Proceedings of the Federated Conference on Computer Science and Information Systems pp. 767–773
DOI: 10.15439/2016F164
ACSIS, Vol. 8. ISSN 2300-5963

Cyber Security Impact on Power Grid Including Nuclear Plant

Yannis Soupionis, Roberta Piccinelli and Thierry Benoist
European Commission, Joint Research Centre (JRC)
Institute for the Protection and Security of the Citizen (IPSC)
Security Technology Assessment Unit (STA)
Via E. Fermi, 2749, 21027 Ispra, Italy
Email: yannis.soupionis, roberta.piccinelli, thierry.benoist @jrc.ec.europa.eu

***Abstract*—Decentralized Critical infrastructure management systems will play a key role in reducing costs and improving the quality of service of industrial processes, such as electricity production. The recent malwares (e.g. Stuxnet) revealed several vulnerabilities in today's Distributed Control Systems (DCS), but most importantly they highlighted the lack of an efficient scientific approach to conduct experiments that measure the impact of cyber threats on both the physical and the cyber parts of Networked Critical Infrastructures (NCIs). The study of those complex systems, either physical or cyber, could be carried out by experimenting with real systems, software simulators or emulators. Experimentation with production systems suffers from the inability to control the experiment environment. On the other hand the development of a dedicated experimentation infrastructure with real components is often economically prohibitive and disruptive experiments on top of it could be a risk to safety. In this paper, we focus on the implementation of a Cyber-Physical (CP) testbed which includes physical equipment. We illustrate and the cyber security issues on the communication channel between the Critical Infrastructures(CIs), such as a power grid, a nuclear plant and the energy market. We simulate the power grid network (including nuclear plant), but we emulate the Information and Communications Technology (ICT) part which is the focus of our work. Within this context we assume that we are able to implement scenarios, which produce consequences on the normal operation of the power power grid and the financial area.**

***Index Terms*—Networked Industrial Control Systems; Cyber security; Cyber physical system; power grid; power market; Nuclear plant;**

I. Introduction

EUROPEAN security, both physical and economic, rests upon a foundation of highly interdependent critical infrastructures. A critical infrastructure [1] refers to an asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, such as health, safety, security, economic or social well-being of people. The disruption or destruction of such infrastructures would have a significant impact on a Member State as a result of the failure to maintain these functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact on the security of the EU and the well-being of its citizens [2].

Given the lack of practical experience with massive infrastructure failures, modeling a multi-CI testbed is highly crucial. Interdependencies between CIs are similarly highlighted in numerous technical publications [3][4][19][20]. The underlying technical theme is that modeling and designing of critical infrastructures must take a holistic, systemic perspective and incorporate interdependencies. In this paper, we examine the complexity of the infrastructure interdependency and highlight the relevant cyber security impact.

In the past, CIs were isolated environments and used proprietary hardware and protocols, thus limiting the threats that could affect them. Nowadays, CIs or more accurately Distributed Control Systems (DCS) are exposed to significant cyber-threats; a fact that has been highlighted by many studies on the security of Supervisory Control And Data Acquisition (SCADA) systems [5], [6], [7].

In this paper, we explore the complexity of the infrastructure interdependency security issues and we design a testbed (Fig. 1), which combines:

- simulated physical infrastructures (e.g. power grid and nuclear plant),
- simulated power stock market,
- emulated ICT controlling infrastructure, and
- real physical equipments, i.e. Programmable Logical Controllers (PLCs).

Based on this implementation, the Network & Information Security Laboratory (NIS Lab) created a cyber-physical system/prototype in order to underline and motivate the need for modeling multiple interconnected critical infrastructures, since the behavior of an interconnected one can be propagated. We discuss the implementation of the testbed and illustrate a possible attack scenario, which shows that network anomalies can produce financial and power disturbances.

The paper is structured as follows. Our study is presented in the context of other related approaches in Section II. In section III we show in detail our experimentation infrastructure and its elements. The experimental scenarios and setup are presented in Section IV. Conclusions are presented in Section V.

