



| | |
|---|---|
| **Project no.:** | **IST-FP6-STREP - 027513** |
| **Project full title:** | **Critical Utility InfrastructurAL Resilience** |
| **Project Acronym:** | **CRUTIAL** |
| **Start date of the project:** | **01/01/2006 Duration: 36 months** |

# Deliverable no.: D24

# Title of the deliverable: Testbeds deployment of representative control algorithms – Interim Report

**Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)**

| | |
|---|---|
| **Contractual Date of Delivery to the CEC:** | **31/12/2006** |
| **Actual Date of Delivery to the CEC:** | **17/01/2007** |
| **Organisation name of lead contractor for this deliverable:** | **K.U.Leuven** |
| **Author(s):** | **G.Deconinck[5] (Editor), G.Dondossola[1], F.Garrone[1], T.Rigole[5]** |
| **Participant(s):** | **[1]CESI, [5]KUL** |
| **Work package contributing to the deliverable:** | **WP3** |
| **Nature:** | **R** |
| **Dissemination level:** | **PU** |
| **Version:** | **005** |
| **Total number of pages:** | **23** |

**Abstract:**

**In CRUTIAL, the deployed testbeds are composed of two platforms. The first platform is based on power electronic converters that are controlled from PCs that are interconnected over an open communication network (at K.U.Leuven). The second platform consists of power station controllers on a real-time control network, interconnected to corporate and control centre networks (at CESI RICERCA).**

**This deliverable describes the testbeds in detail, as well as how they will be used in CRUTIAL. The workpackage has been running for 6 months, and this first phase has been used to prepare the testbeds for usage in the CRUTIAL project.**

**Keyword list: testbeds, combined electrical and ICT infrastructure**

## DOCUMENT HISTORY

| Date | Version | Status | Comments |
|---|---|---|---|
| 5 Dec 2006 | 001 | Int | Table of contents distributed (GD/TR) |
| 18 Dec 2006 | 002 | Int | KUL part integrated, new CRUTIAL template used (GD/TR) |
| 20 Dec 2006 | 002 | Int | CESI part integrated, comments |
| 20 Dec 2006 | 003 | Int | Complete draft for consortium discussion |
| 11 Jan 2007 | 004 | Int | Final draft, integrating comments |
| 15 Jan 2007 | 005 | App | Final version, approved by consortium |

# Table of Contents

# 1 INTRODUCTION

In CRUTIAL, the deployed testbeds are composed of two platforms. The first platform is based on power electronic converters that are controlled from PCs that are interconnected over an open communication network (at K.U.Leuven). The second platform consists of power station controllers on a real-time control network, interconnected to corporate and control centre networks (at CESI RICERCA).

Both testbeds integrate elements both from the *electrical* infrastructure as well as from the *information* (computing and communication) infrastructure, in order to focus on their interdependencies, and specifically on the vulnerabilities that occur in the electric power system when a part of the information infrastructure breaks down.

The two testbeds are complementary to each other:

- The CESI RICERCA-testbed focuses on the operation and supervision of a distribution grid (high and medium voltage levels) with classic (local and hierarchically distributed) control algorithms.
- The K.U.Leuven-testbed focuses on a distribution grid (low voltage levels) with innovative (local and decentralised, distributed) control algorithms.

The goal of CRUTIAL work package WP3 is to design and implement these two testbeds, both of which integrate the electric power system and the information and control infrastructure. In the project, these testbeds will be used to investigate

- local, hierarchical and distributed control scenarios at transmission and distribution level in order to better identify them (related to WP1);
- how architectural patterns can be integrated in a realistic setup (related to WP4);
- which interdependencies occur from a practical perspective (complementary to WP3).

The workpackage has been running for 6 months (M7-M12), and this first phase has been used to prepare the testbeds for usage in the CRUTIAL project. At M24, this will result in a deliverable (D9) describing the deployment of several representative control algorithms on these testbeds. This first deliverable (D24, called *interim report*) describes the ongoing developments of the testbeds. Several adaptations and extensions need to be performed to the preliminary versions of these testbeds in order to tailor them to the project requirements.

The deliverable is structured along two parts, describing the setup and foreseen usage of both testbeds, as well as their representativeness for their real-world equivalents.

## 1.1 Acronyms and terminology

| | |
|---|---|
| ac | alternating current |
| ACC | Area Control Centre |
| CC | Control Centre |
| COTS | Commercial Off-The-Shelf hardware or software component |
| dc | direct current |
| DER | Dispersed Energy Resource |
| DG | Dispersed Generation |
| DoS | Denial of Service |
| DSO | Distribution System Operator |
| DSP | Digital Signal Processor |
| EMS | Energy Management System |
| EPS | Electric Power System |
| FPGA | Field-Programmable Gate Array |
| FTP | File Transfer Protocol |
| GENCO | GENeration COmpany |

| | |
|---|---|
| HMI | Human-Machine Interface |
| HV | High Voltage |
| ICT | Information and Communication Technology |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IP | Internet Protocol |
| LAN | Local Area Network |
| LV | Low Voltage |
| MCD-TU | Monitoring Control and Defence Terminal Unit |
| MV | Medium Voltage |
| NIC | Network Interface Card |
| NTP | Network Time Protocol |
| OSI | Open System Interconnection |
| PDU | Protocol Data Unit |
| PI | Proportional-Integral |
| PMU | Phasor Measurement Unit |
| PS | Primary Substation |
| PSAS | Primary Substation Automation System |
| SAS | Substation Automation System |
| SCADA | Supervisory Control and Data Acquisition |
| TCP | Transmission Control Protocol |
| TMI | TeleMonitoring Interface |
| TSO | Transmission System Operator |
| TSP | Telecommunication Service Provider |
| UART | Universal Asynchronous Receiver Transmitter |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

In order to avoid confusion between terminology used differently in the electricity and computer science world, this document adopts two conventions.

- The term '*network'* is used in its telecommunication meaning (the communication net that transmits messages) and the term '*grid'* in its electricity meaning (the wire and cable net that transports electrical energy).
- The term '*dispersed generation'* is used in its electricity meaning of having electricity generation on multiple places spread in the electricity grid, while '*distributed'* is used in its ICT meaning as a being running on multiple, loosely coupled computer systems.

# 2 THE K.U.LEUVEN TESTBED

The number of Dispersed Energy Resources (DER) is constantly increasing. Main factors causing this shift from central electricity production to a decentralized generation are the availability of small-scale units which offer an increased flexibility in the liberalized energy market and the growing tendency towards sustainable development which favours energy efficient and low $CO_2$ emitting plants [Kueck & Kirby 2003], [Pepermans et al. 2005]. Whereas the first small-scale diesel generators served as back-up for local sites, a growing DER landscape could turn the high voltage transmission network into a backbone for local self-sustaining regions. This image remains an extreme case as several barriers in the integration of DER, market-related as well as technical, still have to be overcome. Regarding line losses, voltage profiles, reliability, etc… integrating DER units can bring benefit, as well as deteriorated grid performance.

In any case, the power grid is evolving from a centrally controlled grid with a only a handful of regulated monopolies to an open liberalized electricity market. As more and more small scale dispersed generators are being deployed in the distribution grid, this puts extra stress on the power grid in an era where electricity is one of the most important commodities for economical, industrial and everyday activities. Therefore new control strategies are being proposed to maintain the desired degree of dependability for electricity supply [Chandorkar et al. 1993], [Marwali et al. 2004], [Vanthournout et al 2005]. Many of these control algorithms are distributed over several computing nodes and rely on the ICT infrastructure for communication. Also, new services can be delivered by exploiting both infrastructures. For instance, external information, such as the instantaneous electricity price from real-time market places, can be incorporated into the control strategies in order to optimise economic control objectives; intelligent loads switch on or off in order to implement demand side management and avoid costly electricity peak costs; etc.

