Testbeds for assessing critical scenarios in Power Control Systems

G. Dondossola[1], G. Deconinck[2], F. Garrone[1], H. Beithollahi[2]

[1] Power System Development CESI RICERCA, Milan, Italy

[2] ESAT/Electa Katholieke Universiteit, Leuven, Belgium

Contact information

Name: *DONDOSSOLA Giovanna*
Phone: *+39-02-3992 5779*
Fax: *+39-02-3992 5557*
e-mail: *Giovanna.Dondossola@cesiricerca.it*

Name: *DECONINCK Geert*
Phone: *+32-16-31 11 26*
Fax: *+32-16-32 19 85*
e-mail: *Geert.Deconinck@esat.kuleuven.be*

CESI RICERCA

CRUTIAL

Models

Power control infrastructures

Evaluations

Architectures

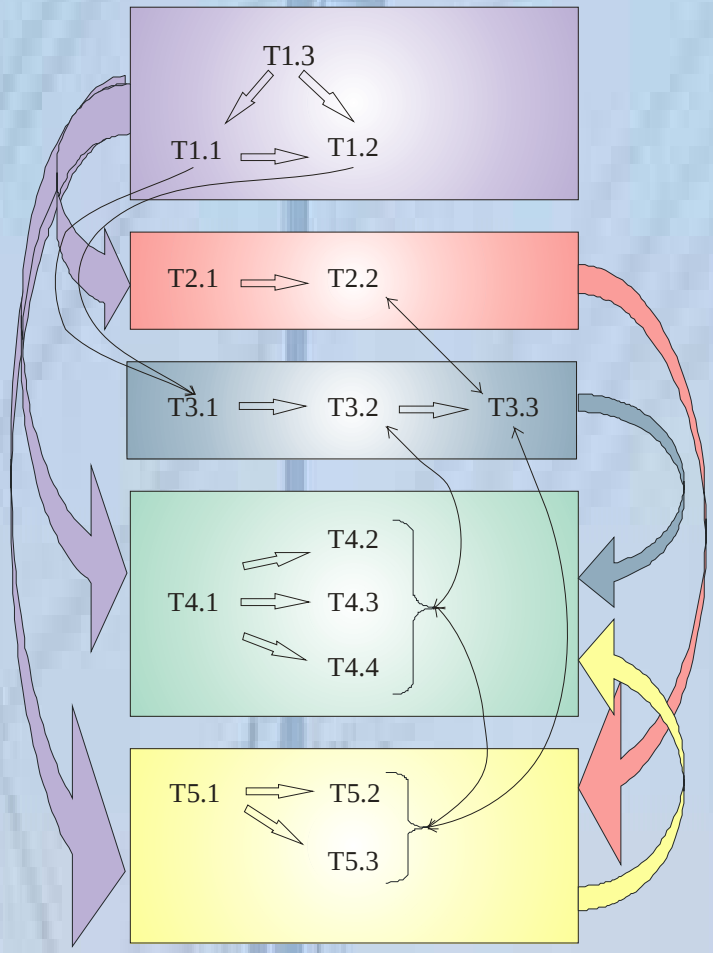


Table of Content

- Testbed activity in CRUTIAL WP3
- Control system scenarios
- T1 – Hierarchical Teleoperation of Macrogrids with Bulk Generation
  - Architecture, control scenarios, test plan
- T2 – Distributed Control of Microgrid with Distributed Generation
  - Architecture, control scenarios, test plan
- Conclusions

Testbed activity in CRUTIAL

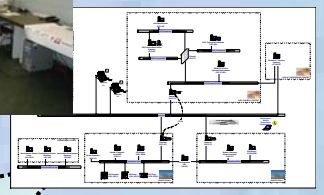
- CESI RICERCA Grid teleoperation testbed (T1): power substation controllers on real-time control networks, interconnected to control centre operation networks in turn connected to corporate networks
- K.U.Leuven testbed Microgrid testbed (T2) : power electronic converters controlled from PCs interconnected over an open communication network
- Aims
  - identify critical aspects of power-ICT dependencies
  - assess the ICT infrastructure vulnerability to plausible cyber attacks
  - assess the severity of potential damages
  - evaluate the resiliency of possible architectures/mechanisms/solutions to cyber threats

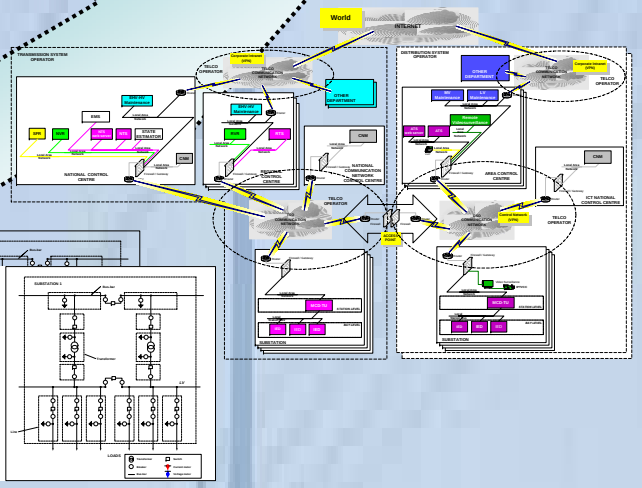
Control system scenarios

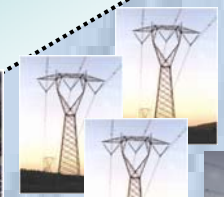
- scenario 1: DSO teleoperation
  - use of an IP backbone for DSO supervision and control
  - assess redundant communication architecture
  - assess vulnerabilities of standard protocols and their impact on control functions
- scenario 2: interaction between TSO/DSO in emergency
  - assess defense plan actuation (automatic load shedding)
  - assess security of the TSO-DSO communications
  - evaluate the impact of attacks in emergency conditions
- scenario 3: ICT driven decentralised control algorithms in microgrids with Distributed Energy Resources
  - Evaluate the impact of network latency, packet loss, network unavailability, DoS attacks on overlay networks, incorrect values on tertiary (economic) and secondary (voltage) control

T1: Grid teleoperation

- The Grid Teleoperation testbed implements a scaled down power control platform with its integrated ICT infrastructure for testing the cyber security of **SCADA, substation automation and communication systems**



