2021

# Strategies for Implementing Internet of Things Devices in Manufacturing Environments

Todd Efrain Hernandez
*Walden University*

# Walden University

College of Management and Technology

This is to certify that the doctoral study by

Todd Hernandez

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. Steven Case, Committee Chairperson, Information Technology Faculty
Dr. Gary Griffith, Committee Member, Information Technology Faculty
Dr. Joline Burchell, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Strategies for Implementing Internet of Things Devices in Manufacturing Environments

by

Todd Efrain Hernandez

MS, Keller Graduate School of Management, 2013

BS, DeVry Institutes of Technology, 1992

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2021

## Abstract

The Internet of Things (IoT) has been exploited as a threat vector for cyberattacks in manufacturing environments. Manufacturing industry leaders are concerned with cyberattacks because of the associated costs of damages and lost production for their organizations. Grounded in the general systems theory, the purpose of this multiple case study was to explore strategies electrical controls engineers use to implement secure IoT devices in manufacturing environments. The study participants were eight electrical controls engineers working in three separate manufacturing facilities located in the Midwest region of the United States. The data were collected by semistructured interviews and 15 organizational documents. Data were analyzed using methodological triangulation to identify codes and themes. Four themes emerged: (a) a collaborative work environment, (b) employ existing cybersecurity practices, (c) adequate resources must exist to maintain security, and (d) learning and education. One recommendation for controls engineers is to embrace life-long learning, as technology is ever-changing. The implications for positive social change include the potential to improve manufacturing efficiencies and profits, thereby enhancing community support by manufacturing companies and increased wages and benefits for their employees.

# Strategies for Implementing Internet of Things Devices in Manufacturing Environments

by

Todd Efrain Hernandez

MS, Keller Graduate School of Management, 2013

BS, DeVry Institutes of Technology, 1992

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2021

# Dedication

I dedicate this work to my two children, Alison and Caleb. Continue to forge your own paths knowing that I love and support you. You are limited only by your own imagination.

# Acknowledgments

I acknowledge and thank all of the following people:

My wife and children, Lorrie, Alison, and Caleb for the patience and understanding you all demonstrated throughout my doctoral journey. Dr. Steven Case, for guidance and encouragement, without which I would never have been able to complete this work. Finally, to all of my peers in Higher Education that have committed themselves to the betterment of individuals and society as a whole.

Table of Contents

List of Tables....iv

Section 1: Foundation of the Study....1

Background of the Problem....1

Problem Statement....2

Purpose Statement....2

Nature of the Study....3

Research Question....4

Interview/Survey Questions....4

Conceptual Framework....5

Definition of Terms....6

Assumptions, Limitations, and Delimitations....6

Assumptions....7

Limitations....7

Delimitations....7

Significance of the Study....8

Contribution to IT Practice....8

Implications for Social Change....9

A Review of the Professional and Academic Literature....9

GST 10

Analysis of Similar Theories....15

Analysis of Contrasting Theories....19

Critical Analysis of Potential Themes and Phenomena ..... 22
Holistic IoT Security ..... 22
Manufacturing Environments ..... 30
Relationship of This Study to Previous Research ..... 34
Transition and Summary ..... 36
Section 2: The Project ..... 37
Purpose Statement ..... 37
Role of the Researcher ..... 37
Participants ..... 39
Research Method and Design ..... 41
Method ..... 41
Research Design ..... 43
Population and Sampling ..... 45
Ethical Research ..... 47
Data Collection ..... 48
Instruments ..... 48
Data Collection Technique ..... 50
Data Organization Techniques ..... 52
Data Analysis Technique ..... 53
Reliability and Validity ..... 55
Dependability ..... 55
Credibility ..... 56

Transferability....57
Confirmability....57
Transition and Summary....58
Section 3: Application to Professional Practice and Implications for Change....59
Overview of Study....59
Presentation of the Findings....60
Theme 1: A Collaborative Work Environment....60
Theme 2: Employ Existing Cybersecurity Practices....65
Theme 3: Adequate Resources Must Exist to Maintain Security.....69
Theme 4: Learning and Education....73
Applications to Professional Practice....77
Implications for Social Change....78
Recommendations for Action....79
Recommendations for Further Study....80
Reflections....81
Summary and Study Conclusions....82
References....84
Appendix A: Interview Protocol....112
Appendix B: Document Collection Protocol....114
Appendix C: Training Certificate From the National Institute of Health Office of Extramural Research....115

List of Tables

**Table 1** *References to a Collaborative Work Environment*.....61

**Table 2** *References to Employ Existing Cybersecurity Practices*.....66

**Table 3** *References to Adequate Resources Must Exist* .....70

**Table 4** *References to Learning and Education* .....73

# Section 1: Foundation of the Study

The manufacturing sector is a popular target for cyberattacks. Manufacturing environments have many unique cybersecurity challenges, as does the Internet of Things (IoT). As manufacturers move towards Industry 4.0 and Smart Factories, they have begun implementing IoT in their environments. The introduction of IoT in manufacturing environments may enhance existing cybersecurity challenges as well as introduce new challenges.

## Background of the Problem

Security vulnerabilities introduced by IoT should not be ignored. IoT introduces various security and privacy challenges, including new threat vectors that can be exploited due to poorly configured or faulty devices (Sivabalan & Radcliffe, 2017). IoT has already been exploited to disable a uranium enrichment plant in Iran (Slayton, 2016) and take down electricity in Ukraine for 6 hours (Sullivan & Kamensky, 2017). The number of cyberattacks geared at industrial environments is likely to increase.

In manufacturing environments, electrical controls engineers are the practitioners that implement IoT devices. Unfortunately, electrical controls engineers may not be classically trained in information security. Additionally, their focus is drawn towards keeping systems operational and recovering from downtime as quickly and efficiently as possible. This mantra often leads them to leave default configurations, a security risk. Successful cyberattacks in manufacturing environments may lead to production downtime, equipment damage, or personnel injury. This study identified strategies that

electrical controls engineers use to securely implement IoT in manufacturing environments.

## Problem Statement

As manufacturers become more reliant on IoT devices, their risk of cyberattacks also increases (Jang-Jaccard & Nepal, 2014). The number of installed IoT devices is expected to grow to approximately 25 billion by 2020, and much of this growth will be in the manufacturing sector (Bi et al., 2014; Farooq et al., 2015). The general information technology (IT) problem is that some manufacturing facilities are experiencing an increase in security breaches due to the use of IoT devices in their environments. The specific IT problem is that some electrical controls engineers lack strategies to securely implement IoT devices in manufacturing environments.

## Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies that electrical controls engineers used to securely implement IoT devices in manufacturing environments. The specific population included electrical controls engineers of three manufacturing facilities in the Midwest region of the United States who have strategies to securely implement IoT devices. The completed study may contribute to positive social change by enhancing the safety of production personnel and manufacturing equipment as strategies to securely implement IoT devices in manufacturing environments have been identified.

## Nature of the Study

A qualitative research method was chosen for this study as it most appropriately addresses the research purpose to explore strategies that electrical controls engineers use to securely implement IoT devices in manufacturing environments. Qualitative research methods allow researchers to explore a phenomenon and gain a more in-depth understanding of the topic (Bristowe et al., 2015). I chose the qualitative method to explore and understand the key strategies to securely implement IoT devices in manufacturing environments. A quantitative design is utilized to examine relationships between variables and test hypotheses (Trochim & Donnelly, 2008). Examining relationships among variables was not the purpose of this study, so a quantitative design was not applicable. Mixed methods research includes both quantitative and qualitative analysis to develop completeness (Leedy & Ormrod, 2015). A mixed-methods approach was not appropriate because the quantitative analysis would not significantly contribute to answering the research question. Qualitative research methods are most appropriate because strategy identification implies an in-depth understanding of technical, organizational, budgetary, and other dimensions of the problem that a brief survey would not capture.

I considered using case study, phenomenological, and ethnographic designs for this study; I selected a case study design. According to Yin (2013), exploratory case study designs allow the researcher to gain an in-depth understanding of a specific problem and explore a phenomenon within time and location parameters. A case study was appropriate because it allowed exploration of strategies within the context of

individual organizations to gain an in-depth understanding of technical, organizational, budgetary, and other dimensions of the problem. Phenomenological designs are appropriate for a researcher to describe the essence of experiences (Gill, 2014). However, describing the essence of the participants' experience was not the purpose of this study, so a phenomenological design was not relevant. Ethnography is the study of a group or culture where a researcher immerses themselves in the population's environment to understand its behavior (Small et al., 2014). Ethnography was not appropriate for this study because understanding the participant's behavior was not the research question's intended focus. In reviewing the possible designs, I determined that a case study was most appropriate for the study and best answered the research question.

## Research Question

Data from this research provides strategies that electrical controls engineers can use to securely implement IoT devices in manufacturing environments. The overarching research question that guided this study was as follows: What strategies do electrical controls engineers use to securely implement IoT devices in manufacturing environments?

## Interview/Survey Questions

1. What strategies have you used to securely implement IoT devices in your manufacturing environment?
2. Which of those strategies worked well, and why?
3. What issues or problems did you encounter?

4. How do you assess the effectiveness of the strategies used to securely implement IoT devices in your manufacturing environment?
5. How do the strategies fit or interact with other parts of the manufacturing environment?
6. What else would you like to add that might apply to the strategies you have used to securely implement IoT devices?

## Conceptual Framework

For this study, I used general systems theory (GST) as a conceptual framework. GST was first conceptualized in 1937 by von Bertalanffy (von Bertalanffy, 1972). The theory was refined in 1949 and again in 1972 (Drack & Schwarz, 2010). The foundational concept of systems theory is the whole system itself (Hammond, 2010; von Bertalanffy, 1972). Consequently, the theory's premise is human beings, social interaction, and technology working together to achieve the organism's objectives (von Bertalanffy, 1972). Von Bertalanffy's work has been expanded to explain that systems include inputs and outputs that work together to achieve the system's overall objectives (von Bertalanffy et al., 2008). A system is complete when all system mechanisms are working correctly (Hammond, 2010).

