2022

Exploring Cyber-Physical Systems' Security Governance in the Oil and Gas Industry

Soliman Mahmoud
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Soliman Abdel Hamid Abdel Gawad Mahmoud

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Danielle Wright-Babb, Committee Chairperson, Management Faculty
Dr. Carol Wells, Committee Member, Management Faculty
Dr. Anton Camarota, University Reviewer, Management Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Exploring Cyber-Physical Systems' Security Governance in the Oil and Gas Industry

by

Soliman Abdel Hamid Abdel Gawad Mahmoud

MA, University of Liverpool, 2008

BS, Cairo University, 2003

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

February 2022

Abstract

The Fourth Industrial Revolution, which utilizes modern communication-dependent technologies, including cyber-physical systems (CPS), has made exploration and production operations more efficient in the oil and gas industry. CPS in this industry should be secured against operational threats to prevent interruption of critical oil and gas supplies and services. However, these systems are vulnerable to cyberattacks, and many oil and gas companies have not incorporated effective cybersecurity measures into their corporate management strategies. This qualitative, multiple-case study, which was guided by the routine activity theory, explored how cybersecurity governance was applied to develop controls that stopped or mitigated the consequences of cyberattacks against the CPS. Interview-based data were obtained through Zoom meetings with 20 global cybersecurity experts selected from cybersecurity-specialized groups on LinkedIn. These data were then triangulated with global CPS cybersecurity governance standards and methods. The data analysis resulted in nine themes, including CPS vulnerabilities and failure consequences, predominant cybersecurity governance, the efficiency of cybersecurity governance, governance challenges, offenders and motives, cybersecurity enhancement, CPS governance endorsement, cybersecurity performance assessment, and governance mandate. This study's implications for positive social change include recommendations for applying cybersecurity governance strategies that reduce health and environmental incidents and prevent interruption of critical oil and gas deliveries due to cyberattacks. These results may also help improve the living conditions of the communities surrounding oil and gas fields and similar CPS-based industries worldwide.

Exploring Cyber-Physical Systems' Security Governance in the Oil and Gas Industry

by

Soliman Abdel Hamid Abdel Gawad Mahmoud

MA, University of Liverpool, 2008

BS, Cairo University, 2003

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

February 2022

Dedication

I thank God for the strength he has given me to begin and complete my Ph.D. I dedicate this work to the souls of my father, Abdel Hamid, and my mother, Amal, who provided me with continuous inspiration in all my career success and academic achievements. This work is also dedicated to my wife, Vian, my daughter, Aamal, and my sons, Hazem and Basem, who have been understanding and supportive through the stressful period of this doctoral journey. Finally, this work is dedicated to my friends Hassan Taher, Reda Sallam, Majed Al.Qarni, and Salah Al.Luqman for their support, encouragement, and unconditional love throughout my doctoral journey.

Acknowledgments

I want to thank my Dissertation Chair Dr. Danielle L. Wright-Babb, my committee member Dr. Carol M. Wells, and the University Research Reviewer Dr. Anton G. Camarota for the exceptional guidance, motivation, and support they have offered to help me achieve the successful completion of this doctoral journey. I would also like to thank my instructors who taught me the Ph.D. program courses, and the kind individuals who have helped me and contributed to the successful completion of this dissertation, including peer reviewers and the cybersecurity professionals who have contributed their knowledge through the interviews. I am also grateful to my family members and friends who offered me their love, trust, and support, without which I would not have achieved the successful completion of my Ph.D.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Cyber-physical systems (CPS) refer to a complex structure that encompasses computers, communication devices, sensors, and actuators of the physical infrastructures, either in systems-of-systems, assorted, open, or hybrid (Al-Mhiqani et al., 2018; Friedberg et al., 2017). CPS allows a broader range of products and electronic services that positively affect peoples' lives, including e-commerce, e-health, and smart cities (Yaacoub et al., 2020). In the oil and gas industry, CPS has made the exploration and production operations more efficient than ever before (Fataliyev & Mehdiyev, 2018). However, CPS-based oil and gas operations and similar industries and services use industrial control systems (ICS) that are vulnerable to cyberattacks (Kolisnyk et al., 2020). Thus, in this study, I addressed the role of cybersecurity governance (i.e., cybersecurity policies, standards, and best practices), in working towards more dynamic controls to stop or alleviate the effects of cyberattacks against CPS. There is a crucial need to secure CPS against cyberattacks and the consequential loss of control over operational safety in the oil and gas industry (Syed et al., 2017; Yaacoub et al., 2020). The results of this study may lead to a positive social change to the oil and gas industrial communities. For instance, governmental authorities' leaders and corporate managers may use this study to explore concepts, tools, and techniques to use cybersecurity governance to avoid interruption of critical supplies for communities, such as electricity and water.

In this chapter, I address the background of the study, problem statement, purpose of the study, research question, conceptual framework, nature of the study, definitions of operational terms, assumptions, scope and delimitations, limitations, and significance of the study. I conclude this chapter by providing a summary of its major sections and a transition to Chapter 2.

Background of the Study

CPS incorporates ICS to monitor and control industrial operations. Supervisory control and data acquisition (SCADA) is a form of ICS that encompasses graphical user interface, communication networks, and computers to manage the safe and optimum operations of remote processing equipment (see Alladi et al., 2020). Presently, one of the highest concerns correlated with most old-style ICS is that they use outdated software and operating systems that make them vulnerable to cyberattacks (Alladi et al., 2020; Kolisnyk et al., 2020). The 2017 Global Report about the state of ICS-based industries and services stated that approximately 54% of organizations worldwide had experienced an ICS security breach in 2017 (as cited in Schwab & Poujol, 2018, p. 15). According to Jindal et al. (2020), there is likely to be an upsurge in the risk of cyberattacks against CPS/ICS-based industries. Protecting CPS-based digital critical assets and infrastructures against cyberattacks has become crucial for survival and requires that corporate management of critical industries, such as oil and gas, incorporate proactive cybersecurity measures into their corporate management strategy (Shaik et al., 2017). The gap in knowledge on the CPS cybersecurity discipline that this study addressed was the use of governance as proactive measures to secure CPS operational safety and ensure uninterrupted supplies of critical services to communities, such as electricity and water supplies. Addressing this knowledge gap is essential because the current CPS safety and security policies, standards, and best practices are not yet operative enough in protecting the CPS-based industries and services, including the oil and gas industry (Asplund et al., 2018). CPS safety and security will bring new research challenges to researchers for decades to come as long as the industries continue to integrate physical things with computing capabilities (Cardenas & Cruz, 2019).

This study may contribute to enhancing CPS safety and security by promoting the role of cybersecurity governance as preemptive measures to prevent cyberattacks or mitigate their consequences, including operational incidents and interruptions of communities' critical services and supplies.

Problem Statement

Industry 4.0 refers to the Fourth Industrial Revolution, which utilizes modern communication-dependent technologies and systems (e.g., the Industrial Internet of Things [IIoT]) and CPS to develop smart manufacturing systems and electronic services (Vaidya et al., 2018). CPS allows a broader range of products and electronic services that can positively affect peoples' lives, including e-commerce, e-health, and smart cities (Yaacoub et al., 2020). In the oil and gas industry, CPS has made the exploration and production operations more efficient than ever before (Fataliyev & Mehdiyev, 2018). The downside is that connecting the cyber and physical aspects of CPS gives rise to new cybersecurity challenges; hence, there is a crucial need to secure CPS against cyberattacks and the consequential loss of control over operational safety in the oil and gas industry (Syed et al., 2017; Yaacoub et al., 2020). There are essential gaps in the literature related to CPS because the current CPS safety and security policies, standards, and best practices are not yet effective enough in safeguarding the CPS-based industries and services, including the oil and gas industry (Asplund et al., 2018).

The general problem is that CPS-based oil and gas operations use ICS that are vulnerable to cyberattacks (Kolisnyk et al., 2020). The latest global trends of the reported cyberattacks on ICS-based industries and services revealed that an average crash of a cyberattack on a company's ICS costs approximately $5M and 50 days of system downtime (Alladi et al., 2020). The 2017 Global Report on the state of ICS-based industries and services stated that approximately 54% of organizations worldwide had experienced an ICS security breach in 2017 (as cited in Schwab & Poujol, 2018, p. 15). There is likely to be an upsurge in the risk of cyberattacks against CPS-based industries and associated ICS (Jindal et al., 2020).

The specific problem is that 82% of the oil and gas respondents reported that their organizations were subject to cyberattacks in 2015, and 69% of these organizations indicated that they were not confident that their systems could detect cyberattacks (Tripwire, 2016, p. 1). The risk mitigation costs money, service interruption, and reputation consequences on the industry; cybercrimes and cyberattacks could harm a company's performance and the nationwide economy (Venkatachary et al., 2017). The current CPS safety and security policies, standards, and best practices are not yet operative enough in protecting the CPS-based industries and services, including the oil and gas industry (Asplund et al., 2018).

This study was essential and unique because it included analyses of three data sources with goals to bridge a noteworthy gap in the existing literature and added to the body of knowledge in the cybersecurity field. To achieve these goals, I explored the role of cybersecurity governance in working towards more dynamic controls to stop or alleviate the effects of cyberattacks against CPS.

Purpose of the Study

The purpose of this qualitative, multiple-case study was to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. The focus was on the safe and secure use of CPS as a pillar of Industry 4.0 in the oil and gas industry to provide an increased understanding of the safety and security concepts, tools, and techniques of CPS. The new knowledge gained from this study may help the standardization firms, regulatory bodies, and corporate cybersecurity managers discover new safety and security control elements to enhance the current CPS defense system through the effective use of cybersecurity governance.

Research Question

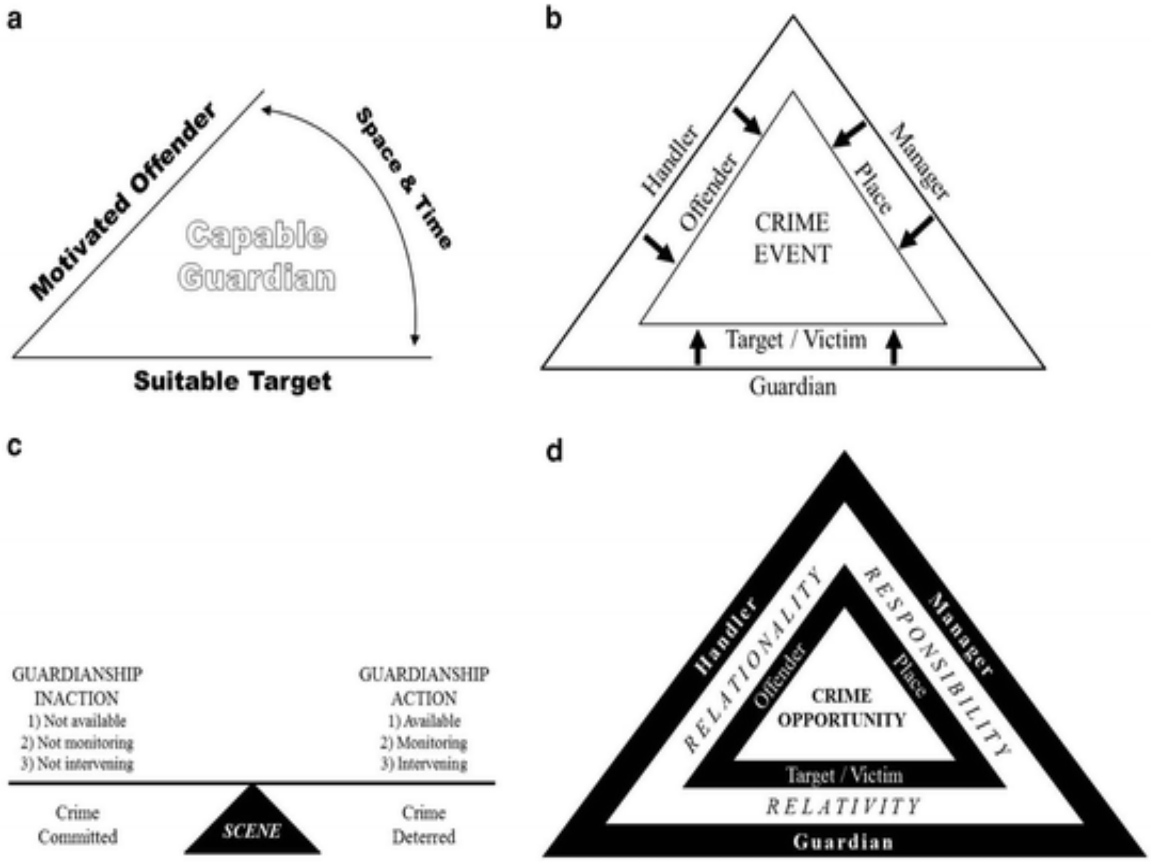
The main research question that guided this study was as follows: How can cybersecurity governance be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry? The interview questions used to gather data for this study are listed in Appendix A, which served as an instrument for this study.

Conceptual Framework

For this qualitative, multiple-case study, I employed the routine activity theory (RAT; Cohen & Felson, 1979) as a conceptual theory to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. The RAT became one of the principal descriptive theories on cybercrime; RAT may demonstrate a guiding theoretical framework for the daily practices of community-based cybercrime mitigation (Brady et al., 2016; Harada, 2018). The concepts in the RAT that grounded this study were Cohen and Felson's notions that every successful violation requires at least three factors: (a) an offender with criminal dispositions and the skill to carry out those predispositions, (b) a vulnerable target for the offender, and (c) a lack of protectors qualified to prevent violations. These three factors could help explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS-based industries and services by envisaging the target, threat, and protection in day-to-day routine activities (see Cohen & Felson, 1979). RAT was an appropriate conceptual theory for this study because it helped me explore the role of cybersecurity governance in stopping or mitigating the consequences of cyberattacks against the CPS through envisaging the target, threat, and protection in day-to-day routine activities. Figure 1 was developed by Schaefer and Mazerolle (2017), illustrating the waves of the RAT.

Figure 1

Waves in RAT



Note. Figure 1 was developed by Schaefer and Mazerolle (2017), showing waves in the RAT: (a) original formulation of routine activity theory, (b) extension of routine activity theory, (c) guardianship extension of routine activity theory, and (d) social process extension of routine activity theory. From "Putting Process Into Routine Activity Theory: Variations in the Control of Crime Opportunities", by L. Schaefer and L. Mazerolle, 2017, *Security Journal, 30*(1), p. 268 (https://doi.org/10.1057/sj.2015.39). Copyright 2017 by Schaefer and Mazerolle. Reprinted with permission.

The main research question, interview questions, and the RAT as a conceptual theory guided the literature review in Chapter 2. The literature search strategy was built on the three elements forming the RAT: (a) CPS security offenders, (b) vulnerable targets, and (c) the lack of protectors qualified to prevent violations of cybersecurity governance. More details about the literature search and review strategies are provided in Chapter 2.

Nature of the Study

I chose a qualitative, multiple-case study to explore the phenomenon of strategies on how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. A qualitative study was appropriate for this guiding research question and is suitable when a researcher needs to gain a deep understanding of a phenomenon and when asking *how* and *why* research questions to guide a study (see Solesvik, 2017). A qualitative, multiple-case study was a proper design for this study because it allows researchers to understand the phenomenon of study by analyzing and triangulating data from multiple resources, including governmental and corporate documents, archival data, and semistructured interviews (see Yin, 2018).

I used the RAT as a conceptual theory for this study because it could lead to answering the research question through foreseeing the target, threat, and protection in day-to-day routine activities (see Cohen & Felson, 1979). This research's primary data collection method was Zoom interviews with cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn. I audio-recorded and transcribed these interviews using Sonix audio-to-text converter software (see Sonix, n.d.). Such an online environment was suitable because the target participants were distributed across many geographical locations worldwide.

To ensure the generalizability and transferability of the study results, I conducted Zoom interviews with 20 CPS cybersecurity experts selected from a large population comprised of various professional associations, organizations, and industries, focusing on cybersecurity professionals with a minimum of 10 years of experience in the oil and gas industry so that they had the relevant knowledge to contribute to the study. I aimed for 20 participants from those whom I had initially invited via email and LinkedIn connect messages. I found that 20 participants were sufficient; Ogallo (2018) included 20 participants for a similar study. However, I intended to do fewer than 20 valid interviews if saturation had been achieved earlier. I conducted a thematic analysis of the interview transcripts.

I selected CPS safety and security governance endorsed and made publicly available by the international regulatory bodies and standardization firms as a secondary source of data. I conducted thematic analyses to make sense of the collected data. Another consideration to ensure this study's transferability was that only CPS security governance endorsed by internationally recognized standardization/regulatory firms and adopted globally by most CPS-based industries were selected for thematic analysis. The aim of thematic analyses of selected cybersecurity governance and the interview transcripts was to develop themes and conclude CPS cybersecurity threats, protection tactics, and a possible means to enhance these tactics. The framework was linked to the instrument used to gather data as I (a subject matter expert) served as the primary instrument to conduct the interviews, analyze their transcripts, and select and analyze relevant CPS cybersecurity documents. Information-rich cases were derived from experience and thematic analyses of the transcripts of the interviews as a primary data source, and the cybersecurity governance was selected as a secondary data source. Chapters 2 and 3 include more information on possible types and sources of data relevant to the nature of this study.

Definitions of Operational Terms

The following key operational terms were used in this study.

Cyber-physical system (CPS): A system comprised of physical processes, and a computational subsystem that encompasses computing devices and networking processes (Legatiuk et al., 2017).

Cybersecurity: The process of protecting internet-connected systems that encompass hardware, software, and data from cyberattacks by adversaries (Srinivas et al., 2019).

Cybersecurity threat: There are two types of threats to an organization's cybersecurity: (a) threats from people, including current and former employees, customers, vendors, and black-hat hackers and (b) nonpeople threats, including environmental factors such as flood and adverse weather (Alexander & Panguluri, 2017).

Governance: The act of using regulations, internal policies, standards, and procedures (Govindji et al., 2017).

Industrial control system (ICS): An ICS encompasses sensors, actuators, and a communication network to monitor and control the operation of physical equipment coupled with it (Zhang et al., 2019).

Assumptions

The oil and gas industry is a highly regulated industry due to the intrinsic health, safety, and environmental risks connected with the exploration, drilling, processing, production, and distribution activities. These regulatory requirements, in addition to a growing skill gap due to the retirement of highly experienced employees and the long-lasting low oil prices, have motivated oil and gas companies to find creative ways to increase productivity and efficiency and reduce operational risks through improving regulatory compliance (Wanasinghe et al., 2020). The oil and gas companies use CPS for their exploration, extraction, processing, and distribution operations (Shaik et al., 2017). There is an essential need for CPS security policies, standards, and procedures as governance to bridge the competence gap and reduce operational risks (Wanasinghe et al., 2020). A wide range of industrial CPS-based developments has been created and used as a part of Industry 4.0 (Lu, 2017).

The assumption is that the CPS security governances for the oil and gas industry apply to similar CPS-based industries such as smelters, chemical plants, smart transportation, aviation, marine, manufacturing, electrical power plants, and water supply stations. This assumption is necessary for ensuring the study’s external validity. To ensure the external validity of the entire study and increase its transferability, I thematically analyzed only CPS security governance endorsed by internationally recognized standardization/regulatory firms and adopted globally by most CPS-based industries. I also conducted Zoom interviews with 20 CPS cybersecurity experts selected from a large population comprised of various professional associations, organizations, and industries.

Scope and Delimitations

The scope of this study was delimited to the use of cybersecurity governance to protect CPS-based industries and services from cyberattacks. The specific focus on the use of cybersecurity governance was chosen to address particular aspects of the research problem in this study. A qualitative, multiple-case study using the RAT as a conceptual theory was conducted. The information was gathered from three primary sources: CPS/ICS cybersecurity governance ISA/IEC 62443 (also referred to as ISA 99/IEC 62443 or IEC 62443), NIST Special Publication (SP) 800–82, and interviews with cybersecurity professionals. To attain transferability of the study,

- The participants were 20 cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn, working for a wide range of international CPS-based industries and services, including oil and gas, petrochemicals, chemicals, smart transportation, electrical power plants, water treatment, cement smelters, IIoT development and transformation, and manufacturing.
- Only CPS security governance that are endorsed by internationally recognized standardization/regulatory firms and adopted globally by most CPS-based industries were selected for thematic analysis.

Limitations

Cybersecurity governance, such as policies, standards, and best practices, is a critical issue for organizations that struggle for success in protecting CPS-based assets from cyberattacks. What constitutes successful cybersecurity governance and practices is not yet clear, partly because concluding an exact percentage measuring cybersecurity success is not simple (Clark et al., 2020). Due to many variables affecting the success or failure of cybersecurity (e.g., employees' competencies, training, and the quality of the technologies used), sorting out a percentage measuring the contribution of governance alone to the success of cybersecurity in protecting CPS-based infrastructure may be inaccurate and doubtful. To overcome this limitation, quantifying the cybersecurity governance's efficiency against other variables was not considered part of this research scope. Consequently, a quantitative design approach was not used for this study.

Another limitation of this study was that it focused on cybersecurity governance designed to protect CPS-based industries as a pillar of the IIoT, which evolved from the Industry 4.0 revolution. Hence, the result of this study may be of limited use to non-CPS-based organizations that do not use monitors, sensors, communication means, transmitters, actuators, and final actors for their processes.

Significance of the Study

This study is significant because it may fill a gap in understanding the role of cybersecurity governance in enhancing the safety and security management of CPS. The literature reviewed suggested that the consequences of cyberattacks on the critical industries and services using CPS are upsurging (Gao et al., 2020). In the oil and gas industry, cyberattacks on CPS and associated ICS have resulted in a loss of control over the safety of critical operations, such as oil and gas exploration, extraction, processing, and distribution (Lamba, 2018). Potential health, safety, and environmental consequences of loss of control over operational safety include loss of lives, fires, explosions, emission of toxic substances, air pollution, and marine pollutions from oil spills (Shen et al., 2020). Response to such potential cybersecurity incidents has become a crucial need for the oil and gas industry and similar critical businesses and services. Organizations pursuing control over such cybersecurity threats must acquire or develop governance policies to provide a framework for their human and technical resources (Clark et al., 2020; Gao et al., 2020). This study may contribute to these efforts by adding to the current knowledge on using the cybersecurity governance to protect CPS from cyberattacks.

Significance to Practice

One of the essential gaps in the literature related to the safety and security of CPS is that the current CPS governances are not yet successful enough in protecting the CPS-based industries and services, including the oil and gas industry (Asplund et al., 2018). The cybersecurity practitioners, scholars, policymakers, regulatory specialists, and corporate managers may use this study to understand better how to manage cyberattacks by enhancing and enforcing CPS cybersecurity governance.

Significance to Theory

This study may contribute to advancing the knowledge in the cybersecurity discipline as it addresses the research problem through envisaging the three elements forming the RAT: the CPS security offenders, vulnerable targets, and the lack of protectors qualified to prevent violations of cybersecurity governance. Data were gathered from multiple sources and analyzed to help explore how cybersecurity governance can be used as security controls to prevent or mitigate the harmful consequences of cyberattacks on CPS-based infrastructures. At organizational and societal levels, this study may contribute to promoting CPS safety and security measures endorsed by the industrial communities using the CPS-based products and services, cybersecurity standardization firms, and regulatory bodies.

Significance to Social Change

The results of this study could lead to a positive social change to the oil and gas industrial communities. For instance, governmental authorities' leaders and corporate managers may use this study to explore concepts, tools, and techniques to use cybersecurity governance to avoid interruption of critical supplies for communities, such as electricity and water. This study could also help reduce the number of health and environmental incidents resulting from cyberattacks on CPS and subsequently improving the living conditions of the communities surrounding oil and gas fields and similar industries and services worldwide.

Summary and Transition

In this chapter, I provided an introduction, followed by a background of the study. I described the research problem and specified the general problem and specific problem concerning the cyberattacks on the CPS-based infrastructures and the role of cybersecurity governance in precluding or eradicating the harmful consequences of these cyberattacks. I specified the purpose of the study, stated the research question, and provided detailed explanations of the conceptual framework and the nature of the study. This chapter also included descriptions of the operational terms, assumptions, scope and delimitations, limitations, and significance of the study.

Chapter 2 includes the results from the search and review of published literature supporting the propositions and claims in this study. The literature search strategy was built on the problem statement, main research question, and supplementary interview questions concerning the use of cybersecurity governance as controls to protect CPS from cyberattacks.

Chapter 2: Literature Review

CPS-based oil and gas operations use ICS that are vulnerable to cyberattacks (Kolisnyk et al., 2020). The 2017 Global Report on the state of ICS-based industries and services stated that approximately 54% of organizations worldwide had experienced an ICS security breach in 2017 (as cited in Schwab & Poujol, 2018, p. 15). In 2015, 82% of the oil and gas respondents reported that their organizations were subject to cyberattacks, and 69% of those organizations indicated they were not confident about their systems' capability to detect cyberattacks (Tripwire, 2016, p. 1). There is likely to be an upsurge in the risk of cyberattacks against CPS-based industries and associated ICS (Jindal et al., 2020). Cybercrimes and cyberattacks could harm a company's performance, as well as the national economy (Venkatachary et al., 2017). The purpose of this qualitative, multiple-case study was to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry.

The purpose of this chapter is to analyze and synthesize the current literature on the phenomenon of cyberattacks on CPS-based industries, especially the oil and gas industry. This chapter addresses the literature search strategy and introduces the RAT and qualitative document analysis as a conceptual theory and framework consistent with the scope of this study. Key concepts addressed and topics related to the problem on which this research project was structured and addressed in this chapter include CPS and ICS as critical infrastructure, cyberattacks as threats to CPS/ICS, CPS/ICS cybersecurity countermeasures, cybersecurity concerns in oil and gas industry, state of cybersecurity governance, conceptual framework and methodology, and gaps in literature.

Literature Search Strategy

I searched, reviewed, and selected literature on the safety and security of CPS from many sources and in various formats, including books, publicly available governmental regulations, standards and procedures by standardization and regulatory bodies, peer-reviewed articles published in specialized journals and international conference proceedings, and master's theses and doctoral dissertations. Databases searched included EBSCO Host, ERIC, Google Scholar, ProQuest, OnePetro, Springer, IEEE Xplore, and ScienceDirect. Search string used (*Industrial Internet of Things* OR *IIoT* OR *cyber-physical systems* OR *CPS* OR *industrial control systems* OR *ICS*) AND (*oil* AND *gas*) AND (*policy* AND *standard*) AND (*cybersecurity* OR *cyber security*). Using these keywords, I searched for articles published from 2017 onwards. I obtained 905 articles, out of which 420 articles were identified as relevant to the research problem, research design, and research question if they fell under one or more of the following topics: CPS and ICS as critical infrastructure, cyberattacks as threats to CPS/ICS, CPS/ICS cybersecurity countermeasures, cybersecurity concerns in oil and gas industry, state of cybersecurity governance, conceptual framework and methodology, and gaps in literature.

The relevance of the articles to the study was decided after manual screening of their titles, abstracts, introductions, and conclusion sections, and analyzing their content against the problem statement, main research question, and interview questions, focusing on the following keywords: Industry 4.0, IoT, IIoT, CPS, cybersecurity, policies, standards, oil and gas, cybersecurity threats, types of attacks, protection against cyberattack, management role, organizational resources, CPS safety and security framework, incident reporting, and knowledge sharing. I used the general search keywords *Industry 4.0, IoT, IIoT* to obtain literature addressing CPS as a pillar of these developments and the use of cybersecurity governance within their context. I prioritized the articles published in the last 4 years and created a weekly alert on Google Scholar to obtain more original references as they become available through Google Scholar's search engine. The in-text citations were checked against the reference list in this document using the *Reference Checking Made Easy* on the Recite Beta (2020) Website.