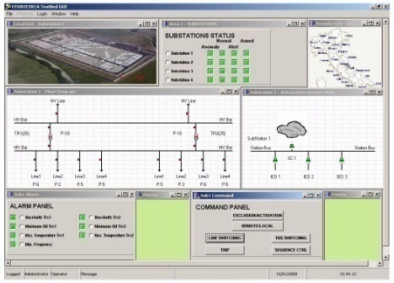


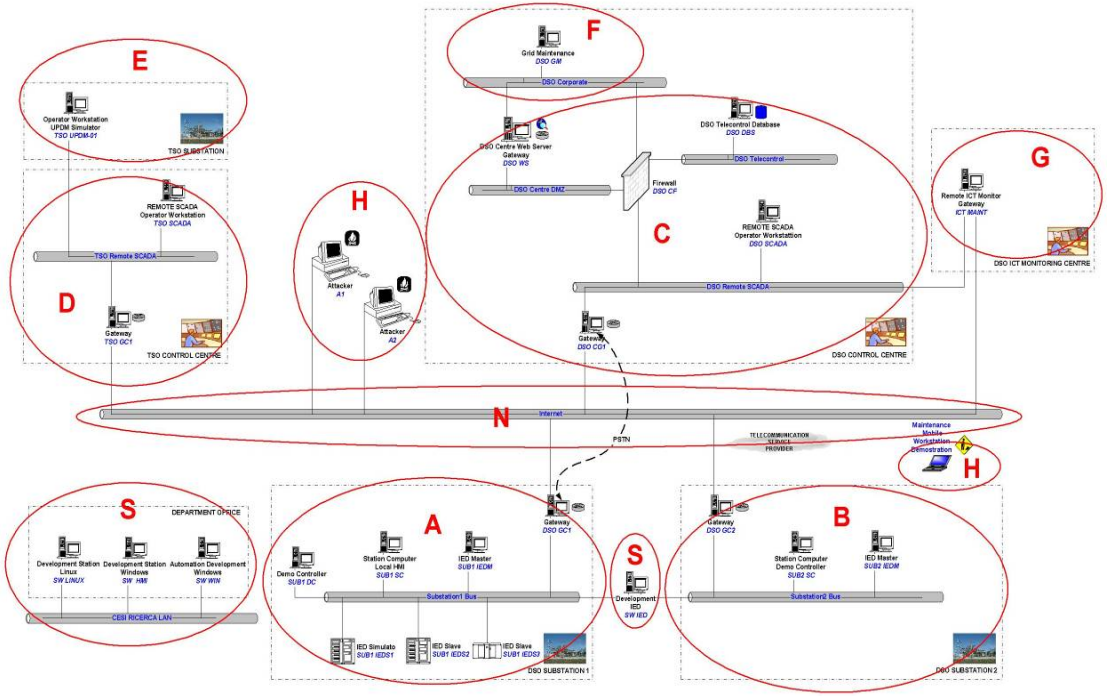


T1: Grid teleoperation

- Aims
  - to improve the **security know-how** in power control
  - to mitigate the **vulnerabilities** of the standard protocols (e.g. IEC 60870-6, IEC 60870-5-104, IEC 61850)
  - to assess the capability of **secure and redundant architectures** to tolerate the threat hypotheses
  - to offer a **testing infrastructure** for SCADA and automation system properties, difficult to reproduce in real infrastructures
  - to facilitate the development of cyber security **standards, guidelines** and **practices** for industrial usage (e.g. NERC, IEC, IEEE, NIST, ISA)
  - to support **risk assessment** and **model based evaluation** with statistics from experiments

Grid Teleoperation Testbed

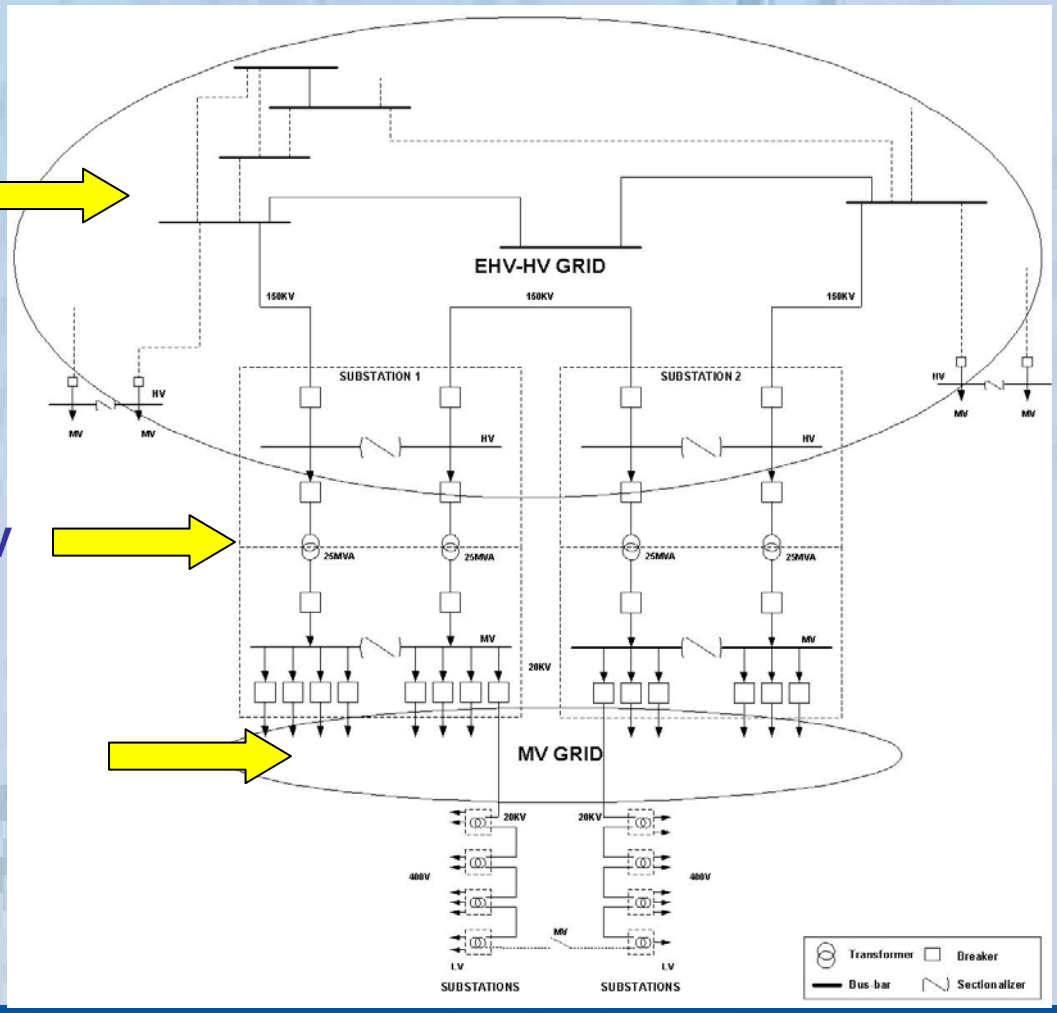




T1: power infrastructure

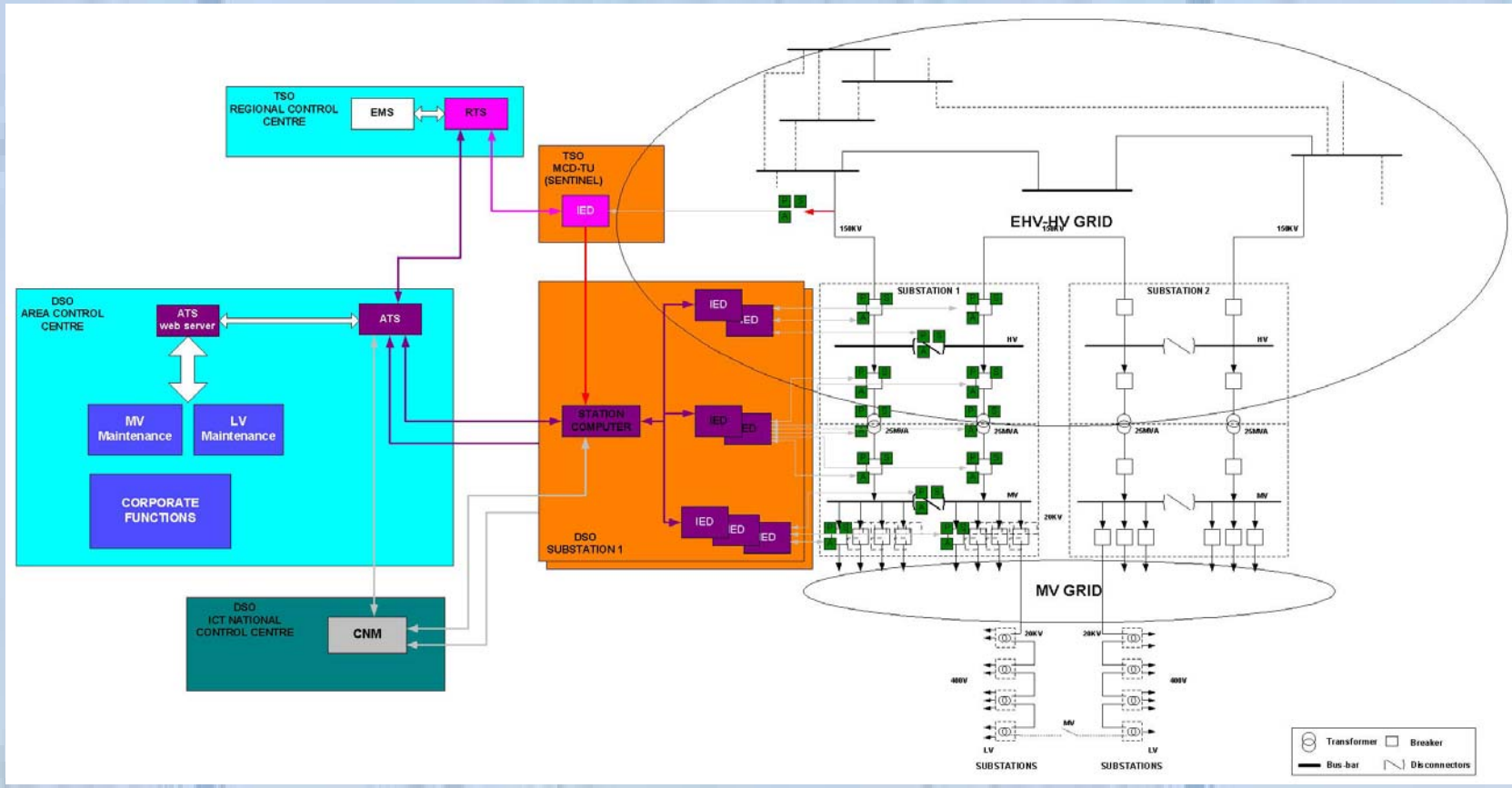
- The Electric Infrastructure is currently simulated through pre-compiled Input sequences