I used GST as the lens for exploring strategies for securely implementing IoT devices in manufacturing environments. The concepts of GST are as follows: (a) hierarchical structures should exist in all systems; (b) all systems have distinct boundaries; (c) all systems have interfaces to the bigger system; (d) a system is defined as a whole; and (e) all systems communicate with themselves via a feedback loop (von

Bertalanffy, 1972). GST aligns well with manufacturing environments because such environments comprise a hierarchical system of systems with distinct boundaries that interface with larger systems and contain feedback loops for communication. I used the theory to explore security within manufacturing environments, including different hierarchical levels, system boundaries, system interfaces, and the system as a whole. I used GST as the viewpoint from which to understand strategies that electrical controls engineers use to securely implement IoT devices in manufacturing environments.

## Definition of Terms

*Cyber-physical system*: a system that links the virtual world of IT and software to the physical world (Mourtzis et al., 2016).

*Industrial IoT*: the use of IoT devices in industrial environments to continuously capture information from various sensors and objects with the motivation to improve manufacturing systems (D. Zhang et al., 2016).

*Industry 4.0*: the fourth stage of industrialization brought forth by the proliferation of cyber-physical systems (D. Zhang et al., 2016).

*Internet of Things (IoT)*: the worldwide network of connected objects or devices where each device is uniquely addressed and uses standard protocols for communications to collect and process data (Bandyopadhyay & Sen, 2011; Barnaghi et al., 2012).

## Assumptions, Limitations, and Delimitations

Many different internal or external factors may influence research and outcomes. This section contains details on three items that have been considered for this study: (a)

assumptions, (b) limitations, and (c) delimitation. The following sections identify three assumptions, two limitations, and three delimiters that exist for this study.

## Assumptions

There are several assumptions associated with this study. An assumption is taking something for granted that has not been theoretically proven (Schoenung & Dikova, 2016). The first assumption for this study was that the cases chosen adequately represented the overall industry. The second was that the number of cases and interviews conducted was enough to achieve quality. Third, I assumed that the participants were knowledgeable of the research topic and provided informative answers to the interview questions.

## Limitations

This study has limitations that should be acknowledged. A limitation is an inherent facet of the study that is out of the researcher's control (Moore et al., 2015). Data analysis in qualitative case study design is subjective (Yin, 2014). A limitation inherent to this study is the subjective nature of data analysis in qualitative case study design. Generalization is another limitation of qualitative case study design due to a limited number of cases (Yin, 2014). This study was limited to three cases and was subject to a generalization limitation.

## Delimitations

Just as I considered assumptions and limitations for this study, I also considered delimitations. Delimitations are aspects of a study within the control of the researcher and are implemented to limit the scope and create boundaries for a study (Rosenberg &

Koehler, 2015). The first delimiter was the selection of manufacturing facilities located within the Midwest region of the United States. A second was that the participants all had current responsibilities in a manufacturing environment and had at least 5 years of experience as electrical control engineers. The final delimiter is that only three cases were studied.

## Significance of the Study

While reviewing the academic literature, I identified studies related to IoT and studies related to manufacturing environments; however, I did not find any studies specifically related to electrical controls engineers' strategies to securely implement IoT devices in manufacturing environments. The following sections contain further information regarding the significance of this study.

### Contribution to IT Practice

Production downtime is one of the costliest events in a manufacturing environment (Liu et al., 2012). Poor or insecure implementation of IoT devices in manufacturing environments can lead to significant production downtime. Additionally, if implemented improperly, IoT devices in manufacturing environments may jeopardize the safety of production personnel and manufacturing equipment. This study identified strategies necessary to securely implement IoT devices. Electrical controls engineers might utilize these strategies in their manufacturing environment to ensure that IoT devices are secure.

## Implications for Social Change

The study promotes positive social change as it identified strategies to securely implement IoT devices in manufacturing environments. Presumably, IoT devices are only used to create efficiencies, thereby creating savings in the manufacturing process. If manufacturing costs decline and profits increase, socially responsible manufacturers will provide increased wages and benefits to their employees. When employees have increased spending power, economic growth occurs.

## A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore strategies that electrical controls engineers use to securely implement IoT devices in manufacturing environments. The research question provided a focus for the literary search. I chose GST as the conceptual framework; however, I also explored and considered system dynamics, complexity theory, security risk planning model, technology acceptance model, and diffusion of innovation. In addition to theories, I reviewed literature pertaining to or related to information security, IoT, and manufacturing environments. There are many examples of these topics contained in the literature.

In total, I considered 169 articles for review, of which 117 articles are included in the literature review. Of the referenced articles, 106 (91%) are peer reviewed as verified by a search of Ulrich's database. Ninety-four (80%) of the articles included in the literature were published in 2015 or later. The primary search tools used to find the articles were Google Scholar and the Walden University Library's Thoreau. I used

Boolean logic to employ multiple keywords in the database searches. Search terms used included the following:

- general systems theory OR gst
- general systems theory AND (Internet of things or IoT)
- IoT AND (information security OR cybersecurity)
- IoT AND (cyber-physical system)
- IoT AND (industrial control system OR SCADA)

**GST**

I selected GST as the conceptual framework for this study. GST is the study of a phenomenon from a perspective of wholeness (von Bertalanffy, 1972). Before GST, scientists broke systems into their most elemental units and studied those units individually; the purpose of this type of research is often an attempt to identify causal relationships between variables (von Bertalanffy, 1972). In this research method, scholars failed to identify more significant problems that arose due to the interrelations of many variables (von Bertalanffy, 1972). GST offers a framework for performing research on a phenomenon at a broader systems level.

Systems can be broadly identified in many ways. In GST, a system is defined "as a set of elements standing in interrelations" (von Bertalanffy, 1972, p. 55). Some systems can be easily observed in the real world (von Bertalanffy, 1972). Systems can be abstract as well (von Bertalanffy, 1972). Systems may be open or closed; however, regardless of the type, all systems reach an equilibrium state where each system's piece is performing its function (von Bertalanffy, 1972). Systems are hierarchal in construction, with each

system being a subsystem of a more extensive system where interfaces between systems exist (von Bertalanffy, 1972). Every system has distinct boundaries (von Bertalanffy, 1972). Systems have feedback mechanisms that drive the system's behavior (von Bertalanffy, 1972). Given these characteristics and attributes of systems, nearly any phenomenon can be classified and studied as a system. Also, when all components of a system are functioning properly with appropriate feedback, the system operates efficiently. The next section contains information about the application of GST in research.

### *The Application of GST in Research*

There is some debate in the literature about the extent and value of applying GST in information systems research. Demetis and Lee (2016) proposed that GST has largely been ignored by information systems researchers and has lessened the domain compared to other fields of study. Robey and Abdalla Mikhaeil (2016) agreed that GST itself has not been prevalent in information systems research, due in part to information systems not being in existence when GST was postulated. Robey and Abdalla Mikhaeil diverged from Demetis and Lee's views about GST's value and the complete absence of GST in information systems research. Robey and Abdalla Mikhaeil argued that GST is too abstract and complicated for information systems research but that GST exists in information research through other theories that have spawned from GST, such as the structuration theory (Orlikowski & Robey, 1991) and the complexity theory. Mingers (2017) agreed that GST has produced other theories, and these offshoot theories have applicability to information systems research. Schultze (2017) furthers the conversation

in stating that systems theory is unlikely to advance information systems because of its vertical hierarchical organization and horizontal input-output processes. Broks (2016) noted that GST is necessary and a good cognitive theory to solve theoretical problems, but theories branched from GST are necessary to solve modern problems. A main counterpoint to these claims is that systems theory concepts have informed mathematics, biology, law, chemistry, social sciences, etc., and such is likely to enhance information systems (Demetis & Lee, 2017). Regardless of arguments to the contrary, there are many examples in the literature where GST has been successfully applied in research to study both technical and nontechnical phenomena.

Scholars have used GST to study information security and other technical phenomena. Haimes et al. (2015) applied GST to cloud computing technology (CCT) systems. By viewing CCT as a complex system of systems, Haimes et al. used advanced systems engineering techniques to propose a fault tree for a mini CCT that improved cybersecurity posture for the CCT. Y. Wang et al. (2015) employed GST and modeled IT management, IT assets, and organization as systems and subsystems. Y. Wang et al. concluded that IT management and the interaction between IT management and IT assets positively impact firm performance. Oesterreich and Teuteberg (2018) modeled a building information management (BIM) program as a system by including organization departments, customers, and suppliers to better understand the true costs and benefits of using a BIM. Oesterreich and Teuteberg built a simulation that concluded that profits improve after year one of implementing a BIM for the stated scenario. The awareness boundary model, first presented by Rasmussen (1997), provides a broad model that can

be applied to various domains (Allam et al., 2014). Allam et al. (2014) adapted the awareness boundary model using GST to add a feedback loop to create an adapted awareness model that can improve smartphone users' information security awareness. Based on these and other studies found in the literature, GST is an effective framework for studying various technical phenomena.

GST is not only used as a theory to analyze technical phenomenon; it is also used by scholars in many different fields. Vargo et al. (2017) argued that markets should be viewed as systems to be understood as a whole. Vargo et al. modeled markets as systems that allowed them to shift from viewing markets as a collection of buyers and sellers to a view that includes relationships, processes, and mapping. Wallace (2016), who created systems for patients near the end of life, healthcare providers, insurance companies, and families, proposed a program model for overcoming barriers to end-of-life healthcare. Bridgen (2017), who applied GST to study academic advising at several universities, concluded that misconceptions about the purpose and process of advising existed between staff, students, and faculty and proposed that university administrators might build a more robust advising structure if they used systems theory to develop the model. Von Der Tann et al. (2016) noted that systems theory has been used to study urban areas and postulate that the application of system thinking and methodologies could lead to a better understanding and categorization of the urban subsurface. Given the examples provided, GST is a versatile framework that can help study a wide variety of problems in different domains, including strategies to securely implement IoT devices in a manufacturing environment.

### *GST, Manufacturing, and IoT*

Scholars have employed GST to study phenomena related specifically to manufacturing. Eyers and Potter (2017) identified manufacturing as a system of systems that resides within organizational systems; systems thinking regarding manufacturing is well represented in academic literature. GST, coupled with graph and chaos theories, has been applied to study industrial sector data to create a method of data analysis that organizations can use to identify causal relationships in their organizations to foster improvement (Lloret-Climent et al., 2019). In part, Shin and Konrad (2017) used the GST tenets of wholeness, feedback, inputs, and outputs to validate a positive causal relationship between high-performing work systems and performance in Canada's manufacturing and service sectors. Pasman et al. (2013) relied on holism to describe complexities and barriers to safety in manufacturing plants. GST is often coupled with other established theories to research phenomena related to manufacturing and IoT (Lloret-Climent et al., 2019; Ng & Wakenshaw, 2017; Shin & Konrad, 2017). GST is a practical theory for studying problems in manufacturing. Scholars have also used GST to describe phenomena related to IoT and other related technologies.

