CONDUCTING CYBER SECURITY STUDIES ON CRITICAL INFRASTRUCTURES

KISS István, Assistant Lecturer,
GENGE Béla, Associate Professor PhD,
HALLER Piroska, Associate Professor PhD,
„Petru Maior" University of Tîrgu Mureş

Abstract: *Critical Infrastructures (CI) are viewed as "systems of systems", which normal operation should not be accidentally or deliberately interrupted by unauthorized actors. In the category of CI we can enumerate energy transportation and distribution networks, energy production plants, chemical plants, etc. Nowadays, modern CI increasingly integrate off-the-shelf Information and Communication Technologies (ICT). Once using off-the-shelf ICT equipment, CI are exposed to cyber threats targeting the physical layer of these systems. In this paper we propose two slightly different frameworks designed to be used by cyber security experts in security stress studies of CI. Moreover, using the developed frameworks experts can perform studies using real ICT software and hardware combined with the simulated physical layer. The effectiveness of the frameworks is demonstrated on the IEEE 14-bus electricity grid model and on the Tennessee Eastman chemical plant.*

Keywords: *critical infrastructure security, cyber-physical security, cyber attacks, power grid.*

Introduction

Critical Infrastructures are complex cyber-physical systems in which the pervasive adoption of commodity, off-the-shelf Information and Communication Technologies (ICT) caused a significant reduction of costs and paved the way towards greater flexibility, efficiency and interoperability between components. In the past, CI were perceived as closed environments and comprised of proprietary hardware, software and protocols. However, nowadays, the dramatic shift from a completely isolated environment to an open, "system of systems" integration with traditional ICT systems raises serious concerns on the security of CI. By leveraging attack vectors that are commonly found in traditional computer systems, e.g., phishing and USB key infections, malware aimed at the disruption of CI have become effective cyber weapons [1]–[3]. Stuxnet [1], [2], the first malware specifically designed to attack the Industrial Control Systems (ICS) of CI, is generally acknowledged as the turning point of the way that ICS security is seen today. Stuxnet, together with the more recently reported cyber espionage weapons such as Duqu [4],

Flame [3], and Dragonfly [5], continue to raise many open questions, but they also confirm serious concerns about the capabilities and the objectives of future malware.

Based on the aforementioned issues, in this work we tackle with the problem of performing realistic cyber security experiments on ICS coupled with CI. Obviously, on-line experiments in the presence of critical processes have been excluded due to safety reasons. In turn we developed two frameworks to make possible cyber security studies with real ICT hardware and software, but with simulated physical processes. To be realistic we employ the widely used IEC 61850 [6]–[8] substation automation protocol. Furthermore, we analyzed the architectures described in NIST SP 800-82 [9] to bring the developed frameworks closer to the industry. Accordingly, the first framework extends AMICI, i.e. CI assessment framework proposed by Genge et al. in [10], with the IEC 61850 communication protocol. Using this framework, one can conduct security studies on CI modeled in Matlab, e.g. the Tennessee Eastman chemical process. In contrast, the second framework proposed in this paper is intended to conduct studies on electricity grids modeled by the PSAT toolbox [11].

Finally, experimental studies have been conducted on the IEEE 14-bus electricity grid and the Tennessee Eastman chemical plant to show the effectiveness and usability of the techniques. In these studies we have emulated some popular cyber attacks, i.e. DoS-like attacks and integrity attacks.

The remaining of this paper is structured as follows. The first section provides a brief overview of the related work. The CI and the targeted infrastructures are described in the second section. Then, in the third section the proposed frameworks are presented and demonstrated in the section of cyber security studies.

