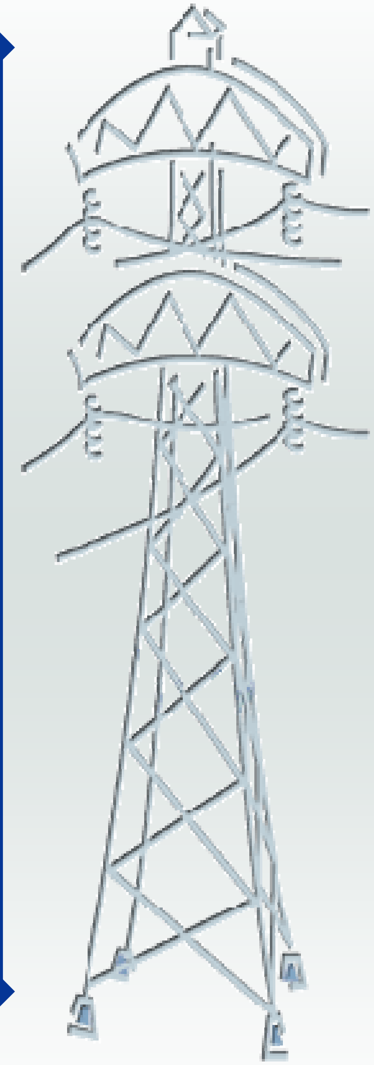
GRID

A Coordination Action on ICT Vulnerabilities of Power Systems and the Relevant Defense Methodologies



Securing Critical Infrastructures: The power and ICT perspective

The GRID Initiative

N. HADJSAID,

Grenoble Institute of Technology

INP Grenoble

EUROPEAN COMMISSION
DIRECTORATE GENERAL
Joint Research Centre

SINTEF

KATHOLIEKE UNIVERSITEIT LEUVEN

CESI RICERCA

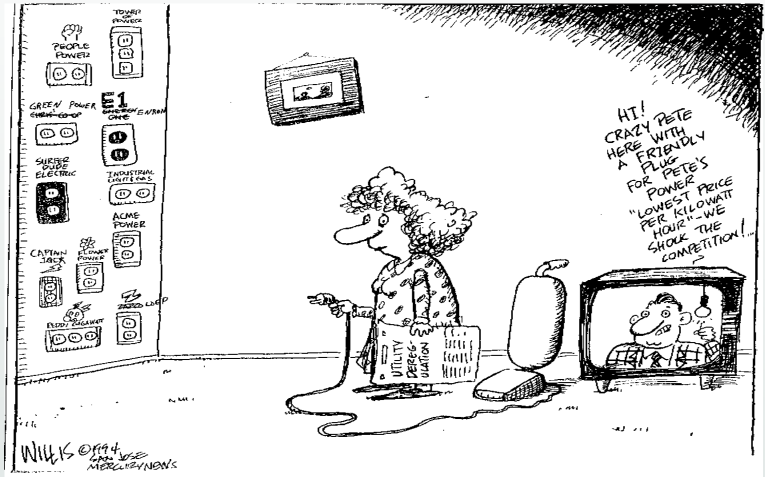
SIT
Institut Sichere Informations-Technologie

Background

- Recent power blackouts in different parts of the world
- Communication blackouts
- Increased awareness of malicious attacks, interdependencies and system vulnerabilities

Power System perspective: The Scene

- **Power system**:
  - A vital infrastructure for our modern society
  - Subject to various disturbances
  - Electricity can not be stored (LS)
    - System adequacy
  - Open access and deregulation
    - Multi actors - Transactions amount
    - Extended use of open IC infrastructures
  - Complex system
    - Large scale - Multi layer system – interdependent
    - Control system complexity grows – responsibilities partitioning
    - Difficult to master, Chaotic behavior

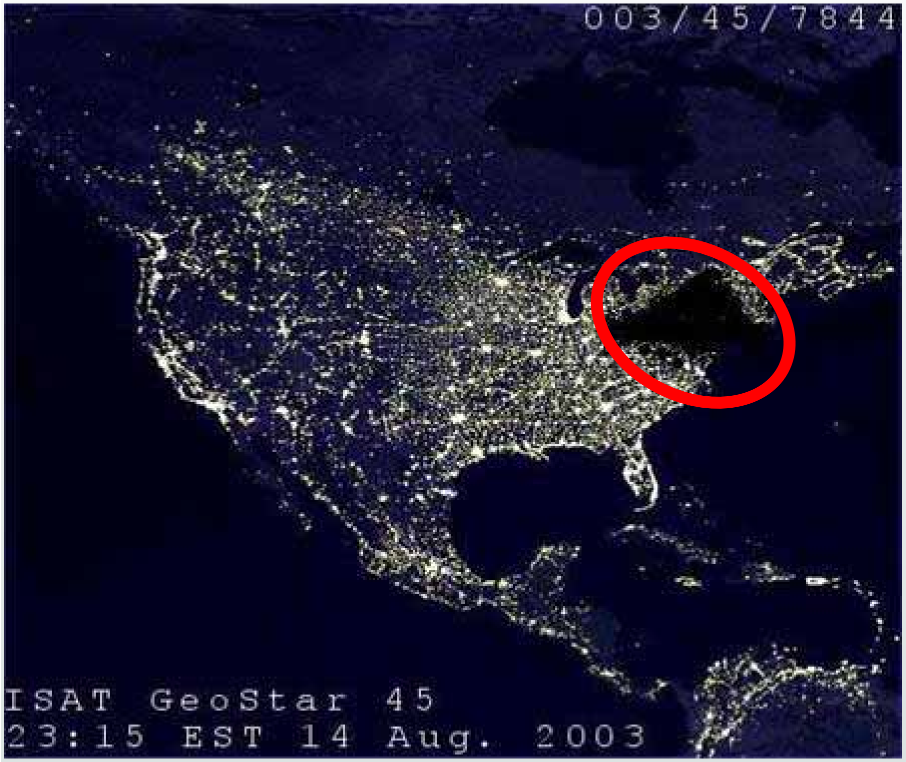


- **System vulnerability & failure**:
  - Huge economical & societal impact
  - Less and less accepted

Last blackouts

- USA (14-08-2003)
- London (28-08-2003)
- Italy (28-09-2003)
- Sweden & Denmark (23-09-2003)
- Iran (31-03-2003)
- Finland (23-08-2003)
- Algeria (03-02-2003)
- Australia (2004)
- Greece (2004)
- Jordan (2004),
- Bahrain (2004)
- EU power shortage (2006)
- ….

US/Italy blakouts



Crucial aspects of some Blackouts

- Initiating event compounded by malfunction of monitoring, control & protection systems
  - In some situations, Distributed Generation has played adverse role
- When events happened at the boundary between control areas, they were allowed to spread due to insufficient coordinated response
- Vulnerabilities in the infrastructure – interdependencies
- Millions of people effected (50 M In US and Italy)
- High economical and societal cost

Cyber incidents on Power Grid

- 6 months following the 9/11 energy industry suffered intrusions at twice the rate of other industries, attacks requiring immediate intervention averaging 12.5 per company.
- January 2003, worm "Slammer" of the Internet infected the monitoring network of the nuclear plant Davis-Besse in Ohio, the reactor happened to be offline. The electric utility lost control of their EMS/SCADA for system nearly 5 hours.
- September 2001, NERC know of an electric utility whose EMS/SCADA network was compromised by the Nimda worm.

Recent events*

- **Hackers Have Attacked Foreign Utilities, CIA Analyst Says**
  - In a rare public warning to the power and utility industry, a CIA analyst said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case **causing a power outage that affected multiple cities.**
  - cyber attackers have made increasingly sophisticated intrusions into corporate computer systems, costing companies worldwide more than **$20 billion each year**, according to some estimates.
  - Over the past year to 18 months, there has been "**a huge increase in focused attacks** on our national infrastructure networks, . .
  - "This threat is a conscious threat posed by a single hacker, or even an organized group that may be **deliberately trying to disrupt the grid**."

