Develop a Cyber Physical Security Platform for Supporting Security Countermeasure for Digital Energy System

Mike Mekkanen Tero Vartiainen Duong Dang

School of Technology and Innovation, University of Vaasa, Finland,
{mike.mekkanen,tero.vartiainen,duong.dang}@uwasa.fi

Abstract

The paper develops a cyber physical system (CPS) security platform for supporting security countermeasures for digital energy systems based on real-time simulators. The CPS platform provides functions that trainers or trainees can be able to operate and test their scenarios with a state-of-the-art integrated solution running at a real-time simulator. Those integrated solutions include energy systems simulation software and communication systems simulation/emulation software. The platform provides practical "hand-on-experiences" for participants and they are able to test, monitor and predict behaviors of both systems at the same time. The platform also helps achieve training's objectives that meet skilled requirements for the future generation in both smart energy systems evaluation and cyber physical security fields. In particular, we present the CPS platform's architecture and its functionalities. The developed CPS platform has also been validated and tested within different simulated threat cases and systems.

Keywords: cyber physical system laboratory, critical infrastructures, attack vectors, real time simulator, operational technology, information technology

1 Introduction

Numerous energy firms are undergoing digital transformations (Dang and Vartiainen 2019; Dang et al., 2021; Mekkanen et al., 2021; Mekkanen and Kauhaniemi 2018) and digital transformation has significant impact to the energy sector (Dang and Vartiainen, 2020; Mekkanen, 2021). It also brings threats to the sector as the information and communications technology (ICT) is embedded in energy systems. For example, cyber-attacks are one of the most common threats in the energy sector that causes severe consequences to organizations and even national security. To prevent cyber-attacks, several solutions are proposed, such as legislations, standards (Pearson, 2011), or testbeds (Sun et al., 2018). In particular, testbeds often use a Real-Time Simulator as a tool to test different scenarios that cannot test in a real physical system or it is very challenging if we put the real physical system in hazard mode as it may cause damage to the real-world systems. As a result, Real-Time Simulators thus have been widely used in the energy sector (Vellaithurai et al., 2017). In addition, one of the conventional solutions to prevent cyber attack is training persons-in-charges to acquire practical skills through a real time simulator.

However, engineering training faces several difficulties. First, the difficulties of setting up and executing scenarios in a diverse environment that allow learners to conduct and evaluate cases that align between labs' environments (e.g., equipment, software, threads, and technologies) and real-world environments (e.g., digital twins). Second, the difficulties in the multidisciplinary nature of energy systems that also integrate ICT and its threat to the systems. For example, smart grid systems increase cybersecurity threats. In that sense, if an attack happens in the energy systems, the damage is likely costly and it could potentially impact national security as in the case of cyber-attacks physically destroying Iran's nuclear centrifuges (Pearson, 2011).

This paper aims to tackle this issue by developing a cyber physical system (CPS) for an education environment. We use a state-of-the-art integrated solution running at real-time simulator. Those integrated solutions are the energy systems simulation software and the communication systems simulation/emulation software. We propose a CPS platform that provides abilities for trainers to train or coach trainees (e.g., students/security experts) for conducting tasks with a real simulator via online power system modeling, communication system emulation and cyber-attack emulation integrating and running in real-time in one target. Here a CPS is understood as a co-simulation platform, which links software that simulates the modern digital energy system (energy system unites, ICT and threats) aspects, and captures the complex interactions between them which meet the requirements of physical processes (Ison et al., 2020; de Reuver et al., 2018). The co-simulation allows more adaptable setup, scalable, simpler cyber-attacks testing/mitigation,

and comprehensive instrumentation via software probes to discover exactly what happened at every component of the CPS.

Our proposed platform has an ability to mimic the operation of the real instruments subject to cyber-attack at the lab's environment. Through the platform, trainees can perform their tasks in a state-of-the-art integrated solution real-time simulator via online physical/virtual devices, such as personal computers (PCs), servers, routers, firewalls, intrusion detection system (IDS), protocols, defender, intelligent agent, simulate attack and other information technology/operational technology (IT/OT) CPS system management solutions/tools that connected via different existing/designed communication protocols/medium to the real-time simulator, such as hardware-in-the-loop (HIL), software-in-the-loop (SIL), and processor-in-the-Loop (PIL). By doing so, it is expected that learners can learn practical "hand-on-experiences" and they become physical security experts in the future.

