Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Cyber-Physical System Security and Impact Analysis

Alexandru Stefanov* Chen-Ching Liu*,**

**University College Dublin, Belfield, Dublin 4, Ireland*
(e-mail: alexandru.stefanov@ucdconnect.ie).
*** Washington State University, Pullman, WA 99164-2752, USA*
(e-mail: liu@eecs.wsu.edu).

Abstract: Electric power grids have been identified as critical infrastructures. They are increasingly dependent on Information and Communication Technologies (ICTs) for the operation and control of physical facilities. It can be envisioned that on top of the power infrastructure reside ICT layers that are coupled with the electric grids. As the ICT connectivity increases, so does the potential for cyber intrusions. This paper describes the importance of cyber security for power systems. A testbed architecture provides an accurate and powerful tool for identification of cyber-physical system vulnerabilities, security enhancement, impact analysis, and mitigation of cyber attacks. Simulation scenarios of cyber intrusions and attacks on the power grid, using the testbed, are discussed. The impact analysis' simulation results capture the dynamic behavior of IEEE 39-bus system as a response to cyber attacks which may evolve into a partial or complete blackout. The problem of fast restoration from blackout after cyber attacks is identified.

Keywords: cyber attacks, cyber-physical system, cyber security, impact analysis, restoration

1. INTRODUCTION

Electric power grids have been identified as a critical infrastructure. They are increasingly dependent on Information and Communication Technologies (ICTs) for the operation and control of physical facilities. It can be envisioned that on top of the power infrastructure reside ICT layers that are coupled with the electric grids. The Supervisory Control And Data Acquisition (SCADA) system for the electric power industry is a wide area information, communication, and remote control network to coordinate the power infrastructure as reported by Wu et al. (2005). It provides power system operators with real-time monitoring, command, and control capabilities.

The power grid, SCADA system, and Energy Management System (EMS) form a large, complex, and interdependent cyber-physical system. In the past, each of these layers was studied as a separate entity. Physical security of the power grid has long been widely recognized as an important issue and actions have been taken to restrict access to various facilities. However, ICTs on the power grids have evolved from isolated structures into an open and networked environment. The power and cyber systems are becoming more and more interdependent. Models of the interactions are needed between the power devices and ICTs. A model of cyber-physical energy systems for distributed sensing and control was reported by Ilic et al. (2010). Any disruption of service in the cyber layer has a direct impact on the power system's operation. Denial of Service (DoS) and increased time delays for measurements and control commands transmitted via SCADA affect the power grid's observability and controllability. In case of large disturbances, the grid might experience instability and, without proper control, it may lead to a sequence of cascading events and finally to blackout. Thus, it is important to incorporate both cyber and power layers for vulnerability analysis, especially in the cyber security context.

Research efforts have been made worldwide to secure the power grids. The key security technologies for a smart grid are summarized by Metke and Ekl (2010). They proposed an overall security solution for the smart grid by using public key technologies along with trusted computing elements based on the security requirements, system scale, and required availability. A conceptual layered framework and strategies for protecting the smart grid and automation systems against cyber attacks without compromising the availability of data was presented by Wei et al. (2011). Attack and defense modeling to understand the cyber attack mechanisms and enhance cyber security of the critical infrastructures was proposed by Ten et al. (2010). An algorithm for early anomaly detection in the computer network of a substation was proposed by Ten et al. (2011). Experimental evaluations of cyber attacks and risk assessment of power control systems were reported by Dondossola et al. (2011). The proposed solutions to prevent malicious attacks on ICTs are encouraging, but further security issues need to be addressed especially in the context of smart grids. Rigorous defense is needed against the broad range and continuously evolving cyber threats. This research can be better conducted in the context of cyber-physical systems. The interactions between ICTs and physical facilities must be considered to identify the weak points of the system and assess the potential impact of cyber attacks on power grid operation. Impact analysis performed with an integrated cyber-physical system indicates that, in the worst case scenario, cyber attacks can lead to blackouts. Restoration plans for the power grids exist. However, the recovery from a major outage caused by cyber attacks is a particular case of grid restoration. The SCADA system may be affected and not operational. Strategies for

coordinated restoration of the cyber-physical system are needed.