Academic literature contains examples of the use of GST to study IoT and supervisory control and data acquisition (SCADA) systems. GST's holism and feedback artifacts have been used to inform a proposed cybersecurity framework for SCADA systems (Nazir et al., 2017). The IoT has been described as ever-evolving, and the use of systems theory is a useful conceptualization for future research on IoT (NG & Wakenshaw, 2017). Holism is a vital perspective viewpoint in studying IoT and SCADA

systems. As noted in the section, Holistic IoT Security, the IoT has many challenges, both technical and nontechnical. GST and systems thinking approaches allow all aspects of the IoT to be researched, including technical and nontechnical challenges such as social, legal, and ethical (Ryan & Watson, 2017). However, when identifying a practical theory as an overarching theme for the application of IoT in production, systems dynamic theory proved more desirable than GST in one study (Griffy-Brown et al., 2019). A common theme in the literature regarding GST and technology is that GST is valuable. Still, researchers may need to involve other supporting theories to thoroughly analyze, explore, and describe technical phenomena.

## Analysis of Similar Theories

In researching theories for this study, I learned of several theories that have either been derived from or are closely related to GST. The following sections contain information on two theories that are similar to GST: system dynamics and complexity theory. The sections below contain both a comparison and contrast of these theories against GST and reasoning why GST, and not system dynamics or complexity theory, was ultimately selected for this study.

### *System Dynamics*

System dynamics was first introduced by Forrester (1961). Several system dynamics principles include feedback loops, a holistic perspective, affecting one part of a system has effects on other parts, and that a system is not defined solely by its individual parts (Hjorth & Bagheri, 2006). System dynamics have similarities to GST. In system dynamics, a system contains five properties (Hjorth & Bagheri, 2006): (a) bounded

rationality, (b) limited certainty, (c) limited predictability, (d) indeterminate causality, and (e) evolutionary change. Additionally, one role of system dynamics is understanding a complex system's behavior to simulate the system with a model (Hjorth & Bagheri, 2006). System dynamics differs from GST in its definition of a system and its focus on studying the behavior and modeling of systems.

Much like GST, there is some debate in the literature on system dynamics' maturity and usefulness. Forrester (2007) argued that the quality of work in system dynamics to date is subpar. He further stated that, for system dynamics to mature and be truly impactful, academia must build schools that focus primarily on system dynamics, much like the medical and business schools that exist (Forrester, 2007). Homer (2007) disagreed with Forrester, citing multiple books authored by senior faculty that suggest system dynamics has rigor and is a mature field. Like GST, although there is some disagreement among researchers on system dynamics' applicability and usefulness, there are many examples in the literature where scholars have successfully employed system dynamics in their research.

System dynamics is in the literature review because of its relevance and continued recent use by scholars to research problems in many different domains. Using causal-loop diagrams and other system dynamics tools, one simulation demonstrated that cybercrime in the Czech Republic and European Union is likely to increase unless there is an increase in awareness (Dolezal & Tomaskova, 2019). Jiang et al. (2019) proposed and tested a trust model for mobile cloud computing using system dynamics as a foundation for their research. In another study, researchers used Anylogic, a simulation development

tool for dynamic system models, to create a framework for scheduling jobs to support Industry 4.0 operations (Leusin et al., 2018). Scholars have also used system dynamics to identify a negative correlation between labor input and investment value in studying urban water supply and demand (Li et al., 2019). System dynamics is an applicable theory that is still currently employed by scholars in research. However, I decided not to use system dynamics for my research because of its focus on identifying and simulating systems' behavior. My research is to identify strategies to securely implement IoT devices and not study systems' behavior.

### *Complexity Theory*

Complexity theory is another theory founded in GST and was first introduced in the 1970s (Ryan & Watson, 2017); complexity theory's basic premise is the system's behavior. Complexity theory maintains several of the tenets of GST. For example, complexity theory maintains that a system must be studied holistically and that a system cannot be described by studying parts individually (Cairney, 2012). Complexity theory expands GST with additional characteristics: (a) outputs may not be predicted simply by understanding the system inputs, (b) system outputs are not predictable, nor are they unpredictable, and (c) a systems history is immutable (Basile et al., 2018). Manson (2001) maintained that complexity theory differs from GST in that it evaluates nonlinear relationships in changing entities, whereas GST holds that system component relationships are linear. Another differentiation between GST and complexity theory is the system performance itself. GST maintains that all systems eventually reach an equilibrium state where each system's piece is performing its function (von Bertalanffy,

1972). Complexity theory states that complex systems never reach equilibrium due to evolving behaviors induced by system components' interactions over time (Manson, 2001). Although complexity theory is founded in GST, there are significant differences in the theories; regardless, complexity theory is well represented in the literature as a foundation for studying many problems in a wide array of disciplines.

The literature contains many examples of researchers employing complexity theory to study a variety of problems. Turner and Baker (2019) argued that the necessity and value of using complexity theory in social sciences. Organizations are widely regarded as complex systems (Lowell, 2016). Complexity theory may provide insight into organizational change (Lowell, 2016); it may also assist in developing and deploying effective performance management systems (Okwir et al., 2018). Complexity theory can be a basis for risk management in complex environments (Emblemsvag, 2020). Complexity theory has value beyond social sciences and organizational research. Complexity theory has been used to identify relationships between sources of losses in water distribution systems and the effectiveness of mitigation methods (Azevedo & Saurin, 2018). When combined with lean manufacturing principles, complexity theory may improve production efficiencies in cyber-physical systems (Brinzer et al., 2017). Complexity theory may enhance cyber-physical systems' safety when coupled with traditional hazard identification techniques (Bolbot et al., 2019). Complexity theory has applicability to cyber-physical systems as well as the IoT. However, I chose GST as it allows a broader view than complexity theory. Complexity may prove helpful as a supplement to GST during data analysis, and therefore it is included in the literature

review. The following section contains information regarding other theories considered for this study.

## Analysis of Contrasting Theories

In addition to system dynamics and complexity theory, I reviewed theories that are unrelated to GST. The theories in this section are specifically related to information security or technology. The security risk planning (SRP) model, technology acceptance model (TAM), and diffusion of innovation (DOI) are all detailed in this section; the information includes a comparative analysis of GST and why these theories were not selected for this study.

### *SRP*

One model that I found particularly interesting and considered for this study is the SRP. SRP was proposed by Straub and Welke (1998). I found this theory interesting because it precedes similar models introduced by National Institute of Standards and Technology (NIST, 2012) and International Standards Organization (ISO) 27005 (2013), and it continues to be relevant towards current research; examples include Udo et al. (2018), Yang et al. (2017), and Nicho (2018). Given the data in the literature, the SRP model is one theory that can be successfully used to study information security.

The SRP is a process model with specified action steps to enhance information security and risk management. Straub and Welke (1998) introduced this model to provide a formalized method of securing parts of security systems. The model contains five phases: (a) recognition of security problems, (b) risk analysis, (c) alternatives generation, (d) decisions, and (e) implementation (Straub & Welke, 1998). In practice, the model

uses a countermeasure matrix for decision-making and feedback loops to determine effectiveness (Straub & Welke, 1998). Although the SRP provides a process definition, challenges are associated with risk management models, including SRP. According to Fenz et al. (2014), risk management models are susceptible to risk misidentification, overconfidence, and risk versus trade-off analysis. The SRP model has many benefits and has contributed much to the literature, but it is only a piece of a holistic view of information security.

I decided not to select SRP as the theory for this study for a few reasons. SRP is a process model implemented on individual security risks over time (Straub & Welke, 1998); my intent with this study is to research IoT security in manufacturing environments from a holistic viewpoint that includes state, inputs, outputs, feedback loops, and relationships between systems. SRP is more narrowly focused than GST as it focuses on individual risks versus studying a phenomenon in a systems holistic manner. Conceivably, SRP could be used as a framework to secure parts of systems once analyzed and identified using a GST lens. Because of the time factor and the narrower view of SRP, I chose not to use the theory for this study; however, I did consider other theories as a basis for this study before deciding on GST.

***TAM***

The TAM can be used to research a technology phenomenon. TAM was developed by Davis in 1986 and is grounded in the Fishbein model (Davis, 1986). In the TAM, perceived usefulness and perceived ease of use of technology affect an individual's attitude towards using the technology and subsequently actual use of the

technology (Davis, 1986). Perceived ease of use and perceived usefulness are swayed by system design features (Davis, 1986). The TAM is a theory that can be employed as a framework to research technology acceptance.

***DOI***

In addition to GST, DOI can be used as a framework to study technology. In the DOI, diffusion is the process of how an innovation is communicated through a medium over time to a population (Rogers, 2003). The adoption of innovation follows an S curve over time (Rogers, 2003). Initially, during the process, there are few early adopters (Rogers, 2003); in cases where the change is successful, adoption reaches a critical mass as more people adopt the innovation (Rogers, 2003). The number of adopters and the rate of adoption is determined by factors including perceived advantages and compatibility of the innovation (Rogers, 2003). DOI is a theory that can provide a framework for studying the adoption of technology innovations.

I chose GST instead of TAM or DOI for several reasons. GST requires the researcher to view the problem in a more holistic or wholeness manner (von Bertalanffy, 1972). Both TAM and DOI have a more limited focus as they address the acceptance and diffusion of technology and not technology from a holistic manner. Identifying strategies to securely implement IoT devices in manufacturing environments may be easier when holistically viewing the phenomenon. Although implementing IoT devices will require acceptance and adoption to be successful, that is not the lens from which I wanted to explore the problem.

## Critical Analysis of Potential Themes and Phenomena

This section contains a synthesis of academic literature related to IoT, information security, and manufacturing environments. The references included in this section were chosen for specific reasons such as the significance of the research, a seminal reference related to this study, the number of occurrences of a theme or topic within the literature, the recency of the research, or the relevance to this study. Many other articles were reviewed but deemed unnecessary, extraneous, or did not inform this study.