  - **EHV-HV Grid**
  - **Substations HV/MV**
  - **MV Grid**



T1: functional components

- The laboratory architecture is based on building blocks implementing functional components
  - **Grid Control Centres, control devices, substations, ICT Control Centres**



Laboratory: building blocks

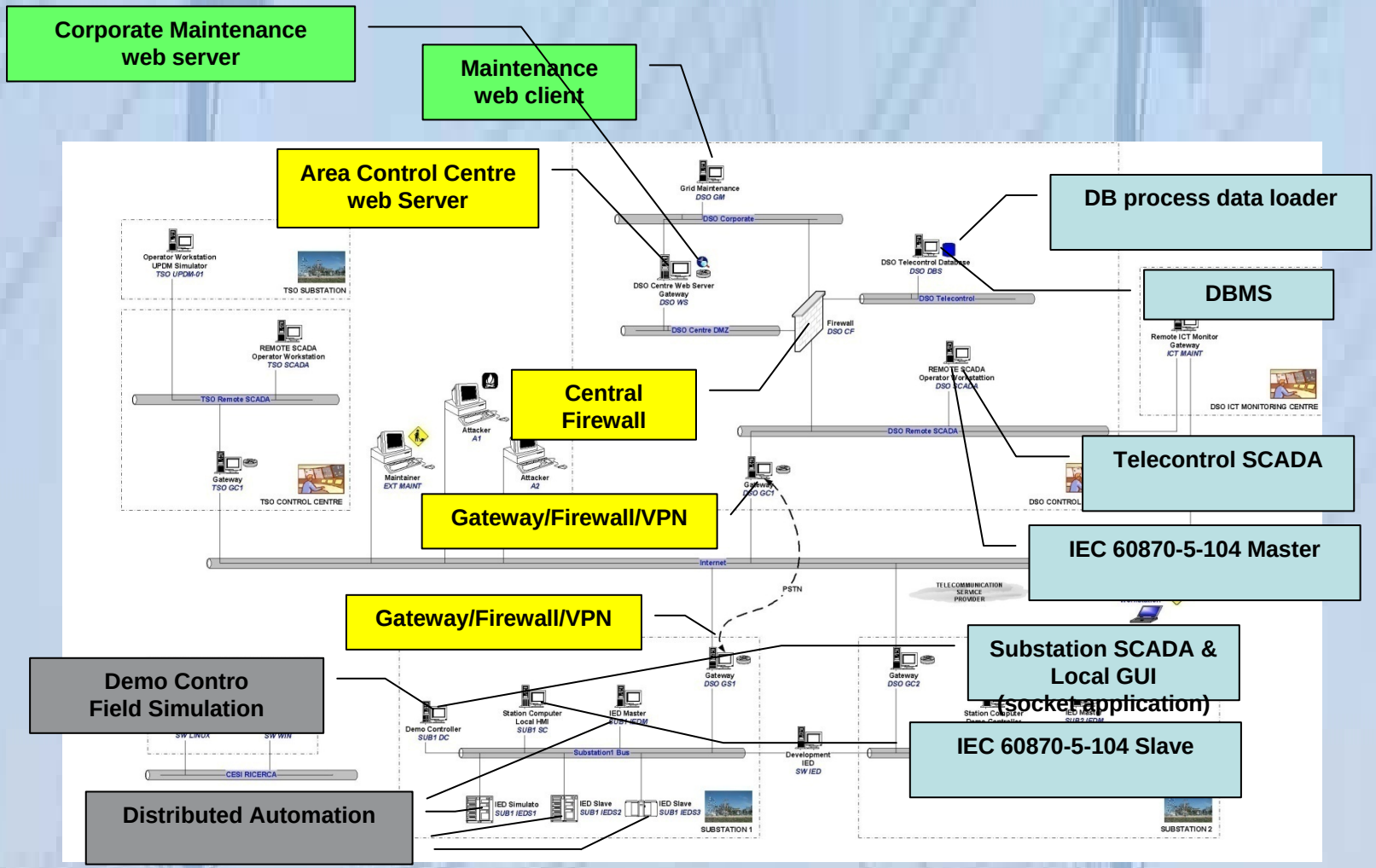
- The ICT components are related to these functions
  - Automation
  - Communication
  - SCADA
  - HMI
- The ICT components are developed as prototypes to easily produce logs
- Automation relevant aspects
  - Automatic code generation (bug free)
  - Distributed architectures (IEC 61850)
  - Fault tolerant architectures

Laboratory: building blocks

- Communication relevant aspects
  - Open transport/network layer standard protocols (TCP/IP, UDP/IP)
  - Power domain - application layer standard protocols (IEC 60870-5-104)
  - Security standard protocols (IPSEC, VPN)
- SCADA relevant aspects
  - Standard DBMS
  - Standard Web servers
  - Process vs corporate network separation
- HMI
  - Both Power and ICT views
  - Both Power and ICT alarm warnings
  - To increase operators' awareness on the ICT Infrastructure status

Laboratory: software components

- The test bed software components layout



Threats

- DoS attacks to the teleoperation communications, generated by enemies located on the Telecom IP backbone
- Intrusions into the Centre/Substation communication flow followed eventually by the execution of faked commands
- Authentication violations of a Substation Computer on the process control LAN through hostile use of maintenance activities

Grid Teleoperation: Scenario 1

DoS attack to Centre/Substation communications

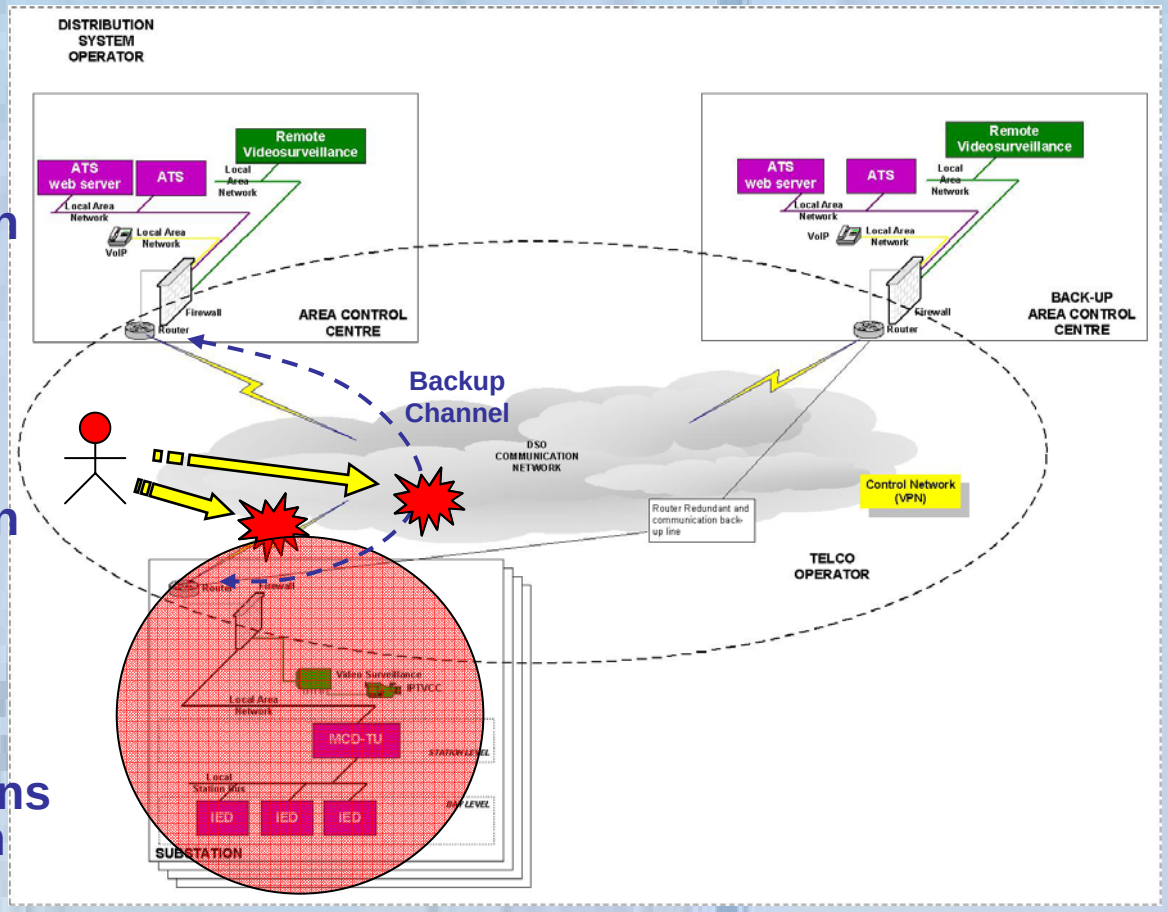
- **Attack to a Substation router/gateway by TSP insider**

