A LABORATORY TESTBED FOR THE EVALUATION OF CYBER ATTACKS TO INTERACTING ICT INFRASTRUCTURES OF POWER GRID OPERATORS

Giovanna DONDOSSOLA
Cesi Ricerca – Italy
dondossola@cesiricerca.it

Fabrizio GARRONE
Cesi Ricerca – Italy
garrone@cesiricerca.it

Judit SZANTO
Consultant – Italy
szanto@cesiricerca.it

Fiorenza GENNARO
Enel Distribuzione - Italy
gennaro.fiorenza@enel.it

ABSTRACT

In order to evaluate the resiliency of architectures supporting teleoperation functions, a laboratory testbed, described in the paper, is being developed by CESI RICERCA in the context of the European Project CRUTIAL. The testbed implements a prototypal but significant power system control architecture with its integrated ICT infrastructure.

INTRODUCTION

Within the several challenges posed to power system utilities by the liberation of the power markets, a clear need has emerged to increase the on line monitoring and control functions at the different hierarchical layers of the power system topology. As a consequence to the occurrence of major incidents (e.g. recent black outs and interruptions) relevant innovations are taking place in the national defense plans: current dedicated communication infrastructures are being replaced by externally provided IP (Internet Protocol) based services, current manual operations are becoming automatic, and new manual/automatic functions are being introduced in the current systems [1]. This trend in the evolution of the defense plans implies a number of heterogeneous ICT (Information and Communication Technologies) based components to be upgraded, introduced and integrated at both national and European level, with the SCADA (Supervisory, Control and Data Acquisition) systems positioned in the Operators' Centers playing a central role in the integration process. ICT networks are becoming more and more extensively used to support both real-time and non real-time information exchange with obvious benefits, thus assuming a major role in power system management. The extensive introduction of such advanced ICT technologies in the implementation of the defense strategies impressively increases the dependency of the power system on its ICT based control infrastructures, whose security and resilience requirements have to be carefully addressed. The realization of cooperative defense plans requires a powerful ICT architecture (in term of responsiveness, resilience and security) both to assist operators in manual actions - executed via a combination of SCADA systems, third party communication networks, station-level automation and control systems – and to carry out automatic response actions in urgent emergency conditions. In both cases an up-to-date view of the ICT & Power system state is required.

The power control and management infrastructures of different operators have to be interconnected in order to exchange updated information on the system status and to be able to cooperate in the execution of defense actions under emergency conditions.

Due to exposure of the ICT infrastructures to evolving types of intentional cyber threats, cyber security has become an important issue for utilities managing critical infrastructures [2] . Cyber attacks may have a more or less relevant impact if they occur during normal operation but if they happen when a power contingency is being processed, they may lead to a catastrophic result [3].

In order to evaluate the resiliency of architectures supporting teleoperation functions, a laboratory testbed, described in the paper, is being developed by CESI RICERCA in the context of the European Project CRUTIAL [4]. The testbed implements a prototypal but significant power system control architecture with its integrated ICT infrastructure which shall be used to: i) identify the critical aspects of the interdependency between the Electric and ICT infrastructures; ii) highlight the ICT system's vulnerability to potential cyber attacks; iii) evaluate the resilience of possible architectures/mechanisms/solutions to cyber threats.

Focus has been placed on the development of those aspects of the actual power control systems which can be used for the implementation of different sets of attack scenarios, in order to evaluate their feasibility and plausibility, to demonstrate the possible evolution of the attack processes and to assess the severity of the potential damage on the attack's targets.

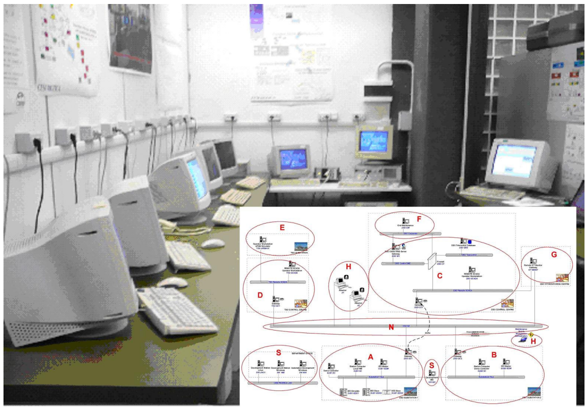


Figure 1: Laboratory layout

TESTBED LAYOUT

The testbed architecture in the CESI RICERCA Laboratory (Figure 1) has been designed and implemented according to a strong scalability requirement.

Focusing on power control systems, scalability applies to i) the capability of the network infrastructure and the application software to support, depending on the operation structure and control scenarios, a different number of control centers and substations; ii) the levels of distribution of the peripheral functions for substation automation and control; iii) the degree of redundancy supported by the automation, control and communication functions.

