RACI Workshop Panel

Resilience assessment of critical infrastructures: From accidental to malicious threats

Mohamed Kaâniche
mohamed.kaaniche@laas.fr

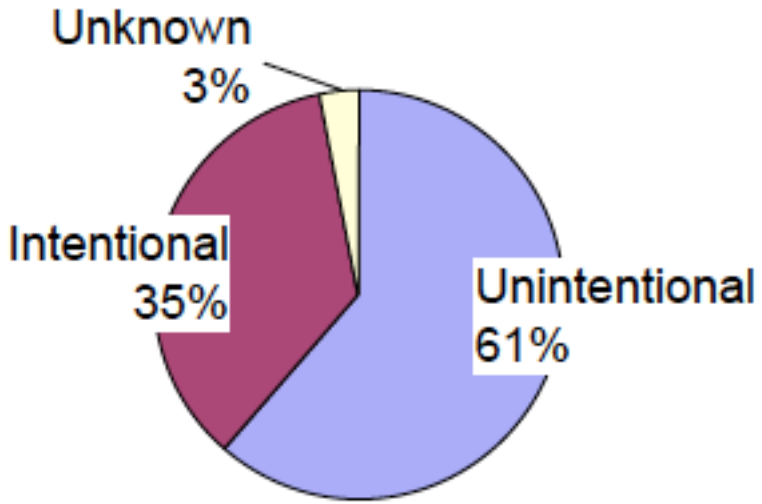
LAAS-CNRS

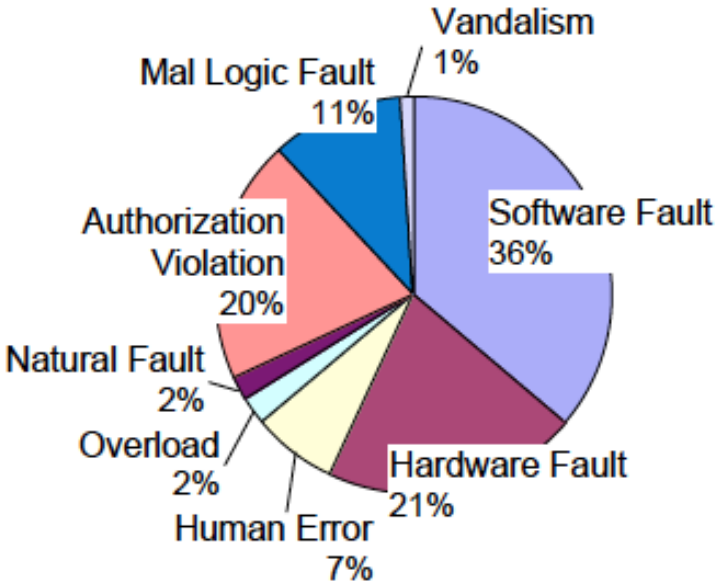
April 25, 2011

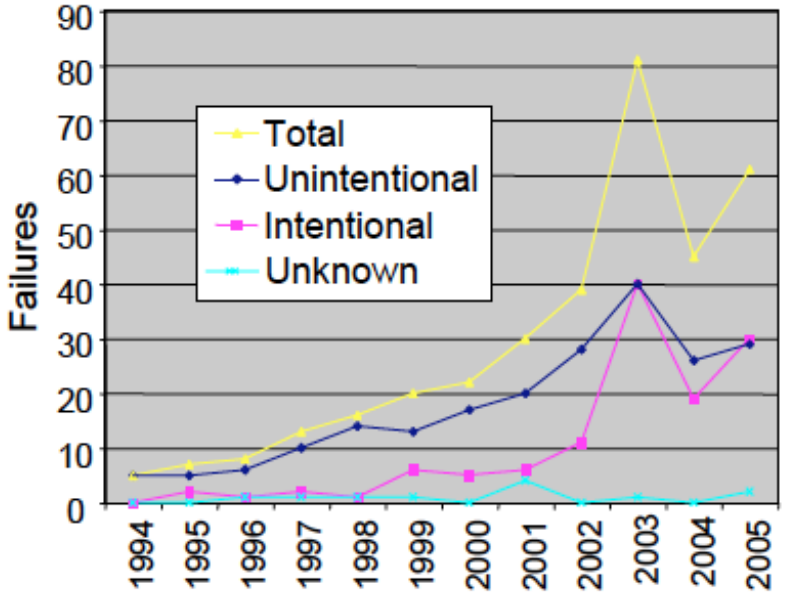
Fifth Latin American Symposium on
Dependable Computing (LADC- 2011)
São José Dos Campos, Brazil, April, 25-29, 2011