*Washington Post, January 19, 2008

Aurora Experiment

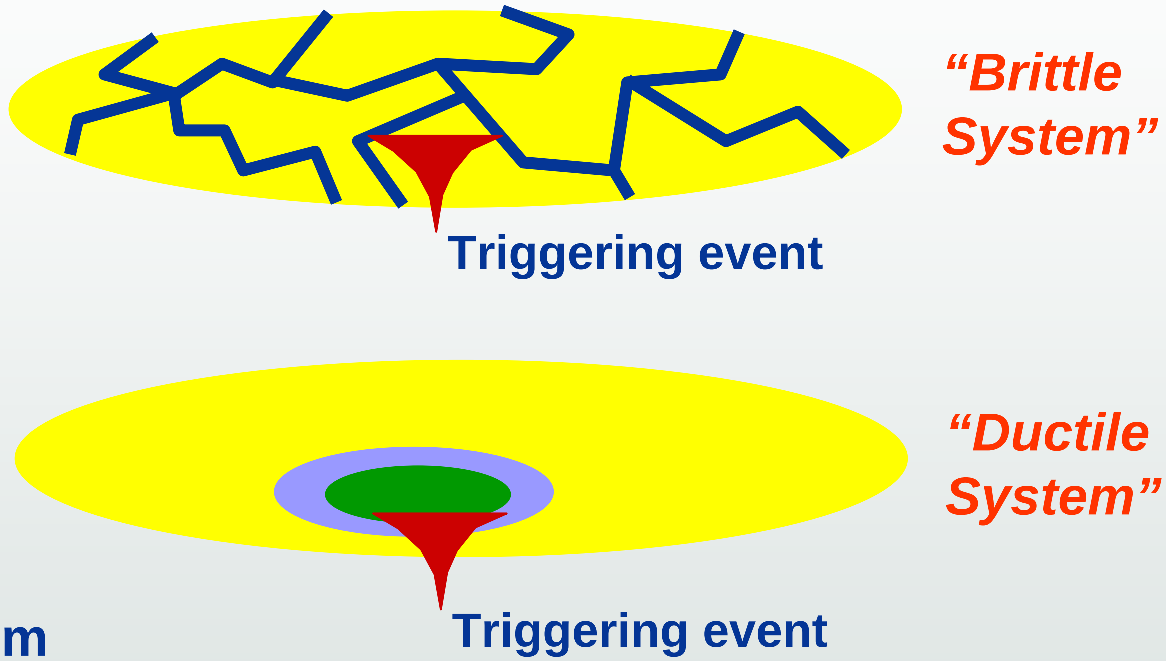
- The experiment, called "Aurora" that alarmed the committee members was conducted in March 2007 by the Idaho National Laboratory for DHS
- The attack involved a controlled hack of a replicated control system commonly found throughout the bulk-power system.
- The generator was destroyed
- CNN :" **Staged cyber attack reveals vulnerability in power grid »**
- House Committee on Homeland Security urges FERC chairman to investigate grid security

Aurora Experiment: the Video

Challenges

- How to cope with vulnerabilities of present day power systems
- How to cope with increased interdependencies between Power & ICT
- Design and maintenance of dependable *open* systems!
- Change from brittle system to ductile system

Design a ductile system Instead of Brittle system



Ductile system

- **New system component**
- **New reconfigurations**
- **Renewable architectures**

- Source: CRIS Institute

A system that confines disturbances

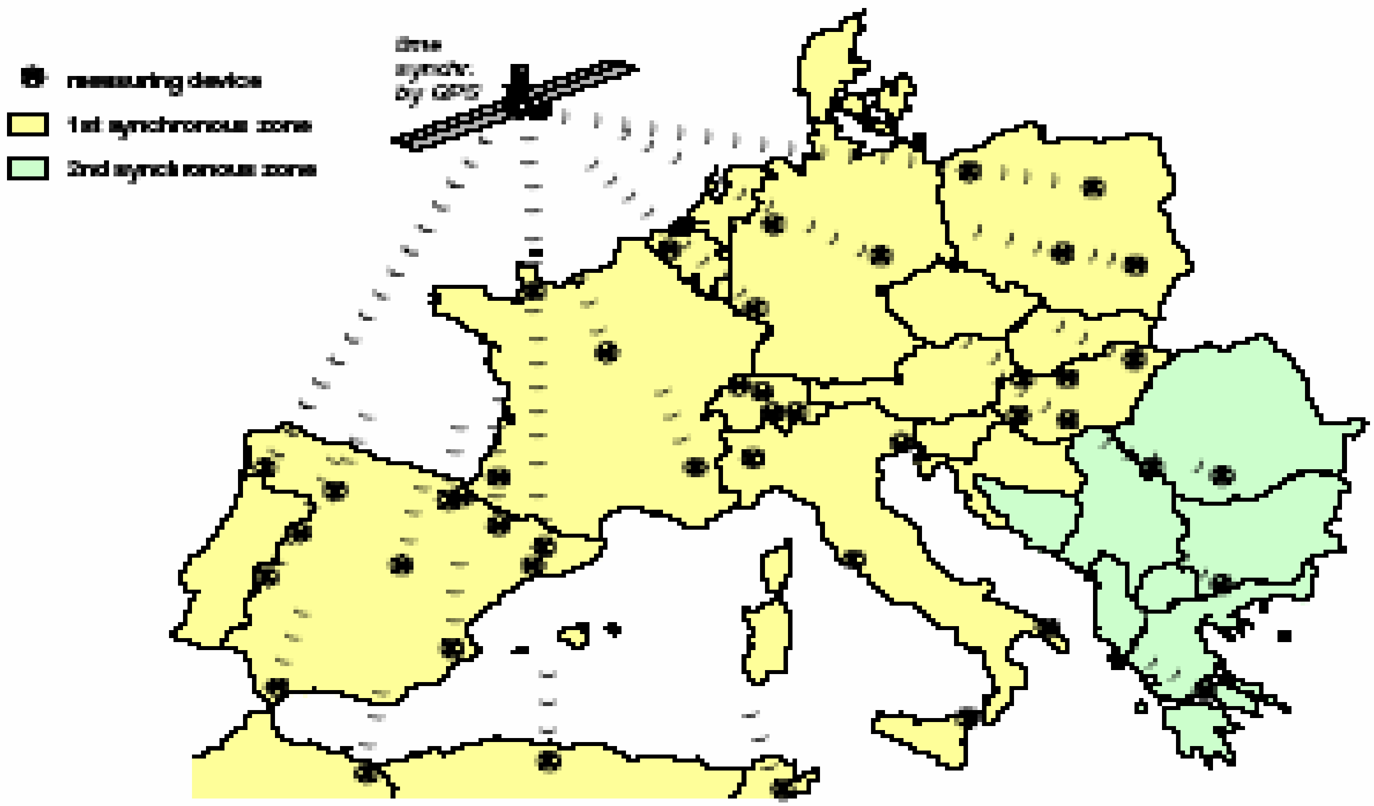
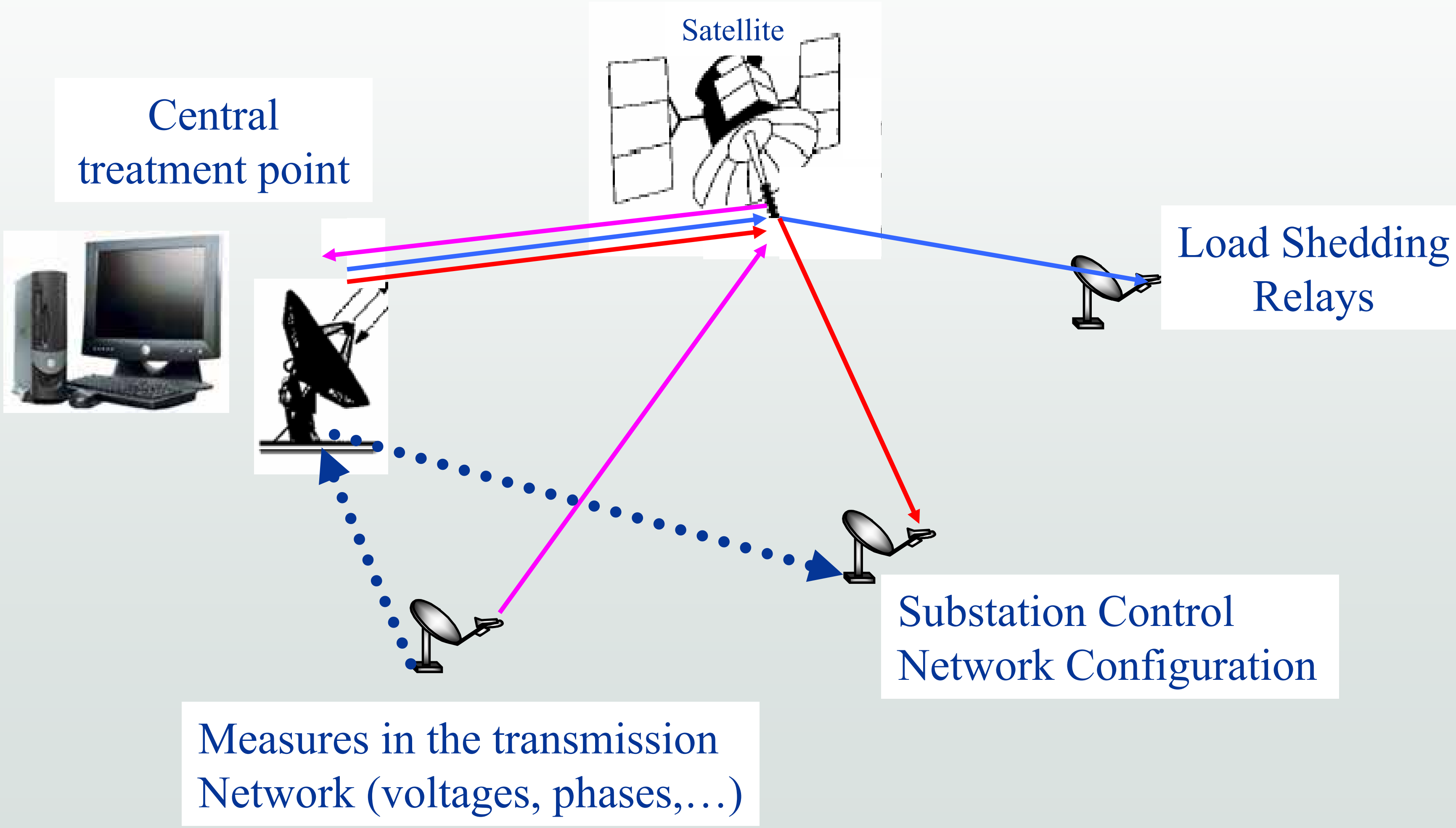