The remainder of this study is structured as follows. First, the background section is presented. Second, we describe the development of the CPS platform. Third, the CPS platform scenarios are presented. Finally, we present the conclusions.

2 Background

2.1 A brief history of simulation development

A simulation has been widely employed in electrical *system planning and design for decades. There are a* wide range of energy sector applications that have successfully developed simulation for their experiments. The rapid evolution of computing technologies has helped the improvements of simulation tools during the past decades. Figure 1 shows the timeline of the evolution of real-time simulators from physical/analog to fully digitalization.

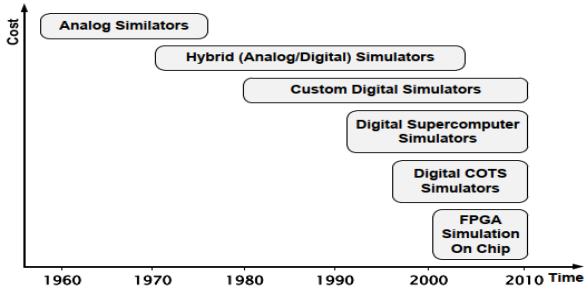

Figure 1. Real-time simulator evolution

Moreover, the emergence of low-cost multi-core processors has also paved the way for the development of simulators as it considerably helps more affordable and scalable real-time simulators. The ability of a real-time simulator to distribute work across different dedicated cores within a multi-core processor dramatically reduces processing time and allows the integration of different tools, as well as the capacity to interact with other software, applications, and devices, resulting in a co-simulation-approach. Co-simulations are a complex combination of different sorts of simulations that are run or solved in separate runtime environments. Real time co-simulations merge multiple types of simulations to create a hybrid simulation model (power system, ICT, cyber-security etc.), where various representations must be synchronized in order to run in universal time.

2.2 Real-time simulation

A simulation is "a representation of the operation or features of a system through the use or operation of another" (Sun et al., 2018). In this paper, we use a discrete-time simulation or fixed time-step simulation for the platform development as it is suitable for the real-time simulation. Each system state or variable will be solved mathematically based on a selected solver at a given time-step. We obtain the results via off-line and in real-time simulations, however offline is faster than online. A given discrete time-step simulation might be differ (e.g., shorter or longer) in comparison to the actual required time to compute equations and functions that represent a system model. Figure 2. represents these two possibilities: (a) computing time is shorter than a fixed time-step, (b) computing time is longer than a fixed time-step. Whereas in (c) both times are synchronized. It also shows all operations including driving inputs and outputs (I/O) to and from externally connected devices. In addition, it is noted that the solving system speed relies upon the accessible calculation power and the system numerical model complexity.

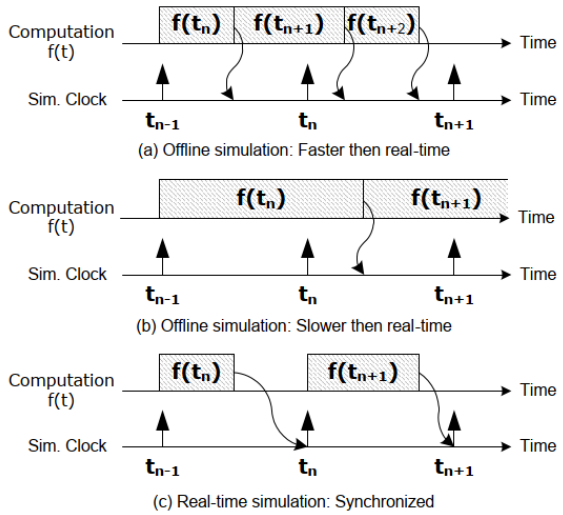

Figure 2. Real-time simulator computation

Computation accuracy is determined by two factors: the precise dynamic representation of the system and the time required for producing results. The accuracy and

validity of a real-time simulation is determined by performing all internal computations and performing results outputs that are compared to actual devices.

