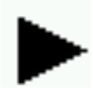
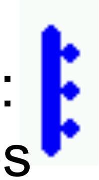
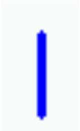
Stochastic Petri Net Review

One of the simplest high-level modeling formalisms is called *stochastic Petri nets*. A stochastic Petri net is composed of the following components:

places:		which contain tokens, and are like variables
tokens:		which are the “value” or “state” of a place
transitions:		which change the number of tokens in places
input arcs:		which connect places to transitions
output arcs:		which connect transitions to places

SAN Symbols

Stochastic activity networks (SANs) have four new symbols in addition to those of SPNs:

- Input gate:  used to define complex enabling predicates and completion functions
- Output gate:  used to define complex completion functions
- Cases:  (small circles on activities) used to specify probabilistic choices
- Instantaneous activities:  used to specify zero-timed events

Completion Rules

When an activity ***completes***, the following events take place (in the order listed), possibly changing the marking of the network:

1. **If the activity has cases, a case is (probabilistically) chosen.**

2. **The functions of all the connected input gates are executed (in an unspecified order).**

3. **Tokens are removed from places connected by input arcs.**

4. **The functions of all the output gates connected to the chosen case are executed (in an unspecified order).**

5. **Tokens are added to places connected by output arcs to the chosen case**.

Ordering is important, since effect of actions can be marking-dependent.

General Delay Distributions

SANs (and their implementation in *Möbius*) support many **activity time distributions**, including:

- Exponential
- Hyperexponential
- Deterministic
- Weibull
- Conditional Weibull
- Normal

- Erlang
- Gamma
- Beta
- Uniform
- Binomial
- Negative Binomial

- All distribution parameters can be marking-dependent
- The obvious implication of general delay distributions is that there is no conversion to a CTMC. Hence, no solutions to CTMCs are applicable. However, simulation is still possible.
- Analytical/numerical solution is possible for certain mixes of exponential and deterministic activities. See the Möbius manual for details.

Reward Variables

Reward variables are a way of **measuring** performance- or dependability-related characteristics about a model.

Examples:

- Expected time until service
- System availability
- Number of misrouted packets in an interval of time
- Processor utilization
- Length of downtime
- Operational cost
- Module or system reliability

Reward Structures

Reward may be "**accumulated**" in two different ways:

- A model may be in a certain state or states for some period of time, for example, "CPU idle" states. This is called a *rate reward*.
- An activity may complete. This is called an *impulse reward*.

The reward variable is the sum of the rate reward and the impulse reward structures.

Model Composition

A **composed model** is a way of connecting different SANs together to form a larger model.

Model composition has two operations:

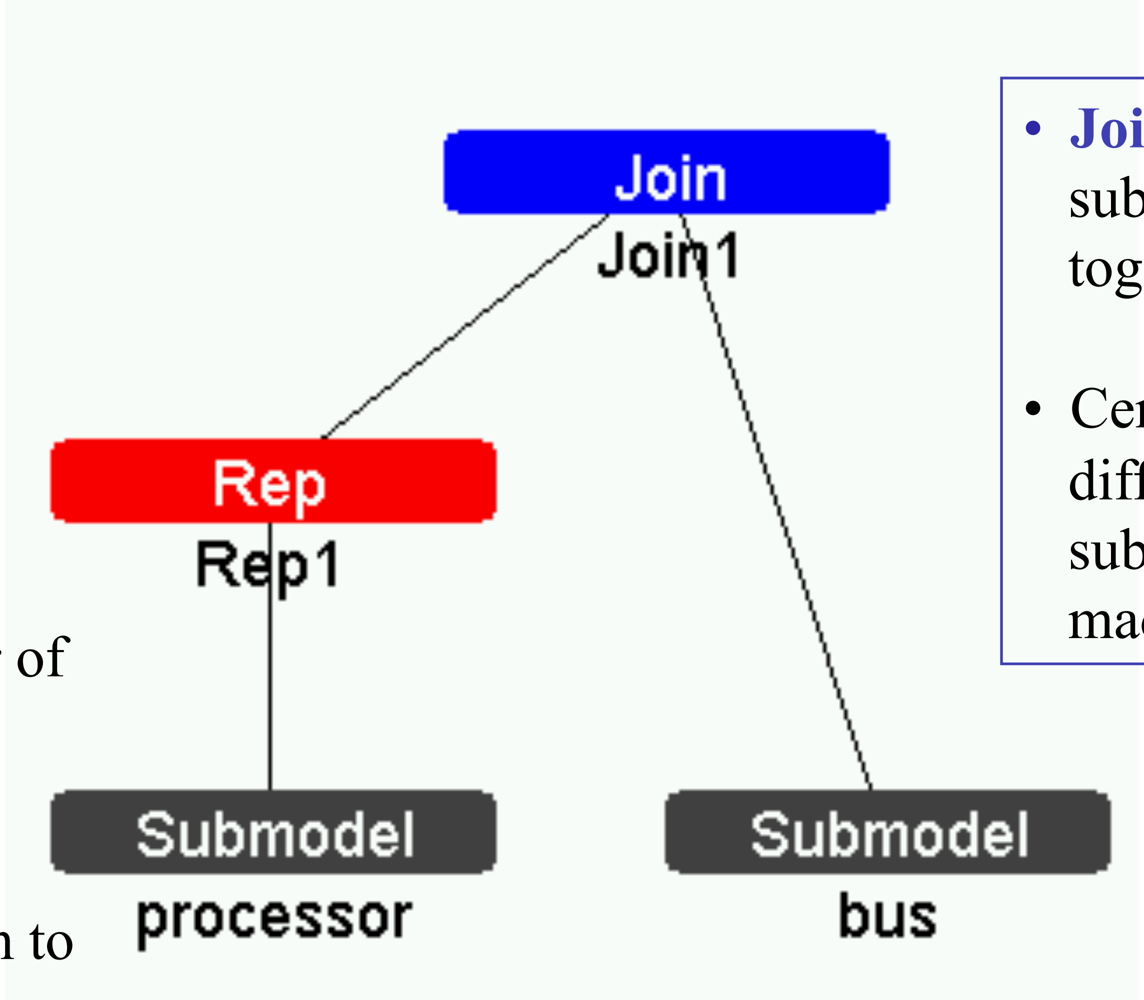
- **Replicate**: Combine 2 or more identical SANs and reward structures together, holding certain places common among the replicas.

- **Join**: Combine 2 or more different SANs and reward structures together, combining certain places to permit communication.

Composed Model Specification

- **Replicate** submodel a certain number of times

- Hold certain places common to all replicas



- **Join** two or more submodels together

- Certain places in different submodels can be made common

Rationale for model composition

There are many good reasons for using composed models.

- Building highly reliable systems usually involves redundancy. **The replicate operation models redundancy in a natural way**.
- Systems are usually built in a modular way. **Replicates and Joins are usually good for connecting together similar and different modules**.
- Tools can take advantage of something called the ***Strong Lumping Theorem*** **that allows a tool to generate a Markov process with a smaller state space**.

Möbius

Möbius™ is a software tool for modeling the behavior of complex systems, originally developed to study dependability and performance indicators of computer and network systems

Möbius Features (from the tool website https://www.mobius.illinois.edu/):

- **Multiple modeling languages**, based on either graphical or textual representations: Supported model types include stochastic extensions to Petri nets, Markov chains and extensions, and stochastic process algebras. Models are constructed with the right level of detail, and customized to the specific behavior of the system of interest.

- **Hierarchical modeling paradigm**: Build models by combining individual components from the ground up. Allows to easily examine alternative system designs.

Möbius Features - 2

- **Customized measures of system properties**: Construct detailed expressions that measure the exact information desired about the system (e.g., reliability, availability, performance, and security). Measurements can be conducted at specific time points, over periods of time, or when the system reaches steady state.

- **Study the behavior of the system under a variety of operating conditions**: Functionality of the system can be defined as model input parameters, and then the behavior of the system can be automatically studied across wide ranges of input parameter values to determine safe operating ranges, to determine important system constraints, and to study system behaviors that could be difficult to measure experimentally with prototypes.

Möbius Features - 3

- **Distributed discrete-event simulation**: Evaluates the custom measures using efficient simulation algorithms to repeatedly execute the system, either on the local machine or in a distributed fashion across a cluster of machines, and gather statistical results of the measures.

- **Numerical solution techniques**: Exact solutions can be calculated for many classes of models, and advances in state-space computation and generation techniques make it possible to solve models with tens of millions of states. Previously, such models could be solved only by simulation.

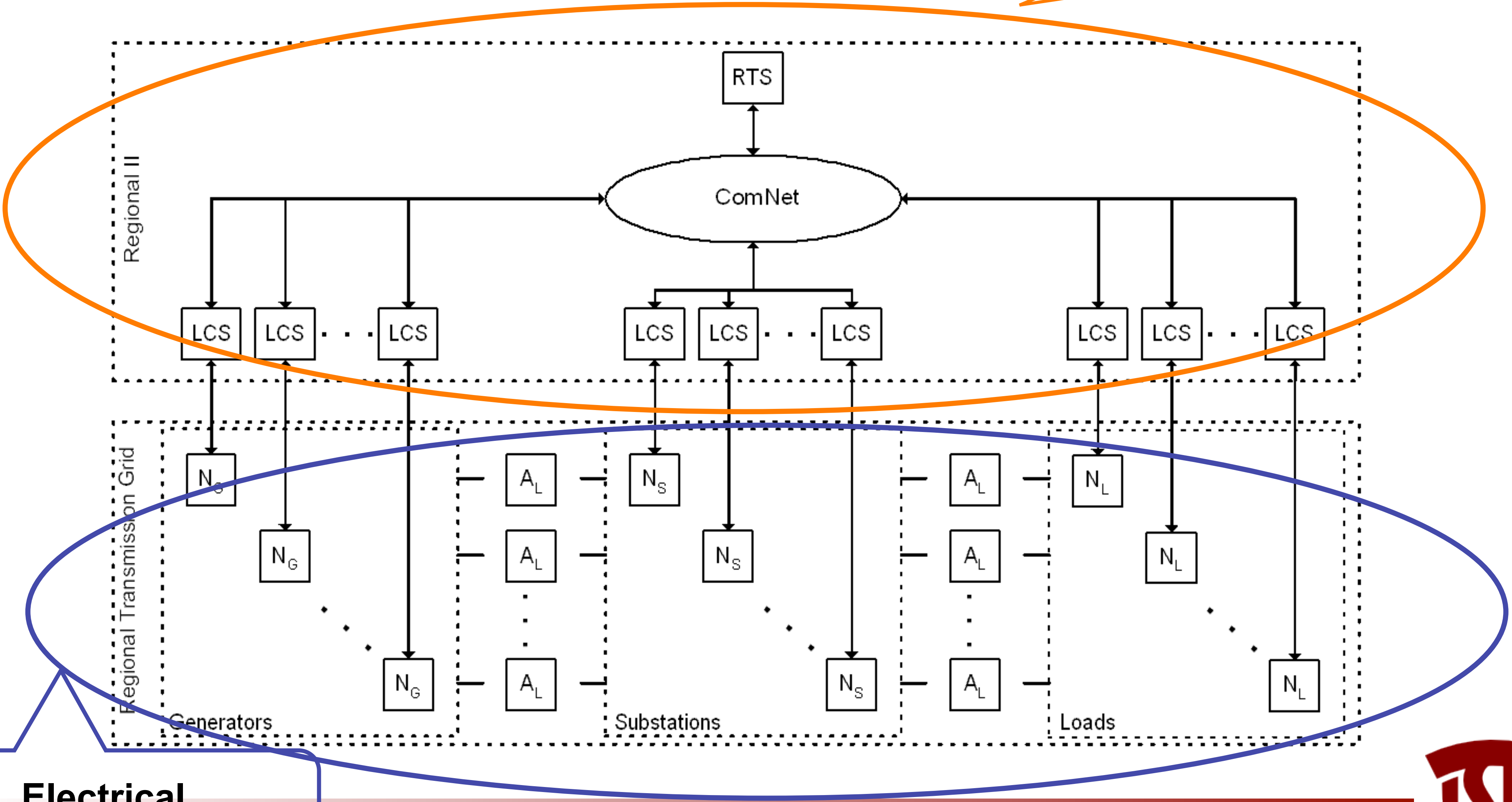
Supported Platforms

- Möbius is available for the following operating systems: Windows XP-8, Mac OSX 10.6-10.8, and Ubuntu Linux 12.04-12.10.

Study of a Region of the Electrical Power Systems (EPS)

Logical structure of a Regional EPS

Control Infrastructure



Electrical Infrastructure

Major assumptions

The EI state is determined by the equations for the DC power flow approximation (derived from the standard AC circuit equations), which give a linear relationship between:

- the power at the nodes and
- the power flow on the lines

The definition of **RS$_1$()** and **RS$_2$()** depends on the policies and algorithms adopted by II. They are obtained by solving a linear programming problem **to minimize the change in generation or load shedding, subject to the system constraints.**

$$C_2 = \sum_{i \in G} \left| P_i - P_i^0 \right| + W_L \sum_{i \in L} \left| P_i - P_i^0 \right|$$

Where:

- P_i is the injected power after the occurrence of the failure
- P_i^0 is the injected power at initial time 0

The new state determined by **RS$_1$()** is suboptimal wrt **RS$_2$()** (being based on local information);

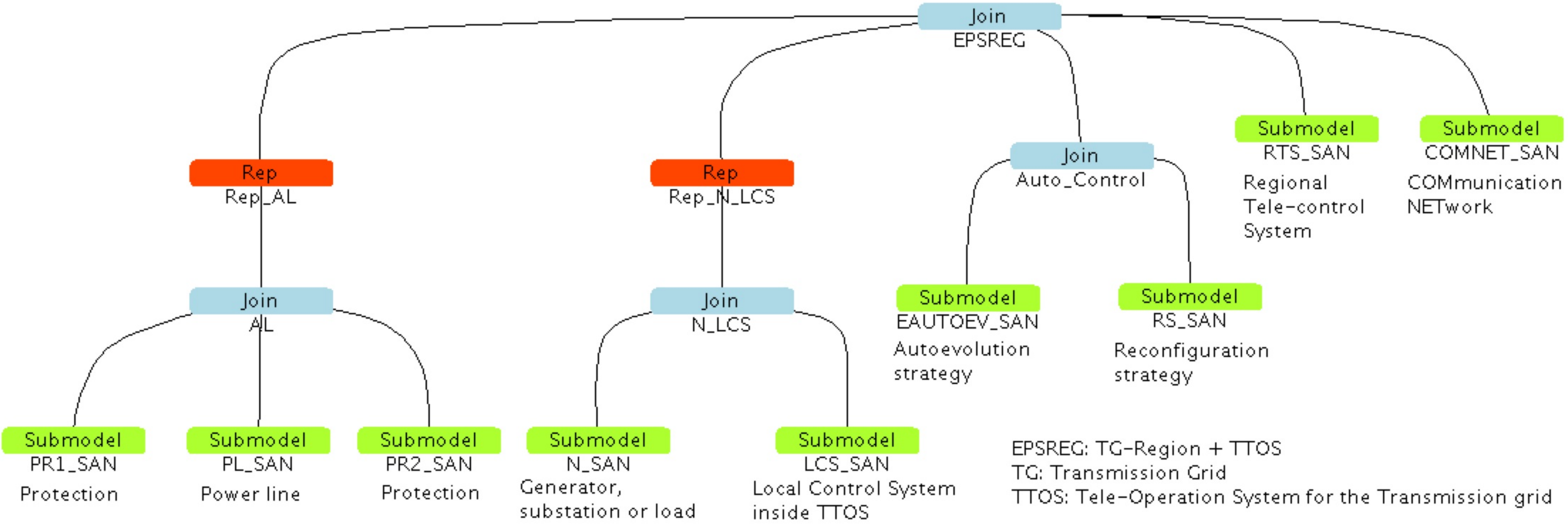
RS$_1$() completes in time **T_1=0**, while **RS$_2$()** in time **T_2>0**

Modeling Approach

Definition of atomic models for the major components identified in the logical architecture of EI and II, adopting the SAN formalism and the Mobius tool:

- **PL_SAN** represents the generic power line with connected transformers.
- **PR1_SA**N and **PR2_SAN** represent the generic protection mechanisms and breakers connected to the two extremities of the power line.
- **N_SAN** and **LCS_SAN** represent a node in the grid (generator, load or substation) and the associated LCS, respectively.
- **AUTOEV_SAN** represents the automatic evolution (autoevolution) of the electrical infrastructure when an event modifying its state occurs.
- **RS_SAN** represents the computation and application of the local reconfiguration strategy RS1(), and the computation of the regional reconfiguration action RS2() (its application is modeled by RTS_SAN).
- **RTS_SAN** and **COMNET_SAN** represent the regional telecontrol system RTS where the regional reconfiguration strategy RS2() is applied, and the public or private communications network, respectively.

