International Conference on Renewable Energies and Power Quality (ICREPQ'16)
Madrid (Spain), 4th to 6th May, 2016
Renewable Energy and Power Quality Journal (RE&PQJ)
ISSN 2172-038 X, No.14 May 2016

Design and development of a test environment to analyze the impact of cyber attacks on the electrical distribution network

Ioannis Moschos[1], David Lavérnia Ferrer[1], J.-I. Cairó[1]

[1] IREC, Catalonia Institute for Energy Research
C. Jardins de les Dones de Negre, 1, Pl. 2a, 08930 Sant Adriá del Besós, Barcelona, Spain
Phone: +34 933 562 615. e-mail: **icairo@irec.cat**

Abstract. Extensive use of information and communication technology infrastructure (ICT) in today's electrical networks is empowering the Smart Grid growth, but at the same time lays the foundation for cyber threats to the more vulnerable premises of the system. The purpose of this work is twofold. First, to build a simulation environment that covers the impact assessment of cyber attacks on a distribution network´s power components. Second, to propose a testbed architecture which will be comprised from the aforementioned simulation tool combined with a hardware-implemented microgrid. The final cyber-to-physical environment would provide a more accurate embodiment of information data flow through real communication paths. This will enable developing, integrating and conceiving cyber attacks' impact on realistic scenarios. The testbed environment would have a strong emphasis on Distributed Renewable Energy Resources (DER). The power system simulation tool used in this work is DIgSILENT Powerfactory. IREC's microgrid SmartLab facilities are utilized in the complete test bed formulation.

Key words

cyber attack, distribution grid, power system simulation, DIgSILENT, DER

1. Introduction

Critical Infrastructures like electrical networks become increasingly dependent on ICT resources, since there is a growing need for higher data flow, remote monitoring and control and better interoperability between different network components. The novel schemes that enable Smart Grid functions, such as self-healing, Demand Side Management and centralized control of generation and demand premises are based on complex ICT systems that are unavoidably more vulnerable to cyber threats. For instance, a SCADA environment utilizes protocols such as Modbus and DNP3, which are proven susceptible to cyber intruders [1].

What makes cyber attacks really threatening is their immediate and sometimes devastating effect at a very low cost. In addition, they are usually deceptive –the intruders make the system operators 'blind' to the attack– as it was the case with the Stuxnet computer worm that forced nuclear centrifuges in Iran to tear themselves apart [2]. This results in two major problems; the attack can reach its final process disruption (e.g. blackout) without being detected and the authorities cannot trace back the identity of the attacker.

Efforts in grid resilience against cyber threats are constantly improving. The U.K. is going to increase spending on its cyber security program to 860 million pounds by December 2015, in order to reduce the cyber threat risks [3]. National security centers are also being established all over Europe to monitor and protect critical infrastructure [4]. European Commission has already determined a cybersecurity strategy in the European Union that addresses industrial, economical and organizational milestones which will lead a strengthened cyberspace [5]. Despite all these ventures, a recent attack at the Sony Pictures entertainment company demonstrated that hackers still possess high ability in acquiring control of critical IT services [6].

A. Related research work

Several studies have been conducted in the past related with cybersecurity in the smart grid. The topic is vast and the literature covers many different schemes, for instance the vulnerability of components, risk assessment, prevention and mitigation of the attacks. Studies that use simulation techniques for examining the impact of cyber attacks can be classified in three main categories:

- Based on the time scale of phenomena that are investigated. Power system simulations can be steady-state, transient or real-time. Communication and control components however, require a discrete event simulation approach. Authors in [7] discuss all these aspects in detail.
- Depending on the Smart Grid layers being modeled, which also affects the number of software tools used. Cyber attacks occur at the information/control or the communication layer

of the SGAM architecture [8], but their usual purpose is to impair the physical layer processes. Studies in [9], [10] and [11] focus on the later, while [12], [13] on the former.

- Based on whether a stand-alone simulation environment such as in [9] or one that combines virtual and physical components is utilized, such as the work carried out in [14] and [15]. The study in [16] proposes a testbed setup using power system simulation (Powerfactory) and communication emulation in a real time digital simulator (RTDS). In [17], the authors provide an interesting overview of various testbed formulations and discuss on the components needed for an accurate cyber-physical environment.