Literature Review

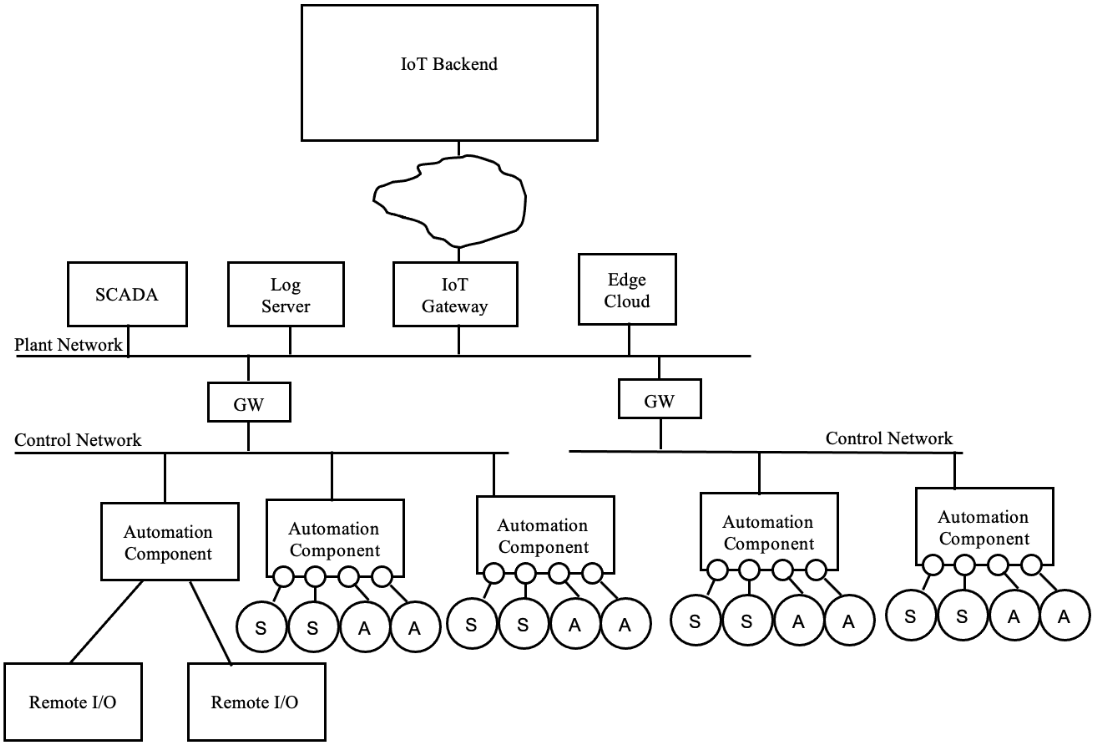
This section includes a thorough review of the current literature that includes information concerning the key concepts of this study.

CPS and ICS as Critical Infrastructures

CPS are controllable and extensible network physical systems, integrated with communication, computation, and control capabilities to interact with humans via many modern modalities. CPS are the base and the core of Industry 4.0 and the IIoT, and they operate based on real-time process monitoring and control functionalities (Lyu et al., 2019). A typical CPS contains an ICS that encompasses monitors, sensors, transmitters, and control elements to operate a production or processing unit automatically. Examples include energy automation, machine control, process automation, and cloud robotics. In an ICS, sensors (S) and actuators (A) are directly linked with automation elements or via remote input/output (I/O) modules. The mechanical process is controlled by measuring its current state using the sensors, then regulating the corresponding signals to actuators to achieve the desired state (Falk & Fries, 2020). Figure 2 shows an example of CPS/ICS as described by Falk and Fries (2020).

Figure 2

Example of CPS/ICS



Ding et al. (2020) suggested that the well-organized integration of physical processes and cyberinfrastructure with universal computation things and communication means significantly increasing CPS's rapid development in theoretical searches and engineering applications. CPSs use networks of multifunctional sensors, actuators, and cyber components to allow numerous monitoring and control operations. These computing and communication devices are linked together via shared communication networks, either wireless or wired, to achieve data sensing, gathering, processing, and transmitting functions. CPS plays a critical role in the Fourth Industrial Revolution; CPS forms the core of modern industries, innovative manufacturing systems, and essential applications including smart cities, medical monitoring systems, distributed robotics, intelligent transportation systems, and generation and distribution of critical supplies (e.g., electrical power, water, and gas; Ding et al., 2020; Lamba, 2020).

Alladi et al. (2020) noted that CPS use ICS to monitor and control industrial operations. SCADA is a kind of ICS that encompasses graphical user interface, communication networks, and computers to safely operate remote processing equipment while obtaining the maximum production from the equipment. ICS comprise integrated hardware and software mechanisms to monitor and control numerous industrial processes and are deployed in many key industries and critical infrastructures such as oil and gas processing, chemical processing, electrical power plants, water treatment stations, transportation, and manufacturing (Feng et al., 2019; Shen et al., 2020).

Stouffer et al. (2015) provided a wider description of the ICS constituents, stating that ICS combine a variety of control systems, including SCADA systems, distributed control systems (DCS), and other control system designs such as programmable logic controllers (PLC) that are usually found in the critical infrastructures and industrial sectors. To conclude, CPS/ICS contain combinations of control elements (e.g., pneumatic, hydraulic, mechanical, electrical) that interact through a predefined process to accomplish an industrial objective such as manufacturing and transport of matter or energy.

Cyberattacks as Threats to CPS/ICS

CPS and associated ICS are vulnerable to cyberattacks by many people, including an organization's current and former employees, customers, vendors, and black-hat hackers (Alexander & Panguluri, 2017). As a critical infrastructure, the oil and gas companies are more susceptible to face the escalating risk of cyberattacks than those threatening other companies. Cyberattacks on ICS in the oil and gas industry can have disastrous consequences on the economy and national security (Lamba, 2018).

Ding et al. (2020) classified cyberattacks on CPSs into two types, denial-of-service (DoS) attacks and deception attacks and explained that the objective of DoS attacks is to disturb data availability and exchangeability by maliciously consuming the capacity of communication/computation assets. One of the tactics to do so is by occupying channels or overriding the central processing unit or depleting memory capacity. As a result of such hostile acts, data may not be obtained or directed successfully to its intended destination. If data availability is completely disrupted, the sender and receiver's mapping function may be denoted as a null set. The goal of deception attacks is to compromise data integrity and trustworthiness by deploying packets over communication networks while keeping them stealthy to detectors (Ding et al.).

Ahmad et al. (2018) claimed that security threats and privacy are some of the most severe aspects of CPS, which is true as CPS components share enormous information and data. Ahmad et al. divided the CPS security/vulnerabilities into two main categories, information security/vulnerabilities and control security/vulnerabilities, specifying that information security/vulnerabilities involve CPS-related systems (e.g., embedded system, communication, networking, databases, and cloud services). In contrast, control security/vulnerabilities include attacks on sensors, actuators, and control devices. Based on Ahmad et al.'s claims, Table 1 provides the descriptions of possible attacks and countermeasures related to the two categories of CPS security/vulnerabilities.

Table 1

Overview of CPS Security Threat Events and Countermeasures

Attack/vulner. category	Threat event	Attack/threat event description and countermeasures
Control/hardware	Physical exploitation	One of the most superficial CPS attacks for an attacker is the physical exploitation of hardware and sensors networks. Physical exploitation attack is more prominent in open access CPS, where sensors network is effortlessly accessible to the public. An example of physical exploitation is an attack on a smart energy meter that automatically calculates energy consumption and conveys it to the energy company. This energy meter is accessible to the attacker who may corrupt the data by corrupting the sensing elements, causing financial losses to the energy company (Ahmad et al., 2018; Wurm et al., 2016). One of the possible solutions to such hardware vulnerabilities is using smartly protected hardware. In such a manner, the sensor and its internal circuitry are adequately sealed and may generate an alarm when an attacker attempts to remove the seal.
Control/control systems	System model estimation (also known as key plan text attack)	System Model Estimation: An attack occurs when the attacker figures out the model of the control system of CPS by detecting the data flow between sensors, actuators and associated control system, then launch various attacks. So, the primary purpose of detecting the model is to manipulate all system vulnerabilities (i.e., the main target of such an attack is the closed-loop control system). The countermeasure to this attack is implementing encryption into the controller to improve its design. Ahmad et al. (2018) noted that typical controllers have limited computation capability; thus, encryption may affect the controller performance. Since encryption is an essential security measure, the designers have to make a wise compromise between CPS performance and security.
Control/sensors and controllers	False data injection attack (FDIA)	In this method of attack, an attacker injects false sensor data into the sensor controller. FDIA can be mainly used to damage smart grids, smart homes and CPS-based services. The ultimate goal of an FDIA attack might be preventing a physical device or an actuator from performing its intended operation or cause financial loss to a company. FDIA effectively be detected using a cross-correlator. Other countermeasures to prevent FDIA include data encryption, using Intelligent Checkers (IC), using the system's dynamic property to deliver strong observability of the physical and control elements, and including a security layer in smart devices and sensors (Abdallah & Shen, 2010; Ahmad et al., 2018; Chen et al., 2015; Mo et al., 2010; Potluri et al., 2020; Sabaliauskaite & Mathur, 2013, 2014; Wei & Mendis, 2016). Embedding a security layer in smart devices and sensors may reduce the CPS performance due to the limited computational power of the sensors and other small appliances. Yet, the designers must make a wise balance between CPS safety and performance.

Attack/vulner. category	Threat event	Attack/threat event description and countermeasures
Control/Sensors	Zero state inducing	An attacking method that can be continued for an arbitrarily long time, beginning at zero. In zero state inducing attack, the alteration in output is equal to the system's response when its initial state is zero (i.e., x (0) = 0). These attacks strike the CPS's weakly monitored places. Usually, zero state inducing attack is undetectable. A practical solution to control Zero State Inducing Attacks is using Dynamic Attack Detector (Ahmad et al., 2018; Chen et al., 2017).
Information/ embedded systems	Bootstrap vulnerabilities	One of the significant risks to CPS is experienced during system boot-up. At boot-up time, the system loads resources with the help of a bootstrap program. A standard bootstrap program has no security assurance. There is no mechanism to stop the execution of an unauthorized program, which is a kind of security threat to CPS. A secure bootstrap program contains code authorization. Before executing any code, the safe bootstrap program authorizes that code. The authorization is typically obtained through the signature of a trusted authority. Any unauthorized code is instantly stopped from being executed (Ahmad et al., 2018).
Information and control/internet services for sensors	Malware	According to Min and Varadharajan (2014), Malware refers to software that grants unauthorized access to any system and gathers sensitive information. Malware is one of the probable threats to the CPS. Malware can impair or pervert CPS-based applications like smart grids, smart homes, power plants, and water treatment and distribution stations. Malware can steal sensitive data or induce harmful behavior of physical systems. Min and Varadharajan (2015) have introduced an attack technique acknowledged as FDM (feature distributed Malware), which can be used to attack Internet-enabled CPS. The proposed FDM launches attack on the low-computation and less-secure smart devices such as network cameras, LEDs etc. FDM targets intelligent sensors and other low-cost devices due to their limited security compared to other cyber systems with high computation capabilities. FDM uses their service connection to launch other hateful attacks. Increasing sensor security is the solution to FDM attacks.
Information/ communication	Man-in-the-middle (MitM) attack	MitM is an attack on the CPS, takes place when an attacker attempts to snoop on communication between a cyber-system and a server. While inserting himself into the communication, the attacker may inject false information and interrupt data transfers between elements of a cyber system. MitM attacks can be prevented by using virtual private networks for CPS communications.

Attack/vulner. category	Threat event	Attack/threat event description and countermeasures
Information/ control of CPS	Service degradation attack	This type of attack targets the control loop to reduce the overall efficiency of the CPS. Service Degradation may also decrease the mean time between failures (MTBF) of the system by injecting false data into the system. Some of the attackers' tactics to degrade the CPS is creating a steady-state error or producing an overshoot during the system's transient response time. These attacking tactics may damage physical systems in CPS. Prevention of Service Degradation attacks is possible using network segmentation, firewall governance, and demilitarized zones in the system. These measures may prevent the attackers from accessing the CPS control loops, consequently prevent Service Degradation attacks.
Information/ remote communication	Backdoor attack	A computer program enables an attacker to gain unauthorized access and maintain access to a CPS. The attacker may use such unauthorized access for launching various attacks. A system Backdoor may be a serious security concern for CPS since it targets the design of hardware and other embedded systems. Backdoors may either be generated by a software developer for remote administration purposes or by an intruder (Ahmad et al., 2018). Hashemi and Zarei (2020) conducted a comprehensive study of the Backdoor attacks in the IoT context, in which they explain that Backdoor can bypass security devices to gain unauthorized access to the IoT system remotely without any authentication, identification, or authorization access control. Therefore, every smart device that includes firmware may have a backdoor problem. Hashemi and Zarei concluded that there are limitations in detecting Backdoors or malware analyses as Backdoors display different behaviors in different situations; hence, Backdoor detection is very complicated. Researchers need to search new methods, develop devices, or create algorithms that have never been deployed before to prevent Backdoors
Information/ software	Software exploitation	Any hardware in CPS is driven by software that is similar to the general cyber systems in traditional PC. Therefore, the vulnerabilities discovered in these traditional computing systems could also be threats to CPS. The solution lies in the software updates that are always available to CPS when released for these general computing systems (Ahmad et al., 2018; Wurm et al., 2016).

Attack/vulner. category	Threat event	Attack/threat event description and countermeasures
Information/ embedded systems	Denial of service (DoS)	Ahmad et al. (2018) suggested that DoS refers to the event when the system resources are over drowned to the extent the appropriately privileged user is restricted from the access or unable to use system resources. A more harmful sort of DoS is Distributed DoS (DDoS), in which many hosts attack the target concurrently. On October 21, 2016, the largest Distributed DoS attack was launched against Dyn servers in the USA through a small CPS and IOT devices, shutting down sites like CNN, Twitter, and Guardian. This attack shows that little, non-secure CPS devices may be a security risk for themselves and other systems. Countermeasures to such attacks are implementing improved network infrastructure, DoS mitigation ability in the CPS scheme itself or a nearby cloud network, or forward path to the target. (Ahmad et al., 2018; Nur & Tozal, 2016)

Appendix E in the NIST SP 800-30 Revision 1 classifies a comprehensive set of threat events that could impact information systems (see Joint Task Force Transformation Initiative, 2012). Some of these threat events have been addressed in recent works on CPS and ICS (see Ahmad et al., 2018; Potluri et al., 2020). Stouffer et al. (2015) suggested that a threat is an event or situation that might produce an undesirable consequence or impact on the ICS, resulting from some threat source. Stouffer et al. have also noted that properties of an ICS may present unique threat events, addressing how the threat events can manipulate the process of the ICS to cause physical damage. Table 2 was developed based on Stouffer et al. (2015), Table C-8, p. C-10, showing examples of common threats to ICS.

Table 2

Examples of ICS Threat Events

Threat event	Description reference
Control devices reprogrammed	Unauthorized changes to programmed commands in PLCs, RTUs, DCS, or SCADA control units, alarm thresholds, or unauthorized orders to control equipment. Such unauthorized could damage equipment (if tolerances are exceeded), sudden shutdown of processes (such as injudiciously shutting down transmission lines), causing an environmental incident, or deactivating control equipment.
Control logic manipulated	Modifying the control system software or its configuration settings modified, aiming at producing unpredictable results.
Denial of control action	Interrupting the operation of control systems by delaying or blocking the flow of information, thus restricting the network availability to control system operators, or triggering information transfer bottlenecks or denial of service (DoS).
Malware on control systems	Injecting malicious software into the ICS (e.g., virus, worm, Trojan horse).
Safety systems modified	Manipulating the safety systems' operation so that they either do not operate or deliver their functions when needed or perform inappropriate or unsafe control actions.
Spoofed system status information	Sending false information to the control system operators either to hide unauthorized changes or to pledge inappropriate or unsafe actions by system operators.

According to Nygaard and Mukhopadyay (2020), Dragos Inc. released a report in August 2019, highlighting five opponents targeting the oil and gas industry that include: (a) XENOTIME, which was first detected in Saudi Arabia in 2017, then expanded to attack oil and gas companies in Europe and the US in 2018. According to Dragos Inc., these attacks compromised the ICS of numerous manufacturers and threatened a supply chain; (b) MANELLIUM, which has been affecting petrochemical corporations since 2013, but they seem to lack an ICS-specific capability; (c) CHRYSENE was linked to the 2012 Shamoon cyberattack on Saudi Aramco Oil Company and is still evolving in more areas; (d) HEXANE, which was first introduced by Dragos Inc. in 2019, but there has not been much identified yet about its capabilities; (e) DYMALLOY, which is a very aggressive and talented activity group with the ability to acquire long-term and persistent access to IT and operation technologies like ICS for intelligence gathering and possible future distraction events (Nygaard & Mukhopadyay, 2020). Comprehensive analyses of the past ICS disruptive events like these are necessary to identify the proactive measures to be taken to prevent these attacks or mitigate their consequences.

Slowik (2019) conducted detailed analyses of the ICS disrupting incidents from the past 4 years to understand how these threats have progressed over time and concluded that defensive measures are needed to conquest these attacks. Slowik suggested that an in-depth understanding of the risks posed by ICS attacks will help stakeholders from ICS operators to policymakers to identify and implement rigorous controls and security measures to protect critical infrastructure and preclude potential catastrophic cyberattacks.

An analysis of previous cybersecurity incidents could help to gain an in-depth understanding of the risks posed by ICS attacks. Iaiani et al. (2020) conducted a comprehensive study of cybersecurity-related incidents, in which they developed “Table A.2. Cybersecurity-related incidents used in the discussion of the phases of intentional attack and countermeasures” (pp. 40–42). That Table A.2. provided deep analyses of 67 international attacks launched on CPS/ICS parts and describes the attacks, attackers, impacts, and countermeasures implemented. Such deep analyses provide understanding of risks to CPS/ ICS and insights into possible counterparts to prevent the release of these risks. The ICS incidents reported suggest that besides physical damage, the threat events resulted in fatalities, interruption of critical services and supplies, environmental damage, and reputation damage.

CPS/ICS Cybersecurity Countermeasures

Alladi et al. (2020) conducted case studies of significant attacks on ICS in the last 20 years and concluded that cybersecurity could be more enhanced by compliance with the International Electrotechnical Commission (IEC) 62443, which is a worldwide standard for the security of ICS networks. Based on analyses of cyberattack cases in their studies, Alladi et al. recommended the following six protection measures for the protection of ICS: regular updates to the firmware and software on CPS’s industrial computers; using at least two-factor authentication for logging into private ICS servers; changing passwords for CPS/ICS at methodical intervals; enhancing and updating (through regular professional training) the competency of employees who oversee and manage ICS’s security; establishing a provision for manual overrides and fail-safe modes so that detection and shutdown of the system can occur once the system is interfered with; and imposing a policy to prohibit the use of USB drives on CPS/ICS without rigorous antivirus checks.

The U.S. Department of Homeland Security (DHS) recommended defense-in-depth practices, composed of the following five countermeasures for the protection of networks: identifying, decreasing, and securing all network connections; strengthening the network and supporting systems by restricting redundant services, ports, and protocols while enabling existing security features and implementing vigorous configuration management practices; continual monitoring and assessment of the cybersecurity systems, networks, and interconnections; applying a risk-based defense-in-depth method to secure systems and networks; and managing the human element through specifying security requirements for networks, creating policies, and providing network security training for all administrators and operators (see Lamba, 2018).

Cybersecurity measures have the most significant effect when they are proactive rather than reactive. The following proactive control measures are recommended for managing the CPS/ICS cybersecurity: monitoring of systems configurations to detect security flaws, intrusions, and signs of compromise; obtaining filtered standardized logs, associating, and analyzing records with state-of-the-art technologies; providing training for employees; and carrying continuous hunting of threats grounded on proactive cybersecurity policy. More proactive cybersecurity measures include performing irregularity analyses; detecting artifacts or adversary tools: using indicators of compromise (IoCs), generating hypotheses to test against diverse data sources while watching for hidden new threat activity, and using automated detection tools to detect security weaknesses in the dynamic domain of ICS (see Dimitrov & Syarova, 2019; Pfrang et al., 2018).

Iaiani et al. (2020) suggested that the current international cybersecurity governance provides security countermeasures, tools, risk management approaches, policies, and best practices intended to protect a user or organization's cyber environment. Some cybersecurity standards are information-specific, while others are intended for the security of operation technology (OT) systems, such as CPS/ICS. ISO/IEC 27000 family of standards addresses information security management. Standard ISO/IEC 27005 is primarily intended to aid with the implementation of information security grounded on a risk management method that includes risk assessment, risk treatment, and monitoring. The standard ISA/IEC 62443 addresses the OT's security by providing a dynamic framework to identify and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS). Notably, part 3-2 of ISA/IEC 62443 guides organizations to assess risks to IACS, identifying and executing appropriate security countermeasures to reduce IACS risks to tolerable levels (see Iaiani et al.).

Stouffer et al. (2015), in the NIST SP 800-82 rev. 2, introduced the defense-in-depth strategy as an effective cybersecurity program that ICS-based organizations should apply by layering security mechanisms such that the impact of a failure in any one mechanism is minimized, while the expense of an attack is maximized. Stouffer et al.

suggested that an ICS security program based on the defense-in-depth strategy should include the following:

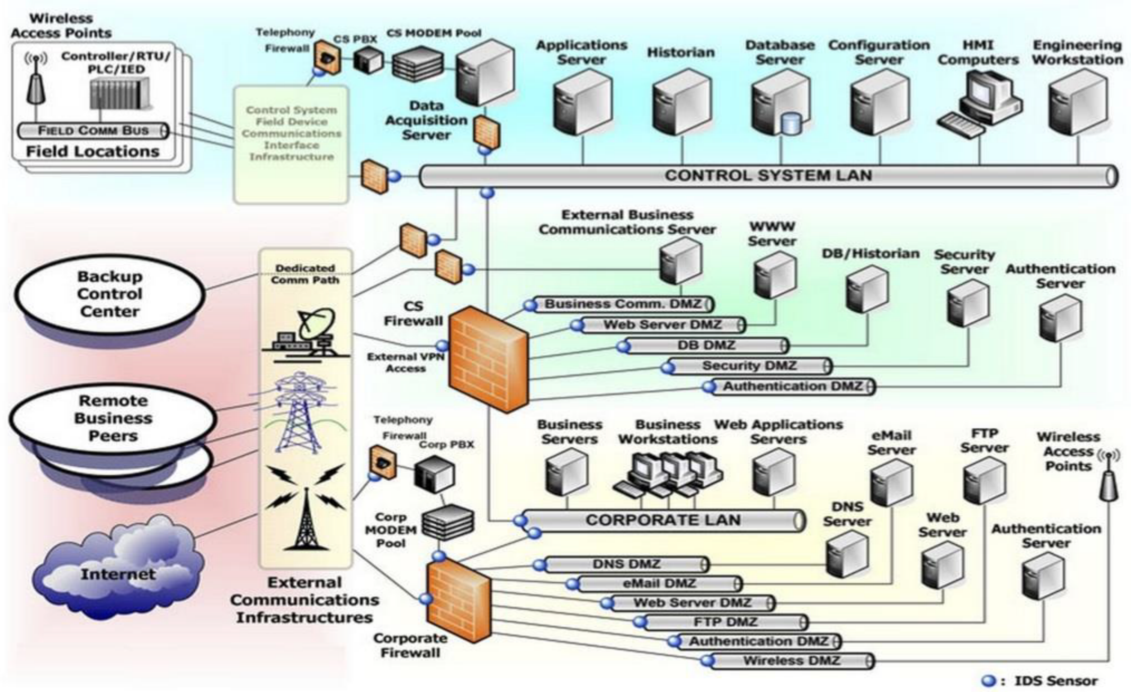
- ICS-specific security policies, procedures, training, and educational material addressing security throughout the ICS's lifecycle from architecture design to decommissioning.
- ICS security governance based on the Homeland Security Advisory System Threat Level.
- Employing a network topology for the ICS with multiple layers.
- Logical split between corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).
- Using a demilitarized zone network architecture to stop direct traffic between the corporate and ICS networks.
- Critical components are redundant on redundant networks.
- Scheming critical systems for graceful degradation or fault tolerance to avoid disastrous cascading events.
- Deactivating idle ports and services on ICS devices.
- Confining physical access to ICS's network and associated devices.
- Limiting ICS user privileges to only those that are required to perform each person's job.
- Separate credentials and authentication methods for users of ICS network and the corporate network.

- Using modern technologies, like smartcards for Personal Identity Verification (PIV).
- Using updated software intrusion detection, antivirus, and file integrity checking software to secure the ICS.
- Using security methods such as encryption and cryptographic hashes to ICS data storage and communications.
- Monitoring and tracking audit trails for critical parts of the ICS.
- Using secure network protocols.

Abdelghani (2019) suggested that defense-in-depth strategy encompasses people on technology, processes, governance, and other pillars of a typical defense-in-depth strategy, including governance, physical, network, computers, applications, and devices. Figure 3 was developed by Stouffer et al. (2015), showing a recommended defense-in-depth architecture.

Figure 3

Recommended Defense-in-Depth Architecture



Note. Figure 3 was developed by Stouffer et al. (2015), showing a recommended defense-in-depth architecture. From "*NIST Special Publication 800-82 rev 2: Guide to Industrial Control Systems (ICS)",* p. 62, by Stouffer et al., 2015, National Institute of Standards and Technology (NIST*),* U.S. Department of Commerce, (http://dx.doi.org/10.6028/NIST.SP.800-82r2). In the public domain.

Cybersecurity Concerns in Oil and Gas Industry

DNV-GL prepared a report for the Lysne Committee, listing the following top 10 factors contributing to the vulnerabilities of cybersecurity in the oil and gas industry: the absence of cybersecurity awareness and training amongst employees; remote activities during operations and maintenance; the use of standard IT products with recognized vulnerabilities in the production areas; a limited cybersecurity culture amongst suppliers, vendors, and contractors; inadequate separation of data networks; using mobile devices and storage units, including USBs and smartphones; data networks between onshore and offshore facilities; inadequate physical security of data-storage facilities; vulnerable software; and using obsolete ICS (Winther, 2015).

Graham et al. (2018) implicitly highlighted the above cybersecurity concerns, adding the following *operational challenges* to ICS operators: a lack of new initiatives' buy-in from higher managers due to an underestimated valuation of the return on investment in the resources available to strengthen the ICS cybersecurity, management incapability to make a balance between IT security governance and ICS operation and maintenance procedures, lack of a well-developed business case for ICS cybersecurity, lack of risk management incorporation across the enterprise, and cultural differences hindering the collaboration between IT and OT at many enterprises. A corporate strategy is needed to use all resources available for strengthening the CPS/ICS safety and security, using cybersecurity governance as a tool.

State of Cybersecurity Governance

Governmental authorities, regulatory bodies, and standardization firms endorse many policies, standards, and guidelines as governances that CPS-based businesses can use to defeat cyberattacks on critical infrastructure. Many researchers suggested that the CPS cybersecurity governances are publicly available from the following well-reputed and internationally-recognized standardization and regulatory bodies: the International Society of Automation (ISA), IEC, American National Standards Institute (ANSI), the

U.S. National Institute of Standards and Technology (NIST), and the North American Electric Reliability Corporation (NERC) (Cardenas & Cruz, 2019; Lyu et al., 2019; Ross et al., 2018; Yoo & Shon, 2016; You et al., 2019).

You et al. (2018) expected that the research guided by the existing information protection and ICS-related standards would enhance the ICS security level. In a study funded by the Korean government, You et al. (2018) identified the following CPS/ICS safety and security related governances: ISO/IEC 27001 as an international standard describing the requirements for the information protection management systems; ISA 62443 is recommended for the protection of ICS's information; ISA 62443 3–3 defines security technologies and security requirements for ICS's physical security and software security, authentication, access control, log auditing, and cryptography.