The Composed Model



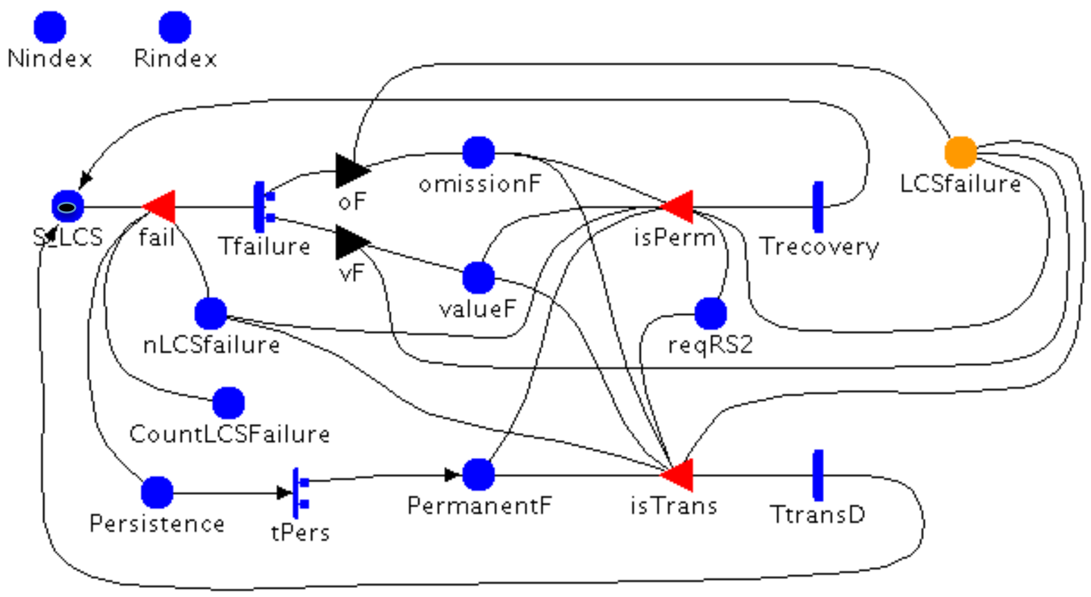
EPSREG: TG-Region + TTOS
TG: Transmission Grid
TTOS: Tele-Operation System for the Transmission grid

Rep_AL: nA not anonymous replicas of the model AL

Rep_N_LCS: nN not anonymous replicas of the model N_LCS

The submodels interact through common places

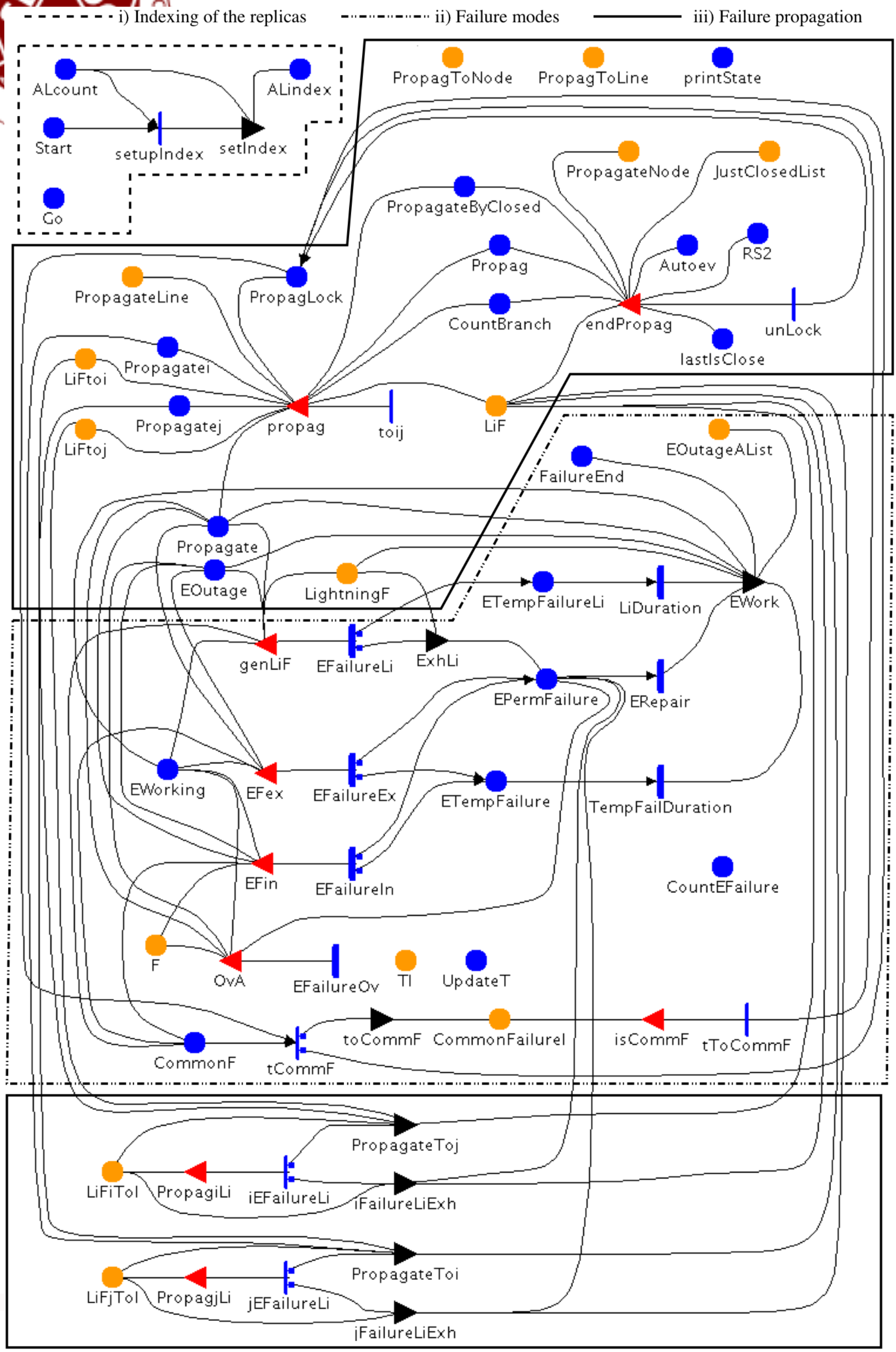
A (rather simple) atomic model: the LCS SAN



- It represents the behaviour of the **Local Control System** associated to each node of the grid.
- From the state of correctly working (place **S_LCS**), it can become failed (activity **Tfailure**) when subject to an omission or a value failure (**omissionF** or **valueF**).
- The failure is modelled with a token in the place **Persistence**, which enables the instantaneous activity **tPers**, modelling the persistence of the failure (permanent or transient). If permanent, a recovery action is started (activity **Trecovery**, which has a deteministic time). **TtransD** (exponentially distributed) models the time of persistence of a transient failure.
- At the end of a failure, a token is put in the place **S_LCS**.

The extended place **LCSfailure**, common to the whole model, stores the info related to the failed LCS and this info is removed after recovery of the LCS
When the LCS is correctly working, a token is put in the place **reqRS2** to model the availability of the LCS to perform the reconfiguration operations to the performed on the node controlled by the LCS

A more complex model….



The atomic model **PL_SAN** for a generic power line

Basic modeling elements grouped in boxes based on:

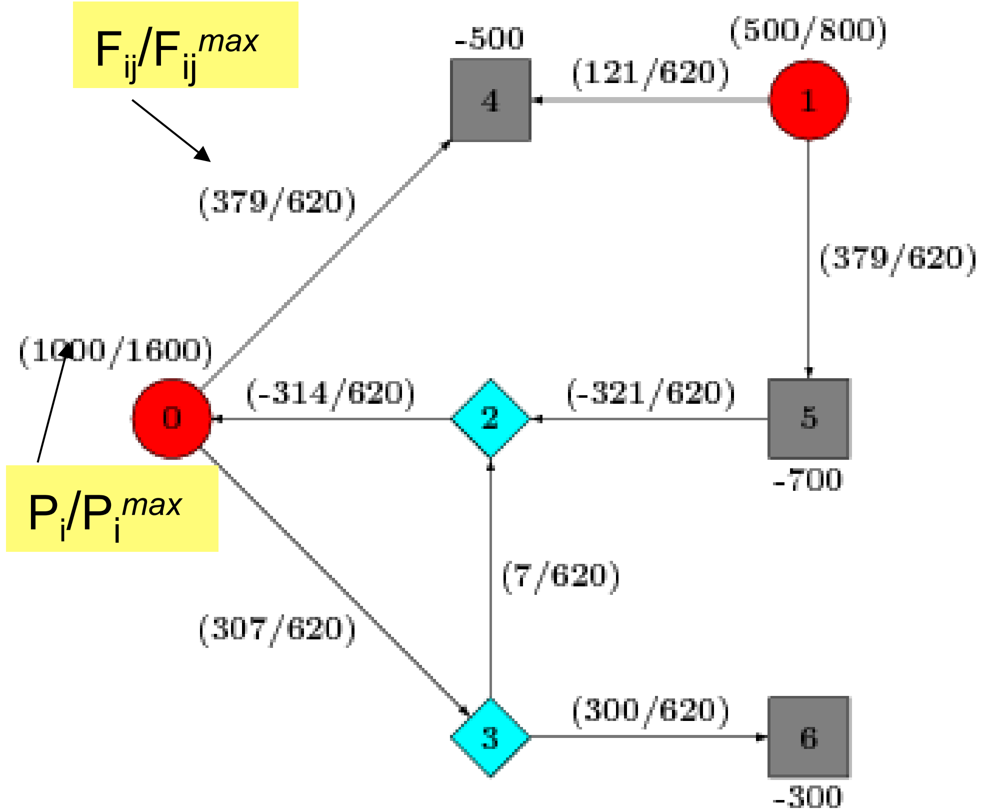
- The indexing of the replicas
- The failure modes
- The failure propagation to connected nodes

Types of analysis

- Analysis of the EI state evolution in response to EI failure events, useful to
  - trace the propagation of failure and the triggering of related phenomena along time
  - Validate the method and the models in simple, well understandable situations

- Analysis to identify critical power lines and assess the effects of a few failure scenarios on blackouts related indicators
  - Useful to understand the relative impact of involved failure/repair processes and the criticality of the electric grid elements

EI state evolution


F_{ij}/F_{ij}^{max}

P_i/P_i^{max}

2 Generators (red)
2 Substations (cyan)
3 Loads (gray)
8 Power lines

Considered failures:

- external permanent failure of line (0,4)
- omission failure of the communication network (delayed application of RTS)

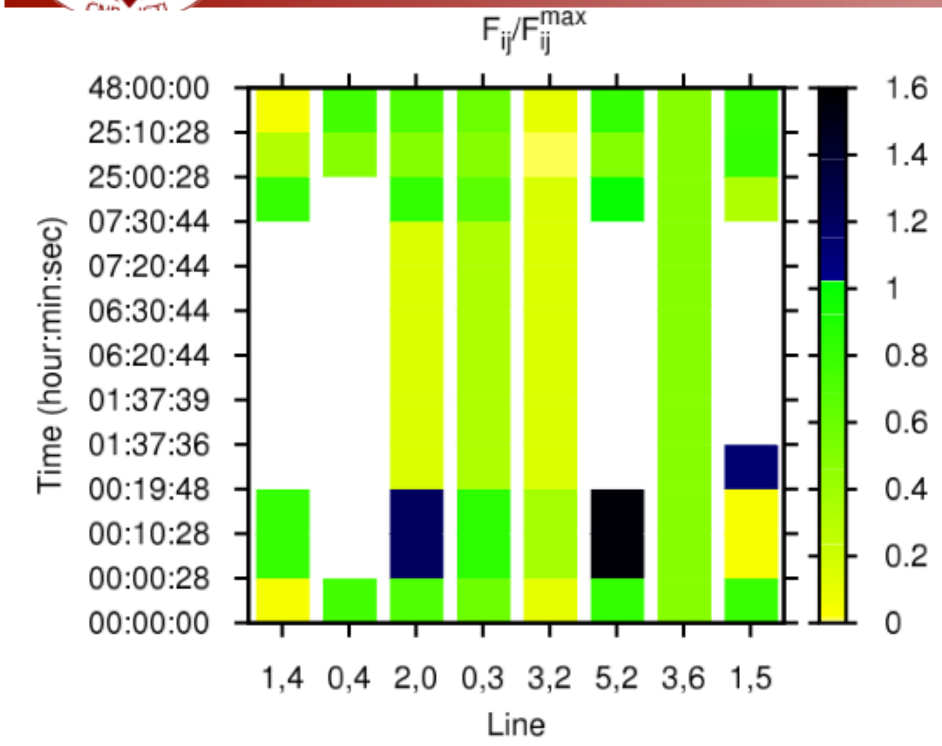
Considered time interval: 48 hours

F_{ij}^{max}= 620 MW for each i,j

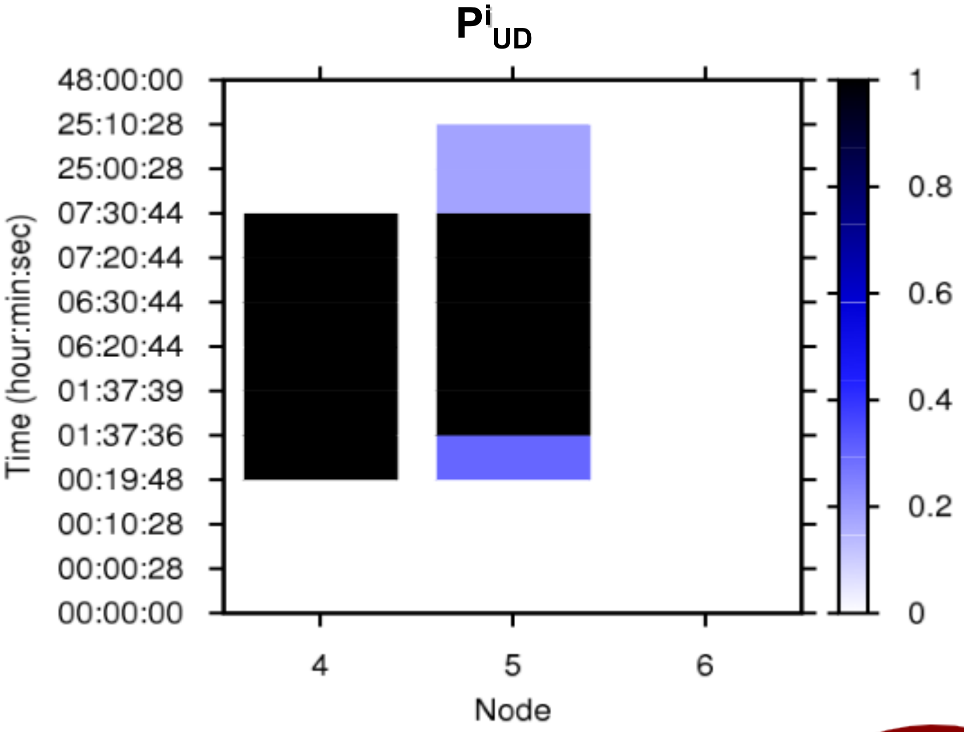
The stress level α, defined as the ratio P_i/P_i^{max}, which is equal to 0.75