B. Contribution

An electrical distribution network including models of DERs and Smart Grid control functions is developed in Powerfactory. Local controllers are integrated using the program's DSL language, while remote supervisory control logic is implemented through communication with an OPC Server. A series of cyber attacks can be evaluated using this virtual environment and the impact can be assessed using voltage, frequency or thermal loading violations. In addition, a virtual-to-physical testbed is established that adds real ICT interconnections to the final concept (e.g. by Modbus links). Comparing with other similar testbed configurations, this setup would allow cybersecurity investigation of novel concepts, such as the droop control and ancillary services provision from arrays of residential microgrids, or the Vehicle-to-Grid role in cyber attack mitigation. Eventually, this environment will also be used in innovative cyber threats detection and prevention techniques.

2. Virtual environment

A. Overview of CIGRE MV network and implementation in DIgSILENT

CIGRE Task Force has developed benchmark electrical networks to enable integration of Distributed Energy Resources (DER) and testing of new smart grid techniques [24]. The European MV case was adopted and adjusted for the purposes of this study. This benchmark consists of 14 nodes and part of it is shown in Figure 1.

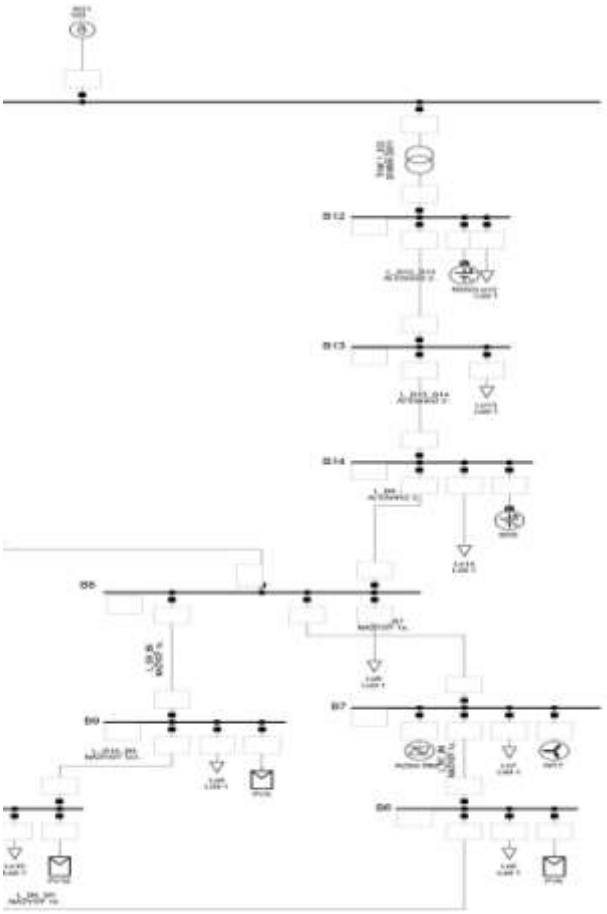

Fig. 1. Part of CIGRE MV Network topology, including Distributed Energy Resources

Several loads with time variant power consumption are connected to the nodes. The total load peak is approximately 27MW. There are also 3 wind turbines with total peak capacity of 4.5MW and 6 photovoltaics with 415kW peak capacity, distributed along the network. A large spinning synchronous generator (SG) of 120MVA rated power represents the HV system slack. Considering the peak generation vs demand, the machine's inertia is proven sufficient to sustain a stable frequency close to 50Hz, along with the frequency controllers. The model of the SG includes the speed governor and the exciter in order to regulate the system's frequency and voltage at its connection point, accordingly. The speed governor is the IEEEG1 turbine-governor type (1981) [18], while the exciter is the IEEE DC1A type [19].

A secondary controller (or so-called Automatic Generation Control - AGC) is also implemented. Tie line deviations are not considered, since the network consists of a single area. Hence, the error signal is calculated as:

$$ACE = B \cdot \Delta f \tag{1}$$

where B is the frequency bias and Δf is the frequency deviation from nominal.