Specific CPS/ICS governances recommended by researchers include: NIST SP 800–82, which is intended for the protection of ICS (see Ross et al., 2018); CPS safety standards that include IEC 61508, IEC 61511, and IEC 61850 (Lyu et al., 2019; Yoo & Shon, 2016). Table 3 provides more descriptions of the recommended information safety and security governance, including the CPS security governance.

Table 3

Recommended Information Safety and Security Governance

Governance	Description	References
ISO/IEC 27001	ISO/IEC 27001 is one of ISO 27000 set of standards aiming to guide organizations in keeping their information assets secure. ISO/IEC 27001 provides requirements for an information security management system (ISMS), which is a systematic tactic for managing the security of sensitive information throughout organizations' lifecycle. It applies to all sizes of businesses in any sector. ISO/IEC 27001 specifies mapping for establishing, implementing, sustaining and persistently improving ISMS by using the Plan-Do-Check-Act (PDCA) model.	(Accerboni & Sartor, 2019; Barafort et al., 2017; Ganji et al., 2019)
ISA/IEC 62443	ISA/IEC 62443 has been established by the IEC and ISA99 committees to enhance the security, availability, integrity, and confidentiality of the constituents or systems used in industrial automation and control and is the cybersecurity governance that defines the fundamental safety barriers and measures for the control and autonomous systems in cyberspace. ISA/IEC 62443 also specifies how to apply the technical and operational measures of these safety barriers, for example, in production networks of Industry 4.0.	(ANSI/ISA, 2013; Mlynek et al., 2020; Prochazka et al., 2020; Ruiz et al., 2020)

Governance	Description	References
IEC 61508	IEC 61508 series stipulate functional safety standards for the lifecycle of electrical, electronic, or programmable electronic (E/E/PE) systems and products and addresses the safety of elements or systems that execute automated safety functions such as sensors, programmable logic control, actuators and micro-processors. IEC 61508 provides guidelines for developing an undeviating technical policy that can be used for all electrically based safety systems across a wide range of industry sectors and requires the analysis of possible risks or hazards to a given system or device. IEC 61508 suggests categories to decide the level of likelihood of a potential hazard and associated consequences should it arise and defines four safety integration levels (SIL) to designate the degree to which an electrically based system will perform its specified safety functions.	(International Electrotechnical Commission (IEC), 2021; Zhang et al., 2020)
IEC 61511	IEC 61511 Functional safety - Safety instrumented systems for the process industry sector. This series of standards addresses numerous hazards to process industries that may lead to loss of containment, resulting in harm to health, safety, environment, and plant assets. IEC 61511 series were developed based on the assumption that process safety is best achieved by adopting inherently safe processes. When this goal is not practically possible, protective systems are needed to mitigate the potential risk of hazards to an acceptable level. There are three parts to IEC 61511 series: • IEC 61511-1:2016, Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware, and application programming requirements • IEC 61511-2:2016, Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1:2016 • IEC 61511-3:2016, Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels.	(International Electrotechnical Commission (IEC), 2018)

Governance	Description	References
IEC 61850	Cai et al. (2018) noted that IEC 61850 standard establishes an integrated communication protocol. International Electrotechnical Commission (IEC) (2013) suggested that IEC/TR 61850-1:2013 is used for power utility automation systems and specifies the communication amongst intelligent electronic devices in such automation systems and associated system requirements. IEC/TR 61850-1:2013 provides an overview of the IEC 61850 standard series and defines the scope of the IEC 61850 standard: • Power quality domain; • Statistical and historical data; • Distributed generation monitoring and automation purpose; • Substation to substation communication; • Smart grid considerations. International Electrotechnical Commission (IEC) (2020) produced IEC TS 61850-1-2:2020 as technical specifications, intended for all users but mainly for standardization bodies using IEC 61850 as a base standard within the scope of their work and are ready to extend it as indorsed by the IEC 61850 standards. IEC TS 61850-1-2:2020 identifies the high-level requirements and step-by-step guidelines for expanding the scope of IEC 61850.	(Cai et al., 2018; International Electrotechnical Commission (IEC), 2013; International Electrotechnical Commission (IEC), 2020)
NIST SP 800-82r2	The NIST SP 800-82r2 *Guide to Industrial Control Systems (ICS) Security* explains a series of high-level procedures to assess the security of ICS. NIST SP 800-82r2 also provides brief descriptions of possible mitigation tactics (Jillepalli et al., 2017). According to Stouffer et al. (2015), this NIST SP 800-82r2 offers guidelines for securing ICS constituents, including SCADA systems, DCS, and PLC, while describing their unique reliability, performance, and safety requirements. The NIST SP 800-82r2 delivers an outline of ICS and typical system characteristics, classifies distinctive threats and vulnerabilities to these systems, and endorses security countermeasures to mitigate these risks (Stouffer et al., 2015). Table 4 provides a list of selected NIST SP 800 governance with significant relevance to the ICS security community.	(Jillepalli et al., 2017; Stouffer et al., 2015)

I made an initial review of the recommended documents and concluded that the ISA 99/IEC 62443 and the NIST SP 800–82 are the most relevant cybersecurity governance to protect the CPS/ICS against cyberattacks. Table 4 provides listings of ISA 99/IEC 62443 groups along with associated numbers and contents (ANSI/ISA, 2013; Fujdiak et al., 2018; Mlynek et al., 2020). Table 5 provides a listing of selected additional NIST SP 800 series that have substantial importance to the ICS security community. A full list of NIST SP 800 is publicly available from https://csrc.nist.gov/publications/sp800.

Table 4

Parts of ISA 99/IEC 62443

Group title	Part number	Content
General	IEC 62443-1-1	Terminology, concepts and models
	IEC 62443-1-2	Master glossary of terms and abbreviations
	IEC 62443-1-3	System security compliance metrics
	IEC 62443-1-4	IACS security lifecycle and use-case
Policies & standards	IEC 62443-2-1	Requirements for an IACS security management system
	IEC 62443-2-2	Implementation guidance for an IACS security management system
	IEC 62443-2-3	Patch management in the IACS environment
	IEC 62443-2-4	Installation and maintenance requirements
System	IEC 62443-3-1	Security technologies for IACS
	IEC 62443-3-2	Security levels for zones and conduits
	IEC 62443-3-3	System security requirements and security levels
Component	IEC 62443-4-1	Product development requirements
	IEC 62443-4-2	Technical security requirements for IACS components

Table 5

Selected ICS Security Related NIST SP 800

SP 800 #	Title/Description	Date released
SP 800-115	Technical Guide to Information Security Testing and Assessment	9/30/2008
SP 800-116 Rev. 1	Guidelines for the Use of PIV Credentials in Facility Access	6/29/2018
SP 800-12 Rev. 1	An Introduction to Information Security	6/22/2017
SP 800-123	Guide to General Server Security	7/25/2008
SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	10/10/2019
SP 800-137A	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment	5/21/2020
SP 800-150	Guide to Cyber Threat Information Sharing	10/04/2016
SP 800-160 Vol. 2	Developing Cyber Resilient Systems: A Systems Security Engineering Approach	11/27/2019
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	4/08/2015
SP 800-177 Rev.1	Trustworthy Email	2/26/2019
SP 800-184	Guide for Cybersecurity Event Recovery	12/22/2016
SP 800-189	Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation	12/17/2019
SP 800-192	Verification and Test Methods for Access Control Policies/Models	6/27/2017
SP 800-202	Quick Start Guide for Populating Mobile Test Devices	5/10/2018
SP 800-205	Attribute Considerations for Access Control Systems	6/18/2019
SP 800-210	General Access Control Guidance for Cloud Systems	7/31/2020

SP 800 #	Title/Description	Date released
SP 800-211	2019 NIST/ITL Cybersecurity Program Annual Report	8/24/2020
SP 800-213	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (Draft)	12/15/2020
SP 800-30 Rev. 1	Guide for Conducting Risk Assessments	9/17/2012
SP 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy	12/20/2018
SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations	12/10/2020
SP 800-53B	Control Baselines for Information Systems and Organizations	12/10/2020
SP 800-63B	Digital Identity Guidelines: Authentication and Lifecycle Management	3/02/2020
SP 800-70 Rev. 4	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers	2/15/2018
SP 800-18 Revision 1	Guide for Developing Security Plans for Federal Information Systems	02/24/2006
SP 800-37 Revision 1	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	6/10/2014
SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View	3/1/2014
SP 800-40 Revision 3	Guide to Enterprise Patch Management Technologies	9/5/2012
SP 800-41 Revision 1	Guidelines on Firewalls and Firewall Policy	9/28/2009
SP 800-50	Building an Information Technology Security Awareness and Training Program	10/1/2003
SP 800-53 Revision 4	Security and Privacy Controls for Federal Information Systems and Organizations	1/23/2014

SP 800 #	Title/Description	Date released
SP 800-53A	Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans	12/12/2014
SP 800-61 Revision 2	Computer Security Incident Handling Guide	2/1/2012
SP 800-63-2	Electronic Authentication Guideline	4/9/2015
SP 800-127	Guide to Securing WiMAX Wireless Communications	
SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	5/21/2020
SP 800-77	Guide to IPsec VPNs	6/30/2020
SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)	7/25/2012
SP 800-73-4	Interfaces for Personal Identity Verification	2/12/2016
SP 800-81-2	Secure Domain Name System (DNS) Deployment Guide	9/18/2013

Note. The full list of NIST SP 800 series, including the documents listed above, are available to download from https://csrc.nist.gov/publications/sp800.

Conceptual Framework and Methodology

RAT

The RAT (Cohen & Felson, 1979) became one of the principal descriptive theories on cybercrime and may demonstrate a guiding theoretical framework for the daily practices of community-based cybercrime mitigation (Brady et al., 2016; Harada, 2018). The concepts in the RAT relevant to this study are Cohen and Felson's notions that every successful violation requires at least three factors: (a) an offender with criminal dispositions and the skill to carry out those criminal predispositions, (b) a vulnerable target for the offender, and (c) a lack of protectors qualified to prevent violations.

Merien et al. (2018) suggested that the RAT evaluates the circumstances needed for a crime to take place by comprising three-dimensional and temporal patterns together with situational awareness. The RAT suggests that cybercrimes happen due to three factors:

- *Lack of a capable guardian* (e.g., network firewall, antivirus, and access control lists);
- *Presence of a suitable target* (e.g., a user vulnerable to social engineering attacks and a weak host on a network); and
- *Presence of a motivated offender* (e.g., a script kiddie and a malicious user).

These three factors could help explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS-based industries and services by envisaging the target, threat, and protection in day-to-day routine activities (Cohen & Felson, 1979).

I did not use the general systems theory (GST) that the Austrian biologist Ludwig von Bertalanffy first proposed at a philosophical symposium at the University of Chicago in 1937 and then specified its patterns, principles, and laws during 1947 and 1948 (Song & Zhang, 2019). Issitt (2020) concluded that the GST is a holistic discipline concerned with inspecting the role of systems as whole entities rather than adopting the mechanistic method of performing analytical explorations of the individual elements, functions, or processes within each system. Accordingly, I concluded that the focus of the GST was on examining the interrelations between systems and therefore rejected it as a fundamental theory for this study, of which the focus is only on the role of cybersecurity governance in protecting the CPS from cyberattacks in the oil and gas industry.

Qualitative Multiple Case Study

Yin (2018) suggested that a qualitative, multiple-case study allows researchers to understand the phenomenon of study by analyzing and triangulating data from multiple resources, including governmental and corporate documents, archival data, and semistructured interviews, therefore, suitable for this study. A narrative approach is not suitable for this study, as the purpose is not about telling stories about participants' personal experiences (Parker, 2019). A phenomenological research design is improper for this study because it intends not to perceive the meaning of a particular phenomenon by envisaging experiences lived by an individual or a group (Flynn & Korcuska, 2018). An ethnographic research design is inappropriate for this study because its objective is not to know the cultural practices of a particular group (Cardoso et al., 2017). A quantitative approach is not appropriate for this study because I will not seek to obtain precise and reliable numerical measurements that allow a statistical analysis (Queirós et al., 2017). I rejected the mixed methods research design because researchers use it to understand relationships between variables, which is not the purpose of this research (Lyons et al., 2020).

Qualitative Data Analysis Tools

Considering that the manual coding and analysis using MS Word files and Excel spreadsheets may not be sufficient, I searched for a possible data analysis tool to use for this research. ATLAS.ti® software is a Web-based qualitative data analysis tool that allows scholars and educational institutes to analyze documents, social media data, and Websites (ATLAS.ti, n.d.). Castleberry and Nolen (2018) suggested that ATLAS.ti® (Scientific Software Development GmbH), MAXQDA (VERBI GmbH), and NVivo® (QSR International Pty Ltd) are broadly used software tools that offer technological support to the qualitative research that restructures the data analysis process and enables for a more complex and deeper analysis of the data. Castleberry and Nolen have used NVivo® for some projects and concluded that it is easy to use while generating attractive graphical displays for the data.

Gaps in Literature

On an Industry 4.0's level, a pillar of which is the CPS, because Industry 4.0 is still new there is a literature gap in identifying the main models and characters of safety management within the context of Industry 4.0 (Liu et al., 2020). The oil and gas industry is a highly regulated industry due to the intrinsic health, safety, and environmental risks connected with the use of the CPS and ICS for exploration, drilling, processing, production, and distribution activities (Shaik et al., 2017). Potential health, safety, and environmental consequences of loss of control over CPS/ICS-based operations include loss of lives, fires, explosions, emission of toxic substances, air pollution, and marine pollutions from oil spills (Shen et al., 2020). Organizations pursuing control over such cybersecurity threats must acquire or develop governance policies to provide a framework for their human and technical resources (Clark et al., 2020; Gao et al., 2020; Wanasinghe et al., 2020).

There are essential gaps in the literature related to CPS's security because the current CPS safety and security policies, standards, and best practices are not yet operative enough in protecting the CPS-based industries and services, including the oil and gas industry (Asplund et al., 2018). There are insufficient studies on the security controls to help understand and enhance the security of target CPS and associated ICS (You et al., 2018). Cybercrimes against CPS have resulted in numerous calls for government involvement via laws and regulations (Vardi, 2017). Cybersecurity governance as a defensive means requires substantial advancement before they can produce valuable results in protecting CPS from cyberattacks (Asplund et al., 2018). The initial review of the literature for this research revealed that the CPS security governances' inefficiency may be because these governances specify what the cybersecurity requirements are without offering enough guidelines on how to comply with the requirements. The findings from this study (interpreted in detail in Chapter 5) may contribute to bridging this gap and extend the literature on how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry and similar CPS-based industries worldwide. The cybersecurity practitioners, scholars, policymakers, regulatory specialists, and managers may use the results of this study to understand better how to manage cyberattacks by enhancing CPS's cybersecurity governance as follows:

1. The vulnerabilities and consequences of cyberattacks on CPS/ICS are key findings derived from the participants' responses. The vulnerabilities and threat levels rise as CPS/ICS are connected to an outside world. CPS/ICS are exposed to two types of cyberattacks: (a) the general white noise attack that affects Windows operating systems all within its application and Linux nodes, (b) nation-state-sponsored cyberattacks, in which the offender is a nation-state-backed threat agent or sophisticated industrial espionage agents that are motivated through industrial espionage backgrounds, spending a significant number of resources on the design of the attack on developing malware sabotage opponents' critical infrastructure. Catastrophic consequences of such sabotage include loss of lives, damage to critical assets, interruption of critical supplies to communities (such as electricity and water), and environmental disasters such as emission of toxic substances and river and marine pollution. This finding increases the awareness of risks from cyberattacks and the importance of using robust governance that provides guidance on how to protect CPS/ICS against cyberattacks, including the recommended defense-in-depth architecture (see Figure 3).

2. Predominant governance is an essential finding derived from Theme 2 that emerged from the participants' responses. Figure 7 shows that 18 participants (90%) identified IEC 62443, while 11 participants (55% of the total participants) identified NIST SP 800-82 as predominant governance. This finding helps corporate management in the oil and gas industry and other CPS/ICS-based industries identify the best governance to use to protect their critical infrastructures against cyberattacks.
3. Governance efficiency is a key finding derived from Theme 3 that emerged from the participants' responses. The majority of the 20 participants (70%) have anticipated that the general white noise attacks on the IT foundation and the underlying CPS/ICS layer could be prevented by compliance to robust governance that enforces limiting access and exposure to the cloud, monitoring the networks, and preventing access to physical assets. Participants 01, 11, and 12 noted that compliance with strict governance provides the primary defense line. Still, the strength of CPS/ICS governance depends on three factors: well-trained people, adherence to governance or process, and the use of access management technology. This finding informs that the efficiency of a cybersecurity system does not depend only on governance but also on well-trained people and the use of network access management technology and promotes the need for balanced investment in these three actors.

4. The governance challenges is a significant finding derived from Theme 4 that emerged from the participants’ responses. Analysis of 14 interview transcripts (70% of the total participants) suggested that the nation-state-sponsored attacks cannot be prevented or mitigated by the governance only. This finding extends the literature by indicating that nation-state-sponsored attacks require more than robust governance. As a result, this study recommended (as a unique solution) is to have nation-states recognize that cyberattacks on critical infrastructures can only be solved jointly, ideally upon an agreement to criminalize cyberattacks endorsed by the United Nations Security Council.
5. The offenders and motives is a major finding derived from Theme 5 that emerged from the participants’ responses. Analysis of 14 interview transcripts (70% of the participants' responses) revealed that CPS/ICS offenders include insiders (rogue employees), script kiddies, hacktivists, organized crime, cybercriminals, and nation-state-sponsored attackers. Types of cyberattacks vary depending on the motives between ransomware and destructive malware. This finding increases awareness of CPS/ICS offenders and their motives. This knowledge is needed to design the defenses accordingly.
6. System enhancements is a key finding derived from Theme 6 that emerged from the participants' responses. Analysis of 70% of the participants' responses showed that replacing or upgrading the legacy equipment encompassed into CPS/ICS might be challenging to execute. Legacy equipment upgrades or replacement entails a significant investment, and the

return on investment is not usually feasible for those upgrades. Participant 01 the CPS and ICS are not easy to keep updated due to the production requirements of 24/7 operations for months and even years make it challenging to deploy updates. In a safety-regulated industry like oil and gas, deploying an update to see whether things still work is not permissible before rigorous testing and validation of all the potential routes. Such complicated processes are costly; therefore, keeping legacy equipment up to date is not always possible. This finding extends the literature by specifying the challenges faced in updating the legacy systems from the experts' perspective. Therefore, this finding helps the regulatory authorities, standardization firms, and corporate management design the CPS/ICS governance accordingly.

7. System endorsement is a crucial finding derived from Theme 7 that emerged from the participants' responses. Analysis of 70% of the participants' responses revealed unanimity on the importance of cybersecurity management practices, highlighting that they can be very effective only when corporate management promotes and endorses them as part of the corporate management system. Participant 02 suggested that training, knowledge management, and incident reporting practices can be efficient by monitoring the cybersecurity management system. Participants 01, 02, 03, 05, 07, 08, 09, 10, 11, and 14 have identified incident reporting as an area for improvement by compliance with corporate governance and mandatory regulations. Not all countries have mandatory regulations imposing reporting on cybersecurity

incidents. Participant 01 claimed that cybersecurity incident reporting is one of the areas that the industry has to improve. He noticed that there were conflicts of interest. For example, regulators were enforcing regulations in cases of non-compliance, issuing hefty fines that typically demotivate organizations from reporting because every report of an incident potentially shows that they have not been following regulations or that they missed at least some part. If reporting such non-compliance leads to a significant fine, the concerned organization would rather hide it. This finding extends the literature by identifying the challenges faced in incident reporting from the experts' standpoint. Also, this finding may encourage the regulatory authorities, standardization firms, and corporate management to endorse incident reporting (by CPS/ICS governance) as part of the corporate safety management system.

8. Performance assessment is a key finding derived from Theme 7 that emerged from the participants' responses. Analysis of 70% of the participants' responses showed that the role of corporate management is essential in establishing healthy organizational culture by promoting and endorsing cybersecurity governance as an intrinsic part of the corporate management system. Participants 01, 02, 03, 04, 05, and 11 noticed that the top management at some of the CPS/ICS-based industries operating on legacy systems have the mindset that production availability always has the priority over safety and security (including CPS and ICS cybersecurity) because

production availability increases the company revenue while spending on safety and security increases the cost. From this perspective, those managers are unwilling to stop the production to patch their OS (operating system) or upgrade their legacy equipment, especially, these systems that have been working for decades. This finding extends the literature by highlighting this cultural change issue and advising that it can be solved by adopting a cybersecurity performance assessment program as part of the corporate management system, through which a plan for updating the legacy system can be mandated and assessed using smart key performance indicators.

9. The governance mandate is a crucial finding derived from Theme 9 that emerged from the participants' responses. Analysis of 14 interview transcripts (70% of the participants' responses) displayed that more collaboration between the standardization firms and regulatory bodies on one side, and the CPS/ICS-based business owners and vendors on the other side could help enhance the quality and efficiency of governance against cyberattacks. Participant 02, who worked for one of the standardization firms, noted that it was difficult to get asset owners involved in the activities of standards and regulatory bodies. He thought that the asset owners tended to be less vocal because they are worried about the image of their companies, or they are concerned about the image of their own involvement in things. This finding expands the literature by proposing the solution to these issues (as concluded from the responses of Participants 01, 03, 04, 05, 07, 08, 09, 12, 13, and 14),

which lies in mandating incident reporting by the regulatory authorities. Other recommendations (by the participants) that may help fill the gap and expand the literature on CPS/ICS safety and security governance include:

a. Regulatory authorities should enforce CPS/ICS cybersecurity incident reporting and oblige all regulatory bodies from the individual member states to share incidents' experiences, cases, and threat intelligence across each other.
b. Nation-states need to recognize that cyberattacks on critical infrastructures can only be solved jointly, ideally upon an agreement to criminalize cyberattacks endorsed by the United Nations Security Council
c. In Europe, one ICS legislation mandates that critical infrastructure needs to be cyber secure and obliges organizations to report cyber incidents to their respective governments. This legislation is a good start to protect CPS-based infrastructures. Still, the regulatory authorities must start conducting audits to ensure this legislation is being implemented and impose fines for noncompliance with the requirements of that legislation.

Summary and Conclusions

The literature search strategy presented the databases and keywords used to obtain literature on the CPS/ICS safety and security, and the screening approach to select only the articles relevant to the study. The Literature Review section covered the following topics: CPS and ICS as critical infrastructure, cyberattacks as threats to CPS/ICS, CPS/ICS cybersecurity countermeasures, cybersecurity concerns in oil and gas industry, state of cybersecurity governance, conceptual framework and methodology, and gaps in literature. The literature review led to identifying many cybersecurity governances endorsed by standardization bodies and regulatory firms to govern the safety and security of CPS/ICS. The review of these cybersecurity governances revealed that ISA 99/IEC 62443 and the NIST SP 800–82 are the most pertinent cybersecurity governance to protect the CPS/ICS from cyberattacks. The literature review has also led to identifying the vulnerabilities and threats to CPS/ICS, existing cybersecurity governance and the protection measures, the conceptual theories and framework appropriate for the study, and gaps in the literature. By implementing the research method described in Chapter 3, I expanded on the main knowledge gained from the literature review by exploring how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry.

Chapter 3: Research Method

The purpose of this qualitative, multiple-case study was to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. The focus of the study was on the role of the CPS security governance in the oil and gas industry. The new knowledge gained from this study may help the standardization firms, regulatory bodies, and corporate cybersecurity managers discover new safety and security control elements to enhance the current CPS defense systems. This chapter begins with the research design and rationale, which include an explanation of the research design, the purpose of using the chosen method, and the reasons why other approaches would be less suitable. Other key sections of this chapter are the role of the researcher; a methodology section that explains in detail the approach to the study; and issues of trustworthiness, including creditability, transferability, dependability, confirmability, and ethical procedures. This chapter ends with a summary that includes an overview of the main points and a transition statement to Chapter 4.

Research Design and Rationale

The main research question that guided this study was as follows: How can cybersecurity governance be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry? These industries exist worldwide, and their relevance to the research problem and purpose is attained as they use CPS for their operations and use the cybersecurity governance explored in this study. Appendix A provides a list of interview questions designed to complement the study's main question and help achieve the objectives of this qualitative, multiple-case study. I chose a qualitative study because it was appropriate for this guiding research question and supplementary interview questions. Solesvik (2017) suggested that a qualitative study is suitable when a researcher needs to gain a deep understanding of a phenomenon and when asking *how* and *why* research questions to guide a study.

A qualitative, multiple-case study was a proper design for this study because it allows researchers to understand the phenomenon of study by analyzing and triangulating data from multiple resources, including governmental and corporate documents, archival data, and semistructured interviews (see Yin, 2018). I reviewed other qualitative research designs, including narrative, phenomenological, and ethnographic. A narrative approach was not suitable for this study, as the purpose was not about telling stories about participants' personal experiences (see Parker, 2019). A phenomenological research design was improper for this study because it intends not to perceive the meaning of a particular phenomenon by envisaging experiences lived by an individual or a group (see Flynn & Korcuska, 2018). An ethnographic research design was inappropriate for this study because its objective was not to know the cultural practices of a particular group (see Cardoso et al., 2017). A quantitative approach was not appropriate for this study because I did not seek to obtain precise and reliable numerical measurements that allow a statistical analysis (see Queirós et al., 2017). I rejected the mixed methods research design because researchers use it to understand relationships between variables, which was not the purpose of this research (see Lyons et al., 2020).

I used the RAT as a conceptual theory for this study because it could help answer the main research question and supplemental interview questions (see Appendix A and Table 6) by foreseeing the target, threat, and protection in day-to-day routine activities (see Cohen & Felson, 1979). I did not use the GST that the Austrian biologist Ludwig von Bertalanffy first proposed at a philosophical symposium at the University of Chicago in 1937 and then specified its patterns, principles, and laws during 1947 and 1948 (Song & Zhang, 2019). Issitt (2020) concluded that the GST is a holistic discipline concerned with inspecting the role of systems as whole entities rather than adopting the mechanistic method of performing analytical explorations of the individual elements, functions, or processes in each system. Accordingly, I concluded that the focus of the GST is on examining the interrelations between systems and therefore rejected it as a fundamental theory for this study, which explores only the role of cybersecurity governance in protecting the CPS from cyberattacks in the oil and gas industry.

The primary method of data collection in this research was Zoom interviews with cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn (see Table 7). I audio-recorded and transcribed these interviews using Sonix audio-to-text converter software (Sonix, n.d.). Such an online environment was suitable because the target participants were distributed across many remote geographical locations worldwide. To ensure the generalizability and transferability of the study results, I conducted Zoom interviews with 20 CPS cybersecurity experts selected from a large population comprised of various professional associations, organizations, and industries, focusing on cybersecurity professionals with a minimum of 10 years of experience in the oil and gas industry so that they had the relevant knowledge to contribute to the study. I aimed for 20 participants from those whom I had initially invited via email and LinkedIn connect messages. I found that 20 participants were sufficient. Ogallo (2018) included 20 participants for a similar study. Data saturation was achieved after thematic analysis of the transcripts of Zoom interviews with 14 participants. As planned, I conducted and analyzed the remaining six Zoom interviews to generalize the results to a larger population (see Figures 4, 5, and 6 in Chapter 4) and to confirm saturation by ensuring no more themes would emerge from the analysis.