Measures of interest: $\mathbf{P^{i}_{UD}(t)}$ percentage of power demanded by load I that is not met a time t

EI state evolution



- white means zero power flow
- values higher than 1(right color bar) indicate grades of overloads



- color bar represents the percentage of load not met
- white means that all demand is met and black indicates the demand is not met

Effects of failures in EI and II

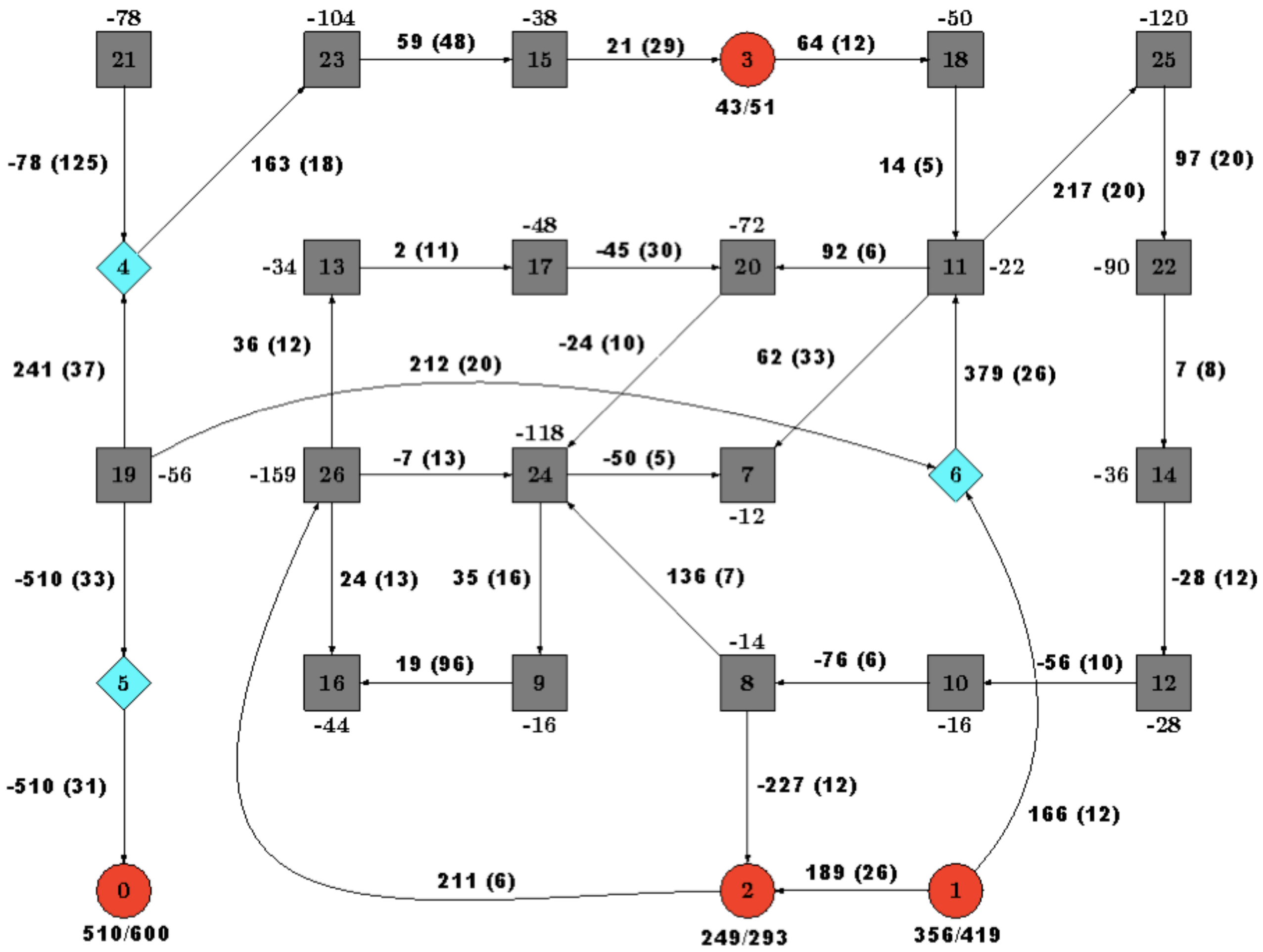


Diagram of the EI grid (a portion of the IEEE 118 Bus Test Case)

Maximum power flow through the lines = 620 MW

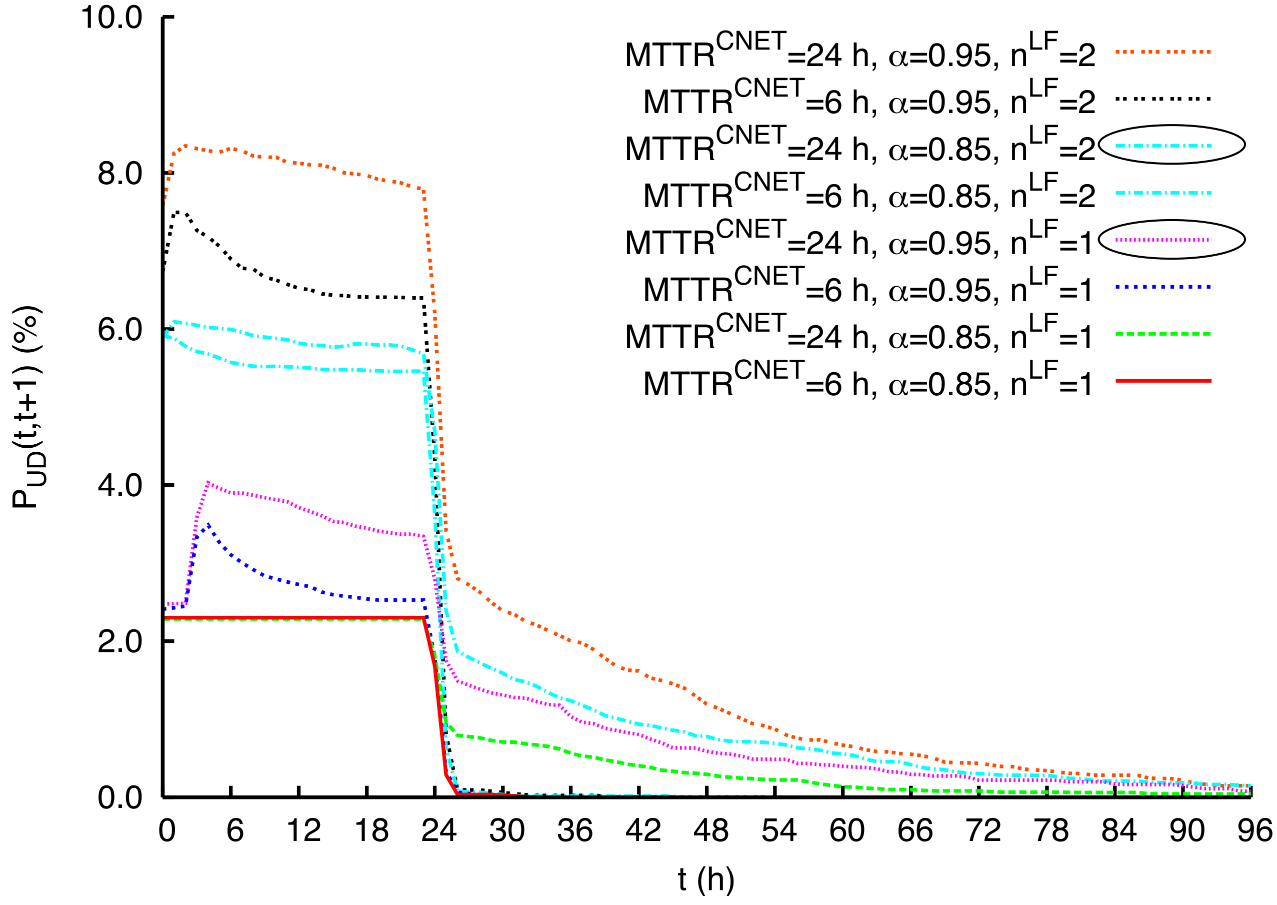
The analyzed scenario

- At time zero, **n^{LF} power lines are simultaneously affected by a permanent failure** (e.g., due to a tree fall or a terrorist attack), thus becoming unavailable.
  - The power lines that fail are randomly (*uniformly*) selected from the set of all available power lines.
  - All the failed power lines are (*deterministically*) repaired after 24 hours.

- At the same time zero, **ComNet is simultaneously affected by a denial of service (DoS) attack**.
  - The DoS attack ends after an *exponentially* distributed time with mean $MTTR^{CNET}$, and from that time RTS can start computing the RTS reconfiguration action that will be (*deterministically*) applied after 10 minutes.

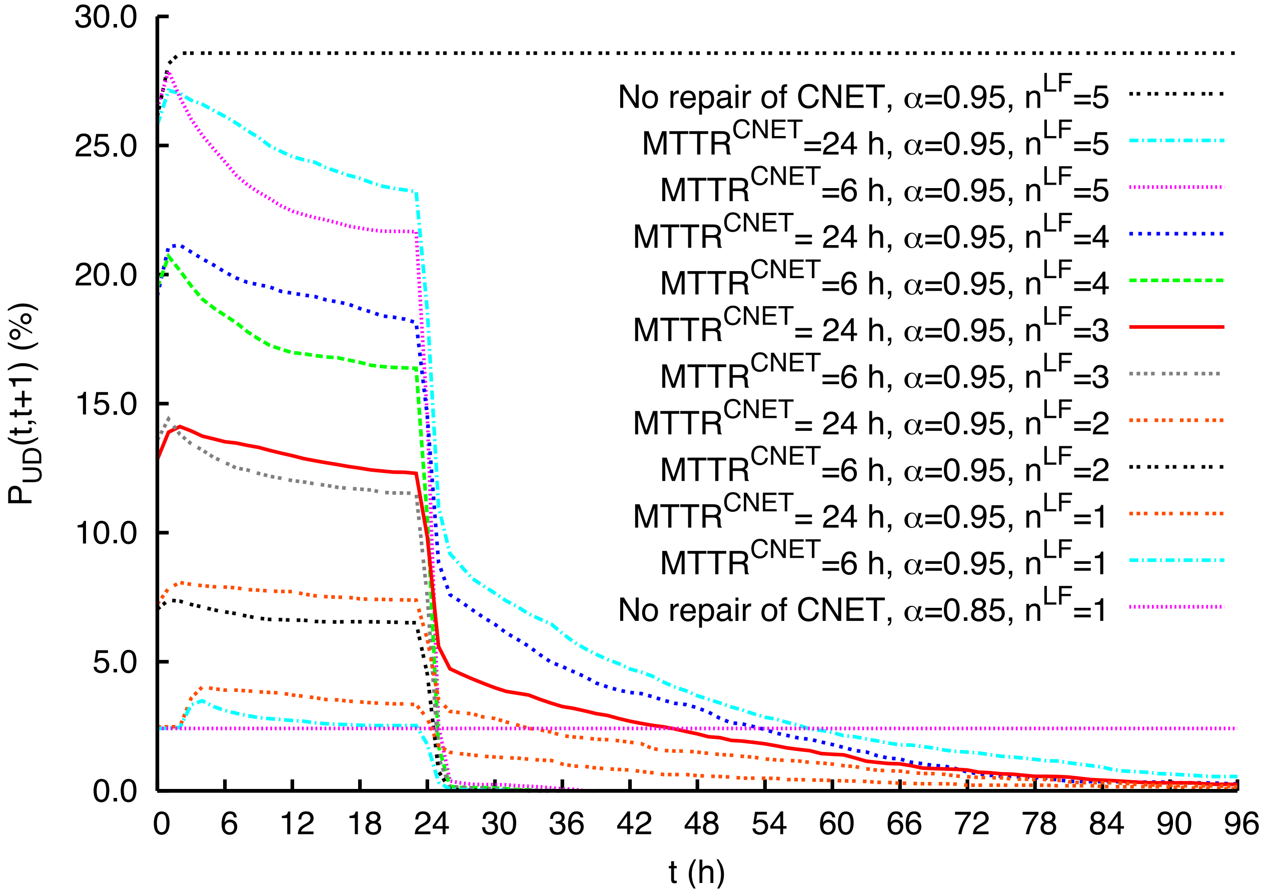
- **Measure of Interest**: **$P_{UD}(t,t+1)$**: *percentage of the mean power demand that is not met in the interval [t,t+1]* hours

$P_{UD}(t,t+1)$,with t=0,1,…,96 h., for different values of $MTTR^{CNET}$ (6,24 h.), n^{LF} (1,2) and α (0.85,0.95)



- Unless for the lowest curves (α=0.85, n^{LF}=1), the failure of even a single line at time zero produces and increment of $P_{UD}(t,t+1)$ until the reconfiguration is applied.
- At t=24 hours there is a big improvement (the failed power lines are repaired).
- The impact of the system stress level α is less heavy than the failure of power lines

P_{UD}(t,t+1) ,with t=0,1,…,96 hours, for different values of $MTTR^{CNET}$ (6,24 h.) and n^{LF} (1,…,5), fixing α=0.95