The testbed infrastructure [4] is constituted by a set of (logical) software building blocks that may be deployed on a (physical) hardware infrastructure for demonstrating the behavior of control scenarios which are the target of assessment. The testbed building blocks prototype automation, communication, SCADA and Operator Interface functions.

Automation functions are implemented by using an automaton based development environment executed over a distributed run time support system with fault tolerant capabilities. The deployment of the automation building blocks on a sample distributed substation automation systems is illustrated in Figure 2.

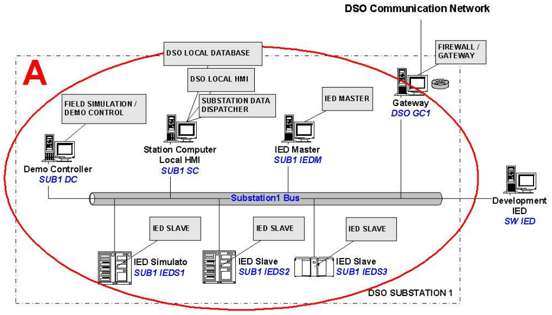
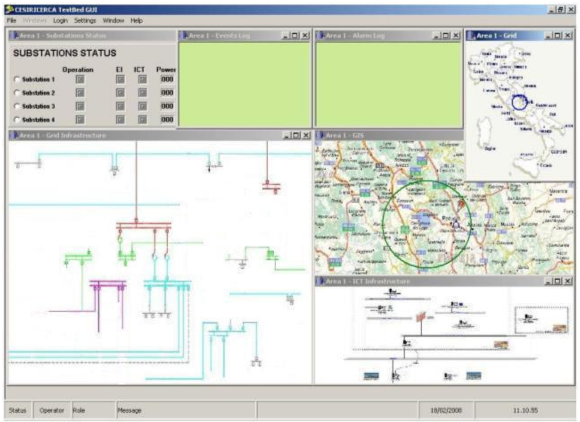


Figure 2: Substation Automation – ICT Layout

The testbed communication architecture reflects a Wide Area Network (WAN) of Local Area Networks, protected by means of Virtual Private Networks and firewall filtering techniques (see Figure 1). Standard communication stacks are deployed: i) the physical and datalink layers of the OSI stack are modelled by switched Ethernet, both for local and wide area communications; ii) TCP/IP and UDP/IP are used at the transport and network layers; iii) application layer data exchange does not make use of commercial protocols, but the contents of the Application Protocol Data Units (APDU)s are compliant with the appropriate standard (IEC 60870-6 Inter-Control Centre Communications Protocol-ICCP/TASE-2 [5], IEC 60870-5-104 for Centre-Substation communications [6], IEC 61850 for communications within the substations); iv) IPSEC is deployed for implementing security in wide area communications.

SCADA functions are prototyped through standard database and web server technologies with specific attention to the separation of the process versus corporate networks.

In order to increase the operator's awareness on the control system status, both power and ICT views and alarms are provided by the Operator Interfaces (see Figure 3).



SUBSTATIONS STATUS

	Operation	EI	ICT	Power
○ Substation 1	▣	▣	▣	000
○ Substation 2	▣	▣	▣	000
○ Substation 3	▣	▣	▣	000
○ Substation 4	▣	▣	▣	000

Figure 3: Control Center – Human Machine Interface

DEPLOYMENT OF CONTROL SCENARIOS

The CRUTIAL testbed deploys the scenarios described in [7] on the laboratory architecture: 1) Grid manual teleoperations in ordinary and pre-emergency management; 2) Automatic telecontrol involving both DSO (Distribution System Operator) and TSO (Transmission System Operator) control infrastructures in emergency management; 3) Integration of Teleperation and Maintenance functions; 4) Maintenance of control infrastructures of power operators.

Manual teleoperations

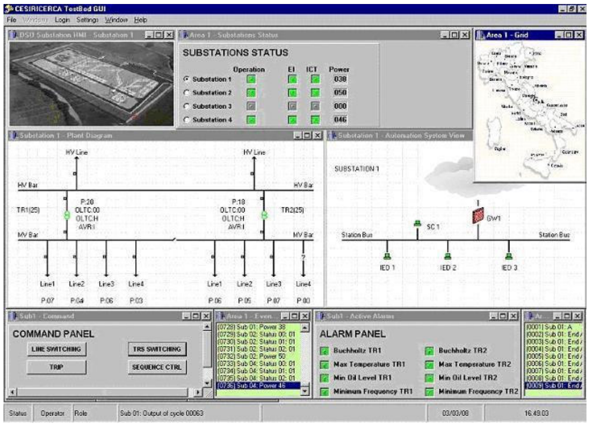
The main purpose of the first scenario consists in the assessment of the security of the ICT components involved in the teleoperation activities of a DSO operator through the analysis of cross-cascading effects [8] due to threat occurrence in both normal and abnormal power conditions.