1 - TSP insider starts attack

2 - Communication bandwidth reduction

3 - Communication backup line

4 - Loss of remote control functions of a Substation



Grid Teleoperation: Scenario 1

DoS attack to Centre/Substation communications

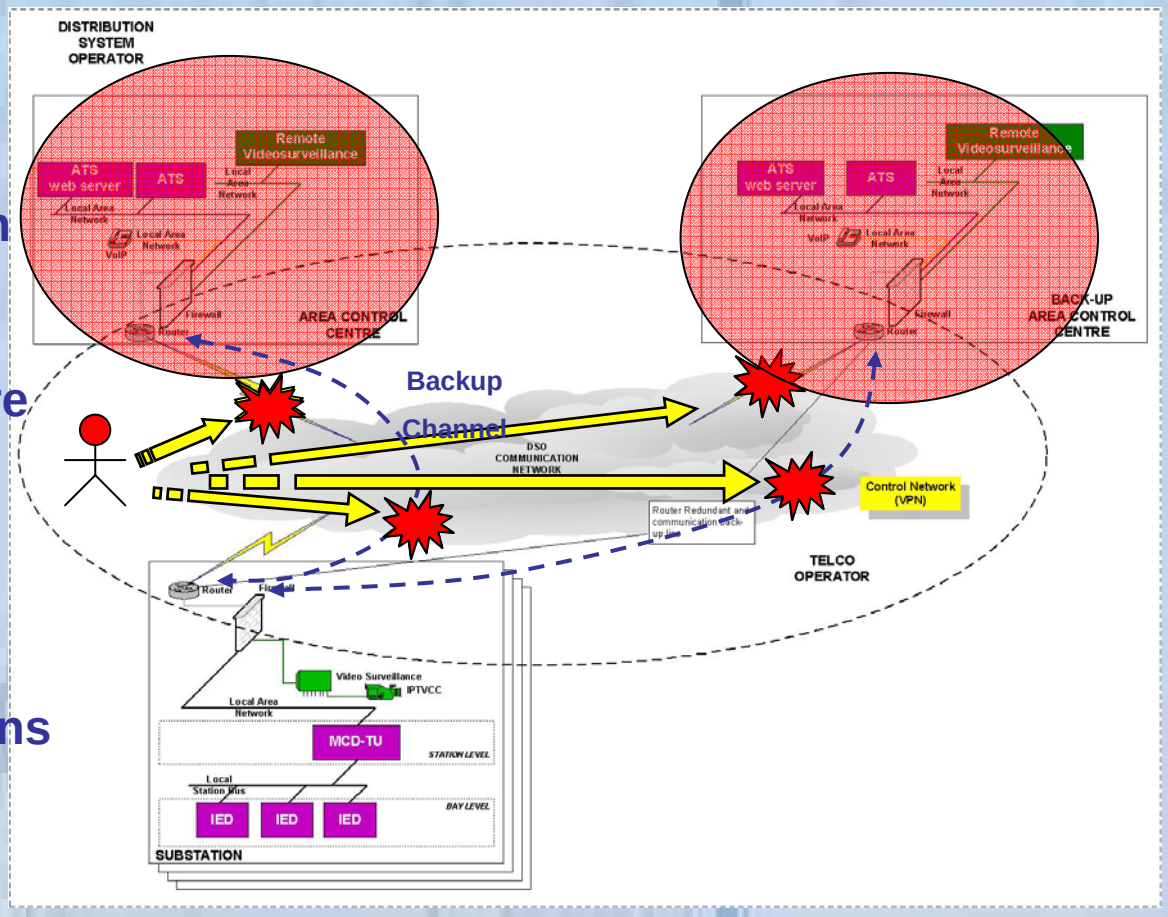
- **Attack to Centre router/gateway by TSP insider**

1 - TSP insider starts attack

2 - Communication bandwidth reduction

3 - Loss of a Centre remote control functions of a group of Substations

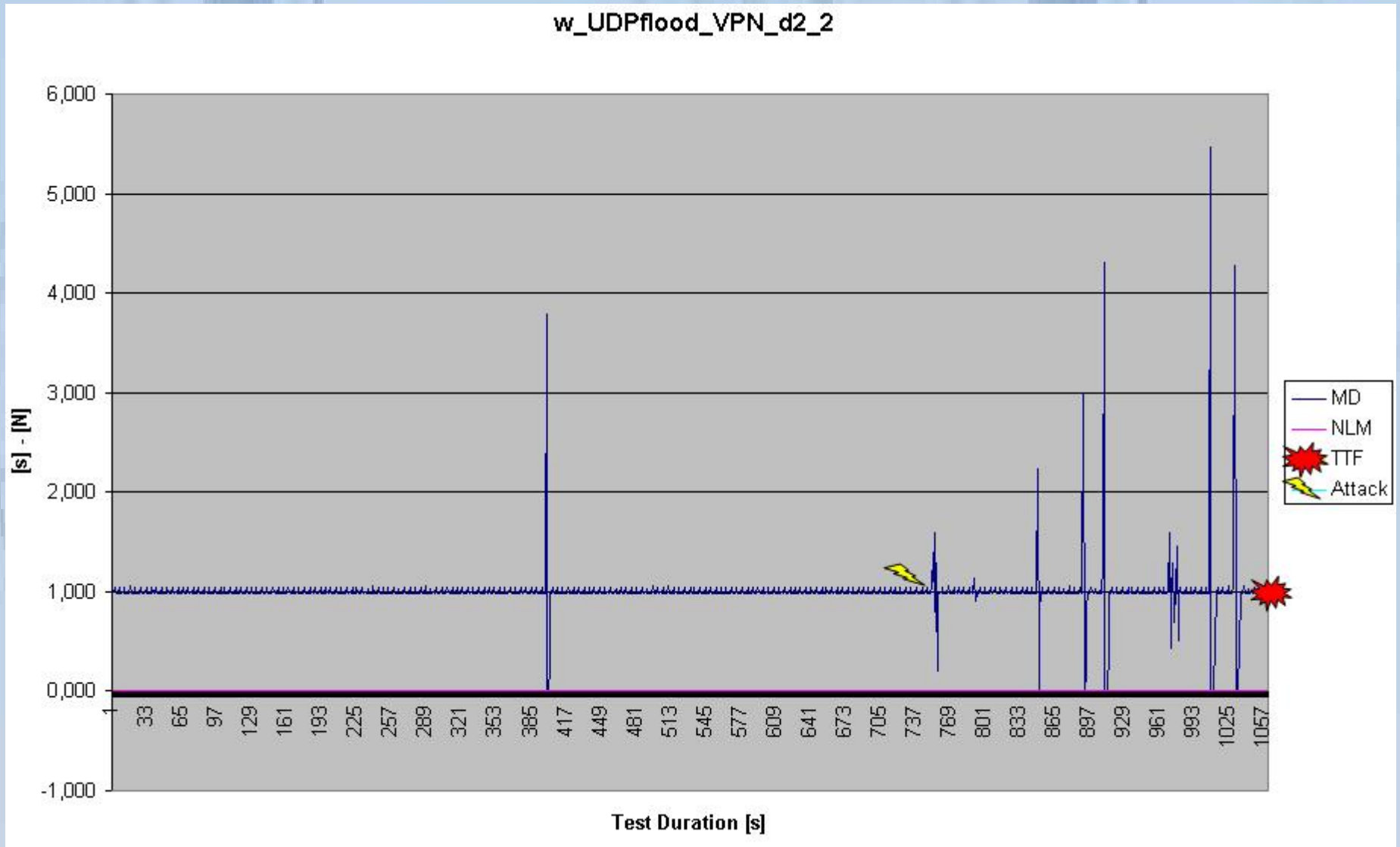
4 - Loss of remote control functions of a group of Substations