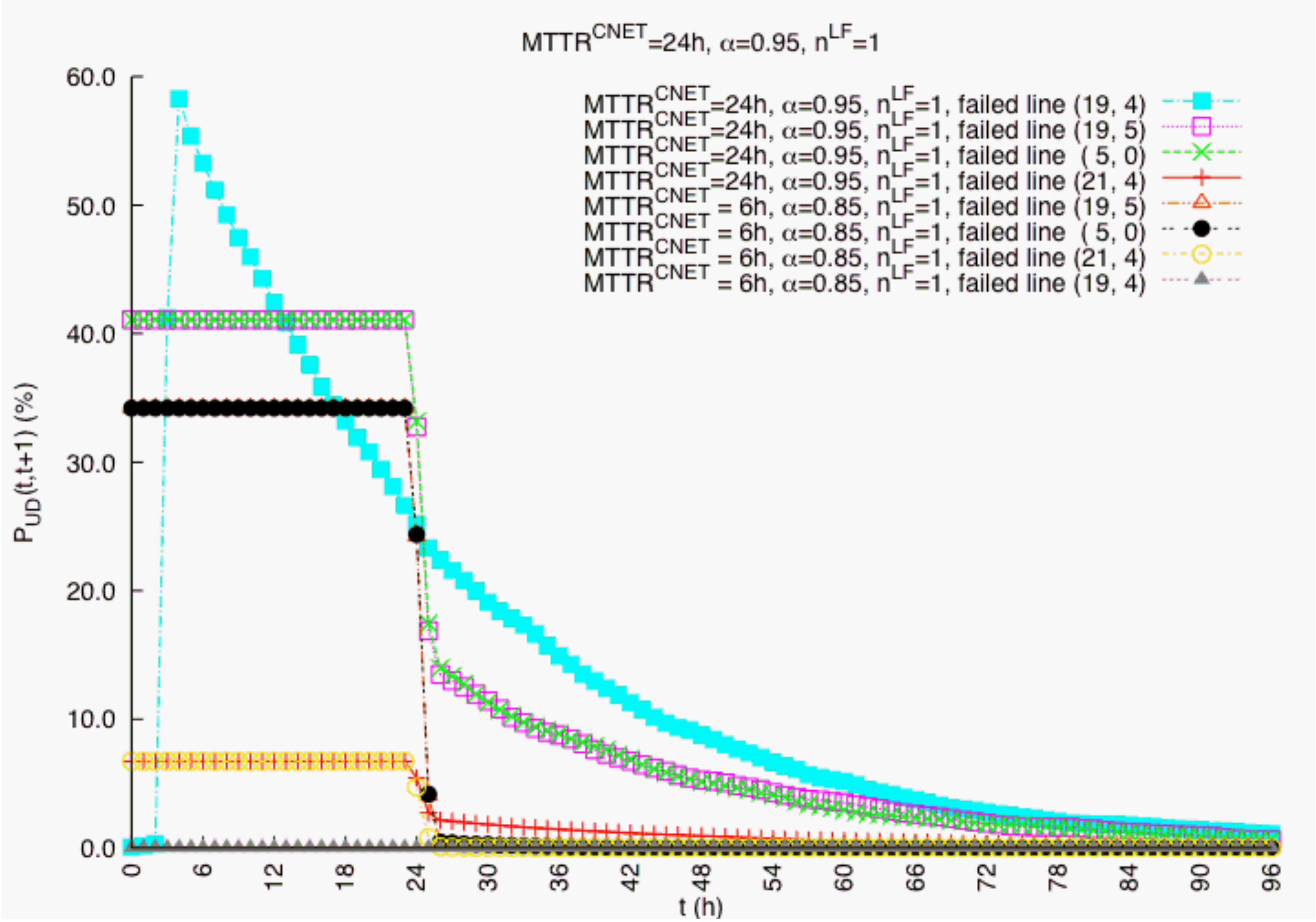


P_{UD}(t,t+1) increases considering higher n^{LF} values, and fixing the value for n^{LF}, P_{UD}(t,t+1) gets worse in the case in which the DoS attack has a longer duration (24 hours).

After 24 hours the disrupted power lines are repaired, and consequently P_{UD}(t,t+1) rapidly decreases until reaching the zero value.

The top most curve represents the case of RTS omission failure

$P_{UD}(t,t+1)$ at varying the failed power line, with t=0,1,…,96 hours, for different values of $MTTR^{CNET}$ (6,24 h.) and α (0.95, 0.85)



- Only power lines for which $P_{UD}(t,t+1) > 0$ are displayed
- Allows to determine critical power lines

Integration of SWN with SAN

- **Combination of:**
  - **SWN approach**: it is based on a Stochastic Well-formed Net (SWN) model. It represents in details the control algorithms and the communication protocol, but it makes stochastic assumption on the EI.
  - **SAN approach**: it is based on the integration of a Stochastic Activity Network (SAN) model with techniques to model and simulate the electrical state of the GRID, but control algorithms and the communication protocol are modeled in abstract way.
- In a scenario that accounts for communications between the EI and II for tele-control operations, in presence of DoS attack.
- To improve on the accuracy of the analysis of the effects of DoS on blackout-related indicators

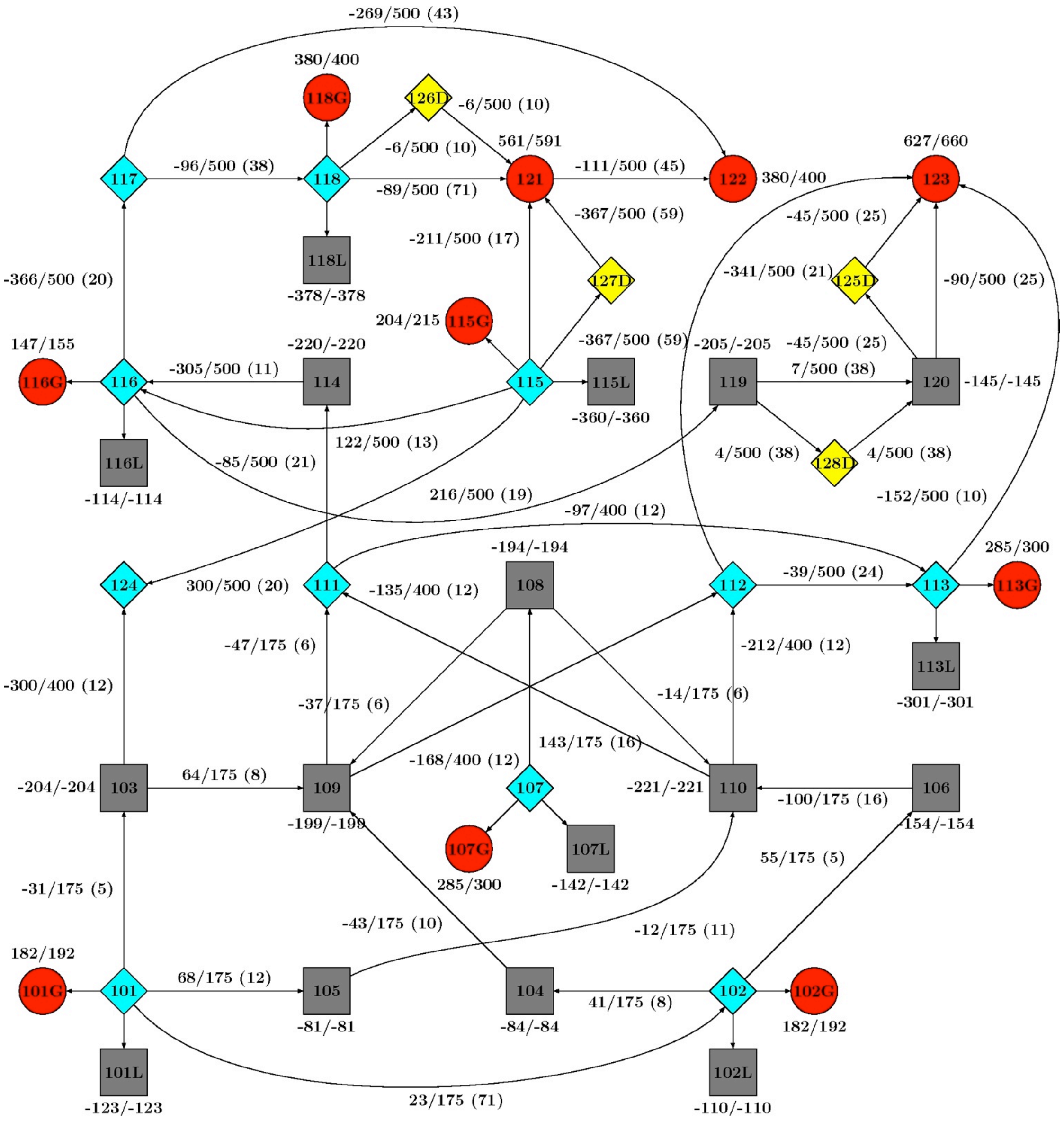
Integration of SWN with SAN - 2

- SWN focuses on the II infrastructure under a DoS attack with reference to the arming and load shedding procedure triggered by a perturbation in the EI - it has no possibility of representing efficiently the power variables
- On the other side, the SAN model does not represent the II protocol complexity in it

The interaction between the SWN and SAN models

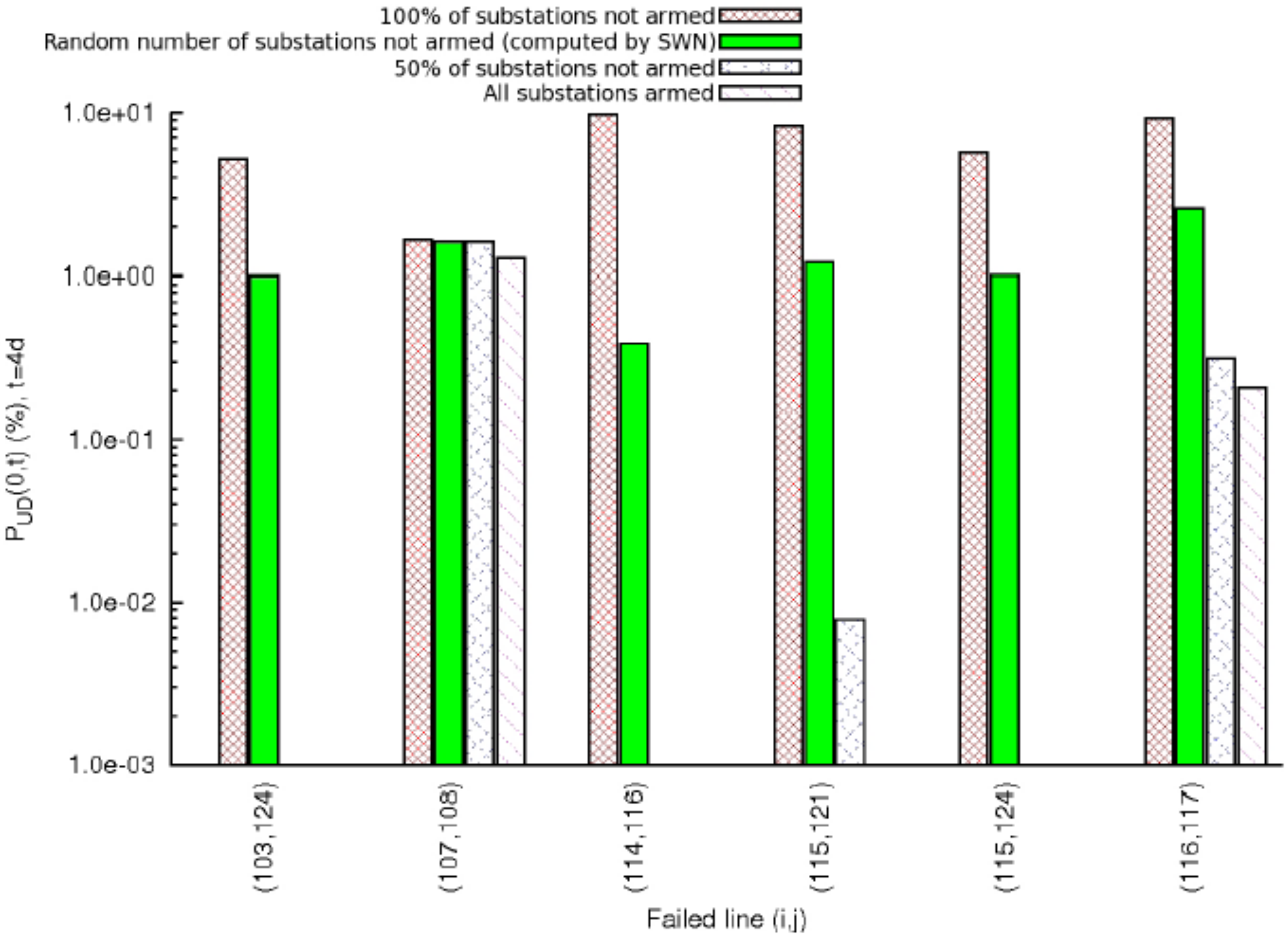
- SWN computes the probability distribution of the number of reachable and armed LCS's at time t, given the arming process started at time 0 and given an initial DoS severity level
- these distributions are used in the SAN model as an input parameter representing the number of available LCS, necessary to compute RS2() reconfiguration

Diagram of the EI grid corresponding to the RTS96 test grid



- Typically used in EPS reliability evaluation studies;
- 42 nodes (10 generators and 17 loads) and 56 power lines;
- The EI state is initially in electrical equilibrium;
- Measure of interest: $\mathbf{P}_{UD}$ (0; **l**) is the percentage of the mean power demand that is not met in the interval [0; **l**];
- Failure of a power line and a subset of the local controls not responsive because f a DoS attack.

Obtained analysis: an example



Extension to a Multi-Region Electrical Power System (EPS)

Extensions wrt the single EPS region

- □ **The Electrical Infrastructure EI** consists of a number (n_R) of interconnected regions
  - each region consists of the components already described: nodes, power lines, and protections
  - regions of the grid are connected through boundary lines

- □ **Information Infrastructure II** consists of:
  - **Local Control System LCS**, one for each node of the grid
  - **Regional Tele-Control System RTS**, one for each region
  - **TSOcomNet:** public or private network

New issues to be tackled

The new multi-regional structure implies a number of re-planning and modifications to the CRUTIAL framework:

- representation of the interconnections among the EPS regions;
- redefinition of reconfiguration functions;
- redefinition of data structures;
- adjustments to the already developed sub-models and
- introduction of new ones.

Multi-Regional Reconfiguration Functions

In case of failure, only a subset of RTS is involved in the reconfiguration: principle of **Minimum Involvement**.