II. Related Work

Recent events such as Stuxnet [8], Duqu [9] and Flame [10], caused the scientific community to address cyber security concerns regarding CP systems. In this section we provide a brief presentation of the most relevant approaches addressing

978-83-60810-90-3/$25.00

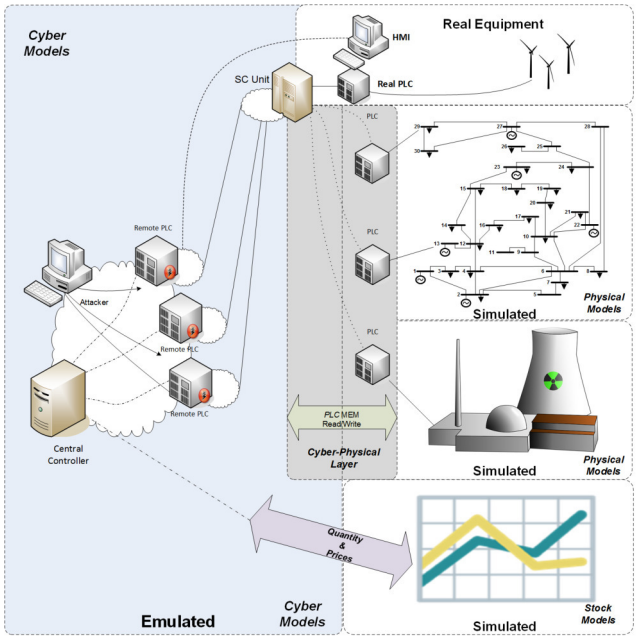

Fig. 1: Experimentation framework architectural overview

the resilience of cyber physical systems, which take into consideration both the communication infrastructure and the control of physical processes.

Nai Fovino *et al.* [18] proposed an experimental platform to study the effects of cyber attacks against NICS. In their paper the authors described several attack scenarios, including DoS attacks and worm infections that send Modbus packets to control hardware. Although the authors provided a wide range of countermeasures, they did not however identify communication parameters that affect the outcome of the attacks. They took into consideration the skills and efforts required by the attacker, as was the case of Stuxnet, where developers also had knowledge of the PLC code, OS and hardware details.

An approach where a cyber physical system is tested for cyber events, has been proposed by Hahn *et al.* [12]. They offer a high level overview of testbed functionality, including its control, communication, and physical components along with a mapping of components to research requirements. Additionally, Yardley *et al.* [13] propose that complex cyber-physical systems like the ones found in the smart grid require a combination of methodology, quantification, and testbed environments to drive tool creation to assist in the evaluation of the systems under test. They present an approach to security testing methodology and illustrate the use of testbeds in developing tools for cutting-edge systems. Both papers highlight the issue but they do not integrate additional infrastructures in order to show the interdependency issues.

Finally, a similar experiment has also been documented by Davis, *et al.* [14] that used the PowerWorld server to study the effects of communication delays between the physical process and human operators.

III. Experimentation Framework Overview

The experimentation framework developed in our previous work [16] follows a hybrid approach, where the Emulab-based testbed recreates the control and process network of NICS, including Programmable Logical Controllers (PLCs) and SCADA servers, and a software simulation reproduces the physical processes.. The main two elements of our laboratory are:

- an experimental platform for resilience, security and stability research, called Experimental Platform for Internet Contingencies (EPIC) [11], which supports the security assessment of cyber-physical systems. The EPIC test-bed can efficiently recreate realistic network topologies and conditions (e.g. delay and loss characteristics of Wide Area Network - WAN links) of the Internet infrastructure.
- a physical system simulator, called the Assessment platform for Multiple Interdependent Critical Infrastructures (AMICI)[16], which can simulate in real time critical physical infrastructures, e.g. a power grid, and can interact with the emulated network test-bed.

The architecture of EPIC suggests the use of an emulation testbed based on the Emulab software [11] in order to recreate the cyber part of NCIs, e.g., servers and corporate network, and the use of software simulation (AMICI) for the physical components, e.g., power grid and nuclear plant.

A. The controlling ICT network

The cyber layer is recreated by an emulation testbed that uses the Emulab architecture and software [17] to automatically and dynamically map physical components (e.g. servers, switches) to a virtual topology. In other words, the Emulab software configures the physical topology in a way that it emulates the virtual topology as transparently as possible. This way we gain significant advantages in terms of repeatability, scalability and controllability of our experiments.