DoS Attack: Simulation

- Simulation of DoS attack processes to IEC 60870-5-104 communications
  - Based on standard TCP/IPSEC communication
- Attack phases
  - Pre-attack phase
    - TSP Scanning/sniffing/dump activities
  - Attack execution
    - Message flooding: Syn packets
    - Message flooding: ICMP packets
    - Message flooding: UDP packets
    - TCP replay: ICMP, TCP, ESP
  - Attack monitoring
    - Firewall logs
    - IPSEC logs
    - Tcpdump
    - Communication sniffing
    - IEC 60870-5-104 communication logs

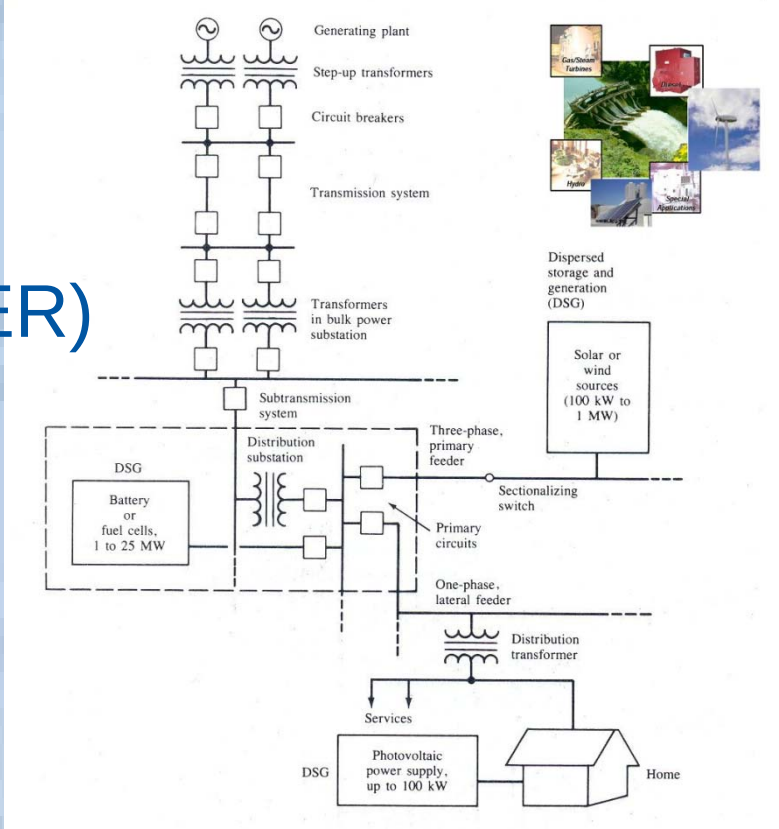
UDP flooding: experimental data



Grid Teleoperation: evaluation plan

- Scenario 1: manual teleperations
  - fault-free (*reference TCP/IP/*overhead of VPN)
    - for different VPN configurations
  - Threats: DoS, autentication violation, viral infection
  - Measures: delayed packets, lost packets, time to failure
  - Consequences: grid supervision, preventive maintenance, normal operation, pre-emergency operation
- Scenario 2: automatic teleoperations
  - fault-free (*reference/*overhead of VPN)
    - for different VPN configurations
  - Threats: DoS, intrusion
  - Measures: delayed packets, lost packets, time to failure
  - Consequences: grid supervision, emergency operation

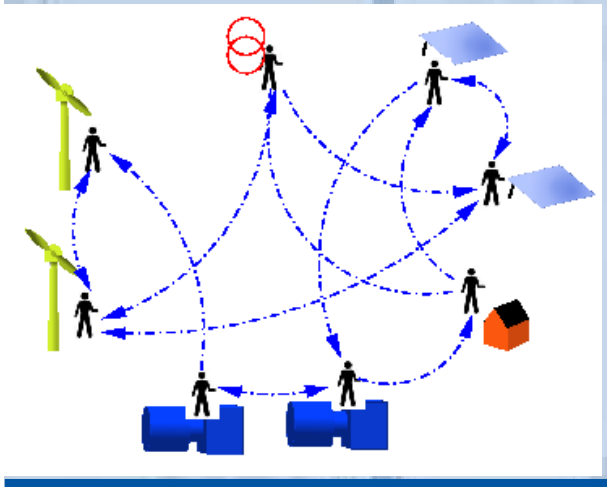
T2: Distributed microgrid control



- dispersed energy resources (DER)
  - at distribution level (MV, LV)
  - renewable sources
    - PV, CHP, wind, fuel cell, etc.
  - storage systems
    - supercaps, fuel cells, UPS, …
  - intelligent loads
- → IEDs (intelligent electronic devices)
  - connected to grid via power electronics
    - inverter front-ends
  - interconnected via communication network

Distributed control systems

- distributed control of DER
  - optimize voltage level (*secondary* control)
  - optimize production costs (*tertiary* control)
  - data aggregation, system monitoring etc.
- layout of communication architecture
  - point to point infrastructure vs. overlay network
  - distributed agents vs. centralised control
    - + small capital investment
    - + no single point of failure
    - - security more difficult

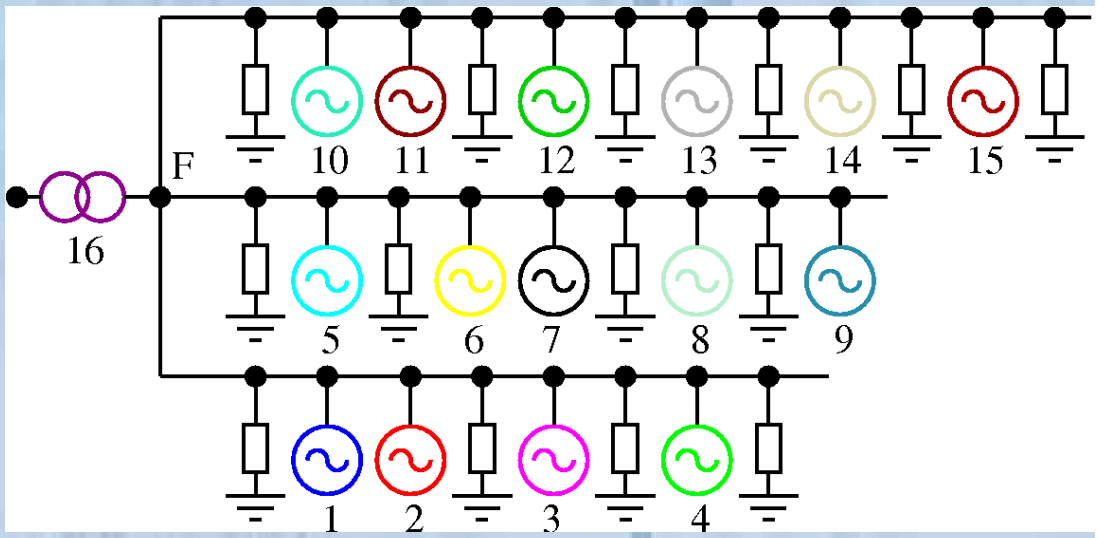


ICT threat assessment in distributed microgrid applications

- accidental fault scenarios
  - network delays/packet loss
  - → *slower convergence of 2nd-ary / 3rd-ary control loops*
  - communication failure; soft-/hardware crash
  - → *overlay network can manage dynamism, if available*
- malicious fault scenarios
  - denial-of-service attacks → *similar, not critical*
  - intrusions on control PCs
    - attacks on middleware level → *critical*
      - e.g. influence overlay topology
    - attacks at application level→ *critical*
      - e.g. tampering with *3rd-ary* control (financial gain)
      - e.g. tampering with *2nd-ary* control (voltage profile disturbance)