The error signal is inserted in a PI block that represents the secondary controller. The output control signal is served as an input in the turbine's governor. The AGC is

utilized as a supplement to the primary controller and restores the frequency to the steady state value of 50Hz. Also, its control reaction is in the scale of minutes, in order to not interfere with the quick primary control response to frequency deviations.

Wind Turbines are modeled as current sources. The aerodynamic and the mechanical parts are designed as in [20]. However, the fast electromagnetic transients in the generator and the harmonics introduced by the power converters are omitted, since they are not relevant to the presented study.

The photovoltaics' modeling also follows the current source principle. The voltage-current equations that construct the models can be found in [21]. Both WTs and PVs integrate two reactive power dispatch mechanisms:

- Voltage Control: In which the supplied/consumed reactive power is regulated according to the local voltage measurements:

$$Q = k \cdot (U_{meas} - U_{set}) \quad (2)$$

where k is the reactive power regulation ratio, U_{meas} is the measured voltage and U_{set} is the local setpoint

- Reactive power control: In which the controller receives external Q setpoint signals from the system operator:

$$Q = Q_{set} \quad (3)$$

The load profiles are synthesized from real data measurements of domestic households in Barcelona, Spain. The wind speed data is obtained from NREL´s [22] database and it is composed of 10min resolution average wind speed measurements. Solar global horizontal irradiation data is composed of real data values from Plataforma Solar de Almeria [23], in Spain. Finally, the parameters for modeling the distribution lines and the power transformers can be found in [24].

The simulations are conducted using the DIgSILENT Powerfactory power system simulator [28]. Since the data inputs used have 10-15min sampling resolution, an RMS simulation that considers only electromechanical dynamics is sufficient to have a clear picture of the system's behavior.

B. OPC interface / co-simulation approach

OLE for Process Control (OPC) stands for an industry standard communication interface, utilized by process and control systems. This chapter describes the use of OPC link in the purpose of illustrating a Distribution System Operator's (DSO) remote connection with the CIGRE grid. The same link is used for deploying remote cyber attacks on network components.

As seen in Figure 2, on one side the OPC client represents the DSO's SCADA console, receiving measurements and status of devices, while sending supervisory control signals to the power system elements. On the other side, the power system model in Powerfactory simulates the physical system's dynamic behavior and its response on the control signals of the DSO. The core components needed for this simulation are:

- The OPC Server Explorer which acts as the client that invokes control actions according to data measurements (DSO's operator panel).
- The Powerfactory simulator that models the CIGRE network and simulates the local controllers' behavior.
- The OPC Server as the central component that realizes the communication described above.

The free versions of Matrikon OPC Server and OPC Server explorer [25] were used for the purposes of this study. OPC connected applications run asynchronously with system time, hence simulation time steps are not synchronized.

The current implementation of this co-simulation environment includes the following basic functions:

- monitoring and control of active and reactive power of DERs
- monitoring and control of reactive power dispatch status of DERs
- monitoring status of switches and control of circuit breakers
- monitoring status of transformer taps and control of tap changers

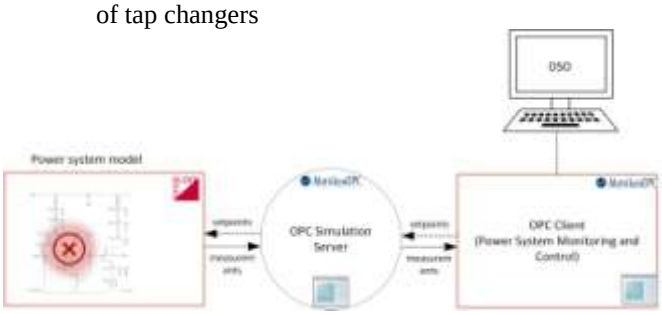

Fig. 2. OPC client-server implementation

3. Cyber attack scenarios based on the simulation environment

Four cyber attack scenarios have been identified and simulated in the CIGRE network, but for the sake of simplicity, only two of them are shown here. The rest of the work will be available in PREEMPTIVE Fp7 project [26].