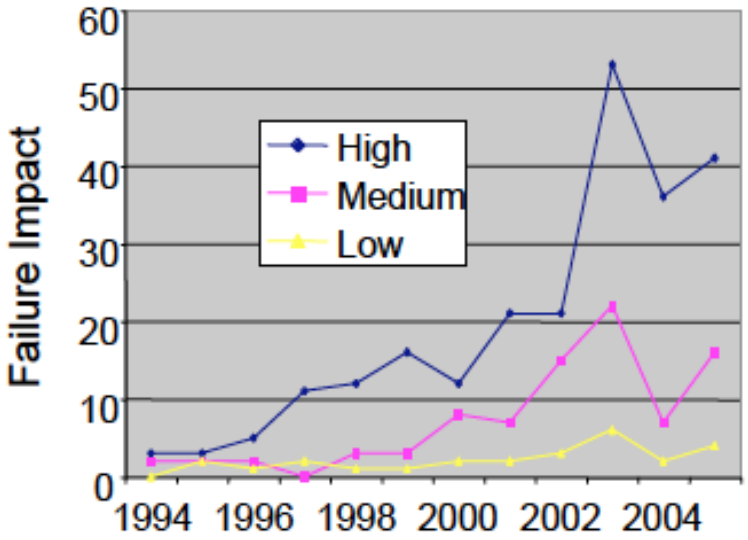
Analysis of 347 computer-related infrastructure failure cases

[Rahman, Beznosov, Marti, “Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports“, Int. Journal on Critical Infrastructures, vol.5, n°3, 2009]









Resilience assessment

Dependability Assessment

Quantitative, model-based and measurement, decision-making

Security assessment

Qualitative, process-oriented

Need for a unified framework and tools enabling the combined analysis of accidental and malicious threats

- Model based + experimental techniques
- Qualitative + quantitative approaches

Challenges

- Interdependencies
  - interdependencies related failure scenarios
    - ✓ Cascading, escalating, and common cause failures
- Scalability
  - Master complexity through the use of abstractions and composition of different types of models & formalisms
- Dynamic evolution of system and threats
  - Adaptive assessment frameworks

CESIRICERCA
Network and Infrastructures Department

Faculty of Sciences
University of Lisboa
FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

Consiglio Nazionale delle Ricerche
ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"

LAAS-CNRS
Centre National de la Recherche Scientifique

Katholieke Universiteit Leuven

consorzio nazionale interuniversitario per le telecomunicazioni
Torino Research Unit
Alessandria Research Unit