2.3 Model for designing and testing a real-time simulation

We apply the Mode-based Design (MBD) method. MBD is a mathematical and graphical methodology for expressing the system under test, and it adheres to the "V" diagram workflow as shown in Figure 3.

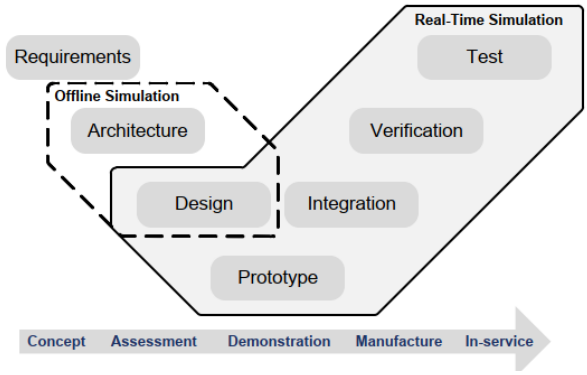

Figure 3. Model-based Design Workflow

This model provides a comprehensive view of the system under development with diverse domain knowledge. It also provides abilities for engineers who are involved in designing, modeling, testing, and utilizing models in an efficient and organized manner. For example, it allows automated testing with different parameters under different circumstances. It is reusable and the designed environment can remain homogeneous through different design tools via import/export model tool's features. The majority of those tools provide an automatic code generator for the designed models. As a result, the import/export features in those tools are easy to use. Even if they are developed using different design tools, the predesigned/old model will be imported and included as a block in the new design model. Thus, the use of an automatic code generator adds value to real-time simulation in MBD.

Combining an automatic code generator and a real-time simulator make a rapid control prototyping (RCP) implementation from the testing model point view with minimal effort. The prototype can then be used to speed up integration and verification testing, something that offline simulation cannot do. The same concept is valid also for the HIL testing. By using an HIL test, hardware testing can be performed earlier in the process, sometimes before an actual plant is available. For example, electrical system automotive controller testing functionality can be performed early even before a physical plant is completed. As a result, designed issues can be identified earlier in the process, allowing required tradeoffs to be determined and applied, lowering development cycle/costs.

2.4 Cyber physical security platform

As discussed in the aforementioned section, the energy system is a multidisciplinary study due to the involvement of various fields, ranging from electric power, ICT systems, cyber security to computing science. As a result, universities have recently updated their engineering programs curriculum, such as adding new courses or updating materials for existing courses (Langner, 2011; de Reuver et al., 2018). Those courses are often designed with lab practices, this leads to a high demand for labs that allow learners to be able to practice and learn hands-on-skills. The dilemma is that an energy system contains several devices (e.g., generators, transmission line transformer) while establishing a lab and managing those devices are challenging in terms of technical difficulties, costs, and human resources.

A real-time CPS platform includes a simulator that combines energy system simulation software and emulation (e.g., communication system and cyber physical security), software/tools (e.g., co-simulation). The platform provides a holistic experience to both trainers and trainees. Also, it enables the trainer to visualize their specific energy system and/or communication network environments in a manageable laboratory setting (digital twins; replica of real physical system). Moreover, CPS platform provides functions to analyze a variety of "what if" scenarios in order to assess impacts of different circumstances.

CPS platform supports researchers who are working to find solutions beyond the state-of-the-art. This is because of its designed and development capabilities, such as energy system components, communication system interfaces/protocols and cyber security entities.

3 Development of CPS Platform

A digital energy system has a cross-disciplinary nature that has different domain competencies. This cross-disciplinary is amplified by combining required CPS competence with others (e.g., power system simulation model, communication simulation/emulation model) competencies. To this end, educators are subject to a variety of tools and concepts that are associated with various domains. Subsequently, new instructive teaching/training methods/techniques should be developed along with tools. This enables relevant parties in dealing with various domains and combining their knowledge into a single solution. This solution enables educators to comprehend coupling and interaction among entities that comprise the integrated developed solution. As a result, it is natural that the CPS platform be developed in such a way that educators can learn by bridging the gap between theory and real-world application.