Dispersed electricity generation (often from renewable energy sources, such as photovoltaic and wind energy) is proliferating rapidly, with several sources claiming for 20% penetration of electricity generation from renewable resources in Europe by 2020 [EREC 2004a], and to 50% of the global energy world-wide generated from renewable by 2040 [EREC 2004b].

If sufficient generation (and storage) facilities are available in a part of the electrical grid, such part can become an energy island (or microgrid) which functions independently from the major grid (e.g. during a blackout or for economic reasons). However, in such islanding mode, control is different from non-islanding mode. Several technical issues need to be solved regarding protection and control (e.g. the selectivity of the protection needs to react on different threshold) by power engineers. However many of these solutions require an appropriate communication and control infrastructure that continues to function in both modi. Such ICT infrastructure and associated control algorithms are also required when re-synchronising the microgrid to the main grid after islanding (recovery).

If such dependable information infrastructure becomes available, autonomous, decentralised control systems provide a tremendous opportunity to improve monitoring and control operations, optimising the overall electric power system. This opportunity will become even more attractive as ever more intelligent electronic devices (IEDs) are being deployed, while new measurement devices, such as synchronous phasor measurement units (PMUs), gather data several times in each power cycle.

As control applications rely ever more on the ICT infrastructure, more and more electrical applications also follow the trend of deploying heterogeneous off-the-shelf information and communication technology for hardware, software and networking. This provides flexibility for the application, but also implies vulnerabilities as the electrical energy infrastructure depends on the correct functioning of the info'structure, in spite of random (physical) and malicious faults. In order to provide robust application behaviour for the energy application, this information infrastructure needs to be fault-tolerant and able to deal with a dynamic

environment; middleware can provide the required graceful degradation in case of unrecovered failures, rather than resulting in a complete breakdown.

## 2.1 Description of the testbed

The laboratory testbed at the K.U.Leuven is tailored to this context of dispersed generation, intelligent electrical devices, distributed and decentralised control, etc.

The testbed is built around power electronic converters. Such power electronic converter (or inverter) is a device which is able to switch electric currents, hereby allowing to transform the input current and voltage to a different output current and voltage (different in shape, amplitude, etc.) A typical application is to transform an input dc current into an ac output, or to change voltage levels of input to output signal. Also in practice, many types of dispersed electricity generation (e.g. wind turbines, photovoltaic cells) are connected to the grid through a converter, which makes the setup even more realistic.

Such a converter, integrated in a platform as described below, can emulate a dispersed energy resource, such as a small-scale electricity generator, a load (possibly voltage/frequency dependent), an energy storage devices (e.g. a battery, fuel cell) or any other IED.

Several of such power electronic converters can be combined to jointly feed an isolated microgrid. These are all attached to the electricity distribution grid (low and medium voltage grid), not to the transmission grid that is typically high voltage. Furthermore, other loads can be connected to this distribution grid, such as resistors to emulate simple loads.

In the laboratory setup all converters are fed by the same dc bus, and transformers are used at the ac side to isolate the converters. The converter belongs to a larger platform, which enables control algorithms to be executed on them. Such *Herakles* platform [Van den Keybus et al. 2004] composes of a *measurement module*, a *power electronic converter* and a *processing core* containing a Texas Instruments 'C6711 DSP (Digital Signal Processor) and an Altera EP1K100 FPGA (Field-Programmable Gate Array), as displayed in Figure 1. The DSP is embedded in a 'C6711 DSP Starter Kit development board, on which a self-made daughter-card is mounted, which contains the FPGA and, amongst others, two high-speed RS-232 serial ports. The DSP runs the real-time operating system DSP/BIOS and can be programmed both in C or from Matlab/Simulink. Also runtime supervision and control of the DSP is possible from Matlab/Simulink. The FPGA handles the interconnection between DSP and hardware modules, i.e., the converter containing four half bridge output stages and the LV distribution grid voltage and current measurement module. The combined converter, measurement module, FPGA and DSP platform can implement local control algorithms and represent the front-end of DER units or other intelligent equipment.

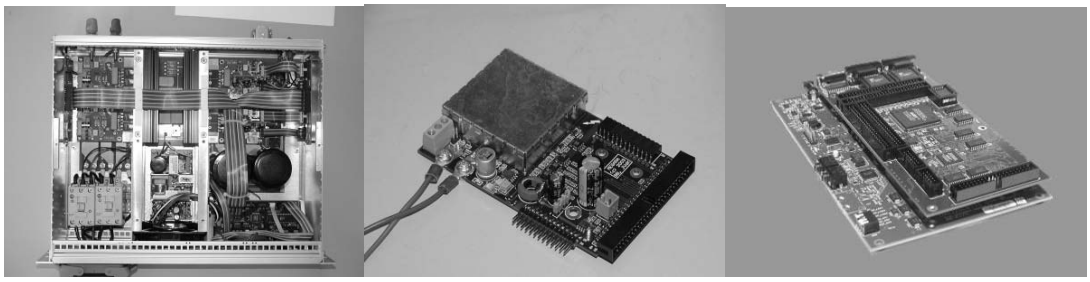

**Figure 1: (left) converter. (middle) voltage and current measurement module. (right) processing core development board with a daughter-card containing the FPGA.**

Attached to this platform, via the standard UART (universal asynchronous receiver/transmitter) serial link is a standard PC running Linux. This PC can be connected to a local area network (LAN) via an Ethernet connection. The LAN is used as a communication channel between the Herakles platforms.

This configuration is schematically shown in Figure 2, and a picture of this testbed is shown in Figure 3.