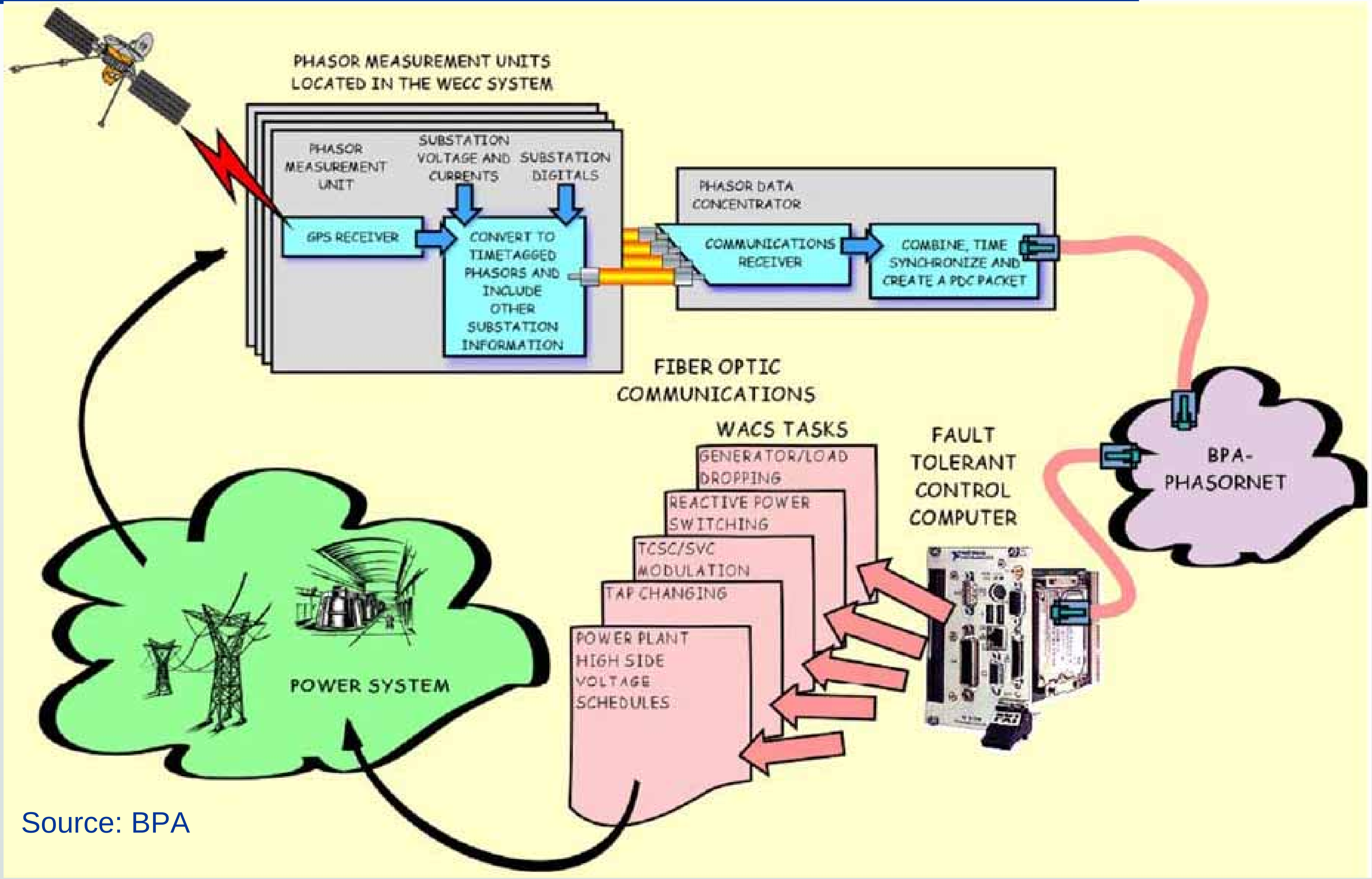
Figure 6.1: UCTE WAMS

Islanding operation

- Communication and control: Reconfiguration of the network



WAMS / WACS



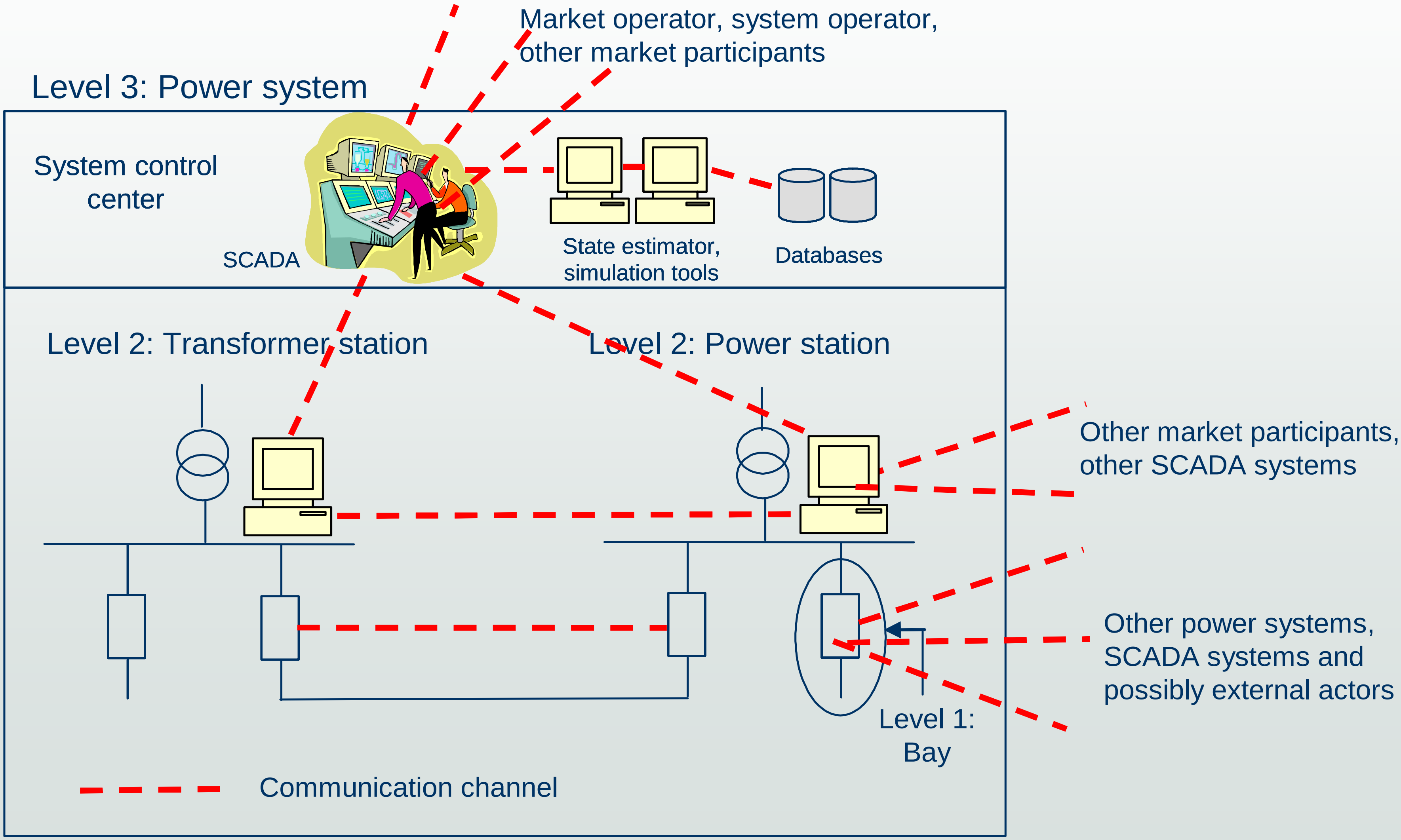
Source: BPA

The GRID Initiative

- ***Purpose***
  - Establish consensus at the European level on the key issues involved in power systems vulnerabilities
    - Establish most urgent and significant R&D challenges to be tackled at the EU level
    - Raise awareness on security concerns at the policy, industrial, and academic level.
- ***Topics***
  - Methods to assess reliability, security and risks affecting the power grid, especially concerning vulnerabilities arising from increased control complexity and the openness of the supporting ICT
  - Management, control, and protection schemes and the relevant architectures and devices