A. Scenario 1: Malicious MV Circuit Breaker Trip Command

This is considered a False Data Injection attack [27], because the adversary would need to change the status of the breakers from 'close' to 'open'.

Three cases can be identified, which could lead to a circuit breaker (CB) control acquisition by the perpetrator:

- Acquiring authorization rights of a remote workstation in the control networks that has access to some of the main SCADA functions in the system, such as the CB control. Then sending an 'open' setpoint signal. The automatic reclosure would not work in this case, as this is a manual command.
- Gaining physical access to the process WAN and intercepting the connection (e.g. DNP3/IEC61850) between the substation RTUs and the SCADA system. The next action would be the launching of a man-in-the-middle attack.
- Similarly to the previous case, but now by gaining physical access to the internal substation's network environment (e.g. 61850-multicast Ethernet) and directly attacking the IED relays that control the CBs.

The systems responding to this attack would be: the voltage control of DER (Q [VAr] provision) based on local measurements; the tap changing control of distribution Transformers; the load shedding relay; the Automatic Voltage Regulator (AVR) of the synchronous machine.

In the simulated scenario, at 04:30 the attacker, acting as the system operator, sends an 'open' command at the CB of the Transformer connected at node 12. The CB opening action immediately changes the system's topology. There is an immediate voltage drop, which is compensated by the DERs in the system. In Figure 3, this VAr provision is shown for Wind Turbine at Bus 7. All other DERs follow similar behavior, as their voltage controllers have the same characteristics. However, as the total system's demand increases, DERs' voltage control response cannot keep up with the fast increase of demand during the day's peak. In this case, and when the voltage at Bus 12 drops below 0.90p.u., the load shedding activation of Load 12 is triggered (by 20%) and depicted in Figure 4. This action occurs 4 times, leading to a significant loss of load of approximately 3.3MW.

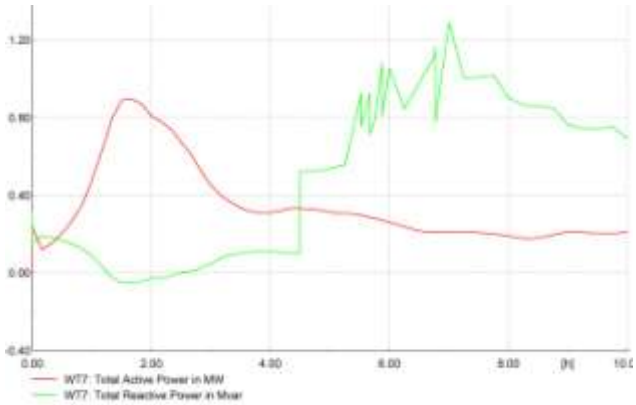

Fig. 3. WT7 VAr compensation after the attack (MVAr)

A Demand Side Management system employed by the DSO could mitigate such kind of attack. However, the results also showed that increased penetration of DERs would not help the system regain stability; the system's voltage would be compensated, but the heavily loaded lines would eventually surpass their thermal limits (130%), inevitably leading to a more serious disaster (black-out).

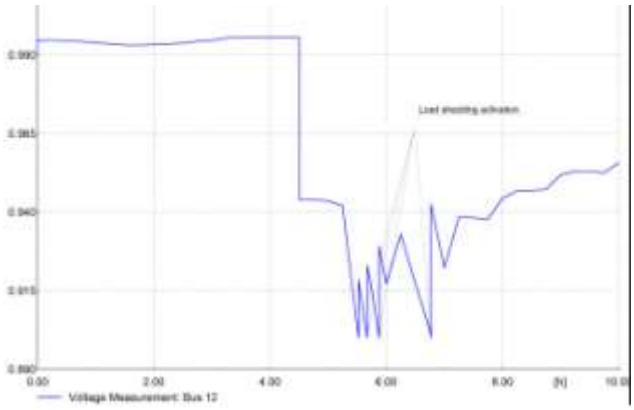

Fig. 4. Load shedding of Load12 after the attack (MW)

B. *Scenario 2: Attack at the Voltage Control scheme of DER*

Wind turbines and photovoltaics included in the system can improve power quality by enabling their reactive power dispatch controllers.