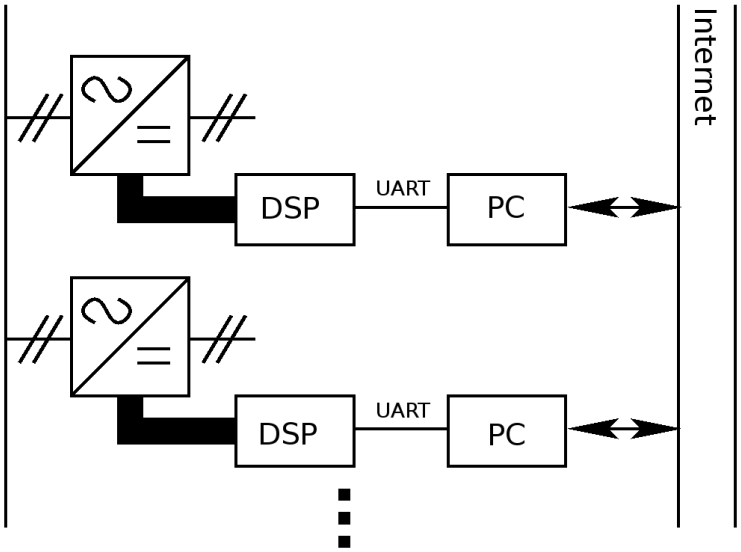


**Figure 2: Schematic overview of the testbed to emulate a LV distribution grid with high DG penetration.**

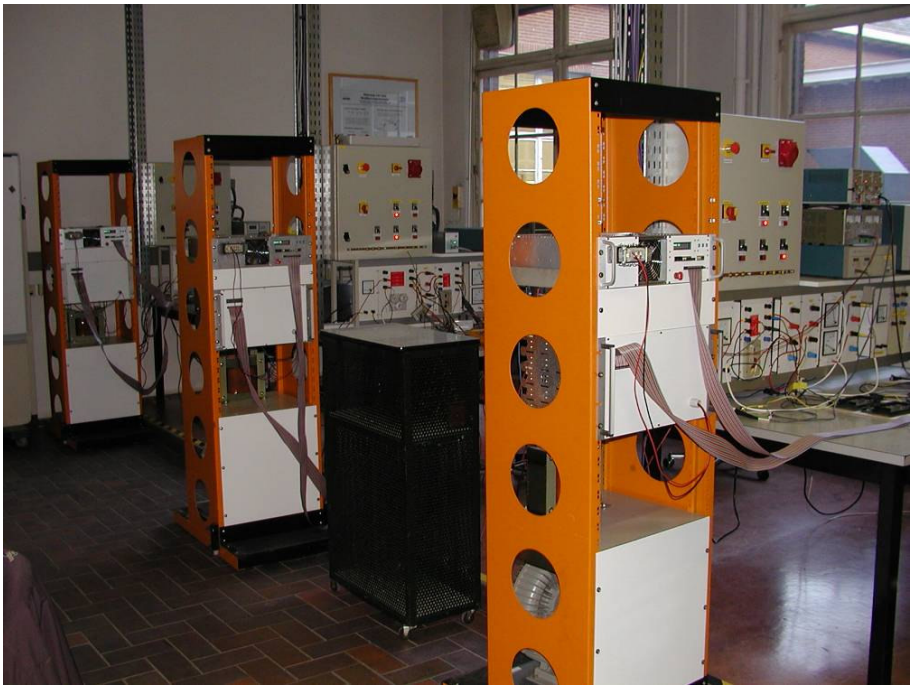

**Figure 3: The laboratory setup showing 3 towers, each with a converter.**

The Herakles platform allows different control ideas (voltage/frequency/current control, power quality control, etc.) to be modelled in a high level programming tool such as Matlab, after which it can be swiftly prototyped on a 4-quadrant power electronic converter (i.e. it can be used as generator or as a load). As these Herakles platforms are connected to PCs, they can be interconnected via TCP/IP modules in order to extend the control scope from local towards distributed (hierarchical and decentralised) control algorithms. By deploying the converters on top of standard ICT infrastructure, they become representative for the context of DER and IEDs described above.

## 2.2 Related testbed usage in other projects

This Herakles platform as described above has been used – in a *stand alone* version without the LAN - in several *power engineering* research projects. Examples include power quality measurements [Gherasim et al. 2004] [Gherasim et al. 2006], for power line communication [Van den Keybus et al. 2002], for control of a switched reluctance motor [D'hulster et al. 2004], for sensorless motor control [Dragu & Belmans 2002], for a kart design [Van den Keybus & Deconinck 2004], for local droop control [De Brabandere et al. 2004], for protection applications [Van den Keybus et al. 2005], etc.

Before the CRUTIAL project, the Herakles platform has only been used in two proof-of-concept applications in which *communication* among the converters played a role.

As a first case study, this approach has been used to interconnect two converters and to use their information to control a*ctive filters* in order to mitigate power quality problems. Both converters measure voltage and current locally, exchange data, and calculate new converter settings, based on a control algorithm [Macken et al. 2004]. This setup was used in a power engineering context to validate that converters connecting windmills to the grid can be used for power quality enhancement. Indeed, the active power production for some sources of renewable energy (e.g. windmills) is rarely at its maximum and, consequently, a considerable amount of non-active power is available for power quality unbalance compensation during such periods. Therefore, power quality parameters are measured on two positions in the electrical grid, and forwarded to each other over the information infrastructure to the other converters, which can react properly to mitigate the power quality problems.

As a second case study, distributed control in a micro-grid has been evaluated. Besides the electrical connection between all generators, load and storage unit in a grid segment, these elements are also connected via the above-mentioned info'structure, based on the self-organizing semantic peer-to-peer network Agora [Vanthournout et al 2005]. At start-up, all entities broadcast some identification information (type, static and dynamic information) which results in the setup of peer-to-peer network. On top of this communication overlay network control applications are run. Primary control is realized by means of an enhanced droop control [De Brabandere et al. 2004], which requires no communication, thus guaranteeing a stable system, even when all communication fails. Secondary and tertiary control are performed by exploiting the peer-to-peer network on top of the LAN. Secondary control consists of an innovative gossiping-based distributed PI-controller, which keeps voltage and frequency into the correct range [Vanthournout 2006]. The economic optimization or tertiary control is based on a variation of the averaging gossiping algorithm, using local generation cost-curves at each generator to re-dispatch the generated power, such that all operate at the same marginal cost. The practical validation of this microgrid with overlay networks on the testbed took place with four Herakles platforms.

Up to now, the Herakles platforms have been a useful proof-of-concept for rapid prototyping of local control algorithms for power engineering applications, and have begun to show their potential for use in distributed control approaches. However, as the platform is becoming outdated (the TI 'C67 DSP has been on the market since more than 5 years and is not being offered any more; the programming environment based on DSP/BIOS is rather unstable, etc.), only 1 functional platform is left, that is soon to be abandoned. A new version of the platform, based on an embedded single board computer (SBC) is close to being finalised. This industrial PC will replace the DSP to run the local control algorithm. This industrial PC will also be the starting point for interconnecting the new platforms in a distributed setup.

## 2.3 Testbed requirements for CRUTIAL and required adaptations

During the CRUTIAL project, this new K.U.Leuven platform will be further developed to be able to execute different hierarchical and distributed control algorithms, and to analyse the effects of a failing information infrastructure on these electrical control applications.

As such, it will be used to evaluate the aspects of interdependencies between the information infrastructure and the electric power system, and to identify the robustness of the control algorithms to disturbances, and to provide feedback to the modelling and architectural parts based on the experiments.

For this, work is required on the hardware and software of the platform, as well as on the middleware modules to interconnect them into a network – as such creating an information infrastructure.

### 2.3.1 Modifications to electrical subsystem and control algorithms

The testbed currently operates only in isolated mode; it is not connected to an external grid through a feeder transformer as is usually the case in distribution grids. Although isolated mode is –for what stability and power balances are concerned- the hardest mode to operate the microgrid in, grid connected mode should be tested too. Especially voltage control and economical control may become more of a challenge in this case.

Also, the testbed is a single phase system, which may be applicable to some kind of DG (e.g. photovoltaic panels) and loads (many households have a single phase connection to the power grid), but it is nevertheless a simplification of a real distribution grid. Next to putting additional hardware in the system, the droop control (or primary control) scheme and the agent logic for the secondary and tertiary control could be optimized to deal with the complexity of three phases and a neutral connector.

Also, the electrical subsystem could be extended to allow more DG units (converters) and loads (resistors banks, electrical drives, etc.) into the system. The larger the system, the more accurate a real distribution segment can be simulated.

Several electrical control algorithms will be integrated onto this platform. They can be categorized into *local* control algorithms that do not require any communication, and *distributed* control algorithms which build upon communication among platforms. The latter can be further split among hierarchical (with a single or hierarchical decision structure) or decentralised algorithms (without a single decision point). Any of these categories can have algorithms with and without real-time constraints.

As such, there are six possible categories of control algorithms that need to be supported. The following enumeration provides some examples:

- Local control – non real-time: data aggregation, logging, etc.
- Local control – real-time: droop control, primary control, etc.
- Distributed control – hierarchical – non real-time: system monitoring, demand side management (intelligent switching on and off of loads), peak shaving (avoiding peaks in electricity usage), secondary control, tertiary control (optimisation for economic, ecologic criteria), power quality analysis, market & trading applications, etc.
- Distributed control – hierarchical – real-time: load shedding (if generated power < demand), resynchronisation after islanding, power quality mitigation, etc.
- Distributed control – decentralised – non real-time: system monitoring, demand side management (intelligent switching on and off of loads), peak shaving (avoiding peaks in electricity usage), secondary control, tertiary control (optimisation for economic, ecologic criteria), power quality analysis, market & trading applications, etc.
- Distributed control – decentralised – real-time: load shedding (if generated power < demand), resynchronisation after islanding, power quality mitigation, etc.

### 2.3.2 Modifications to ICT subsystem

The platform needs to integrate the communication infrastructure with the electrical converter, in order to allow implementation of the above-mentioned distributed control algorithms, or to extend the local control algorithms with monitoring and supervision. The first required extension is extensive monitoring and supervision capabilities.

