Towards Establishing Principles for Designing Cybersecurity Simulations of Cyber-Physical Artefacts in Real-Time Simulation

Duong Dang
University of Vaasa, Vaasa, Finland *duong.dang@uwasa.fi*

Tero Vartiainen
University of Vaasa, Vaasa, Finland *tero.vartiainen@uwasa.fi*

Mike Mekkanen
University of Vaasa, Vaasa, Finland *mike.mekkanen@uwasa.fi*

Abstract

Our modern world is dependent on cyber-physical artefacts (e.g., smart grids, cars, mobile phones). Those artefacts are being attacked by cyber-criminals entailing substantial harm to individuals, organizations, and governments. Those artefacts need to be designed properly to prevent and recover from inevitable cyberattacks. We offer a solution based on a Real-Time Simulator (RTS). Our solution is meta-principles for using RTS when designing simulations in Cyber-Physical artefacts. Our solution considers both social and technical layers of cyber-physical artefacts.

Keywords: Design Science, Cyber Physical Security, Real-time Simulator, Principles.

1. Introduction

We are living in a digital world. This results in rapidly digitalizing and changing traditional successful business models [6], and the energy sector is changing at a rapid pace due to the disruptive changes of digital technologies [5]. For example, there is an increasing ratio of renewable and decentral energy generation around the world [27]. This leads to growing trends in integration of Information and Communication Technologies (ICT) into electrical power systems, especially in smart grid systems. This trend also brings cybersecurity threats to energy systems and cyber-attacks could lead to physical consequences as if an attack happens in the energy systems, the damage is very costly. For example, cyber-attacks brought down a power grid in Ukraine or physically destroyed Iran's nuclear centrifuges [25]. To minimize the consequences of cyber-attacks, several solutions are proposed, such as legislations/standards [20], cooperation [8] or testbeds [26].

Testing in a real physical system in the energy sector is very difficult or very challenging when we put a real physical system in a hazard mode. In that sense, a Real-Time Simulator (RTS), which refers to the computer model runs at the same rate as the actual physical system, would help to reduce development costs and time. It also would help simulate different scenarios of cyber-attacks in a physical system and propose scripts to respond with those scenarios. RTS thus has been widely used in the energy sector [28]. However, the majority of RTS literature are focused on either regulations or standards [17], or power systems themselves [1] or cyber security issues related to the energy discipline in a technical perspectives, but not, for example, principles for designing cybersecurity simulations of cyber-physical artefacts in real-time simulation. Our research thus fills this gap, we propose principles for designing simulations of cyber-physical artefact (RSC).

We use design science as our research approach [9]. Our proposed principles are designed, demonstrated, refined, evaluated, and facilitated in the context of a smart grid. The Cyber Physical Security (CPS) lab is used to assist our research. Here a cyber physical system is understood as integrations of computation, communication, and control that meet requirements of physical processes [11]. The principles are our contribution to literature, principles also help practitioners in several ways, such as improving in the performance of the simulations being designed for assessing cyber-physical artefacts, recommend solutions for addressing the unforeseen cyber threats of the emerging artefacts, and guidance for cybersecurity assessment.

2. Literature Review

2.1. Information Systems in Energy Systems

The time of energy as a commodity are increasingly replaced by decentral energy generation or distributed energy which is defined as compromising of a range of smaller-scale and modular devices to provide energy in locations close to consumers [13]. One example of distributed energy is renewable energy, which accounted for 40% of Finland's total consumption in 2020, this number is higher than consumption of fossil fuels and peat for the first time in history [24]. It is argued that information systems (IS) play a central role in the transition of the energy sector [13], [27]. For example, there is growing ICT dependence in the European grid [20]. IS acts as integrating and enabling technologies to energy sector [4], IS impacts on reducing carbon emissions [16], IS improves the efficient of energy generation and distribution [16], or change customers behaviors providing personalized feedback about their energy consumption in real time via IS devices (e.g., smart meters) [22], [23].