Related Work

There have been numerous efforts to make cyber security experiments more straightforward in the context of CI. In this section we discuss several of them and their relation with our frameworks. Liu et al. [12] proposed a technique for modeling the cyber attacks that compromise switching devices of the electricity grid. The approach uses variable structure theory to model the interaction between cyber and physical layer. Finally, the authors demonstrate their findings on the WECC 3-GENERATOR (Western Electricity Coordinating Council 3-machine) 9-bus system. Another work written by Teixeira et al. [13] introduces some high level attack models, i.e. replay attack, zero dynamics attack and integrity attack. Attack scenarios similar to these models will be reproduced later in this work using the experimentation frameworks. By

assuming that cyber attacks influence the control loops, Kundur et al. [14] proposed a graph-based model to evaluate the influence of control loops on a physical process.
In the category of simulation frameworks, Guo et al. [15] developed a real time simulation platform which takes into account the communication infrastructure as well as the electrical infrastructure of the electricity grid. The platform is best suited to simulate microgrids and does not consider the effects of cyber attacks. Consequently, Siaterlis et al. [16] designed a testbed named EPIC for cyber-physical security experimentation. Similarly, Genge et al. in [10] proposed a platform for security experimentation conducted on interdependent CI. The industrial communication protocol used in this work is Modbus over TCP. The platform is experimentally applied against a power grid coupled with a railway system. Especially, our first framework complements AMICI with the modern and widely adopted IEC 61850 communication protocol and employs it for performing experiments on the Tennessee Eastman (TE) chemical plant.
Therefore, the approaches presented in this work can be used as complement tools for security-aware network design [17], cyber attack impact assessment [18], [19] and for studying stealthy cyber-physical attacks [20].

Modern Critical Infrastructures

As an overview we considered the typical architecture of CI. According to Fig. 1, the ERP (Enterprise Resource Planning) of the company performs the high level coordination of CI. An IT infrastructure interconnects ERP with lower level SCADA systems and ICS (Industrial Control Systems). Obviously human operated high level resource planning software applications are in connection with SCADA and local ICS through the IT infrastructure. Furthermore, sensor and actuator devices maintain the connection between physical process parameters and local controller devices (PLC, RTU).

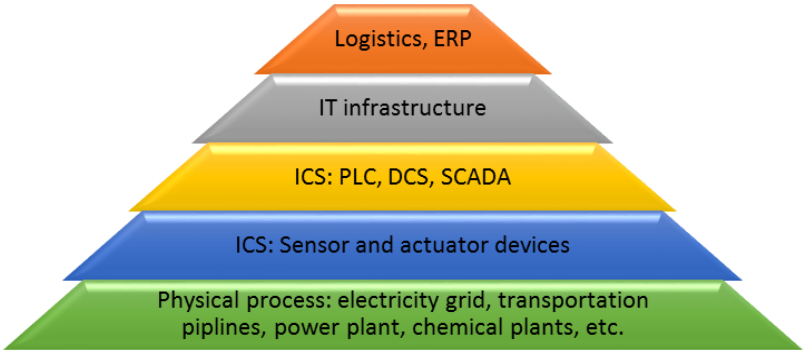

Fig. 1 Hierarchical structure of modern CI

Essentially, CI has two basic layers: (i) the physical layer, including the physical equipment and the physical part of sensor and actuator devices and (ii) the cyber layer, which encompasses the cyber part of sensor and actuator devices and all of the ICT hardware and software installed to monitor and control the physical processes. Physically, there are situations when the infrastructure is spread over large geographical areas, which motivates the existence of remote locations connected to the cyber layer via wide area communication lines.

From an operational point of view, on-site controllers perform local actuation strategies at the level of each remote location. These local controllers are also in connection with regional and national Supervisory Control and Data Acquisition (SCADA) servers and operator stations. They also receive data from sensors and send commands to the actuator devices according to the set-points defined by SCADA operators. Consequently, the operation of CI depends on sensor/actuator devices and the data communication between them and SCADA servers. The transferred data between devices enclose *observed* and *control* variables, corresponding to sensor and actuator devices respectively.

As all of the cyber layer devices are part of the communication infrastructure, by making use of security lacks, the adversary is able to manipulate original measurements and send malicious data to supervisory servers or by compromising control variables, he can also issue malicious commands to the actuators. As a consequence, in order to ensure the security of critical devices we need to be able to conduct security studies on CI.

Cyber security experimentation frameworks

Mainly, we propose two frameworks to cover the differences between geographically distributed CI, e.g. power grids and CI placed in a restricted area, e.g. power plants, chemical plants.