Besides the process network, the cyber layer also includes the control logic code, that in the real world is implemented by PLCs. The control code can be run sequentially or in parallel to the physical model. In the sequential case, a *tightly coupled* code (TCC) is used, i.e. code that is running in the same memory space with the model, within the SC unit. In the parallel case, a *loosely coupled* code (LCC) is used, i.e. code that is running in another address space, possibly on another host, within the *R-PLC* unit (Remote PLC). The cyber-physical layer incorporates the PLC memory, seen as a set of registers typical to PLCs, and the communication interfaces that glue together the other two layers.

In Fig. 2, we illustrate the emulated cyber-part of our experimental setup. Each simulation of the physical processes runs at a different host. Moreover, in conjunction with Fig. 1 (i) the simulation of the main power grid is running on the lower right part of the network, (ii) the PLC is connected on the upper right, (iii) the power market on the upper left, and (iv) the nuclear plant on the left lower part. All these simulated infrastructures communicate though the ICT network .

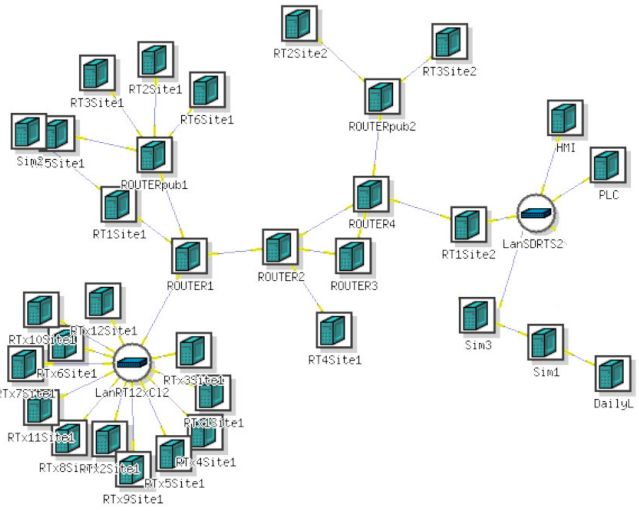

Fig. 2: The EPIC network topology for the specific implementation taken directly from Emulab's web interface.

B. Description of Nuclear Plant

In this section we present our simplified Pressurized Water Reactor (PWR). PWRs constitute the most established and diffuse types of operational Nuclear Power Plants (NPPs), so they have been included in this study to represent the nuclear typology of the generating capacity of the power grid [25].

The proposed reactor model serves as an example to illustrate the concept behind the framework of analysis of cyber-attacks on ICT communicating infrastructure of a power grid including nuclear power plants: it is admittedly simplified in its technical features and strong assumptions are made to keep the focus on the methodological framework.

In a PWR, the energy generated by the fission of atoms heats water, which is pumped under high pressure from the primary circuit to the reactor core. The heated water then flows through a heat exchanger, where it transfers its thermal energy to a secondary circuit, where steam is generated and flows to turbines, which in turn spin an electric generator [26]. The model presented here concentrates on the primary circuit. In the reactor, water, which acts as the moderator and the coolant, passes through the core with upward flow and removes the heat, which the fuel contained in the fuel bars has generated through fission (Fig. 3).

Water enters the bottom of the reactor core at about 275 °C (T_{IN}) is heated and flows upwards through the reactor core at a temperature of about 315 °C (T_{OUT}). Despite the high temperature, water remains liquid due to the high pressure in the primary coolant loop, usually around 155 bar.

