ICT resilience of power control systems: experimental results from the CRUTIAL testbeds

G. Dondossola[1], G. Garrone[1], J. Szanto[1], G. Deconinck[2], T.Loix[2], H.Beitollahi[2]
[1]*CESI RICERCA, Power System Development Department, Via Rubattino 54 20134 Milan (I),*
[2]*K.U.Leuven ESAT / ELECTA, Kasteelpark Arenberg 10 BE-3001 Leuven (B)*
Giovanna.Dondossola@cesiricerca.it Phone: +39 02 39925779 Fax: +39 02 39925557

Abstract

Distributed intelligence and secure interconnected communication networks constitute recognized key factors for the economic operation of electricity infrastructures in competitive power markets. Hence, electric power utilities need to extend risk management frameworks with adequate tools for assessing consequences of ICT (Information and Communication Technologies) threats on their critical business. This requires realistic probability estimates to cyber threat occurrences and consequent failure modes. Due to data sensitivity and rapid discovery of new vulnerability exploits, historical data series of ICT failures affecting power control infrastructures are not sufficient for a timely risk treatment. Such lack of data can partially be overcome by setting up testbeds to run controlled experiments and collect otherwise unavailable data related to cyber misbehaviours in power system operation. Within the project CRUTIAL (CRitical UTility InfrastructurAL resilience) two testbed platforms have been set up for experimentally evaluating malicious threats on macro and micro grid control scenarios. Results from experimental campaigns are analyzed in the paper by means of an evaluation framework.

1. Introduction

In the CRUTIAL project [1], the deployed testbeds are composed of two platforms. One platform – the Telecontrol Testbed – consists of power station controllers on a real-time control network, interconnected to corporate and control centre networks. The other platform – the Microgrid Testbed – is based on power electronic converters that are controlled from PCs that are interconnected over an open communication network. Both testbeds integrate elements 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 [2-5]. These testbeds are used to investigate

- local, hierarchical and distributed control scenarios at transmission and distribution level;
- how architectural patterns for enhancing robustness can be integrated in a realistic setup;
- which interdependencies occur in practice.

The two testbeds are complementary. The Telecontrol 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 Microgrid Testbed focuses on a distribution grid (low voltage levels) with innovative (local and fully distributed) control algorithms.
This paper presents the implementation of several scenarios on both testbeds, as well as the corresponding evaluation results. The paper is structured along two parts: section 2 describes the experiments with the Telecontrol Testbed and section 3 those with the Microgrid Testbed.

2. Teleoperation testbed

The Teleoperation testbed (Figure 1) addresses load reduction scenarios which may occur in power conditions presenting different degrees of severity. Load reduction usually occurs when the power system is exposed to disturbances due to deficiency conditions (faults, loss of generation, switching errors, lightning strikes, etc). The testbed platform [6] implements i) Manual teleoperations by grid operators in maintenance as well as pre-emergency management and ii) Automatic telecontrol actions involving both Transmission System Operators (TSO) and Distribution System Operator (DSO) control infrastructures in emergency conditions.

The selected scenarios address both concrete needs and envisaged evolutions, related to the Distribution Grid's control system. They have been conceived in view of a full integration in the operation and control infrastructures of the Power System, i.e. Generation, Transmission and Distribution, for the implementation

978-1-4244-4421-2/09/$25.00 ©2009 IEEE

of wide area defence plans. The scenarios cover emerging themes like information and communication security aspects of power substation control, support to emergency management by the distribution grid control, interactions between process control and corporate activities and remote maintenance of ICT automation devices. The testbed applications have been stressed by a sequence of Denial-of-Service (DoS) attacks to demonstrate the increasing severity of their effect on the implemented control functions: first the denial of the supervision function and control activities, then the preclusion of the manual intervention of the grid operator, and last the denial of the execution of automatic actions in full emergency conditions.