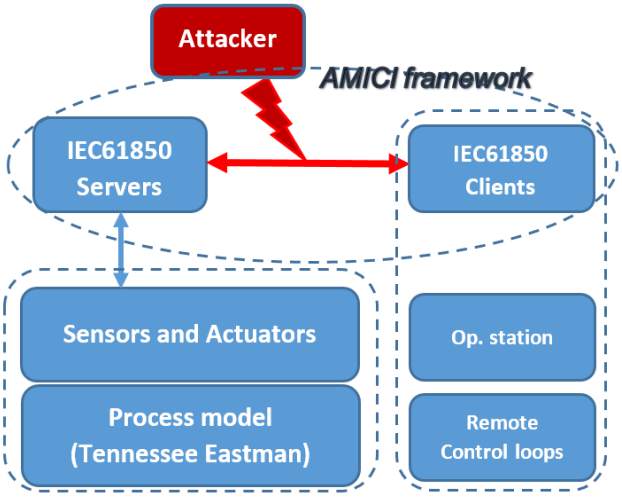

Fig. 2 AMICI extended with IEC 61850

The platform of AMICI [10] approaches the interdependencies between multiple CI. In contrast the first framework described in this work adopts the main architecture of AMICI and complements it with the IEC 61850 protocol. In this manner we intend to use the framework in conducting cyber security studies on chemical plants as well as power plants and any other processes that can be modeled similarly. On the contrary, power grids represent a huge sector of CI, therefore to solve the issues of accurate modeling, in the second framework we present a platform that enables security experimentation on electrical grids simulated using the PSAT toolbox [11] available in Matlab.
On the other hand, in the place of real physical infrastructure the frameworks consider simulated, but realistic processes. Furthermore, the frameworks can easily be extended to recreate real ICT infrastructures used in CI, thus ensuring reliable security studies.

AMICI extended with IEC 61850

Fig. 2 gives an illustration of the framework. The cyber threats are supposed to disturb the communication lines between sensor and actuator device's IEC 61850 server and IEC 61850 clients. The devices that are compatible with the IEC 61850 are often referred as IED (Intelligent Electronic Devices). According to the figure, the sensor and actuator values are being generated by the process simulation model and are tied to IED servers. In practice these servers are integrated in each IED. On the other side IED clients are ready to read the server values and to set the setpoint variables. Among IED clients there can play role devices of an operator station, e.g. SCADA servers or even these clients can serve as actors of remotely implemented control loops. In the

implementation of this framework we employed the libIEC61850[1] open-source library. In case of Tennessee Eastman chemical process the process itself takes place in the server and the control actions are made via IED clients. Once the framework started, the communication line signaled with red in Fig. 2 will be "full" of measurement and setpoint values transferred in each sample time between IED server and client.

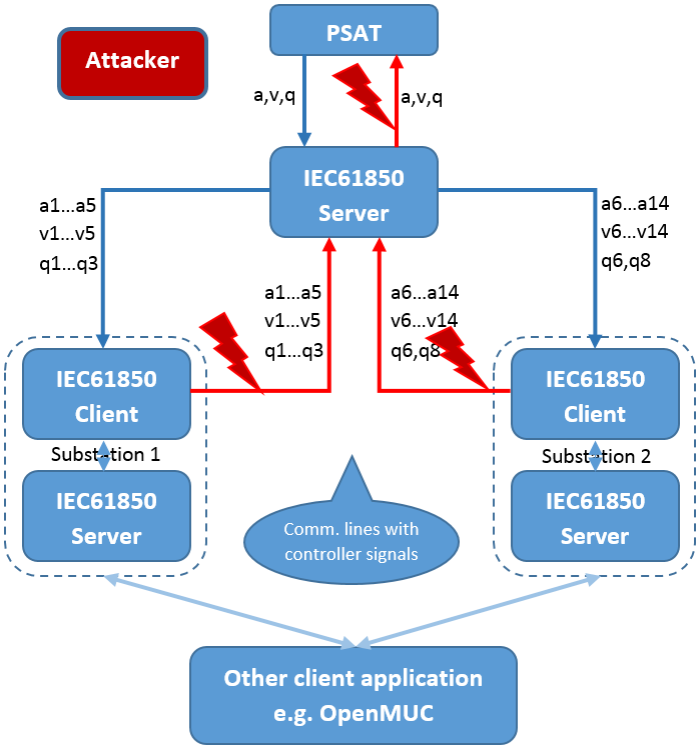

Fig. 3 The framework combining PSAT and IEC 61850

Through this scenario the study of cyber attacks that target communication lines between devices and thus the analysis of the effects of cyber attacks on the physical process become straightforward.