Within the hypothesis of a thermal power P_{TH} uniformly distributed along the core, the dynamics of the reactor can be modeled considering the variation of the power generated by the fuel and the power absorbed by the moderator [26]:

$$M_F C_F \frac{dT_F}{dt} = P_{TH} - k\,(T_F - T_M) \tag{1}$$

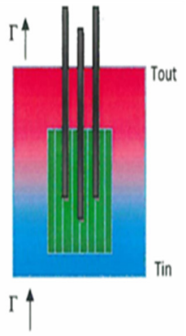

Fig. 3: Simplified model of the core of a PWR. The water flow Γ enters the bottom of the reactor at temperature T_{IN} and is heated to a temperature T_{OUT} while flowing upward through the core.

$$M_M C_M \frac{dT_M}{dt} = (T_F - T_M) - \Gamma C_M\,(T_{OUT} - T_{IN}) \tag{2}$$

$$T_{OUT} = 2T_M - T_{IN} \tag{3}$$

where

- M_F and M_M are respectively, the fuel and moderator masses,
- C_F and C_M are the fuel and moderator thermal coefficients,
- k is the global thermal coefficient, which accounts for the thermal exchange between fuel and water,
- Γ is the moderator flow and it can vary within the range of 104-105 tonn/h, and
- T_F and T_M are the fuel and the moderator temperatures. In particular, T_M is computed as the average between the inflow (T_{IN}) and the outflow (T_{OUT}) temperature of the water.

The equations (1), (2) present energetic balances on fuel and on moderator respectively. On the fuel side (first equation), the change in the produced energy is given by a source term P_{TH}, the produced thermal power, subtracted by the energy exchanged with the moderator. On the moderator side (second equation), the change in the absorbed energy is given by the difference between the energy exchanged and absorbed by the moderator. The equation (3) represents the assumed tie between the inflow and the outflow temperature of the water.

In the model, the demanded power P_{TH} and the inflow temperature T_{IN} of the moderator are the inputs. When an increase of 1kW of power and of 1 °C is given to the input variables, the step response of the system (Fig. 4) evidences that temperature rises by a factor of P/($M_F C_F$) ≈ 0.2. Since power acts mostly on the fuel temperature, the effects on the moderator temperature are negligible (Fig. 4). It is noteworthy that if the power is considered uniformly distributed inside the core, the thermal exchange between fuel and moderator is slow (Fig. 4).

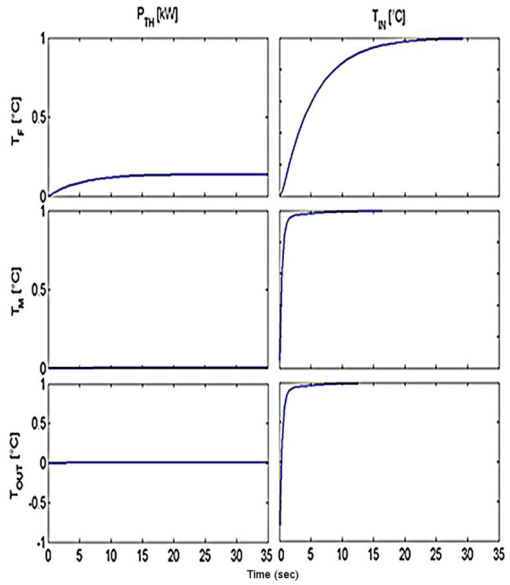

Fig. 4: Step response of the system. Thermal power P_{TH} and inflow temperature T_{IN} have been given respectively a raise of 1 kW and 1 °C.

C. Power market

Since more than one decade, a political change of mind has led to the liberalization of the power markets. Its goal: the creation of an internal European market that achieves security of supply and competitive prices and services for the customers. In this market, a growing variety of enterprises organizes the production, the trading, the marketing, the transmission and the supply of electricity, respecting appropriate regulation.

Producers compete to sell energy at the best possible price. The suppliers which deliver electricity to the final consumers buy the energy on the wholesale market from the producers or the trading companies. Power markets or spot markets offer trading platforms [21][22][23][24] to allow members to exchange information on values and prices and to submit bids for buying and selling power. Therefore a possible interruption between the communication of the power grid and the power market can lead to financial disturbances and even to market/prices manipulation.

In our testbed we have implemented a spot market, which provides automatically the prices on the requested quantity. If the requested energy quantity is not able to be provided by the lowest price energy producer, then the rest is obtained by the next one. For example, if the requested quantity is 100 KW and the lowest price producer is able to provide only 70 KW, the remaining 30 are going to be obtained by the second lowest one.