### Holistic IoT Security

#### *Information Security*

The literature on information security contains various models that can be used to improve data security posture. I chose to include three such models in this literature review because they offer a holistic view of information security. Alhogail (2015) designed and tested a framework that approaches information security holistically by addressing both human and technical controls and improving employee behavior by changing organizational culture. Although Alhogail's research confirmed the framework's validity, it is seemingly complex and may be difficult to implement. Sohrabi Safa et al. (2016) proposed a model for information security compliance based on the social bond theory and involvement theory; the model focuses on employee behavior and attitude toward information security operating procedures (ISOP). A weakness of this model is that it assumes an organization has mature and effective ISOPs in place. Researchers have attempted to address the creation of ISOP. Carcary et al. (2016) provided a framework for information security governance and management. Their

framework holistically views information security and addresses the technical, process, and human aspects of information security (Carcary et al., 2016). There are frameworks that organizations can use to improve their information security environment, and a standard component of many of them includes performance metrics.

Performance metrics for information security controls should be an integral part of an organization's overall information security structure. Jansen (2009) called for research and development of security metrics that included both quantitative and qualitative metrics and were capable of measuring composite systems' performance. Since then, researchers have heeded the challenge and proposed information security metrics and measurement programs. Bernik and Prislan (2016) proposed a ten by ten measurement system that predefined ten critical success factors, each with ten key performance indicators. The system contains quantitative metrics for technical controls and compliance; it also contains qualitative measures to track items like employee management and organizational culture. Pendleton et al. (2016) proposed a less prescriptive model for security metrics that includes four dimensions: (a) vulnerability, (b) defenses, (c) attacks, and (d) situation. Pendleton et al. (2016) attempted to develop a model of metrics to approach security on a systems level. The literature contains frameworks, models, and metrics for information security in general; the next section provides information specific to IoT information security.

### *IoT Information Security*

Information security, in general, has challenges, and many of those same challenges exist within the IoT ecosystem as well. Vulnerabilities inherent with wireless

networks, lack of device maintenance and upgrades, poor device design and implementation, authentication, and identification are common within the literature on IoT information security (Khan & Salah, 2018; Lin & Bergmann, 2016; Sajid et al., 2016; Tweneboah-Koduah et al., 2017). There are a few IoT vulnerabilities uniquely identified in the literature. The rapid growth of the number of IoT devices in use and the ubiquitous nature of IoT is a vulnerability as it has made IoT a popular cybersecurity target (Abomhara & Geir, 2015). IoT solutions are being integrated with legacy systems that previously were not connected to a network and were not designed with data security as a focus (Baskaran et al., 2019). Another vulnerability identified in some of the literature is the lack of end-to-end connectedness in IoT (Razzaq et al., 2017), without which common security practices such as encryption cannot be implemented (Khan & Salah, 2018). IoT information security has many of the same challenges as information security overall.

The nature of IoT introduces new challenges in information security as well. One characteristic of IoT that allows for additional vulnerabilities is the lack of computing, storage, and network resources available to IoT devices and applications (Lin & Bergmann, 2016). IoT devices are often deployed to low-power and lossy networks with limited resources that lack energy, processing power, and memory capacity to implement standard network security measures (Alaba et al., 2017). The lack of computing resources in IoT devices prohibits using complex security schemes necessary to enhance device security (Khan & Salah, 2018). The IoT vulnerabilities are well documented; the next section will contain information on IoT threat vectors and cyberattacks.

The IoT has different threat vectors and is susceptible to multiple cyberattack methods. One threat vector is the physical layer, or the IoT device itself (Tweneboah-Koduah et al., 2017); IoT devices are susceptible to spoofing, malware, and botnets, Denial of Service (DoS), loss of control, and eavesdropping (Alaba et al., 2017; Tweneboah-Koduah et al., 2017). Attacks at the device level vary in technique and severity. Another threat vector is the network layer (Alaba et al., 2017). The network layer is vulnerable primarily to Dedicated DoS (DDoS) attacks, man-in-the-middle, and code execution (Alaba et al., 2017; Baskaran et al., 2019; Tweneboah-Koduah et al., 2017). One final layer to consider as a threat vector is the application layer (Tweneboah-Koduah et al., 2017). Attacks at this layer include DDoS, advanced persistent threats (APT), SQL injection, code execution, and many others (Baskaran et al., 2019; Tweneboah-Koduah et al., 2017). The IoT is vulnerable to several different types of attacks from multiple vectors.

Some cyberattack methods are more common and detrimental than others. One particular attack method that is growing in frequency and is particularly devastating includes a DDoS using IoT devices that have been infected with botnets (McDermott et al., 2019); a contributing factor on the effectiveness of this method of attack is that an IoT device may be infected with a botnet and still operate normally (McDermott et al., 2019). Part of the challenge in creating defenses for this type of attack is the lack of realistic IoT datasets and test environments for research and testing (Koroniotis et al., 2018). While there may not currently be a standardized defense for all IoT cyberattack vectors,

standards and architectures have been developed and proposed that organizations can implement to enhance their security posture.

### *IoT Architecture*

The literature contains different representations for IoT architecture with a varying number of layers. A 3-layer representation is common in the literature (Gubbi et al., 2013; Khan et al., 2012; Wu et al., 2010; Yang et al., 2011). Except for Gubbi et al. (2013), the three layers are essentially the physical or perception layer, a network layer, and an application or presentation layer. Gubbi et al. (2013) proposed a 3-layer architecture that cites cloud computing as the middle layer. Representing IoT in a 3-layer architecture may be too rudimentary or simplistic to capture IoT technologies' full breadth.

Representing IoT in more than three layers may provide advantages for IoT solution design and implementations. Five-layer architectures have been proposed (Tan & Wang, 2010; Wu et al., 2010; Yang et al., 2011); these models add a layer of object abstraction between the physical and network layers for more scalability (Al-Fuqaha et al., 2015). One particularly interesting architecture is the 5C architecture for CYBER-PHYSICAL SYSTEM (Lee et al., 2015). The 5C includes a cyber layer that other architectures only imply and is flexible enough for IoT applications. Once an IoT architecture is defined, each layer can be isolated for further standardization.

### *IoT Layer Security*

The following discussion on securing layers refers to IoT architecture layers and should not be confused with either the Open System Interconnection (OSI) or the

Transmission Control Protocol/Internet Protocol (TCP/IP). There are techniques for securing IoT at the physical layer. Due to resource constraints in the IoT, securing the physical layer using traditional key pair generation/exchange and encryption methods is not feasible (Mukherjee, 2015). Researchers have addressed these limitations in different ways. One of the physical layer vulnerabilities is device takeover; a preventive measure may be to load only binaries that have been cryptographically signed and verified (Arias et al., 2015). Identification and authentication are also concerning. Huberman (2016) proposed a protocol that incorporates both hashing and public key. A light-weight wireless communications protocol uses radiofrequency fingerprinting for authentication and wireless channel properties for key generation (J. Zhang et al., 2019). Soni et al. (2019) proposed a pre-processing key generation method to keep the process simple and efficient. Techniques for device security exist; manufacturers of the devices need to incorporate security measures.

In the IoT, the network layer often includes wireless sensor networks (WSN). Common WSN's in IoT include Bluetooth, Zigbee, and 6LoWPAN (Kocakulak & Butun, 2017); others include Z-Wave, EnOcean, and Cellular (Burg et al., 2017). Each protocol uses electromagnetic waves for communication, and each uses different regions of the radio frequency spectrum (Burg et al., 2017). WSN networks are normally arranged in linear, star, or mesh topologies (Kocakulak & Butun, 2017). The advantages of WSN include reduced installation cost and ease of installation (Burg et al., 2017). While common in IoT, WSN's raise information security concerns.

The nature of WSN's introduces security concerns. WSN's are potentially the most extensive security vulnerability within the IoT (Khattak et al., 2019). Much like IoT itself, WSN's have constrained resources (Siddiqi et al., 2018), and therefore traditional network security tactics are not always feasible (Pirbhulal et al., 2017). Researchers have addressed WSN security concerns in different ways. Pirbhulal et al. (2017) and Memos et al. (2018) proposed new encryption algorithms that are more efficient than existing methods. Porambage et al. (2015) introduced a group key authentication protocol for WSN. A single strategy for WSN security does not yet exist. Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are two technologies to provide network security. Granjal and Pedroso (2018) proposed an IPS / IDS framework for WSN that successfully enhanced security. Almomani et al. (2016) created a dataset for further research and testing of IDS. There is much in the literature on WSN, but more work still needs to be completed to provide security for WSN in the IoT.

Establishing secure communications at the application layer of the IoT is an area of concern. Huberman (2016) proposed a public-private key exchange protocol with hash algorithms to ensure data security. He acknowledges public key decryption is slow compared to other techniques. However, his protocol does not address the limited resources in the IoT; also, there is no clear explanation of the implementation of the protocol. Researchers have provided other protocols that consider these issues. Abdmeziem and Tandjaoui (2015) use third parties and a remote server to offload the resource-intensive cryptography operations from IoT devices to create an end-to-end key management protocol. Symmetric cryptographic techniques during key pair negotiations

can create a secure environment for data exchange while requiring fewer resources than asymmetric cryptography (Chen et al., 2016). Key pair exchanges are not the only valid ways to establish secure communications at the application layer. Hou and Yeh (2015) proposed a single sign-on (SSO) technique using tokens that incorporates an authentication server and a trusted third party to establish a secure connection. The use of SSO and third parties reduces the resource requirements of the IoT application. Techniques exist for establishing secure connections at the application layer; it is equally essential that the communications protocols at the application layer account for information security.

Information security at the application layer of IoT requires efforts to secure protocols at this layer. Common application layer protocols include MQTT, XMPP, and CoAP (Nastase, 2017). Many researchers, including Randhawa et al. (2019) and Amaran et al. (2018), attempt to resolve security concerns at this layer by creating enhanced encryption methods for these protocols that account for IoT's limited resources. However, alternative methods for securing the IoT application layer are contained in the literature. Dinculeana and Cheng (2019) proposed a Value-to-Keyed-Hash Message Authentication Code that requires few resources as it eliminates encryption while still maintaining the confidentiality and integrity of data. Hernandez Ramos et al. (2018) created a lightweight fuzzing tool for the MQTT protocol to identify security vulnerabilities. An additional alternative means of securing the IoT application layer employs blockchain technology. Deploying IoT in a blockchain environment eliminates the need to provide protocol security (Khan & Salah, 2018). Blockchain also provides

data security as the data become immutable (Reyna et al., 2018). Researchers have provided many opportunities to secure the IoT application layer, but many of them are untested and in their infancy; more research and testing are required before these methods are mature.