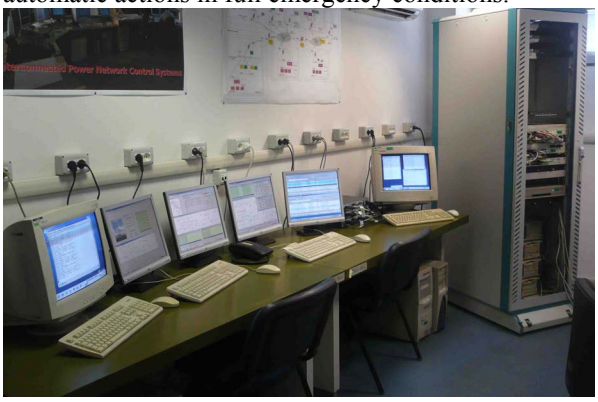

Figure 1. Teleoperation Testbed

The testbed platform, shown in the Figure 2, is a strongly simplified version of interconnected control systems related to a small scale grid fragment [7]. The circles in the figure group the hardware components involved in a given operation area, together with the software development network.

A. DSO Substation Automation System that controls the HV/MV Substation 1
B. DSO Substation Automation System that controls the HV/MV Substation 2
C. DSO Area Control Centre (DSO ACC) that remotely controls Substation 1 and Substation 2 belonging to a portion of a distribution grid
D. TSO National Control Centre (TSO NCC) that supervises critical regions of a transmission grid and implements defence actions
E. TSO Substation Automation System (TSO SENTINEL) that supervises portion of Transmission Grid and triggers DSO Substation trips
F. DSO terminal for Corporate functions (e.g. MV Maintenance activities)
G. DSO ICT system's supervision centre
H. maintenance or attackers' terminals
N. DSO communication network (untrusted)
S. Software development network

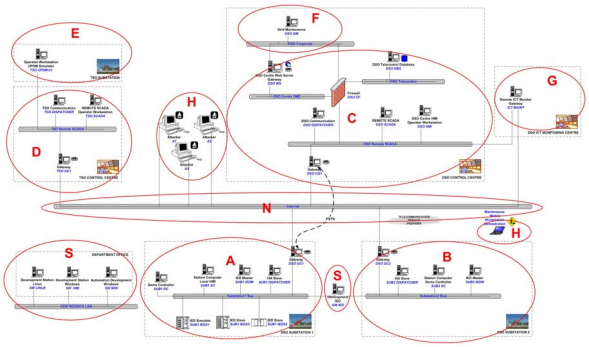

Figure 2: Testbed - deployed architecture

In the testbed the information flow among Substations and Control Centres is based on a simulator of the IEC 69870-5-104 standard protocol [8]. The standard uses the TCP/IP transport profile to exchange data packets and communication control information, with the data packets containing process information in the monitor direction and commands in the control direction.

2.2 Experimental evaluation framework

The execution of controlled experiments has the final objective of making available data statistics about the effects of the attacks on telecontrol applications. In order to achieve that objective logging extensions have been included in the testbed application able to record communication data in text files. From available logs the following metrics have been defined:

i) Inter Message Time - IMT, a measure of the time distance between two consecutive receptions of teleoperation messages;
ii) Inter Reconnection Time – IRT, a measure of the time to recovery of the application protocol derived from the time distance between two consecutive TCP connections successfully performed by the telecontrol protocol;
iii) Time To Failure – TTF, a measure of the resilience to an attack before communications are blocked;
iv) Number of Lost Messages – NLM, the number of expected messages not received;
v) Number of Reconnections – NR, the number of TCP connections successfully performed by the telecontrol application protocol.

The experimental data collected through repeated experiments are then off-line elaborated and the above measures are graphically plotted. The experimental activity consisted of a series of attack experiments whose settings are reported in the Table 1.

Type	DoS
Technique	Packet replying, Packet flooding
Tool	UDP flooding, Syn flooding, TCP replay, Ping
Target	<Centre/Substation Gateway – Port Number>
Attack Source / Number of attackers	<n>
Attack sequence number	<n>
Architectural pattern / Security Level	IP forward, firewall, VPN, Redundancy
WAN Implementation	Hub Ethernet network 10Mbps, Switched Ethernet 10/100 Mbps
Communication Protocol	TCP/IP, IEC 69870-5-104

Table 1: Testbed - Experiment settings

Simulation of DoS attacks may be carried out by means of many craft tools available from the web, using different techniques to generate massive spurious traffic: packet replying and packet flooding are the most popular ones. However the efficacy of the technique on a given testbed platform varies depending on the protocol and the architectural patterns deployed. In the testbed repeated series of DoS attack processes have been generated by insiders located inside the DSO Communication Network, targeting IPv4/IPSEC channels of the Control Centre or Substation gateways. The effect of the attack experiments is influenced by the operating point of the attack target when the attack process starts. Also the efficacy of flooding experiments varies depending on the device used for the WAN simulation.