D. The power grid model

The IEEE electrical grid models [15] are extensively used by the scientific community since they are known to accurately encapsulate the basic characteristics of real infrastructures. As such, AMICI provides a broad range of grid models to experiment with, including the Western System Coordinating Council's (WSCC) 3-machine 9-bus system, and the 30-bus, 39-bus and 118-bus test cases, which represent a portion of the American Electric Power System as of early 1960. These constitute realistic models which are well-established within the power systems community and provide a wide range of power system configurations. An example graphical "bus-view" of the IEEE 30-bus power grid test system is given in Fig. 5. The IEEE 30 Bus Test Case represents a portion of the American Electric Power System (in the Midwestern US). Apart from the connecting buses, it consists of 6 generators and 20 load consuming buses. This is the main IEEE power grid we are going to use for our testbed.

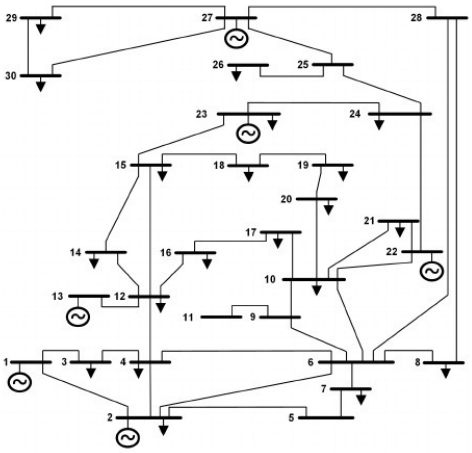

Fig. 5: The IEEE 30-bus test system.

E. Integration into AMICI

We have developed a generic approach to integrate a wide range of IEEE electrical grid models into Simulink and to prepare them for real-time simulation. This way AMICI [16] facilitates the timely integration of other models and eliminates manual, error-prone operations, which are mainly due to the large number of vectors and matrices that must be set-up.

The physical processes are implemented into AMICI by creating the Simulink models via the mathematical functions, but from a technical point of view real-time simulation of IEEE grid models in AMICI is enabled through a combination of two Matlab open-source libraries: MatPower [27] and MatDyn [28]. MatPower is an open-source Matlab package for solving power flow and optimal power flow problems. It is a simulation tool that includes several built-in IEEE test systems, which are already prepared for analysis. Since MatPower only provides static analysis of power systems, it needs to be coupled with MatDyn in order to benefit from its support for dynamic analysis, i.e., real-time simulation.

IV. Description of the Experimental Setup

A. Experimental Setup

The following experimental setup was implemented in the Joint Research Centre's (JRC) EPIC laboratory. The Emulab testbed included nodes with the following configuration: FreeBSD OS 8, Intel Xeon E5606 @2.1GHz and 2GB of RAM.

As shown in Fig. 2 the experimental setup consisted of 2 Routers (Cisco 6503), which have four Gigabit experimental interfaces and one control interface, and 22 hosts:

- one (1) host runs the power grid unit (AMICI model),
- one (1) host runs the nuclear plant (AMICI model),
- two (2) hosts for running the R-PLC units for the interconnection between power grid, nuclear plant and network,
- one (1) host for running the power market unit, and
- the (3) hosts to run the malicious software (attackers).
- the rest of the hosts to produce normal traffic.

The reason to use such a large testbed is to try replicate the attack from various hosts and verify the results. Within the Emulab testbed we emulated packet losses and background traffic (potentially DoS attack) in order to recreate a dynamic and unpredictable environment such as the Internet. For the background traffic we used UDP packets generated with both PathTest [1] and Iperf [2]. We have installed those tools in all the attacker nodes.

Additionally, we adjusted our networks in order to emulate the bandwidth limitations (10Mb/s) not only for the Internet but also for the communication to PLC. The communication between R-PLCs and the power grid model was implemented with a 100Mb/s to provide maximal performances for the interaction between R-PLC units. Finally, we should state that there is a synchronization algorithm between the models execution time and the system clocks ensuring reliable exchange of data.

B. Scenarios

The implemented scenarios are two, the first one affects the nuclear plant and the second one the real PLC, which is connected to the power grid.