For the decentralised and hierarchical control algorithms, the necessary approaches need to be developed and integrated (communication protocols, agent logic, overlay networks, …).

Furthermore, the ICT-system needs to be updated in order to allow fault injection into the system. This could comprise adding network delays by routing through a router which adds random delays or drops packets to simulate an Internet-like environment, a changing topology, etc.

Also, the ICT-system needs to investigate malicious behaviour, simulating Denial-of-Service attacks, malicious agent behaviour, and so on. This is important to assess impact of certain types of attacks which are hard to simulate on a computer or to validate computer simulations of the system.

In a later phase, developed middleware from WP4 will be implemented on this ICT system, and previous fault and attack scenarios can be tested to see how resilient the system is as a result of its enhanced fault and intrusion tolerant system.

## 2.4 Supporting simulation environment

In order not to be bound by power engineering hardware problems, a dedicated simulation environment is being set up. The algorithm used to simulate the behaviour of the microgrid with distributed control, simulates both the electrical and ICT level of the application.

Since DER is typically working in a radial segment in the distribution grid, power flow calculations on are relatively simple when the system is connected to the transmission level; the voltage at the feeder transformer is kept constant by the external grid, and voltage drops over the distribution segment are proportional to currents flowing from the transformer. Primary control will, when the system is grid connected, only control active power output based on local voltage levels, since frequency is kept stable by the external grid. This again simplifies the simulations.

The agent behaviour (secondary and tertiary control loop), the IP-network and the 'virtual' overlay network are simulated too. For these simulations we assume that communication delays and gossiping intervals are a few orders of magnitude larger than the time needed for settlement of the primary control loop (proportional controller and power). This means that power flow calculations and the primary control action are calculated first until convergence is observed. Only then generators gossip, and adjust their parameters for the primary control loop according to the results of secondary and tertiary control loop. When all generators have finished gossiping, new power flow calculations are done until convergence, and so on. The total number of time steps of the simulations is chosen in advance, and some script is applied during each of these discrete time steps, which can be a load increase or some failure in the system.

```
for(i=0; i<nb_of_iterations; i++){
      applyScript(i);
      for(each agent A){
            A.gossip();
            A.adjustPQ();
      }
      while(no convergence){
```

Apply script, e.g. fault injection

Gossiping:
secondary and tertiary control loop

```
            doPowerFlow();
            for(each agent A){
                  A.applyDroopControl();
            }
      }
}
```

Powerflow calculations and primary control until convergence

## 2.5 Example usage of testbed for control scenarios

The K.U.Leuven-testbed will be used to integrate, in order of increasing complexity, a local control algorithm (e.g. voltage droop control) without and with monitoring facilities, a centralised control algorithm (e.g. dispatching) without and with strict deadlines, a distributed, hierarchical control algorithm (e.g. power quality control by active filters) as well as a distributed, decentralised control algorithm (e.g. tertiary control).

It will allow assessing the assumptions and approaches of the developments for their compatibility with realistic scenarios of dispersed electricity generation and intelligent electronic devices. As such it provides the perspective of the electrical control applications onto the ICT-based infrastructure that is assumed to be more robust and resilient against random and malicious faults.

As such, these testbeds complement the modelling activities. They will provide them with ideas about how electric power systems and information infrastructures depend on each other, from a control and application perspective. Besides, they will verify if dependencies that became eminent from the modelling activities are also appearing in the realistic testbeds. Feedback from the experiments carried out on the testbeds will be used to enrich and refine the modelling activities.

# 3 THE CESI RICERCA TESTBED

## 3.1 Description of the testbed

As evidenced in WP1, today's Electric Power Systems (EPSs) rely on the concepts of remote supervision and control, interconnection of power structures and online power system monitoring.

Communication networks are extensively used by technically advanced power utilities to support both real-time and non real-time information exchange with obvious benefits, thus assuming a major role in power system management.

Due to the intensive use of information and communication systems, which are exposed to a vast amount of accidental and intentional cyber threats, cyber security has become a relevant issue for utilities managing critical infrastructures.

The testbed which is being designed by CESI RICERCA, implements a prototypal but significant power system management architecture with its integrated ICT infrastructure. Focus shall be placed on the development of those aspects of the actual EPS which can be used for the implementation of a subset of the attack scenarios described in WP1, deliverable D2, chapter 5, in order to evaluate their feasibility and plausibility, to demonstrate the possible evolution of the attack process and to assess the severity of the potential damage on the attack's target.

The testbed shall be used to:

- identify the critical aspects of the interdependency between EPS and ICT systems
- highlight the ICT system's vulnerability to potential cyber attacks, and
- evaluate the resilience of possible architectures/mechanisms/solutions to cyber threats.

### 3.1.1 Reference architecture

Essential parts of the power grid control system are the substation control systems and the communication network implementing the information exchange between the different actors (TSOs, DSOs, GENCOs, power exchange, energy authority, etc.) involved in the electrical system's management.

There are basically two kinds of communication over the communication network:

- Real-time communication between grid control centres ((supervisory control and data acquisition (SCADA) systems and energy management systems (EMS)) and substation control systems;
- Non real-time communications directed to back-office departments for the transmission of data (e.g. statistics, trends, condition related data) to be used for protection engineering, maintenance, planning and asset management, etc.

Consequently, the communication system itself consists of a set of interconnected network segments each with their own performance requirements, with extensive use of public networks.

Both DSOs and TSOs rely, for instance, on maintenance services from external providers, who mostly use public communication networks, to receive up-to-date status information about the equipment to be maintained.

A centralised control centre provides monitoring and management functions for the whole ICT infrastructure (communication networks, Intelligent Electronic Devices (IED), etc.).

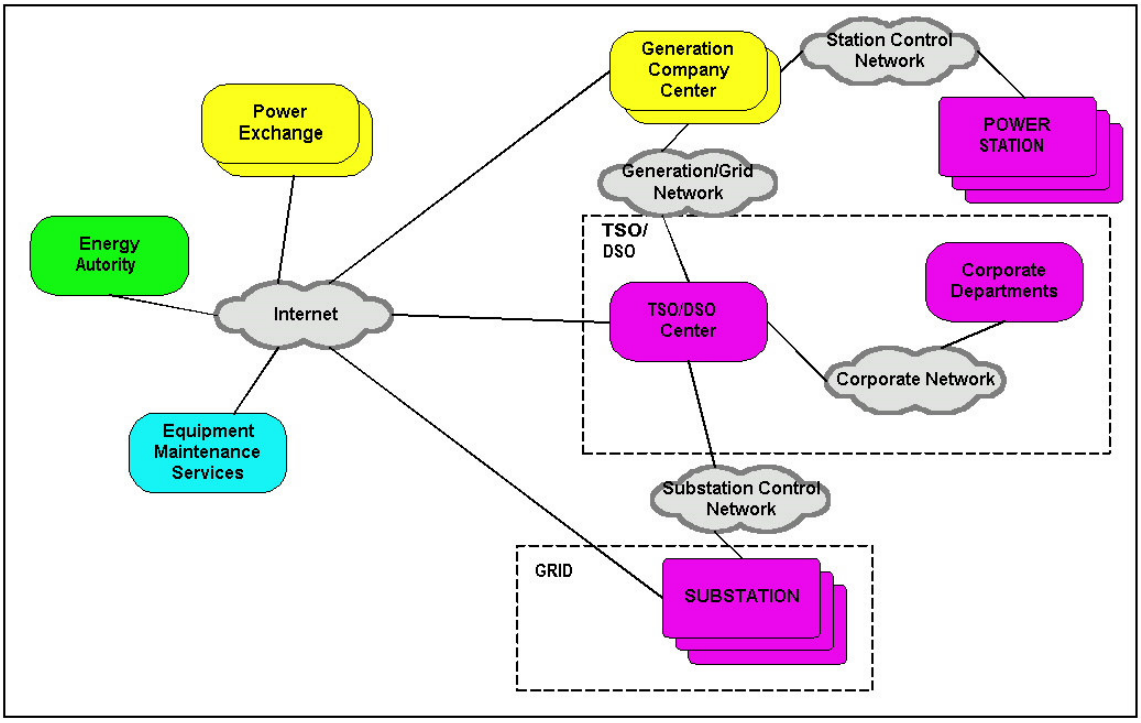


**Figure 4: Overview of the information flow in the power grid management system.**

Figure 4 offers a rough overview of the information exchange in the power grid management system.