2.3 Experimental results

The experimental results summarized in this section are related to the assessment of VPN tunneling techniques in conjunction with IEC 60870-5-104 communication protocol, affected by DoS attacks to firewall and VPN architectural patterns.

UDP flooding attacks to a Substation or a Centre gateway have been repeated with a different number of attacking nodes over both unsegmented and switched networks. The communications of the Substation under attack systematically crashes, notwithstanding the reconnection attempts by the telecontrol protocol.

The block of the communications between a Centre and its controlled Substations provokes the loss of monitoring and supervision functions which are essential to the a timely emergency management.

In a load shedding scenario simulated in the testbed, upon detection of a pre-emergency condition the TSO Centre sends a requests of preventively arming the Automation System of specific Substations to the interested DSO ACC. These requests are delivered through communication channels between TSO NCC and DSO ACC. The DSO ACC forwards the arm request to the Substations, and returns their status to the TSO NCC. If the potential emergency condition evolves into a real emergency situation, the TSO sentinel sends the trip command to all the Substations participating to the emergency plan, but only the substations that have been previously armed will be actually detached. TSO sentinels also periodically send test packets toward detachable substations. In absence of three consecutive test packets the automation system automatically disarms the substation. Depending on when the Substation DoS attack occurs, a different scenario evolution has been observed. Figure 3 reports the IMT and TTF measures over time elaborated from the communication data of a sample experiment. In the plotted experiment two attackers initiate a UDP flooding DoS to a Substation gateway before the TSO Centre issues an arming requests for that substation.

The arming request reaches the Substation Automation System (pink square mark) and is correctly executed, but then the communication crash (TTF mark) provokes the interruption of the test flow with the consequent Substation automatic disarming, thus preventing the possibility of tripping the Substation.

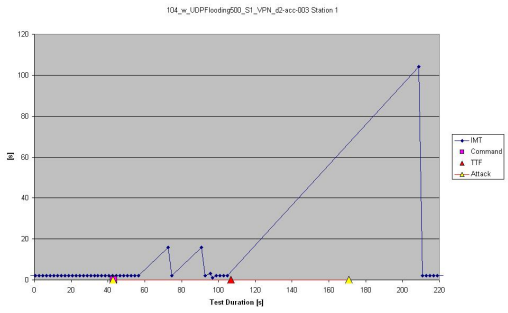

Figure 3: 104 Protocol Test – measures.

3. Microgrid testbed

As the number of distributed generation units connected to the distribution grid continues to increase, it will be impossible to exclude these generators from participating to the control of the utility grid voltage and frequency. The use of a power electronic converter for connecting these energy sources to the grid allows such flexible control of the active and reactive power supplied to or drawn from the grid as well as the provision of ancillary services. Another future development divides the grid in smaller microgrids [9],

each comprising a certain amount of loads and local energy sources and able to operate connected to the utility grid as well as autonomously (island mode). In a microgrid structure a part of the distributed generation units needs to be able to support the grid voltage and frequency. One way in which this can be accomplished is by using a power electronic converter with droop control [9], [10], which is a control method that is well known from the control of large synchronous generators. Droop control is an example of a *primary* control scheme in power systems, which adapts the local voltage magnitude and frequency on sensing the values of active and reactive power [11]. Such primary control algorithm runs on the IED (*intelligent electronic device*) associated to inverter and requires no communication.

In case more than one distributed source is producing energy, such inverters are connected in parallel to the electrical grid. On each of these, the primary control algorithm is running on their associated IEDs. In addition, these IEDs can be connected via a communication network, allowing non-local control algorithms to be executed (Figure 4), e.g. based on exchange of local frequency and voltage values. As such, a secondary control loop keeps voltage magnitude and frequency within its normal limits by communicating among the different generators, and globally adapting values for decreasing or increasing the amount of power that is supplied by a given inverter.