Microgrid simulation model

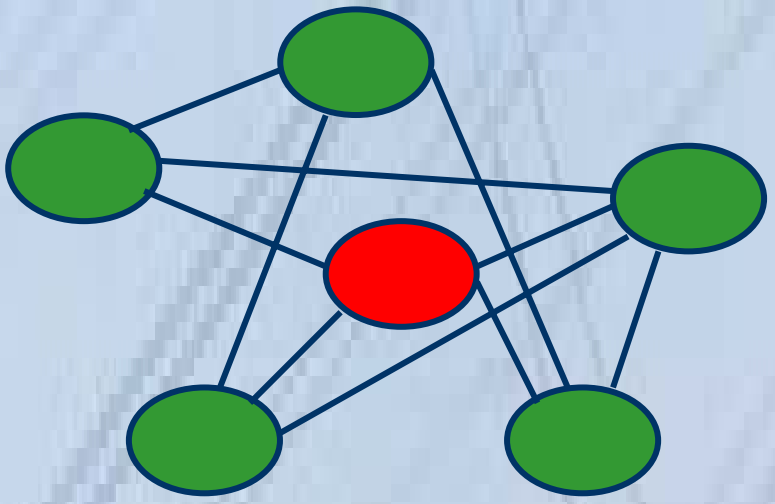
- low voltage power distribution segment
  - grid connected
  - high DG penetration
  - variable loads
- agents
  - form overlay network
  - control power output
- primary, secondary, tertiary control



- ➔ many scenarios (ICT fault →EPS)

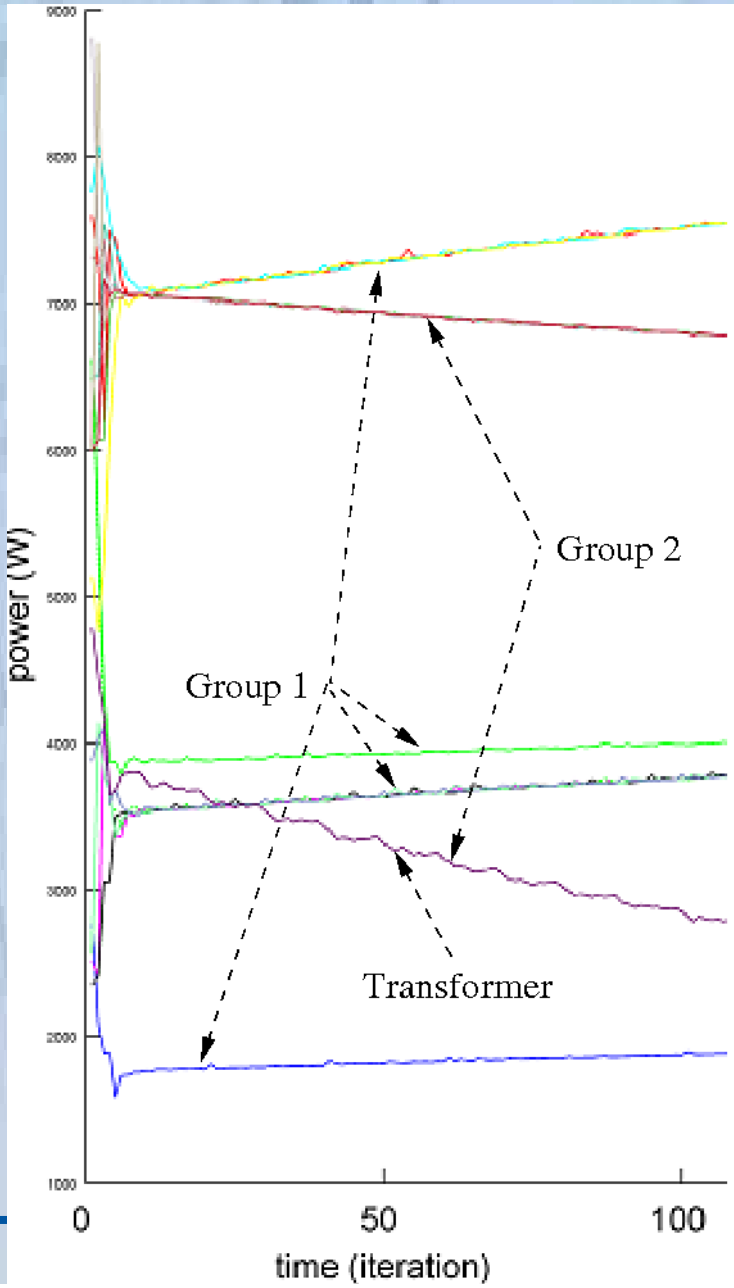
Overlay topology attack (1)

- overlay networks dynamically constructed
  - here: neighbour choice based on node description
- malicious node send wrong descriptions
  - other nodes choose it as a direct neighbour



Overlay topology attack (2)

- malicious node more powerful
  - e.g. network partitioning
    - disable 2nd-ary / 3rd-ary control
  - leads to non optimal behaviour

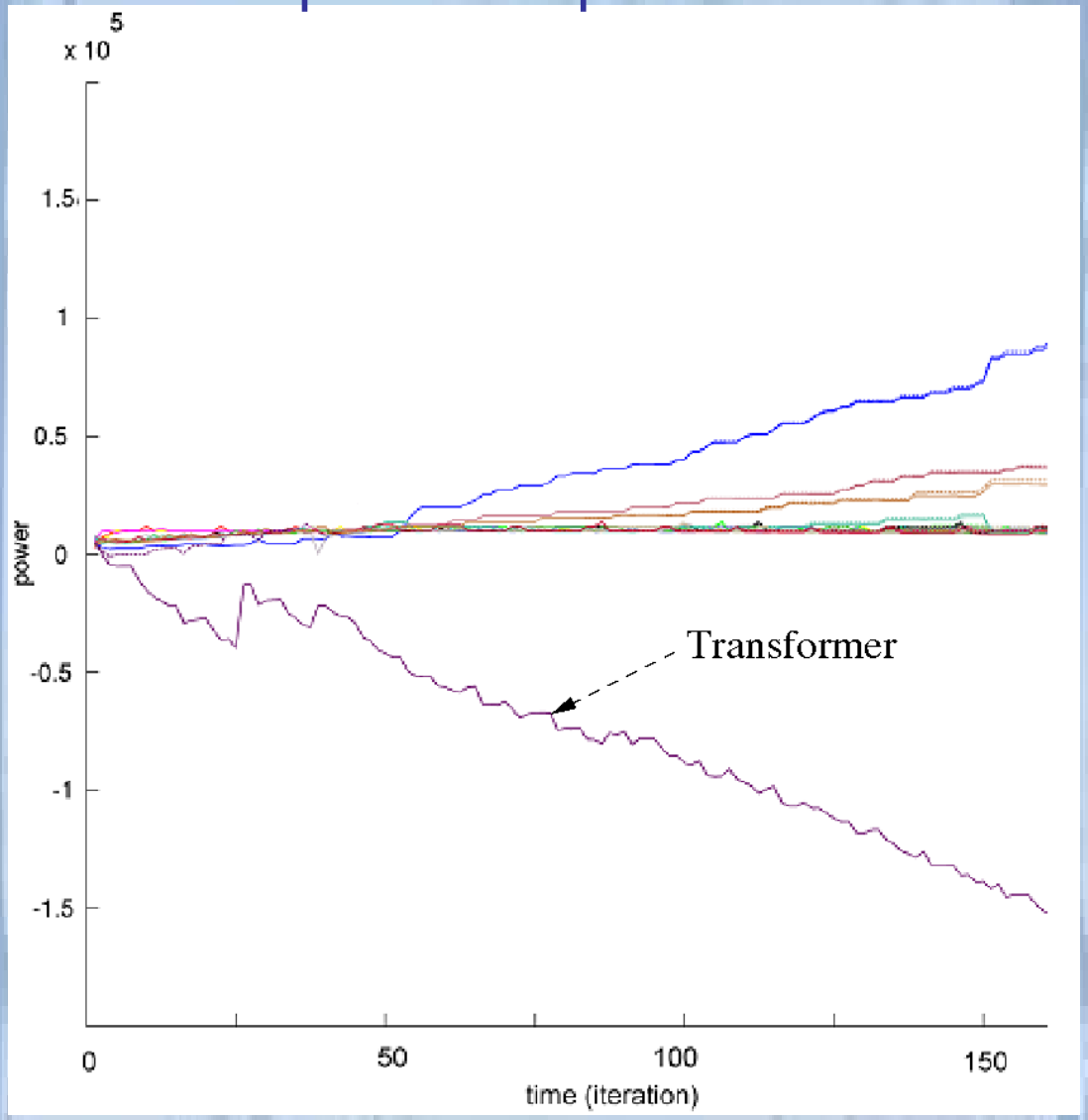


Secondary control attack (1)