This paper describes the importance of cyber security for cyber-physical systems. A cyber security framework and SCADA testbed architecture at University College Dublin are presented. The testbed capabilities are enhanced by integrating computer networks and power grids simulators. Large cyber-physical systems can be modeled. Simulation scenarios of cyber intrusions and attacks on the power grid, using the testbed, are discussed. The simulations are performed with IEEE 39-bus system. The problem of fast restoration from a blackout after cyber attacks is identified.

The remaining of the paper is organized as follows. Section 2 describes the cyber-physical system security. Section 3 presents a SCADA testbed architecture. Section 4 discusses cyber intrusion scenarios and impact analysis. Section 5 provides the simulation results. The conclusion is discussed in Section 6.

2. CYBER-PHYSICAL SYSTEM SECURITY

As the ICT connectivity increases, so does the potential for cyber intrusions. Major intrusion incidents have confirmed the importance of cyber security for SCADA systems as reported by Liu et al. (2012). An overview on the cyber security for electric power control and automation systems is provided by Ten et al. (2007). Power system communication and cyber security are reported as essential parts of a smart grid infrastructure by Ericsson (2010).

The ICT networks are based on TCP/IP and Ethernet for higher speed data exchange at reduced costs. However, the technology is known to be susceptible to IP based attacks. Firewalls and electronic security perimeters are used to enhance the security of SCADA systems and prevent cyber intrusions. However, this widely adopted access control method against intruders does not guarantee cyber security. Misconfiguration of firewalls is a common vulnerability. Even with proper configuration, the vulnerabilities are still not completely removed. For example, an access control method based solely on firewalls cannot detect insider attacks and connections from trusted side. Remote access points to substation Local Area Network (LAN) are used by site engineers, operators, and vendor personnel for maintenance purposes. Accessing IEDs remotely through different technologies, e.g., dial-up, Virtual Private Networks (VPNs), wireless, from locations external to the grid has become a common practice. If not secured properly, they represent vulnerabilities in the SCADA system that can be exploited by attackers as unauthorized access points.

Two major types of attacks on critical systems are identified, i.e., intrusion-based and DoS attacks. The intrusion attack refers to intruders penetrating the ICT networks of one or more critical assets, causing damage to infrastructures by taking undesirable control actions, e.g., operating circuit breakers to create power outages. Cyber security issues are concerned with direct intrusions as well as malware attacks. Machines can be infected with viruses, worms, and Trojan horses that disrupt their normal operation. DoS attacks affect data processing and communication performances through resource exhaustion. They can be conducted by creation of traffic avalanches over short periods of time to overflow buffers and consume communication bandwidth, e.g., packet flooding attack. DoS attacks on control centers and substations can have a serious effect on SCADA and EMS systems, causing a catastrophic disruption of services. Cyber attacks can have a great impact on the grid, which involves dynamic behaviors, loss of load, equipment damage, and partial or total blackouts. A method for assessing the vulnerabilities of SCADA systems and quantifying the impact of cyber attacks was proposed by Ten et al. (2008).

3. DEFENSE AGAINST CYBER ATTACKS

The cyber security research is intended to develop the mathematical and computational foundations for ICTs vulnerability assessment and mitigation. Models of the interdependency between the ICTs and power systems are a key requirement for the successful assessment and enhancement of the cyber-physical system security. Thus, analytical security concepts, methods, and algorithms for the integrated cyber-physical system are needed. Computational testbeds can be used to validate the proposed methodologies.

A research program at University College Dublin (UCD) sponsored by Science Foundation Ireland (SFI) is summarized in Figure 1. It is intended to improve situational awareness against cyber attacks on critical infrastructures. The focus is on developing methods and computer algorithms for ICT vulnerability assessment, cyber attacks prevention and detection by correlating events from various sources, impact analysis on grid operation, and mitigation to alleviate the attack consequences. Four main tasks were identified to enhance the cyber security for SCADA systems, i.e., real-time monitoring, anomaly detection, impact analysis, and mitigation strategies.