## Manufacturing Environments

The manufacturing landscape is changing to become integrated as manufacturers migrate towards cyber-physical systems, industry 4.0, and smart factories. It is essential to identify the technologies involved in the smart factory to understand the information security implications. Industrial IoT (IIoT) and cyber-physical systems are susceptible to all the information security vulnerabilities, risks, and threats related to IoT; however, there are information security challenges and concerns unique to and exacerbated by the IIoT cyber-physical systems. Also, some manufacturers are not implementing some basic cyber defenses in their industrial control systems (ICS) and IIoT applications. The risks in IIoT / cyber-physical system can have catastrophic effects on the real world. Each of these concepts is explored further in the sections below.

### *Cyber-Physical Systems, Industry 4.0, and the Smart Factory*

The manufacturing landscape is changing to become integrated. A cyber-physical system integrates computing functions with physical systems (Oztemel & Gursev, 2018); modern cyber-physical systems are capable of real-time system monitoring and performing functions to control the physical processes (Boyes et al., 2018). Traditionally, manufacturing processes consisted of isolated business and engineering systems with little interconnectivity between the systems (Pereira et al., 2017). Examples of business

and engineering systems include Enterprise Resource Planning, Manufacturing Execution System, Supervisory Control and Data Acquisition (SCADA), Industrial Control System, Process Control Systems, and Distributed Control System (Boyes et al., 2018; Chen et al., 2017). Industry 4.0 comprises IoT and cyber-physical systems within industrial environments and includes people, products, machines, and smart devices (Lezzi et al., 2018). A key component of achieving Industry 4.0 is integrating these systems to create a smart factory (Pereira et al., 2017). Integration of these systems allows for improved efficiencies (S. Wang, Wan, Li, & Zhang, 2016); however, integrating these systems introduces new information security concerns.

It is also important to identify the smart factory's technologies to understand the information security implications. Smart factories comprise cyber-physical systems that automate the production process (Sengupta et al., 2019). S. Wang, Wan, Zhang, et al. (2016) identify IoT, WSN, big data, and cloud computing in their proposed framework for smart factories. Chen et al. (2017) explained the function of IIoT, industrial WSN, big data, and cloud computing in a smart factory. There is consensus in the literature that these technologies are necessary for smart factories. Researchers also identify artificial intelligence as an emerging technology used in the smart factory (Wan et al., 2018; S. Wang, Wan, Li, & Zhang, 2016). Oztemel and Gursev (2018) highlight virtual reality, augmented reality, simulations, and virtual prototyping have in the smart factory. The technologies used in smart factories are identified in the literature; their use's breadth and scope continue to evolve. Further research is necessary to determine the impact these technologies and integrated systems have on information security.

### *Information Security Challenges*

IIoT and cyber-physical systems are susceptible to all the information security vulnerabilities, risks, and threats previously discussed regarding IoT; however, there are information security challenges and concerns unique to and exacerbated by IIoT and cyber-physical systems. IIoT and cyber-physical system applications are generally maintained by traditional controls engineers, which typically leave information security to IT professionals (Wolf & Serpanos, 2018). Controls engineers may not approach system development, implementation, and maintenance with a focus on information security. Also, system availability takes precedence over confidentiality and integrity in manufacturing (Ashibani & Mahmoud, 2017). Therefore, necessary security patches and system upgrades are often delayed or even skipped altogether to ensure the availability of systems is not compromised (Kobara, 2016; Lezzi et al., 2018). As systems become outdated, they may be more susceptible to security threats.

Legacy ICS components can be highly vulnerable in manufacturing environments. In the IIoT/cyber-physical system, the ICS components such as SCADA, programmable logic controller, distributed control system, and human-machine interface (HMI) are regular cyberattack targets (Sengupta et al., 2019). The ICS components' lifecycle is considerably longer than traditional information communication technologies and equipment (Kobara, 2016). Many ICS were designed for existing on proprietary communication networks and were not expected to be exposed to the internet (Gurtov et al., 2016; Kobara, 2016). Companies are increasingly connecting ICS to the internet to achieve IIoT (Lezzi et al., 2018). The legacy nature of ICS and that they are frequented as

cyber targets further challenges information security in the IIoT. The methods used to interconnect ICS and expose them to the internet creates information security vulnerabilities.

Some manufacturers are not implementing some basic cyber defenses in their ICS and IIoT applications. In terms of the communication network, some manufacturers create flat, unsegmented networks for their ICS (Lezzi et al., 2018). A segmented network is the first line of defense as it prevents attack propagation and simplifies system monitoring (Corbo et al., 2018; Gurtov et al., 2016). In some cases, default passwords are left intact & network ports are opened (Lezzi et al., 2018). The lack of cybersecurity best practice implementation is creating vulnerabilities in manufacturing environments. The next section contains information on risks associated with cyberattacks on cyber-physical system systems.

The risks in the IIoT / cyber-physical system can have catastrophic effects on the real world. Since the cyber-physical system integrates computing systems and physical systems, a cyberattack on a cyber-physical system can cause loss of observability, control, or even power of a control system (Corbo et al., 2018). For example, IoT has been exploited to disable a uranium enrichment plant in Iran (Slayton, 2016) and take down electricity in Ukraine for six hours (Sullivan & Kamensky, 2017). The risk associated with cyberattack on cyber-physical systems includes equipment damage and personnel safety.

**Relationship of This Study to Previous Research**

The literature contains research on IoT and related topics that are founded on qualitative case study design. Boutwell (2019) conducted a qualitative multi-case study to discover strategies to protect critical infrastructure, including ICS, from cyberattack. Boutwell's (2019) study included four cases, five participants, in the Pacific Northwest United States. Boutwell's (2019) research identified four themes: (a) a security training program is vital, (b) infrastructure durability must be a priority, (c) security awareness is necessary, (d) organizational leadership must support and invest in security. This proposed study differs from Boutwell's (2019) in that it will be conducted in the Midwest Region of the United States. It focuses on IoT and manufacturing environments and not critical infrastructure. Griffin (2017) performed a single case study in the United States' southeastern region to explore strategies to prevent data breaches caused by mobile devices. Griffin (2017) concluded that information security policy and procedures, security awareness, technology management tools, and defense-in-depth are key strategies to prevent data breaches enabled by mobile devices' exploitation. Griffin's (2017) study is like this study as the topics included cybersecurity and an IoT device; Griffin's (2017) study differs in that it used a single case design. Kamin (2017) performed a study to explore strategies that enable the adoption of IoT. Kamin (2017) identified securing IoT devices, separating private and confidential data from analytical data, customer satisfaction requires more than reliability and using IoT to retrofit products as key IoT adoption strategies. The studies above inform this study in that each used a similar qualitative case study design. Each researcher used thematic coding as part

of their data analysis. The key strategies identified in the studies have overlap and are similar to themes identified by this research.

Researchers have conducted studies on the IoT, manufacturing, or related technologies, citing GST as a conceptual framework. Nazir et al. (2017) employed GST to study SCADA systems; they concluded that future research is necessary and that newer security measures, including autonomic computing, are essential for successful cybersecurity in the future. NG and Wakenshaw (2017) state that the IoT is ever-changing, and they call for further research, suggesting that systems theory is a useful conceptualization to study IoT. Research using systems theory to study manufacturing is prominent (Eyers & Potter, 2017); however, more research that connects systems theory and industrial practice is necessary for further advancement (Eyers & Potter, 2017). These studies are testaments that research of IoT and manufacturing that employs GST exists in the literature. However, each identifies their prospective technology as evolving, and each call for further research. While the studies employ GST in topics related to this study, none of them identify strategies to implement the IoT in manufacturing environments.

The literature contains research on IoT security and implementation, but existing literature is lacking as it applies to manufacturing environments. Abomhara and Geir (2015), Griffy-Brown et al. (2019), Farooq et al. (2015), and Khan and Salah (2018) provide potential strategies to secure the IoT; however, they do not contain data specific to manufacturing environments. Methods for secure IoT device updates (Arias et al., 2015), data encryption (Huberman, 2016), device authentication (J. Zhang et al., 2019),

and network IDS/IPS (Granjal & Pedroso, 2018) exist in the literature; however, none of the studies identify strategies to implement IoT in manufacturing environments. Tuptuk and Hailes (2018) provide detailed cybersecurity concerns in the IIoT in the form of a narrative, but practical strategies to securely implement IoT are not contained in the article. There are studies in the literature that are related to the proposed study but differ in significant ways.

## Transition and Summary

This section provided a background of the proposed research topic and the approach used during research. I chose a qualitative multi-case study design to explore the strategies electrical controls engineers use to securely implement IoT devices in manufacturing environments. The conceptual framework chosen for this study is GST, as it provides the ability to research the topic using a broad perspective. The results of this study identified strategies to securely implement IoT devices in manufacturing environments, thereby improving the efficiency and safety of manufacturing processes and stakeholders. The literature focused on topics related to GST, information security, IoT, and manufacturing environments.

Section 2 contains more specific information about the project. The section details the purpose of the project and the role that the researcher plays during research. The research method and design are thoroughly explained in section 2 as well. I also address population and sampling, ethical research, and data collection in the next section. Finally, information regarding data analysis, reliability, and validity are contained in section 2. Section 3 will contain the findings of the data analysis.

# Section 2: The Project

Section 2 contains information specific to the project, including the purpose of the project. Additionally, in this section, I define the role of the researcher, set parameters for the participants, and identify that the study will include three cases. This section contains details and explanations on the population and sampling technique, ethical research, data collection, data analysis, reliability, and validity.

## Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies that electrical controls engineers use to securely implement IoT devices in manufacturing environments. The specific population included electrical controls engineers of three manufacturing facilities in the Midwest region of the United States that have strategies to securely implement IoT devices. Findings from this research may contribute to positive social change by enhancing the safety of production personnel and manufacturing equipment because the study identified strategies to securely implement IoT devices in manufacturing environments.

## Role of the Researcher

The role of the researcher is dependent on the type of study being conducted. For qualitative case study designs, multiple sources of data are required, and a best practice is to use an instrument for each source of data (Yin, 2014). For this study, I collected data using semi structured interviews and by obtaining documents. To support the data collection, I developed an interview protocol (see Appendix A) that I used to conduct all

of the semi structured interviews and a document collection protocol (see Appendix B) that I used during document collection.