The secondary method of data collection in this research was thematic analyses of selected documents and archival data on CPS safety and security governance endorsed and made publicly available by the international regulatory bodies and standardization firms. Another consideration to ensure the study's transferability is that only CPS security governance endorsed by internationally recognized standardization/regulatory firms and adopted globally by most CPS-based industries were to be selected for thematic analysis. Based on the literature review and analysis of Zoom interviews, the two documents that met these criteria were IEC 62443 and NIST SP 800-82 and thus were selected for thematic analysis. The aim of thematic analyses of selected cybersecurity governance and the interview transcripts was to develop themes and conclude the CPS cybersecurity threats, protection tactics, and possible means to enhance these tactics. The framework was linked to the instrument used to gather data as I (a subject matter expert) served as the primary instrument to conduct the interview and analyze the content of their transcripts, and I selected and analyzed the content of relevant CPS cybersecurity documents. Information-rich cases were derived from experience and analyses of interview transcripts as the primary data source as well as the review and analysis of the two-cybersecurity governance (IEC 62443 and NIST SP 800-82) as the secondary data source.

Role of the Researcher

As the researcher, I served as the main data collection instrument for this qualitative study. My relationship with the traditional ICS and advanced CPS in the oil and gas industry has extended over 32 years of experience with the health, safety, and environmental issues associated with the failures of ICS/CPS-based industries and services. I conducted the research and applied a robust data collection method that ethically portrayed my role as a principal intermediary. Besides analyzing the most predominant CPS/ICS cybersecurity governance (IEC 62443 and NIST SP 800-82), I conducted 20 Zoom interviews as a powerful technique to gain an awareness and understanding of participants' proficiencies and perceptions about the subject of study. I analyzed the data, taking into consideration the issues of trustworthiness.

Methodology

The following subtitles provide detailed explanations of the methodology employed in this study, including the conceptual framework; sources of data; participant selection logic; instrumentation; procedures for recruitment, participation, and data collection; and data analysis plan.

Conceptual Framework

For this qualitative, multiple-case study, I chose the RAT (Cohen & Felson, 1979) as a conceptual theory. The concepts within the RAT that grounded this study are Cohen and Felson's notions that every successful violation requires at least three factors: (a) an offender with criminal dispositions and the skill to carry out those predispositions, (b) a vulnerable target for the offender, and (c) a lack of protectors qualified to prevent violations. These three factors of the RAT, the main research question, and the supplemental interview questions have guided the literature review process.

In a seminal study, Boutwell (2019) used the RAT as a conceptual theory guiding a qualitative, multiple-case study to explore cybersecurity tactics employed by compliance officers and information technology (IT) managers to lessen cyberthreats to critical infrastructure. The application of the RAT allowed Boutwell to identify key tactics that can help advance cybersecurity strategies employed by IT and compliance experts to alleviate possible attacks on critical infrastructure (Boutwell, 2019). Ab Rahman et al. (2017) conducted a study to understand the challenges of evolving threats to incident management and digital forensic by applying the RAT, which is comprised of three main factors: motivation, opportunities, and guardianship. The research findings revealed that emerging technologies pose substantial motivations and opportunities to cybercriminals, raising the challenges in incident management and digital forensics to deliver successful guardianship (Ab Rahman et al., 2017).

The RAT is used to investigate cybercrimes and criminal events in the technology domain. Tyler (2018) conducted a qualitative case study, guided by the RAT, to explore strategies senior IT leaders in the healthcare industry have used to establish cloud security to decrease cyberattacks on electronic health records. Data collection incorporated phone interviews, semistructured interviews, and analysis of organizational documents. The results of this study can create awareness of the need to protect electronic health records in the cloud to reduce cyberattacks (Tyler, 2018). This study benefitted from the RAT as the data analyzed were arranged according to the knowledge areas, interview questions, and corresponding RAT factors (see Table 6). The goal was to use the RAT factors to help explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks on the CPS in the oil and gas industry.

Table 6

Distribution of Supplemental Interview Questions Based on the RAT Factors

Knowledge area	Interview questions	RAT factor
CPS detection system	1. What critical system failure may occur due to cyberattacks on CPS and ICS?	Vulnerable target
Existing CPS cybersecurity governance	2. What policies, standards, procedures, and best practices are endorsed to provide safety and security for the CPS and ICS?	Protector
The efficiency of CPS policies and standards	3. What type of cyberattacks can the proper application of policies, standards, procedures, and best practices prevent or mitigate? 4. What are the types of cyberattacks that the proper application of policies, standards, procedures, and best practices cannot prevent or mitigate?	Protector
CPS vulnerability	5. Why CPS and ICS are subject to cyberattacks?	Offender
CPS security improvement	6. What type of equipment upgrade, software, and governance would help enhance CPS and ICS safety and security?	Protector
Role of corporate management	7. How effective are organizational practices such as training, knowledge management, and incident reporting about various cyberattacks in identifying threats and developing standards or procedures to strengthen the CPS and ICS safety and security systems? 8. How do you describe corporate management's role in establishing and sustaining the CPS and ICS safety and security systems?	Protector
Role of standardization and regulatory bodies	9. What can the industrial community, especially the standardization and regulatory bodies, do to strengthen the CPS and ICS safety and security systems?	Protractor

Besides reviewing the literature addressing the main research question and the supplemental interview questions, the literature review also included definitions of the main concepts about CPS's safety and security and the literature gaps in this domain.

Sources of Data Collection

I collected the data from three sources: Zoom interviews with 20 CPS/ICS cybersecurity professionals as a primary data source, and the two governances IEC 62443, and NIST SP 800–82 as a secondary data source:

1. I collected the primary data through open-ended questions in semistructured Zoom interviews with 20 CPS/ICS cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn (see Table 7).
2. The main governance standard I reviewed and thematically analyzed (as a secondary data source) was the ISA/IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards), which incorporates the regulatory requirements for the ICS's cybersecurity. Analysis of the whole parts of ISA 99/IEC 62443 as listed in Table 4 was not logically possible within the duration of this study.
3. The second document selected as a secondary source of data was obtained from the Information Technology Laboratory (ITL) at the NIST. The ITL's duties include developing technical guidelines and physical standards (Ross et al., 2018). The ITL governance I reviewed and analyzed thematically was the NIST SP 800–82 (a guide to ICS security).

The data collected were thematically analyzed against the main research question and supplemental interview questions and associated three factors of the RAT, using Table 6 as an instrument. The Data Analysis Plan, later in this chapter, provides more information about this process.

Participants Selection Logic

There are two types of population sampling in a case study: (a) probability sampling, which includes simple random sampling, systematic sampling, stratified sampling, and cluster sampling; and (b) nonprobability sampling, which provides for quota sampling, purposive sampling, self-selection sampling, and snowball sampling (Sharma, 2017). I chose purposive sampling for this study and used Zoom for interviewing 20 members of worldwide CPS cybersecurity-specialized groups on LinkedIn. The participants' specific roles and positions included CPS cybersecurity consultants, advisors, managers, engineers, and CPS security governance development specialists. To link the sample selection strategy to the problem, purpose, and research question, all participants were purposively selected from cybersecurity professionals with a minimum of 10 years' experience in CPS-based industries. These participants had the relevant knowledge to contribute to the study through sharing their experiences by answering the interview questions about using the governance more effectively to protect CPS against cyberattacks. I aimed for 20 participants from those whom I had initially invited via email and LinkedIn connect messages.

The challenge lies in making a balance between the advantages and disadvantages of purposive sampling. Maestripieri et al. (2019) noted that purposive sampling in qualitative research allows the researcher to choose only cases that possess the knowledge about the phenomenon under investigation and offers insight into the problems and associated solutions. The disadvantage of purposive sampling is that it can be viewed as subjective and thus involves the researcher's bias, consequently limiting potential transferability. To overcome the disadvantage of purposive sampling, Maestripieri et al. suggested that researchers ground their selection judgments on specific selection criteria that are transparent and clearly explained.

To attain external validity, I conducted Zoom interviews with 20 CPS cybersecurity experts selected purposively from worldwide cybersecurity-specialist groups on LinkedIn. They worked for a wide range of international CPS/ICS-based industries and services, including oil and gas, petrochemicals, chemicals, smart transportation, electrical power plants, water treatment, cement smelters, IIoT development and transformation, and manufacturing (see Table 7). Purposive sampling was suitable for this study because it allows the researcher to choose interviewees who are exceptionally knowledgeable about the phenomenon of interest (see Yin, 2018). I aimed for 20 participants from those whom I had initially invited via email and LinkedIn connect messages. I found that 20 participants were sufficient; Ogallo (2018) included 20 participants for a similar study.

Table 7

Potential Participants From LinkedIn Groups and Inclusion Criteria

Cybersecurity specialized group	Total members*	Target positions	Target years of experience	Target CPS industries/companies
ICS security S99 IEC62443 cyber and physical	1,263	CPS/ICS cybersecurity managers, advisors, consultants, engineers, developers, team leaders, methodologists	10 years +	Oil and gas, petrochemicals, chemicals, smart transportation, electrical power plants water treatment, cemen smelters, IIoT development and transformation, and manufacturing.
Cyber laws, patents, copyrights, trademarks, intellectual property IPR & online security	4,121			
Industrial control system cyber security (ICS-CS)	4,904			
Global cyber security group	2,113			
Cyber security experts panel (CSEP)	2,408			
Cyber law & information security	17,333			
Cyber security in real-time systems	13,365			
Cyber security forum initiative - CSFI	138,424			

**Note.* Total members as of January 7, 2021.

Interview Plan and Considerations

The following factors and arrangements were considered while planning for the interviews and executed through the process.

- Interview technological aids: The interviews were conducted and audio-recorded online using Zoom and transcribed using the Sonix audio-to-text automatic conversion software (Sonix, n.d.).
- Identifying participants: The members' profiles for the cybersecurity-specialized groups on LinkedIn were used for identifying potential participants who meet the inclusion criteria.
- Variation of participants: For transferability considerations, the participants were selected from various CPS-based industries and services as listed in Table 7 so that the result can be generalized. The majority of participants were chosen from the oil and gas industry.
- Sample size: Initially, Zoom meeting initiations were sent via LinkedIn messages and email messages to 200 potential participants who meet the inclusion criteria, with an aim to obtain approval from 20 participants. Sending invitations continued until the target number of 20 valid Zoom interviews was achieved. (I had to send 386 invitations before the target number of 20 valid Zoom interviews was achieved).
- Invitation process: Zoom Interviews' invitation email requests were sent to potential research study participants after obtaining the Institutional Review Board's (IRB's) approval number 04-23-21-0725679. The invitation emails

included detailed explanations of the goals and nature of the study. The consent form was used to inform the participants that their contribution to this study was voluntary, with no special benefits to them. Also, to let the participants know that the interview were audio-recorded.

- Interview setting: Open-ended questions were asked in semistructured interviews with 20 participants over the internet using Zoom. Such an online environment was suitable as the target participants were distributed across many remote locations worldwide.
- Saturation: The saturation point was reached to when more interviews resulted in no new data or information.
- Terms of confidentiality: Confidentiality of interviewees was retained by using codes instead of actual names. Maintaining confidentiality enables group participants to freely express their judgements individually and without social force that could arise from dominant individuals (see Yin, 2018).
- Purpose of interview: The participants answered the interview questions to help me address the role of cybersecurity governance in protecting CPS and ICS from cyberattacks.
- Interview time: Estimated at 1 hour in length. (average time for the 20 interviews was 39 minutes).
- Preparatory note: The introductory notes in Appendix C was used to treat the participants and ask them if they had any questions before the interview took place.

- Follow-up, clarifications, and validations: The closing notes in Appendix D were used to exchange with the participants the contact means and suitable methods to get in touch for further clarification, member checking, or if an additional interview round needed.
- Interview category: The interviews were started as standardized open-ended, and extremely structured in terms of the wording of the questions. Participants were always asked the identical questions included in Appendix A. Based on the participants' responses, I asked additional semistructured and open-ended questions to obtain more data/information.
- Number of rounds: The interviews were conducted in one round with the possibility for a second round (which was not needed) based on the results from the data analysis. There was a possibility of a follow-up to clarify the results as needed through Zoom interviews or emails.
- Interview questions: I created the interview questions based on my experience and the knowledge gained from the literature review. Another rationale behind the formulation of the interview questions was the alignment with the research problem, research purpose, and the main research question.
- Interview protocol: An interview protocol was used (following obtaining the IRB approval number 04-23-21-0725679) to control the interview process. The interview protocol included an interview invitation email (Appendix B), informed consent to be emailed to all participants, introductory notes (Appendix C) and closing notes (Appendix D).

Instrumentation

The data collection instrumentation and sources used for this study included an interview logbook, interview protocol, audio-recorded Zoom interviews, CPS/ICS cybersecurity governance, and interviews transcription (audio to text conversion) software.

Interview Logbook

To manage the Zoom interview events, I used an MS Excel spreadsheet to record (for each participant) each participant identifier, participant name, contact information, link to participant profile on LinkedIn, job title, years of experience, country, industry, date of invitation email, participant response date, data of consent form, planned interview date, actual interview date, interview duration, interviewer notes, date audio files transcribed, dates audio files analyzed, and member checking sent and reply dates.

Interview Protocol

Following the IRB approval to execute the research plan, an interview protocol was used to formalize and manage the interview process. The interview protocol included Zoom interview invitation email (Appendix B), informed consent emailed to all participants, introductory notes used during the interviews (Appendix C), and interview closing notes (Appendix D).

Zoom Interviews

Yin (2018) suggested that a qualitative, multiple-case study allows researchers to understand the study phenomenon by analyzing and triangulating data from multiple resources, including governmental and corporate documents, archival data, and semistructured interviews. In-depth semistructured interviews, which I audio-recorded using Zoom as a software tool, were the primary data collection instrument in this research. I used the open-ended questions listed in Appendix A to conduct semistructured Zoom interviews with 20 cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn (see Table 7).

CPS/ICS Cybersecurity Governance

Another data collection instrument in this research was the CPS/ICS cybersecurity governance. Iaiani et al. (2020) suggested that the current international cybersecurity governance provides security countermeasures, tools, risk management approaches, policies, and best practices intended to protect a user or organization's cyber environment. The standard ISA/IEC 62443 addresses the OT's security by providing a dynamic framework to identify and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS). Stouffer et al. (2015), in the NIST SP 800-82 rev. 2, introduced the defense-in-depth strategy as an effective cybersecurity program that ICS-based organizations should apply by layering security mechanisms such that the impact of a failure in any one mechanism is minimized, while the expense of an attack is maximized.

The main governance standard I reviewed and thematically analyzed against the themes evolved from the interview transcripts was the ISA/IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards), which incorporates the regulatory requirements for the ICS's cybersecurity. The second governance document was obtained from the ITL at the NIST. The ITL's duties include developing technical guidelines and physical standards (Ross et al., 2018). The ITL governance I reviewed and analyzed thematically was the NIST SP 800–82 (a guide to ICS security). These two governances (IEC 62443 and NIST SP 800-82) were selected as secondary data collection instruments because they are endorsed by internationally recognized standardization firms (IEC and NIST). Also, the literature review and the Zoom interviews with cybersecurity experts revealed that these two are the most predominant governance to protect CPS/ICS against cyberattacks.

Interviews Transcription (Audio-To-Text Conversion Software)

I conducted verbatim transcripts of the Zoom interviews' audio-recorded files as the first step towards data analysis. This process was possible with audio-to-text conversion software (see Ganesan et al., 2017). I used Sonix audio-to-text automatic conversion software (see Sonix, n.d.). The outputs were editable MS Word files that I used to adjust the transcripts manually. Verbatim transcripts aided the development of audit trails of data analyses. Verbatim transcription allowed highlighting the keywords, which I later categorized to develop codes and themes that helped answer the research question and the supplemental interview questions. I tried several audio-to-text automatic conversion software, including Sonix, Transcribe, Vocalmatic, and Bear File Converter and concluded that Sonix was the more accurate amongst them. By fixing the typographical errors in Sonix output files and arranging codes, categories, and themes in sequential order, I created an analytical framework that helped me make sense of data.

Manual Vs. Software-Aided Data Coding and Analysis

Ose (2016) noted that applied social science projects involving many interviews produce a vast amount of data or texts that is hard to structure and analyze systematically. Ose also noted that computer-assisted qualitative data analysis software is too advanced and sophisticated to sort and structure the texts. Therefore, Ose developed a new method using Microsoft Word and Excel and claimed that this method produces a flexible Word document of interview data separated into logical chapters and subchapters. All text is coded, and the codes correspond with headings in the final manuscript. Ose suggested that this method is efficient when there are four or more interviews; the method is also suitable for coding and structuring answers to open-ended questions, which is the case in this qualitative, multiple-case study.

To avoid the complexity of analytical software tools, I used MS Word files and Excel spreadsheets to analyze the contents of the interview transcripts and the CPS/ICS governance standards ISA 99/IEC 62443 and NIST SP 800–82. MS Word files and Excel spreadsheets were sufficient to provide meaningful analyses of the gathered data and answers to the research question and the supplemental interview questions. The manual data analyses using MS Word and Excel files were possible because the interview questions were well-structured and categorized by specific categorical knowledge areas and RAT factors (see Table 6). The manual thematic analyses using MS Word and Excel are explained step-by-step, later in this chapter, under the Data Analysis Plan.

ISA, IEC, ANSI, NERC, and NIST are the well-reputed and internationally-recognized regulatory bodies who have developed or contributed to the development of the CPS/ICS governance standards ISA 99/IEC 62443 and NIST SP 800–82, which were used as a secondary source of data (Cardenas & Cruz, 2019; Lyu et al., 2019; Ross et al., 2018; Yoo & Shon, 2016; You et al., 2019). The initial review of these documents suggested that they include sufficient information to answer the main research question and to validate the participants' answers to the supplemental interview questions through triangulation.

Procedures for Recruitment, Participation, and Data Collection

The Conceptual Framework and Nature of the Study sections of Chapter 1 included detailed but scattered information about recruitment, participation, and data collection procedures. The following bulleted points provide a summary of these processes.

- I collected the data from three sources: The standard IEC 62443, NIST SP 800–82 (a guide to ICS security), and individual interviews with 20 cybersecurity professionals (see Table 7).
- I served as the main data collection instrument for this qualitative, multiple-case study.
- I downloaded the ICS security governances ISA/IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards), and NIST SP 800–82 (a Guide to ICS Security). Both documents are publicly available online.
- The ICS security governances were downloaded instantly. The data processing and analysis of these governances were completed in 30 days.

- Using Zoom software as a tool, I conducted semistructured interviews with 20 participants, comprised of CPS/ICS cybersecurity professionals, on one round basis. Based on the satisfactory results from the interviews' data analysis, no more rounds were required.
- Finding 20 CPS/ICS cybersecurity professionals with 10 years of experience or more and willing to donate their time for this research was a challenging task. The first Zoom interview was conducted on May 3, 2021, and the last one was conducted on August 30, 2021.
- MS Word files and Excel spreadsheets were used for taking notes and conducting manual coding, thematic analyses, and concluding themes from the ICS security governances and interview transcripts (see the Data Analysis Plan below). These processes were completed in 60 days.
- The informed consent form and introductory statement stated that participants are free to exit the study at any time; the interview audio recordings will be stopped or deleted at the participant's request.
- As a follow-up, clarifications, and validations procedure (included in the informed consent form), I exchanged with the participants the contact means and suitable methods to get in touch for further clarification or if an additional interview round is needed.
- The Zoom interviews were conducted using my personal laptop. As a precautionary action, I installed Zoom software on my smart mobile phone

and made it ready to use if my laptop or the Wi-Fi internet router connected to it failed.

Data Analysis Plan

For the three sources of data (i.e., interview transcripts, IEC 62443, and NIST SP 800–82), I used interview and document review notes and conducted manual coding using MS Word files and Excel spreadsheets for thematic analyses and concluding themes. This method of developing themes from codes is termed as *holistic coding*. This type of coding refers to the process of analyzing the data corpus as a whole and identifying the underlying themes or issues in the data; and *theming the data*, which is defined as the process of identifying codes in the form of sentences capturing the essence and essentials of participant meanings (Onwuegbuzie et al., 2016).

I conducted manual thematic analysis in two batches: one batch to analyze the interview transcripts and another batch to analyze the two governances to validate the themes evolved from the thematic analysis of the interview transcripts. Both analyses were done using MS Word files and Excel (see Onwuegbuzie et al., 2016; Ose 2016). As suggested by Ose, I executed the following 12 steps to complete the thematic analysis processes.

1. Converted the ICS security governance standard ISA/IEC 62443 from PDF to MS Word format and named it IEC 62443.
2. Converted the ICS security guide NIST SP 800–82 from PDF to MS Word file format and named it NIST SP-800–82.

3. Transcribed the 20 Zoom interviews audio-recorded files by converting them to MS Word files, using Sonix audio-to-text automatic conversion software (see Sonix, n.d.).
4. Ranked the interview transcribed files based on the knowledge and contribution of each respondent (from 1 to 20) and gave each participant a unique code to protect their identity.
5. Transferred the texts from MS Word to an Excel spreadsheet.
6. Arranged the MS Excel spreadsheet for coding.
7. Performed the coding in the MS Excel spreadsheet, connecting the data with the research question and supplemental interview questions, and associated seven knowledge areas and the three factors of the RAT (vulnerable target, offender, and protector), using Table 6 as a tool.
8. Prepared the coded documents for sorting, making quotes and references to categories, groups, and subgroups.
9. Sorted the data.
10. Transferred the sorted quotes and references from MS Excel to MS Word.
11. In MS Word files, I sorted the texts into logical structures based on the coding.
12. Analyzed the data sorted from the two governances and interview transcripts to develop themes addressing the research question and each of the supplemental interview questions by envisaging the CPS/ICS's vulnerable target, behaviors of the offender, and the protector's role. Also conducted data

triangulation to conclude consistency/inconsistency amongst the themes evolved from the thematic analysis of the primary and secondary data sources as outlined in Chapters 4 and 5.

The specific elements of each governance and interview transcripts were integrated with the knowledge areas, the RAT elements, and questions in Table 6. Main analytical themes and patterns that resulted from this integration helped in covering the following:

- Vulnerabilities and threats to CPS/ICS.
- Commonly used governance.
- Types of cyberattacks that the use of governance can help prevent or mitigate.
- Types of cyberattacks that the use of governance cannot help prevent or mitigate.
- CPS/ICS' offenders.
- Enhancements to CPS/ICS cybersecurity.
- Role of corporate management.
- Role of standardization and regulatory bodies.

Castleberry and Nolen (2018) suggested the following five steps summarizing the thematic analysis process that leads to developing themes addressing the research question and each of the supplemental interview questions.

1. Compiling the data into a useful form is the first step to finding meaningful answers to the research question and supplemental interview questions.

2. Disassembling the data is the next step after compiling and organizing the data. The process of disassembling the data involves splitting the data into parts and creating meaningful groupings.
3. Reassembling codes, or categories, to which each concept is mapped and then put these codes into context with each other to generate themes.
4. Interpreting is a critical stage of thematic analysis, through which the researcher makes analytical conclusions from the data presented as codes and then themes.
5. Concluding response to the research question and supplemental interview questions from codes, themes, and thematic maps.

The results were presented by the distribution of participants across the countries, continents, and CPS/ICS industries to determine the generalization and transferability of the research results (see Figures 4, 5, and 6). Thematic analyses have led to more understanding of how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS-based industries.

Issues of Trustworthiness

Credibility

A participant's review of the researcher's notes and transcribed data provides quality control over the content and adds to the credibility of the study (see Perrotta, 2017). I used interview transcripts and conducted member checking by sharing my perception and interpretation notes, the transcribed data, and interview findings with each participant via email. I intended to do follow-up via telephonic interviews when necessary. To ensure that member checking is a value-added validation technique, I analyzed each participant’s feedback and intended to conduct supplementary interviews until saturation is achieved. I considered additional factors to attain this study’s credibility, including using recognized and approved research methods, maintaining familiarity with the context, using only confirmed and approved research methods, using transparent recruiting and informed consent, using triangulation as a method to achieve data credibility and validity by making association of data collected from multiple sources, and discussing the discrepant cases or findings with the participants.

Transferability

Transferability is described as the overall comparison of research findings against similar studies to conclude possible commonality (see Allred et al., 2017). To attain transferability and provide the reader with the necessary information to make a well-informed decision, the researcher should provide a precise explanation of the research methods employed in the study (see Sidhu et al., 2017). My considerations to attain transferability of the study were:

- Only CPS security governance that are endorsed by internationally recognized standardization/regulatory firms and adopted globally by most CPS-based industries have been selected for thematic analysis.
- To attain external validity, I conducted Zoom interviews with 20 CPS cybersecurity experts selected purposively from worldwide cybersecurity-specialist groups on LinkedIn. They work for a wide range of international CPS/ICS-based industries and services, including oil and gas, petrochemicals,

chemicals, smart transportation, electrical power plants, water treatment, cement smelters, IIoT development and transformation, and manufacturing (see Table 7).

- I also provided in this chapter a full description of the context and setting of data collection, an explanation of pertinent participant selection criteria, and a specified recruitment process. I explained the research design and conceptual framework and described the data analysis plan. The study results and recommendations are presented in Chapters 4 and 5, respectively.

Dependability

The tactic needed to ensure dependability and confirmability depends on using an audit trail. The researchers provide a complete set of notes on choices made throughout the research process (see Korstjens & Moser, 2018). To ensure this study's dependability, I maintained an updated audit trail documenting the evolution of research design and methods, data collection strategies. I kept timely reports on the flow and any changes to procedures. I ensured that the study participants were cybersecurity professionals who met the eligibility criteria specified in Table 7. I adhered to the doctoral study governance and complied with the university's rules.

Confirmability

A thorough explanation of the research processes should be provided to guarantee the study's confirmability (see Kalu & Bwalya, 2017). Confirmability can be enhanced by reflexibility, which is a process that permeates the entire research effort; therefore, it is proper to address the steps taken throughout the manuscript (see Dodgson, 2019). To enhance the confirmability of this research, I demonstrated the findings through extraction from the result of participants' experiences and ideas rather than my own characteristics and preferences. In doing so, I provided detailed descriptions of the researcher's role and his affiliation with the setting, context, and phenomenon. I performed triangulation of the CPS/ICS governance and the interview transcripts to increase the credibility and validity of the research findings and results. I preserved the transparency of the audit trail throughout the process from data collection through interpretation. I presented in figures and texts how I moved from data to codes to categories to themes.

Ethical Procedures

I complied with the IRB requirements for ensuring that all Walden University researches comply with the University's ethical standards and the U.S. federal regulations governing research on human subjects. After my committee chair uploaded the first three chapters of this document into the MyDR system as a research proposal and the University Research Reviewer (URR) approval was obtained, I followed the directions for obtaining ethics approval for a doctoral study. I did not begin participant recruitment, data collection, or dataset access before obtaining IRB approval number 04-23-21-0725679.

Summary

This chapter began with an introductory statement into which I restated the purpose of the study. I then explained the research design and rationale, starting with the main research question. I further explained the role of the researcher, followed by a detailed explanation of the methodology, which included the conceptual framework, sources of data collection, participant selection logic, interview plan and considerations, the manual instrumentations, and possible software tools that may be used for the study, interviews' transcription method, procedures for participants recruitment and data collection. I ended the methodology by explaining the data analysis plan. The last section of this chapter addressed the issues of trustworthiness, including credibility, transferability, dependability, confirmability, and the ethical procedures concerning the submission of an IRB after the URR approval of the research proposal. This chapter fulfilled the research proposal and provided the information essential to obtain the IRB permission to conduct the study. Following the approval of the research proposal, I received the IRB approval number 04-23-21-0725679 and then began the data collection process. Chapter 4 is designed to address the research setting, demographics, data collection, data analysis, evidence of trustworthiness, and the study results.

Chapter 4: Results

The purpose of this qualitative, multiple-case study was to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. The main research question that guided this study was as follows: How can cybersecurity governance be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry? This chapter is organized mainly to outline the research findings. It includes the research setting, demographics, data collection, data analysis, evidence of trustworthiness, and my summary of the study findings.