2.2. Cyber Security in Smart Grids

Cyber security has been paid attention in the energy sector. This is particularly more important when IS/ICT is being introduced to the energy sector. It brings new and serious threats to the secure operation of the field, especially in a smart grid. For example, there were more than 45 cyber attacks in the energy sector in 2015 [19] and the actual number of cyber attacks is higher than those reported [7]. Cyber security is thus identified as one of the challenges for safety operations of Smart Grids [15], [20], transactive energy systems [14], and power grids [26]. Main vulnerabilities factors and potential threats in smart grids can be summarized in Table 1 as follows (adopted from [26]).

Table 1. Vulnerability factors of cyber attacks in smart grids.

Vulnerability	Description	Example and references
Cyber infrastructures	Attackers unauthorize access to infrastructures	Attack via network packets
Vulnerability assessment	Attackers exploit vulnerability between the cyber system and physical system.	Stuxnet attacked the SCADA network
Standard and regulations	Attackers exploit systems that does not complement with regulations and standards	IEC 60870-6, IEEE C37 series, ANSI C12 series

To minimize vulnerabilities of cyber security, several approaches have been introduced or suggested, such as legislations/standards [20], cooperation [8] or testbeds [26]. In particular, real-time cyber physical system testbeds are designed to study the interactions between cyber and physical systems [26]. Testbeds are used because if we test a cyber attack on a real-world physical system, it may cause great damage to the system. Testbeds generally comprise three parts, including power systems simulation tools, communication system simulation/emulation tools, and connection between the previous two.

Although those testbeds have their own strengths and advantages, there is a lack of literature on designing a proper test. One of the reasons is the multiple disciplinary nature of this field, including computer science, electricity engineering, and information systems. It is argued that good guidance can provide a good proposal that helps organizations having a good plan in response to the risks of cyber attacks into their systems. This motivated us to study designing principles for using RTS when designing simulations of cyber-physical artefacts with respect to smart grids.

3. Research Methods

For the purposes of this study, Design Science Research Methodology (DSRM) Process Model [10] was adopted to develop a nascent design theory for designing the use of a real-time simulator for development of cybersecurity of a cyber-physical system. We followed DSRM phases, including (a) identifying problems and motivation, (b) defining objectives of a solution, iii) designing and development, (c) demonstration, (d) evaluation, and (e) communication. After problems are identified, the final phase is a solution. In this paper we will report the first proposal for design principles and we will also show how we continue development of principles (design and development). Evaluation is based on case

study with our partners' companies. Case study has been used as an approach to evaluate artefacts in IS [9], [21]. Data will be collected via workshops and interviews. In addition, Cyber physical Security Lab's results will be used (e.g., output of scenarios).

4. Principles for Designing Cybersecurity Simulations (PDCS) for Cyber-Physical Artefacts

Principles in this study are designed based on IS design theory [12] and design science research methodology [9]. Cyber security in smart grids is challenging because existing security mechanisms may not be applied to the smart grid environment [18]. Design a simulation in a cyber-physical artefact should cover potential threats, which are documented through standards, existing body of knowledge, prior cyber events, and tacit knowledge of the experts. For example, each system/subsystem or devices need to follow a certain standard(s) as seen in Table 1, such as the IEC 60870-6 standard is used for the SCADA system that applies for monitoring and controlling over a WAN or the ANSI C12 series standard is used for AMI systems that define communication protocol for metering applications [2], [26]. If we fail to follow those established standards (e.g., IEC, ANSI, NIST, and IEEE), the system's reliability is in question. In that sense, those sources of knowledge incorporated in the principles that are being suggested would help to prevent severely damaging the systems. As a result, we propose the following preliminary principle 1:

Principle 1. Principle of covering the scenarios. PDCS should cover the scenarios of cyber-physical attacks, those scenarios include the legislation, standards, guidelines, testbeds, and existing body of knowledge, in which the sources of knowledge come from prior cyber events and tacit knowledge of the experts.