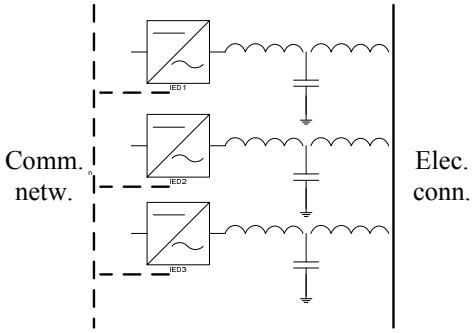

Figure 4. Three one-phase inverters, in parallel connected to the electrical grid, with associated IEDs interconnected via the communication network

Such microgrid testbed, with primary and secondary control algorithms, combining electrical (grid) connections and logical (communication) connections, is the focus of this section. Its goal is to identify the effects of communication faults on the control algorithms and to propose mitigation actions.

3.1 IED/inverter testbed setup

Figure 5 shows the laboratory setup for a single IED/inverter combination. The Triphase inverter platform [12, 13] is the central part of the setup. An FPGA is used to generate the pulse width modulation based control signals for the power transistors as well as to pass on the measurement data of the inverter module and the measurement boards to the server PC. This is a Linux-based server, extended with Xenomai, which allows real-time functionality. It is connected to a user PC, where the droop control scheme is implemented in Matlab Simulink. This allows the user to obtain measurement data and change several control parameters on-line. Together, these PCs and FPGA form the IED of the inverter.

The measurement boards allow to obtain additional measurements, in this case of the LCL filter capacitor voltages and the grid currents, which are the control variables. A solid-state relay is used to be able to operate in grid-connected as well as island mode.

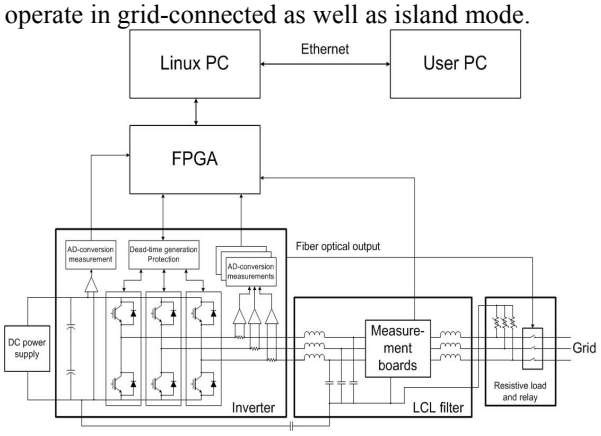

Figure 5. Experimental setup of single IED/inverter

3.2 Impact of ICT faults on primary and secondary control

Multiple (2 to 4) IED/convertor combinations have been electrically connected and communicate via the Matlab interface on the user PC. This TCP/IP based communication takes place over a static topology as different IEDs are connected to a single hub, forming a separate Ethernet segment with point-to-point connections from a one inverter to the others.

By replacing the point-to-point communication infrastructure, other reference cases are possible. If an open or closed internet is used with routers and switches, one can evaluate the effect of transmission delay and varying latencies on the control algorithms that imply communication. Furthermore, if an overlay network is used on top of a physical communication infrastructure, it implies on the one hand additional overhead, due to the overlay management, but also provides additional resilience towards random faults

and denial-of-service attacks [14]. Such overlay networks are well suited for dynamic microgrids with intermittent renewable sources (sun, wind) for which IED-nodes periodically leave or join (secondary or tertiary) control applications. Both cases can be extended by additional fault tolerance mechanisms for power communication networks [15, 16].

We have evaluated the impact from the different ICT faults on microgrid control algorithms. These include the impact of network latency, and the impact of packet loss and network unavailability (e.g. resulting from DoS attacks to the network). Besides these problems resulting in missing messages, a second step evaluated the impact of incorrect values on the different control algorithms.