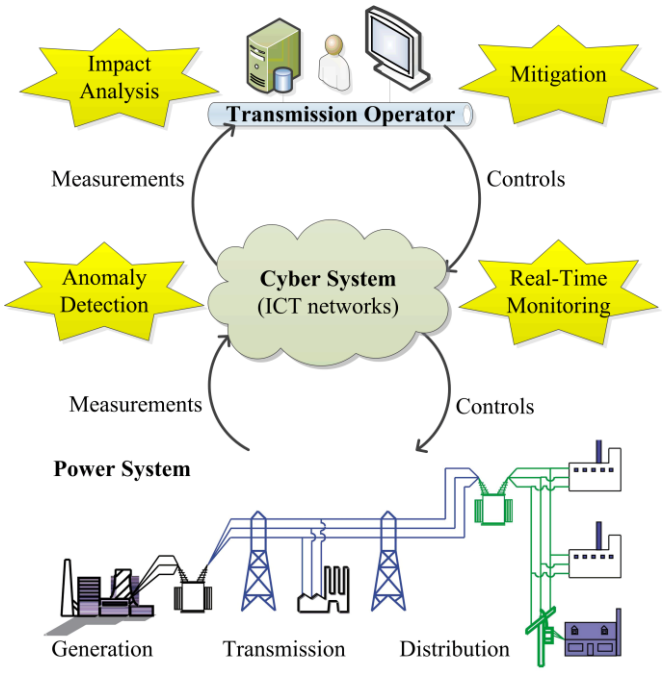

Fig. 1. Cyber-physical system security framework.

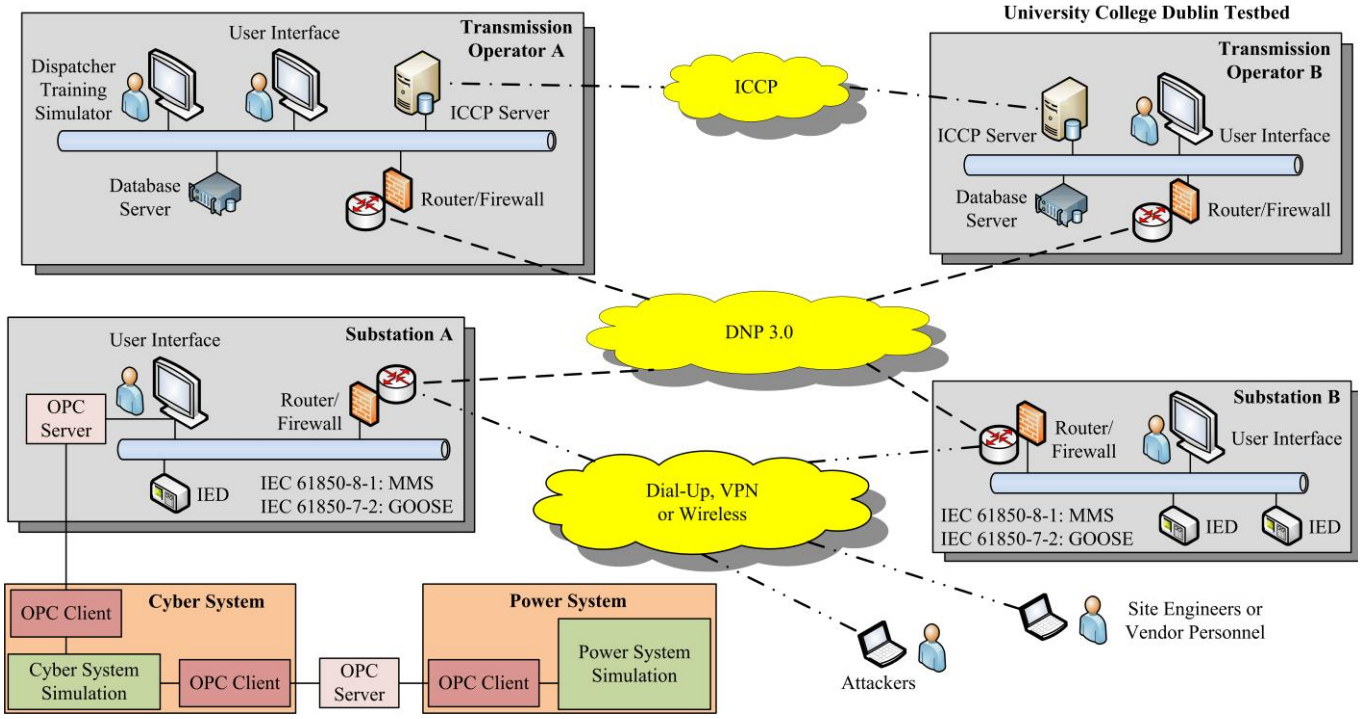

Fig. 2. Cyber-physical security testbed at UCD.