I was the sole researcher and data collector for this study. Often, industrial controls systems in manufacturing require the use of IoT devices. I have been designing and implementing industrial controls systems in manufacturing environments in varying capacities since 1999. Given my experience in using IoT devices in manufacturing environments, I needed to take steps to mitigate any bias my previous experience may have had in influencing the study. I live in the Midwest region of the United States. However, I did not select organizations where I have a previous connection, and I excluded participants from previous personal or professional associations.

Personal experiences and biases could affect my data collection and study. According to Fusch and Ness (2015), the researcher's worldview or personal lens must be considered during data collection and analysis to mitigate bias (Fusch & Ness, 2015). One means of mitigating a researcher's bias is to use multiple sources of data (Roulston & Shelton, 2015; Yin, 2014). I used multiple sources of data, such as interviews and documents, for this study. I have developed an interview protocol for semi structured interviews. I conducted all the interviews using the protocol. Reflexive practices are another method for removing bias during a study (Roulston & Shelton, 2015; Yin, 2014). Accordingly, I kept a reflexive journal while conducting the study.

Part of my role as the researcher is to ensure the ethical treatment of study participants. *The Belmont Report*, released by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research in 1979, provides guidelines

for participants' ethical treatment. According to this report, the basic principles for treating study subjects are respect for persons, beneficence, and justice. In practice, these principles are achieved through informed consent, assessment of risks and benefits, and selection of subjects. I obtained an email consent from each participant after they reviewed the consent form that informed them of their right to opt-out of the study at any time. I will always keep all participant names confidential and keep all collected information secure.

Interview questions and protocols are an essential part of data collection. I used semi structured interviews during data collection as this format allows further exploration and leads to more objective data (see van de Wiel, 2017). To ensure consistency between interviews, it is vital to develop interview protocols (van de Wiel, 2017). The protocol I created (see Appendix A) contains the initial questions I asked all participants.

## Participants

I conducted a purposive sample to select participants for this study. Participants for this study met the following requirements: (a) must have at least 5 years' experience as an electrical controls engineer in manufacturing environments, (b) must currently have industrial controls responsibilities in a manufacturing facility located in the Midwest region of the United States, (c) must have worked on projects involving implementation of IoT devices in manufacturing environments, and (d) must have information security experience or knowledge. I chose these requirements to ensure experience with securely implementing IoT devices in manufacturing environments.

Before contacting any potential participants, I obtained institutional review board (IRB) approval. IRB approval ensures proper protections are in place to study human subjects (Domenech Rodriguez et al., 2017). Gaining access to organizations and participants in qualitative research is often thought to be simple by some (Peticca-Harris et al., 2016); unfortunately, it can be difficult or even awkward without an identified process for gaining access (Peticca-Harris et al., 2016). I identified organizations by asking my network of professional contacts for referrals of individuals employed by manufacturers that use IoT devices in their environments. Once a potential site was identified by referral, I contacted individuals at the organization and asked them to provide a letter of participation if they chose to do so. I was then provided information for the gatekeeper. A gatekeeper can aid in ensuring access to the organization and participants during research and assist in overcoming challenges during the interview process (Rimando et al., 2015). Once I had IRB approval, I recruited participants by communicating with the gatekeeper at the organizations. In some cases, the gatekeeper informed potential participants of my study and asked them to contact me if they were interested in participating in the study. In other cases, the gatekeeper provided contact information for potential participants, and I communicated with them directly. In each scenario, all participants were provided the consent form and responded to me directly with a consent email. Once a qualified candidate agreed to participate in the study, I coordinated with the participant and established a time and place to conduct the interview.

I established rapport and trust with the participants in several ways. First, I explained to participants how I would maintain the privacy of the data they provided and that their identity would remain anonymous. Telling one's own story and experience is an effective means to establish rapport with interview participants (Harvey, 2015; Rinke & Mawhinney, 2014); therefore, I identified with participants by explaining my professional background regarding information security, controls engineering, and working in manufacturing environments. Third, I sought their input for the interview site to ensure they would be comfortable and enhance privacy. Finally, I explained that I was an interested observer and that I cast no judgments or opinions.

## Research Method and Design

In structuring research, according to Yilmaz (2013), there are four fundamental issues to consider. First is the worldview that will inform the study. The second is to determine who or what will be studied. The third issue is to select the research strategies for the study. Finally, the research methods used to collect and analyze the study need to be identified. In this section, I expand on the justification for choosing a qualitative methodology and design over quantitative or mixed-methods design.

### Method

I selected a qualitative multi-case study design for the study. Qualitative methods are exploratory and allow the researcher to gain an in-depth understanding of the phenomenon being studied (Da Mota Pedrosa et al., 2012). I explored strategies with this study. Qualitative research draws from various paradigms and allows that more than one reality may exist (Bristowe et al., 2015). Qualitative research supports the possibility that

there may be more than one set strategy to securely implement IoT devices in manufacturing environments. Finally, qualitative research allows collecting documents and other data that is not quantitative (Kruth, 2015). I collected documents during this study.

Quantitative methodology is another type of research that I could have used for my study. Quantitative research involves statistical analysis of numerical data to prove or disprove a hypothesis (McCusker & Gunaydin, 2015). However, it was not my intent to collect only numerical data; I examined participants' personal experiences because this was essential to answering the research question. Data analysis in quantitative research allows researchers to understand the relationship between variables (Park & Park, 2016), but I did not identify variables for this study because discovering the strategies individual engineers use better aligned with my identified IT problem. The goal of quantitative research is to prove or disprove a hypothesis (Trafimow, 2014). However, I did not have a hypothesis to test. I did not choose a quantitative method because I collected data other than numerical, I did not have variables to evaluate, and I had no hypothesis for this study.

The final research method I could have chosen for the study is mixed methods. Mixed methods are a combination of both qualitative and quantitative methods (Mabila, 2017). As a quantitative method is not well-suited to this study, neither is mixed methods as it contains a quantitative component. When choosing the research method, the researcher should evaluate the method against the research question and choose a method that most appropriately answers the research question (Stockman, 2015). The research

question for this study was best answered by a qualitative design. Mixed methods research essentially requires that the researcher conduct two studies (Malina et al., 2011). Due to time constraints in the DIT program, it was not feasible to concurrently conduct two studies.

**Research Design**

I chose a multi-case study design for this study. Case study research allows the researcher to gain a deep understanding of an issue or phenomenon (Stake, 1978). I attempted to obtain an in-depth understanding of electrical controls engineers' strategies to securely implement IoT devices in manufacturing environments. The rationale for a single-case study design requires a single case that is grounded in theory, is unique or extreme, is a critical case, or is a revelatory case (Yin, 2014). Given the research topic, I would not likely identify a single case that meets the required rationale for a single-case study, so a multi-case study design was most appropriate.

Another research design I considered is ethnography. A goal of ethnographic research is to study a group or culture to understand their behavior (Small et al., 2014). The purpose of my study was to explore strategies, not to gain an understanding of a population's behavior. Ethnographic research is meant to describe people, how they act, and how their culture or group influences their behavior, and vice versa (Draper, 2015). It was not my intent with this study to describe people or their interactions with groups or cultures. In ethnographic research, the researcher immerses themselves in the group or culture being studied, sometimes for extended periods (Mannay & Morgan, 2015). For my study, it was not my intent to immerse myself in manufacturing environments, but

rather to explore strategies to securely implement IoT devices in manufacturing environments.

The final research design I considered for this study is phenomenological. In phenomenological research, one attempts to fully understand an experience, not necessarily understand individuals (Kruth, 2015). With my study, I aimed to explore strategies to securely implement IoT devices in manufacturing environments. I was not attempting to gain an understanding of an experience. Phenomenology attempts to understand the essence of a phenomenon or lived experience by eliciting information from many individuals with shared experiences (Bristowe et al., 2015). With this study, I did not intend to seek participants with shared experiences to understand lived experiences. Data collection for phenomenological typically requires multiple interviews with each participant that are relatively lengthy, 1-2 hours (Stanley & Nayar, 2014). Due to the time constraints of the researcher, the phenomenological design was not a good fit. Given the desire to explore strategies to securely implement IoT devices in manufacturing environments, a multi-case study design was the preferred research design for this study.

Data saturation in qualitative case study research can be ensured using several techniques. Data saturation is achieved when no new data is discovered during an investigation (El Hussein et al., 2015). A researcher must collect enough data to analyze to achieve data saturation (Aldiabat & Navenec, 2018). I conducted semi structured interviews with eight participants, spanning three cases, to obtain enough data to analyze. To achieve data saturation, a researcher must ensure data saturation is achieved during

each interview by continuing inquiry until no new data is provided (Saunders et al., 2018). I asked follow-up questions during each interview until no new information was revealed. Collecting data from an entire population ensures all possible data is collected and no new data exists. I performed total population sampling (TPS) at each of the three selected cases. Data saturation can be achieved using data triangulation with multiple sources of data (Fusch & Ness, 2015). I collected multiple sources of data in the form of semi structured interviews and organizational documents. Member checking allows the interviewee to review the researcher's interpretation of the interviewee's answers and allow corrections (Morse, 2015); member checking informs data saturation as well. I performed member checking in this manner.

## Population and Sampling

The population for this multiple case study is electrical controls engineers that work in three manufacturing facilities in the Midwest region of the United States. The number of electrical controls engineers in a single facility varies depending on the manufacturing facility's size. I interviewed the entire population at each case that met the selection criteria; in total, I conducted eight semi structured interviews.

I have established specific selection criteria for participants in this study. In qualitative research, the participants can become the primary source of data (Baskarada, 2014). Therefore, it is essential to identify participants who can accurately describe their experience or knowledge of the studied phenomenon (Asiamah et al., 2017). As such, I have identified the following characteristics for participants: (a) must have at least 5 years' experience as an electrical controls engineer in manufacturing environments, (b)

must currently have industrial controls responsibilities in a manufacturing facility located in the Midwest region of the United States, (c) must have worked on projects involving implementation of IoT devices in manufacturing environments, and (d) must have information security experience or knowledge.