As a reference architecture for the CESI RICERCA testbed, the distribution power grid has been chosen, together with some of its interconnections with external subsystems (essentially the transmission power grid.)

Figure 5 exemplifies the architecture of the reference DSO centre and some of its interactions. The architecture of the distribution power grid has been described in WP1.

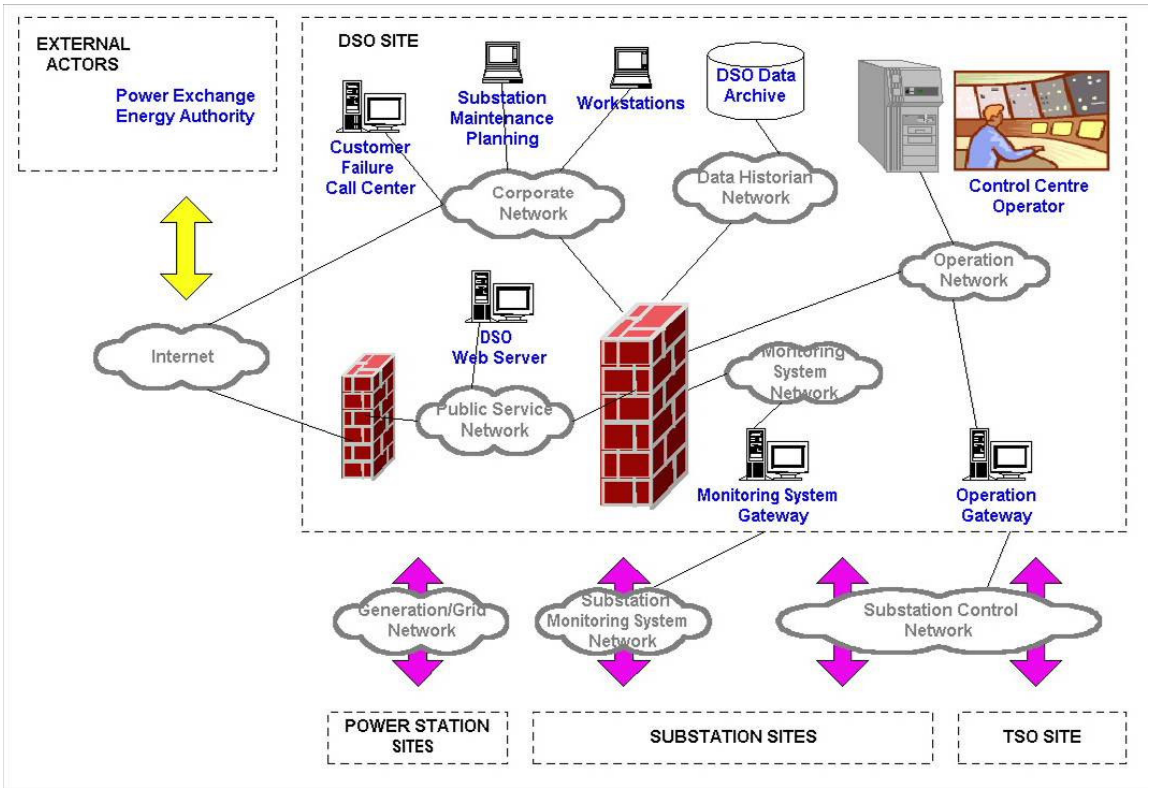


**Figure 5: Example of distribution power grid section.**

### 3.1.2 Reference communication scheme

Figure 6 summarises the information flow among primary substations and control centres of a power grid section. As cyber attacks may exploit the vulnerabilities of the standard application layer protocols, the figure associates to each connection the generally used transport and application level communication protocols.

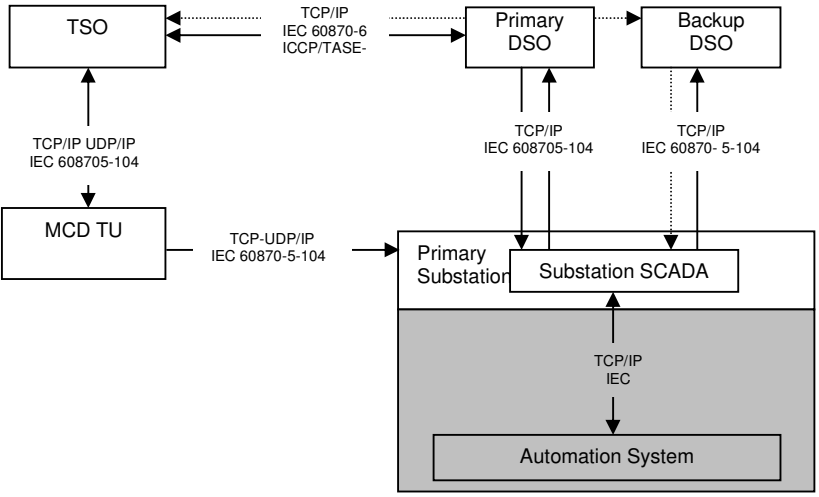


**Figure 6: Information flow and communication protocols.**

The following assumptions apply to inter-site communications:

- At the application level, communications among control centres comply with the standard [IEC 60870-6] Inter-Control Centre Protocol (ICCP/TASE-2), while centre-to-substation communications are based on the [IEC 60870-5-104] standard.
- Both high level protocols are IP-based and they mostly rely on a connection-oriented transport layer (TASE-2 uses MMS [MMS]), although UDP/IP may also used for multicast datagram transmission.
- The datalink level consists of standard telecom IP backbones (owned by independent telecommunication service providers), with redundant communication paths, implemented over physically independent carrier lines, granting the system's availability requirements in case of accidental failures of ICT components.

Although the testbed has been modelled on a section of the distribution power grid, as mentioned in the previous paragraph, many aspects of the communication scheme apply generically to the whole EPS.

TASE-2 is the application protocol commonly used for communication between any two control centres of the power grid and similarly IEC 60870-5 is the standard adopted for communications between control centre and substation both in the transmission and the distribution grid.

[IEC 61850] is the standard specifying communication networks and systems in generic electrical substations.

### 3.1.3 Laboratory architecture: ongoing development

The CESI RICERCA testbed's architecture shall be a strongly simplified version of the reference power grid architecture on which it is being modelled. As the main purpose of the laboratory testbed consist in the evaluation of the cyber security issues related to the power grid infrastructure, the prototype shall be designed according to the following guidelines:

- all those components of the reference architecture which can be involved in the cyber attack scenarios to be demonstrated shall be modelled as faithfully as possible
- the implementation of the other components shall instrumental to the demonstration i.e. shall be a simplified representation of the actual control system component.

Figure 7 gives an overview of the proposed CESI RICERCA prototype architecture.