Research Setting

I conducted semistructured Zoom interviews with 20 cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn. After participants consented to volunteer for the study, I asked every participant to choose a time for a one-on-one online interview using Zoom. I gave the participants the freedom to select the continent time for them (in their local times); then, I arranged my schedule accordingly. The time difference between Egypt, from where I conducted the interviews, and the participants' countries ranged between no time difference and 11 hours. All participants chose to attend the Zoom interviews after working hours, using laptops. Zoom's online interview setting was ideal as the participants are distributed across many remote locations worldwide (see Figures 4 and 5).

The Zoom interviews were audio-recorded; they began as standardized open-ended and highly structured in terms of the wording of the questions. Participants were always asked the identical questions included in Appendix A. The participants were free to answer the questions reflecting their own views based on their personal experience rather than their organizations' standpoint. I asked additional semistructured and open-ended questions based on the participants' responses to obtain more data or information. The interviews were conducted in one round, and there was no need for a second round because the data analysis led to precise results and the member checking was performed via emails. The Zoom interview audio recordings were generally clear, thus easily transcribed using Sonix (n.d.). The setting was convenient for the participants and me. None of the participants had to quit before the interview was complete.

Demographics

I conducted semistructured Zoom interviews with 20 cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn. All participants who shared their experience about the subject of study were cybersecurity experts with at least 10 years' work expertise with one or more CPS/ICS-based organizations (see the inclusion criteria outlined in Table 7). The geographical locations for the 20 participants included 13 countries distributed across five continents. Figure 4 shows the distribution of participants by country; Figure 5 shows the distribution of participants by continent.

Figure 4

Distribution of Participants by Country

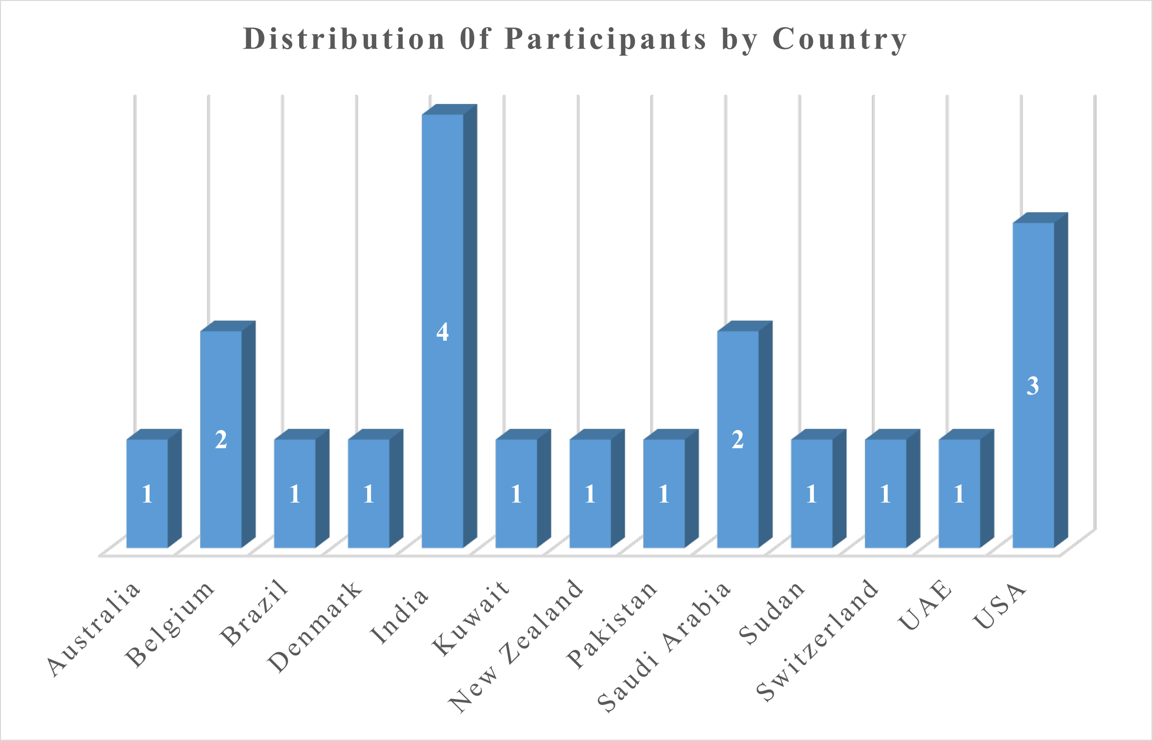
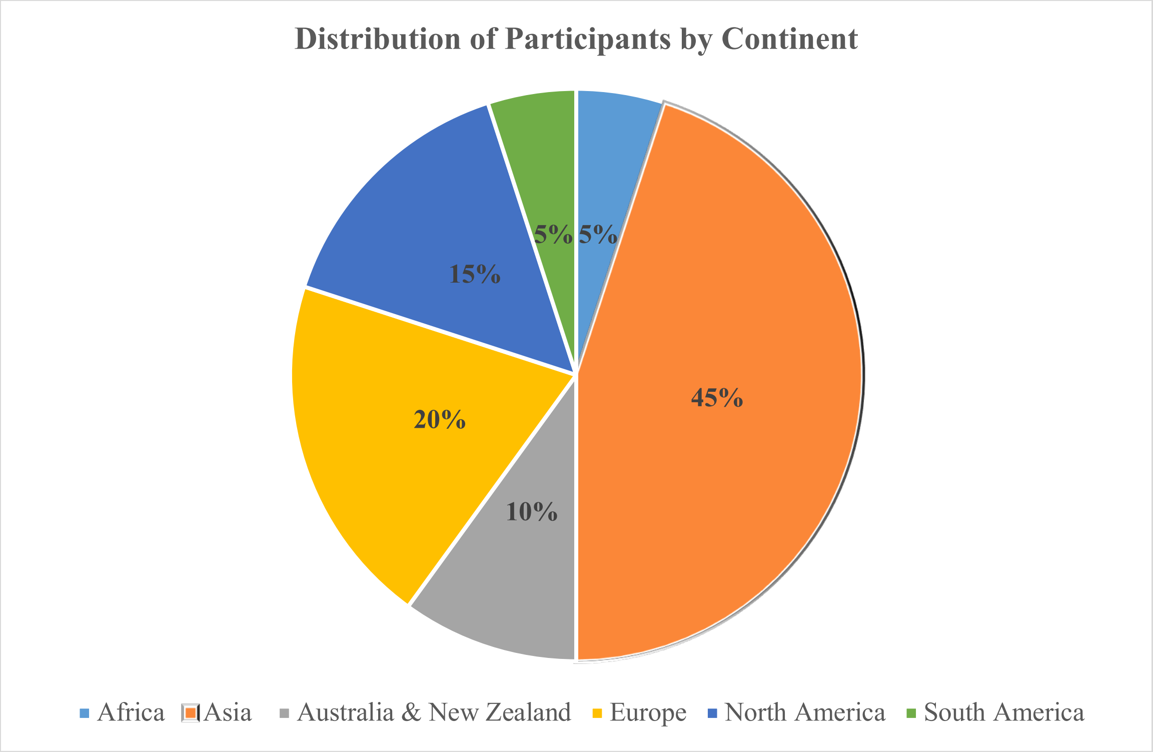


Figure 5

Distribution of Participants by Continent



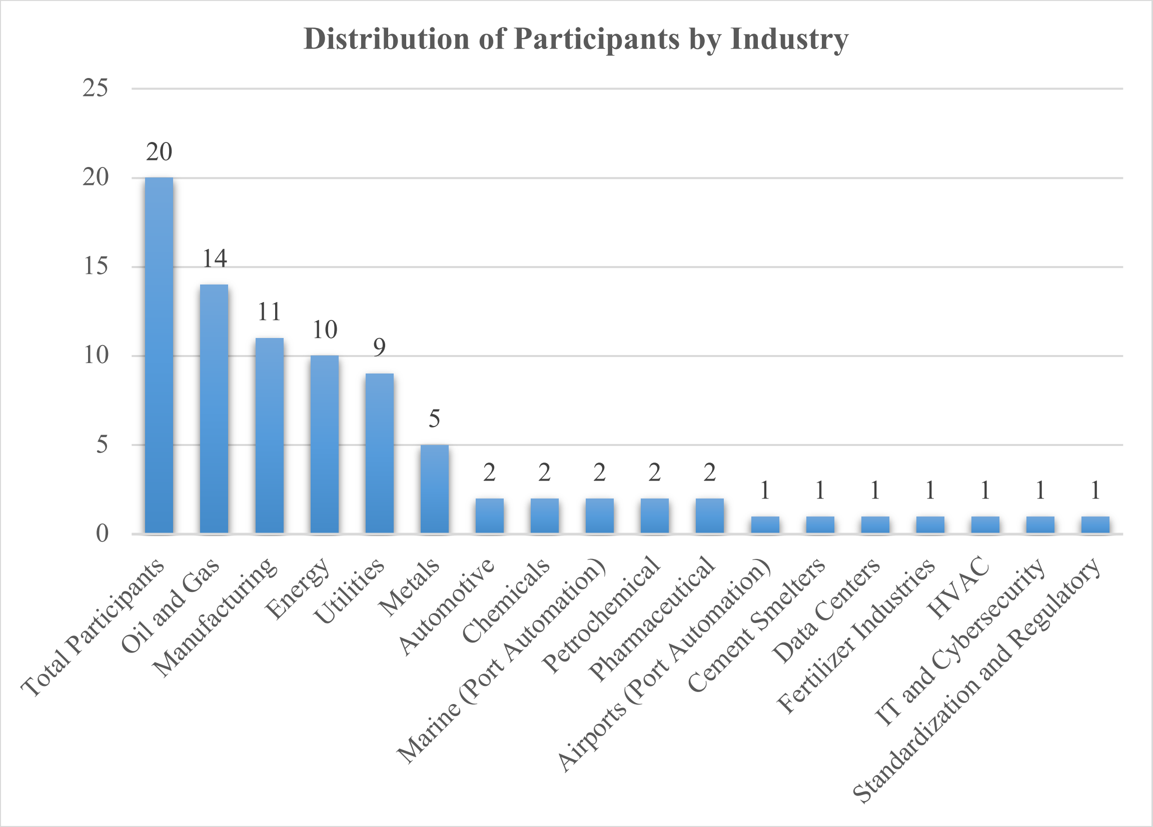
Data Collection

Interviews

I collected the primary data through one-on-one in-depth semistructured interviews using Zoom. I included 20 cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn. The participants were distributed across 13 countries and five continents, as shown in Figures 4 and 5. All participants met the inclusion criteria outlined in Table 7; they were purposively chosen from cybersecurity professionals with a minimum of 10 years of work experience with a wide range of CPS/ICS-based industries. Figure 6 shows the distribution of participants by industry.

Figure 6

Distribution of Participants by Industry



Note. Nineteen of the 20 participants have worked for more than one CPS/ICS-based industry.

All of the interviews began as standardized open-ended and highly structured in terms of the wording of the questions. Participants were always asked the identical questions included in Appendix A. The participants were free to answer the questions reflecting their own views based on their personal experience rather than their organizations' standpoint. I asked additional semistructured and open-ended questions based on the participants' responses to obtain more data or information. The first Zoom interview was conducted on May 3, 2021, and the last one was conducted on August 30,

2021. The primary data collection through interviews took longer than expected because it was difficult to find 20 CPS/ICS cybersecurity professionals with at least 10 years of experience and willing to volunteer for this study.

The interviews duration ranged between 16 minutes and 64 minutes, with an average of 39 minutes for the 20 interviews conducted. The interviews were conducted in one round; there was no need for a second round because the data analysis led to precise results, and the member checking were performed via emails to ensure the validity of the results. All Zoom interviews were audio-recorded, then the audio-recorded were converted into MS Word files using Sonix audio-to-text automatic conversion software (Sonix, n.d.). The MS Word files produced by this automatic transcription process were used for data analysis as outlined in Chapter 3.

CPS/ICS Cybersecurity Governance

A qualitative, multiple-case study was a proper design for this study because it allows researchers to understand the phenomenon of study by analyzing and triangulating data from multiple resources, including governmental and corporate documents, archival data, and semistructured interviews (see Yin, 2018). To increase the credibility and validity of the research findings and results through triangulation of data, in addition to analyzing the interviews, I also reviewed and conducted a qualitative thematic analysis of the following two cybersecurity governances:

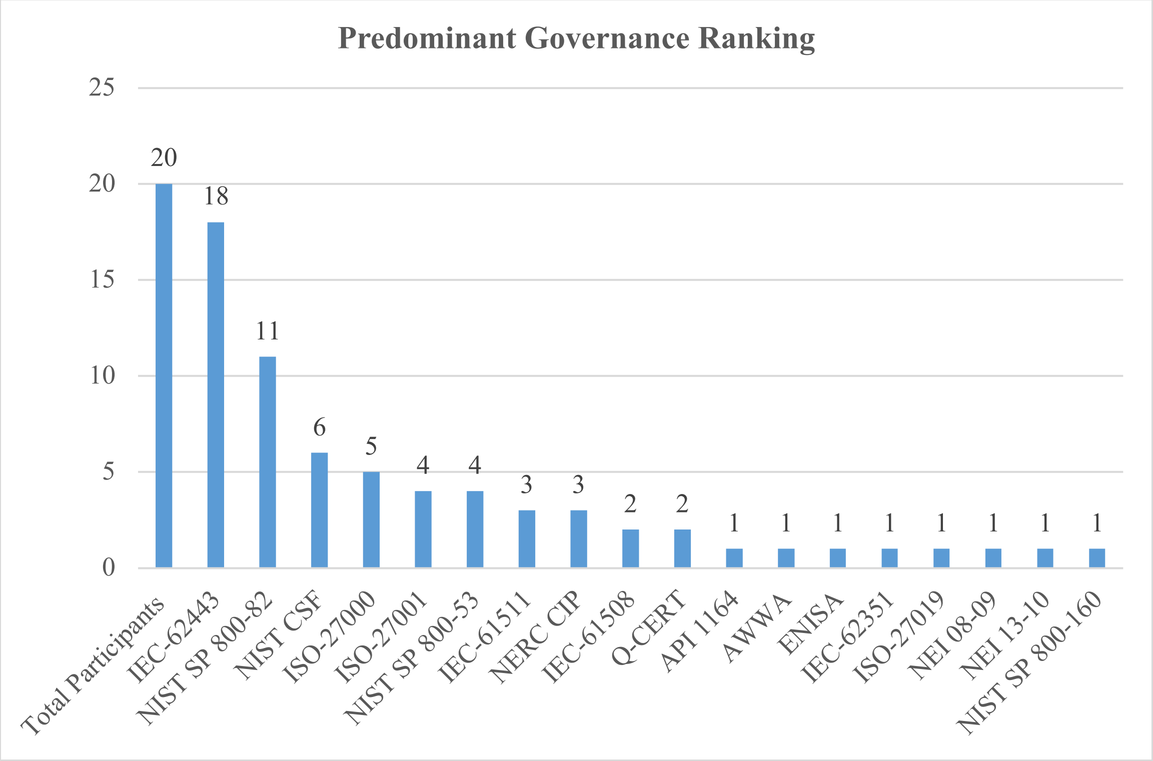
1. ISA/IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards), which incorporates the regulatory requirements for the ICS's cybersecurity.

2. NIST SP 800-82 rev. 2 (a guide to ICS security).

The literature review and the majority of the participants suggested that these two documents are the predominant governance to protect CPS/ICS against cyberattacks (see Figure 7).

Figure 7

Predominant Governance Ranking



I downloaded the ISA/IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards) from ISA Global Cybersecurity Alliance (n.d.). The qualitative thematic analysis of this document started on October 3, 2021 and was completed on October 10, 2021. The document NIST SP 800-82 rev. 2 (a guide to ICS security) was downloaded from Stouffer et al. (2015) and thematically analyzed during the period from

October 11, 2021, to October 24, 2021. The qualitative thematic analysis of both documents was conducted as per the plan outlined in Chapter 3.

Data Analysis

Interviews

I performed the data analysis manually using MS Word and Excel, following the Ose (2016) method outlined in Chapter 3; I began by analyzing the 20 Zoom interview transcripts. In the first analytical step, I read the whole transcript to highlight the texts that meaningfully addressed the interview questions. In the second step, I analyzed the participants' responses to the introductory question to ensure they met the inclusion criteria outlined in Table 7. I also sorted out the participants by country, continent, and CPS/ICS-based industry with goals to increase the result's validity and conclude how the predominant governance (identified in Figure 7) are spread across the world. The analysis of the data gathered from the introductory question was conducted quantitatively using MS Word and Excel. The quantitative results from the analysis of the introductory question are shown earlier in Figures 4, 5, and 6. In the third step of the analysis, I used Appendix A as a tool to link the participants' answers to each question with a knowledge area as a category, then associated each answer with a code. In the fourth step of the analysis, I developed labels of themes from the respondents' answers as presented in Table 8.

Table 8

Theme Labels Development

Theme #	Interview question	Category (knowledge area)	Code	Theme label
1	What critical system failure may occur due to cyberattacks on CPS and ICS	CPS detection system	Vulnerabilities	Vulnerabilities and consequences
2	What policies, standards, procedures, and best practices are endorsed to provide safety and security for the CPS and ICS	Existing CPS cybersecurity governance	Protection	Predominant governance
3	What type of cyberattacks can the proper application of policies, standards, procedures, and best practices prevent or mitigate	Efficiency of CPS policies and standards	Efficiency	Governance efficiency
4	What are the types of cyberattacks that the proper application of policies, standards, procedures, and best practices cannot prevent or mitigate	Efficiency of CPS policies and standards	Threats	Governance challenges
5	Why CPS and ICS are subject to cyberattacks	CPS vulnerability	Threats	Offenders and motives
6	What type of equipment upgrade, software, and governance would help enhance CPS and ICS safety and security	CPS cybersecurity improvement	Protection	System enhancements
7	How effective are organizational practices such as training, knowledge management, and incident reporting about various cyberattacks in identifying threats and developing standards or procedures to strengthen the CPS and ICS safety and security systems	Role of corporate management	Protection	System endorsement
8	How do you describe corporate management's role in establishing and sustaining the CPS and ICS safety and security systems	Role of corporate management	Protection	Performance assessment
9	What can the industrial community, especially the standardization and regulatory bodies, do to strengthen the CPS and ICS safety and security systems	Role of standardization and regulatory bodies	Protection	Governance mandate

Note. To conclude the predominant governance (Theme 2), I performed a quantitative analysis of the participants' answers using MS Word and Excel. Figure 7 shows that IEC 62443 and NIST SP 800-82 are the predominant governance, which conforms to the literature review.

During the fourth step of the analysis, I created nine detailed themes from clusters of meanings concluded from the participants' responses to the interview questions. The contribution of each participant to each theme is presented in Table 9.

Table 9

Participants' Contribution to Themes

Participant identifier	Themes								
	Theme 1	Theme 2	Theme 3	Theme 4	Theme 5	Theme 6	Theme 7	Theme 8	Theme 9
01	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
02	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
03	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
04	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
05	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
06	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
07	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
08	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
09	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
11	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
12	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
14	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
15		Yes							
16		Yes							
17		Yes							
18		Yes							
19		Yes							
20		Yes							

Theme 1: Vulnerabilities and Consequences

The theme CPS/ICS vulnerabilities and consequences emerged from the participants' responses to the first question (What critical system failure may occur due to cyberattacks on CPS and ICS?). There are two categories of typical system failures or attack scenarios, one of which is what Participant 01 referred to as the general white noise, in which as soon as a system is connected to an outside world, the threat level rises. A general white noise attack affects Windows operating systems and associated applications and Linux nodes. The failures that arise from those are also generic, such as ransomware that locks up the system entirely. Those failures are not directly CPS related because they target the IT infrastructure (PCs, desktop computers and associate applications).

Participant 01 and 13 others (70% of the total participants) indicated that general attacks on the IT infrastructure affect the underlying CPS that is controlled by Human-Machine Interface, or the DCS layer. The consequences may include shutdown to the process under control or at least efficiency limitations. Thus, CPS may not be as productive as they use to be before the attack. Still, typically that is not a catastrophic consequence because all the designed resilience, such as redundancy and safety systems, are typically beyond the reach of the general white noise attacks that are intended and prepared for the common IT layer. Because the IT layer provides control functionalities to the CPS, a general white noise attack on an IT layer could also affect CPS. Still, the consequences may not be catastrophic (depending on the criticality of the targeted organization and the production and service it delivers).

The second category is nation-state-sponsored cyberattacks, in which the offender is a nation-state-backed threat agent or sophisticated industrial espionage agents that are motivated through industrial espionage backgrounds, spending a significant number of resources on the design of the attack on developing malware. In such kind of predetermined attack scenario, offenders would spend a substantial amount of time on intelligence, on reconnaissance, then potentially even design exploits specifically for their target with an intent to develop malware to sabotage the target CPS/ICS. Unlike the general white noise attacks, nation-state-sponsored attacks are a lot less frequently happen. Still, when they happen, they sabotage safety systems, control systems, monitoring and visibility systems, and production systems. Catastrophic consequences of such sabotage include loss of lives, damage to critical assets, interruption of critical supplies to communities (such as electricity and water), and environmental disasters such as emission of toxic substances and river and marine pollution.

Theme 2: Predominant Governance

The CPS/ICS predominant governance were identified based on the participants' response to the second question (What policies, standards, procedures, and best practices are endorsed to provide safety and security for the CPS and ICS?). I performed a quantitative analysis of the participants' answers, 20 participants, using MS Word and Excel. Figure 7 shows that 18 participants (90%) identified IEC 62443, while 11 participants (55% of the total participants) identified NIST SP 800-82 as predominant governance, which conforms to the literature review.

Theme 3: Governance Efficiency

The theme CPS/ICS cybersecurity governance efficiency emerged from the participants' responses to the third question (What type of cyberattacks can the proper application of policies, standards, procedures, and best practices prevent or mitigate?). 70% of the respondents proposed that the general white noise attacks that target the IT foundation and the underlying CPS/ICS layer could be avoided by compliance to robust governance that mandate limiting access and exposure to the cloud, monitoring the networks, and preventing access to physical assets. Participant 02 suggested that compliance to good standards by well-trained people constructs the first defense line, but it all depends on how much money, time, and effort an organization is willing to spend to monitor and manage CPS access control. In theory, a completely locked down system or a completely managed and monitored system could probably deal with 90% plus of cyberattacks, but nothing is foolproof; nothing is entirely cyber secure. Participant 09 advised that besides the governance, proper segmentation design, and the use of effective monitoring and safeguarding technology could help enhance the safety and security of the CPS and ICS. Participants 01, 11, and 12 noted that the strength of CPS/ICS safety and security depends on three factors: well-trained people, adherence to governance or process, and the use of access management technology.

Theme 4: Governance Challenges

The theme challenges to CPS/ICS cybersecurity governance emerged from the participants' responses to the fourth question (What are the types of cyberattacks that the proper application of policies, standards, procedures, and best practices cannot prevent or mitigate?). Analysis of 14 interview transcripts (70% of the participants' responses) suggested that nation-state-sponsored attacks cannot be prevented or mitigated by the governance only because (according to participants 01 and 03) attackers analyze the policies and procedures, and the technology used by the target organization, and they design their attack schemes based on that organization's background. For an organization facing such an attacker, just application of governance alone will not help. Even if they have people who are rigorously following those procedures, the threat agent would probably find some gaps in that organization's procedures or technology and use it to launch a harmful attack. Rogue employees, supply chain and suppliers, and service providers who have access to the system were defined by Participants 02 and 05 as sources of insider threats against which CPS and ICS cybersecurity governance are less effective. Participant 02 said that social engineering is still probably the best class of attacks that can get through all defenses. Legacy systems and outdated systems' protections are other challenges for the CPS and ICS cybersecurity governance; Participant 10 noted that CPS and ICS cybersecurity governance are less effective in protecting the legacy and obsolete systems.

Theme 5: Offenders and Motives

The theme CPS/ICS offenders and their motives evolved from the participants' responses to the fifth question (Why CPS and ICS are subject to cyberattacks?). From the analysis of 14 interview transcripts (70% of the participants' responses), I concluded that the offenders could be a Script Kiddie, which is (according to participant 03) someone who is starting spoofing on the internet until he sees an exciting victim to reach out and to test his skills on. Motives also include hacktivism (hackers with political or social reasons), malware to blackmail organizations, offenders seeking publicity, offenders with a financial motivation (e.g., to get rid of the competition). Then there are the nation-state-sponsored attacks, where the motives include sabotaging critical infrastructures such as a power plant or a water station to interrupt supplies to a large community. Participant 05 noted that CPS and ICS systems are subject to cyberattacks because there is more network interconnectivity between IT and OT environments to enhance business processes. However, creating such interconnectivity exposes many vulnerable assets to the internet or the IT-managed systems, consequently increasing the likelihood of cyberattacks on those assets.

Theme 6: System Enhancements

The theme CPS/ICS system enhancement evolved from the participants' responses to the sixth question (What type of equipment upgrade, software, and governance would help enhance CPS and ICS safety and security?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed that replacing or upgrading the legacy equipment encompassed into CPS/ICS might be difficult to execute, unlike the IT infrastructures. Participants from 01 to 04 suggested that the equipment is what many people consider legacy and cannot be updated or upgraded in the same way as IT systems. The equipment itself is multiple times the price of the IT equivalent systems. Legacy equipment upgrades or replacement entails a large investment, and the return on investment is not usually feasible for those upgrades. Similar clusters were found in the responses of the Participates from 06 to 14.

Participant 01 emphasized the importance of updating the software running on the IT side and noted that the downside lies in the CPS and ICS that are not easy to keep updated due to the production requirements of 24/7 operations for months and even years makes it difficult to deploy updates. The deterministic management of change and the validation measures for certain applications make changing things much more difficult. For example, in a safety-regulated industry like oil and gas, deploying an update to see whether things still work is not permissible before rigorous testing and validation of all the potential routes. Such processes are complicated and costly, so especially in CPS/ICS environment, keeping CPS/ICS up to date is not always possible.

Theme 7: System Endorsement

The theme system endorsement evolved from the participants' responses to the seventh question (How effective are the organizational practices such as training, knowledge management, and incident reporting about various cyberattacks in identifying threats and developing standards or procedures to strengthen the CPS and ICS safety?). Analysis of 14 interview transcripts (70% of the participants' responses) disclosed unanimity on the importance of cybersecurity management practices, highlighting that they can be very effective only when corporate management promotes and endorses them as part of the corporate management system. Participant 02 suggested that training, knowledge management, and incident reporting practices can be very practical, at least by being an additional type of monitoring of cybersecurity management system. Even if an organization has the best technology, the cybersecurity system would not be effective if people do not monitor and report cybersecurity incidents.

All participants agreed to the importance of knowledge sharing and incident reporting. Participant 01 stated that knowledge management helps situational awareness and understanding of the threat landscape, what errors have been made elsewhere, what type of consequences have led to, and how they could have been avoided. Incident reporting is one of the essential cybersecurity practices; if organizations do not report what's going wrong, it would not be possible to derive any new knowledge about cyberattacks and associated prevention methods. Participants 01, 02, 03, 05, 07, 08, 09, 10, 11, and 14 have identified incident reporting as an area for improvement by compliance with corporate governance and mandatory regulations. Not all countries have mandatory regulations imposing reporting on cybersecurity incidents.

Participant 01 claimed that cybersecurity incident reporting is one of the areas that the industry has to improve. He noticed that there were conflicts of interest. For example, regulators were enforcing regulations in cases of non-compliance, issuing hefty fines that typically demotivate organizations from reporting because every report of an incident could potentially show that the concerned organization has not been following regulations or that they missed at least some part. If reporting such non-compliance leads to a significant fine, the concerned organization would rather hide it.

Theme 8: Performance Assessment

The theme performance assessment evolved from the participants’ responses to the eighth question (How do you describe corporate management's role in establishing and sustaining the CPS and ICS safety and security systems?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed that the role of corporate management is essential in establishing healthy organizational culture by promoting and endorsing cybersecurity governance as an intrinsic part of the corporate safety management system.