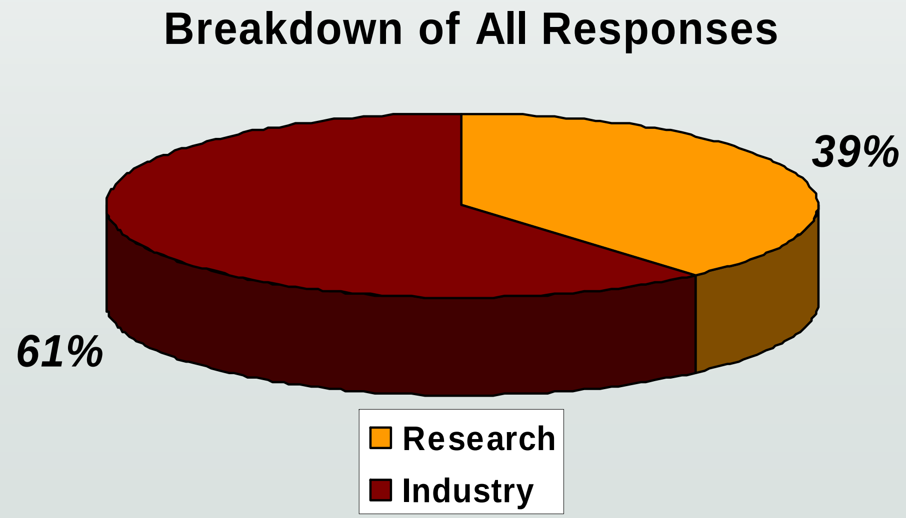
The scope of power system security and ICT in GRID

GRID

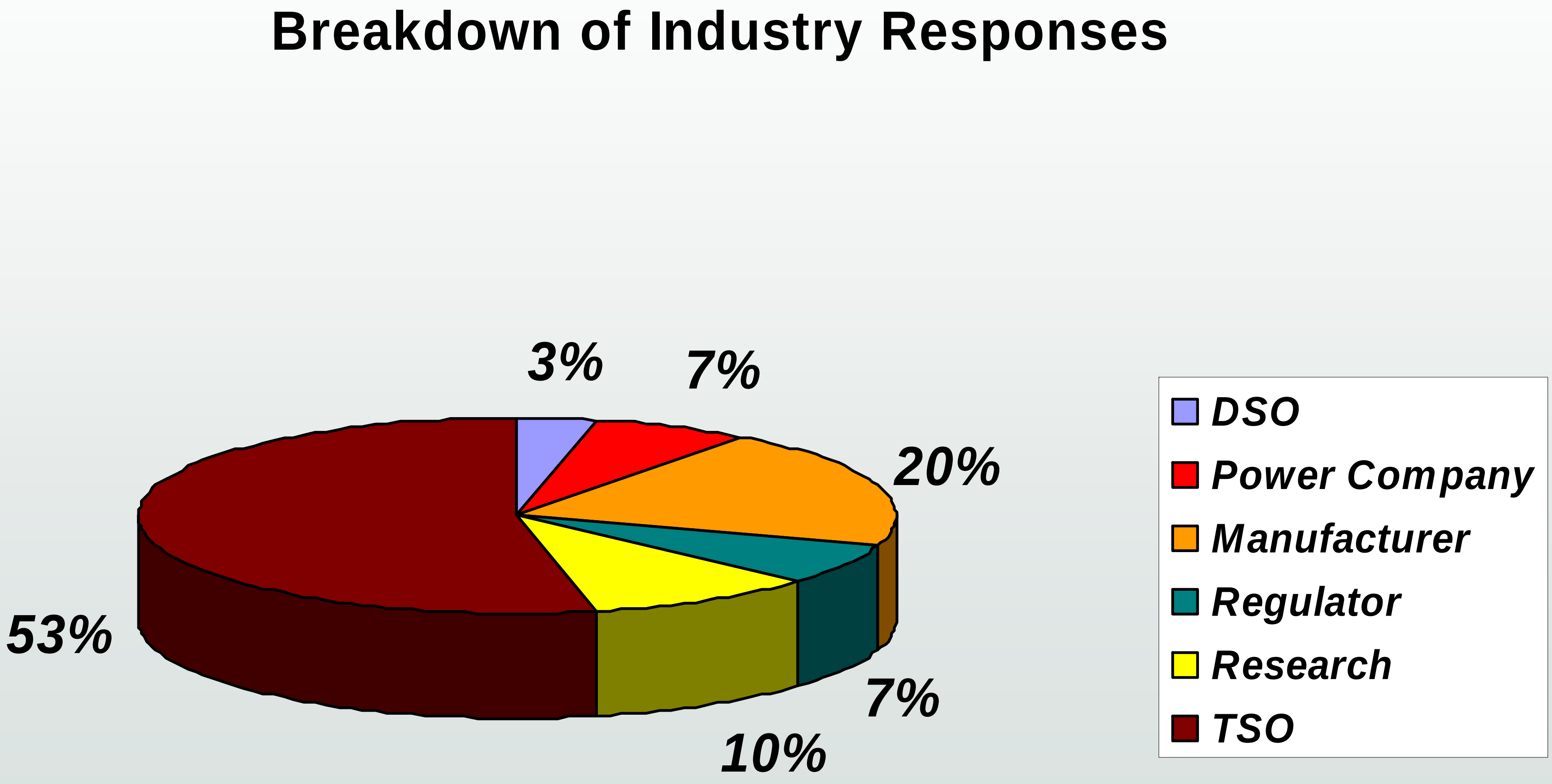


Dialogue & Stakeholder consultation: Response demographics

- **Approximately 600 members of industry and research**
- **57 total responses (~10%)**
  - **35 industry**
  - **22 research**
- **19 countries represented**
  - 18 European countries
  - United States



Dialogue & Stakeholder consultation : Response Demographics (Cont'd)



Dialogue & Stakeholder consultation : Emphasis Response

- Risk and Vulnerability Tools ranked highest by significant margin

- Control Upgrade vs. Redesign

- Risk Scenarios and Risk Education
  - Operator training should include risk scenarios
  - Education on risk encouraged at earliest stage of learning for power engineers