The proposed algorithms are structured in steps:

①**First Step** → region(s) where the failure(s) occur constitute the first subset, then 3;

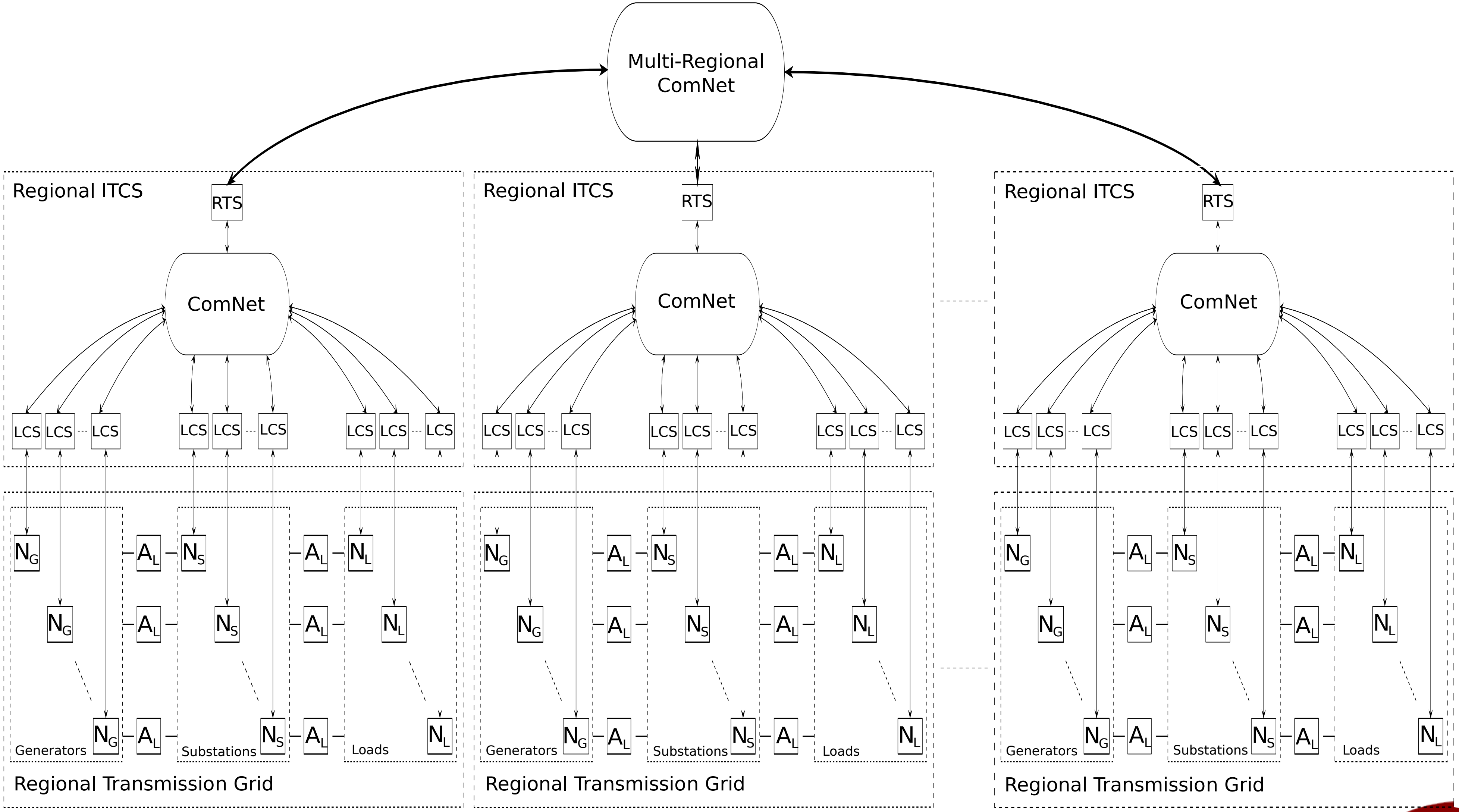
②**Next Steps** → Update the subset;

③ The LP problem is applied on the subset;

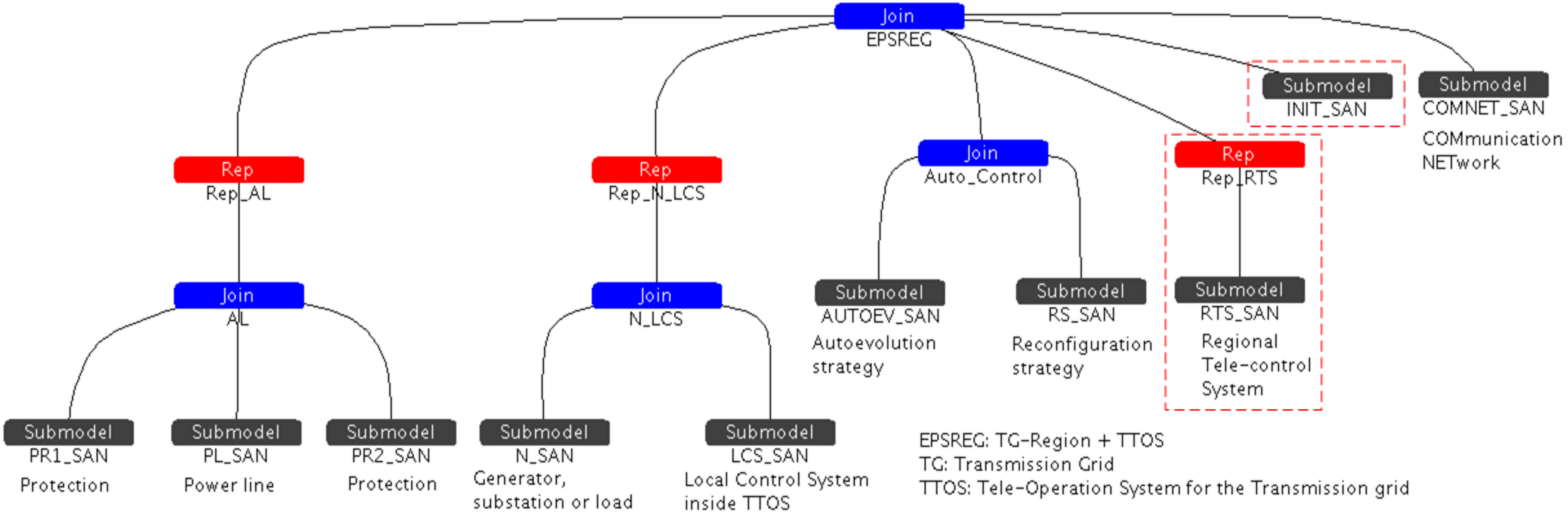
④ If LP returns a solution, the reconfiguration can be applied, otherwise 2, until all regions are exhausted.

*The new regions **to involve at the step i** are those whose Power flow on boundary lines is requested to change by the LP at **the step (i – 1)**.*

Logical structure of a Multi-Regional EPS



The extended Overall Model



EPSREG: TG-Region + TTOS
TG: Transmission Grid
TTOS: Tele-Operation System for the Transmission grid

- □ Atomic SAN models were modified taking into account the elements of the regions
- □ Added the new INIT SAN model to represent the initialization of the grid at time 0
- □ Rep_RTS: nR non anonymous replicas of the model RTS_SAN

Reconfiguration functions

RS$_1$() and **RS$_2$()** solutions are obtained by a **LP** problem to minimize the C_1 **and** C_2 cost functions, respectively.

$$C_1 = W_G \sum_{i \in G} (|P_i - P_i^*|) + W_L \sum_{i \in L} (|P_i - P_i^*|)$$

minimizes the difference between the current power value and the power value immediately before the failure occurs

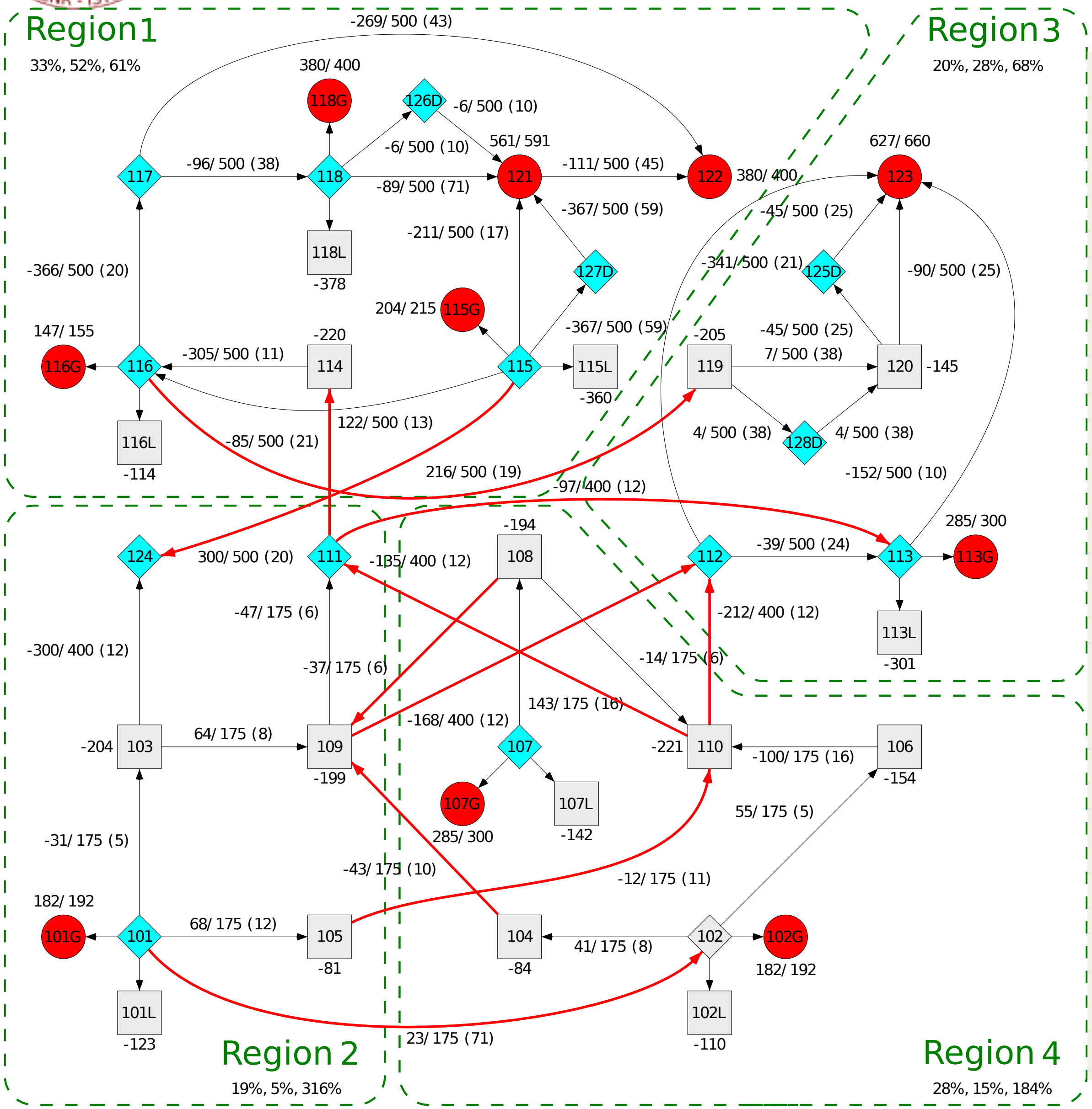
$$C_2 = W_G \sum_{i \in G} (|P_i - P_i^0|) + W_L \sum_{i \in L} (|P_i - P_i^0|)$$

minimizes the difference between the current power value and the initial power value (but other definitions could be adopted to reflect different economic conditions, e.g. minimization of costs associated to generators and/or loads)

Where:

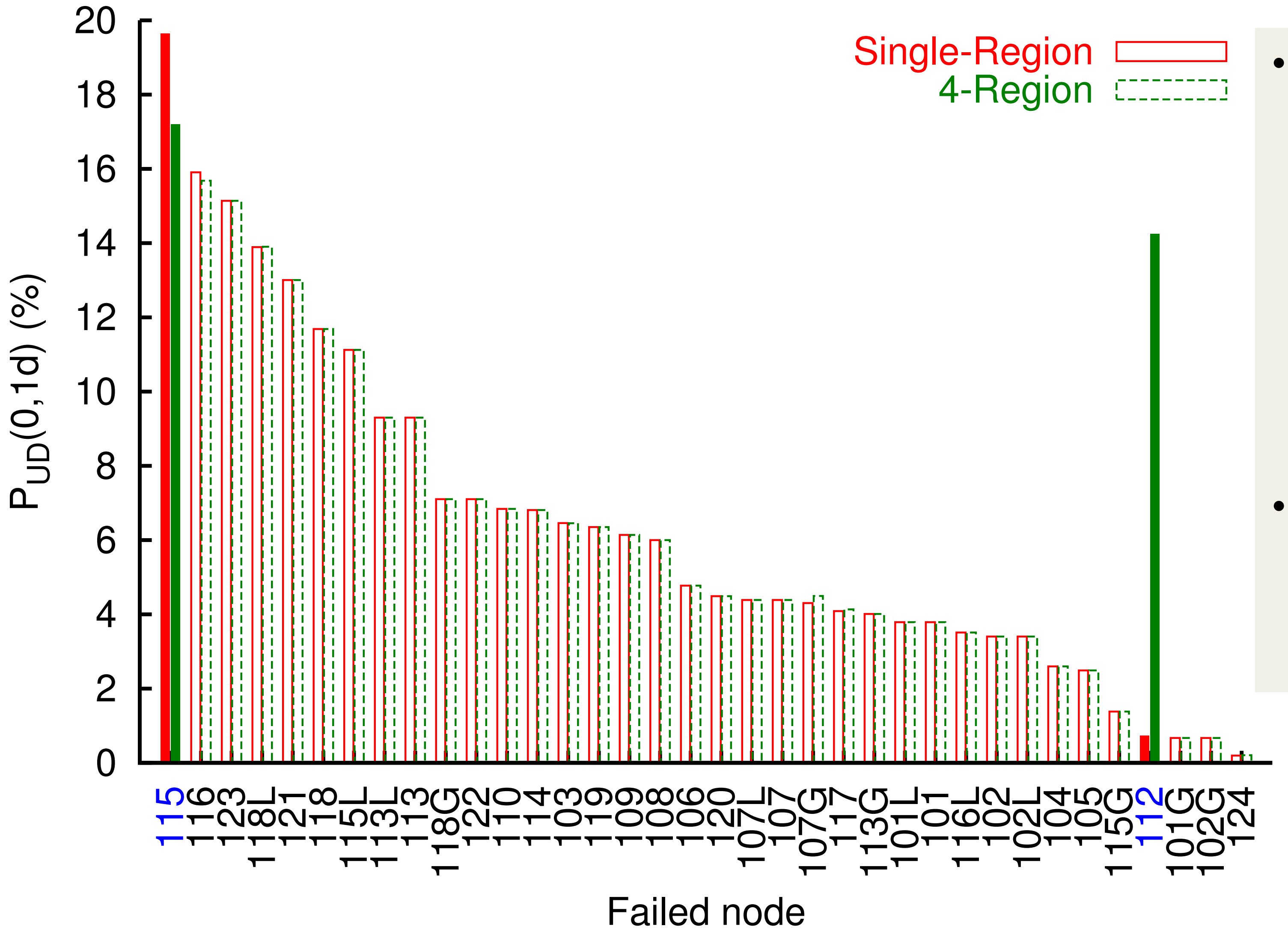
- P_i^* is the injected power immediately before the occurrence of the failure
- P_i^0 is the injected power at initial time 0
- *G* and *L* correspond to the generator and loads, including the external nodes
- W_G and W_L are the associated weight