Participants 03 and 04 suggested that the role of corporate management is crucial as their approval and sponsorship are needed before any new technology or approach (such as CPS/ICS cybersecurity) can be adopted or implemented. Participants 01, 02, 03, 04, 05, and 11 noticed that the top management at some of the CPS/ICS-based industries operating on legacy systems have the mindset that production availability always has the priority over safety and security (including CPS and ICS cybersecurity) because production availability increases the company revenue while spending on safety and security increases the cost. From this perspective, those managers are unwilling to stop production to patch their operating systems or upgrade their legacy equipment, considering they have been working for decades. To change this cultural issue, Participants 01, 02, 04, and 11 suggested corporate management and regulatory bodies may endorse a performance assessment program that includes equipment certification and key performance indicators to measure the efficiency of CPS/ICS cybersecurity-related activities.

Theme 9: Governance Mandate

The theme governance mandate evolved from the participants’ responses to the ninth question (What can the industrial community, especially the standardization and regulatory bodies, do to strengthen the CPS and ICS safety and security systems?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed that more collaboration between the standardization firms and regulatory bodies on one side, and the CPS/ICS-based business owners and vendors on the other side could help enhance the quality and efficiency of governance against cyberattacks. Participant 02, who worked for one of the standardization firms, stated that his organization made active efforts to collaborate and reach out to as many different organizations as possible. He said that we have an active group of liaisons, and one of the issues that we deal with is that we are constantly struggling to get asset owners as part of our organization. Getting asset owners to take on cybersecurity is critical because they are doing the work and have to make those risk-based decisions whether to keep production up by continually running the process equipment or stop them to make updates to improve cybersecurity. They also manage the balance between production availability and associated revenue against financial impacts related to safety and cybersecurity expenditures.

Participant 02 explained why it was difficult to get asset owners involved in the activities of standards and regulatory bodies. He thought that the asset owners tended to be less vocal because they are worried about the image of their companies, or they are concerned about the image of their own involvement in adverse events. "Removing the stigma of things going wrong is crucial, and I do not know how to accomplish that," said Participant 02. The solution to these issues (as concluded from the responses of Participants 01, 03, 04, 05, 07, 08, 09, 12, 13, and 14) lies in mandating incident reporting by the regulatory authorities.

Participant 01 suggested that regulatory authorities should enforce CPS/ICS cybersecurity incident reporting and oblige all regulatory bodies from the individual member states to share incidents' experiences, cases, and threat intelligence across each other. He claimed that the right direction is to have nation-states recognize that cyberattacks on critical infrastructures can only be solved jointly upon an agreement to criminalize cyberattacks, preferably endorsed by the United Nations Security Council. Participant 01 also suggested that regulatory authorities need to establish interfaces among each other, regulatory bodies, and agencies with the necessary information and insight. The aim should be to motivate the entities that operate these CPS/ICS critical infrastructures, not by punishing them for reporting incidents but by encouraging them to learn from each other.

Participant 03 stated that in Europe, one ICS legislation mandates that critical infrastructure needs to be cyber secured and obliges organizations to report cyber incidents to their respective governments. He thought that this legislation is a good start to protect CPS-based infrastructures. Still, the regulatory authorities must start conducting audits to ensure this legislation is being implemented and impose fines for non-compliance with the requirements of that legislation. This viewpoint contradicts the one proposed earlier by Participant 01. Analysis of 14 interview transcripts (70% of the participants' responses) showed consensus about what the standardization firms can do to strengthen the CPS and ICS safety and security; they can simplify the standards to a reasonably practicable level so that the organizations can implement them.

CPS/ICS Cybersecurity Governance Review and Analysis

I triangulated the primary data obtained from the semistructured interviews and member checking against the secondary data obtained from the CPS/ICS governances

(IEC 62443 and NIST SP 800-82) to increase the credibility and validity of the research findings. The triangulation analysis was done by reviewing each document to find an answer to each interview question and then comparing these answers to the themes evolved from the interview transcripts' analysis to conclude conformity/disconformity amongst the data sources. The triangulation analysis results for both documents are outlined as follows:

Document IEC 62443 Triangulation Analysis

1. IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards) defined the consequences of critical system failure that may occur due to cyberattacks on CPS/ICS as: (a) safety or health hazard to public or employee, (b) environment damage, (c) equipment damage, (d) product integrity loss, (e) Loss of proprietary or confidential information, (f) legal or regulatory requirements violation, (g) financial loss, (h) company reputation or public confidence loss, and (i) entity, local, state, or national security threats. These undesired consequences conform to Theme 1 (CPS/ICS vulnerabilities and consequences), which evolved from the analysis of the interview transcripts.
2. IEC 62443 stated that the goals of its series are to advance the reliability, integrity, safety, and security of the Industrial Automation and Control Systems (IACS), or simply ICS, by using a methodical, risk-based, and comprehensive process through the whole ICS lifecycle. This goal statement conforms to Theme 2 (Predominant governance), which evolved from the analysis of the interview transcripts.

3. IEC 62443 stated that the efficiency of the ICS depends on more than the technology that encompasses a control system; it also comprises the work processes and people needed to ensure the integrity, reliability, safety, and security of the control system. Without adequately trained people, risk-fitting technologies, work processes, and countermeasures, an ICS could be more exposed and vulnerable to cyberattacks. These statements conform to Theme 3 (CPS/ICS cybersecurity governance efficiency), which evolved from the analysis of the interview transcripts.
4. IEC 62443 described cyber threat actors as insiders (unintentional or intentional), organized crime, cybercriminals, hacktivists, and state-sponsored attackers. Forms of cyberattacks include ransomware, destructive malware, coordinated and directed remote access attacks on ICS and linked infrastructure. These descriptions of cyber threat actors and forms of cyberattacks conform to Theme 4 (Challenges to CPS/ICS cybersecurity governance) and Theme 5 (CPS/ICS offenders and their motives), both of which evolved from the analysis of the interview transcripts.
5. IEC 62443 acknowledged that not all of its requirements could be met by legacy systems. Thus, recompensing countermeasures may be required to secure the ICS service providers. IEC 62443 also stated that the asset owner must specify and endorse the ICS security requirements throughout the supply chain to meet the overall conditions of the ICS cybersecurity program. This acknowledgement statement suggests that the update of the legacy systems is

a challenge to cybersecurity governance, which conforms to Theme 6 (CPS/ICS system enhancement) as it evolved from the analysis of the interview transcripts.

6. Part 3-2 of the IEC 62443 outlined the requirements for the risk assessment process without providing a specific methodology to be used. IEC 62443 suggested that the asset owners must establish and develop the cybersecurity risk assessment methodology and embed it into the corporate risk assessment methodology. This statement conforms to the shortfalls identified in Theme 7 (System endorsement), which evolved from the analysis of the interview transcripts.
7. IEC 62443 defined the asset owners' activities as: (a) establish and sustain a cybersecurity program that outlines ICS-specific requirements, (b) divide zones, communication channels, and execute related cybersecurity risk assessments, (c) specify the ICS requirements in a cybersecurity requirements specification document, (d) secure services and products necessary to meet the ICS requirements, (e) run and maintain the ICS cybersecurity program, and (f) measure the effectiveness of the ICS cybersecurity program. These activities conform to Theme 8 (Performance assessment), which evolved from the analysis of the interview transcripts.
8. Security level 4, as described in the IEC 62443, provided process metrics to control the effectiveness and performance of a typical cybersecurity system,

which also conforms to Theme 8 (Performance assessment) that evolved from the interview transcripts' analysis.

9. IEC 62443 (Quick Start Guide: An Overview of ISA/IEC 62443 Standards) provided a reference to a piece of news stating that “the United Nations Economic Commission for Europe (UNECE) has confirmed it will integrate the widely used ISA/IEC 62443 series of standards into its forthcoming Common Regulatory Framework on Cybersecurity (CRF). The CRF will serve as an official UN policy position statement for Europe.” (ISA Global Security Alliance, 2019). This piece of news conforms to Theme 9 (Governance mandate), which evolved from the analysis of the interview transcripts.

Document NIST SP 800-82 Triangulation Analysis

1. NIST SP 800-82 suggested that CPS/ICS reliance on interconnectivity upsurges the risks of cyberattacks. Denial of Service (DoS) and malware (e.g., viruses, worms) have become common cyberattacks against CPS/ICS. Possible consequences of a CPS/ICS incident include: (a) threat to national security, (b) loss or reduction of production at one or several producing facilities, (c) death or injury of employees, (d) death or injury of people in the community, (e) equipment damage, (f) environmental damage, (g) diversion or release of hazardous materials, (h) regulatory requirements violation, (i) product infection, (k) legal liabilities, (l) confidential information or proprietary loss, and (m) customer confidence or brand image loss. These

cyberattacks and consequences conform to IEC 62443 and Theme 1 (CPS/ICS vulnerabilities and consequences), which evolved from the analysis of the interview transcripts.

2. NIST SP 800-82 offered guidance to securing ICS, including SCADA systems, DCS, and PLC, while directing their unique performance, safety, and reliability requirements. NIST SP 800-82 also provided an overview of ICS and archetypal system topologies, classifies typical threats and vulnerabilities to these systems, and recommends cybersecurity countermeasures to alleviate related risks. This scope conforms to Theme 2 (Predominant governance), which evolved from the analysis of the interview transcripts.
3. NIST SP 800-82 introduced possible incidents a CPS/ICS may face as: (a) obstructed or delayed flow of information over CPS/ICS networks, which could disrupt the operation of CPS/ICS, (b) unapproved changes to commands, instructions, or alarm thresholds, which could disable, damage, or shutdown processing equipment, cause environmental damage, or threaten human life, (c) incorrect information sent to system operators, either to hide unauthorized changes, or to deceive the operators into initiating actions that could result in negative consequences, (d) software configuration or modification, or malware-infected software that could cause adverse results, (e) biasing the operation of protection systems, which could cause costly equipment damage, and (f) biasing the operation of safety systems, which could result in catastrophic incidents. NIST SP 800-82 provided guidelines for

preventing these types of incidents. Therefore, it conforms to Theme 3 (CPS/ICS cybersecurity governance efficiency), which evolved from the analysis of the interview transcripts.

4. Table C-1 of the governance NIST SP 800-82 provided a comprehensive list of threat sources to ICS, suggesting that governance's efficiency in preventing them may vary depending on their magnitude, frequency, and ability to compound other interconnected events. This statement conforms to IEC 62443 and Theme 4 (Challenges to CPS/ICS cybersecurity governance) that evolved from the analysis of the interview transcripts.
5. NIST SP 800-82 suggested that initially, CPS/ICS had little similarity to IT systems in that these systems were isolated systems running branded control protocols and using specified hardware and software. Broadly available, low-cost Ethernet and Internet Protocol (IP) devices are now replacing the older proprietary technologies, increasing the likelihood of cybersecurity vulnerabilities and catastrophic incidents. CPS/ICS incorporate IT solutions to support corporate connectivity and remote access capabilities and are designed to use customary industry computers, OS, and network protocols. Such integration causes less separation from the outside world, generating a more need to secure these systems. These statements conform to IEC 62443 and the system vulnerabilities included in Theme 5 (CPS/ICS offenders and their motives) that evolved from the analysis of the interview transcripts.

6. NIST SP 800-82 stated that today's CPS/ICS are typically a combination of legacy systems with an estimated lifetime ranging between 20 and 30 years or a mixture of legacy systems supplemented by newer hardware and software interlocked with other systems. Thus, it is difficult or impracticable to implement some of the security controls recommended by NIST SP 800-53. This statement provides proof that the update of the legacy system is a challenge to cybersecurity governance, as concluded by the participants, and therefore it conforms to IEC 62443 and Theme 6 (CPS/ICS system enhancement) that evolved from the analysis of the interview transcripts.
7. NIST SP 800-82 suggested operators to effectively integrate security into CPS/ICS by defining and implementing an all-inclusive program that addresses all aspects of cybersecurity, ranging from specifying objectives to day-to-day operation and continuing compliance auditing and improvement. Efficiency of a CPS/ICS cybersecurity system depends on assigning information security manager with adequate responsibility and authority. The fundamental process for developing a CPS/ICS cybersecurity program include: (a) create a business case for cybersecurity, (b) specify charter and scope, (c) form and train a cross-disciplinary team, (e) develop specific CPS/ICS cybersecurity policies and procedures, (f) develop and execute a CPS/ICS cybersecurity risk management framework, and (g) offer training and adopt security awareness for CPS/ICS staff. These practices conform to

IEC 62443 and Theme 7 (System endorsement) that evolved from the analysis of the interview transcripts.

8. NIST SP 800-82 suggested that the commitment to a CPS/ICS security program commences at the top. It is essential for the success of CPS/ICS security program that the organization's top-management buy-in and participate in the CPS/ICS security program. Tier 1 organization level management that incorporates both IT and CPS/ICS operations has the perception and authority to comprehend and take responsibility for the cybersecurity risks. The Tier 1 business leadership are responsible for approving and enforcing information security policies, setting cybersecurity roles and responsibilities, executing the cybersecurity program across the organization, and funding for the entire program in phases. These roles and responsibilities conform to IEC 62443 and Theme 8 (Performance assessment) that evolved from the analysis of the interview transcripts.
9. NIST SP 800-82 stipulated that the information security manager should create a policy that outlines the information security organization's supervisory charter and specifies mission, business process managers, system owners' roles, responsibilities, accountabilities, and users. The information security manager should document and decide upon the goals and objectives of the cybersecurity program, defines the business groups affected, the computer systems and networks to be protected, the sources and budget required, and the breakdown of responsibilities. The scope should also address

business, training, audit, legal and regulatory requirements, and execution schedules and commitments. This scope suggests collaboration with regulatory bodies and standardization firms as partial activities within the cybersecurity management program. Therefore, it conforms to the shortfalls identified in Theme 9 (Governance mandate), which evolved from the analysis of the interview transcripts.

Evidence of Trustworthiness

Credibility

As outlined in Chapter 3, the participant's review of the researcher's notes and transcribed data provides quality control over the content and adds to the credibility of the study (see Perrotta, 2017). I used interview transcripts and conducted member checking by sharing my perception and interpretation notes, the transcribed data, and interview findings with each participant via email. I intended to follow up for further clarifications via telephonic interviews, but that was unnecessary as the participants' responses were clear and sufficient. To ensure that member checking is a value-added validation technique, I conducted a complete analysis of each participant's feedback until the saturation was achieved after 14 interviews.

To attain this study’s credibility, I used recognized and approved research methods (qualitative, multiple-case study using RAT), maintained familiarity with the context, used transparent recruiting and informed consent. I used triangulation of the CPS/ICS governance and the interview transcripts to increase the credibility and validity of the research findings and results to other CPS/ICS industries. Out of 14 interviews analyzed until the saturation was achieved, 14 (100%) interview transcripts contained similar clusters that led to producing the nine themes, titles of which were presented earlier in this chapter and presented in detail later in the study findings section. I intended to discuss the discrepant cases or findings with the participants, but there were no discrepancies to discuss.

Transferability

Transferability is described as the overall comparison of research findings against similar studies to conclude possible commonality (see Allred et al., 2017). To attain transferability and provide the reader with the necessary information to make a well-informed decision, the researcher should provide a precise explanation of the research methods employed in the study (see Sidhu et al., 2017). To support the transferability of this study, I did the following:

- The two CPS/ICS cybersecurity governances that I selected for thematic analysis (IEC 62443 and NIST SP 800-82) are endorsed by internationally recognized standardization/regulatory firms and adopted globally by most CPS-based industries. Out of the 20 participants included in the study, 18 (90%) identified IEC 62443 as one of the predominant cybersecurity governance. 11 participants (55%) identified NIST SP 800-82 as one of the predominant cybersecurity standards (see Figure 7).
- To attain external validity, I conducted Zoom interviews with 20 CPS cybersecurity experts selected purposively from worldwide cybersecurity-specialist groups on LinkedIn. These participants were from 13 countries

spread across five continents (see Figures 4 and 5); they work for a wide range of 17 CPS/ICS-based industries worldwide (see Figure 6).

- The study's participants were cybersecurity experts selected purposively from a large spectrum of CPS/ICS-based industry; the consistency of the themes developed from participants' answers to each interview question support the validity and transferability of the study findings and results to other CPS/ICS industries.
- In Chapter 3, I provided a full description of the context and setting of data collection, explained participant selection criteria, and specified the recruitment process. Also, I explained the research design and conceptual framework and explained the data analysis plan.
- I present the study results later in this chapter and propose the recommendations in Chapter 5.

Dependability

As outlined in Chapter 3, the tactic needed to ensure dependability and confirmability depends on using an audit trail. The researchers provide a complete set of notes on choices made throughout the research process (see Korstjens & Moser, 2018). I maintained an updated audit trail documenting the evolution of research design and methods, data collection, and analysis strategies to sustain this study's dependability. I kept timely reports on the flow and any changes to procedures. I ensured that the study participants were cybersecurity professionals who met the eligibility criteria specified in

Table 7. I adhered to the IRB-approved protocol and all ethical procedures to recruit participants, using the approved consent form.

Confirmability

A thorough explanation of the research processes should be provided to guarantee the study's confirmability (see Kalu & Bwalya, 2017). Confirmability can be enhanced by reflexibility, which is a process that permeates the entire research effort; therefore, it is proper to address the steps taken throughout the manuscript (see Dodgson, 2019). To enhance the confirmability of this research, I presented the findings through extraction from the result of participants' experiences and ideas rather than my own characteristics and preferences. In doing so, I provided detailed descriptions of the researcher's role and his affiliation with the setting, context, and phenomenon. I performed triangulation of the CPS/ICS governance and the interview transcripts to increase the credibility and validity of the research findings and results. I preserved the transparency of the audit trail throughout the process, from data collection through interpretation. I presented in figures and texts how I moved from data to codes to categories to themes.

Study Results

The main research question that guided this study was as follows: How can cybersecurity governance be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry? This question was broken down into the nine (open-ended) interview questions outlined in Appendix A. 20 cybersecurity experts from 13 countries, five continents, and 17 CPS/ICS-based industries shared their knowledge and experiences by answering the questions through one-to-one semistructured interviews using Zoom. I analyzed the interview transcripts and explained how I linked every interview question with a category, code, and concluded themes from the participants’ responses (see the data analysis section of this chapter). The findings from the themes concluded from participants’ responses are presented as follows:

Result 1: CPS/ICS Vulnerabilities and Consequences

The participants were asked what critical system failure may occur due to cyberattacks on CPS and ICS. The participants' responses revealed that the system failures depend on the type of cyberattack. There are two categories of typical system failures or attack scenarios, one of which is what Participant 01 referred to as the general white noise. This category of attacks directly targets the IT infrastructure (PCs, desktop computers and associated applications) and indirectly targets the underlying CPS/ICS that the Human-Machine Interface, or the DCS layer control. The second category is nation-state-sponsored cyberattacks. The offender, in this case, is a nation-state-backed threat agent or sophisticated industrial espionage agent motivated through industrial espionage backgrounds and spending unlimited resources on the design of malware to design sabotage the DCS/ICS. According to 14 participants (70% of the participants' responses), the consequences of cyberattacks on CPS-ICS vary depending on the type of cyberattack and the criticality of the targeted organization and the production and service it delivers. Vulnerable items targeted by offenders include IT infrastructure, process control and visibility systems, safety systems, and production system. Catastrophic consequences due to cyberattacks on CPS/ICS-based industries may include loss of lives, damage to critical assets, interruption of critical supplies to communities (such as electricity and water), and environmental disasters such as emission of toxic substances and river and marine pollution.

Result 2: Predominant CPS/ICS Cybersecurity Governance

The CPS/ICS predominant governances were identified due to the participants' responses to the second question (What policies, standards, procedures, and best practices are endorsed to provide safety and security for the CPS and ICS?). Figure 7 shows that 18 participants (90%) identified IEC 62443, while 11 participants (55% of the total participants) identified NIST SP 800-82 as predominant governance, which conforms to the literature review.

Result 3: Efficiency of CPS/ICS Cybersecurity Governance

The efficiency of the CPS/ICS cybersecurity governance was linked to the third question (What type of cyberattacks can the proper application of policies, standards, procedures, and best practices prevent or mitigate?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed that the general white noise attacks that target the IT foundation and the underlying CPS/ICS layer could be avoided by compliance to robust governance that mandate limiting access and exposure to the cloud, monitoring the networks, and preventing access to physical assets. Additional findings from the analysis of participants' responses are as follows:

- Participant 02 suggested that compliance to good standards by well-trained people constructs the first defense line. Still, it all depends on how much money, time, and effort an organization is willing to spend to monitor and manage access control. In theory, a completely locked down system or a completely managed and monitored system could probably deal with 90% plus of cyberattacks, but nothing is foolproof; nothing is entirely cyber secure.

- Participant 09 advised that besides the governance, proper segmentation design, and the use of effective monitoring and safeguarding technology could help enhance the safety and security of the CPS and ICS.
- Participants 01, 11 and 12 noted that the strength of CPS/ICS safety and security depends on three factors: well-trained people, adherence to governance or process, and the use of access management technology.

Result 4: Governance Challenges

Challenges to CPS/ICS were linked to the fourth question (What are the types of cyberattacks that the proper application of policies, standards, procedures, and best practices cannot prevent or mitigate?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed the following results:

- Nation-state-sponsored attacks cannot be prevented or mitigated by the governance only because (according to Participants 01 and 03), attackers analyze the governance and the technology used by the target organization, and they design their attack schemes based on that organization’s background.
- Rogue employees, supply chain and suppliers, and service providers who have access to the system were defined by Participants 02 and 05 as sources of insider threats, against which CPS and ICS cybersecurity governance are less effective.

- Social engineering (according to Participant 02) is still probably the best class of attacks that can get through all defenses.
- Legacy systems and outdated systems' protections are challenges for the CPS and ICS cybersecurity governance. Participant 10 noted that CPS and ICS cybersecurity governance are less effective in protecting the legacy and obsolete systems.

Result 5: Offenders and Motives

The CPS/ICS offenders and their motives were evolved from the participants' responses to the fifth question (Why CPS and ICS are subject to cyberattacks?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed that the offenders include the following:

- Script Kiddie, which is (according to Participant 03) someone who is starting spoofing on the internet until he sees an exciting victim to reach out and test his skills on.
- Hacktivism (hackers with political or social reasons).
- Malware to blackmail organizations.
- Offenders seeking publicity.
- Offenders with a financial motivation (e.g., to get rid of the competition).
- Nation-state-sponsored attacks, where the motives include sabotaging critical infrastructures such as a power plant or a water station to interrupt supplies to a large community.

Participant 05 noted that CPS and ICS systems are subject to cyberattacks because there is more network interconnectivity between IT and OT environments that can enhance business processes. However, by creating such connections, we are exposing many vulnerable assets to the internet or the IT-managed systems.\.

Result 6: CPS/ICS Safety and Security Enhancement

The theme CPS/ICS system enhancement was evolved due to linking the CPS cybersecurity improvement as a category with the sixth question (What type of equipment upgrade, software, and governance would help enhance CPS and ICS safety and security?). Analysis of 14 interview transcripts (70% of the participants' responses) showed the following findings:

- Replacing or upgrading the legacy equipment encompassed into CPS/ICS might be difficult to execute, unlike the IT infrastructures. Participants from 01 to 04 suggested that the equipment is what many people consider legacy and cannot be updated or upgraded the same way as IT systems. Legacy equipment upgrades or replacement entails a large investment, and the return on investment is not usually feasible for those upgrades. Similar clusters were found in the responses of the Participates from 06 to 14.
- Participant 01 stressed the importance of updating the software running on the IT side and noted that the downside lies in the CPS and ICS that are not easy to keep updated due to the production requirements of 24/7 operations for months and even years make it difficult to deploy updates.

- According to Participant 01, the deterministic management of change and the validation measures for certain applications make it much more difficult to change things. For example, in a safety-regulated industry like oil and gas, deploying an update to see whether things still work is not permissible before rigorous testing and validation of all the potential routes. Such processes are complicated and costly, so especially in CPS/ICS environment, keeping up to date is not always possible.

Result 7: Cybersecurity System Endorsement

The system endorsement as a theme evolved due to linking the role of corporate management as a category with the seventh question (How effective are the organizational practices such as training, knowledge management, and incident reporting about various cyberattacks in identifying threats and developing standards or procedures to strengthen the CPS and ICS safety?). The results concluded from this theme are as follows:

- Analysis of 14 interview transcripts (70% of the participants' responses) showed unanimity on the importance of cybersecurity management practices, highlighting that they can be very effective only when corporate management promotes and endorses them as part of the corporate management system.
- Participant 02 suggested that training, knowledge management, and incident reporting practices can be very practical, at least by being an additional type of monitoring of cybersecurity management system. Even if an organization

has the best technology, the cybersecurity system would not be effective if people do not monitor and report cybersecurity incidents.

- Participant 01 stated that knowledge management helps situational awareness and understanding of the threat landscape (what errors have been made elsewhere, what type of consequences have led to, and how they could have been avoided).
- Participants 01, 02, 03, 05, 07, 08, 09, 10, 11, and 14 have identified incident reporting as an area for improvement by compliance with corporate governance and mandatory regulations. Not all countries have mandatory regulations imposing reporting on cybersecurity incidents.
- Participant 01 claimed that cybersecurity incident reporting is one of the areas that the industry has to improve. He noticed that there were conflicts of interest. For example, regulators were enforcing regulations in cases of non-compliance, issuing hefty fines that typically demotivate organizations from reporting because every report of an incident potentially shows that they have not been following regulations or that they missed at least some part. If reporting such non-compliance leads to a significant fine, the concerned organization would rather hide it.

Result 8: CPS/ICS Cybersecurity Performance Assessment

The theme performance assessment was developed by linking the role of corporate management as a category (knowledge area) and the eight-question (How do you describe corporate management's role in establishing and sustaining the CPS and ICS safety and security systems?). Analysis of 14 interview transcripts (70% of the participants' responses) revealed the following results:

- The role of corporate management is essential in establishing healthy organizational culture by promoting and endorsing cybersecurity governance as an intrinsic part of the corporate management system.
- Participants 03 and 04 suggested that the role of corporate management is crucial as their approval and sponsorship are needed before any new technology or approach (such as CPS/ICS cybersecurity) can be adopted or implemented.
- Participants 01, 02, 03, 04, 05, and 11 noticed that the top management at some of the CPS/ICS-based industries operating on legacy systems have the mindset that production availability always has the priority over safety and security (including CPS and ICS cybersecurity) because production availability increases the company revenue while spending on safety and security increases the cost. From this perspective, those managers are unwilling to stop production to patch their operating systems or upgrade their legacy equipment because they have been working for decades.
- Participants 01, 02, 04, and 11 suggested that corporate management and regulatory bodies may endorse a performance assessment program that includes equipment certification and key performance indicators on CPS/ICS cybersecurity-related activities to change the cultural issue stated above.

Result 9: Governance Mandate

The governance mandate as a theme evolved from linking the role of standardization and regulatory bodies as category (knowledge area) with the ninth question (What can the industrial community, especially the standardization and regulatory bodies, do to strengthen the CPS and ICS safety and security systems?). Analysis of 14 interview transcripts showed the following results:

- More collaboration between the standardization firms and regulatory bodies on one side, and the CPS/ICS-based business owners and vendors on the other side could help enhance the quality and efficiency of governance against cyberattacks.
- Participant 02, who worked for one of the standardization firms, stated that it is difficult to get asset owners involved in the activities of standards and regulatory bodies because asset owners tend to be less vocal as they are worried about the image of their companies, or they are concerned about the image of their own involvement in things. The solution to these issues (as concluded from the responses of Participants 01, 03, 04, 05, 07, 08, 09, 12, 13, and 14) lies in mandating incident reporting by the regulatory authorities.
- Participant 01 suggested that regulatory authorities should enforce CPS/ICS cybersecurity incident reporting and oblige all regulatory bodies from the individual member states to share incidents' experiences, cases, and threat intelligence across each other. He claimed that the right direction is to have nation-states recognize that cyberattacks on critical infrastructures can only be

solved jointly, ideally upon an agreement to criminalize cyberattacks endorsed by the United Nations Security Council.