A framework combining PSAT and IEC 61850

Technically, this framework is based on the OpenIEC61850[2] open source java implementation of the protocol. We maintained the open source nature of the framework, therefore the components of Fig. 3 all are implemented using open-source java implementations except PSAT which runs in Matlab. For the connection between PSAT and IEC server we have employed the

[1] http://libiec61850.com/libiec61850/

[2] https://www.openmuc.org/index.php?id=24

Matlabcontrol API[3], which uses MatlabProxy to make possible read and write operations across Matlab variables.

The scope of the framework is to firstly distribute the measured values and the controller signals present in the PSAT environment. Basically, as the Fig. 3 shows, the framework separates the grid's buses into two or more substations which will then send back and receive values from PSAT. Nevertheless, the measurement variables used for central area controller (CAC) are distributed across the substation machines and then resent via the IEC server to PSAT. In this way, practically we have separated the CAC module from PSAT, and everything happens via communication lines. Furthermore, real widely used software applications, e.g. OpenMUC[4], can be connected to the substation machines to emulate a complete industrial environment. Red communication lines in the figure are exposed to cyber threats and the cyber security studies are to be made on these channels.

The framework is heavily based on the PSAT simulation environment, which enables a large variety of power grid experiments starting from microgrids to high scale electrical grids, e.g. 300-bus system. From an operational view the signals corresponding to the case study, i.e. IEEE 14-bus grid, and transmitted via IEC61850 communication channels are the following:

- a – Phase angles.
- v – Voltages.
- Vpilot – Pilot bus – input of CAC controller (bus 13)
- q – Power values – the outputs of central area controller (CAC) and the inputs of cluster controllers (CC).
- Substation 1 includes buses 1, 2, 3, 4, 5
- Substation 2 includes buses 6, 7, 8, 9, 10, 11, 12, 13, 14

It has to be noted that there can be added more than two substation machines to emulate the real industrial network. Once started, the framework is a suitable environment for testing the effects of cyber attacks on the underlying electricity grid.

Cyber security studies

As resulted from the frameworks we plan to perform experimentation on communication line disturbances, i.e. cyber attacks. Following is a short overview of cyber threats that can be considered and tested with the proposed frameworks:

- Disturbing the communication services: measurement loses, control signal delays.

[3] https://code.google.com/p/matlabcontrol/

[4] https://www.openmuc.org/

- Taking control over the physical process.
  - Sending malicious commands.
  - Manipulating measurements.
  - Altering databases.
  - Man-in-the-Middle attacks.

Just for illustration, there are many publicly available powerful tools to elaborate such complex cyber attacks, e.g.: nmap. dsniff, tcpkill, arpspoof, dnsspoof, macof, scapy, sshmitm, webmitm, etc.