To achieve this goal, we design a CPS platform with a real-time simulator as the mean core of the lab, along

with other different development boards and Field-programmable gate arrays (FPGAs). The simulator is from Opal RT (e.g., OP5700 Real-Time Simulator) with HYPERSIM modeling software which simulates the power system. Our platform's emulator is Scalable EXata communication simulation/emulation software, which simulates/emulates the communication network with cyber-attack modules. This HYPERSIM-software's simulator has the capability to accurately mimic the response of an actual physical system in real-time. Also, it has multiple interface modules, including analog and digital channels, as well as, a variety of communication protocols including IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and SV, IEEE C37.118, DNP3, Modbus.

In the context of CPS, using an RTS allows a simulation to interface with a cyber system in real-time and achieve a more complete and realistic testing environment. Here, SCALABLE has developed a highly-specialized kernel to exploit contemporary multi-core architectures for real-time execution of large-scale, high-fidelity network and cyber models. It uses a network digital twin to represent entire CPS communication networks, various protocol layers, application layers, physical layers, and devices. It includes a low-skew synchronization kernel to connect with live applications and equipment, which communicates throughout the digital twin just as it would run on physical networks. A suite of simulated cyberspace attacks and defenses interact with every layer of the emulated network. These include network security protocols, firewall models, port and network scanning, DoS, stimulation of intrusion detection systems, vulnerability exploitation, packet modification, virus and worm propagation and defense, backdoors, rootkits, botnets, and others. The system can also integrate real exploitation tools into a safe lab environment. Running real data feeds e.g., GOOSE, though the system can subject these feeds to delay, degradation or even substitution. The system enables actual cyber defense technologies to be deployed and integrated with the emulated network, the cyberspace attacks, and the virtual representations of systems to assess the effectiveness of tools, techniques and architectures to ensure system-of-systems availability. These two software are tightly linked together via a developed functionality to automate virtual link creation. Using the virtual links ensures mapping between HYPERSIM and EXata dedicated sender and receiver, that a packet being sent at one interface of the link will be only received at the other interface as illustrated in Figure 4.

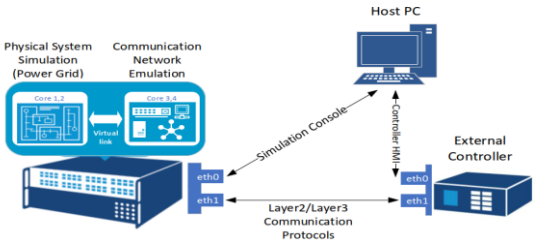

Figure 4. CPS platform setup

The closed-loop testing environment offered by CPS platform will allow the unit under test to interact with the CPS platform in a real-time manner. Using this closed-loop testing specifically for cyber security research is more beneficial, because in this situation, based on cyber incidents cascaded events in the energy system that will generate large-scale disruption. Studying such events by performing after-fault analysis, developing prediction strategies, and testing mitigation solutions can be easily implemented by using the automatic statistical reports generation for each entity with the test.

In addition, the CPS platform has great benefits that has a graphical user interface on the Host PC to facilitate scenario creation and real-time visualization of the power system and the communication system parameters. In addition, it can be used at runtime to launch cyber-attacks, or alternatively, the attacks can be predefined in the scenario while it's running which accelerates the workflow and eliminates human errors in configuration. Given the benefits of using a real-time simulator, particularly with this new integrated solution, there's several challenges to consider.

4 CR-DES CPS Platform scenarios

The provided SIL "Cyber-Physical Simulation of a Microgrid Subject to Cyber-Attacks" example developed by Opal RT and Scalable EXata forms the basis for the development of HIL use-cases. These examples are used to validate and test the CPS platform's operation and results validation. The first SIL is an example of a cyber-physical simulation involving a cyber-attacked microgrid. An OPAL-RT Real-Time Simulator co-simulates a microgrid system, including its distributed energy resources (DERs), power converters, and loads modeled in HYPERSIM, as well as the underlying communication network in EXata CPS as illustrated in Figure 5. Technical descriptions of microgrid units and testing results discussions are beyond the scope of this paper and will be published in other works as part of the CR-DES project dissemination plan.