- Participant 03 stated that in Europe, one ICS legislation mandates that critical infrastructure needs to be cyber secure and obliges organizations to report cyber incidents to their respective governments. Still, the regulatory authorities must conduct audits to ensure this legislation is being implemented and impose fines for non-compliance with the requirements of that legislation. This viewpoint contradicts the one proposed earlier by Participant 01.
- Analysis of 14 interview transcripts (70% of the participants' responses) showed consensus about how standardization firms can strengthen the CPS and ICS safety and security; they can simplify the cybersecurity governance to a reasonably practicable level so that the organizations can implement them.

Summary

In Chapter 4, I presented an analysis of the data collected through one-on-one in-depth semistructured interviews using Zoom provided 827 minutes of audio recordings with 20 cybersecurity experts selected from worldwide cybersecurity specialist groups on LinkedIn. Nine themes that emerged from the analysis of the interview transcripts were consistent with each other and the reviewed literature, as outlined in Chapter 2. In Theme 1, the participants addressed the research question by sharing their experiences about the CPS/ICS vulnerabilities to cyberattacks and associated consequences. In Theme 2, the participants addressed the research question by identifying the predominant cybersecurity governance. In Theme 3, the participants addressed the research question by evaluating the efficiency of cybersecurity governance. In Theme 4, the participants addressed the research question by describing the challenges of cyberattacks against which the governance are less effective. In Theme 5, the participants addressed the research question by identifying the CPS/ICS offenders and motives. In Theme 6, the participants addressed the research question by introducing a cybersecurity system enhancement method. In Theme 7, the participants addressed the research question by describing the corporate management's role in endorsing cybersecurity governance. In Theme 8, the participants addressed the research question by describing the role of corporate management in authorizing the cybersecurity performance assessment. In Theme 9, the participants addressed the research question by explaining the role of standardization and regulatory bodies in creating and mandating cybersecurity governance.

The consistency of the data and the adherence of the study to the qualitative, multiple-case study method using RAT (which served as a conceptual theory for this study, as outlined in Chapter 3) support the trustworthiness of this study. I also triangulated the data obtained from the semistructured interviews and member checking with the CPS/ICS governance, then tied them back to RAT to increase the credibility and validity of the research findings. Chapter 5 includes interpretation of the study findings, and limitations of the study. Chapter 5 also contains recommendations for further research, implications for positive social change and concludes with the key essence of the study.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this study was to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. A qualitative, multiple-case study using the RAT (Cohen & Felson, 1979) as a conceptual theory was conducted. Primary data collected via in-depth semistructured Zoom interviews with 20 cybersecurity experts selected from worldwide cybersecurity groups on LinkedIn. Interview transcripts' analysis delivered the study results in nine themes, consistent with the literature and document reviews.

Theme 1 (Vulnerabilities and consequences) emerged from the participants' explanations of the critical system's failure and consequences due to cyberattacks on CPS/ICS. Theme 2 (Predominant governance) emerged from the participants' identification of the predominant CPS governance. Themes 3 and 4 (Governance efficiency and Governance challenges, respectively) emerged from the participants' experiences on the cyberattacks that can and cannot be prevented using CPS governance. Theme 5 (Offenders and motives) emerged from the participants' explanations of why CPS are subject to cyberattacks. Theme 6 (System enhancements) emerged from the participants' explanations of how to enhance CPS cybersecurity. Theme 7 (System endorsement) emerged from the participants' evaluation of organizational cybersecurity practices. Theme 8 (Performance assessment) emerged from the participants' descriptions of corporate management's role in establishing a cybersecurity system. Theme 9 (Governance mandate) emerged from the participants' views of what standardization and regulatory bodies can do to strengthen the CPS cybersecurity systems.

Interpretation of Findings

The research question that guided this study was as follows: How can cybersecurity governance be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry? This question was broken down into the nine (open-ended) interview questions outlined in Appendix A. The key findings presented below were concluded from the nine themes that emerged from the analysis of semistructured interview transcripts as primary data. The below findings conform to the analysis of the two CPS/ICS cybersecurity governances reviewed and analyzed as secondary data (IEC 62443 and NIST SP 800-82), as outlined in the data analysis section of Chapter 4. Both primary and secondary data also conform to the peer-reviewed literature in Chapter 2, as described below.

Finding 1: Vulnerabilities and Consequences

Vulnerabilities and consequences of cyberattacks on CPS/ICS are key findings derived from Theme 1 that emerged from the participants' responses. The vulnerabilities and threat levels rise as CPS/ICS are connected to an outside world. CPS/ICS are exposed to two types of cyberattacks: (a) the general white noise attack that affects Windows operating systems all within its application and Linux nodes, and (b) nation-state-sponsored cyberattacks, in which the offender is a nation-state-backed threat agent or sophisticated industrial espionage agents that are motivated through industrial espionage backgrounds, spending a significant number of resources on the design of the attack on developing malware sabotage opponents' critical infrastructure. Catastrophic consequences of such sabotage include loss of lives, damage to critical assets, interruption of critical supplies to communities (such as electricity and water), and environmental disasters such as emission of toxic substances and river and marine pollution. This finding conforms Ding et al.'s (2020) and Ahmad et al.'s (2018) classifications of cyberattacks on CPSs and the vulnerable target as an element of the RAT (Cohen & Felson, 1979), as outlined in Chapter 2. The participants' responses conformed to the analysis of the governance IEC 62443 and NIST SP 800-82, both of which provide guidance on how to protect CPS/ICS against cyberattacks, including the recommended defense-in-depth architecture (see Figure 3).

Finding 2: Predominant Governance

The predominant governance is an essential finding derived from Theme 2 that emerged from the participants' responses. Figure 7 shows that 18 participants (90%) identified IEC 62443, while 11 participants (55% of the total participants) identified NIST SP 800-82 as predominant governance. These two governances were used as a secondary data source to validate the primary data obtained from the thematic analysis of the interview transcripts. This finding conforms to the state of cybersecurity governance (Cardenas & Cruz, 2019; Lyu et al., 2019; Ross et al., 2018; Yoo & Shon, 2016; You et al., 2019), as outlined in Chapter 2.

Finding 3: Governance Efficiency

The governance efficiency is a key finding derived from Theme 3 that emerged from the participants' responses. The majority of the participants (70%) proposed that the general white noise attacks on the IT foundation and the underlying CPS/ICS layer could be prevented by compliance to robust governance that enforces limiting access and exposure to the cloud, monitoring the networks, and preventing access to physical assets. Participants 01, 11, and 12 noted that compliance with strict governance provides the primary defense line. Still, the strength of CPS/ICS governance depends on three factors: well-trained people, adherence to governance or process, and the use of access management technology. This finding implies that the efficiency of a cybersecurity system does not depend only on governance but also on well-trained people and the use of network access management technology. Therefore, it conforms to the CPS/ICS cybersecurity countermeasures (Alladi et al., 2020; Lamba, 2018), as described in Chapter 2. The participants' responses were also aligned with the analysis of IEC 62443 and NIST SP 800-82, as described in the data analysis section of Chapter 4.

Finding 4: Governance challenges

The governance challenges is a significant finding derived from Theme 4 that emerged from the participants' responses. Analysis of 14 interview transcripts (70% of the total participants) suggested that the nation-state-sponsored attacks cannot be prevented or mitigated by the governance only for the reasons explained earlier (see Finding 1 in this section). The review and analysis of IEC 62443 and NIST SP 800-82 showed that these two governances identified the nation-state-sponsored attacks but provided no clear direction on preventing them (see the data analysis section of Chapter 4). Participants 02 and 05 identified rogue employees, supply chain and suppliers, and service providers who have access to the system as other threats, against which cybersecurity governance are less effective. These findings highlight the challenges facing the CPS/ICS governance and conform to the cyberattacks as threats to CPS/ICS (Ahmad et al., 2018), as outlined in Chapter 2.

Finding 5: Offenders and Motives

The offenders and motives is a major finding derived from Theme 5 that emerged from the participants’ responses. Analysis of 14 interview transcripts (70% of the participants' responses) revealed that CPS/ICS offenders include insiders (rogue employees), script kiddies, hacktivists, organized crime, cybercriminals, and nation-state-sponsored attackers. Types of cyberattacks vary depending on the motives between ransomware and destructive malware. The participants’ responses were aligned with the review and analysis of IEC 62443 and NIST SP 800-82, as defined in the data analysis section of Chapter 4. This finding conforms to the cyberattacks as threats to CPS/ICS (Ahmad et al., 2018) and specifies the CPS/ICS offenders as an element of the RAT (Cohen & Felson, 1979), as described in Chapter 2.

Finding 6: System Enhancements

System enhancements is a key finding derived from Theme 6 that emerged from the participants' responses. Analysis of 70% of the participants' responses showed that replacing or upgrading the legacy equipment encompassed into CPS/ICS might be challenging to execute. Legacy equipment upgrades or replacement entails a significant investment, and the return on investment is not usually feasible for those upgrades. Participant 01 stressed the importance of updating the software running on the IT side. He noted that the downside lies in the CPS and ICS that are not easy to keep updated due to the production requirements of 24/7 operations for months and even years make it challenging to deploy updates. In a safety-regulated industry like oil and gas, deploying an update to see whether things still work is not permissible before rigorous testing and validation of all the potential routes. Such complicated processes are costly; therefore, keeping legacy equipment up to date is not always possible. These participants' responses highlighted the need to enhance the cybersecurity of the legacy systems through well-planned updating and, therefore, conform to the CPS/ICS cybersecurity countermeasures (Alladi et al., 2020) as outlined in Chapter 2. The participants' responses also conformed to the analysis of the governance IEC 62443 and NIST SP 800-82, as described in the data analysis section of Chapter 4.

Finding 7: System Endorsement

System endorsement is a crucial finding derived from Theme 7 that emerged from the participants' responses. Analysis of 70% of the participants' responses revealed unanimity on the importance of cybersecurity management practices, highlighting that they can be very effective only when corporate management promotes and endorses them as part of the corporate management system. Participant 02 suggested that training, knowledge management, and incident reporting practices can be efficient by monitoring the cybersecurity management system.

Participants 01, 02, 03, 05, 07, 08, 09, 10, 11, and 14 identified incident reporting as an area for improvement by compliance with corporate governance and mandatory regulations. Not all countries have mandatory regulations imposing reporting on cybersecurity incidents. Participant 01 claimed that cybersecurity incident reporting is one of the areas that the industry has to improve. He noticed that there were conflicts of interest. For example, regulators were enforcing regulations in cases of noncompliance, issuing hefty fines that typically demotivate organizations from reporting because every report of an incident potentially shows that they have not been following regulations or that they missed at least some part. If reporting such noncompliance leads to a significant fine, the concerned organization would rather hide it. This finding conforms to the CPS/ICS cybersecurity countermeasures (Abdelghani, 2019; Stouffer et al., 2015) as outlined in Chapter 2. In conclusion, the participants' responses highlighted the importance of corporate management role in endorsing the CPS/ICS cybersecurity practices as a critical part of the corporate management system, especially the incident reporting and knowledge sharing (the practices that the participants defined as an area for improvement to the system). These results from the analysis of the participants' responses were aligned with the analysis of the governance IEC 62443 and NIST SP 800-82, as described in the data analysis section of Chapter 4.

Finding 8: Performance Assessment

Performance assessment is a key finding derived from Theme 8 that emerged from the participants' responses. Analysis of 70% of the participants' responses showed that the role of corporate management is essential in establishing healthy organizational culture by promoting and endorsing cybersecurity governance as an intrinsic part of the corporate management system. Participants 01, 02, 03, 04, 05, and 11 noticed that the top management at some of the CPS/ICS-based industries operating on legacy systems have the mindset that production availability always has the priority over safety and security (including CPS and ICS cybersecurity) because production availability increases the company revenue while spending on safety and security increases the cost. From this perspective, those managers are unwilling to stop the production to patch their operating system or upgrade their legacy equipment, especially, these systems that have been working for decades. This cultural change issue can be solved by adopting a cybersecurity performance assessment program as part of the corporate management system, through which a plan for updating the legacy system can be mandated and assessed using smart key performance indicators. This finding conforms to CPS/ICS cybersecurity countermeasures (Dimitrov & Syarova, 2019; Pfrang et al., 2018) and also aligned with IEC 62443 and NIST SP 800-82.

Finding 9: Governance Mandate

The governance mandate is a crucial finding derived from Theme 9 that emerged from the participants' responses. Analysis of 14 interview transcripts (70% of the participants' responses) displayed more collaboration between the standardization firms and regulatory bodies on one side, and the CPS/ICS-based business owners and vendors on the other side could help enhance the quality and efficiency of governance against cyberattacks. Participant 02, who worked for one of the standardization firms, noted that it was difficult to get asset owners involved in the activities of standards and regulatory bodies. He thought that the asset owners tended to be less vocal because they are worried about the image of their companies, or they are concerned about the image of their own involvement in things. The solution to these issues (as concluded from the responses of Participants 01, 03, 04, 05, 07, 08, 09, 12, 13, and 14) lies in mandating incident reporting by the regulatory authorities.

A higher (nationwide) level of collaboration was proposed by Participant 01, who suggested that regulatory authorities should enforce CPS/ICS cybersecurity incident reporting and oblige all regulatory bodies from the individual member states to share incidents' experiences, cases, and threat intelligence across each other. He claimed that the right direction is to have nation-states recognize that cyberattacks on critical infrastructures can only be solved jointly, ideally upon an agreement to criminalize cyberattacks endorsed by the United Nations Security Council. Therefore, according to Participant 01, regulatory authorities, or bodies, need to establish interfaces among each other, regulatory bodies, and agencies with the necessary information and insight by motivating the entities that operate these infrastructures, not punishing them for reporting incidents, but by encouraging them to learn from each other. I perceive this suggestion as a constructive approach to impose incident reporting and knowledge sharing nationwide with the goal to tackle cybersecurity issues through a nationwide collaboration, which may result in better defenses against nation-state-sponsored cyberattacks.

Participant 03 proposed a stricter approach based on compliance audit and penalization. He stated that in Europe, one ICS legislation mandates that critical infrastructure needs to be cyber secure and obliges organizations to report cyber incidents to their respective governments. Participant 3 thought that this legislation was a good start to protect CPS-based infrastructures. Still, the regulatory authorities must start conducting audits to ensure this legislation is being implemented and impose fines for noncompliance with the requirements of that legislation. The peer-reviewed literature in Chapter 2 did not address international collaboration between nations as a way of preventing nation-state-sponsored cyberattacks. Therefore, this area might be a gap in the literature and an opportunity for further research.

Limitations of the Study

Cybersecurity governance, such as policies and standards, is a critical issue for organizations that struggle for success in protecting CPS-based assets from cyberattacks. The study results showed that good governance can provide only the primary defense line against cyberattacks. A full-fledged cybersecurity system depends on three pillars: people, process (governance), and technology. The first limitation to the trustworthiness of this study is that it focused only on one pillar of the cybersecurity system, which is CPS/ICS cybersecurity governance.

Clark et al. (2020) suggested that what constitutes successful cybersecurity governance and practices is unclear, partly because concluding an exact percentage measuring cybersecurity success is not simple. The second limitation lied in measuring the efficiency of the governance alone in protecting the CPS/ICS against cyberattacks. That is because many variables contribute to the success or failure of cybersecurity (e.g., employees' competencies, training, and the quality of the cybersecurity technologies used). Hence, sorting out a percentage measuring the contribution of the CPS/ICS governance alone to the success of cybersecurity in protecting CPS-based infrastructure could be inaccurate and doubtful. To overcome this limitation, quantifying the cybersecurity governance's efficiency against other variables was not considered part of this research's scope. Consequently, a quantitative design approach was not used for this study.

The third limitation of this study was that it focused on cybersecurity governance designed to protect CPS-based industries as a pillar of the IIoT, which evolved from the Industry 4.0 revolution. Hence, the result of this study may be of limited use to non-CPS-based organizations that do not use monitors, sensors, communication means, transmitters, actuators, and final actors for their processes. This limitation is not a sign of a low transferability of the results of this study, into which cybersecurity experts from 17 CPS/ICS-based industries shared their insights (see Table 8).

Recommendations

Recommendations for Action

I explored how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. The recommendations for actions presented in this section are derived from the research findings concluded from thematic analysis of semistructured interviews with 20 cybersecurity experts selected from worldwide cybersecurity-specialist groups on LinkedIn, analysis of the two predominant CPS/ICS cybersecurity governances (IEC 62443 and NIST SP 800-82), and the literature reviewed in Chapter 2. The recommendation for actions proposes what the corporate managements, standardization firms, and the regulatory bodies can do to strengthen the CPS/ICS cybersecurity governance.

Corporate management should promote, establish, and sustain a sound organizational cybersecurity culture through compliance with the best cybersecurity governance. This entails that corporate management endorses CPS/ICS cybersecurity practices as an intrinsic part of the corporate safety management system and allocates the budget and resources necessary to execute these practices, including training and awareness programs, access control technology utilization, and legacy systems replacement and upgrade. Corporate management should also set targets for the corporate cybersecurity program and key performance indicators to monitor the program's execution, follow up, and provide direction on critical issues, especially knowledge sharing and cybersecurity incident reporting. Corporate management must also establish and maintain collaboration dialogue with standardization firms and regulatory bodies, sharing their views and concerns about cybersecurity issues.

Standardization firms should liaise with the CPS/ICS-based organizations to understand their experiences and accordingly develop new industry-specific and simplify the current cybersecurity standards to a limit that is as low as reasonably practicable so that the organizations can implement them. Standardization firms should also liaise with the regulatory authorities on possible ways to mandate these standards and conduct compliance audits and impose progressive sanctions for non-compliance with those standards and regulations. Regulatory authorities should enforce CPS/ICS cybersecurity incident reporting and oblige all regulatory bodies from the individual member states to share incidents' experiences, cases, and threat intelligence across each other. The right direction is to have nation-states recognize that cyberattacks on critical infrastructures can only be solved jointly, ideally upon an agreement to criminalize cyberattacks endorsed by the United Nations Security Council.

Recommendation for Further Research

One of the limitations of this study was the inability to measure the efficiency of the governance alone in protecting the CPS/ICS from cyberattacks. That inability was logical because the efficiency of a typical cybersecurity defense system depends on three actors: people, process (governance), and technology. Since the current study focuses only on cybersecurity governance, measuring the efficiency of that actor alone (while disregarding the other two actors of the system) could result in biased results. Thus, a qualitative approach was chosen for the current study. Interested researchers may expand on the current study by conducting quantitative research to measure the contribution of each of the three actors (people, governance or process, and technology) to successful cyberattacks separately. Such a study would require root cause analyses of a reasonable number of reported incidents to associate each successful attack to a failure in one of the three actors, then quantify each actor's efficiency separately.

Implications

Positive Social Change

The CPS-based critical industries, including oil and gas, manufacturing, energy, utilities, chemical and petrochemical, allowed intelligent processing and increased supplies to large communities worldwide. The downside is that these infrastructures (due to their exposure to the internet) are subject to several kinds of cyberattacks, worst of which are nation-state-sponsored cyberattacks. The consequences vary depending on the motives of the attackers. Still, catastrophic consequences may include loss of lives, damage to critical assets, interruption of critical supplies to communities (such as electricity and water), environmental disasters such as emission of toxic substances and river and marine pollution, and interruption of critical supplies to communities.

This study has implications for positive social change by exploring how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS/ICS. The results of this study showed that adherence to good cybersecurity could serve as the primary defense line against cyberattacks on CPS/ICS-based industries. However, the efficiency of a typical cybersecurity defense system depends on two more actors: (a) people, and (b) technology, both of which can be managed by governance. This study could lead to a positive social change in the oil and gas industrial communities. For instance, governmental authorities' leaders, regulatory bodies, standardization firms, and corporate managers may use the recommendations for action provided in this study to explore concepts, tools, and techniques to use cybersecurity governance to avoid interruption of critical supplies for communities, such as electricity and water. The recommendations for action proposed in this study could also help increase awareness of cyber threats and protection measures to reduce the number of health and environmental incidents resulting from cyberattacks on CPS and subsequently improve the living conditions of the communities surrounding oil and gas fields and similar industries and services worldwide.

Methodological

As explained in Chapter 3, a qualitative, multiple-case study was a proper design for this study because it allows researchers to understand the phenomenon of study by analyzing and triangulating data from multiple resources, including governmental and corporate documents, archival data, and semi-structured interviews (see Yin, 2018). Data were gathered from multiple sources and were analyzed to help explore how cybersecurity governance can be used as security controls to prevent or mitigate the harmful consequences of cyberattacks on CPS-based infrastructures. The thematic analysis of semi-structured interviews with 20 cybersecurity professionals and the governances IEC 62443 and NIST SP 800–82 provided the nine theses presented in Chapter 4. From those nine themes, I concluded the study findings and recommendations for actions presented in this chapter. I performed triangulation of the CPS/ICS governance and the interview transcripts to increase the credibility and validity of the research findings and results.

Theoretical

By the use of RAT (Cohen & Felson, 1979) as a conceptual theory for this study, I was able to identify the three factors necessary for a successful cybercrime against CPS/ICS infrastructure: (a) CPS/ICS offenders and their motives, (b) vulnerable targets in the system, and (c) protection measures and protectors needed to prevent cyberattacks. Accordingly, I explored how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS, applying a qualitative, multiple-case study as described in Chapter 3. Interested researchers may use RAT as a conceptual theory for similar studies.

Practice

One of the essential gaps in the literature related to the safety and security of CPS was that the current CPS governances are not yet successful enough in protecting the CPS-based industries and services, including the oil and gas industry (see Asplund et al., 2018). The study results and the recommendations for action presented in this chapter provide detailed information about CPS/ICS vulnerabilities, offenders, and the effective use of governance as a primary defense against cyberattacks. The cybersecurity practitioners, scholars, policymakers, standardization and regulatory specialists, and corporate managers may use this study to understand better how to manage cyberattacks through enhancing CPS cybersecurity governance.

Empirical

The efficiency of a typical cybersecurity defense system depends on three actors: people, process (governance), and technology. Since the current study was focused only on governance, measuring the efficiency of that actor alone (while disregarding the other two actors of the system) could have resulted in biased results. Thus, a qualitative approach was chosen for the current study. This limitation offers interested researchers the opportunity to expand on the current study by conducting quantitative research to measure the contribution of each of the three actors (people, governance or process, and technology) to cyberattacks separately. Such a study entails conducting root cause analyses of a reasonable number of reported incidents to attribute each attack to a failure of one of the three actors, then quantify each actor's efficiency separately.

Conclusions

I used a qualitative, multiple-case study approach to explore how cybersecurity governance can be applied to develop controls that stop or mitigate the consequences of cyberattacks against the CPS in the oil and gas industry. The answer to this research question lies in the following recommendations for action that were evolved from the thematic data analysis: (1) corporate management to sponsor and endorse CPS/ICS cybersecurity practices as an intrinsic part of the corporate safety management system; (2) corporate management to set targets for the corporate cybersecurity program and key performance indicators to monitor the program's execution, follow up, and provide direction on critical issues, especially cybersecurity incident reporting; (3) corporate management to liaise with standardization firms and regulatory bodies, sharing their views about cybersecurity issues; (4) standardization firms to liaise with the CPS/ICS-based organizations on simplifying current standards to a reasonably practicable limit; (5) standardization firms to liaise with regulatory authorities on mandating their standards, conducting compliance audits, and imposing progressive sanctions for non-compliance; (6) regulatory authorities to enforce incident reporting and oblige regulatory bodies from member states to share incidents' experiences and threat intelligence across each other.

Interested researchers may expand on this study by conducting quantitative research to measure the contribution of each of the three actors comprising cybersecurity systems (people, governance, and technology) to cyberattacks separately. That requires root cause analyses of a reasonable number of reported incidents to attribute each attack to a failure of one of the three actors, then quantify each actor's efficiency separately.