1) Attack against a nuclear plant's PLC: In the implemented scenario the attacker interacts with PLCs by sending legitimate Modbus packets. This scenario assumes an attacker is able to access an internal network by bypassing the security of either the control center or substation networks. By doing so, it is possible to compromise the PLC, produce different values, and hide the fact that the plant produces approximately 30MW/h less without having any specific alarm. Since, the additional power is produced by the rest of the power grid, this means that the additional cost is around 793 euros/h, taking into account the average price for 30MW provided by the spot market (section III-C).

In Fig. 6 we see the minimal change of the temperature on the two different stages with normal and compromised PLC. It should be stated that the graph considers a timeframe of 10 hours: every hour the system registers a different level of energy demand and reacts accordingly. Since power acts mostly on the fuel temperature T_{fuel}, the effects on the moderator temperature T_m are negligible. When the system experiences a constant increase in the power demand, it reacts accordingly by varying the fuel temperature T_{fuel2} and the moderator temperature T_{m2}.

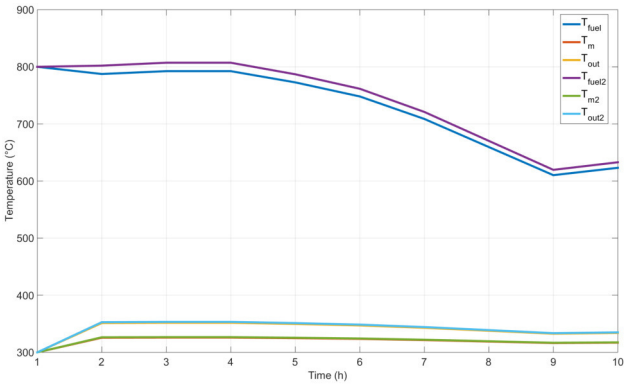

Fig. 6: Behavior of the system. The dynamics of the reactor is described by three quantities: the temperature of the fuel, T_{fuel}, the temperature of the moderator, T_m, and the temperature of the outflow water, T_{out}, and it is represented in two different load demand configurations (T_{fuel}, T_m, T_{out}) and (T_{fuel2}, T_{m2}, T_{out2}). Tm is computed as the average between the inflow (T_{in}) and the outflow temperature (T_{out}) of the moderator.

2) Attack against a generator's PLC: The DDoS attacks were implemented in different bandwidths up to 100Mbit/s, but we minimize our attacks till 20Mbit/s in order to be more realistic. We did not target the attack against a specific equipment because then the attack would be "extremely" successful. We aimed to minimize the network bandwidth between the physical equipment and the power market. Therefore there may be partial loss of communication between those entities.

In this scenario we have a dedicated router connecting the main elements. The router is not reachable through the Internet, but is used to pass communication for other services, such as web services, etc . This means that a DDoS attack cannot be aimed directly at the PLC, but by attacking a specific other service the network bandwidth is going to be limited. When the DDoS attack takes place, additional energy is needed by the consumers of the grid. So following the power market auction procedure, the producers place their bid and the power market decides on who has the best offer. During the scenario the needed load is constant 100MW split over various consumers. Moreover, the real PLC is connected to various simulated generators (each time to a different one) in order to identify any deviations based on the power grid topology.

The parameters we considered for the following experiments are packet losses and background traffic. For packet losses

[1]PathTest, Free Network Capacity Test tool, 2015
[2]Iperf: The TCP/UDP Bandwidth Measurement Tool, 2015

we used 3 rates: 0%, 10% and 20%. Finally, for the attack's background traffic we used: 5Mb/s, 10Mb/s and 20Mb/s. For each configuration setting, representing a combination of packet loss rate and background traffic we executed a separate experiment.

Within this context we measured a maximal success rate of 77% and a minimal success rate of 28%. The results show that even for 15% packet losses and 20 Mb/s the attack success rate is not 100%. More specifically, this means that from 100 attempts, an average of less than 50 will fail to produce some financial gain for the attacker or loss for the consumer. It should not come as a surprise that we measured a higher success rate for a larger loss rate. An explanation for this behavior is that the reduced number of packets does not assist the power market to verify that the offers need confirmation. These results are depicted in Tab. I. The cost is calculated by taking into account the success rate and the average price provided by the spot market for 100 MW.