Implementation of computational solutions to secure the cyber-physical system can be evaluated through testbed studies. A SCADA testbed is a critical facility for testing a broad range of cyber attacks and developing real-time defense and recovery strategies to mitigate their effects on power system operating condition. The effectiveness of different security techniques can be analyzed in a realistic environment.

A cyber-physical security testbed has been developed at UCD. It provides an accurate and powerful tool for identification of cyber-physical system vulnerabilities, security enhancement, impact analysis, and mitigation of cyber attacks.

As illustrated in Figure 2, the testbed consists of two transmission operators and two substations. The distributed network protocol DNP 3.0 over TCP/IP is used for controls and measurements between transmission operators and substations. Inter-control Center Communications Protocol (ICCP) is used for data exchange between transmission operators. Bilateral tables define the data that each operator can access. The LANs are protected with router/firewalls, while the user interfaces are secured with authentication and access controls. At the substation level, IEC 61850-based communication is used. The user interfaces and physical IEDs are networked. The power grid is modeled using industrial grade simulation software that allows steady state and dynamic analysis. The user interface is exchanging monitored and control data with the power system simulation environment through Object Linking and Embedding for Process Control (OPC) communications.

Remote access points using wireless, dial-up, or VPN technology serve as legitimate and intrusion paths. However, security controls are in place to protect the substation LANs, i.e., router/firewalls. Only site engineers and vendor personnel have legitimate remote access to the substation ICT networks. Attackers are trying to bypass or circumvent the network access controls and user authentication mechanisms. At transmission operators, the user interfaces are used to monitor and control the operation of the power grid via the SCADA system. They are connected to real-time databases and include the one-line diagram display of the power grid. By running on-line power flow or time domain simulations, measurements and circuit breaker status are sent to the real-time databases and displayed to transmission operators with an update rate. System operators implement control actions and observe the grid's dynamic response.

The testbed capabilities and limitations are presented by Liu et al. (2012). A restraint is the small number of substation communication networks the testbed is able to accommodate due to high hardware and software costs. To address the scalability issue, a computer networks simulator is proposed to be integrated within the testbed. A large number of cyber substations are simulated. The power and communication simulations are synchronized. The OPC protocol enables data exchange between the simulated power and cyber systems using client-server architectures. The OPC servers are mapping the data points between the user interface and cyber and power system simulators which act as OPC clients. Wide area communication networks and large power grids are modeled and co-simulated. The communication and cyber security issues are better investigated. Therefore, integration of software simulation tools within a testbed environment is an effective way to enhance simulation capabilities while reducing the costs.

The testbed provides a realistic model of the cyber-physical system and allows monitoring of interactions between ICTs and power devices. The dynamics of a power grid and its data infrastructure are combined. The result is a cyber-physical system that enables the study of ICT performances,

communication security, and how different events in the SCADA system, e.g., cyber attacks, will affect the grid's operating condition.

Security controls are installed or modeled to protect the ICTs. Their vulnerabilities are assessed. Cyber attacks are conducted or simulated at the cyber system layer, while an impact analysis is performed at the power system layer. The malicious attacks and grid dynamics are simulated with an integrated tool. The vulnerable ICTs of the SCADA system with a large potential impact on the power grid are identified for cyber security enhancement.

4. CYBER ATTACKS AND IMPACT ANALYSIS

Intrusion scenarios into substation LAN can originate from both inside and remote access connections. Table 1 is summarizing potential intrusion scenarios.

Table 1. Cyber intrusion scenarios.