In general terms a SCADA system is working correctly when it is able to perform all its monitoring and control functions both when the power service is stable (for operational and maintenance needs), and in abnormal or even emergency conditions.

The teleoperation activity, which is performed by means of the operator's console prototyped in Figure 4, includes:

- the continuous monitoring of the substations' status: information is sent from the substations to the Centre, parts periodically (measurements related to active power P, reactive power Q, voltage V values and breaker positions), parts (e.g. alarms and status variations) asynchronously;
- interventions on the grid configuration (opening/closing breakers, line trips, etc.) due to several needs such as predictive maintenance, DSO

contingency management and preventive control requested by the TSO (like rotating load shedding plans and variations in transformer tap changers).



SUBSTATIONS STATUS

	Operation	EI	ICT	Power
● Substation 1	🟩	🟩	🟩	038
○ Substation 2	🟩	🟩	🟩	050
○ Substation 3	▨	▨	▨	000
○ Substation 4	🟩	🟩	🟩	046

```
[0728] Sub 01: Power 38
[0729] Sub 02: Status 00: 01
[0730] Sub 02: Status 01: 01
[0731] Sub 02: Status 02: 01
[0732] Sub 02: Power 50
[0733] Sub 04: Status 00: 01
[0734] Sub 04: Status 01: 01
[0735] Sub 04: Status 02: 01
[0736] Sub 04: Power 46
```

```
[0001] Sub 01: A
[0002] Sub 01: End
[0003] Sub 01: End
[0004] Sub 01: End
[0005] Sub 01: End
[0006] Sub 01: End
[0007] Sub 01: End
[0008] Sub 01: End
[0009] Sub 01: End
```

Status | Operator | Role | Sub 01: Output of cycle 00063 | 03/03/08 | 16.49.03

Figure 4: Substation – Human Machine Interface

The core ICT-systems involved in the supervision and control activities are: the ATC - Area Telecontrol Centers controlling the power substations; the substation automation systems connected to their centers through Wide Area Networks. By following an ongoing trend in the utilities' communication technology renewal, the information flow supporting DSO teleoperation is transmitted by standard telecom IP backbones owned and operated by external providers who supply virtual, dedicated channels over communication links shared with other customers. Such an inter-site communication infrastructure may be assimilated to a public WAN. Due to the strong availability requirements on the communication system (availability equal to 0.99999), redundant communication paths are used, implemented over physically independent carrier lines, possibly owned by distinct telecommunication providers. The correct execution of the DSO teleoperation requires the satisfaction of strict refresh time requirements for measurements/alarms and delivery time requirements for commands by the operator.

Automatic telecontrol

The national integrated defence plans require that in emergency conditions the TSO be authorised by the DSO to activate defence actions, consisting in the automatic execution of load shedding commands on the distribution grid. The second scenario explores the security of the communications between the Transmission and Distribution Operators under emergency operating conditions (i.e. overloading of power lines), assessing the possible cross-cascading effects of ICT threats to the communication channels connecting TSO and DSO Control Centres and Substations.

The TSO Control Center monitors the Electric Power System and identifies potential emergency conditions to be countered with opportune load shedding commands applied to particular areas of the grid. In order to actuate the defence actions the TSO Center chooses a subset of HV/MV substations from the list of substations participating to the emergency plan, then sends a requests to the interested DSO Area Control Centers to preventively arm these substations. These requests are delivered through a communication channel between a TSO Center and a DSO Center. The DSO Center arms the required substations, and returns their status to the TSO Center. In case the potential emergency condition evolves into a real emergency situation, the TSO are sentinel (a Monitoring Control and Defence – Terminal Unit MCD-TU) sends the trip command which has to be delivered through the communication network within 600 ms to recover the emergency.

It is worth of notice that TSO arm requests are asynchronous with respect to the trip commands. The objective of the TSO is to maintain the electric power system in a secure state. In order to prevent the escalation of a possible emergency situation, the TSO Energy Management System makes frequently a selection of detachable loads and emits arm requests to their corresponding control centers. On the other hands trip commands are triggered only for a subset of very extreme conditions.

IMPACT OF ATTACKS TO THE TESTBED

ICT threats that may affect the communication infrastructure range from DoS attacks to the telecontrol communications and intrusions into the Centre/Substation communication flow, eventually followed by the execution of faked commands trough the exploitation of the vulnerabilities of the standard application layer protocols used for monitoring activities and command transmissions [9]. Denial of Service (DoS) attacks to the teleoperation communications, generated by enemies located on the Telecom IP backbone are currently under exploration. Such DoS attack processes to IPv4/IPSEC channels target both DSO Centers and substation routers/gateways/firewalls.