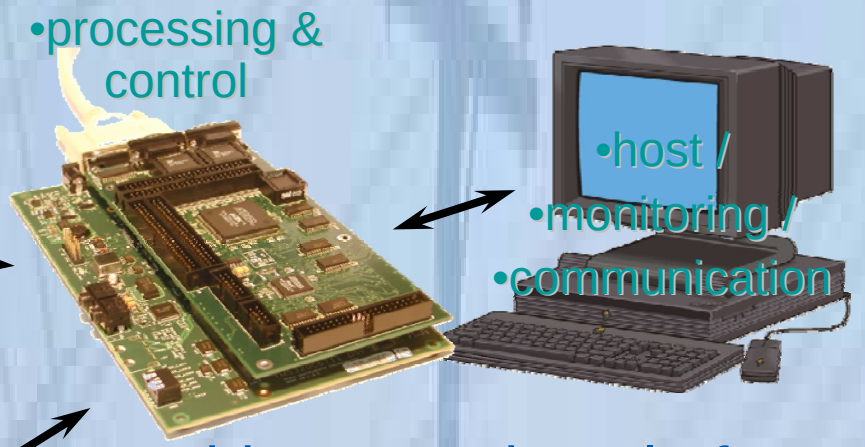
- secondary control
  = voltage profile management
- uses distributed averaging primitive
  - = averages system-wide divergence from optimal voltage level
- malicious node injecting false values
  - false values aggregate
  - leading to system wide power output increase

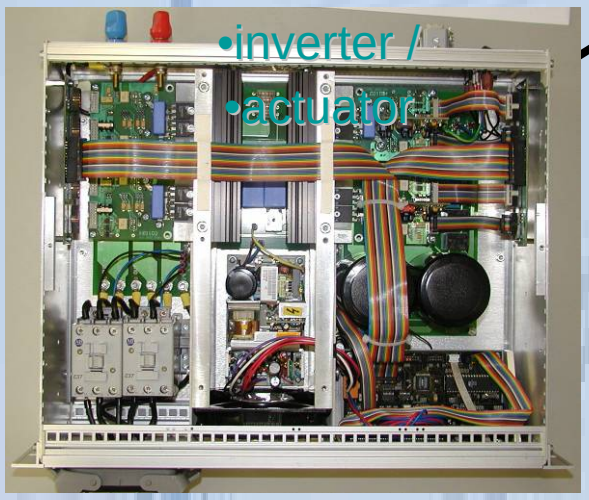
Secondary control attack (2)

DER increases active power output



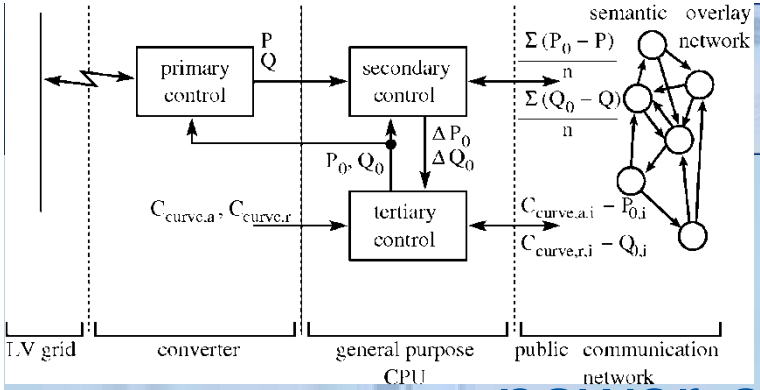
Rapid prototyping platform





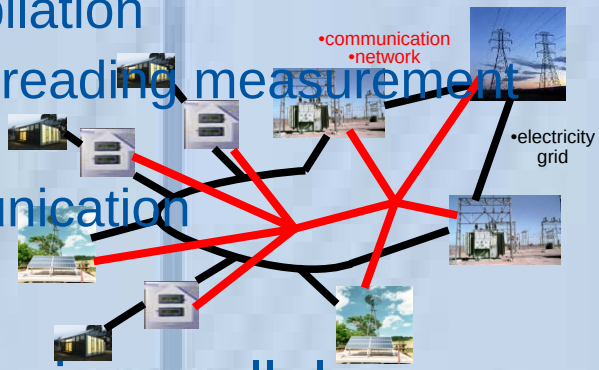
- modular rapid prototyping platform
  - reconfigurable
  - scalable
  - 1-4 phases
  - different types of power stages
- transparent programming
- fast protection
- EMC mitigation

TRIPHASE



Microgrid test set-up

- power-electronics, electrically connected
  - controlled via inverter-server
  - Matlab interface on user-PC
    - algorithm design and compilation
    - for setting parameters and reading measurement data
    - link to inter-inverter communication



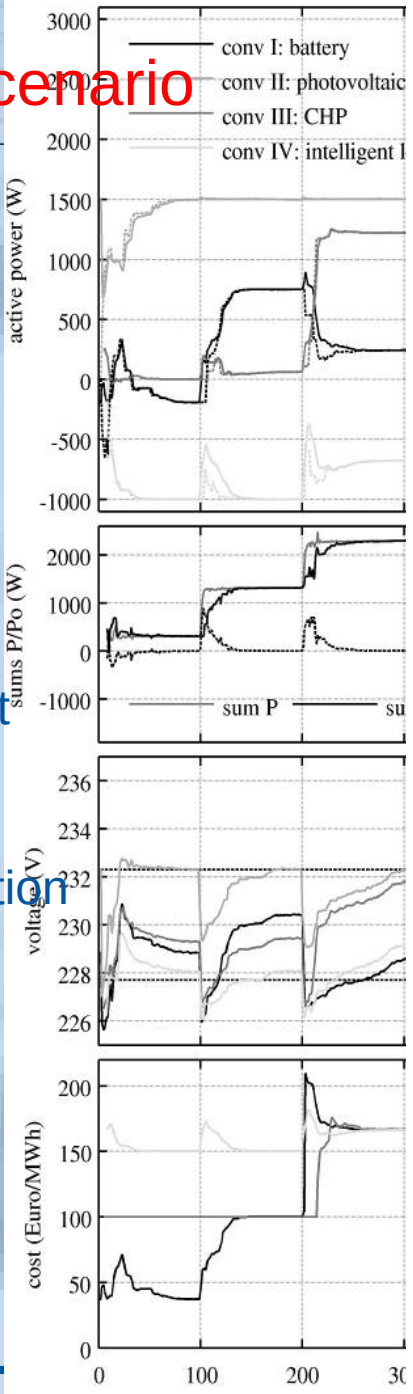
- microgrid algorithm
  - operating several inverters in parallel
  - primary control: no communication needed
  - secondary and tertiary control
    - via TCP/IP network
    - → link into Crutial building blocks