From	Path	To	Method
Outside substation network	Through router/firewall protecting the LAN	IEDs	Bypassing or circumventing the network access controls and user authentication mechanisms by exploiting the existing vulnerabilities
		User interface	
Outside substation network	Through router/firewall protecting the LAN	IEDs	With legitimate access by theft of login credentials of site / vendor engineers
		User interface	
Inside substation network	Through open ports on LAN	IEDs	Physical security breach into substation premises / unhappy employees
		User interface	
Various simulated locations	Diverse ICT paths	Various ICT targets	Simulated cyber intrusions and attacks at the cyber system layer

Experiments on different cyber attacks are conducted with the testbed, e.g., unauthorized access to control assets such as Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs), denial of service by flooding the ICT network, man-in-the-middle by modifying packets carrying measurements and control commands, configuration change of protective relays, etc. The cyber attacks can be directed toward the physical power devices for a direct impact on grid operation, e.g., breakers switching. This is achieved by unauthorized manipulation of RTUs, IEDs or user interfaces at substations once the security controls protecting such assets are defeated. Protective relays are critical devices for system protection. Unlike conventional relays with only local access by serial cable connections, smart relays have network interfaces and are accessed and configured remotely by site engineers. Malicious configuration change of control devices can make a severe impact on grid operation in case of large grid disturbances. Multiple, coordinated, and targeted cyber attacks have a larger impact on system condition than the regular transmission lines tripping caused by faults and misconfiguration of protective relays because of human errors. Power system operation is dependent on a reliable communications infrastructure. The partial or total loss of communications affects the power grid monitoring and control. The target of cyber attacks may be the disruption of SCADA system services. Attackers may generate an avalanche of data packets over the network causing ICTs denial of service. More advanced cyber attacks are the ones directed toward transmission system operators. Attackers modify packets carrying measurements in the man-in-the-middle attack and report fabricated information. The scope is to misguide system operators to take unnecessary control actions. However, the difficulty is to provide enough consistent data and escape the existing mitigation algorithms in the EMS, e.g., state estimator. The feasibility and risk of cyber attacks on power grids are investigated by Sridhar et al. (2012).

Impact analysis quantifies the effects of cyber attacks on the cyber-physical infrastructure. It identifies how much the grid operation is affected and what are the possible short-term and long-term consequences. The cyber-physical security assessment is required to analyze whether the system can survive and recover from cyber attacks. Computer simulations can be used for evaluating the impact of cyber attacks similarly to the contingency analysis for grid security assessment. However, more meaningful simulation results are achieved by considering an integrated model of the cyber-physical system. Cyber attacks are conducted at the cyber system layer against security controls protecting the ICT infrastructure, while time domain simulations are computed at the power system layer. The impact on SCADA system and grid condition is evaluated. Cyber attacks are translated into wide area ICT and grid multiple contingencies that demonstrate severe consequences on the cyber-physical system operation. The SCADA system may experience disruption of services, e.g., communications loss and denial of service. The unauthorized control of RTUs may trip several grid elements. The power system moves from a secure state to an insecure or emergency condition. Stability of the grid can be affected. The impact on the power grid is assessed by monitoring the dynamic behavior of frequency, bus voltage magnitudes, current levels on network elements that cause thermal limit violations, and loss of load. Without proper control, a cascade of events can be initiated, e.g., transmission lines tripping, that finally leads to blackout.

Mitigation actions, e.g., preventive, remedial, and restorative, are required on both cyber and power layers to alleviate the impact of cyber attacks and restore the secure operation of the system. For example, on the ICT side, anomaly-based intrusion detection systems in collaboration with advanced firewalls identify the intrusion and stop the ongoing cyber attack. An algorithm for anomaly detection in the ICT network of a substation was proposed by Ten et al. (2011). The algorithm is extracting malicious "footprints" of intrusion-based steps across the substation network for early detection of cyber-intrusions. Ongoing research is developing computational methods and algorithms to mitigate the risk of cyber attacks against the power grids. At the power layer, mitigation refers to computational algorithms that reconfigure the grid to stop the propagation of cascading events, e.g., wide area protection and control, controlled islanding, power flow readjustment, and voltage control. In case cyber attacks lead to partial or complete blackout, restoration strategies and tools for operator decision support are needed for fast recovery of the cyber-physical system.