Roadmap: The vision 2020

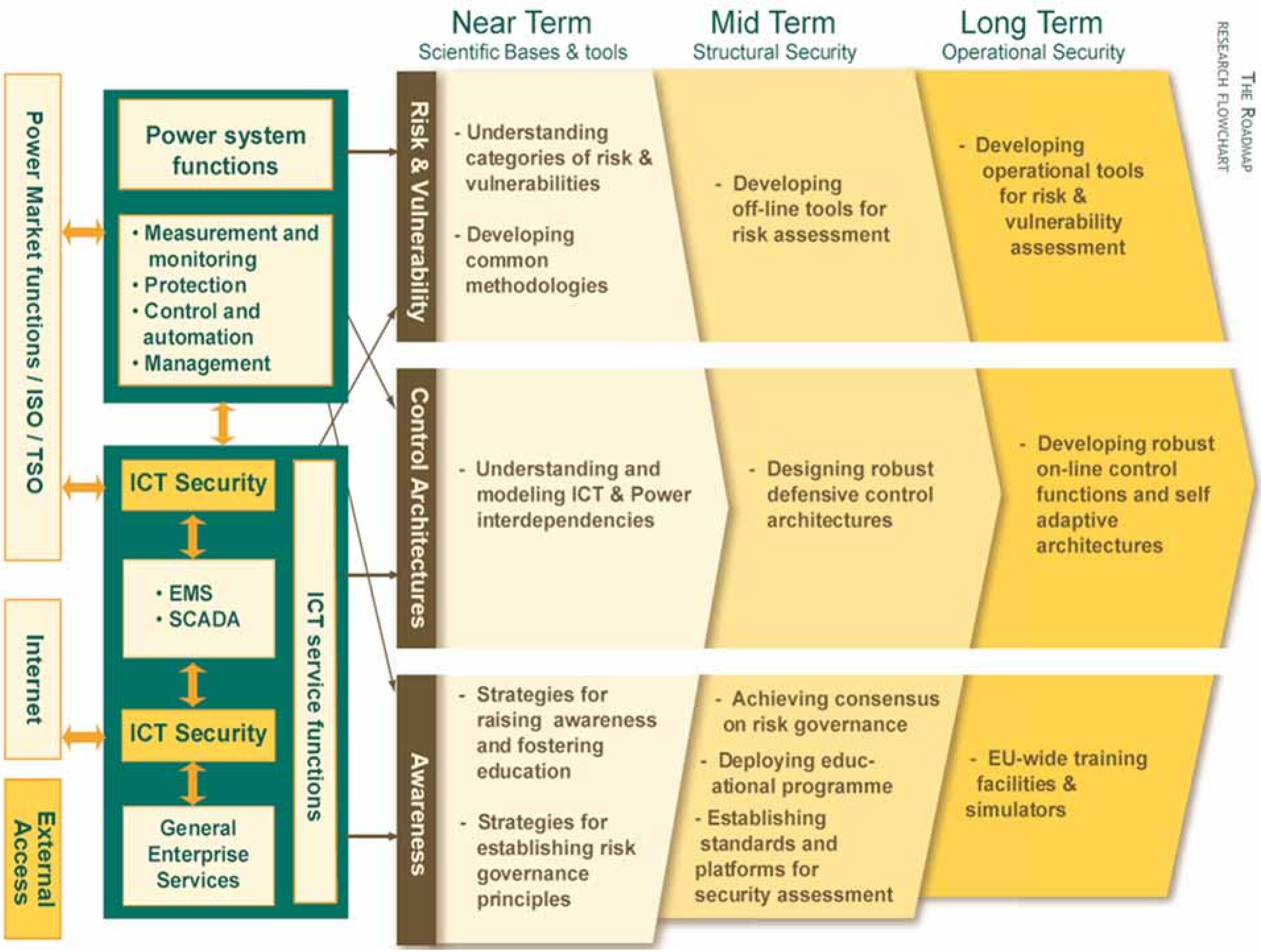
GRID

The power system maintains efficient and secure operation and continues fully utilizing its ICT functionalities without loss of load, in spite of incidents occurring in supporting ICT systems or intentional cyber assaults

Roadmap: Topics

GRID

- ***Risk and Vulnerability Assessment Tools and Methods:***
  - focused R&D is required on the relations between the ICT functions and the power system
  - tools and methods applicable by industry.
- ***Control Architectures and Technologies:***
  - investigation must focus on their upgrade
    - difficulty or barrier on integration of innovative control technologies
  - emergence of new control paradigm based on the use of decentralized intelligence
- ***Awareness and Governance of Risk in Society:***
  - need to increase awareness of control and ICT vulnerabilities
    - a basic and widespread education on risk is lacking
    - focus on the creation of educational tools and structures
  - need for risk governance strategies and for standards
  - need for facilities for security assessment


THE ROADMAP RESEARCH FLOWCHART
Near Term
Scientific Bases & tools
Mid Term
Structural Security
Long Term
Operational Security
Power Market functions / ISO / TSO
Internet
External Access
Power system functions
• Measurement and monitoring
• Protection
• Control and automation
• Management
ICT Security
• EMS
• SCADA
ICT Security
General Enterprise Services
ICT service functions
Risk & Vulnerability
- Understanding categories of risk & vulnerabilities
- Developing common methodologies
- Developing off-line tools for risk assessment
- Developing operational tools for risk & vulnerability assessment
Control Architectures
- Understanding and modeling ICT & Power interdependencies
- Designing robust defensive control architectures
- Developing robust on-line control functions and self adaptive architectures
Awareness
- Strategies for raising awareness and fostering education
- Strategies for establishing risk governance principles
- Achieving consensus on risk governance
- Deploying educ-ational programme
- Establishing standards and platforms for security assessment
- EU-wide training facilities & simulators

Research directions

GRID

Control Architectures and Technologies: Objectives and Research Actions

Chronologically sorted:
Near Term (0-3 years) - Mid Term (3-8 yrs) - Long term (8-15 years) - Final state

Objectives	Research Actions
NEAR TERM (0-3 YRS): ESTABLISHING SCIENTIFIC BASES AND TOOLS: CROSSCUTTING ISSUES	
Understanding interdependencies and cascading effects of ICT faults and scenarios	• Developing models for interdependencies able to take into account evolving IC technologies and control/protection architectures (at the control architecture level) • Developing specific common framework models able to handle failure situations with mutual cascading effects between power and ICT systems Taking advantage of: • Supportive information models such as Common Information Model framework and related common modelling languages • Cross fertilization from other application sectors: nuclear, air traffic control, transportation

Research directions

GRID

MID TERM (3-8 YRS): STRUCTURAL MEASURES (ACTIONS) : COMPONENTS AND ARCHITECTURES	

Identification of transition steps toward more robust systems	• Developing impact assessment tools of various control architectures steps onto existing systems
	  • Taking into account progressive integration of distributed generation and smart control devices & protection into existing systems
	  • Integrating human behaviour in the process elaborating the incremental solutions

Achieve flexible architectures needed to mitigate cascading effects among ICT infrastructures and power systems	• Investigating control architectures limiting fault propagation "local effects" • Designing/adapting control architectures allowing operation with degraded modes based on priorities for both power and ICT
Development of strategies for decentralized intelligence	• Investigating adaptive control concepts for power systems with accurate assessment of the impact of decentralized intelligence and control, in terms of introduced vulnerabilities vs. added value for security • Identifying and developing/adapting key devices and key interfaces as well as protection systems allowing distributed intelligence to be envisaged

Research directions

GRID

Long Term (8-15 yrs): Operational Measures (actions): Protective Measures, Remedial Actions and Real-time Applications	

Assurance of secure supervision & control actions (SCADA & EMS/DMS functions security) allowing acceptable degraded modes	• Integrating and Bridging real time control functions with vulnerability and risk assessment outputs
	  • Advanced ICT-Power state estimators with robust data processing and observability (maintain an acceptable level of observability and controllability in presence of corrupted data)
	  • Real time scenario processing (ICT & Energy contingency analysis) and parries
	• Investigating appropriate decision support tools for operators providing real time prospective views on system behaviour in critical states

Achieve self reconfiguring architectures and protection mechanisms	• Developing self reconfiguring algorithms with optimal solutions from both energy and ICT perspectives with security oriented objective (following threat detection)in order to recover a desired security level • Developing self adapting and robust protection mechanisms covering the whole control architecture chain with respect to centralized/decentralized control structures

What Role Can We Play?

Tremendous Amount of Work Already Underway

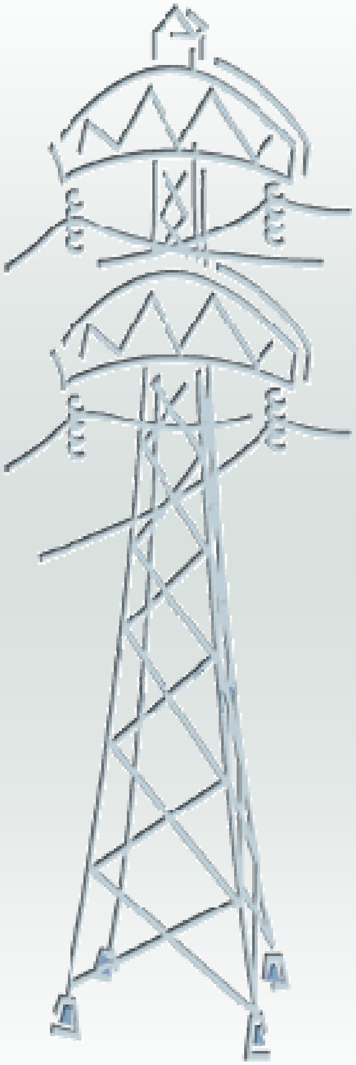
Tremendous Amount Of Work Still Needed

GRID

A Coordination Action on ICT Vulnerabilities of Power Systems and the Relevant Defense Methodologies

see: http://grid.jrc.it

thank you



INP Grenoble

EUROPEAN COMMISSION
DIRECTORATE GENERAL
Joint Research Centre

SINTEF

KATHOLIEKE UNIVERSITEIT LEUVEN

CESI RICERCA

SIT
Institut Sichere Informations-Technologie

Some terminologies

ICT Functions	Functions based on Information and Communication Technology needed for power system observability and controllability. In the context of power systems, they encompass protection, monitoring, control, operator decision support, system management & coordination.
Control architecture	"Architecture" denotes the organisational dimension (hierarchical, functional and spatial) of the control system rather than the technological solutions (information and communication hardware, protocols, software, …) supporting it.
Control system	A control system is a device or set of devices to manage, command, direct or regulate the behaviour of other devices or systems.