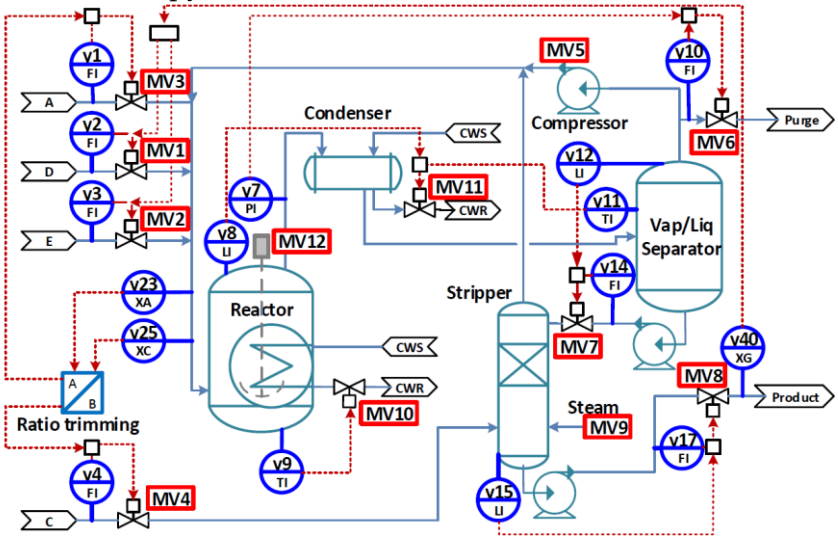

Fig. 4 The Tennessee Eastman chemical process instrumentation diagram

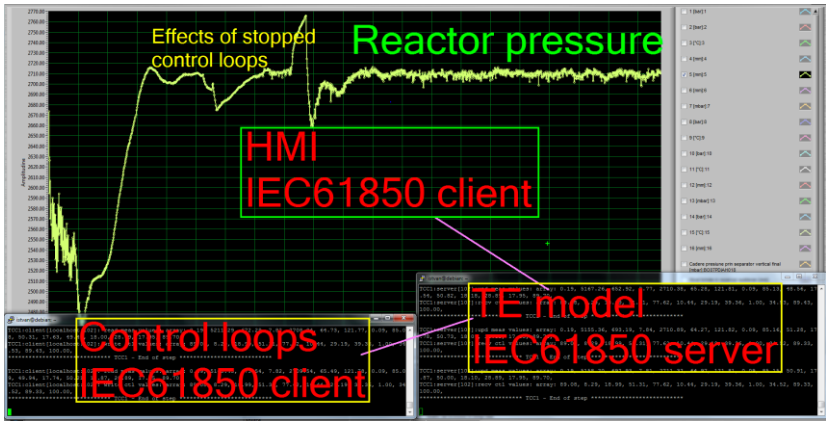

Fig. 5 Experimentation view – attacks that disturb control loops' operation

Therefore, in security studies we can use these already available tools, which with big chances are also used by the adversary in case of real cyber attacks.

In this section we employ the developed frameworks in the security experimentation with two slightly different CI. The first one is the TE chemical plant and the second one is a 14-bus electricity grid.

Case study of TE process

We adopt the model of the TE chemical process [21], that includes 12 control input variables (denoted with MV in Fig. 4), 41 observed output variables (denoted with Y in Fig. 4) and 50 internal states. The corresponding piping and instrumentation diagram of TEP together with the critical control loops are illustrated in Fig. 4. Briefly, TEP builds on 5 main industrial equipment, i.e. reactor, condenser, stripper, vapor/liquid separator and compressor. Each equipment requires an automated control loop structure for the stable operation to be maintained.

We reproduce the effects of cyber attacks by using the proposed framework. In more detail, by using the first framework we separate the control loop structure from the chemical process itself. Through this way, the measured and control variables are transferred via communication channels, thus one can study the effects of cyber attacks on measured (observed) variables as well as on control variables

By starting the framework we'll be provided with a real time graph containing the evolution of each process variable. The malicious effects of the attacks are instantaneously viewed on these waveforms. Accordingly, Fig. 5 presents the evolution of reactor pressure around the moment when the IEC client which serves as controller has been stopped by some means of cyber attacks.