Power system blackouts are likely to occur as the electric grids are operated close to their stability limits. Extensive

research has been undergoing on power system restoration. However, cyber-physical system restoration from blackout, caused by cyber attacks, is a particular case. The cyber attacks may damage not only the power grid, but the SCADA system as well. Multiple contingencies, i.e., *n-k*, may have occurred at both cyber and power layers. System operators rely on the SCADA system and various data sources, e.g., substation personnel, power plant operators, and regional coordination service centers, for fast and effective grid restoration from a blackout condition. The restoration process involves communication systems for remote operations, e.g., switching and manoeuvres in the power system, and exchanging information among operators, e.g., extent of required restoration effort, high-level summaries of initial plans, progress being made to recover the generation capacity and transmission facilities. Thus, SCADA and communication systems are critical for the restoration process. They are used to analyze the extent of an outage, implement restoration actions, and continually assess the grid status. In case the SCADA system is not operational, the power system may not be restored. The restoration process cannot be implemented reliably and optimally only by voice communications and manual operation.

After major events that determine both SCADA and power systems to collapse, e.g., cyber attacks, first the SCADA system is partially or fully restored. The process continues with the power grid restoration. Mitigation actions are required at both cyber and power layers to restore the secure operation of the cyber-physical system. Computer methods and algorithms are being developed to support the decision making of system operators for fast and reliable restoration of the integrated cyber-physical system. The toolbox is installed at the transmission operator layer of Figure 1. It is systematically supporting operators to mitigate the disruption of services after cyber attacks and recover the cyber and power systems to a normal operating condition.

5. SIMULATION RESULTS

The power grid used for testing is the IEEE 39-bus system. An intrusion from outside the substation ICT network is considered for simulations. The attacker is circumventing the router/firewall by exploiting the existing configuration vulnerabilities. The networked ICTs are detected. The target is the substation user interface for its control capabilities over the physical devices. The user authentication mechanism is represented by passwords with low entropies. Brute force password cracking provides the unauthorized access. The attacker is sending unauthorized controls to the substation power devices, e.g., triggering open circuit breakers, modify voltage and active power set points or transformer tap positions. The most destructive scenario is considered. The impact analysis results are presented. They capture the dynamic behavior of IEEE 39-bus system as response to the cyber attack which evolves into a partial blackout.

It is assumed that the power grid was at a steady state condition before the attack. The targeted substation includes buses 11, 12, and 13 of IEEE 39-bus system with their corresponding branches as represented in Figure 3, i.e., four transmission lines, two power transformers, and one load. The attacker modified the tap positions of main transformers 11-12 and 12-13 at 20.5 and 23.7 sec, respectively; while transmission lines 6-11 and 10-13 were disconnected at 25 and 28 sec, respectively. The dynamics of the grid are affected and a high impact on grid operation is found. Figure 4 presents the grid's frequency behavior, Figure 5 shows the voltage levels of three nearby generators, Figure 6 the voltage level at bus 12, and Figure 7 presents the active power output of the reference generator.

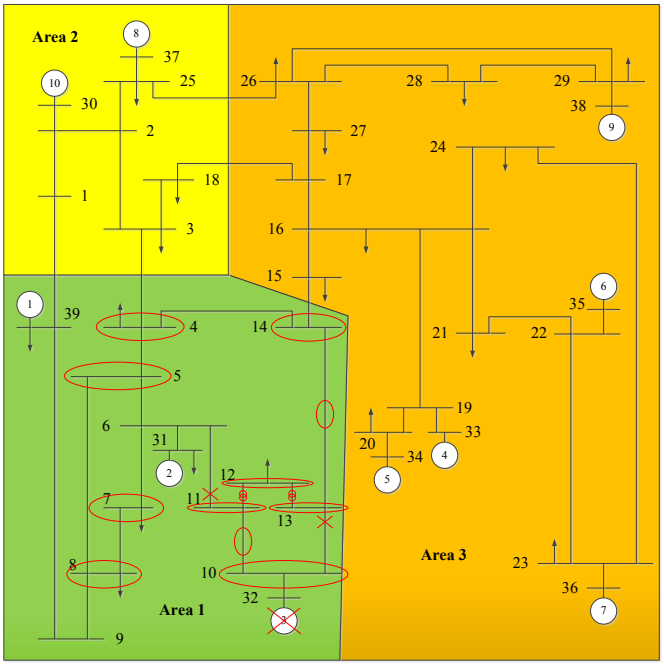

Fig. 3. Impact of the cyber attack on grid operation.