Typically, a large Wind or Photovoltaic plant can be associated with three levels of a SCADA network [9]:

- Local Ethernet-based network
- Corporate LAN connected to vendors through remote connection such as VPN
- Fully integrated Wide Area Network

Authors in [9] have already identified a number of attack opportunities on the communication links above.

In the simulated attack scenario, the adversary remotely changes the dispatch of the DERs to the reactive power control mode. They are then able to craft a malicious Q_{set} (MVAr) setpoint signal. This setpoint value should be below the reactive power capabilities of the respective DERs. Otherwise, this kind of attack will have no success, as the controller will automatically return to the locally controlled voltage control mode.

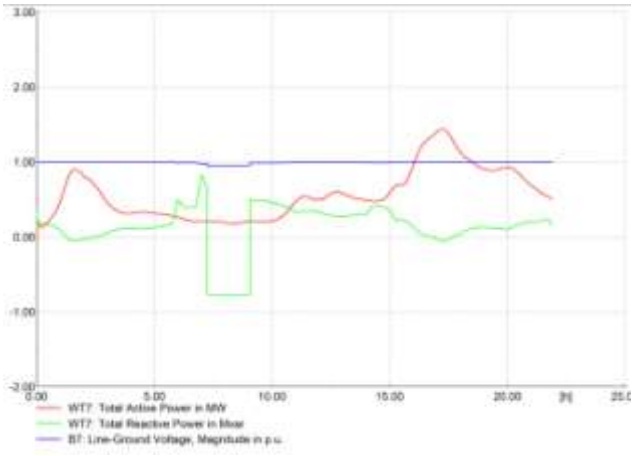

Fig. 5. Voltage at Bus 7 (pu), Active and Reactive Power of WT7 (MW)

The attack forces the DERs to consume a high amount of reactive power that leads to a voltage decrease, whereas the system's actual needs presented a generation of reactive power. The results can be seen at the VAr change for Wind turbine at Bus 7 at Figure 5. Voltage at Bus 7 drops substantially, below 0.95pu. and the system becomes unbalanced, till this attack is mitigated by the System Operator.

4. Conceptual architecture of a virtual-to-physical testbed environment

Figure 6 shows the elements and connections that integrate the test environment, including both the virtual tools and the hardware, to deploy and analyze the attack scenarios. The MV virtual software environment, presented previously, is linked to IREC's SmartLab microgrid through a Modbus TCP/IP node, to which can be connected either through shared csv files or through an OPC service. Now, the virtual environment is used to perform multiple load flows, rather than RMS simulations; certain modifications are committed for this purpose.

IREC's microgrid is composed of several 5kW cabinets that can mimic real Distributed Energy Resources both injecting or consuming power following real power curves of wind turbines, solar systems, storage and loads. The microgrid also includes real systems, such as a second life battery. The programmable devices that manage these cabinets are linked through Modbus TCP/IP to the microgrid Concentrator, to which they send readings and from which they receive setpoints. The microgrid Concentrator is also connected with the Energy Management System (EMS), which optimizes the operation and management of the microgrid. The EMS uses price and weather forecasts that are downloaded and stored on a local folder.

The Grid Emulator is a 200kW converter that sources power to the microgrid and has the capability of changing frequency and voltage levels, or introduce harmonics and sags. The Grid Emulator setpoints will be provided from the DIgSILENT-to-microgrid gateway, so that the power the cabinets receive will follow the values of the point of common coupling (PCC) described on the Virtual Environment. Electrical readings and setpoints are updated every 3-10 seconds, following the rate at which DIgSILENT will write to disk.