Following the first principle is important for achieving a preparedness for a cyber attack. However, although most of the existing testbeds, legislations and standards have tried to address all the possible scenarios and potential threats, we are observing an increasing number of unforeseen attacks. Prediction and prevention of those attacks rely on the expertise of the testers and developers, otherwise they are highly unpredictable. Further, those unforeseen attacks can be also developed with practitioners (e.g., companies) for their emerging needs. As a result, we propose the following preliminary principle 2:

Principle 2. Principle of predicting and preventing unforeseen attacks. PDCS should have capability to predict and prevent unforeseen attacks and provide an improvement in the performance of the simulations being designed for assessing cyber-physical artefacts.

Designing a test in a cyber-physical security system should be able to be implemented in a real-world system. It means that the mitigation recommendations should be doable, clear and feasible with a minimum intervention to a physical system (e.g., automation functions cannot be turned off). Moreover, it would help improve the performance of the simulations being designed for assessing cyber-physical artefacts, as well as recommend solutions for addressing the unforeseen cyber threats of the emerging artefacts. Finally, testing of the scenarios are automated meaning that we could be able to automatically test with different parameters and results can be presented in various types of reports. As a result, we propose the following preliminary principle 3:

Principle 3. Principle of implementable. PDCS should provide a guide that organizations can be able to implement to a real-world system. PDCS should also provide solutions for addressing the unforeseen cyber threats of the emerging artefacts.

5. Demonstration and Evaluation of the Designed Principles

We demonstrate how our proposed principles apply to a PDCS prototype in the context of a smart grid. We also illustrate an evaluation, a validation and a facilitation of the principles.

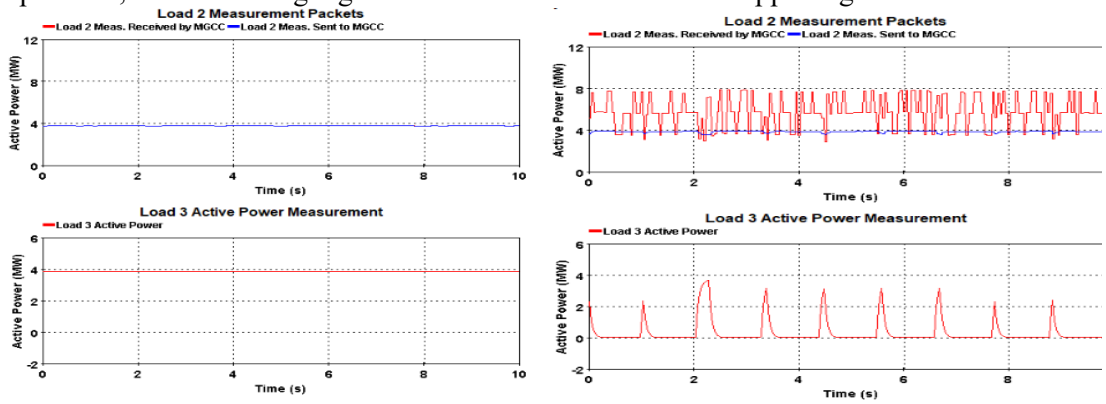
5.1. Demonstration and Evaluation Environment

The proposed principles will be demonstrated and evaluated with the following environments: Cooperation partners and CPS Lab. The partners include Wärtsilä, ABB, Arcteq, Wapice, Vaasan Sähkö, VASEK. CPS Lab is a part of the EU-funded project at the University of Vaasa (e.g., Cyber Physical Security and Resilience for Digital Energy

Systems Project). The architecture of the lab consists of two main parts: simulator and emulator. Simulator is OP5700 Real-Time Simulator with HYPERSIM modeling software, while Emulator is scalable EXata communication simulation/emulation software.