References

Ab Rahman, N. H., Kessler, G. C., & Choo, K. K. (2017). Implications of emerging technologies to incident handling and digital forensic strategies: A routine activity theory. In *Contemporary digital forensic investigations of cloud and mobile applications* (pp. 131–146). Syngress. https://doi.org/10.1016/B978-0-12-805303-4.00009-5

Abdallah, A., & Shen, X. S. (2016, May). Efficient prevention technique for false data injection attack in smart grid. In *2016 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/icc.2016.7510610

Abdelghani, T. (2019). Implementation of defense in depth strategy to secure industrial control system in critical infrastructures. *American Journal of Artificial Intelligence*, *3*(2), 17–22. https://doi.org/10.11648/j.ajai.20190302.11

Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. *Quality Management: Tools, Methods, and Standards. Emerald Publishing Limited*, 245–264. https://doi.org/10.1108/978-1-78769-801-720191015

Ahmad, I., Zarrar, M. K., Saeed, T., & Rehman, S. (2018, April). Security aspects of cyber physical systems. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1–6). IEEE. https://doi.org/10.1109/cais.2018.8442009

Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: A review of cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications*, *9*(1), 499–508. http://doi.org/10.14569/IJACSA.2018.090169

Alexander, R. D., & Panguluri, S. (2017). Cybersecurity terminology and frameworks. In *Cyber-Physical Security* (pp. 19–47). Springer, Cham. https://doi.org/10.1007/978-3-319-32824-9_2

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1—8. https://doi.org/10.1016/j.comcom.2020.03.007

Allred, P. D., Maxwell, G. M., & Skrla, L. (2017). What women know: Perceptions of seven female superintendents. *Advancing Women in Leadership, 37*, 1–11. http://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1092&context=ed-facarticles

ANSI/ISA. (2013). *ANSI/ISA-62443-3-3 (99.03.03)-2013: Security for industrial automation and control systems Part 3-3: System security requirements and security levels*. United States of America: ISA, 2013. https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu

Asplund, F., McDermid, J., Oates, R., & Roberts, J. (2018). Rapid integration of CPS security and safety. *IEEE Embedded Systems Letters*, *11*(4), 111–114. http://doi.org/10.1109/LES.2018.2879631

ATLAS.ti. (n.d.). *All-in-one research software*. https://atlasti.com

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010

Boutwell, M. A. (2019). *Exploring industry cybersecurity strategy in protecting critical infrastructure* (Order No. 27735353). Dissertations & Theses @ Walden University. (2339173025). https://scholarworks.waldenu.edu/dissertations/7965

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the World Wide Web: A research note on social changes, online "places," and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice*, *32*(2), 129–147. https://doi.org/10.1177/1043986215621377

Cai, Y., Chen, Y., Li, Y., Cao, Y., & Zeng, X. (2018). Reliability analysis of cyber-physical systems: Case of the substation based on the IEC 61850 standard in China. *Energies*, *11*(10), 2589. https://doi.org/10.3390/en11102589

Cardenas, A., & Cruz, S. (2019). Cyber-physical systems security knowledge area. *The Cyber Security Body of Knowledge (cybok)*. https://www.cybok.org

Cardoso, C. L., Gontijo, L. A., & Ono, M. M. (2017). Affective memory: An ethnographic approach to design. *Strategic Design Research Journal*, *10*(1), 79–88. https://doi.org/10.4013/sdrj.2017.101.09

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds. *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019

Chen, Y., Kar, S., & Moura, J. M. (2015, April). Cyber-physical systems: Dynamic sensor attacks and strong observability. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1752–1756). IEEE. https://ieeexplore.ieee.org/abstract/document/7178271/

Chen, Y., Kar, S., & Moura, J. M. (2017). Dynamic attack detection in cyber-physical systems with side initial state information. *IEEE Transactions on Automatic Control*, *62*(9), 4618–4624. https://doi.org/10.1109/tac.2016.2626267

Clark, M., Espinosa, J., & Delone, W. (2020, January). Defending organizational assets: A preliminary framework for cybersecurity success and knowledge alignment. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*. http://hdl.handle.net/10125/64266

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org.ezp.waldenulibrary.org/10.2307/2094589

Dimitrov, W., & Syarova, S. (2019, November). Analysis of the functionalities of a shared ICS security operations center. In *2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE)* (pp. 1–6). IEEE. https://ieeexplore.ieee.org/abstract/document/9010607/

Ding, D., Han, Q. L., Ge, X., & Wang, J. (2020). Secure state estimation and control of cyber-physical systems: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. *51*(1), 176-190. https://doi.org/10.29007/z1sj

Dodgson, J. E. (2019). Reflexivity in qualitative research. *Journal of Human Lactation*, *35*(2), 220–222. https://doi.org/10.1177%2F0890334419830990

Falk, R., & Fries, S. (2020). Enhancing the resilience of cyber-physical systems by protecting the physical-world interface. *International Journal on Advances in Security, 13*(1&2), 54–65. http://72.52.166.99/articles/sec_v13_n12_2020_5.pdf

Fataliyev, T. K., & Mehdiyev, S. A. (2018). Analysis and new approaches to the solution of problems of operation of oil and gas complex as cyber-physical system. *International Journal of Information Technology and Computer Science (IJITCS)*, *10*(11), 67–76. https://doi.org/10.5815/ijitcs.2018.11.07

Feng, C., Palleti, V. R., Mathur, A., & Chana, D. (2019, February). A systematic framework to generate invariants for anomaly detection in industrial control systems. In *NDSS*. https://doi.org/10.14722/ndss.2019.23265

Flynn, S. V., & Korcuska, J. S. (2018). Credible phenomenological research: A mixed-methods study. *Counselor Education and Supervision*, *57*(1), 34–50 https://doi.org/10.1002/ceas.12092

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, *34*, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

Fujdiak, R., Mlynek, P., Blazek, P., Barabas, M., & Mrnustik, P. (2018, July). Seeking the relation between performance and security in modern systems: metrics and measures. In *2018 41st International Conference on Telecommunications and*

Signal Processing (TSP) (pp. 1–5). IEEE. https://doi.org/10.1109/tsp.2018.8441496

Ganesan, R., Mohan, P. V., Senthil, V. A., Surianarayanan, V., Boyina, S. X., & Veeraiyan, V. (2017). *U.S. patent application no. 14/924,980*. https://patents.google.com/patent/US20170125019A1/en

Ganji, D., Kalloniatis, C., Mouratidis, H., & Gheytassi, S. M. (2019). Approaches to develop and implement ISO/IEC 27001 standard information security management systems: A systematic literature review. *International Journal on Advances in Software Volume 12, Number 3 and 4, 2019*. http://www.iariajournals.org/software/

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Govindji, S., Peko, G., & Sundaram, D. (2017). A context adaptive framework for IT governance, risk, compliance and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication, 217*, 14–24. https://doi.org/10.1007/978-3-319-77818-1_2

Graham, J., Hieb, J., & Ralston, P. (2018). *Cybersecurity for industrial control systems: Progress and challenges*. ISCA, CAINE 2018, New Orleans, Louisiana, USA

Harada, Y. (2018). Laying the groundwork for testing routine activity theory at the microlevel using Japanese satellite positioning technology. In *Crime and Justice* *in Contemporary Japan* (pp. 137–151). Springer, Cham. https://doi.org/10.1007/978-3-319-69359-0_8

Hashemi, S., & Zarei, M. (2020). Internet of Things backdoors: Resource management issues, security challenges, and detection methods. *Transactions on Emerging Telecommunications Technologies*, e4142. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4142

Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. (2020). Analysis of cybersecurity-related incidents in the process industry. *Reliability Engineering & System Safety*, 107485. https://doi.org/10.1016/j.ress.2021.107485

International Electrotechnical Commission (IEC). (2013, March 13). *IEC TR 61850-1:2013: Communication networks and systems for power utility automation - Part 1: Introduction and overview*. IEC Webstore. https://webstore.iec.ch/publication/6007

International Electrotechnical Commission (IEC). (2018, January 23). *IEC TR 61511-0:2018: Functional safety - Safety instrumented systems for the process industry sector - Part 0: Functional safety for the process industry and IEC 61511*. IEC Webstore. https://webstore.iec.ch/publication/60766

International Electrotechnical Commission (IEC). (2020, June 16). *IEC TS 61850-1-2:2020: Communication networks and systems for power utility automation - Part 1-2: Guideline on extending IEC 61850*. IEC Webstore. https://webstore.iec.ch/publication/59652

International Electrotechnical Commission (IEC). (2021). *Safety and functional safety*. https://www.iec.ch/safety

ISA Global Cybersecurity Alliance (2019, January 8). United Nations commission to integrate ISA standards into cybersecurity regulatory framework. *Research Triangle Park, North Carolina*. https://www.isa.org/news-press-releases/2019/january/united-nations-commission-integrate-isa-standards

ISA Global Cybersecurity Alliance (n.d.). *Your guide to cybersecurity standards.* https://gca.isa.org/isagca-quick-start-guide-62443-standards

Issitt, M. (2020). General systems theory. *Salem Press Encyclopedia*.

Jillepalli, A. A., Sheldon, F. T., de Leon, D. C., Haney, M., & Abercrombie, R. K. (2017, June). Security management of cyber physical control systems using NIST SP 800-82r2. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1864–1870). IEEE. https://doi.org/10.1109/iwcmc.2017.7986568

Jindal, A., Schaeffer-Filho, A., Marnerides, A. K., Smith, P., Mauthe, A., & Granville, L. (2020, February). Tackling energy theft in smart grids through data-driven analysis. In *2020 International Conference on Computing, Networking and Communications (ICNC)* (pp. 410–414). IEEE. https://doi.org/10.1109/icnc47757.2020.9049793

Kalu, F. A., & Bwalya, J. C. (2017). What makes qualitative research good research? An exploratory analysis of critical elements. *International Journal of Social Science Research*, *5*(2), 43–56. https://doi.org/10.5296/ijssr.v5i2.10711

Kolisnyk, M., Kharchenko, V., & Piskachova, I. (2020, May). Availability models of industrial Internet of Things wired system considering cyberattacks. In *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 138–144). IEEE. https://doi.org/10.1109/dessert50317.2020.9125009

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Lamba, A. (2018). Protecting 'cybersecurity & resiliency' of nation's critical infrastructure–energy, oil & gas. *International Journal of Current Research*, *10*, 76865–76876. https://doi.org/10.2139/ssrn.3492694

Lamba, A. (2020). A thorough analysis on protecting cyber threats and attacks on CPS embedded subsystems. *Available at SSRN 3517474*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517474

Legatiuk, D., Theiler, M., Dragos, K., & Smarsly, K. (2017, September). A categorical approach towards metamodeling cyber-physical systems. In *Proceedings of the 11th International Workshop on Structural Health Monitoring (IWSHM). Stanford, CA, USA* (Vol. 9, No. 12, p. 2017). https://doi.org/10.12783/shm2017/13908

Liu, Z., Xie, K., Li, L., & Chen, Y. (2020). A paradigm of safety management in Industry 4.0. *Systems Research and Behavioral Science*, *37*(4), 632–645. https://doi.org/10.1002/sres.2706

Lu, Y. (2017). Cyber physical system (CPS)-based industry 4.0: A survey. *Journal of Industrial Integration and Management*, *2*(03), 1750014. https://doi.org/10.1142/S2424862217500142

Lyons, A. C., Um, J., & Sharifi, H. (2020). Product variety, customisation and business process performance: A mixed-methods approach to understanding their relationships. *International Journal of Production Economics*, *221*, 107469. https://doi.org/10.1016/j.ijpe.2019.08.004

Lyu, X., Ding, Y., & Yang, S. H. (2019). Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*, *4*(3), 221–232. https://doi.org/10.1049/iet-cps.2018.5068

Maestripieri, L. A. R. A., Radin, A., & Spina, E. (2019). Methods of sampling in qualitative health research. *Researching health: Qualitative, quantitative and mixed methods* (pp. 83–92). Sage.

Merien, T., Bellekens, X., Brosset, D., & Claramunt, C. (2018). A human-centered model for cyber attacks analysis. In *2018 2nd Cyber Security in Networking Conference (CSNet), France, 2018-10 - 2018 2nd Cyber Security in Networking Conference (CSNet) –2018*. http://hdl.handle.net/10985/15138

Min, B., & Varadharajan, V. (2014, September). Design and analysis of a new feature-distributed malware. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 457–464). IEEE. https://doi.org/10.1109/trustcom.2014.58

Min, B., & Varadharajan, V. (2015, December). Design and evaluation of feature distributed malware attacks against the Internet of Things (IoT). In *2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS)* (pp. 80–89). IEEE. https://doi.org/10.1109/iceccs.2015.19

Mlynek, P., Fujdiak, R., Mrnustik, P., Krena, B., & Apvrille, L. (2020). Co-engineering gap analysis of ANSI/ISA-62443-3-3. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, *9*(1), 1–9. http://dx.doi.org/10.11601/ijates.v9i1.285

Mo, Y., Garone, E., Casavola, A., & Sinopoli, B. (2010, December). False data injection attacks against state estimation in wireless sensor networks. In *49th IEEE Conference on Decision and Control (CDC)* (pp. 5967–5972). IEEE. https://doi.org/10.1109/cdc.2010.5718158

Nur, A. Y., & Tozal, M. E. (2016, May). Defending cyber-physical systems against dos attacks. In *2016 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 1–3). IEEE. https://doi.org/10.1109/smartcomp.2016.7501685

Nygaard, M., & Mukhopadyay, S. (2020). *Dragonstone strategy kickoff report* (No. LLNL-TR-805864). Lawrence Livermore National Lab. (LLNL), Livermore, CA (United States). https://doi.org/10.2172/1602649

Ogallo, G. G. (2018). *IoT*: *Enhancing data-driven decision-making in higher education*: *Case study of Ohio University* (Order No. 10954386). ProQuest Dissertations &

Theses Global. (2082274526). http://rave.ohiolink.edu/etdc/view?acc_num=ohiou1516193584144817

Onwuegbuzie, A. J., Frels, R. K., & Hwang, E. (2016). Mapping Saldana's coding methods onto the literature review process. *Journal of Educational Issues*, *2*(1), 130–150. http://dx.doi.org/10.5296/jei.v2i1.8931

Ose, S. O. (2016). Using Excel and Word to structure qualitative data. *Journal of Applied Social Science*, *10*(2), 147–162. https://doi.org/10.1177/1936724416664948

Parker, L. A. (2019). *Emotional intelligence: A descriptive study of how employees' describe the impact of leader emotional intelligence on the employees' performance* (Order No. 27672006). Available from ProQuest Dissertations & Theses Global. (2338533619).

Perrotta, C. (2017). Beyond rational choice: How teacher engagement with technology is mediated by culture and emotions. *Education and Information Technologies*, *22*(3), 789–804. https://doi.org/10.1007/s10639-015-9457-6

Pfrang, S., Meier, D., Friedrich, M., & Beyerer, J. (2018). Advancing protocol fuzzing for industrial automation and control systems. In *ICISSP* (pp. 570–580). https://doi.org/10.5220/0006755305700580

Potluri, S., Ahmed, S., & Diedrich, C. (2020). Securing industrial control systems from false data injection attacks with convolutional neural networks. In *Development and Analysis of Deep Learning Architectures* (pp. 197–222). Cham: Springer. https://doi.org/10.1007/978-3-030-31764-5_8

Prochazka, J., Novobisky, P., Prochazkova, D., Rusko, M., Kollar, V., Ferencz, V., ... & Majernik, S. (2020). Urban guided transport management cyber security. *Annals of DAAAM & Proceedings*, *7*(1). https://doi.org/10.2507/31st.daaam.proceedings.052

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies, 3*(9), 369–387. https://doi.org/10.4324/9780203095249-27

Recite Beta (2020). *Reference checking made easy*. Retrieved from http://www.reciteworks.com/

Ross, R. S., McEvilley, M., & Oren, J. C. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems [including updates as of 1-03-2018]* (No. Special Publication (NIST SP)-800-160). https://doi.org/10.6028/NIST.SP.800-160

Ruiz, A., Puelles, J., Martinez, J., Gruber, T., Matschnig, M., & Fischer, B. (2020, January). Preliminary safety and security co-engineering process in the industrial automation sector. In *10th European Congress on Embedded Real Time Software and Systems (ERTS 2020)*. https://hal.archives-ouvertes.fr/hal-02441744/

Sabaliauskaite, G., & Mathur, A. P. (2013, October). Intelligent checkers to improve attack detection in cyber physical systems. In *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 27–30). IEEE. https://doi.org/10.1109/cyberc.2013.14

Sabaliauskaite, G., & Mathur, A. P. (2014, July). Countermeasures to enhance cyber-physical system security and safety. In *2014 IEEE 38th International Computer Software and Applications Conference Workshops* (pp. 13–18). IEEE. https://doi.org/10.1109/compsacw.2014.6

Schaefer, L., & Mazerolle, L. (2017). Putting process into routine activity theory: Variations in the control of crime opportunities. *Security Journal*, *30*(1), 266–289. https://doi.org/10.1057/sj.2015.39

Schwab, W., & Poujol, M. (2018). The state of industrial cybersecurity 2018. *Trend Study Kaspersky Reports*, 33. https://www.engineersonline.nl/download/2018-Kaspersky-ICS-Whitepaper.pdf

Shaik, F., Abdullah, A., & Klein, S. (2017, January). Digital transformation in oil & gas-cyber security and approach to safeguard your business. In *22nd World Petroleum Congress*. World Petroleum Congress. https://www.onepetro.org/conference-paper/WPC-22-2555

Sharma, G. (2017). Pros and cons of different sampling techniques. *International journal of applied research*, *3*(7), 749–752.

Shen, G., Wang, W., Mu, Q., Pu, Y., Qin, Y., & Yu, M. (2020). Data-driven cybersecurity knowledge graph construction for industrial control system security. *Wireless Communications and Mobile Computing*, *2020*. https://doi.org/10.1155/2020/8883696

Sidhu, K., Jones, R., & Stevenson, F. (2017). Publishing qualitative research in medical journals. *British Journal of General Practise, 67*(658), 229–230.

https://doi.org/10.3399/bjgp17x690821

Slowik, J. (2019). Evolution of ICS attacks and the prospects for future disruptive events. *Threat Intelligence Centre Dragos Inc*. https://www.dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf

Solesvik, M. Z. (2017). Hybrid entrepreneurship: how and why entrepreneurs combine employment with self-employment. *Technology Innovation Management Review*, *7*(3). https://doi.org/10.22215/timreview1063

Song, L., & Zhang, L. (2019, October). Comparative analysis of geomechanics and general system theory, earth system science and geomechanics' unique advantages in comprehensive survey of natural resources. In *Journal of Physics: Conference Series* (Vol. 1325, No. 1, p. 012193). IOP Publishing. https://doi.org/10.1088/1742-6596/1325/1/012193

Sonix (n.d.). *The best automated transcription software powered by cutting-edge AI*. https://sonix.ai/features

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Stouffer, K., Pilliteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *NIST special publication 800-82 rev 2: Guide to industrial control systems (ICS) security*. *National Institute of Standards and Technology (NIST)*, U.S. Department of Commerce. http://dx.doi.org/10.6028/NIST.SP.800-82r2

Syed, D., Chang, T. H., Svetinovic, D., Rahwan, T., & Aung, Z. (2017, July). *Security for complex cyber-physical and industrial control systems: Current trends, limitations, and challenges*. In *PACIS* (p. 180). http://aisel.aisnet.org/pacis2017/180

Tripwire, I. (2016). Tripwire study: Cyber attackers successfully targeting oil and gas industry. *Business Wire (English)*. http://www.businesswire.com/news/home/20160114005008/en/

Tyler, L. B. (2018). *Exploring the implementation of cloud security to minimize electronic health records cyberattacks* (Order No. 10815799). Available from Dissertations & Theses @ Walden University. (2042344862). https://scholarworks.waldenu.edu/dissertations/5281

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0–a glimpse. *Procedia Manufacturing*, *20*, 233–238. https://doi.org/10.1016/j.promfg.2018.02.034

Vardi, M. Y. (2017). Cyber insecurity and cyber libertarianism. *Communications of the ACM, 60*(5), 5. https://doi.org/10.1145/3073731

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: a review. *International Journal of Energy Economics and Policy, 7*(5), 250–262. https://ideas.repec.org/a/eco/journ2/2017-05-28.html

Wanasinghe, T. R., Wroblewski, L., Petersen, B., Gosine, R. G., James, L. A., De Silva, O., ... & Warrian, P. J. (2020). Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges. *IEEE Access*. https://doi.org/10.1109/access.2020.2998723

Wei, J. & Mendis, G. J. (2016, April). A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. In *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids* (CPSR-SG) (pp. 1–6). IEEE. https://ieeexplore.ieee.org/abstracct/document/7684102/

Winther, T. (2015, November 30). *DNV GL reveals top ten cyber security vulnerabilities for the oil and gas industry*. https://www.dnvgl.com/news/dnv-gl-reveals-top-ten-cyber-security-vulnerabilities-for-the-oil-and-gas-industry-48532

Wurm, J., Jin, Y., Liu, Y., Hu, S., Heffner, K., Rahman, F., & Tehranipoor, M. (2016). Introduction to cyber-physical system security: A cross-layer perspective. *IEEE Transactions on Multi-Scale Computing Systems*, *3*(3), 215–227. https://doi.org/10.1109/CPSRSG.2016.7684102

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*. https://doi.org/10.1016/j.micpro.2020.103201

Yin, R. K. (2018). *Case study research: Design and methods* (6th Ed.). Thousand Oaks, CA: Sage.

Yoo, H., & Shon, T. (2016). Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. *Future generation computer systems*, *61*, 128–136. https://doi.org/10.1016/j.future.2015.09.026

You, Y., Lee, J., Oh, J., & Lee, K. (2018, January). A review of cyber security controls from an ICS perspective. In *2018 International Conference on Platform Technology and Service (PlatCon)* (pp. 1–6). IEEE. https://doi.org/10.1109/platcon.2018.8472757

Zhang, X. M., Han, Q. L., Ge, X., Ding, D., Ding, L., Yue, D., & Peng, C. (2019). Networked control systems: a survey of trends and techniques. *IEEE/CAA Journal of Automatica Sinica*, *7*(1), 1–17. http://doi.org/10.1109/JAS.2019.1911651

Zhang, X., Liu, J., Zhao, D., Chong, T., & Zhang, H. (2020, October). Research of CPU Functional Safety Based on IEC 61508. In *Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacture* (pp. 440–444). https://doi.org/10.1145/3421766.3421782

Appendix A: List of Interview Questions

Introductory Question: Please specify how many years of Cyber-Physical Systems (CPS)/Industrial Control Systems (ICS) cybersecurity experience do you have, and with which type of CPS/ICS-based industry?

Knowledge Area	Interview Questions
CPS Detection System	1. What critical system failure may occur due to cyberattacks on CPS and ICS?
Existing CPS Cybersecurity Governance	2. What policies, standards, procedures, and best practices are endorsed to provide safety and security for the CPS and ICS?
The Efficiency of CPS Policies and Standards	3. What type of cyberattacks can the proper application of policies, standards, procedures, and best practices prevent or mitigate? 4. What are the types of cyberattacks that the proper application of policies, standards, procedures, and best practices cannot prevent or mitigate?
CPS Vulnerability	5. Why CPS and ICS are subject to cyberattacks?
CPS Security Improvement	6. What type of equipment upgrade, software, and governance would help enhance CPS and ICS safety and security?
Role of Corporate Management	7. How effective are organizational practices such as training, knowledge management, and incident reporting about various cyberattacks in identifying threats and developing standards or procedures to strengthen the CPS and ICS safety and security systems? 8. How do you describe corporate management's role in establishing and sustaining the CPS and ICS safety and security systems?
Role of Standardization and Regulatory Bodies	9. What can the industrial community, especially the standardization and regulatory bodies, do to strengthen the CPS and ICS safety and security systems?

Appendix B: Interview Invitation Email

Dear [I will enter the invitee's name here],

I hope this message finds you well.

I am a Ph.D. student at Walden University. As part of my research project, I am conducting Zoom interviews to explore how the cybersecurity governance (policies and standards) can help prevent or mitigate the consequences of cyberattacks against cyber-physical systems (CPS). I am seeking cybersecurity professionals with a minimum of 10 years' experience to contribute to the study.

The interview should take no more than 45 minutes of your time. I am trying to apprehend your perspectives on using cybersecurity governance for protecting CPS against cyberattacks. Your identity and answers to the interview questions will be kept confidential. The privacy of interviewees will be retained by using codes instead of actual names.

There is no compensation for participating in this study. However, your participation will add value to my research. The research findings could lead to a better understanding of using cybersecurity governance as controls to secure societal CPS-based infrastructure and services.

Please advise a day and time that suits you, and I will do my best to meet your availability. If you have any questions, please do not hesitate to contact me either via phone at XXX or via email at XXX@waldenu.edu.

Appendix C: Introductory Notes

Thank you so much for sparing part of your valuable time for this interview. I appreciate the time commitment and will try to make this interview a good use of your time. As you know, the purpose of this interview is to talk about your experience with using cybersecurity governance as CPS cybersecurity controls. This interview should not take more than 45 minutes. You can stop this interview at any time if you choose to. Your personal information will be protected. All information that would allow someone to identify you will entirely be removed from all documentation.

Also, I would like to let you know that the interview will be audio-recorded, but I can stop or delete the recording if you want. After the interview, I will be transcribing and analyzing your answers. I will email you my transcript to correct me if I misinterpret any of your responses.

Before we proceed to the interview, do you have any questions? Are you ready to start?

Appendix D: Closing Notes

Thank you so much for your valuable time and the insights you have kindly provided about the role of cybersecurity governance in protecting CPS/ICS from cyberattacks.

In covering the subject, did I miss anything?

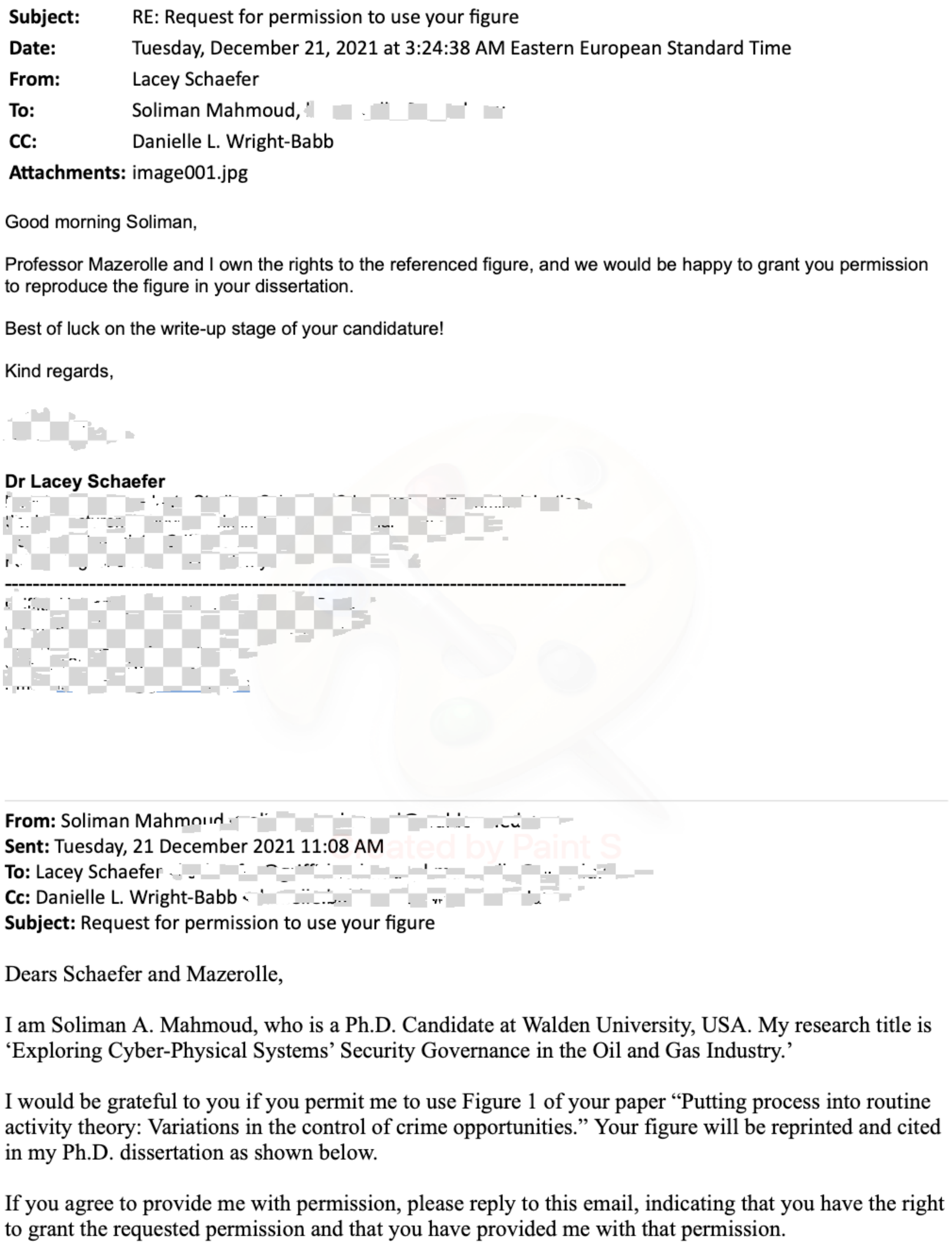
Do you have more information to share?

Do you have any questions for me?

Following this interview, I will analyze your answers against the information I concluded from the review of the literature and existing CPS/ICS cybersecurity governance. The aim is to find specific themes and ideas to help answer the research question and supplemental interview questions. This process may take around six weeks; then, I may revert to you to share my conclusions to ensure that your answers are not unintentionally misinterpreted. Would that be ok with you?

Once again, thank you so much for offering your time and sharing your valuable knowledge of the subject of study. If you have any questions, please do not hesitate to contact me at any time.

Appendix E: Permission to Use Figure 1



Subject: RE: Request for permission to use your figure
Date: Tuesday, December 21, 2021 at 3:24:38 AM Eastern European Standard Time
From: Lacey Schaefer
To: Soliman Mahmoud, [redacted]
CC: Danielle L. Wright-Babb
Attachments: image001.jpg

Good morning Soliman,

Professor Mazerolle and I own the rights to the referenced figure, and we would be happy to grant you permission to reproduce the figure in your dissertation.

Best of luck on the write-up stage of your candidature!

Kind regards,

[redacted]

Dr Lacey Schaefer
[redacted]

[redacted]

From: Soliman Mahmoud [redacted]
Sent: Tuesday, 21 December 2021 11:08 AM
To: Lacey Schaefer [redacted]
Cc: Danielle L. Wright-Babb [redacted]
Subject: Request for permission to use your figure

Dears Schaefer and Mazerolle,

I am Soliman A. Mahmoud, who is a Ph.D. Candidate at Walden University, USA. My research title is 'Exploring Cyber-Physical Systems' Security Governance in the Oil and Gas Industry.'

I would be grateful to you if you permit me to use Figure 1 of your paper "Putting process into routine activity theory: Variations in the control of crime opportunities." Your figure will be reprinted and cited in my Ph.D. dissertation as shown below.

If you agree to provide me with permission, please reply to this email, indicating that you have the right to grant the requested permission and that you have provided me with that permission.