5. Cyber attack scenarios based on the complete test bed environment

Three core cyber attack use cases can be identified, based on the position of the attacker:

- The Distribution Management system (DMS) is compromised and a false control action-opening of a CB is launched (red point 1 in simulated network in DIgSILENT), changing the network state. The value of the power at the PCC is transmitted through the DIgSILENT-to-microgrid gateway (through a csv file). This value is read by the microgrid Concentrator and followed by the Grid Emulator. The microgrid adapts its power flow and writes the value of aggregated power on the PCC on another csv file. This process resembles a real DMS voltage control logic, requesting ancillary services from remote DERs. The csv files are continuously updated. Meanwhile, a DPL program reads the actual measured output power of the microgrid that is stored in the other csv file. By utilizing this process, a cyber attack at any point in the power network is translated into a new behavior on the microgrid.
- A man-in-the-middle cyber attack occurs at the microgrid premises: e.g. by intercepting the Modbus traffic and fabricating a fake setpoint signal (red point 2). In this case, every action issued by the DSO or from a remote workstation acting upon the microgrid, would be compromised.
- An external attack, gaining authorization rights at the corporate network and modifying the price and/or weather forecasting data at the microgrid's Energy Management System (red point 3). From such kind of attack, the expectation would be a non-optimized behavior from the elements of the microgrid.

All these attacks, if coordinated and carefully thought out, could lead to fatal grid faults.

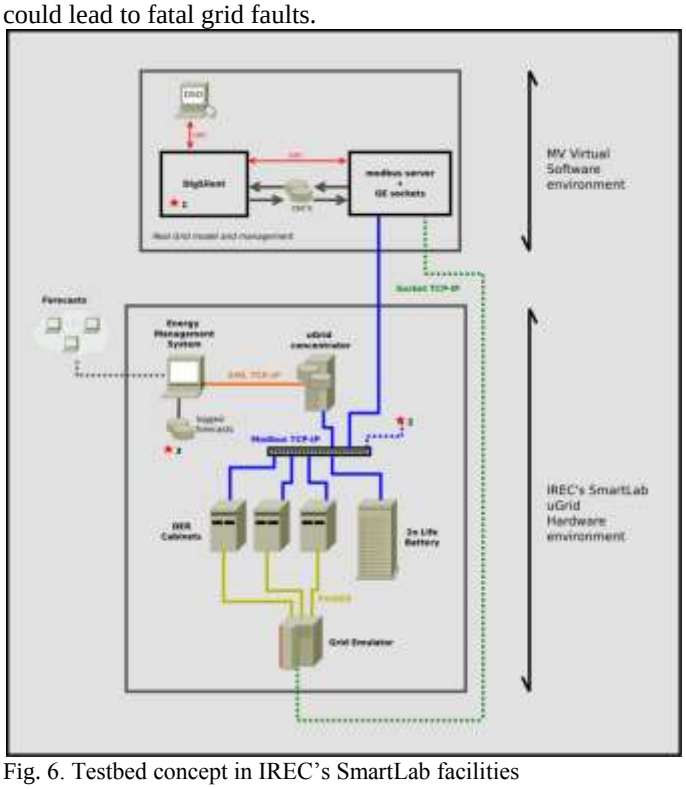

Fig. 6. Testbed concept in IREC's SmartLab facilities

A simple example, based on Scenario (1) has been simulated in order to show the anticipated cyber-physical response: Four nodes in CIGRE network consist of scaled-up microgrids. A cyber attack results in opening of the CB at Line 8-14. Immediately, 7 buses in the system experience a voltage drop below the threshold of 0.95pu. Consequently, voltage control is actuated and a remote

setpoint signal is sent to the microgrid in order to reduce its output power. A proper response from the microgrid´s EMS would stabilize the voltage in the system and will be as fast as the elements of the microgrids that respond to it. In this simulation scenario, voltage is already compensated to its nominal values after 12 seconds, assuming that the second life battery is the core element that provides the flexibility needed.

6. Conclusion

Due to their crucial importance for society and their delicate infrastructure, electrical networks are considered a top target for terrorists and rogue states.

This research work illustrates a built environment that enables the definition and integration of cyber attacks in electrical distribution networks with DER penetration. Furthermore, a real hardware environment is proposed to be utilized in a hybrid virtual-physical concept, in order to serve for future cyber attack detection and mitigation studies, as well as cover cybersecurity topics related with novel microgrid concepts.