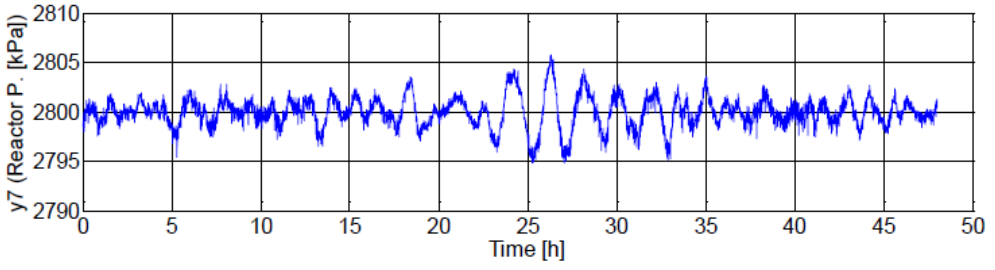

Fig. 6 Effects of interrupted blocking attacks of comm. lines

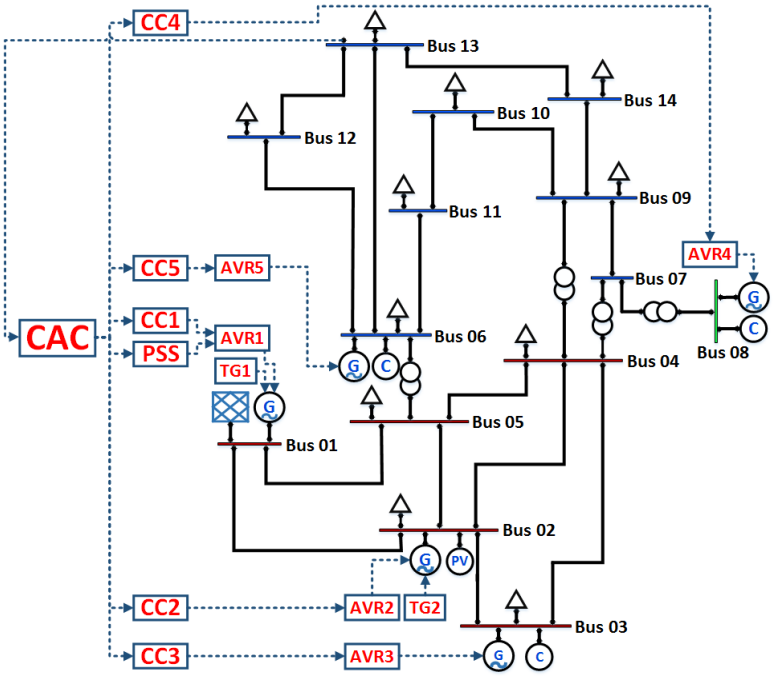

Fig. 7 IEEE 14-bus electrical grid

As a result the reactor pressure increases dramatically until the controllers come back to work. This is a dangerous situation in which the process could enter the emergency shutdown procedure in a relatively small amount of time. On the contrary, if the attack is terminated, the process comes back to a normal operation state which is shown by the stabilization of the pressure value in Fig. 5.

Moreover, in Fig. 6 the effects of interruptedly delivered cyber attacks are shown on the reactor pressure variable. The attacks start in the moment of *20 h* and end in *30 h*. There is a clear evidence of the DoS attacks that disturb the delivery of control variables to the actuators of the chemical process.

Further exhaustive cyber security studies can be made using the proposed framework together with various cyber attack techniques.

Case study of IEEE 14-bus electrical grid

In this section we apply the second framework to the IEEE 14-bus test system. We then conduct experiments with TCP reset and integrity attacks.

The electrical topology, the substations (buses), the electrical line breakers and the governing controllers of the IEEE 14-bus grid are presented in Fig. 7. Additionally, our test grid is enriched with power grid (PG) specific control devices, i.e., Central Area Controller (CAC), Cluster Controllers (CC),

Automatic Voltage Regulator (AVR), Turbine Governor (TG), Power System Stabilizer (PSS). These controllers modify the behavior of PG and make it more realistic and suitable for the experiments to be conducted on.

In this study we use the second framework to separate the central area controller part from the power grid model. Once separated and the key measurements are spread across emulated substations, the framework is ready to be exploited. In the first instance we set up a long term cyber attack-free experiment to verify if everything goes well. A preview of this verification is shown in Fig. 8, on a reduced time interval of *100 s*.