The sampling strategy for this study was purposeful total population sampling. The sampling strategy should be chosen to yield rich information about the phenomenon being studied and consistent with the chosen research method (Moser & Korstjens, 2018). The purposeful selection of participants enables the researcher to identify participants with relevant personal experience (Palinkas et al., 2015). For sampling, I worked with a gatekeeper at each facility to identify participants that met the selection criteria; I included all suitable participants in the study.

I achieved data saturation using multiple techniques and strategies. Data saturation occurs when no new information is found during the inquiry (El Hussein et al., 2015). One key to achieving data saturation is having enough data to analyze (Aldiabat & Navenec, 2018). I selected three cases, yielding eight participants, for data collection to ensure enough data was obtained to reach data saturation. I performed TPS at each of the three selected cases. TPS is a technique often employed in studies with small populations, and it includes the entire population of participants that meet the selection criteria in a study (Etikan et al., 2016). Collecting data from the entire population ensures all possible data is collected and no new data exists. Data saturation can be achieved using data triangulation with multiple sources of data (Fusch & Ness, 2015). I collected multiple sources of data in the form of semi structured interviews and organizational documents.

Member checking allows the interviewee to review the transcribed interview and researcher's analysis and interpretation and allow corrections (Morse, 2015); thus, member checking informs data saturation as well.

## Ethical Research

Ethical behavior towards participants is paramount while conducting research. The Belmont Report offers respect for persons, beneficence, and justice as three primary ethical considerations for researchers (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). Before starting the research process, I completed the required certification by the National Institutes for Health (NIH) Office of Extramural Research (No. 2113426) with the title Protecting Human Research (see Appendix C). I obtained Walden IRB approval and an approval number (No. 08-24-20-0645281) before contacting any study participants. Once I had approval, I obtained an email consent form from each participant. Each participant was notified of any associated risk and informed that they could withdraw from the study, without consequence, by simply stating the desire to do so. No participants chose to withdraw from the study. I did not offer any incentives to the participants for being part of the research study.

All data collected during the study is being treated as private and confidential. As such, I am keeping all data, electronic or otherwise, safe for five years after completing the study. After five years, I will burn all data. Protecting the data from disclosure is a key element of respecting the participants. I did not include the names of individuals or organizations in the results of the data analysis. The results of the study identified strategies that electrical controls engineers use to securely implement IoT devices in

manufacturing environments; sharing the results with participants is a central component of ensuring justice for the participants:

## Data Collection

### Instruments

I used several instruments during data collection: myself, an interview protocol, document collection protocol. Yin (2014) states that the researcher is the primary data collection instrument while conducting case study research. Therefore, as the only researcher conducting this study, I was the primary data collection instrument. Semi structured interviews allow researchers flexibility during the interview process to interact with the interviewee to obtain meaningful information (van de Wiel, 2017). The interview protocol (see Appendix A), which uses the semi structured interview format, was one of the data collection instruments for this study. I also used the document collection protocol (see Appendix B) during document collection. The researcher in qualitative studies performs data collection and analysis (Kruth, 2015). I conducted all of the data collection and analysis for this study.

I was intentional when conducting interviews. The first few minutes of each interview is vital as participants want to feel comfortable and at ease when they tell their story (Moser & Korstjens, 2018). Each interview was conducted at a time and place of the participants choosing, and I began each interview with an introduction and my background as it relates to the research topic. I informed each participant of the study's purpose that they have the option to stop the interview at any point by simply stating the desire to do so and finally discussed confidentiality and privacy of the interview. I then

asked each participant 6 open-ended questions. Follow-up questions allow for obtaining additional information about a research topic (Morse, 2015). I asked follow-up questions of the participants to gain additional information. Each interview was audio-recorded, and I used a transcription service offered by fiverr.com. I had used services like this in the past.

Interviews are only one way that I collected data for this study. Organizational documents are valid data to collect and analyze in case study research (Yin, 2014). I requested organizational documents from members at each organization. The documents include policy and procedures relating to information security, system design and modification, procurement, contracted labor, and other topics pertinent to the study. A document collection protocol can help achieve data consistency and organization during the collection phase (Santaniello, 2018). I used a document collection protocol that records key information about the document: (a) name and a brief description of the document; (b) source of the document, including date received; (c) type and format of the document; and (d) key information contained within the document that is relevant to the study. Data triangulation requires multiple forms of data (Morse, 2015). I performed data triangulation of the data collected from the interviews and organizational documents.

Ensuring the reliability and validity of the data collection instrument is a concern during data collection; I used several techniques to maximize the data's reliability and validity. Using an interview protocol refinement (IPR) framework can enhance an interview protocol's reliability and validity (Castillo-Montoya, 2016). A suggested IPR framework includes four phases: (a) ensure interview questions align with research

questions, (b) construct in inquiry-based conversation, (c) receive feedback on the interview protocol, and (d) pilot the interview protocol (Castillo-Montoya, 2016). I utilized the IPR framework for items a, b, and c to enhance my interview protocol's reliability and validity; however, due to workload and time constraints, I did not pilot the interview protocol. Member checking is a way to enhance data credibility (Connelly, 2016); reflexive journals also contribute to credibility (El Hussein et al., 2015). I conducted member checking by analyzing the interview data and asking each participant to evaluate the analysis for accuracy. I also kept a reflexive journal by recording my thoughts and reflections during the data collection process.

**Data Collection Technique**

I used semi structured interviews and organizational documentation collection for this study. I offered each participant the option to conduct interviews either face-to-face, by telephone, or by using a video conferencing service (Zoom, Google Meet, Microsoft Team, etc.). Each interview was conducted remotely using either a telephone or one of the video conferencing services. Interviews that exceed 90 minutes can lead to participant recruitment difficulties (Jacob & Furgerson, 2012). I kept the interview 45-60 minutes in duration. Video conference interviews have advantages of time savings in traveling as well as allowing participants to feel more comfortable during the interview (Peters & Halcomb, 2015); however, there are disadvantages of dropped or paused calls, inaudible sequences, and inability to read nonverbal cues (Seitz, 2016). The disadvantages of using video conferences to conduct interviews can be mitigated by setting up a test call, mutual agreement to repeat inaudible questions or answers, and paying close attention to facial

cues and body language (Seitz, 2016). I employed these practices during all interviews conducted via video conference. Regardless of modality of the interview, I audio recorded all interviews using Camtasia on my laptop.

I obtained organizational documents in two ways. Yin (2014) states that documents may be obtained in various ways, including asking for them during interviews, while in the field, and looking at open sources such as news sources. First, I searched open sources (news, internet, company website) for any applicable documents. I searched company websites for policies and procedures regarding information security. I used Google and Google News to perform searches for organizational documents using the organization's name and the following keywords: IoT, IIoT, data breach, security breach, data policy, information security, Industry 4.0, production automation, and others that arose during the search process. Second, I asked each participant for copies of organizational documents that are pertinent to the study. Documents include organizational and departmental policy and procedures, system change management, project specifications, product specifications, and system design standards. These techniques provided sufficient data for analysis.

I performed member checking with each participant. Member checking allows the participant to review the researcher's interpretation of the data (Morse, 2015). Once the interview had been transcripted and I had interpreted the data, I conducted a short follow-up meeting via phone or video conference to discuss the results and obtained feedback from the participant. During the follow-up meeting, I asked each participant if any other organizational documents could be provided to inform the study.

**Data Organization Techniques**

To assist with data analysis, I used both Microsoft Office applications and NVivo to organize the data collected for this study. NVivo is a Computer Assisted Qualitative Data Analysis Software (CAQDAS). NVivo can assist and accelerate the data process analysis regardless of the study's methodology and design (Zamawe, 2015). NVivo extends common manual and paper-based techniques for data analysis, including coding and thematic identification (Woods et al., 2016). Also, NVivo has many tools to assist researchers in data synthesis and determining the relevance and significance of data (Houghton et al., 2016).

I organized the data collected for this study in a manner that promoted anonymity and security. I coded each case and participant using an alphanumeric system. For example, case 1 was identified as "C1", case 2 was "C2," and so on; organizational names will not be used. Participants for each case were identified with the case code and an alphanumeric participant code; for example, C2P1, C1P2, etc. Organizational documents were coded simply with the case number and document number as such; C1D1, C1D2, etc.

I utilize VeraCrypt for my data encryption needs. I subscribe to Dropbox to keep data synchronized across all of my devices. For the data collected during this study, I created two VeraCrypt volumes using AES-256 encryption and an SHA-512 hash to house all of the data. All data collected for this study was provided in electronic format; no physical copies of any documents were provided at any time. Likewise, none of the data collected was ever printed during collection or analysis. The VeraCrypt volumes

were saved in my Dropbox, so the data was backed up and accessible to me on any device during data collection and analysis. The file sizes for the audio recording of the interviews were too large for them to be reasonably stored in Dropbox; I stored that data on an encrypted flash drive. All data is now stored on the encrypted flash drive. The flash drive will be stored in a fireproof safe for five years, after which the data will be permanently destroyed.

## Data Analysis Technique

To analyze the data obtained during this study, I employed methodological triangulation. In military terms, triangulation is used to geographically locate a position using multiple signals or satellites (Abdalla et al., 2018); researchers employ data triangulation by using multiple viewpoints or sources to improve their assessment precision (Abdalla et al., 2018). Denzin (1978) identified four types of triangulation: (a) data, (b) theoretical, (c) researcher, and (d); methodological. Theoretical triangulation is performed using multiple theories on the same data set to interpret the data (Abdalla et al., 2018; Amankwaa, 2016). Another form of triangulation, researcher, refers to having multiple researchers analyze and interpret the data (Abdalla et al., 2018; Amankwaa, 2016). Methodological triangulation requires using multiple methods of collecting data from various sources (Fusch & Ness, 2015). I used semi structured interviews and document collection from multiple sources for this multi-case study. Triangulation allows for the researcher to identify converging data, but just as importantly, it also identifies diverging data, which can be just as meaningful (Kern, 2018). Finally, methodological

triangulation supports the research's validity (Morse, 2015) and helps researchers achieve data saturation (Fusch & Ness, 2015).

After I collected the data using semi structured interviews and document retrieval, I analyzed the data. I first used a service by fiverr.com to transcribe the recorded interviews into MS Word. I had used these services in the past with success. Once transcribed, I interpreted the participant's answers, and member-checked each interpretation with the interviewee to ensure I had adequately understood the intent of their answers. This step provided MS Word files of both the interviews and the interpretation. The steps of transcription, interpretation, and member-checking prepared the data for analysis using NVivo software.