Acknowledgement

This work has been partially supported by the European Commission through project FP7-SEC-607093-PREventive Methodology and Tools to protect utilitIEs (PREEMPTIVE) funded by the 7th Framework Program.

References

[1] Parthasarathy, S.; Kundur, D., 'Bloom filter based intrusion detection for smart grid SCADA,' 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pp.1-6, 2012

[2] R. Lagner, 'To kill a centrifuge-A technical analysis of what stuxnet's creators tried to achieve', November 2013

[3] http://www.bloomberg.com/news/articles/2015-01-09/power-grid-under-cyber-attack-every-minute-sees-u-k-up-defenses

[4] C. Hopson, 'Feeling Secure?', rechargenews.com, 08.2014

[5] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', Brussels, 7.2.2013

[6] http://www.zdnet.com/article/sony-hack-cost-it-15-million-so-far/

[7] K. Mets, J. A. Ojea, C. Develder, 'Combining power and communication network simulation for cost-effective smart grid analysis', IEEE Commun. Surveys & Tutorials – Special issue on energy and smart grid

[8] CEN-CENELEC-ETSI Smart Grid Coordination Group First set of standards, November 2012

[9] J. Yan; C.-C. Liu; Govindarasu, M., "Cyber intrusion of wind farm SCADA system and its impact analysis," in Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES , vol., no., pp.1-6, 20-23 March 2011

[10] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, K.L. Butler-Purry, 'Towards modeling the impact of cyber attacks on a smart grid', Int. J. Security and Networking, 2010

[11] A. Anwar, A. n. Mahmood, M. Ahmed, 'False data injection attack targeting the LTC transformers to disrupt smart gird operation', 10th Conference on Security and Privacy in Communication Networks, 09.2014

[12] T. H. Morris, W. Gao, 'Industrial Control System Cyber Attacks', ICS-CSR 2013 Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research, pp. 22-29, 2013

[13] J. Hong, 'Cyber security of substation automation systems', Phd dissertation, Washington State University, August 2014

[14] U.S. Department of Energy, 'National SCADA Test Bed: Enhancing control systems security in the energy sector', Fact Sheet, Idaho National Laboratory (INL), 2007

[15] A. Stefanov, C. Liu, 'Cyber-Physical System Security and Impact Analysis', Preprints of the 19th World Congress The International Federation of Automatic Control, Cape Town, South Africa, August 24-29, 2014

[16] C. Breaden, A. Dysko, G. Burt, E. Davidson, N. Mcneill, 'A testbed for the assessment of active network management applications using simulation and communications emulation', 22th international conference on electricity distribution (CIRED), Stockholm, 10 June 2013

[17] A. Hahn, A, Ashok, S. Sridhar, M. Govindarasu, 'Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid', IEEE Transactions on Smart Grid, Vol. 4, No. 2, June 2013

[18] Siemens PTI. BSOL controllers - Standard 1 (2008)

[19] IEEE Std. 421.5-2005. IEEE Recommended practice for excitation system models for power system stability studies (2005).

[20] F. Diaz-Gonzalez, A. Sumper, O. Gomis-Bellmunt, F.D. Bianchi. 'Energy management of flywheel-based energy storage device for wind power smoothing'. Applied Energy Journal (2013), Vol. 110, pp. 207-219

[21] M. G. Villalva, J. R. Gazoli, E. R. Filho, 'Comprehensive approach to modeling and simulation of photovoltaic arrays', IEEE transactions on power electronics, Vol. 24, No. 5, May 2009

[22]http://www.nrel.gov/electricity/transmission/wind_integration_dataset.html

[23] http://geomodelsolar.eu/data/full-time-series/

[24] CIGRE task force C6.04.02, 'Benchmark systems for network integration of renewable and distributed energy resources'. 2013

[25] http://www.matrikonopc.es/

[26] http://preemptive.eu/

[27] Y. Liu, P. Ning, M. Reiter, False data injection attacks against state estimation in electric power grids, in: Proc. of ACM Computer and Communication Security (CCS), 2009.

[28] DIgSILENT GmbH, DIgSILENT PowerFactory v.14, user manual,
Germany, 2009