Case 1 investigates the effect of introducing additional network latency, packet loss and temporary link unavailability, on the communication and hence on the secondary and tertiary control algorithms, slowing down convergence to a new equilibrium state in case of changes in electricity generation or consumption.

However, if no there are no modifications in these generation and consumption profiles, there is no impact of these faults, as there is no need for secondary control actions in this case. Otherwise, the important parameter is the periodicity within which control parameters are exchanged. For one control action per second, individual packets that are lost or temporary link unavailability result in equally slower convergence of secondary control.

Such faults can also occur from DoS attacks. Experiments with a particular attack rate resulting in random dropping of 80% legitimate messages resulted in equally slower convergence of the secondary control algorithm. Adding an intelligent filter (FOSeL [15]) decreases the message loss to 15% in such case.

Case 2 investigates malicious faults by emulating the wrong values that are expected to drive the secondary control algorithm to set points outside their normal range. For instance, if one inverter-IED reports incorrectly that the local voltage level is too low, then secondary control requires neighbouring inverters to increase their power output, resulting in a higher voltage level. If it insists on the incorrect low voltage, the others will try harder to compensate, effectively rising the voltage to outside the normal limits. (Note that this does not pose a safety problem as electrical protection hardware will trigger and disable the inverters if voltages, currents or frequencies are out of range.) Solutions require value integrity detection and authentication.

Overall, three levels of robustness have been evaluated for microgrid control algorithms: 1) control aspects that make algorithms more robust against disturbances (both islanded and grid-connected); 2) adding an overlay layer to the communication which provides additional flexibility and robustness to deal with dynamic application changes and faults (not discussed here); and 3) the impact of architectural solutions to increase the robustness.

4. Conclusions

The Teleoperation Testbed has been used to implement a testing environment consenting the evaluation of attack processes to hierarchically distributed control schemes. The experiments covered the assessment of VPN tunneling techniques in conjunction with IEC 60870-5-104 based communication flows, affected by DoS attacks to firewall and VPN gateways. The combined deployment of these protocols allowed to discover some unexpected vulnerabilities of the communication, because the time-out parameters of the IEC 60870-5-104 protocol may influence the communication performance of the VPN protocols.

According to the defined evaluation framework the effects of DoS attacks on tunneled IEC 60870-5-104 communications may be measured in terms of i) Inter Message Time; ii) Inter Reconnection Time; iii) Time To Failure; iv) Number of Lost Messages; v) Number of Reconnections.

Results from performed experiments showed that flooding based DoS attacks have severe effects on telecontrol communications in terms of both loss of messages and communication blocks caused by the increasing bandwidth consumption up to the saturation of the network stack resources of the VPN gateways. More sophisticated architectural patterns such as filtering mechanisms [15] implementing more effective defence measures for improving resilience have to be evaluated. The achieved experimental results support the development of appropriate standards for the security of application protocols, with specific reference to the Part 7 of the standard IEC 62351, currently under development, concerning the security through network and system management.

The experiments covered a sequence of Denial-of-Service (DoS) attacks to demonstrate the increasing severity of their effect on the implemented control functions: first the denial of the supervision function and control activities, then the preclusion of the manual intervention of the grid operator, and last the denial of the execution of automatic actions in full emergency conditions. In order to increase the operator's awareness on the control system's status, both power and ICT views and alarms are provided by the testbed Interfaces at the Control Centres.

In this critical situation the power system is exposed to disturbances resulting in major deficiency conditions (power line faults, loss of generation, switching errors, lightning strikes, etc). These can have dramatic impacts

on the performance of power systems and therefore require fast and reliable load shedding actions. Inappropriate or untimely load reduction may be ineffective and even cause cascading effects. The severity of possible cascading effects depends from the power system state during the ICT attacks and on the level of urgency of the teleoperation intervention.

Additionally, the Microgrid Testbed has been running primary and secondary microgrid control algorithms on inverters equipped with IEDs. These control algorithms interact via the power network to control voltage and frequency (primary control). They interchange messages via the communication network allowing secondary control to maintain voltage levels. The impact of fail-silent ICT faults is comparable to changing the periodicity of message exchange and hence to slower adaptation of the inverters to generator/consumption changes. The impact of arbitrary failures may lead to over- or undervoltages, which will trigger the electrical protection and calls for other fault prevention or tolerance solutions.