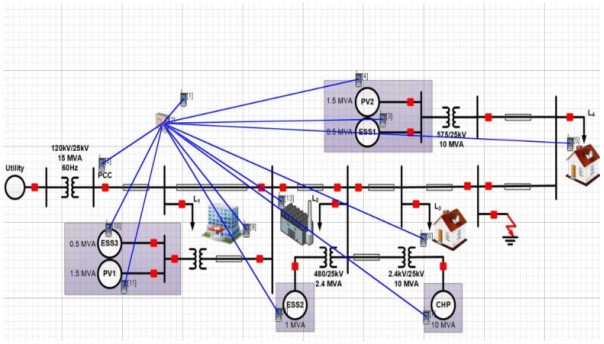

Figure 5. SIL microgrid subject to cyber attack, blue lines show the communication links that every MG node entity (DERs, loads, CB, etc.) send measurements, status to the MGC and received controlling signal from the MGC based on GOOSE IEC 61850 standard protocol

Each microgrid asset has a subsystem measurement that generates P, Q, and Vrms measurements based on voltage and current measurements. Internal microgrid controller MGC (Node 1) is a simulated MGC that has been implemented on the same model (SIL). The primary role of the MGC is to receive measurements from measurement subsystems and use these measurements to send reference set points to some of the DERs. As well as to keep the balance between the generated and consumed power by the DERs and loads respectively. Two scenarios had been designed and tested as follows.

1.1 Scenario 1

The first scenario the grid will be islanded in second 1, and in this islanded mode in order to insure the power balance between DERs power generation and load power consumption. The MGC is designed in a way that needs to send a dispatching signal to shed loads 4 (noun critical load), if there is a difference between DERs power generation and load power consumption as fast as possible. This power difference should be more than 3MW. The MGC is using the IEC 61850 GOOSE protocol for sending and receiving via EXata communication emulation features. In addition, MGC attempts to enable voltage support and keep the microgrid physical parameters measurement values such as (frequency, grid RMS voltages etc.,) close to the nominal operation values.

Next step within scenario one, a delay cyber-attack module will be introduced (1 second delay) via EXat emulation software. According to this delay attack the trip command within the GOOSE messages that send from MGC to open CB Load4 (disconnect Load 4) will be delayed by 1 second. This delay attack will initiate large disturbance that might lead to blackout e.g., Large frequency deviation, before being regulated back to its nominal value, hard and longer voltage dip down under its nominal value, with increased voltage oscillations as illustrated in Figure 6.