The scope of power system security and ICT in GRID

- The purpose of the action concerns ultimately the security of the power system while fully taking advantage of ICT functionality.
- The focus is on the transmission grid.
- Critical events triggered by distribution with large impact on transmission have to be considered.

The consortium

No	Participant organization name	Short name
1	Institut National Polytechnique de Grenoble – Laboratoire d'Electrotechnique de Grenoble	INPG-LEG
2	Joint Research Center - Institute for the Protection and Security of the Citizen	JRC-IPSC
3	Foundation for Scientific and Industrial Research – Energy and ICT departments	SINTEF
4	Centro Elettrotecnico Sperimentale Italiano- RICERCA	CESI-RICERCA
5	Fraunhofer Institute for Secure Information Technology	FhG-SIT
6	Katholieke Universiteit Leuven – ELECTA Division	KU-Leuven

The consortium - SAB

A Stakeholder Advisory Board

- <u>TSO and Power companies</u>
  - EdF – France
  - REE – Spain
  - STATNETT – Norway
  - TENNET - Netherlands
  - TRACTEBEL - Belgium
- <u>Energy and telecom companies</u>
  - ABB - Switzerland
  - SIEMENS - Germany
- <u>Government bodies</u>
  - UKERC (UK Energy Research Center) – UK
- <u>International organization</u>
  - CRIS (International Institute for Critical Infrastructures)

Project organisation

Work-package No	Workpackage title
WP1	Management
WP2	Vulnerability and risk assessment
WP3	Management, control and protection schemes and the relevant architectures and devices
WP4	Strategies and dissemination

Important Progress Steps

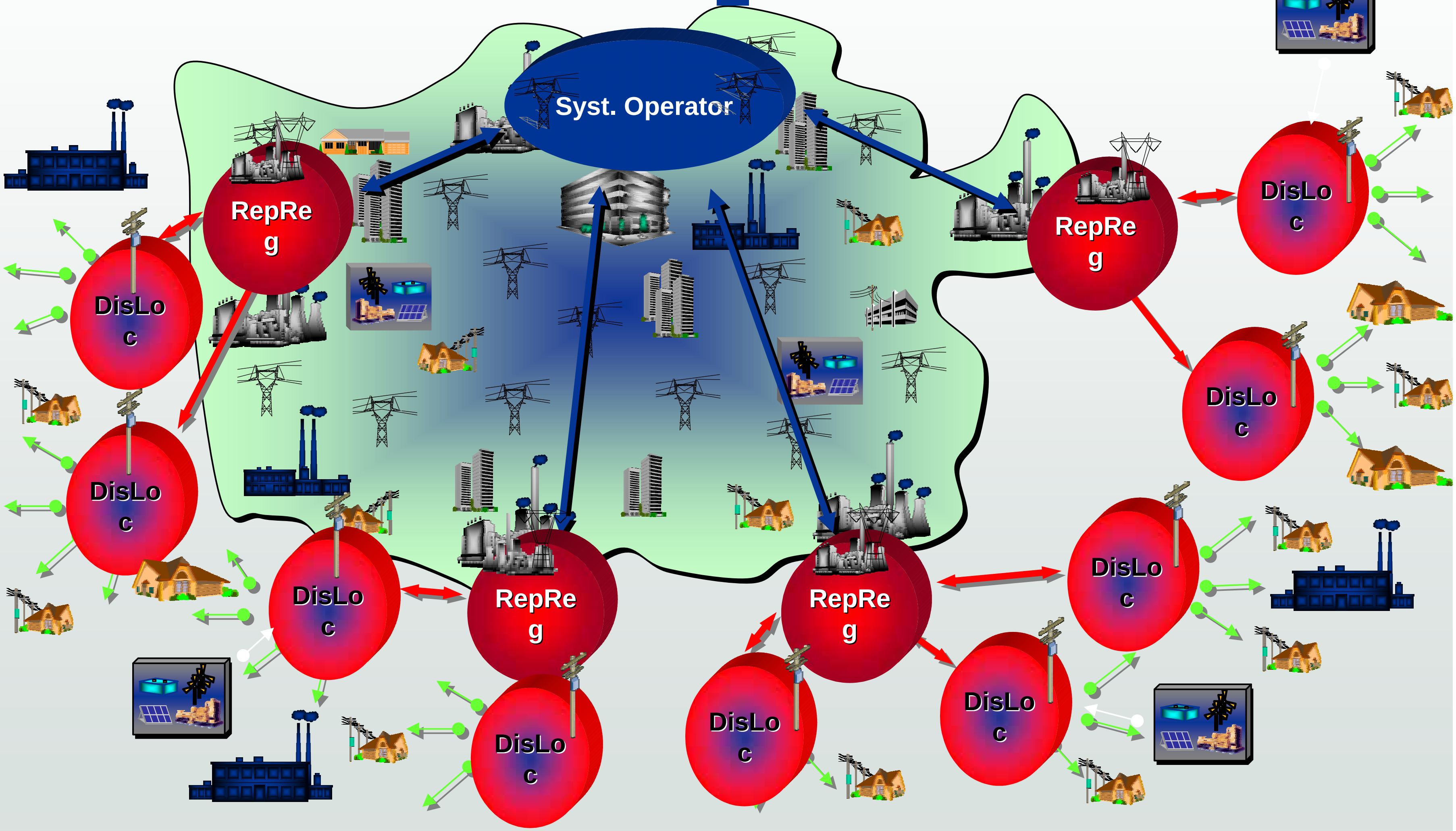
GRID

- ***1st GRID Conference***, Stavanger, Norway: June 15th, 2006
  - Gathering stakeholders needs
- ***Questionnaire***
  - Broad range Stakeholders consultation
- ***Questionnaire processing & analysis***
  - Issuing a position paper
- ***1st GRID Workshop***, Leuven, November 15th, 2006
  - Updating the position paper
- ***Preliminary roadmap***: February 2007
- ***2nd GRID Workshop***, Paris June 20th, 2007
  - Updating the preliminary roadmap
- ***December 2007***
  - Final Roadmap
- ***2nd GRID Conference***, February 2008

The GRID Project: methodology

- ***Methodology***
  - Structure the work, identify key issues, define targets, issue questionnaires
- ***Dialogue*** *– Stakeholders consultation via questionnaire*
  - Regulators, transmission system operators, electric utilities, R&D institutions
  - European representative associations (Eurelectric, UCTE, ETSO).
- ***Evaluation & Analysis***
  - Analysis of the different security issues, the current knowledge and bottlenecks, the on-going or planned initiatives and researches, directly or indirectly linked to the topic;
  - identification of research priorities –roadmapping;
  - Identification of recommendations to be issued for security policies