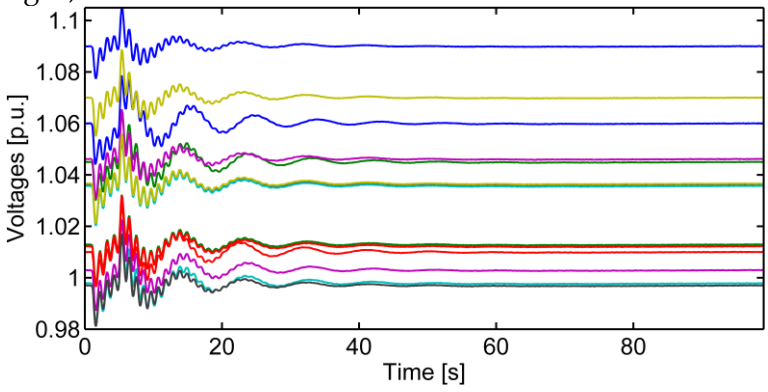

Fig. 8 Normal operation with load variations

The figure shows the voltage evolution over time for the 14 electrical buses. Additionally at the beginning of the simulation there is a predefined load disturbance to illustrate the stabilizing effects of the controllers. More specifically, the overall power grid enters to work in a steady state mode after the time of *20 s*.

In Fig. 9 in turn, we present a more meaningful study, where in the presence of normal load variations (current consumption) a series of integrity attacks disturb the communication between IED. In detail, the integrity attack requires a Man in the middle (MITM) attack scenario to be able to manipulate the transmitted measurement values. Practically, in our experiments the IEC 61850's MMS packets are tampered and the corresponding measurement values are then replaced with fake values. It is shown on the figure where the integrity attacks begin and where exactly they end. There is a clear evidence of the attacks in the bus voltage behavior, and additionally it can be noticed how the first attack starts at around the moment of *58 s*, stops at around *70 s*, then it restarts and finally one more time restarts until the end of the attacks at around *115 s.* It has to be noticed the fact that the controllers fail to work in the presence of successful attacks and as a consequence the bus voltages are dropped below *0.8 p.u.*, which is an unacceptable state and it's the same as

blackout or voltage collapse. Obviously, if the attack ends before voltage collapse, then the controllers bring back the grid to steady state normal conditions (see Fig. 9). As a result of the study we notice how the attack disturbs the normal behavior of the grid, thus significantly reducing the grid performances. Moreover, similarly to the above experiments, security experts are able to perform various exhaustive cyber security studies on CI (as one presented in [20]).

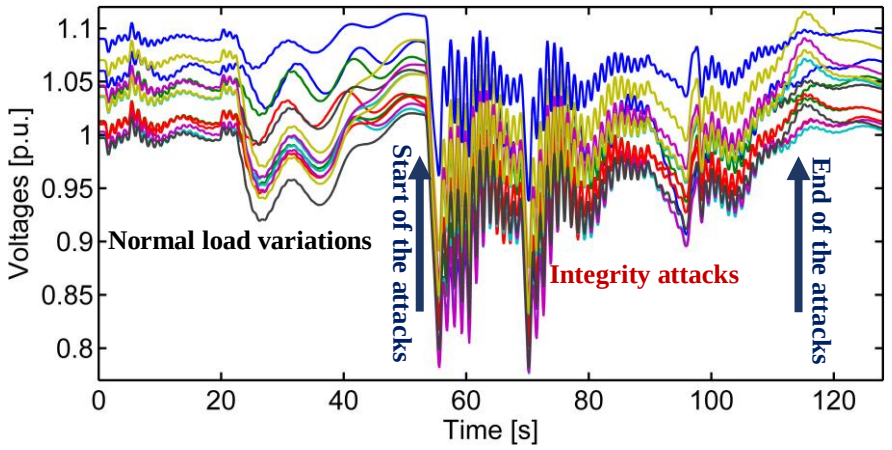

Fig. 9 Effects of integrity attacks on bus voltages

Conclusions

We proposed two frameworks, especially one for cyber security study of industrial plants and another one for security experimentation with large scale electrical grids. The IEC 61850 widely used industrial protocol has been attacked for demonstration purposes. More specifically it was shown how the reactor of the Tenneessee Eastman process behaves different in the presence of disturbing cyber attacks. And similarly it was shown how the bus voltages of the IEEE 14-bus system behave anomalously when integrity attacks target the IEC 61850 protocol. The results show the effectiveness of the frameworks in studying the effects of cyber attacks on the normal operation of the physical equipment in CI.