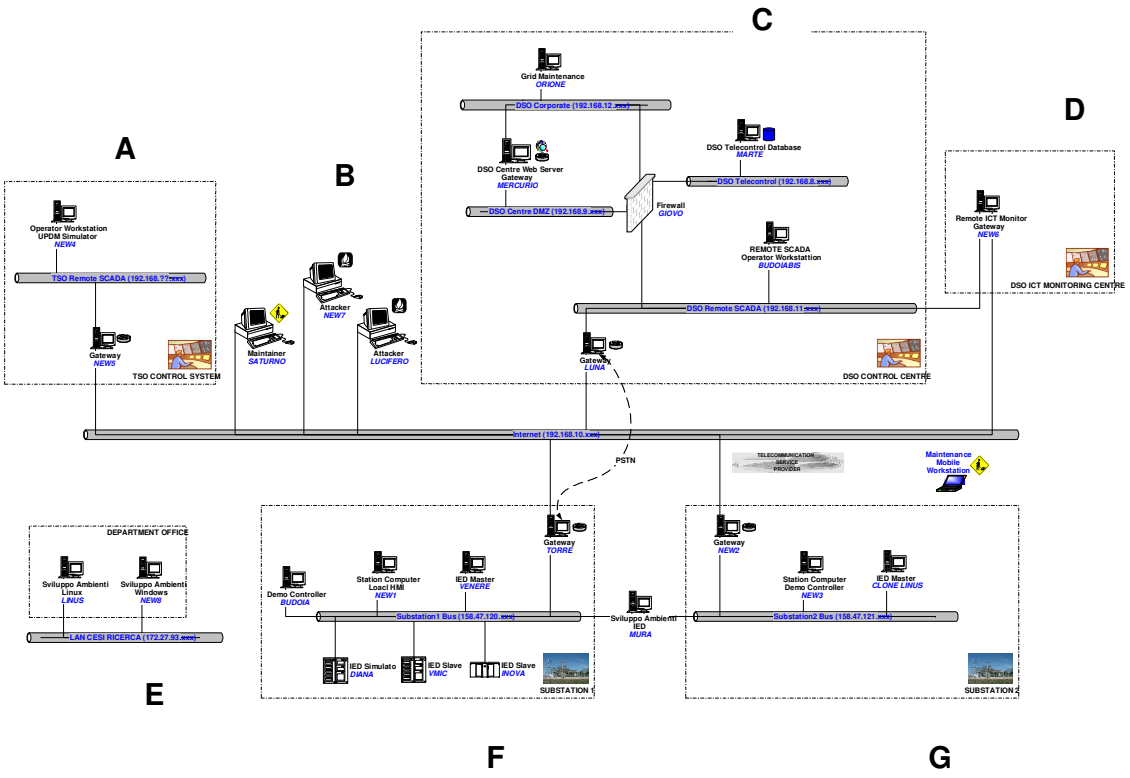


**Figure 7: CESI RICERCA testbed architecture.**

The areas of the figure represent:

A. an MCD-TU to the transmission control system

B. maintenance nodes and hacker machines

C. a DSO control centre

D. the ICT system's supervision centre

E. development machines

F. Primary Substation number 1

G. Primary Substation number2

Due to the complexity of the reference architecture, even a strongly simplified model requires the use of a good number of nodes. At this stage, effort has been mainly directed to model the subsystems involved in real-time communications, typically the SCADA system of the DSO control centre (see **Figure 8**), the primary substations and, of course, a possible communication system.

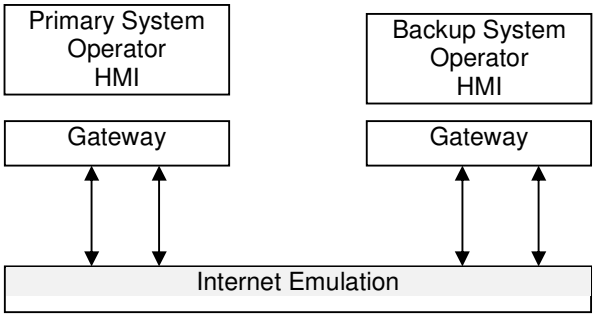


**Figure 8: DSO centre section.**

Where possible, functions have been attributed to elaboration nodes in order to estimate the amount of laboratory equipment needed to implement the prototype.

As evidenced in **Figure 7** the testbed includes two primary substations. Since the objective of the type of attack scenarios being analysed is not the switchgear but the controlling equipment and its communication links, we assume that the two substations have the same (totally simulated) primary equipment which is controlled by two different secondary subsystems.

The two substations in the prototype are supposed to be operated by the remote control centre but can be accessed also by means of a local station HMI which can be possibly used for local operations. This feature is significant in the demonstration of those attack scenarios which cause the remote centre to get a wrong perception of the status information provided by the substation.

The first substation (see **Figure 7**) has a fully distributed architecture which can be used for the demonstration of issues related to the inside aspects of substation automation; the second substation has a minimal architecture to be used for those scenarios affecting multiple control sites.

The same set of local automation functions shall be performed on both substations. Besides the fundamental tasks of (simulated) data acquisition and command execution, we are implementing some higher level automation sequences typically performed by substation automation systems. The set of functions is far from being exhaustive: the tasks have been selected because their performance can be drastically perturbed by malicious interference and their execution has a perceptible impact on the evolution of the process.

The application includes local load shedding functions, automatic power transfer for uninterrupted power supply, parallel transformer operation, control system reconfiguration, maintenance required component exclusion/inclusion functions, etc.

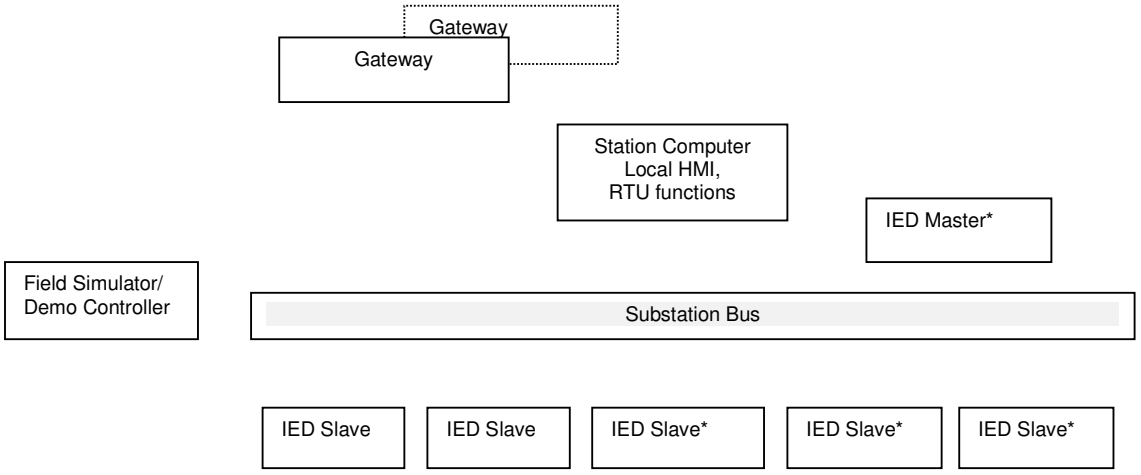


**Figure 9: Architecture of primary substation number 1.**

As illustrated in Figure 9, in the first substation the automation application is distributed over a set of IEDs. Only some of these shall be actual industrial PCs: the other target nodes shall be simulated on one ore more Linux Hosts.

The role of the second substation in the CRUTIAL demonstrator consists in evidencing the interdependencies among substations controlled by the same remote centre and the effects of attack scenarios on multiple control sites. Therefore the structure of this second substation, as shown in **Figure 10**, shall be strongly simplified, comprehending just the most essential subset of nodes.

The automation system consists of two IEDs, a master and a slave, both simulated on the same Linux host, with no backup configuration.

A station computer hosts both the high level substation functions (local HMI, Protocol conversion functions) and the Field Simulation/Demonstration Control functions.