One area of the IEEE Reliability Test System - RTS 96



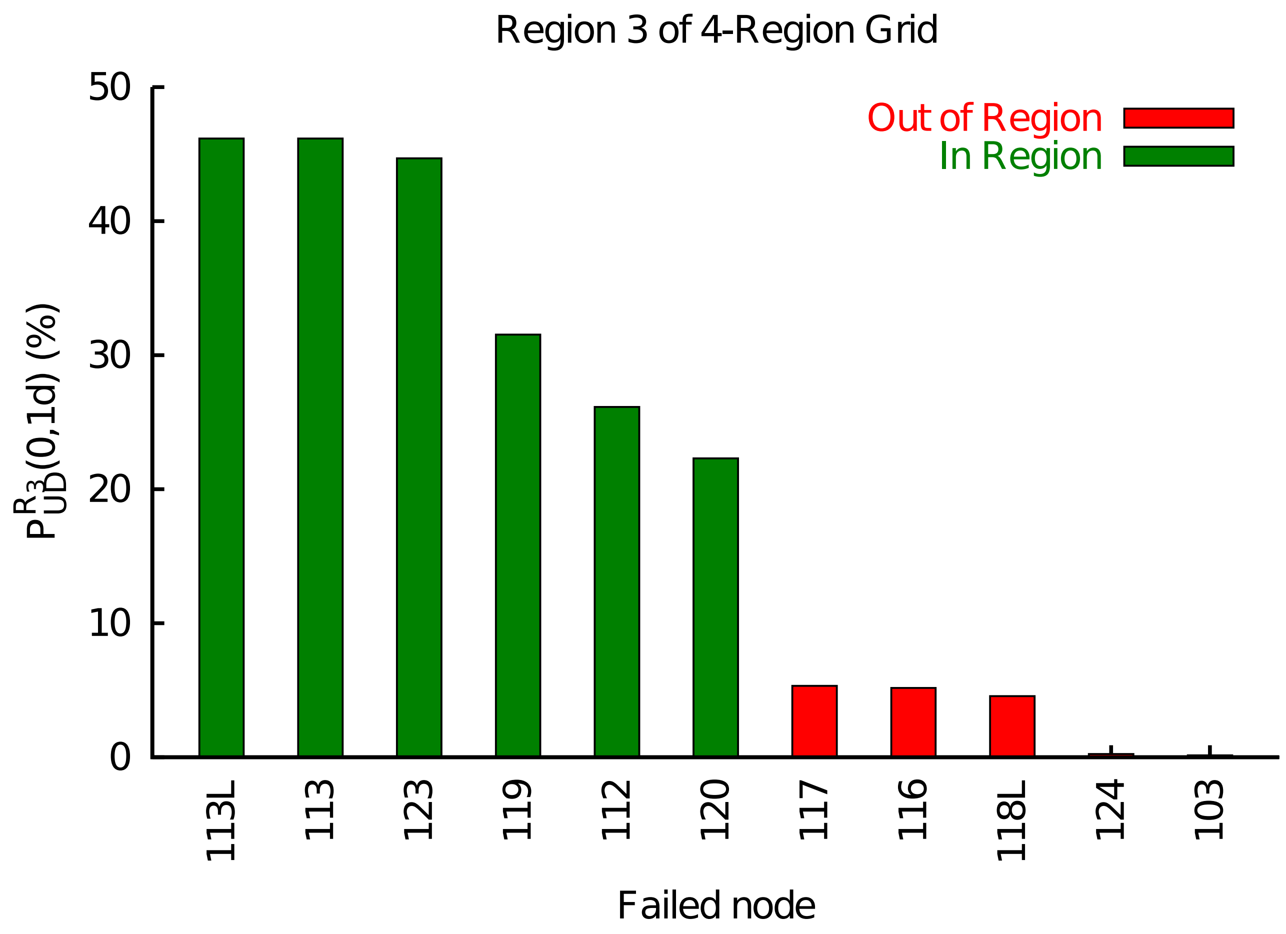
- Typically used in EPS reliability evaluation studies;
- It has been structured into 4 interconnected regions (overall, 42 nodes (10 generators and 17 loads) and 56 power lines);
- The EI state is initially in electrical equilibrium;
- Measure of interest: $\mathbf{P}_{UD}$ (0; **l**) is the percentage of the mean power demand that is not met in the interval [0; **l**];
- Two EI scenarios considered, both in association with a DoS attack to the ITCS ComNet:
  - failure of a node;
  - failure of a power line.

Failure of a node for single region and 4-region grids



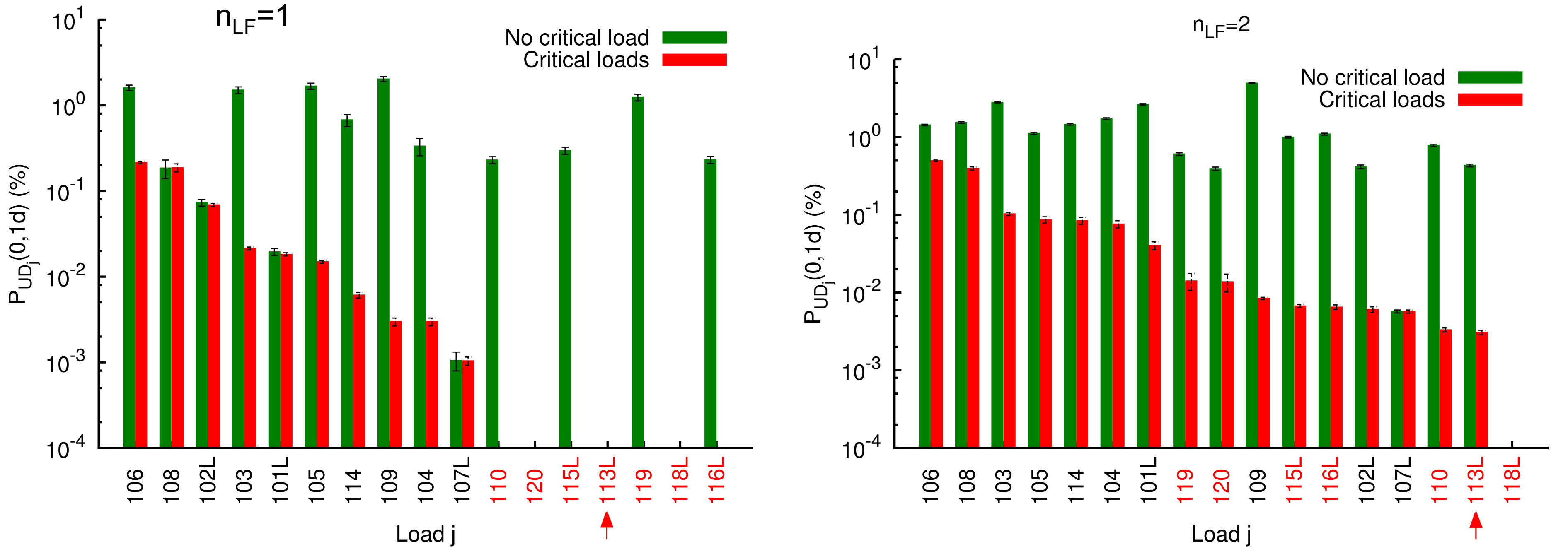
- both the single region and 4-region organizations have almost the same critical nodes and the same level of criticality with respect to $\mathbf{P}_{UD}(0; 1\mathbf{d})$
- remarkable differences for the level of criticality of nodes 112 and 115

Criticality of failed nodes wrt Region 3



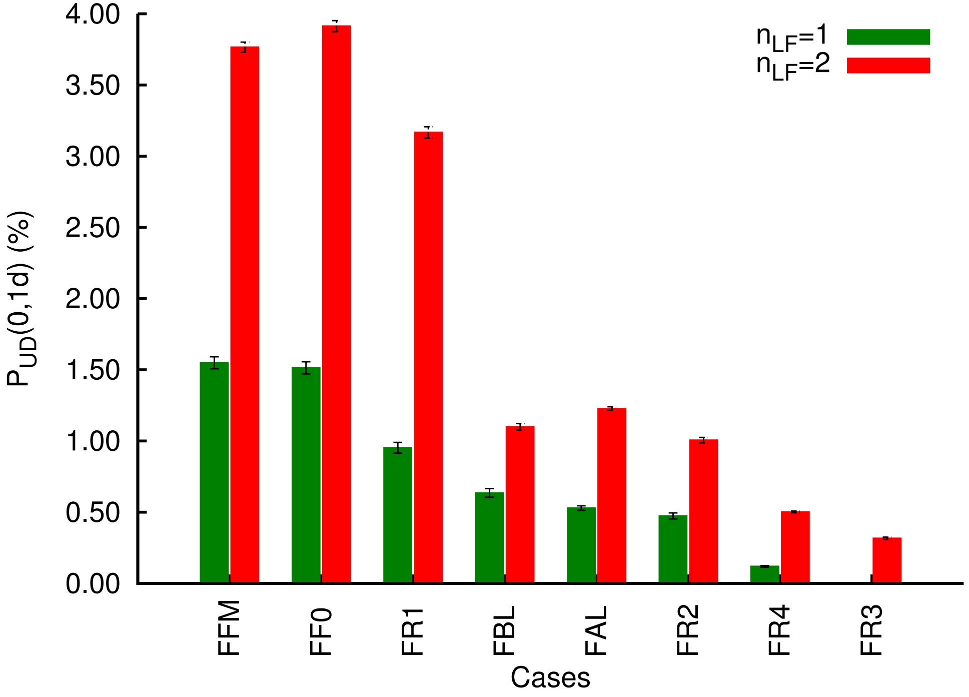
- Every internal node (except 113G) is critical for the Region 3;
- Five external nodes are critical for the Region 3.

Accounting for aspects of heterogeneity: loads of different criticality



Mean of the percentage $\mathbf{P}_{\mathrm{UDj}}$ (0; **l**) of undelivered power demand for the critical load **j** in one day, at varying the critical load **j**

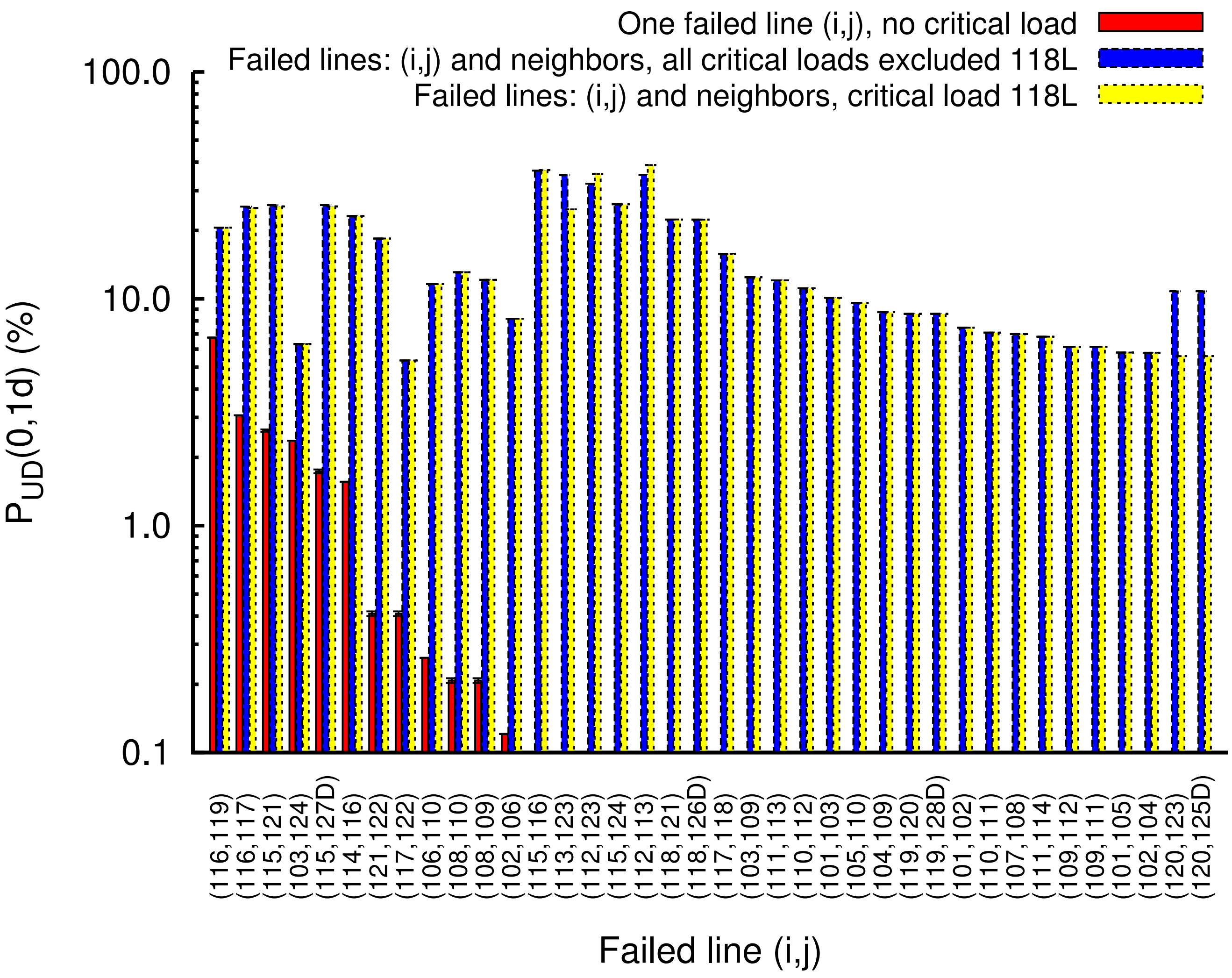
Accounting for aspects of heterogeneity: different failure rates of power lines



Percentage of power demand not delivered in one day $\mathbf{P_{UD}(0; 1d)}$, for each of the eight cases defined to partition the power lines among those exposed to failures and those that are not.

- **FAL**: all power lines can fail
- **FR1**: only power lines in Region1
- **FR2**: only power lines in Region2
- **FR3**: only power lines in Region3
- **FR4**: only power lines in Region4
- **FBL**: only boundary power lines
- **FF0**: only the first 12 power lines can fail, sorted by the initial power flow through the line Fij
- **FFM**: only the first 12 power lines can fail, sorted by the ratio Fij **=**Fmax ij

Accounting for non random events: failure of a cluster of power lines



- $P_{UD}(0; 1d)$ at varying of power line (i ; j) together with its neighboring.
- Three case: no critical loads; 118L critical loads; all the loads are critical except the 118L.