Acknowledgment

This work was supported by a Marie Curie FP7 Integration Grant within the 7th European Union Framework Programme (Grant no. PCIG14-GA-2013-631128).

References

[1] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, Apr. 2011.

[2] M. Hagerott, "Stuxnet and the vital role of critical infrastructure operators and engineers," *Int. J. Crit. Infrastruct. Prot.*, vol. 7, no. 4, pp. 244–246, 2014.

[3] B. Bencsáth, G. Pék, L. Buttyán, and M. Felegyhazi, "sKyWIper (aka Flame aka Flamer): A complex malware for targeted attacks," *CrySyS Lab Tech. Rep. No CTR-2012-05-31*, 2012.

[4] "W32.Duqu: The Precursor to the Next Stuxnet," *Symantec Security Response*. [Online]. Available: http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

[5] "Dragonfly: Western Energy Companies Under Sabotage Threat," *Symantec Security Response*. [Online]. Available: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat.

[6] I. Ali, M. S. Thomas, S. Gupta, and S. M. Hussain, "IEC 61850 Substation Communication Network Architecture for Efficient Energy System Automation," *Energy Technol. Policy*, no. just-accepted, 2015.

[7] N. Higgins, V. Vyatkin, N.-K. C. Nair, and K. Schwarz, "Distributed power system automation with IEC 61850, IEC 61499, and intelligent control," *Syst. Man Cybern. Part C Appl. Rev. IEEE Trans. On*, vol. 41, no. 1, pp. 81–92, 2011.

[8] G. Zhabelova and V. Vyatkin, "Multiagent smart grid automation architecture based on IEC 61850/61499 intelligent logical nodes," *Ind. Electron. IEEE Trans. On*, vol. 59, no. 5, pp. 2351–2362, 2012.

[9] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," *NIST Spec. Publ.*, vol. 800, p. 82, 2014.

[10] B. Genge, C. Siaterlis, and M. Hohenadel, "Amici: An assessment platform for multi-domain security experimentation on critical infrastructures," in *Critical information infrastructures security*, Springer, 2013, pp. 228–239.

[11] L. Vanfretti and F. Milano, "Experience with PSAT (Power System Analysis Toolbox) as free and open-source software for power system education and research," *Int. J. Electr. Eng. Educ.*, vol. 47, no. 1, pp. 47–62, 2010.

[12] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," 2013.

[13] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack Models and Scenarios for Networked Control Systems," in *Proceedings of the 1st International Conference on High Confidence Networked Systems*, New York, NY, USA, 2012, pp. 55–64.

[14] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," in

2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 244–249.
[15]F. Guo, L. Herrera, R. Murawski, E. Inoa, C.-L. Wang, P. Beauchamp, E. Ekici, and J. Wang, "Comprehensive real-time simulation of the smart grid," *IEEE Trans. Ind. Appl.*, vol. 49, no. 2, pp. 899–908, 2013.
[16]C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation," *IEEE Trans. Emerg. Top. Comput.*, vol. 1, no. 2, pp. 319–330, Dec. 2013.
[17]Bela Genge, Piroska Haller, and Istvan Kiss, "Cyber Security-Aware Network Design of Industrial IoT Systems," *IEEE Syst. J. Spec. Issue Ind. IoT Syst. Appl.*
[18]B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures," *Int. J. Crit. Infrastruct. Prot.*, vol. 10, pp. 3–17, Sep. 2015.
[19]I. Kiss, B. Genge, and P. Haller, "Behavior-based critical cyber asset identification in Process Control Systems under Cyber Attacks," in *Carpathian Control Conference (ICCC), 2015 16th International*, 2015, pp. 196–201.
[20]Istvan Kiss, Bela Genge, Piroska Haller, and Gheorghe Sebestyen, "A Framework for Testing Stealthy Attacks in Energy Grids," in *2015 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, Cluj Napoca, 2015. *(To appear)*
[21]J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem," *Comput. Chem. Eng.*, vol. 17, no. 3, pp. 245–255, 1993.
[22] N. Lawrence Ricker, "Decentralized control of the Tennessee Eastman Challenge Process," *J. Process Control*, vol. 6, no. 4, pp. 205–221, Aug. 1996.