The attacker modified the tap positions of the main transformers causing significant under voltage at bus 12. The voltage level falls from 0.95 to 0.80 p.u. The dynamics show that the grid can absorb the shock caused by the loss of the first transmission line. The grid was secured for *N*-1 contingency criterion. The system's dynamics were affected when the second line was disconnected.

The frequency stays within the admissible range. However, the voltage levels are badly affected. For example, the voltage of bus 12 in the attacked substation is experiencing large excursions as shown in Figure 6. The output of the reference generator presents large variations, see Figure 7. In case the oscillations are not damped, the stability of the grid is affected and its operation becomes critical. Figure 3 shows the impact of the cyber attack on grid operation. Lines 10-11 and 13-14 are overloaded. Buses 4, 5, 7, 8, 10, 11, 12, 13, and 14 experience considerable under voltages. After some time, the over load, under voltage, and frequency deviations lead to undesired events, e.g., generator 3 trips, that initiates cascading events. Finally, the grid is experiencing a partial outage, i.e., area 1 is in blackout.

The attack is mitigated by disconnecting the intruder from the ICT network. System operators use the available resources from areas 2 and 3 and interconnection lines to restore area 1.

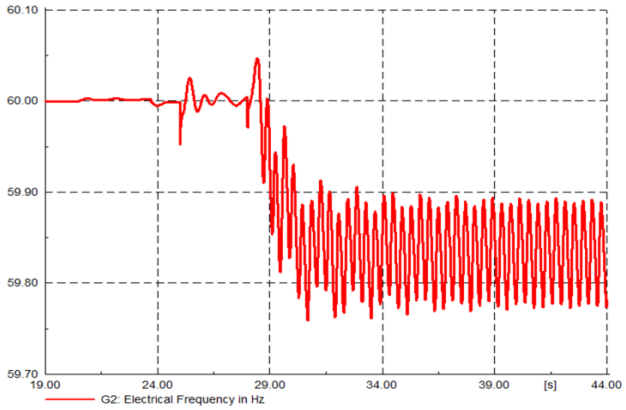

Fig. 4. Frequency variations.

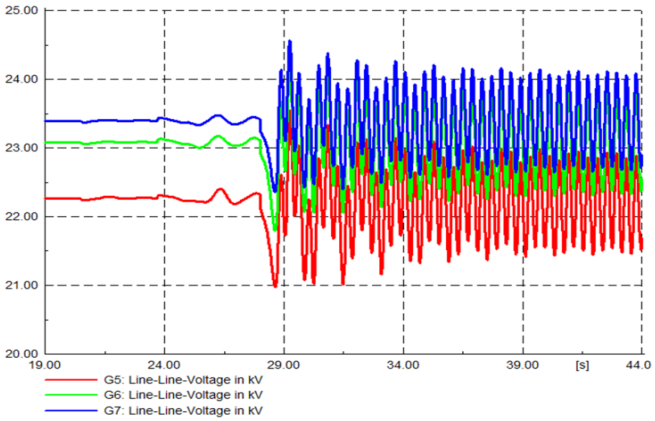

Fig. 5. Voltage variations at buses 34, 35, and 36.

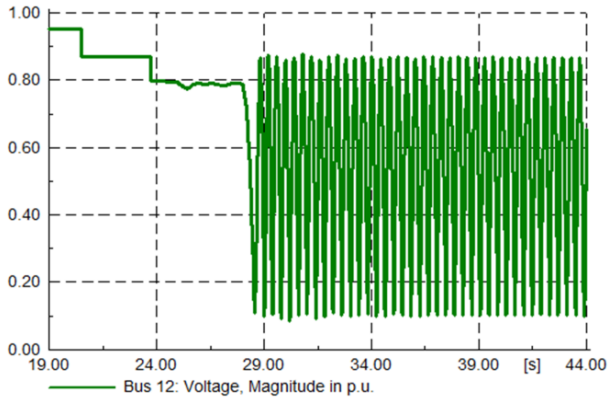

Fig. 6. Voltage variations at bus 12.