Pat II
Distribution power grid
(work in progress)

Distribution grid (MV and LV)

A **distribution system's network** carries electricity from the transmission system and delivers it to consumers

Structured in two segments:

- ❑ **Medium voltage** electrical distribution infrastructure (~10 kV - 60 kV)
  - ▪ Physically connected to the
    - high voltage electrical infrastructure
    - low voltage electrical infrastructure
- ❑ **Low voltage** electrical distribution infrastructure (~220V – 380V)
  - ▪ Physically connected to the
    - medium voltage electrical infrastructure

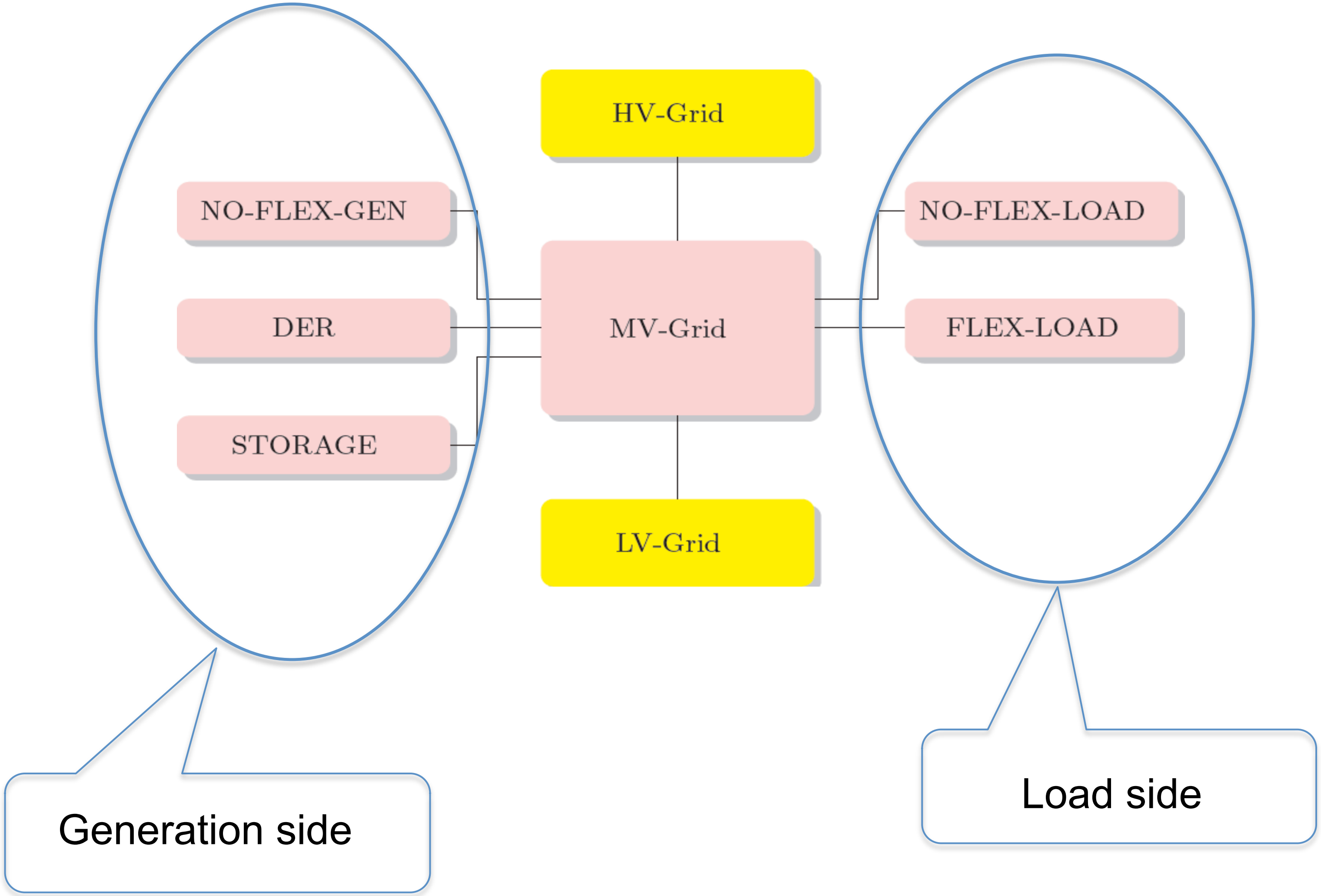
Major variations wrt the transmission grid

Aspects characterizing modern distributions grids are:

- The presence of Distributed Energy Resources, inducing variability in the generated power:
  - Photovoltaic,
  - wind turbines,
  - …
- The presence of flexible loads, to adapt to varying power generation
- Sophisticated (smart) control, which needs to account for:
  - the variability in the generation/load requests
  - Real-time data flow from sensing equipment (smart meters, grid sensors) to control computers and from control computers to power flow actuation devices (controllable loads, inverters, etc..)
  - Market laws, especially in terms of tariffs

➢ **ISSUE: how to manage the flexibility in generation and consumption from the modeling point of view**

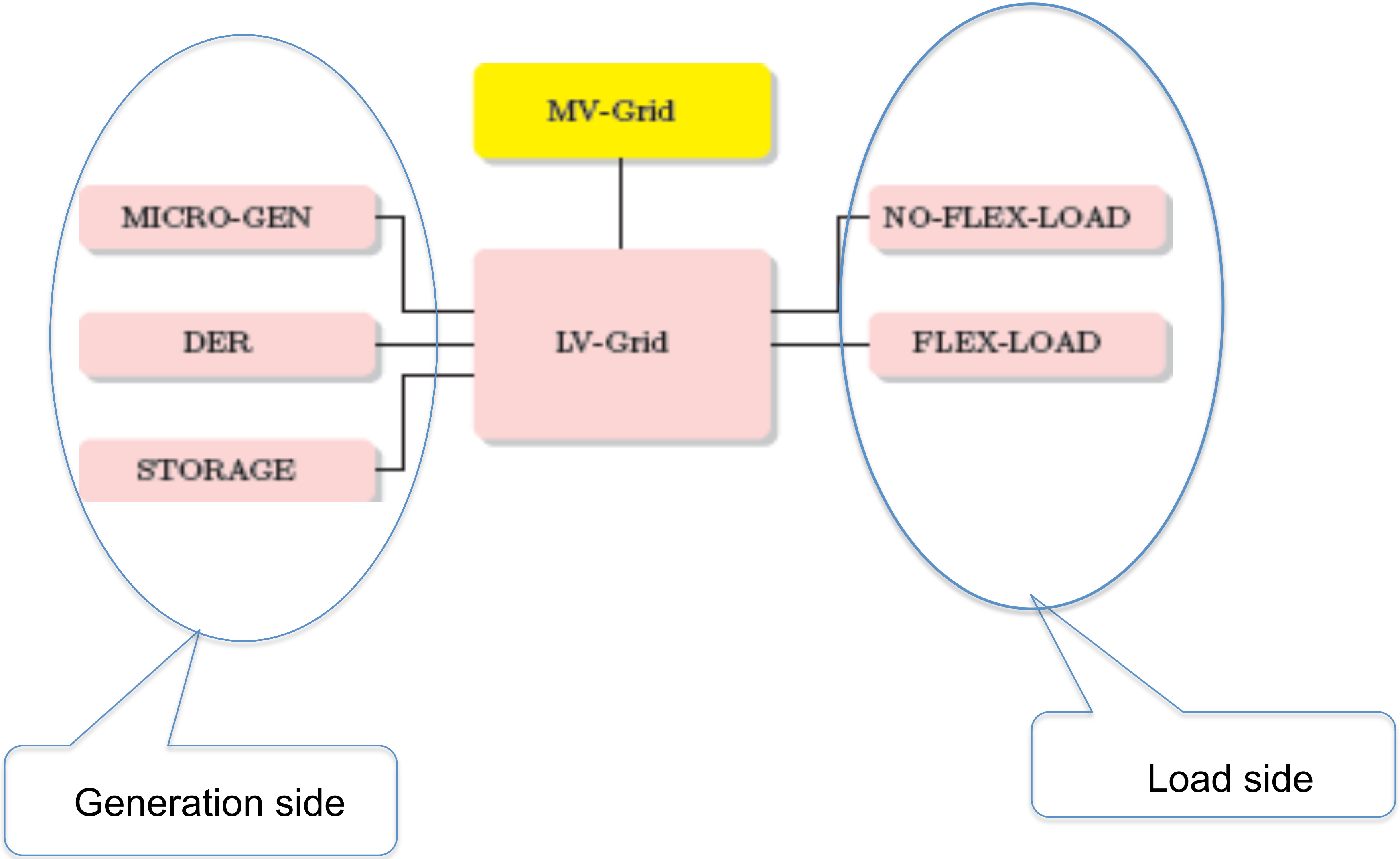
Logical view of the Medium Voltage Grid



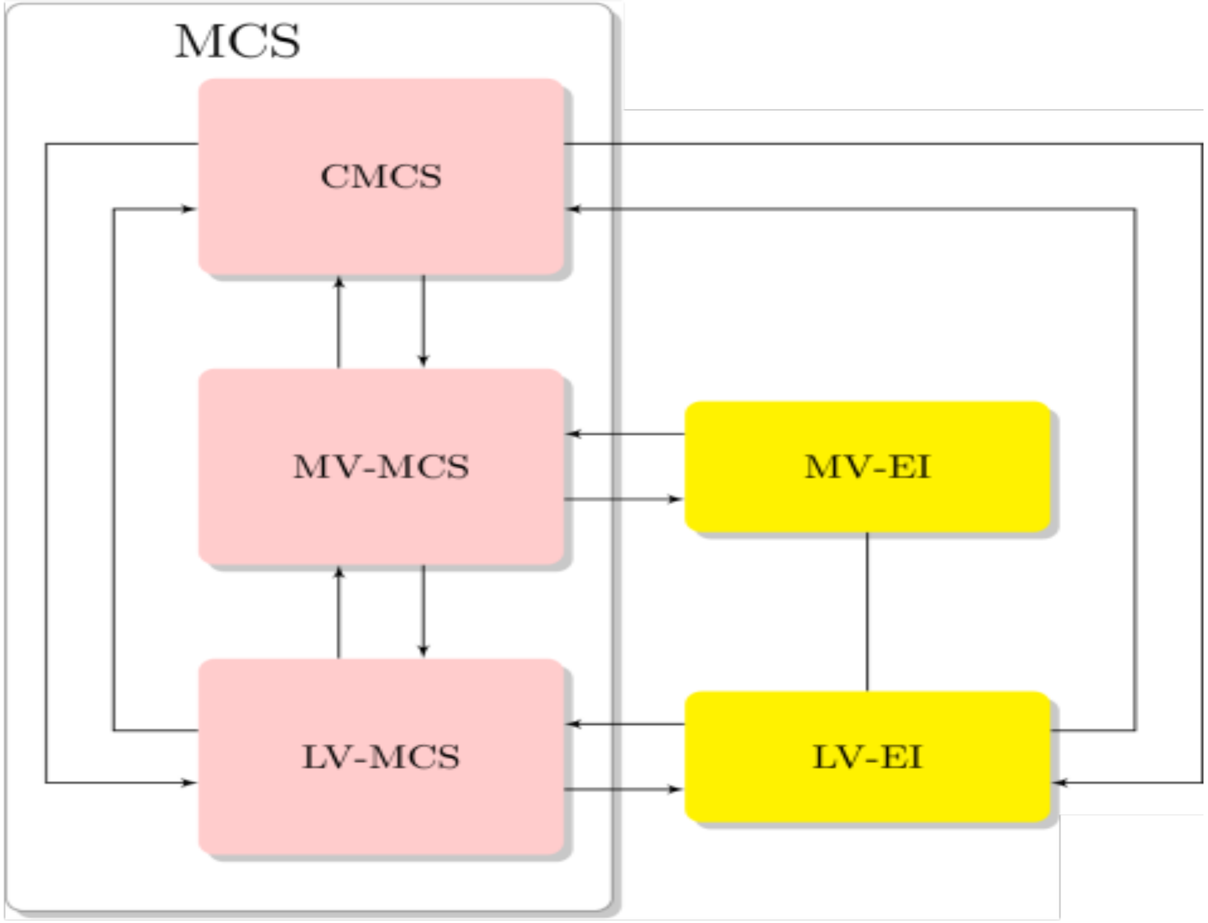
Generation side

Load side

Logical view of the Low Voltage Grid



Logical architecture of the Monitoring and Control System (MCS)

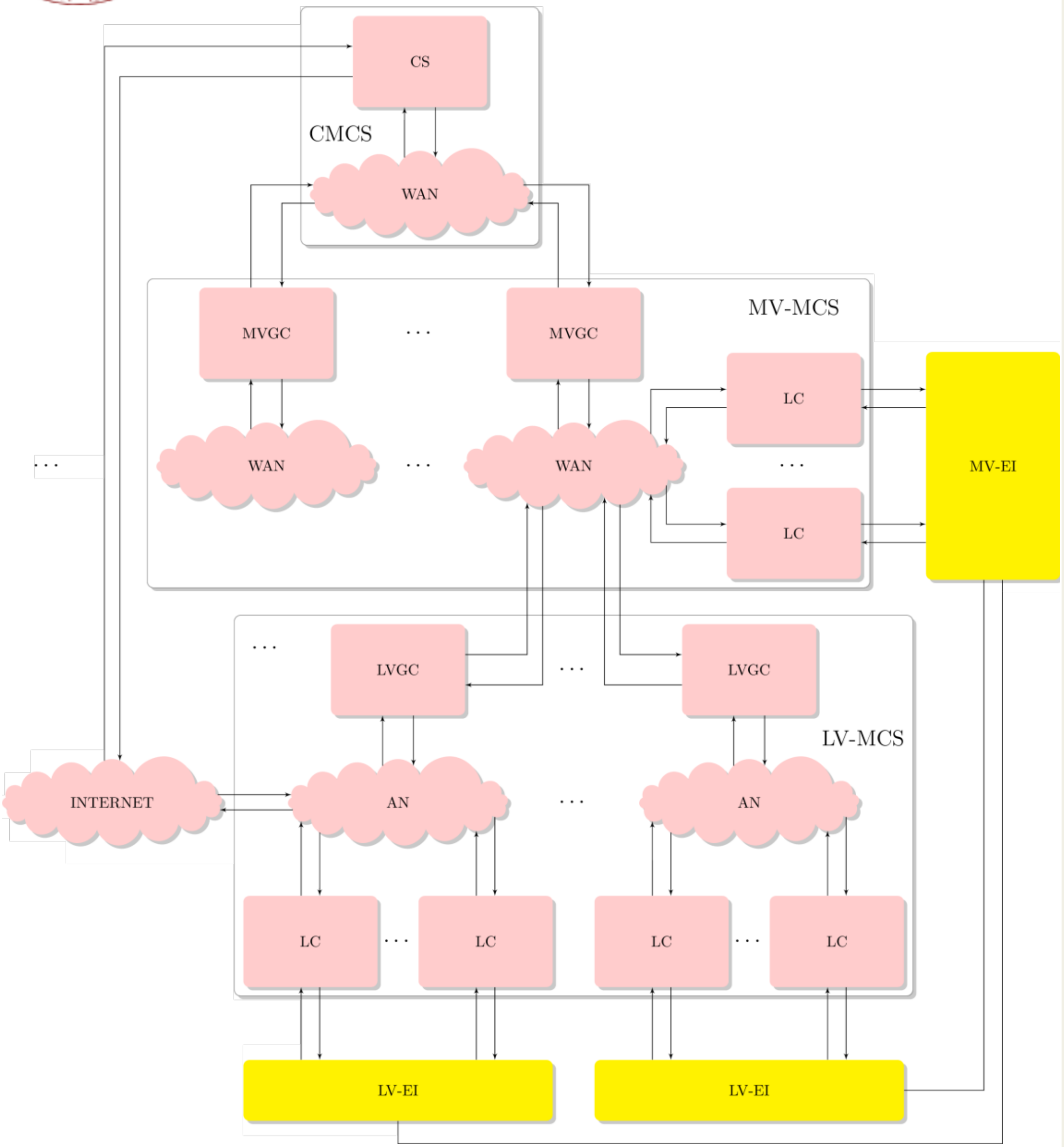


CMCS: Central Management and Control Systems, including DSO Operation Center and enterprise, the Demand Management Control, the Tariff Management and the TSO, and the external systems (e.g, the Weather Forecast, the Aggregator Controller,....)