The identified attack plan includes a sequence of attacks showing the increasing severity of DoS processes: first the denial of the supervision function and maintenance activities, then preclusion of the manual intervention of the grid operator, and last the denial of the execution of automatic actions in full emergency conditions.

A first set of experiments demonstrated that the effectiveness of some packet flooding DoS techniques on permanent TCP/IP connections depends on the resource overloading of the attack targets. On the other hands replayed packet attacks were effective on old versions of Windows based stacks, whilst did not succeed in forcing the robustness of TCP/IP protocols implemented in more recent Linux-based systems.

CONCLUSIONS

The main purpose of the CESI RICERCA Laboratory presented in the paper is to develop a platform for testing the cyber security of power control systems including SCADA, substation automation and communication systems. The development, testing and demonstration activities performed in the Laboratory are addressed to all the stakeholders having a remarkable role in the Power System Security (owners and operators of power infrastructures, power regulators, power system vendors, telecom service providers, security service providers, engineering companies) with the objective:

- to improve the security know-how in power control systems;
- to mitigate the vulnerabilities of the standard protocols (e.g. IEC 60870-5-104);
- to assess the capability of the secure and redundant communication architecture to tolerate the threat hypotheses and evaluate the possible cascading effects in presence of power contingencies;
- to offer an infrastructure for testing SCADA and automation system properties, difficult to reproduce in real infrastructures;
- to facilitate the development of standards and guidelines for industrial usage.

The severity of the cascading effects investigated in the laboratory testbed varies depending on i) the grid operating conditions during the ICT attacks ii) the number of substations involved iii) the level of urgency of the teleoperation intervention.

In normal conditions, an attack to a single substation site is not expected to lead the power system in a critical status. However if the DSO operator is repairing a given contingency the consequence of the attack may lengthen the power service interruption.

Even worse if the DSO operator's intervention is meant to counter a pre-emergency situation occurred in the higher level grid, the impossibility to perform the defence action may lead the whole system into trouble.

Cyber attacks carried out under emergency conditions, when defence actions have to be performed under strict real time constraints, can cause severe damages, e.g. inhibiting the proper execution of the required automatic load shedding actions may cause the degeneration of the emergency in the transmission grid. The effects of the considered ICT attacks on the whole power system depend on the number of components involved. As in the previous cases the severity of possible ICT-Power cascading effects depends on the timing of the attacks during the execution of the emergency procedure.

The Human Machine Interfaces supporting the scenario evolution enrich the typical supervision and control functionality currently available in the control rooms. Several ICT-related information increase the situation awareness of the operators and their capability to promptly recover from ICT-due power failures. In this respect the integrated ICT-Power concepts explored on the testbed are expected to contribute in improving the human aspects involved in the resilience of the electric power supply.

ACKNOWLEDGMENTS

This work has been partially financed by the European Commission with the IST Project CRUTIAL http://crutial.cesiricerca.it/ (contract n. 27513).

REFERENCES

[1] G. Giannuzzi, D.Lucarella, S. Massucco, M. Pozzi, M. Sforna, F.Silvestro, 2005, "Advanced Load-shedding Methodology and Architecture for Normal and Emergency Operation of the Italian Power System" *Power Engineering Society General Meeting*, Vol. 2, 1563 – 1569

[2] Grid Consortium, 2007, "ICT Vulnerabilities of Power Systems: A Roadmap for Future Research", *Grid Project Work Package 4 Deliverable D11*

[3] G. Dondossola, J. Szanto, M. Masera, I.N. Fovino, 2008, "Effects of intentional threats to power substation control systems" *International Journal of Critical Infrastructures*, IJCIS, 4 (1/2), 129-143

[4] G. Deconinck, G. Dondossola, F. Garrone, T. Rigole, H. Beitollahi, 2008, "Testbed deployment of representative control algorithms", *CRUTIAL Project Work Package 3 Deliverable D9*

[5] International Standard IEC 60870-6, 2002, "Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – TASE.2 Service and protocol", *International Standard, Second Edition*, Reference Number IEC 60870-6-503(E)

[6] International Standard IEC 60870-5, 2006, "Telecontrol equipment and systems - Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles", *International Standard, Second Edition*, Reference Number IEC 60870-5-104(E)

[7] G. Dondossola, F. Garrone, J. Szanto, G. Fiorenza, 2007, "Emerging information technology scenarios for the control and management od the distribution grid" *Proceedings CIRED 2007 Conference*, paper n. 0262

[8] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, 2001, "Identifying, understanding, and analyzing critical infrastructure interdependencies" *Control Systems Magazine*, IEEE 21**,** 11-25

[9] International Standard IEC 62351-1, 2005, "Data and Communication Security – Introduction", *Technical Committee 57 Working Group 15 Committee Draft*, Version 1