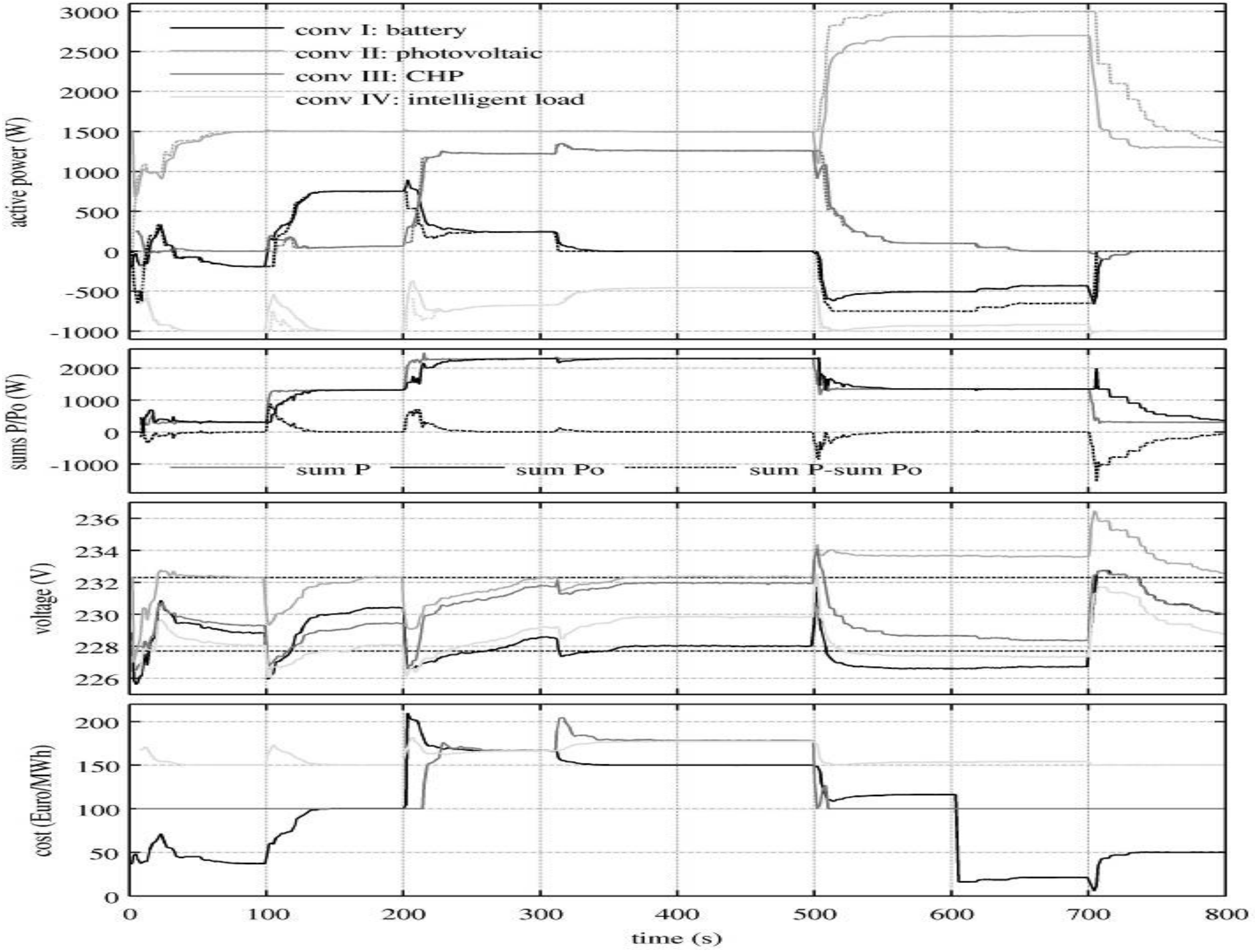
Microgrid control: experimental results

- primary + secondary + tertiary control
  - distributed, decentralised
- 4 IEDs, with specific cost functions
  - photovoltaic (PV) unit (0-3 kW)
  - coupled heat power (CHP) unit
  - battery
  - intelligent load
  - + dummy load → changing
- interconnected by an Agora overlay network
  - subject to a mix of load and supply variations

Microgrid control: reference control scenario

- t = 0 to 100 s: demand is very low
  - IEDs & primary control
    - battery nearly full, no CHP
    - PV unit provides few electricity (cloudy)
    - intelligent load is fully activated
  - small excess power is absorbed by battery
  - marginal cost is about 40 €/MWh
    - determined by most expensive activated unit (c.q. battery)
- at t = 100 s: load increases to 1.3 kW
  - **primary** control → battery @ full output & CHP @ partial output
  - **tertiary** control → equalises marginal costs @ 100 €/MWh
- from t = 200 to 300 s: load increases further to 2.3 kW
  - battery gets empty → marginal cost ↑ → battery lowers generation
  - CHP compensates by increasing output
  - and intelligent load reduces demand
  - marginal cost ↑ to 165 €/MWh
- at t = 300 s
  - battery empty → cost increase furthers → halts generation
  - CHP takes over partially & intelligent load further decreases demand
  - marginal cost increases further to about 167 €/MWh
- etc…




conv I: battery
conv II: photovoltaic
conv III: CHP
conv IV: intelligent load
active power (W)
sum P
sum Po
sum P-sum Po
sums P/Po (W)
voltage (V)
cost (Euro/MWh)
time (s)

Microgrid control: test plan

- scenario point-to-point communication
  - fault-free (*reference*)
  - influence of delayed packets
  - influence of lost packets
  - influence of DoS attack
- scenario overlay communication
  - fault-free (overhead of overlay)
    - for different overlay sizes / configurations
  - influence of lost packets
  - influence of DDoS attack
- integrate Crutial building blocks
  - re-assess

Conclusions

- Current developments
  - Testbed evaluation frameworks
  - Execution of attack experiments
  - Collection of data statistics from experiments
  - Evaluation of collected data
- Possible future developments
  - Integrate a power system simulator into the testbed
  - Develop other CRUTIAL scenarios involving GENCO
  - Integrate Macrogrid Teleoperation and Microgrid Control -> towards SmartGrids

CRUTIAL Testbeds: Deliverables

- D2 Analysis of new control applications
- D24 Testbeds deployment of representative control algorithms – Interim Report
- D9 Testbed deployment of representative control algorithms
- D14 Architectural patterns evaluated on the testbeds
- D17 On EPS-ICT interdependencies in the testbeds

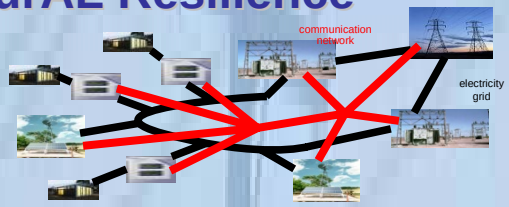
CESI RICERCA

- Home
- Workplan
  - WP1
    - Task 1.1
    - Task 1.2
    - Task 1.3
  - WP2
    - Task 2.1
    - Task 2.2
  - WP3
    - Task 3.1
    - Task 3.2
    - Task 3.3
  - WP4
    - Task 4.1
    - Task 4.2
    - Task 4.3
    - Task 4.4
  - WP5
    - Task 5.1
    - Task 5.2
    - Task 5.3
- Partners
- Events and News
- IAB Members
- Dissemination
  - Deliverables of the proje
  - Publications
- Related Projects
- Management
- Contact us

FP6-2004-IST-4-027513

http://crutial.cesiricerca.it

Critical Utility InfrastructurAL Resilience



CRUTIAL is a RTD Project in the area of **Critical Information Infrastructure Protection** launched by the European Union under the Information Society Technologies priority of the **Sixth Framework Programme**.

The project addresses new networked ICT systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet.

CRUTIAL's innovative approach resides in

modelling interdependent infrastructures

attempting at casting them into new architectural patterns

resilient to both **accidental failures** and **malicious attacks**

Objectives

- Investigation of **models** and architectures that cope with openness, heterogeneity and evolvability endured by electrical utilities infrastructures
- Analysis of **critical scenarios** which ICT faults provoke **serious impact** on the controlled electric power infrastructures
- Evaluation of **distributed architectures** enabling dependable control and management of the power grid

Work Packages

WP1 Identification and description of **Control System Scenarios**

WP2 Interdependencies modelling

WP3 Testbed development

WP4 Architectural **solutions**

WP5 Analysis and **evaluation** of Control System Scenarios

WP6 Dissemination

WP7 Management