System hierarchy



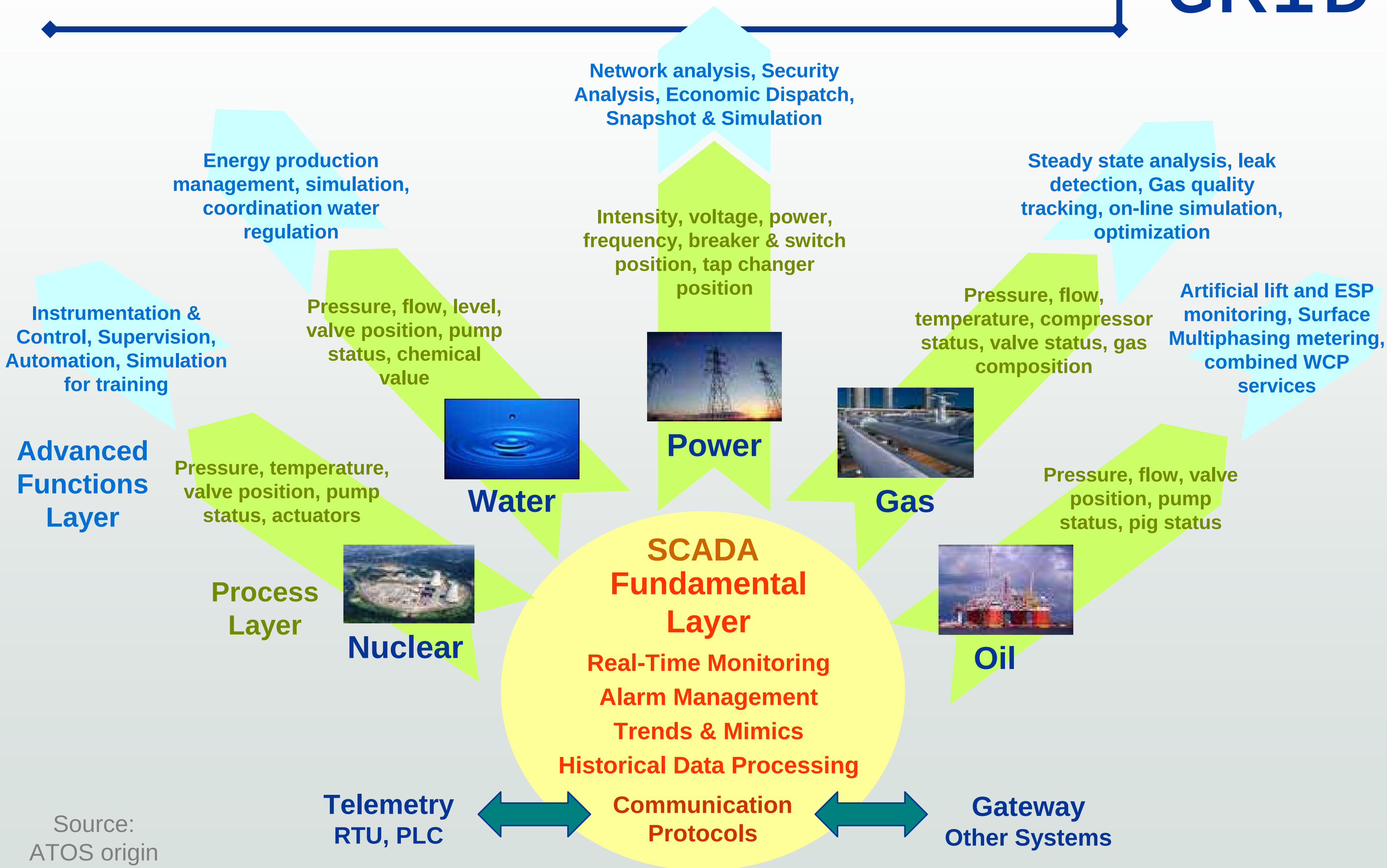
Needs and challenges

GRID

Stakeholders specific Needs

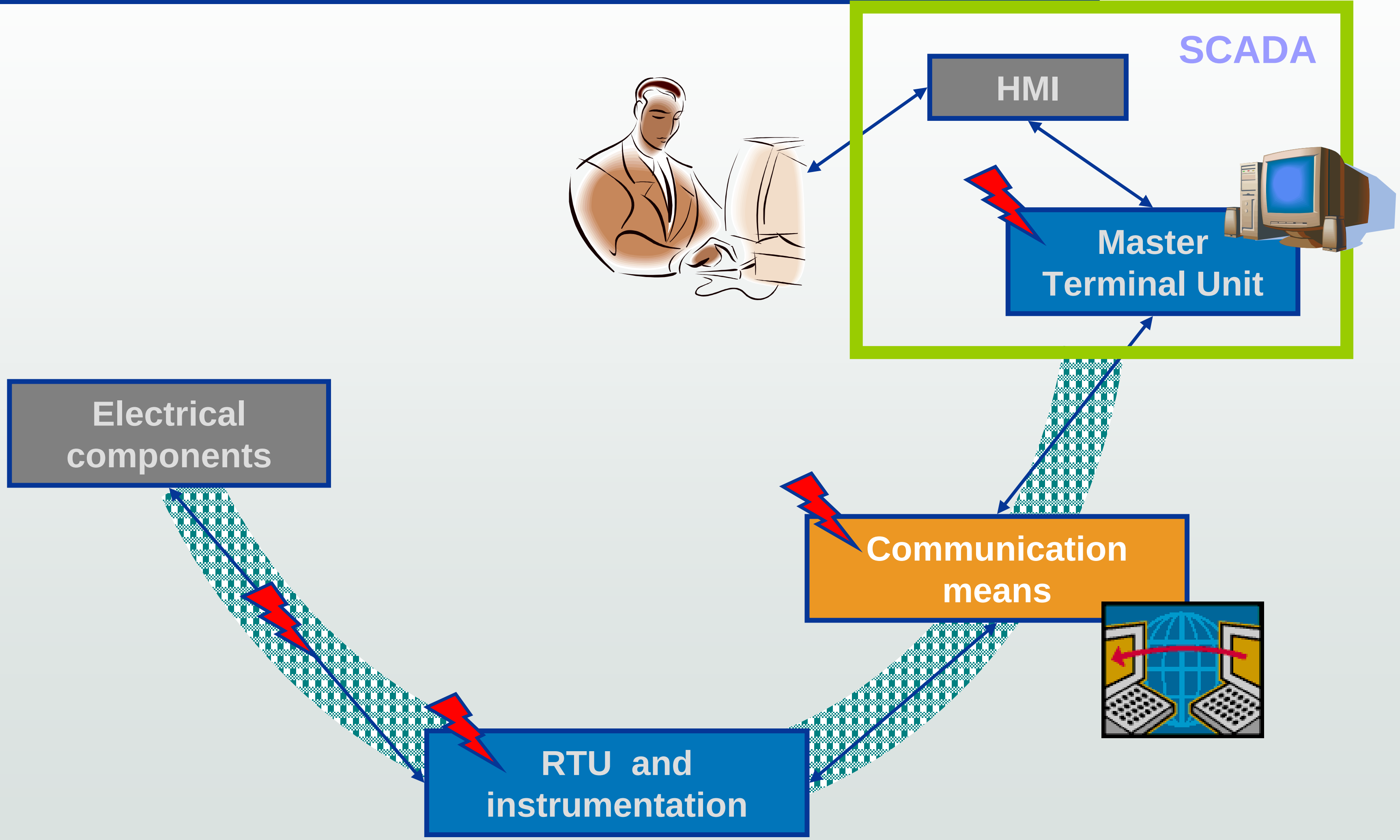
- *New components and devices with built- in information security*
- *Control architectures*
- *Incremental, flexible and inherently robust to ICT attacks and flaws*
  - *Mitigating cascading effects among ICT infrastructures and power systems.*
  - *Able to accommodate new technologies and tools for security evaluation and countermeasures*
- *New protection and Countermeasures algorithms (including intrusion tolerance approaches and access control policies and models)*
- *Specific Operator decision tools, based on online, real-time monitoring results*