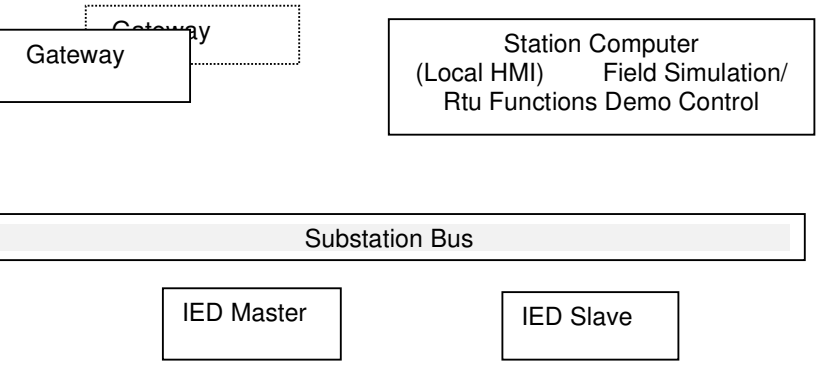


**Figure 10: Architecture of primary substation number 2.**

### 3.1.3.1 Communication scheme of the demonstrator

Figure 11 outlines the communication infrastructure connecting a substation to the external world in the demonstrator.

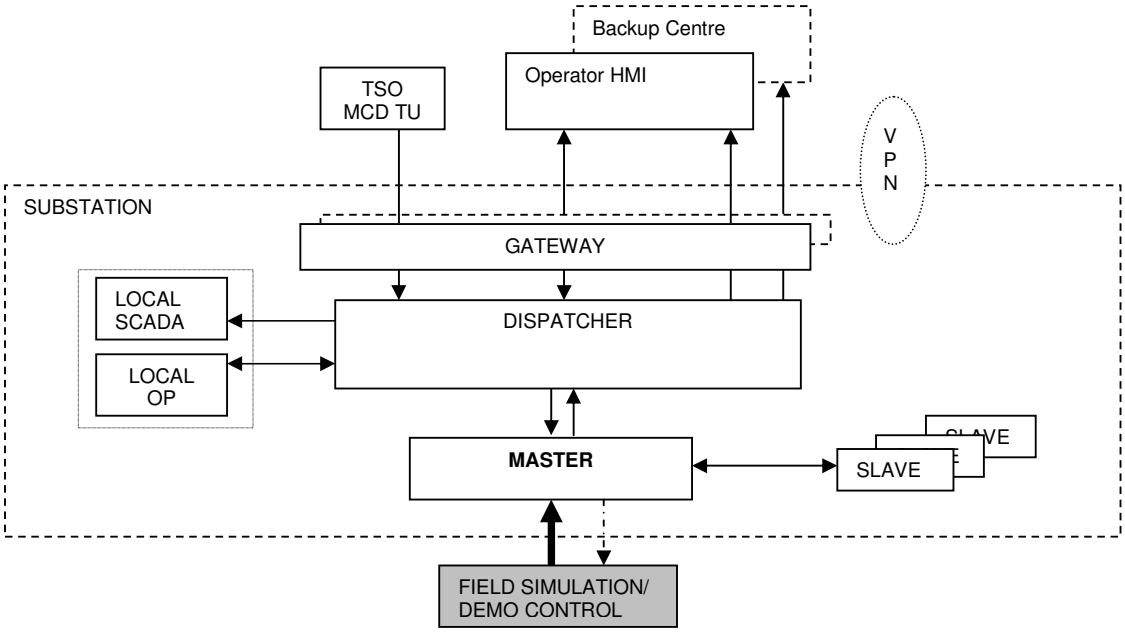


**Figure 11: Communication scheme of the demonstrator.**

The grey box in Figure 11 is the application dedicated to the simulation of the process and the control of the demonstration. The arrows show the direction of the information flow.

The communication architecture is based on the reference communication scheme of Figure 6 but it is being designed according to the same criteria followed in modelling the automation sites: all those aspects which are not considered significant with respect to the proposed attack scenarios shall be strongly simplified. It becomes imperative considering:

- the large number of elaboration nodes versus the normally available laboratory space,
- the consequent necessity of using virtual target nodes allocated to the same host system,

- the cost and complexity of installing the standardised commercially available protocol stacks, reported by the reference architecture, on test/demonstration equipment.

At this very preliminary phase of the testbed development the assumptions are the following:

- the two lower layers of the OSI stack (physical and datalink) are modelled by switched Ethernet, both for local and wide area communications,
- TCP/IP and UDP/IP shall be used at the transport layer,
- application layer data exchange shall not make use of commercial protocols, but the contents of the application PDUs shall be compliant with the appropriate standard.

## 3.2 Related testbed usage in other projects and adaptation to CRUTIAL

The CESI RICERCA testbed has been derived from the demonstrator implemented for the European project DepAuDE (Dependability for embedded Automation systems in Dynamic Environment) [Depaude 2003] and further developed for the subproject RETE21/SITAR of the Italian RdS Program (www.ricercadisistema.it).

While the DepAuDE project had its focus on the resilience of automation systems to accidental faults, the SITAR project was mainly interested in intentional, malicious cyber threats to critical infrastructures.

The CRUTIAL testbed inherits some architectural aspects of DepAuDE demonstrator and some of the attack scenarios experimented in SITAR [Dondossola et al. 2006].

### 3.2.1 The DepAuDE demonstrator

As shown in Figure 12 the DepAuDE testbed infrastructure consisted of two interconnected automation sites: the local site hosting a primary substation with its automation system and a remote Control Centre hosting a Graphical User Interface.

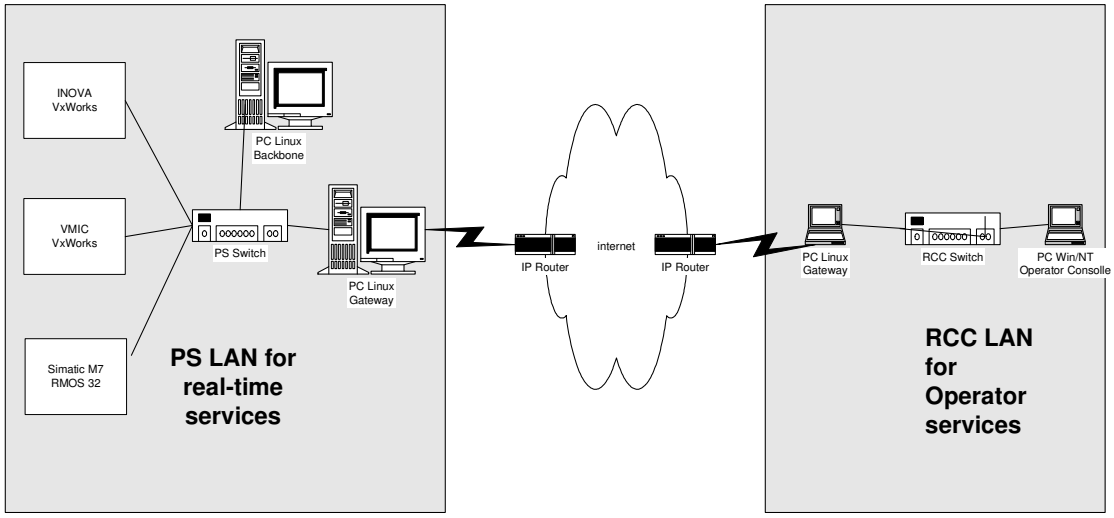


**Figure 12: DepAuDE testbed overview.**

The local site consisted of three dedicated heterogeneous (“target”) processors running a pilot automation application and two standard PCs for support functions interconnected by an Ethernet switch.

The remote site (Remote Control Centre) consisted of two PCs interconnected by an Ethernet switch: one hosting a Gateway and one with Operator Console functions.

Communication between the two sites was supported by an internet connection.

There was no primary equipment and process data exchange with the field was simulated.

The pilot application implemented two automation functions.

The demonstrator included a stand-alone application providing a state-of-the-art graphical interface through which the user/operator could control the evolution of the demonstrator, visualize and eventually change the status of some of the components involved in the application and, at the same time, display low-level information in a controlled way.