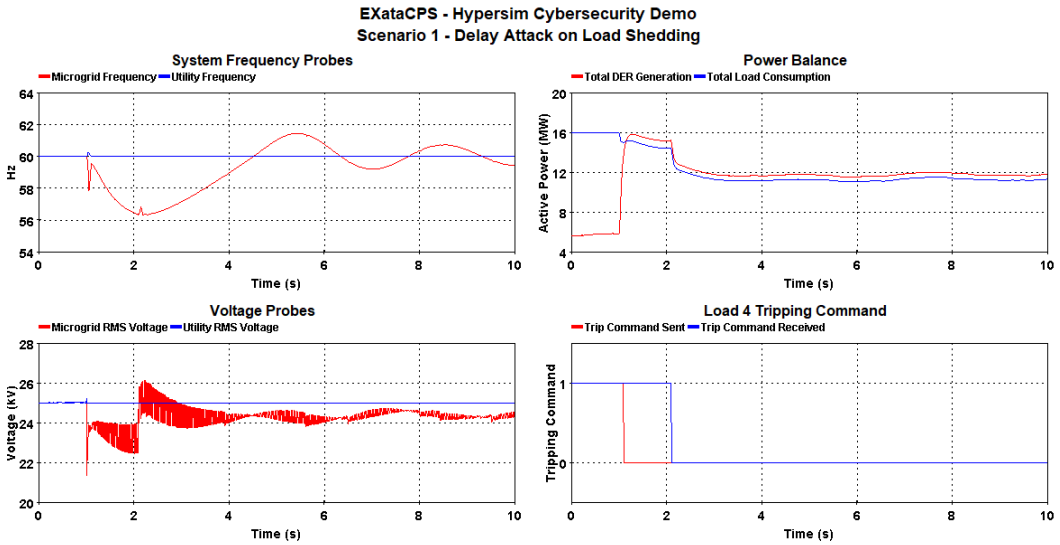

Figure 6. Microgrid subject to delay attack scenario 1. In the bottom right of the figure, the red line is the original trip signal sent from the controller to shed load 4 after the grid is islanded in the second one, which it is in time. Whereas the blue line is the delayed signal. Trip command sent by the MGC is delayed by one second after we apply the cyber delay attack to the controller signal. The bottom left figure shows a hard and longer voltage dip down to 23 kV, with increased voltage oscillations happening along with execution of the delay attack. Also, on the up left figure shows large frequency deviation, before being regulated back to its nominal value after second two. In the right up of the figure it shows the power unbalance and the mismatching between power supply (red curve) and demand (blue curve) before second two (based on the delay attack). However, the grid attempts to tackle the problem and return back to normal operation after the second and keep the balance between the generated and consumed powers.

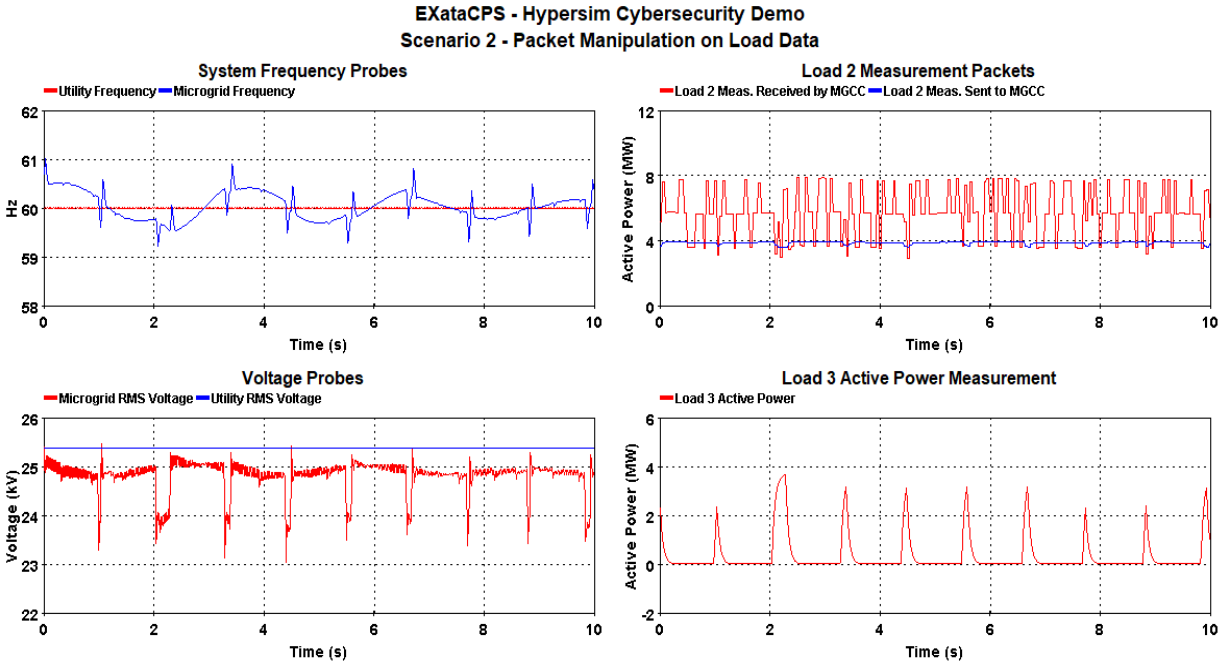

Figure 7. Microgrid subject to man-in-the-middle attack scenario 2. In the top right picture load 2 measurements, red curve is manipulated before they are received by the MGC based on executing the man-in-the-middle attack, blue curve is the normal load 2 measurements before executing the attack. The bottom right shows the load 3 active power consumption which is fluctuated between (0 and 4MW) since it is connected and disconnected to the grid based on the executing the man-in-the-middle attack that duplicate load 2 consuming power and the MGCC is programmed to shed the priority load 3 if the mismatch between generation and load exceeds 3 MW. Smart grid also suffers from declining power quality voltage oscillations as shown in the bottom left of the figure and also high frequency oscillations as shown in the up left of the figure.