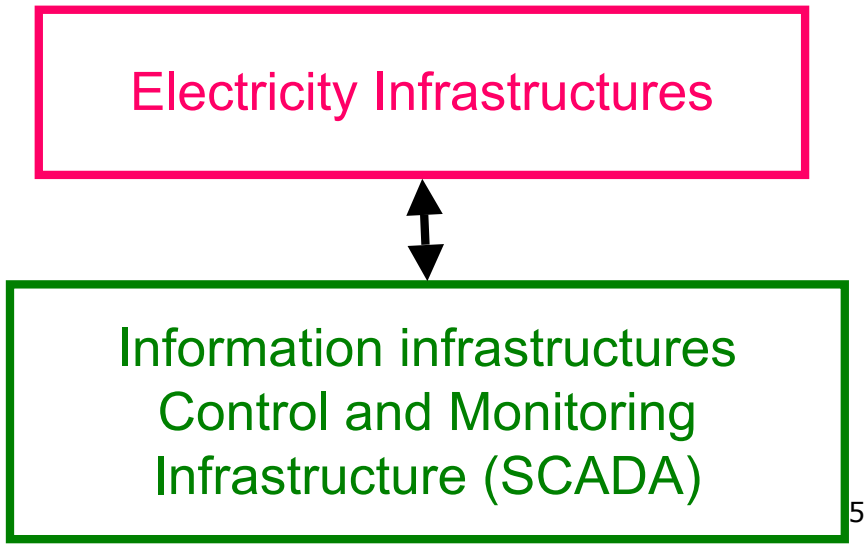
CRUTIAL

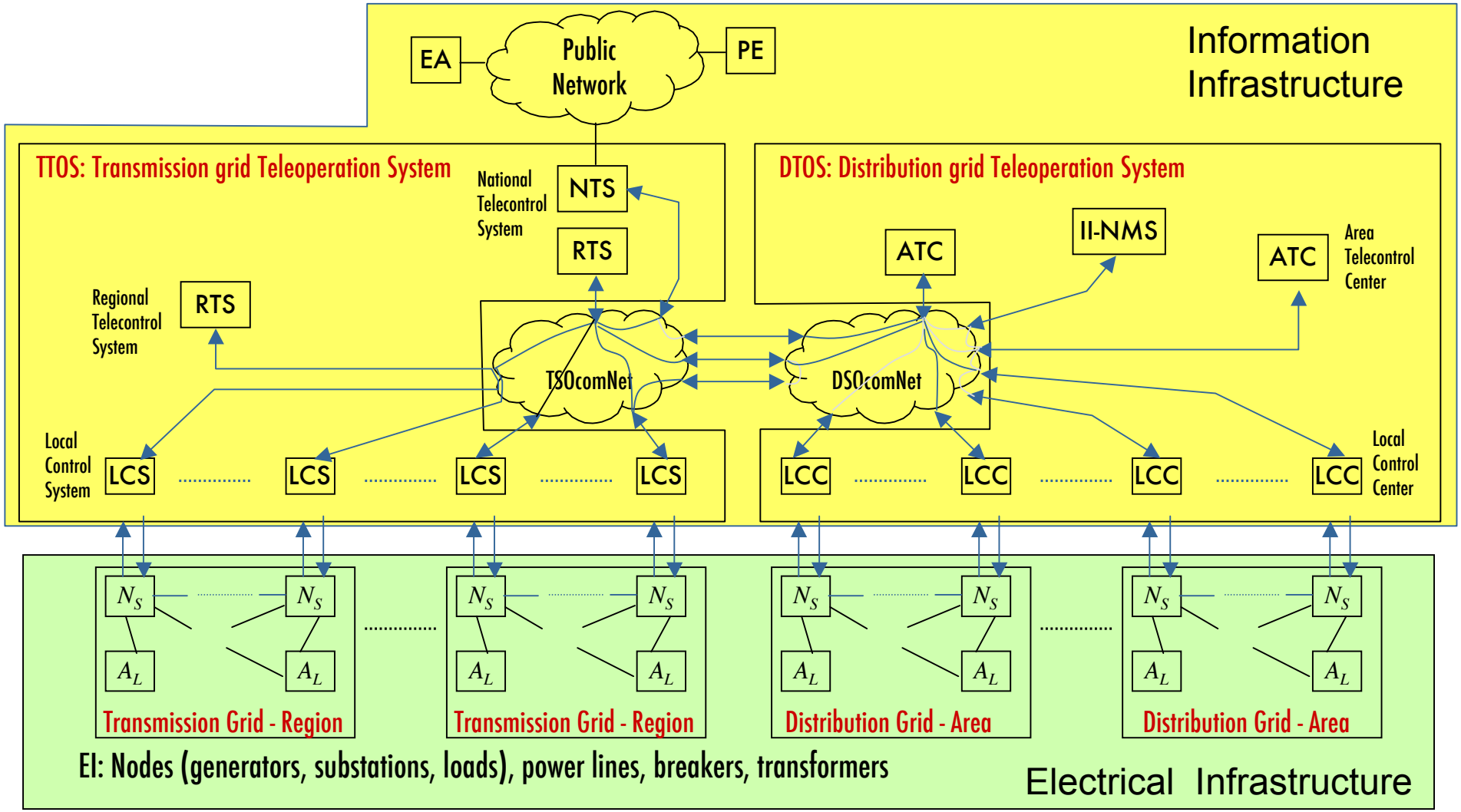
CRitical UTility InfrastructurAL resilience