### 3.2.2 Testbed extensions and adaptations

The CRUTIAL testbed inherits the essential aspects of the architecture of the DepAuDE demonstrator's primary substation and some features of the communications between the substation and a remote control centre.

The architecture of the more complex primary substation has been designed according to the same guidelines as the DepAuDE substation, just increasing the number of automation nodes.

The pilot application has been extended adding new functions to those already implemented for the previous demonstrator.

Both the primary equipment and the field I/O are again simulated but for the new testbed a dedicated module has been designed to handle field simulation and to implement the test and demonstration related activities.

Since these modules are simply instrumental to the demonstration and have no equivalent in a real substation and therefore cannot be involved in any scenarios, they have been intentionally distinguished from the other components of the prototype.

The objectives of the DepAuDE testbed did not require a realistic implementation of a remote control centre: only the interactions functional to dependability related issues had been modelled. In the CRUTIAL architecture interactions between substations and the outside world play a major role therefore the new human machine interfaces bear just a vague resemblance to those implemented in the old testbed.

## 3.3 Example usage of testbed for control scenarios

WP1 presented a set of scenarios related to the distribution grid's control system addressing both concrete needs and envisaged evolutions. The scenarios have been conceived in view of a full integration of the operation and control infrastructures of the power system grid management system, i.e. generation, transmission and distribution, and of the development of a global national defence plan involving the different stakeholders.

These scenarios focus on intentional threat hypotheses, having either external or internal source, such as:

- DoS attacks to telecontrol communications by enemies located on the telecom IP backbone,
- Intrusion into centre-substation communication flow and execution of faked commands,
- exploitation of the vulnerabilities of standard application layer protocols,
- virus infections of the substation network caused by malicious maintenance activities.

The first scenarios to be implemented over the CESI RICERCA testbed shall be those related to the security aspects of

- teleoperation and remote control functions for grid operators, and
- interaction between grid operators in emergency conditions.

# 4 REFERENCES

[Chandorkar et al. 1993] M. C. Chandorkar, D.M. Divan, R. Adapa. “Control of parallel connected converters in standalone ac supply systems”, IEEE Trans. on Industry Applications, 29(1):136–143, Jan. 1993.

[De Brabandere et al. 2004] K. De Brabandere, B. Bolsens, J. Van den Keybus, A. Woyte, J. Driesen, R. Belmans, “A voltage and frequency droop control method for parallel inverters,” Proc. 35th IEEE Annual Power Electronics Specialists Conf., Aachen, Germany, Jun. 2004, pp. 2501-2507.

[Depaude 2003] “FT framework integration in the pilot application”, Deliverable D5.2 of the DepAuDE Project, Dependability for embedded Automation systems in Dynamic Environment with intra-site and inter-site distribution aspects, IST Project 25434, www.depaude.org.

[Dondossola et al. 2006] G. Dondossola, J. Szanto, M. Masera, I. Nai Fovino, “Evaluation of the effects of intentional threats to power substation control systems”, International Workshop on Complex Network and Infrastructure Protection, CNIP 2006, Rome, Italy, Mar. 2006.

[D’hulster et al. 2004] F. D'hulster, K. Stockman, I. Podoleanu, R. Belmans, "Optimal switched reluctance motor control strategy for wide voltage range operation," International conference on electrical machines (ICEM), Cracow, Poland, Sep. 2004; 6 pages.

[Dragu & Belmans 2002] C. Dragu, R. Belmans, "Sensorless control of switched reluctance motor," 15th Int. conference on electrical machines (ICEM), Brugge, Belgium, Aug. 2002; 5 pages.

[EREC 2004a] EREC (European Renewable Energy Council), “Renewable Energy Target for Europe 20% by 2020”, EREC, Brussels, 16 pages, Jan 2004.

[EREC 2004b] EREC (European Renewable Energy Council), “Renewable Energy Scenario to 2040”, EREC, Brussels, 16 pages, May 2004.

[Gherasim et al. 2004] C. Gherasim, J. Van den Keybus, J. Driesen, R. Belmans, "DSP implementation of power measurements according to the IEEE trial-use standard 1459," IEEE Trans. on instrumentation and measurement, vol.53, no.4, Aug. 2004, pp. 1086-1092.

[Gherasim et al. 2006] C. Gherasim, J. Driesen, R. Belmans, “Real-time implementation and comparison of time-varying harmonic measurement methods," IEEE PES Power Systems Conference & Exposition, Atlanta, Georgia, USA, Oct.29-Nov.1, 2006; pp. 239-245.

[IEC 61850] International Standard IEC 61850 “Communication network and systems in substations”.

[IEC 60870-5-104] International Standard IEC 60870–5-104 “Telecontrol equipment and systems - Part 5-104: Transmission protocols – Network, access for IEC 60870-5-101 using standard transport profiles”.

[IEC 60870-6] International Standard IEC 60870–6 “ICCP Inter-Control Centre Communications Protocol”.

[Kueck & Kirby 2003] J.D. Kueck, B.J. Kirby, “The Distribution Grid of the Future,” The Electricity Journal (Elsevier Science), pp. 78-87, Jun. 2003.

[Macken et al. 2004] K.J.P. Macken, K. Vanthournout, J. Van den Keybus, G. Deconinck, R. Belmans, “Distributed Control Of Renewable Generation Units With Integrated Active Filter”, IEEE Trans. on Power Electronics, 19(5):1353-1360, Sep. 2004.

[Marwali et al. 2004] M. N. Marwali, J.-W. Jung, A. Keyhani, "Control of Distributed Generation Systems — Part II: Load Sharing Control", IEEE Trans. on Power Electronics, 19(6), 2004.

[MMS] International Standard ISO/IEC-9506 “Manufacturing Message Specification” (MMS).

[Pepermans et al. 2005] G. Pepermans, J. Driesen, D. Haeseldonckx, R. Belmans, W. D’haeseleer, “Distributed generation: definition, benefits and issues,” Energy Policy, Vol. 33, pp. 787-798, 2005.

[Van den Keybus & Deconinck 2004] J. Van den Keybus, G. Deconinck, “Using a C6000 DSP in educating motor control: the electric go-kart project,” *Proc. of European DSP Education & Research Symp. (EDERS-2004)*, Birmingham, UK, Nov. 2004, 5 pages.

[Van den Keybus et al. 2002] J. Van den Keybus, B. Bolsens, J. Driesen, R. Belmans, "Power line communication frond-ends based on ADSL technology," IEEE Int. Symp. on circuits and systems, Scottsdale, Arizona, USA, May 2002; pp. V425-428.

[Van den Keybus et al. 2004] J. Van den Keybus, B. Bolsens, K. De Brabandere, J. Driesen. Using a fully digital rapid prototype platform in grid-coupled power electronics applications. Proc. of 9th IEEE Conf. on Computers and Power Electronics (COMPEL 2004), Urbana-Champaign, USA, Aug 2004, 10 pages.

[Van den Keybus et al. 2005] J. Van den Keybus, B. Bolsens, K. De Brabandere, J. Driesen, “Protection of digitally controlled inverter units in rapid prototyping applications," 20th Annual IEEE Applied Power Electronics Conference and Exposition (APEC) , Austin, Texas, USA, Mar. 2005, pp. 1105-1111.

[Vanthournout et al 2005] K. Vanthournout, K. De Brabandere, E. Haesen, J. Van den Keybus, G. Deconinck, R. Belmans, “Agora: Distributed Tertiary Control of Distributed Resources,” Proc. of 5$^{th}$ Power Systems Computation Conf. (PSCC-2005), Liège, Belgium, Aug. 2005, 7 pages.

[Vanthournout 2006] K. Vanthournout, "A semantic overlay network based robust data-infrastructure, applied to the electric power grid”, PhD dissertation K.U.Leuven, ESAT-ELECTA, Apr. 2006.