References

[1] G. Dondossola, G. Deconinck, F. D. Giandomenico, S. Donatelli, M. Kaaniche, and P. Verissimo, "Critical Utility InfrastructurAL Resilience," in *Proc. Int. Workshop on Complex Network and Infrastructure Protection (CNIP-2006)* Rome, Italy, 2006, p. 4 p.

[2] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Trans. on Power Systems,* vol. 23, iss. 4, pp. 1836-1846, 2008.

[3] G. Dondossola and O. Lamquet, "Cyber Risk Assessment in the Electric Power Industry," *Cigré Electra Magazine,* vol. 224, Feb 2006.

[4] G. Dondossola, J. Szanto, M. Masera, and I. N. Fovino, "Evaluation of the effects of intentional threats to power substation control systems," in *Proc. Int. Workshop on Complex Network and Infrastructure Protection (CNIP-2006)* Rome, Italy, 2006, pp. 309-320.

[5] G. Deconinck, T. Rigole, H. Beitollahi, R. Duan, B. Nauwelaers, E. Van Lil, J. Driesen, R. Belmans, and G. Dondossola, "Robust Overlay Networks for Microgrid Control Systems," in *Proc. Workshop on Architecting Dependable Systems (WADS-2007), co-located with 37th Ann. IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN-2007)* Edinburgh, Scotland (UK), 2007, pp. 148-153.

[6] F. Garrone, C. Brasca, D. Cerotti, D. C. Raiteri, A. Daidone, G. Deconinck, S. Donatelli, G. Dondossola, F. Grandoni, M. Kaâniche, and T. Rigole, "Analysis of new control applications, CRUTIAL Workpackage 1 Deliverable D2," 2007.

[7] G. Deconinck, H. Beitollahi, G. Dondossola, F. Garrone, and T. Rigole, "Testbed deployment of representative control algorithms, CRUTIAL Workpackage 3 Deliverable D9," 2008.

[8] International Electrotechnical Commission, "IEC 60870–5-104 Telecontrol equipment and systems - Part 5-104: Transmission protocols – Network, access for IEC 60870-5-101 using standard transport profiles," 2006.

[9] R. H. Lasseter and P. Piagi, "Microgrid: A Conceptual Solution," in *Proc. 35th Annual IEEE Power Electronics Specialists Conference* Aachen, Germany, 2004, pp. 4285-4290.

[10] K. De Brabandere, B. Bolsens, J. Van den Keybus, A. Woyte, J. Driesen, and R. Belmans, "A Voltage and Frequency Droop Control Method for Parallel Inverters," *IEEE Trans. on Power Electronics,* pp. 1107-1115, 2007.

[11] T. Loix, K. De Brabandere, J. Driesen, and R. Belmans, "A Three-Phase Voltage and Frequency Droop Control Scheme for Parallel Inverters," in *33rd Annual Conference of the IEEE Industrial Electronics Society (IECON2007)* Taipei, Taiwan, 2007, p. 6.

[12] Triphase, http://www.triphase.com

[13] J. Van Den Keybus and J. Driesen, "Performance of Real-Time Power Electronic Converter Algorithms Implemented on a Personal Computer," in *Proc. 2006 IEEE International Symposium on Industrial Electronics* Montreal, Canada, 2006, pp. 3281-3286.

[14] H. Beitollahi and G. Deconinck, "Dependability Analysis of Overlay Networks," in *Proc. 14th IEEE Int. Symp. on Pacific Rim Dependable Computing (PRDC-2008)* Taipei, Taiwan: IEEE, 2008.

[15] H. Beitollahi and G. Deconinck, "FOSeL: Filtering by helping an Overlay Secure Layer to Mitigate DoS Attacks," in *Proc. 7th IEEE Int. Symp. on Network Computing and Applications (NCA-2008)* Cambridge, MA (USA), 2008, pp. 19-28.

[16] P. Verıssimo, N. F. Neves, and M. Correia, "CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture " in *1st Int. Workshop on Critical Information Infrastructures Security (CRITIS-2006)* Samos, Greece, 2006, p. 6.