Specific Targeted Research Project

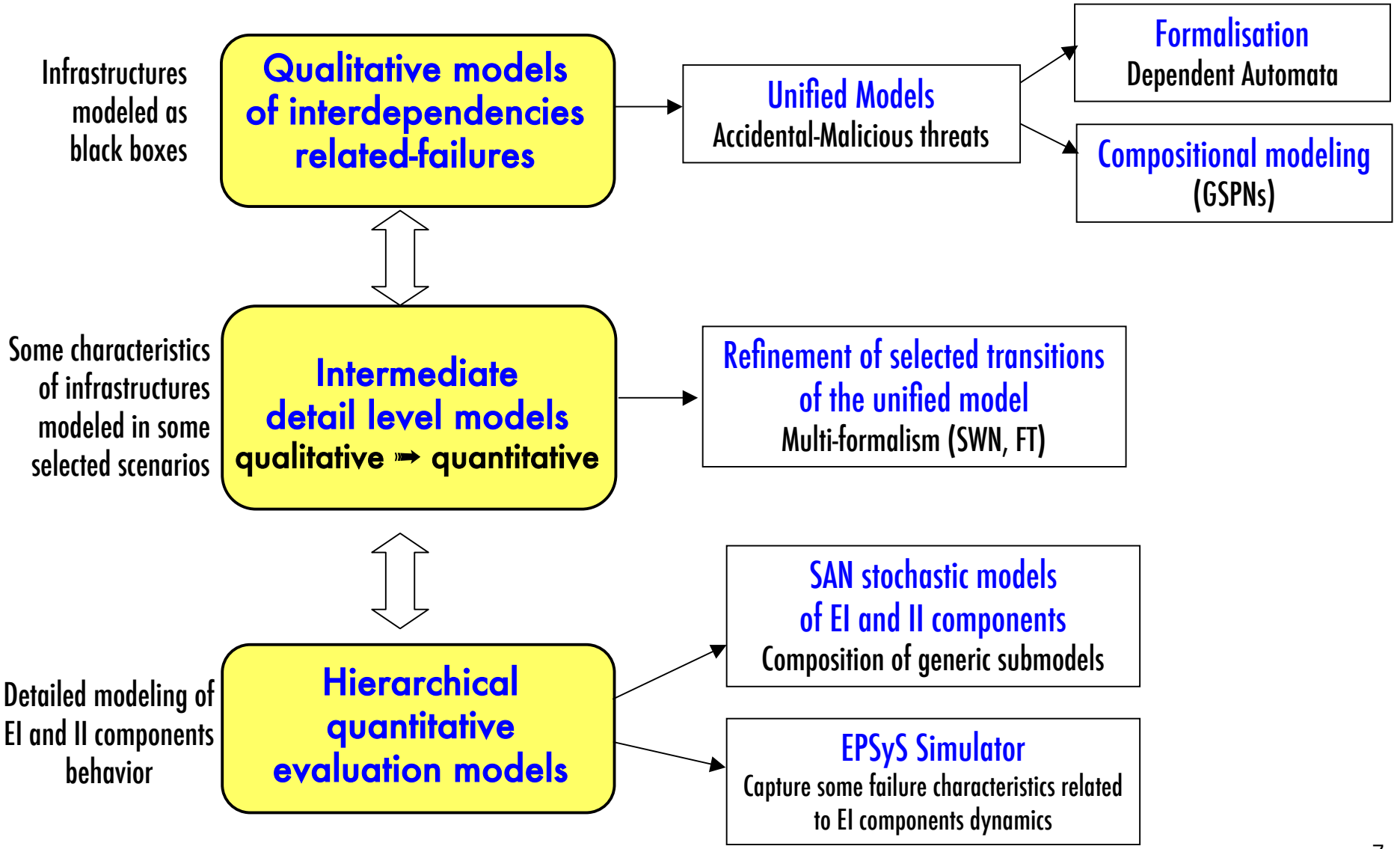
FP6-2004-IST-4-027513

Jan 2006- March 2009

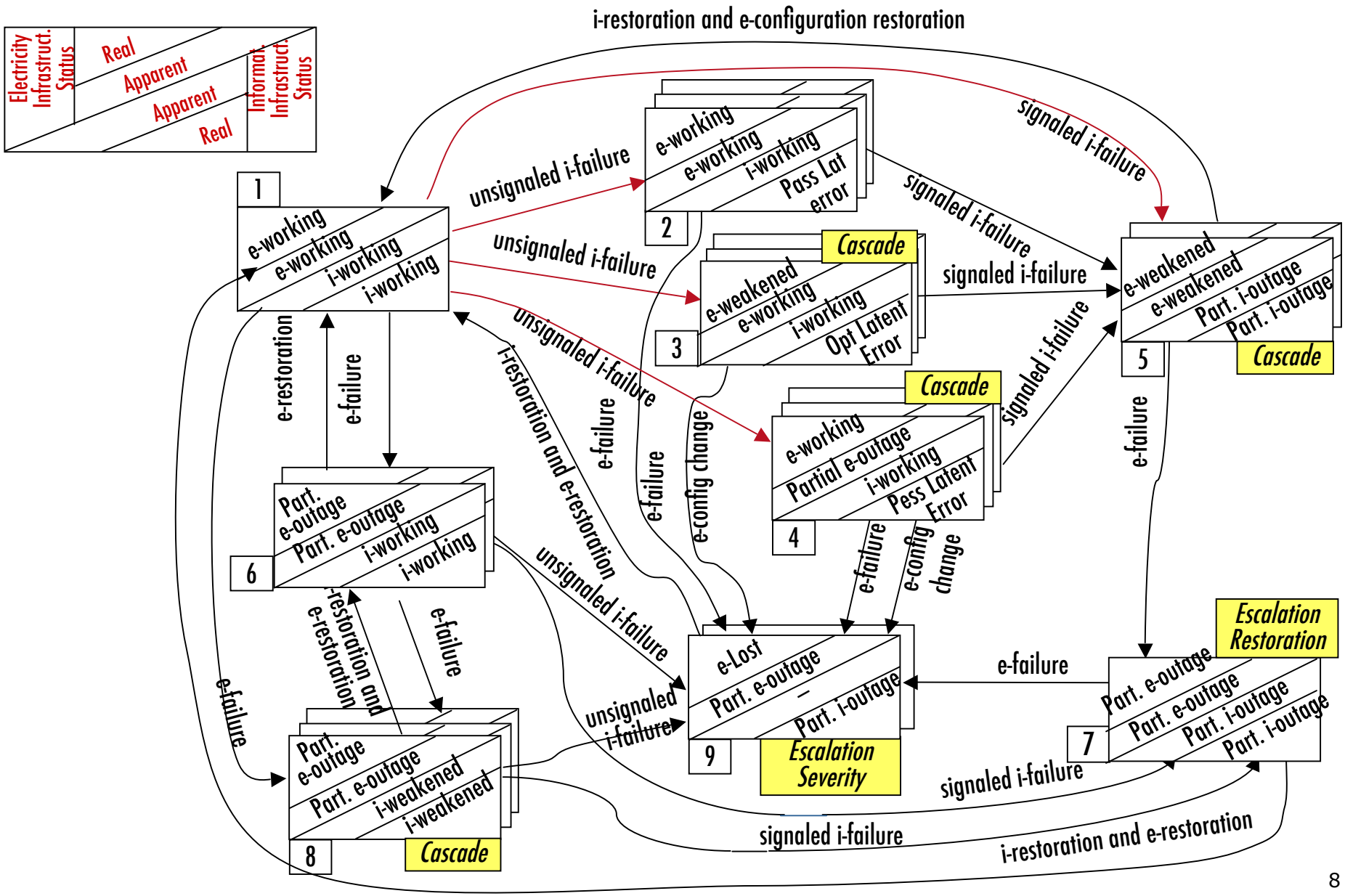



Information Infrastructure
EA
Public Network
PE
TTOS: Transmission grid Teleoperation System
National Telecontrol System
NTS
RTS
Regional Telecontrol System
RTS
TSOcomNet
DTOS: Distribution grid Teleoperation System
ATC
II-NMS
ATC
Area Telecontrol Center
DSOcomNet
Local Control System
LCS
LCS
LCS
LCS
LCC
LCC
LCC
LCC
Local Control Center
N_S
A_L
Transmission Grid - Region
Transmission Grid - Region
Distribution Grid - Area
Distribution Grid - Area
EI: Nodes (generators, substations, loads), power lines, breakers, transformers
Electrical Infrastructure