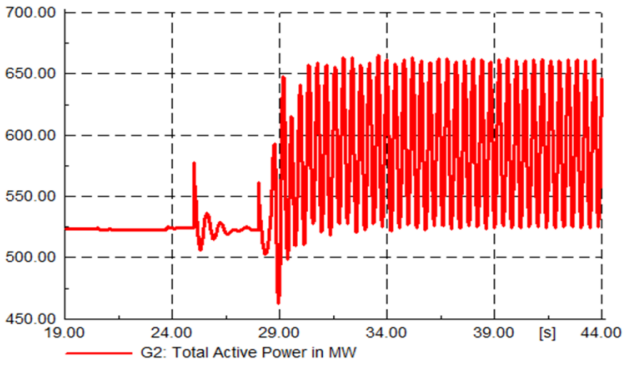

Fig. 7. Active power output of the reference generator.

6. CONCLUSIONS

The paper highlights the importance of cyber security for cyber-physical systems. The EMS/SCADA and protection and control systems in substations become less and less isolated from the ICT system in order to take advantage of the new measurement technologies, e.g., phasor measurement units, and revolutionize the monitoring and control capability of the power grid. To facilitate communications between different entities, while exchanging more information at reduced costs, standardized protocols based on TCP/IP and Ethernet technologies are deployed. The disadvantage is that they introduce security vulnerabilities and are prone to cyber attacks. Intrusions in the substation ICT network have been tested and vulnerability assessment has been performed using the cyber-physical testbed. Simulations of cyber attacks on the SCADA system and power grid show a large impact. The attacks can affect the secure operation of both power and cyber systems. Moreover, they can lead to partial or complete blackout. Computational methods for fast recovery from an extended outage condition after cyber attacks are needed.

ACKNOWLEDGEMENT

This research was supported by Science Foundation Ireland at University College Dublin through a Principal Investigator Award and the follow-on work is partially sponsored by U.S. National Science Foundation, “Collaborative Research: Resiliency Against Coordinated Cyber Attacks on Power Grid.” EECS-1202229.

REFERENCES

Dondossola, G., Garrone, F., and Szanto, J. (2011). Cyber risk assessment of power control systems - a metrics weighted by attack experiments. *Proc. IEEE PES GM*, 1, 1-9.

Ericsson, G.N. (2010). Cyber security and power system communication – essential parts of a smart grid infrastructure. *IEEE Trans. Power Del.,* 25(3), 1501-1507.

Ilic, M.D., Xie, L., Khan, U.A., and Moura, J.M.F. (2010). Modeling of future cyber-physical energy systems for distributed sensing and control. *IEEE Trans. Syst., Man, Cybern. A, Syst,, Humans,* 40(4), 825-838.

Liu, C.C., Stefanov, A., Hong, J., and Panciatici, P. (2012). Intruders in the grid. *IEEE Power Energy Mag.,* 10(1), 58-66.

Metke, A.R., and Ekl, R.L. (2010). Security technology for smart grid networks. *IEEE Trans. Smart Grid,* 1(1), 99-107.

Sridhar, S., Hahn, A., and Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE,* 100(1), 210-224.

Ten, C.W., Liu, C.C., and Govindarasu, M. (2007). Cyber security for electric power control and automation systems. *Proc. IEEE Syst., Man, Cybern.,* 1, 29-34.

Ten, C.W., Liu, C.C., and Govindarasu, M. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Trans. Power Systems,* 23(4), 1836-1846.

Ten, C.W., Govindarasu, M., and Liu, C.C. (2010). Cybersecurity for critical infrastructures: attack and defense modeling. *IEEE Trans. Syst., Man, Cybern. A, Syst,, Humans,* 40(4), 853-865.

Ten, C.W., Hong, J., and Liu, C.C. (2011). Anomaly detection for cybersecurity of the substations. *IEEE Trans. Smart Grid,* 2(4), 865-873.

Wei, D., Lu, Y., Jafari, M., Skare, P.M., and Rohde, K. (2011). Protecting smart grid automation systems against cyberattacks. *IEEE Trans. Smart Grid,* 2(4), 782-795.

Wu, F.F., Moslehi, K., and Bose, A. (2005). Power system control centers: past, present, and future. *Proceedings of the IEEE,* 93(11), 1890-1908.