TABLE I: Attack success rate and additional cost

DDoS success rate				
2.5Mb/s traffic	**5Mb/s traffic**	**10Mb/s traffic**	**Packet loss(%)**	**max Cost (euros/h)**
28%	32%	60%	0%	1586.58
29%	35%	68%	10%	1798.12
28%	37%	77%	20%	2036.11

V. Conclusions and further research

Cyber-physical systems are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. In this paper we present the implementation of a cyber-physical testbed including multiple Critical Infrastructures (CIs):

- two simulated interconnected infrastructures, power grid and nuclear plant,
- a simulated power market for providing the cost for the provided energy,
- a real PLC which is interconnected with a specific bus of the power network,
- an emulated cyber network which interconnects and controls all the aforementioned elements

To the best of our knowledge, this is the first time that those elements were presented/interconnected in a prototype and provides a step forward towards understanding the cyber security vulnerabilities of the current cyber-physical systems. In this paper we have analyzed the effects of network parameters on coordinated attacks and we show that they could be significants.

Based on this implementation, more advanced experiments will be created at the Network & Information Security Laboratory (NIS Lab) in order to show the effect of cyber-attacks against real infrastructure including the actions of real human actors (e.g. human operators) in the cyber-physical testing/simulation process. Moreover, we plan to propose and implement a set of countermeasures to tackle and mitigate the attacks, based on the exchanging signals and their statistical analysis for detecting anomalies [29][30].

References

[1] European commission, Directive on European Critical Infrastructures, COUNCIL DIRECTIVE 2008/114/EC, December 2008

[2] Wolthusen S.D., Modeling critical infrastructure requirements, Information Assurance Workshop, 2004, Proceedings from the Fifth Annual IEEE SMC, pp. 101- 108, 2004, http://dx.doi.org/10.1109/IAW.2004.1437804

[3] Yampolskiy, M., Sztipanovits, J., Yuan Xue, Koutsoukos, X.D., Horvath, P., Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach, Resilient Control Systems (ISRCS), 2012 5th International Symposium on, pp.55-62, 2012, http://dx.doi.org/10.1109/ISRCS.2012.6309293

[4] Zio, E., Sansavini, G., Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins, Reliability, IEEE Transactions on, vol. 60, no. 1, pp. 94-101, 2011, http://dx.doi.org/10.1109/TR.2010.2104211

[5] Zhu, B., Joseph, A., Sastry, S., A taxonomy of cyber attacks on SCADA systems. In Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing (pp. 380-388). IEEE, October, 2011, http://dx.doi.org/10.1109/iThings/CPSCom.2011.34

[6] Nai Fovino, I., Carcano, A., Masera, M., Trombetta, A: An experimental investigation of malware attacks on SCADA systems. International Journal of Critical Infrastructure Protection, vol. 2, no. 4, pp. 139-145, 2009, http://dx.doi.org/10.1016/j.ijcip.2009.10.001

[7] Rysavy, Ondrej, Jaroslav Rab, and Miroslav Sveda. "Improving security in SCADA systems through firewall policy analysis." In Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on, pp. 1435-1440. IEEE, 2013.

[8] Chen T, Abu-Nimeh S., Lessons from Stuxnet. Computer 2011;44(4):913, http://dx.doi.org/10.1109/MC.2011.115

[9] Fidler D., Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think. International Journal of Critical Infrastructure Protection 2012;5(1):289, http://dx.doi.org/10.1016/j.ijcip.2011.12.001

[10] Munro, Kate. "Deconstructing flame: the limitations of traditional defences." Computer Fraud & Security 2012.10 (2012): 8-11, http://dx.doi.org/10.1016/S1361-3723(12)70102-1

[11] Siaterlis, C., Garcia, A.P. and Genge, B., 2013. On the use of Emulab testbeds for scientifically rigorous experiments. Communications Surveys & Tutorials, IEEE, 15(2), pp.929-942, http://dx.doi.org/10.1109/SURV.2012.0601112.00185