5.2. Demonstration and Evaluation of the Designed Principles

We follow the guide for the demonstration and evaluation in design science [21], we demonstrate the ability of our proposed artefacts to solve research problems and we then validate the proposed artefacts [21]. First, the workshop about cybersecurity and resilience of digital energy systems was organized in December 2020. It was based on a questionnaire with 23 questions designed and sent to energy companies (e.g., 170 institutions, including partners, energy companies in Finland, and International partners). The input of the workshop helped us understand the practitioners' experiences, their cyber security management and standards, their needs including communication protocols and testing. They also have been initially used for designing principles. Second, CPS Lab is also used during the designing process. After those steps, design principles will be refined and/or revised. For example, to demonstrate the first principle, several scenarios are designed, and run with CPS Lab. For example, Figure 1 shows the man-in-the-middle attack scenario against the system. This scenario is designed in response to the vulnerability of cyber infrastructures (Table 1). This is one of several scenarios that are being designed to evaluate and demonstrate the first principle. In this scenario, we assume that the data is manipulated in the middle of its way to the microgrid controller (MGC). It means that the MGC may take incorrect actions as it perceives the message is true. As a result, it causes oscillations on microgrids nominal operation parameters such as frequency, voltages, etc. To implement, we use C language and Wireshark to see what's happening on the network.



(a) The LabVIEW under normal operation (b) The LabVIEW GUI under a delay attack

Fig. 1. The LabVIEW of the man-in-the-middle scenario.

In a similar vein, scenarios will cover vulnerabilities from cyber infrastructures, vulnerability assessment, and standard and regulations. Third, Lab results will be discussed with practitioners. Secondary data and interviews are used for the designing principles process. Proposed principles will be discussed with practitioners for the appropriateness. The lesson-learned will be drawn from the demonstration to identify weaknesses and areas of improvement [3], [29]. Through those steps and its process, principles may be also refined, revised or added. The results of the process are the final set of design principles for designing cybersecurity simulations of cyber-physical artefacts in real-time simulation.

6. Conclusion

Three preliminary principles are designed in this research-in-progress paper. The final set of design principles will be finalized through the process of demonstration and evaluation artefacts in IS [9], [21] in the future. These principles cover not only existing guidelines, principles, and prior cyber-attacks events, but also including tacit knowledge of the experts in the field and to be applied to a PDCS prototype. These principles help improve the performance of the simulations being designed for assessing cyber-physical artefacts. Finally, a recommendation for addressing the unforeseen cyber threats of the emerging artefacts are introduced based on these principles.