MV-MCS: Medium Voltage Monitoring and Control System

LV-MCS: Low Voltage Monitoring and Control System

Detailed logical scheme of MCS



- Components **MVGC, LVGC** and **LC** differ for the **locality** of their decisions
- **MVGC**, associated to each different primary substation, monitors and controls all the MV electrical components connected (directly or indirectly) to the primary substation
- **LVGC**, associated to each different secondary substation, monitors and controls all the LV electrical components connected (directly or indirectly) to the secondary substation
- At medium and low voltage, a Logical Controller (**LC**), i.e., an ICT-based component having the ability to monitor/control an electrical component, is associated to each electrical component that can be directly controlled by an LC.

State Definition

- **EI:**
  - **Hybrid-state** composed by 7-tuple **(T, V, F, I, A, P, Q)**, where:
    - **T**: oriented graph, representing the topology of the grid
    - **V, F, I, A, P, Q**: physical parameters of the electric infrastructure (generators, loads, substations and power lines)
  - Addition of **Reactive Power factor Q** wrt to the CRUTIAL framework
    - Assumption on adoption of the DC model as approximation of the AC model for the electrical current flow no more possible: need for **differential equations**
- **MCS:**
  - **Discrete state**: it is only composed by discrete values, e.g:
    - Working
    - Passive latent
    - Omission Failure
    - …

Characterization of the Electrical Components: Focus on the flexible ones

- **FLEX-LOAD:**
  - **Flexibility in demand** can be exploited in three dimensions:
    - **Time**, e.g., defining time intervals during which the demand can be 0
    - **Amount of power**, e.g., agreeing on a total amount in a certain interval of time, not uniformly distributed in the interval
    - **Tariff for the user or the cost for the operator**, e.g. agreement on a tariff t_r with satisfaction request as long as the tariff in place is lower than t_r
  - Each specific characterization determines the condition for a cost/black-out
    - in case of **Time-driven characterization**, no cost/blackout in the intervals where 0 demand has been agreed
    - In case **of Amount of power-driven characterization**, no cost/blackout as long as the total requested load is met at the end of the specified time window
    - In case of **Tariff-driven characterization**, no cost/blackout when the tariff in place in greater than the agreed value

Characterization of the Electrical Components: Focus on the flexible ones – contd.

- **FLEX-GEN:**
  - **Given P(t)**, the generated power at time t (dependent on weather conditions), and **P^D(t)**, the power required to the generator at time t:
    - **If P(t)>P^D(t)**,options for the exceeding power P(t)-P^D (t) could be:
      - it is lost (a cost for the operator)
      - it is stored into a STORAGE (if any)
      - supplied to a flexible load (that can accept higher demand, such as EV)
    - **If**, instead, **P(t)<P^D(t)** then:
      - the power demand P^D(t)-P(t) is not met
      - the required power P^D(t)-P(t) is supplied by a STORAGE (if any)
      - the exceeding demand from a FLEX-LOAD (if any) is shifted over time
      - the required power P^D(t)-P(t) is supplied by a non flexible generator
- **STORAGE:**
  - Given **C(t)**,the current capacity at time t, and its maximum capacity **C^{MAX}**, it can act as:
    - •**Generator**: when it can supply energy, that is C(t)>0,
    - •**Load**: when it can receive exceeding generated energy, that is C(t) <C^{MAX}

Faults and Attacks

- **Accidental Faults,** which may affect both the electric grid and the monitoring and control infrastructure, producing the failure of the affected component(s)

- **Intentional attacks** to the monitoring and control infrastructure resulting in delayed/missing messages/data or fake messages/data about measurements, forecasts, set points, …, thus conveying incorrect info in the control flow

- **Effects on the overall Distribution System:**
  - **Delayed/Omitted** application of a reconfiguration when necessary
  - **Wrong** application of a reconfiguration, either when effectively required or a spurious one
  - leading to overloads or no balance production – consumption, with consequent cascading effects on components failures and experienced black-out

Other covered aspects

- **Interdependencies** between the EI and the MCS:
  - $S_{MCS} \rightarrow S_{EI}$; $S_{EI} \rightarrow S_{MCS}$; $(S_{EI}$ and $S_{MCS}) \rightarrow (S_{EI}$ or $S_{MCS})$

- **Metrics of interest**
  - ***expected percentage of undelivered power***
  - **expected *numbers of components affected by a disruption***
  - ***hours of undelivered power demand***
  - ***reward measures***
  - ***metrics related to the electrical components,*** *e/.g. considering V:*
    - The probability that the actual voltage V_h on component *h* is outside the regulatory limits
    - The probability that the voltage of at least one component (e.g., a load) is outside the regulatory limits
    - …
  - Metrics can be evaluated at a **certain time instant** or in an **interval of time** or at the **steady state**
  - **Mean** values and **distributions** can be determined

Currently addressed challenges

Major challenges under study are:

- **Identification of modelling elements** which map the components of the logical architecture, so as to allow:
  - **Accurate representation** of the infrastructures components (both at EI and ICT-MCS level)
  - **Lightweight models** (as much as possible), to promote efficiency in model solution

- **Representation of the control functions in the hierarchy of controls, accounting for**:
  - The **additional electrical parameters** (voltage and reactive power), which need differential equations to manage the electrical flow
  - **Voltage regulation** in presence of **dynamic generation and loads**
  - Increased **number of elements** involved in
  - Trade-off between **cost of power loss** (with reference to criticality of the loads) and **cost of the control**

Context for the Distribution Power System analysis: the EU SmartC2Net project

❑ **FP7 SmartC2Net:** Smart Control of Energy Distribution Grids over Heterogeneous Communication Networks

- **Objective**: Enable robust smart grid control, utilizing heterogeneous third-party communication infrastructures
- **Duration**: 1/12/2012 – 30/11/2015
- **Partners**:
  - FTW FORSCHUNGSZENTRUM TELEKOMMUNIKATION WIEN GMBH FTW Austria
  - AALBORG UNIVERSITET AAU Denmark
  - TECHNISCHE UNIVERSITAET DORTMUND TUDO Germany
  - RESILTECH SRL RT Italy **(CNR-ISTI as third party)**
  - RICERCA SUL SISTEMA ENERGETICO - RSE SPA RSE Italy
  - VODAFONE OMNITEL N.V. VO Netherlands
  - EFACEC ENGENHARIA E SISTEMAS SA
- http://www.smartc2net.eu/

Some more on SmartC2Net

SmartC2Net Approach:

❑ design **Smart Grid control applications** that

- are aware of communication network behaviour
- react to changes of information and network quality

❑ **dynamically change network configurations** (including QoS settings), information access procedures, and interaction protocols with grid actuators

❑ investigate **protective measures**

- against maliciously created network property fluctuations
- against attacks on the developed adaptivity solution

❑ **assess** QoS/resilience indicators of the designed technologies, **with focus on the effect of faults/attacks and interdependencies**

❑ **integrate** the designed mechanisms into **use-cases,** showing their effectiveness

Some more on SmartC2Net – contd.

❑ Four use-cases:
- Medium Voltage Control
- Self-optimized Low Voltage Grid Domain (3 use-cases)
  - Households and distributed Generation
  - Electric vehicle charging
  - External generation site

❑ Assessment through:
- model-based and simulation approaches
- experimental approach, through testbeds at three partners sites

❑ **The use-cases provide interesting scenarios:**
- **to understand better the challenges to be addressed in the setting up the modelling framework tailored to distribution in smart grids**
- **to exercise the modelling framework under development**

Context for the Distributed Power System analysis: the TENACE project

- ❑ PRIN **TENACE**: Protecting National Critical Infrastructures from Cyber Threats

  - **Objective**: **TENACE** has the objective of defining collaborative technical and organizational methodologies to raise the protection of such CIs with the specific target of looking at the common steps in order to develop a unifying methodology and understanding the underground economics fuelling an attacker.
  - **Partners:**
    - **9 Italian Universities**: Roma, Firenze, Napoli (2), Torino, Milano, Trento, Pisa, Reggio Calabria
    - **Research center**: **CNR-ISTI**
  - **Duration**: 1/2/2013 – 31/1/2016
  - **http://www.dis.uniroma1.it/~tenace/**

Some more on TENACE

- ❑ TENACE will address three scenarios, that represent different settings with distinct interdependencies, threats, vulnerabilities and possible countermeasures:
  - financial infrastructures
  - **power grid systems**
  - transportation systems
- ❑ The study of specific CI vulnerabilities and related attacks will drive the development of
  - Algorithms
  - **Models**
  - Architectures
  - Tools

as the means to **enable the effective protection** of critical infrastructures enhancing their **degree of security and dependability** by considering a continuously **evolving adversary**

(Some) final considerations

- **So far:**
  - ❑ Critical infrastructures, seen as systems of systems with possibly intricate interactions providing vital services, are raising more and more attention at National and International level, in terms of recommendations, standards, agencies, research projects, …
  - ❑ Understanding the impact of interdependencies is a major challenge to identify protection means and countermeasures to attacks/failures
  - ❑ Model-based analysis is a suitable direction to analyse the behaviour of CI when affected by faults/attacks and assess indicators of their resilience/QoS, as discussed for the electric power sector

(Some) final considerations – contd.

➢ Looking ahead:

- ❑ Advances in industrial control systems and technology, such as SCADA systems, enhance sector operations but create additional vulnerabilities and increase interdependencies
- ❑ The largeness and diversity of critical infrastructures and the different characteristics of their parts requires a compositional integrated formalism
- ❑ The necessity of continuous assessment activities calls for a composite (i.e., holistic) evaluation framework, where the synergies and complementarities among several evaluation methods can be fruitfully exploited.
- ❑ ….

Acknowledgements

Thanks to:

- **Silvano Chiaradonna, Paolo Lollini,** and **Nicola Nostro**, who greatly contributed to develop the EPS analysis and evaluation framework, which is the core of this presentation
- **Bill Sanders**, for the material on the overview on the model-based validation methods and the SAN formalism

References

- Chris. W. Johnson, “Analysing the Causes of the Italian and Swiss Blackout, 28th September 2003”, Proceeding SCS '07 Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems - Volume 86 Pages 21-30 , 2007
- A. Berizzi, C. Bovo, M. *Delfanti*, A. Silvestri: “The 28 September 2003 *blackout* in *Italy*: external causes and emergency procedures” CNIP 2006, Rome, 2006
- Andersson, G.; Donalek, P.; Farmer, R.; Hatziargyriou, N. “Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance”, IEEE Transactions on Power Systems, Volume:20 Issue:4, 2005
- "Final Report of Aug 14, 2003 Blackout in the US and Canada: Causes and Recommendations", US-Canada Power System Outage Task Force, April 5, 2004. www.NERC.com
- A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, Vol. 1:1, pp. 11-33, January-March 2004.
- Chiaradonna S., Di Giandomenico F., Lollini P. Assessing the impact of interdependencies in electric power systems. In: International Journal System of Systems Engineering, vol. 1 (3) pp. 367 - 386. INDERSCIENCE Publisher, 2009.
- S. Chiaradonna, F. Di Giandomenico, P. Lollini, “Definition, implementation and application of a model-based framework for the analysis of interdependencies in electric power systems”, International Journal of Critical Infrastructure Protection (ijcip) 4 (1), pp. 24–40, 2011.

References

- S. Chiaradonna, F. Di Giandomenico, N. Nostro, “Modelling and analysis of the impact of failures in electric power systems organized in interconnected regions”. In IEEE/IFIP 41st Int. Conf. on Dependable Systems and Networks (DSN 2011), pages 442–453, June 2011
- M. Beccuti, S. Chiaradonna, F. Di Giandomenico, S. Donatelli, G. Dondossola, G. Franceschinis, “Quantification of dependencies between electrical and information infrastructures”, International Journal of Critical Infrastructure Protectionm (ijcip) 5 (1), pp. 14-27, 2012.
- Chiaradonna S., Lollini P., Di Giandomenico F. On a modeling framework for the analysis of interdependencies in electric power systems. In: IEEE/IFIP 37th Int. Conference on Dependable Systems and Networks. DSN 2007 (Edinburgh, UK, 25-28 June 2007). Proceedings, pp. 185 - 195. IEEE Computer Society, 2007.
- Chiaradonna S., Di Giandomenico F., Lollini P. Evaluation of critical infrastructures: challenges and viable approaches. In: Architecting Dependable Systems V. pp. 52 - 77. Rogerio de Lemos, Felicita Di Giandomenico, Cristina Gacek, Henry Muccini, Marlon Vieira (eds.). (Lecture Notes in Computer Science, vol. 5135). Germany: Springer, 2008.
- National Infrastructure Advisory Council, “CRITICAL INFRASTRUCTURE RESILIENCE FINAL REPORT AND RECOMMENDATIONS”, September 2009, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf
- S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analysing critical infrastructure interdependencies. IEEE Control Systems Magazine, pages 11-25, December 2001

References

- W. H. Sanders and J. F. Meyer. Stochastic Activity Networks: Formal Definitions and Concepts. In European Educational Forum: School on Formal Methods and Performance Analysis, pages 315{343, 2000.
- D. Daly, D. D. Deavours, J. M. Doyle, P. G. Webster, and W. H. Sanders. Möbius: An extensible tool for performance and dependability modeling. In B. R. Haverkort, H. C. Bohnenkamp, and C. U. Smith, editors, 11th Int. Conf., TOOLS 2000, volume 1786 of LNCS, pages 332–336. Springer Verlag, 2000.
- G. Balbo, "Introduction to stochastic petri nets", Lectures on Formal Methods and Performance Analysis, volume 2090 of Lecture Notes in Computer Science, pages 84-155. Springer Verlag, 2001
- J.C. Laprie, "From Dependability to Resilience", Proceedings of the 38th Annual IEEE/ IFIP International Conference on Dependable Systems and Networks(DSN), Fast Abstracts Track, Anchorage, AK, June 2008.