Control center: three layers approach



Source: ATOS origin

Securing the structure : risk assessment of failures or malicious attacks



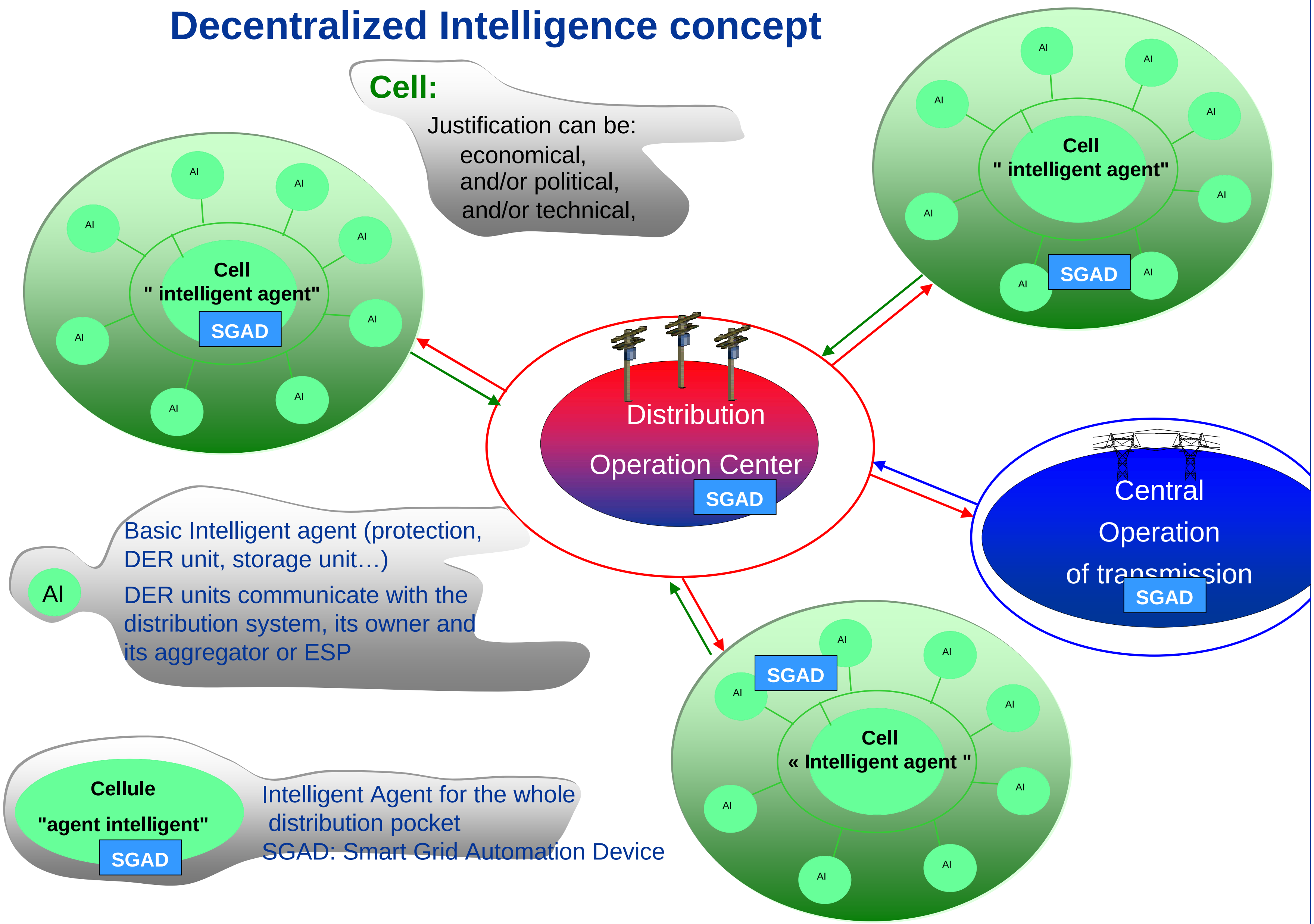
Source: Securing SCADA systems

Conclusion

GRID

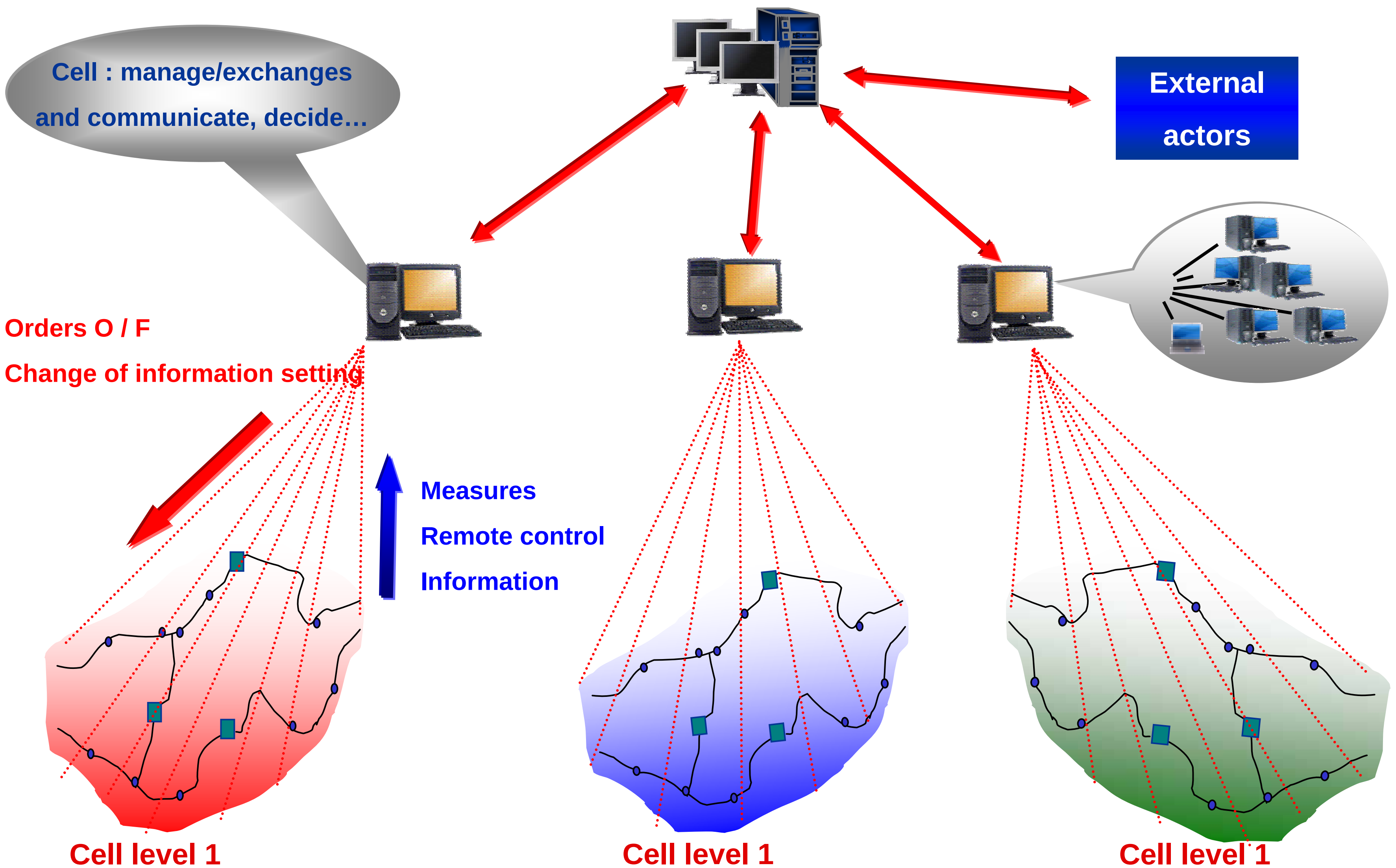
- Current power systems are vulnerable to both “external” and natural events (storms, …)
- Large economical and social impacts
- Several examples all over the world
- Information and communication issues vs impact on cascading effects
- EU initiative: GRID, CRISP, …
- Work on progress…
- Cooperation is an important issue (CRIS)

Decentralized Intelligence concept



Decentralized approach: cell concept

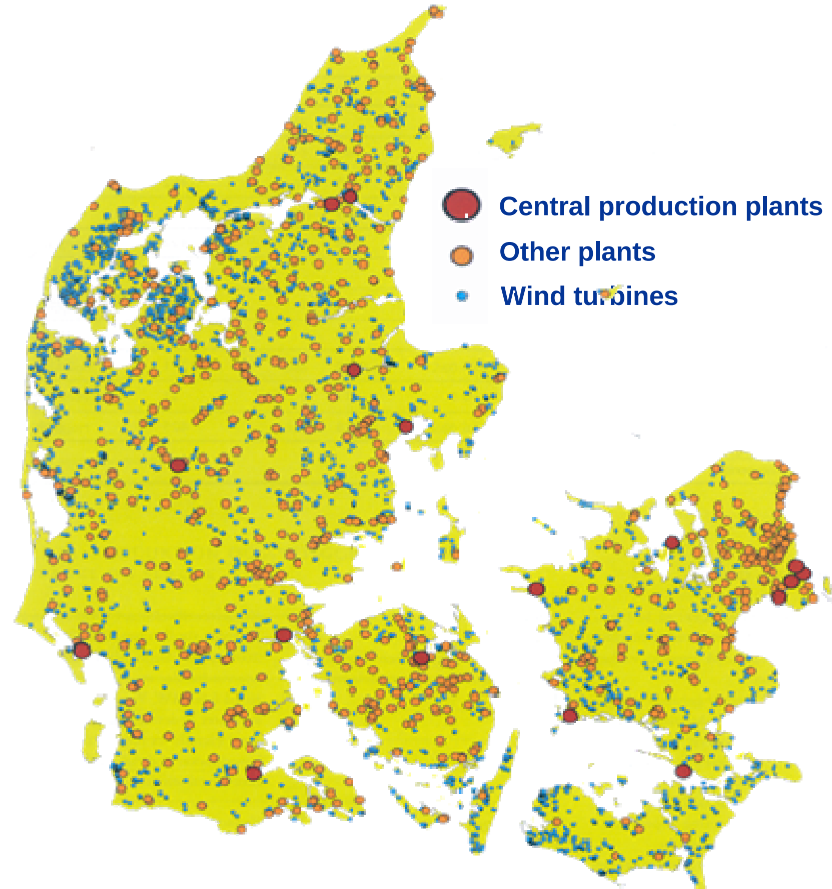
Decentralized organization of energy and information exchange



Context – example of Danemark

Système centralisé de production

Système décentralise de production



Source: Eltra

Toward a Virtual Power Plant