References

1. Aghamolki, H.G., Miao, Z., Fan, L.: A hardware-in-the-loop SCADA testbed. In: 2015 North American Power Symposium (NAPS). pp. 1–6. (2015)
2. Ashok, A., Krishnaswamy, S., Govindarasu, M.: PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid. In: 2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT). pp. 1–5. (2016)
3. Boudreau, M.-C., Gefen, D., Straub, D.W.: Validation in Information Systems Research: A State-of-the-Art Assessment. MIS Quarterly. 25 (1), 1–16 (2001)
4. Casal, C., Wunnik, C., Sancho, L., Burgelman, J., Desruelle, P.: The future impact of ICT on environmental sustainability. European Commission (2004)
5. Dang, D., Vartiainen, T.: Changing Patterns in the Process of Digital Transformation Initiative in Established Firms: The Case of an Energy Sector Company. PACIS 2020 Proceedings. (2020)
6. Dang, D., Vartiainen, T.: Digital strategy patterns in information systems research. PACIS 2019 Proceedings. (2019)
7. Glenn, C., Sterbentz, D., Wright, A.: Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. (2016)
8. Heinl, C.H.: Regional Cybersecurity:: Moving Toward a Resilient ASEAN Cybersecurity Regime. Asia Policy. (18), 131–160 (2014)
9. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly. 28 (1), 75–105 (2004)
10. Iivari, J.: Information system artefact or information system application: that is the question. Information Systems Journal. 27 (6), 753–774 (2017)
11. Ison, S., Budd, L., Mahmoud, M.S., Xia, Y. eds: Chapter 13 - Secure estimation subject to cyber stochastic attacks. In: Cloud Control Systems. pp. 373–404. Academic Press (2020)
12. Jones, D., Gregor, S.: The Anatomy of a Design Theory. Journal of the Association for Information Systems. 8 (5), (2007)
13. Ketter, W., Collins, J., Saar-Tsechansky, M., Marom, O.: Information Systems for a Smart Electricity Grid: Emerging Challenges and Opportunities. ACM Trans. Manage. Inf. Syst. 9 (3), 10:1–10:22 (2018)
14. Krishnan, V.V.G., Zhang, Y., Kaur, K., Hahn, A., Srivastava, A., Sindhu, S.: Cyber-security analysis of transactive energy systems. In: 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T D). pp. 1–9. (2018)
15. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Cyber security challenges in Smart Grids. In: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies. pp. 1–8. (2011)
16. Martiskainen, M., Coburn, J.: The role of information and communication technologies (ICTs) in household energy consumption—prospects for the UK. Energy Efficiency. 4 (2), 209–221 (2011)
17. Min, K.-S., Chai, S.-W., Han, M.: An International Comparative Study on Cyber Security Strategy. International journal of security and its applications. (2015)
18. Moussa, B., Debbabi, M., Assi, C.: A Detection and Mitigation Model for PTP Delay Attack in an IEC 61850 Substation. IEEE Transactions on Smart Grid. 9 (5), 3954–3965 (2018)
19. NCCIC/ICS: NCCIC/ICS-CERT Year in Review (2015). Homeland Security. 24
20. Pearson, I.L.G.: Smart grid cyber security for Europe. Energy Policy. 39 (9), 5211–5218 (2011)
21. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 24 (3), 45–77 (2007)
22. Rehmani, M.H., Reisslein, M., Rachedi, A., Erol-Kantarci, M., Radenkovic, M.: Integrating Renewable Energy Resources Into the Smart Grid: Recent Developments in Information and Communication Technologies. IEEE Transactions on Industrial Informatics. 14 (7), 2814–2825 (2018)
23. Røpke, I., Haunstrup Christensen, T., Ole Jensen, J.: Information and communication technologies – A new round of household electrification. Energy Policy. 38 (4), 1764–1773 (2010)
23. Dang, D., Enterprise Architecture Institutionalization: A Tale of Two Cases. In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, pp 842–857 (2017)
23. Dang, D., Institutional Logics and Their Influence on Enterprise Architecture Adoption. Journal of Computer Information Systems 0:1–11. doi: 10.1080/08874417.2018.1564632 (2019)
24. Statistics Finland: Tilastokeskus: Uusiutuvan energian kulutus ensi kertaa suurempi kuin fossiilisten polttoaineiden ja turpeen kulutus, *Yle Uutiset*, https://yle.fi/uutiset/3-11887128, Accessed: April 18, 2021, (2021)
25. Sullivan, J.E., Kamensky, D.: How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. The Electricity Journal. 30 (3), 30–35 (2017)
26. Sun, C.-C., Hahn, A., Liu, C.-C.: Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems. 99 45–56 (2018)
27. Varela, I.: Energy Is Essential, but Utilities? Digitalization: What Does It Mean for the Energy Sector? In: Linnhoff-Popien, C., Schneider, R., and Zaddach, M. (eds.) Digital Marketplaces Unleashed. pp. 829–838. Springer, Berlin, Heidelberg (2018)
28. Vellaithurai, C.B., Biswas, S.S., Srivastava, A.K.: Development and Application of a Real-Time Test Bed for Cyber–Physical System. IEEE Systems Journal. 11 (4), 2192–2203 (2017)
29. Venable, J., Pries-Heje, J., Baskerville, R.: A Comprehensive Framework for Evaluation in Design Science Research. In: Peffers, K., Rothenberger, M., and Kuechler, B. (eds.) Design Science Research in Information Systems. Advances in Theory and Practice. pp. 423–438. Springer, Berlin, Heidelberg (2012)