CRUTIAL: Multi-level modeling

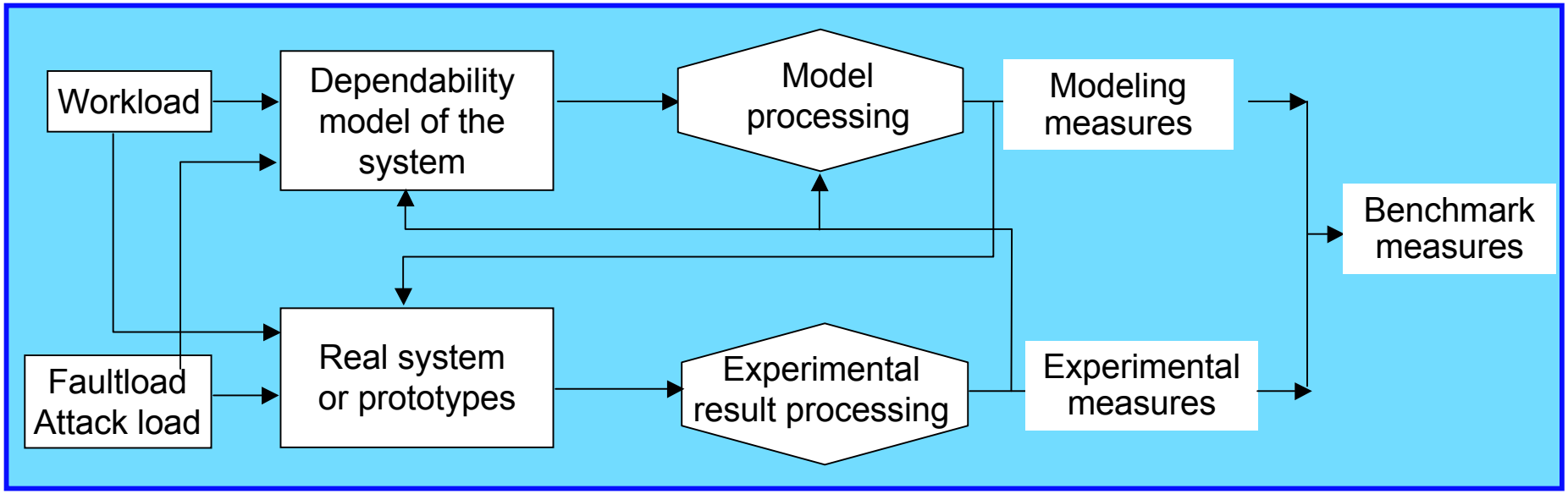


Unified Qualitative Model



Dependability and security experimental assessment

- Failure data and attack data collection
- Controlled experiments



Representativeness, Reproducibility, Repeatability, Portability, Non-intrusiveness, Scalability, Cost effectiveness

Workload and Faultload representativeness

- Workload
  - Building a realistic workload is challenging when considering critical infrastructures and dynamic and changing environments
  - Simulated data may not faithfully capture complex phenomena that characterize real traces
- Faultload and Attack load
  - Fault/errors/attacks categories + statistical likelihood
  - Automatic generation of realistic failure and attack scenarios is difficult
  - Likelihood statistics generally not available
- Need for ‘good quality’, up-to-date, «shared» data

Resilience Argumentation and justification

- From Safety cases and Security evaluation criteria to resilience cases
  - How to structure arguments, assumptions and evidence to provide justified confidence that the critical infrastrutures are able satisfy the requirements?
  - Address safety and security in a combined and coherent way
  - Standardization activities need to move in this direction

- Some initiatives
  - SQUALE project: Security, Safety and Quality evaluation for Dependable Systems (European ACTS project)
  - SEISES project: Convergence of safety and security practices in avionics industry