[12] Hahn, A., Ashok, A., Sridhar, S. and Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. Smart Grid, IEEE Transactions on, 4(2), pp.847-855, 2013, http://dx.doi.org/10.1109/TSG.2012.2226919

[13] Yardley, Tim, Robin Berthier, David Nicol, and William H. Sanders. "Smart grid protocol testing through cyber-physical testbeds." In Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, pp. 1-6. IEEE, 2013, http://dx.doi.org/10.1145/2602575

[14] Davis, C. M., J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol. "SCADA cyber security testbed development." In Proceedings of the 38th North American power symposium (NAPS 2006), pp. 483-488. 2006, http://dx.doi.org/10.1109/NAPS.2006.359615

[15] University of Washington - Electrical Engineering, "Power Systems Test Case Archive," http://www.ee.washington.edu/research/pstca/, 2012, [Online; accessed January 2016].

[16] Genge, Béla, Christos Siaterlis, and Marc Hohenadel. "AMICI: An assessment platform for multi-domain security experimentation on critical infrastructures." In Critical information infrastructures security, pp. 228-239. Springer Berlin Heidelberg, 2012, http://dx.doi.org/10.1007/978-3-642-41485-5_20

[17] White, B., Lepreau, J., Stoller, L., Ricci, R., Guruprasad, S., Newbold, M., Hibler, M., Barb, C., Joglekar, A.: An integrated experimental environment for distributed systems and networks. In Proc. of the Fifth Symposium on Operating Systems Design and Implementation, pp. 255-270, 2002, http://dx.doi.org/10.1145/844128.844152

[18] Nai Fovino, I., Masera, M., Guidi, L., Carpi, G.: An Experimental Platform for Assessing SCADA Vulnerabilities and Countermeasures in Power Plants. In Proc. HSI, pp. 679-686, 2010, http://dx.doi.org/10.1109/HSI.2010.5514494

[19] Bialas, A., 2015, September. Experimentation tool for critical infrastructures risk management. In Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on (pp. 1099-1106). IEEE, http://dx.doi.org/10.15439/2015F77

[20] Preisler, T., Dethlefs, T., & Renz, W. (2015, September). Simulation as a service: A design approach for large-scale energy network simulations. In Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on (pp. 1765-1772). IEEE, http://dx.doi.org/10.15439/2015F116

[21] Bunn, Derek W., "Modelling prices in competitive electricity markets," 2004.

[22] Arroyo, José M., and Antonio J. Conejo. "Optimal response of a thermal unit to an electricity spot market," Power Systems, IEEE Transactions on 15.3 (2000): 1098-1104, http://dx.doi.org/10.1109/59.871739

[23] APX Power Spot Exchange, https://www.apxgroup.com/trading-clearing/spot-market/, last accessed on January 12, 2016

[24] EEX Power Spot Exchange, https://www.eex.com/en/products/power/power-spot-market, last accessed on January 12, 2016

[25] World Nuclear Association: www.world-nuclear.org/ Information-Library/ last accessed on January 12, 2015.

[26] Todreas N. E. and Kazimi M.S., Nuclear Systems Volume I: Thermal Hydraulic Fundamentals, CRC press, 2012.

[27] R.D. Zimmerman, C.E. Murillo-Sanchez, and R.J. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education, IEEE Trans. on Power Systems, vol. 26, no. 1, pp. 12-19, Febr. 2011, http://dx.doi.org/10.1109/TPWRS.2010.2051168

[28] Cole S., Belmans R., "MatDyn, A New Matlab-Based Toolbox for Power System Dynamic Simulation", IEEE Trans. on Power Systems, vol. 26, no. 3, pp. 1129-1136, Aug. 2011, http://dx.doi.org/10.1109/TPWRS.2010.2071888

[29] Soupionis Y., Ntalampiras S., and Giannopoulos G., "Faults and Cyber Attacks Detection in Critical Infrastructures." In International Conference on Critical Information Infrastructures Security, pp. 283-289. Springer International Publishing, 2014.

[30] Kornecki, A. J., Subramanian, N., & Zalewski, J. (2013, September). Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks. In Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on (pp. 1393-1399). IEEE.