1.2 Scenario 2

Microgrid is landed in steady state operation mode subject to man-in-the-middle cyber-attack. According to this scenario manipulation to Load 2 power consumption metermen's is duplicated within the EXata software (cyber-attack modules) on its way before it is received by the MGC. In this case MGCC will periodically trips and reconnects load 3 since MGCC is programmed to shed the priority load 3 if the mismatch between generation and load exceeds 3 MW. In addition, the microgrid under test also suffers from declining power quality, including high frequency and voltage oscillations as illustrated in Figure 7.

Consequently, various types of cyber-attacks, such as denial of service (DoS), buffer issues, virus sniffing, etc., can be carried out. Different monitoring and defensive network techniques, such as firewalls, intrusion detection ID, intelligent agents, defenders, etc., can also be designed and implemented for effective operational testing and assessing the resilience of energy system communication networks to cyber threats.

5 Conclusions

The CPS security platform is proposed in this paper and we show the requirements for testing of complex design systems in a variety of situations (e.g., steady state, transition, and attack) during both the development phase and prior to final system commissioning. As well as we present the feasibility of the developed CPS security platform to accomplish these tasks. Furthermore, we demonstrate one case study (SIL) in which real-time traffic based on the IEC 61850 GOOSE protocol has been exchanged between the smart grid nodes and controller. This real-time traffic is subject to cyber attack. We also present the architecture of cybersecurity and resilience of digital energy systems as well as its basic functionalities.

Acknowledgments

This study was partly funded by the European Regional Development Fund and the Regional Council of Ostrobothnia.

References

Duong Dang and Tero Vartiainen. Digital Strategy Patterns in Information Systems Research. *Pacific Asia Conference on Information Systems (PACIS) 2019 Proceedings,* 2019.

Duong Dang and Tero Vartiainen. Changing Patterns in the Process of Digital Transformation Initiative in Established Firms: The Case of an Energy Sector Company. *Pacific Asia Conference on Information Systems (PACIS) 2020 Proceedings,* 2020.

Duong Dang, Tero Vartiainen, and Mike Mekkanen. Towards Establishing Principles for Designing Cybersecurity Simulations of Cyber-Physical Artefacts in Real-Time Simulation. *Proceedings of International Conference on Information Systems Development (ISD),* 2021.

Stephen Ison, Lucy Budd, Magdi S. Mahmoud, and Yuanqing Xia, eds. Chapter 13 - Secure Estimation Subject to Cyber Stochastic Attacks. Pp. 373–404 in *Cloud Control Systems*, *Emerging Methodologies and Applications in Modelling*. Academic Press, 2020.

R. Langner, Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy* 9(3):49–51, 2011. doi: 10.1109/MSP.2011.67.

Mike Mekkanen, and Kimmo Kauhaniemi. Wireless Light-Weight IEC 61850 Based Loss of Mains Protection for Smart Grid. *Open Engineering* 8(1):182–92, 2018. doi: 10.1515/eng-2018-0022.

Mike Mekkanen, Tero Vartiainen, Kimmo Kauhaniemi, and Duong Dang. Intelligent Micro Grid Controller Development for Hardware-in-the-Loop Micro Grid Simulation Subject to Cyber-Attacks. Oulu, Finland, 2021.

Mike Mekkanen. Cybersecurity and Resilience of Digital Energy Systems. Opal-RT 21, Conference, 2021.

Ivan L. G. Pearson. Smart Grid Cyber Security for Europe. *Energy Policy* 39(9):5211–18, 2011. doi: 10.1016/j.enpol.2011.05.043.

Mark de Reuver, Carsten Sørensen, and Rahul C. Basole. The Digital Platform: A Research Agenda. *Journal of Information Technology* 33(2):124–35, 2018. doi: 10.1057/s41265-016-0033-3.

Chih-Che Sun, Adam Hahn, and Chen-Ching Liu. Cyber Security of a Power Grid: State-of-the-Art. *International Journal of Electrical Power & Energy Systems* 99:45–56, 2018. doi: 10.1016/j.ijepes.2017.12.020.

C. B. Vellaithurai, S. S. Biswas, and A. K. Srivastava. Development and Application of a Real-Time Test Bed for Cyber–Physical System. *IEEE Systems Journal* 11(4):2192–2203, 2017. doi: 10.1109/JSYST.2015.2476367.