I used NVivo as a tool to assist in the data analysis. I imported interview transcripts, the interview interpretations, and all documents into an NVivo project titled "IoT-Mfg." Once the data had been loaded, I used Yin's (2014) method of case study data analysis. Yin (2014) identifies four strategies that can be employed for case study data analysis: (a) relying on theoretical propositions; (b) working the data from the "ground up"; (c) developing a case description; (d) examining plausible rival explanations. I worked the data from the ground up and employed pattern matching and coding; this is an inductive process used to identify themes and patterns in the data (Yin, 2014). During analysis, I used general systems theory as a framework for identifying themes; additionally, I used the ideas, concepts, and themes discovered while reading literature before and after data collection. The analysis identified identify many themes. I

used both the frequency of occurrence of a theme and the significance of a theme's impact to isolate four main themes in the data.

## Reliability and Validity

Reliability and validity are two important concepts to ensure quality when performing research. Validity refers to the extent to which a research study measures what it intends to measure (Kruth, 2015), while reliability is the extent to which a study could be repeated to achieve nearly the same findings (Yin, 2014). In qualitative research, quality and rigor are measured based on dependability, credibility, transferability, and confirmability (El Hussein et al., 2015). I will further explain these concepts and how I addressed each one in the following paragraphs.

### Dependability

There are ways I can achieve dependability when performing academic research. Dependability is a measure of the data's stability over the time and conditions of the study (Connelly, 2016). One method to achieve dependability is to create an audit trail (Morse, 2015), a detailed record of the research process (Connelly, 2016). I kept detailed notes on the research process to create an audit trail for my study. Another method to attain dependability is to maintain a reflexive journal (Amankwaa, 2016). Using a reflexive journal, researchers document their methodological decisions, track analysis, consider their emotions and role in the process, and consider research bias (Orange, 2016). I kept a reflexive journal during the research process. Data triangulation, which requires collecting data from multiple data sources (Yin, 2014), can also foster

dependability in qualitative studies (Morse, 2015). I performed data triangulation on the data I collected from multiple sources.

**Credibility**

I will enhance credibility by maintaining a reflexive journal and performing data triangulation of multiple sources of data. Data is considered credible if it accurately describes or presents an authentic and truthful representation of the studied phenomenon (El Hussein et al., 2015). In qualitative research, a researcher can establish credibility by member checking (Connelly, 2016); member checking is performed by having participants review transcribed interviews or analysis to ensure accuracy (Morse, 2015). I performed member checking by conducting phone or video conference interviews with each member to review all interview data analysis. Data triangulation and reflexive journaling also contribute to credibility (El Hussein et al., 2015). As previously mentioned, I maintained a reflexive journal and performed data triangulation.

Another important concept in research is data saturation. Data saturation occurs when the researcher no longer finds new information during inquiry (El Hussein et al., 2015) or when new data does not inform the research question (Gentles et al., 2015; Kruth, 2015). I achieved data saturation first by collecting multiple forms of data: (a) semi structured interviews, and (b) organizational documents. Secondly, I used member checking to ensure an accurate and complete representation of the data. Finally, I employed data triangulation.

**Transferability**

I recorded detailed field notes that included context, dates and times, and locations during field research. Transferability is the extent to which the study findings apply to others in similar situations (Connelly, 2016). Researchers develop transferability by including detailed descriptions of context, people, and locations in the study (El Hussein et al., 2015), thereby providing sufficient data to allow reviewers to determine the findings' applicability to their situation (Morse, 2015). Researchers can further transferability by describing participants and including descriptions of the sampling process (Gentles & Vilches, 2017). Purposeful sampling also enhances transferability (Cook et al., 2016). To support transferability, I recorded detailed notes to include context, dates and times, and locations while in the field; I also documented the sampling process.

**Confirmability**

I used several methods to build confirmability during my study. Confirmability refers to the degree that the findings are neutral, consistent, and repeatable (Connelly, 2016). Audit trails build confirmability by documenting the research process so that others may repeat the study (El Hussein et al., 2015). Reflexive journals also support confirmability (Morse, 2015) as it encourages the researcher to consider their own emotions and their role in the research process (Orange, 2016). Iterative analysis of the data also builds confirmability as it boosts transparency and appropriate conclusions (Cook et al., 2016). I employed an iterative analysis during data analysis. As previously

mentioned, I documented activities over time to create an audit trail and kept a reflexive journal during the study.

## Transition and Summary

In this section, I provided the purpose of the project and examined the researcher's role. The research method and design are thoroughly explained in this section. I also addressed population and sampling, ethical research, and data collection in this section. Finally, information regarding data analysis, reliability, and validity is contained in this section. Section 3 will contain the findings of the data analysis.

Section 3: Application to Professional Practice and Implications for Change

This section contains a brief overview of the study and a presentation of the findings from the project. This section also includes the application to professional practice and implications for social change. The section concludes with recommended actions, further research, and reflections.

## Overview of Study

The purpose of this qualitative multiple case study was to explore strategies that electrical controls engineers use to securely implement IoT devices in manufacturing environments. I collected the data from eight semi structured interviews and 15 documents retrieved from three different cases. I obtained data from field notes and a reflexive journal that I maintained during data collection. All study participants were electrical controls engineers with at least 5 years of experience and are knowledgeable of strategies to securely implement IoT in manufacturing environments. All three cases were manufacturing facilities located in the Midwest region of the United States.

This qualitative multiple case study revealed four main themes: (a) a collaborative work environment, (b) employ existing cybersecurity practices, (c) adequate resources must exist to maintain security, and (d) continued learning and education. These findings support my use of the GST as a conceptual framework and are congruent with data within the literature review. The following section contains further detail of the data analysis and the identified themes.

## Presentation of the Findings

The study's research question was: What strategies do electrical controls engineers use to securely implement IoT devices in manufacturing environments?

The following paragraphs contain details of the four main themes identified by this study. I used data triangulation to analyze data collected from semi structured interviews with participants, member checking notes, and the organization's documents. I imported the interview transcripts and organizational documents into NVivo for exploration and analysis. According to Zamawe (2015), Nvivo can assist with and accelerate data analysis; NVivo can also be used in place of manual and paper-based techniques for data analysis, including coding and thematic identification (Woods et al., 2016). Also, NVivo has many tools to assist researchers in data synthesis and determining the relevance and significance of data (Houghton et al., 2016). The four themes are linked to the study's conceptual framework, GST, and the literature review in the next section.

### Theme 1: A Collaborative Work Environment

A collaborative work environment was the first theme identified during data analysis. Recent literature confirms that a collaborative work environment fosters close working relationships between organizational members and contributes positively to organizational success (Abubakar et al., 2017). Wolf and Serpanos (2018) identified that security is traditionally an IT professionals concern while control systems are the electrical controls engineers' responsibilities. Both electrical controls engineers and IT professional groups must be involved in projects to securely implement IoT in

manufacturing environments. Additionally, roles and responsibilities between these two groups need to be clearly defined to achieve and maintain information security. Table 1 highlights the number of references to the theme collaborative work environment.

**Table 1**

*References to a Collaborative Work Environment*

| Major theme | Participant | | Document | |
|---|---|---|---|---|
| | Count | References | Count | References |
| Collaborative work environment | 8 | 112 | 6 | 46 |

The concept of a collaborative work environment was prevalent throughout the data. All eight participants commented on the importance of a collaborative working relationship between electrical controls engineers, IT professionals, and other stakeholders. When asked what strategies he used to securely implement IoT, C3P2 responded, “The main thing we need is a very good working relationship with IT.” C3P1 noted that a successful implementation includes participation from both IT and electrical controls engineers as each has their area of expertise. Engineers understand the production equipment controls, and IT understands networks and security. Six of the participants stated that a clear line of responsibilities for the controls engineers and IT is necessary to complete a successful IoT implementation; each working group needs to understand what part of the system the other is responsible for. The organizational document, C1D1, provides a straightforward process for identifying and assigning engineering and IT responsibilities when implementing system changes. C3D2 also demonstrates that individual responsibility for each working group is identified before IoT implementation.

Interestingly, two of the cases had individuals who had worked in one profession, either as a controls engineer or an IT professional, and transitioned to work in the other profession full time. Both C1P3 and C2P1 discussed having a former controls engineer working as an IT professional as being very beneficial to the working relationship between the two groups because communications between them were far more effective. The importance of a collaborative work environment is repeated and throughout the data. The following section discusses a changing landscape in manufacturing that is requiring a collaborative work environment.

The data demonstrates that a changing landscape in manufacturing is driving the need for a collaborative work environment. Five participants stated the need for collaboration between electrical controls engineers and IT is brought on by a changing landscape in manufacturing. Both C1P1 and C2P2 stated that there is a blending of manufacturing control systems with business systems. The notion of these systems blending coincides with Boyes et al.'s (2018) findings that there is a convergence between operational technology, industrial control systems, and information and communication technology. The blending of the two systems is often accomplished using IoT. According to C2P2, engineers want to maintain and control the plant floor systems but not anything beyond the machine level, hence the need to have IT involvement in projects involving IoT. A changing landscape in manufacturing is making a collaborative work environment that fosters close working relationships among team members, in part due to the nature of ethernet-connected devices.

A second driver for the need for a collaborative working relationship is that, as identified by six participants, nearly all devices are now networked together via ethernet TCP/IP protocol. There was consensus in the data that controls engineers understand the protocol and how to establish a network, but IT professionals are the individuals who have the knowledge to secure an ethernet network. Participants from all three cases discussed using IoT TCP/IP networked devices to connect legacy systems with proprietary networks and little or no security to business networks. Having a significant number of TCP/IP devices is part of what necessitates a collaborative work environment. The theme of a collaborative work environment is prevalent in the literature as well.

The theme of the need for a collaborative work environment in general, and between electrical controls engineers and IT specifically, aligns with existing literature. A recent study by Ahmed et al. (2020) confirmed findings of another recent study by Abubakar et al. (2017) that collaboration between stakeholders leads to organizational success. Recent work by Alcaraz (2019) highlighted the importance of collaboration between operational technologists, including electrical controls engineers and IT, to secure IIoT. Wolf and Serpanos (2018) acknowledged that control engineers tend to leave security to IT professionals. C1P1 responded to the question of security as "I don't do security; IT does all of that." The idea that controls engineers do not address security suggests that the two groups need to coordinate and collaborate on projects involving IoT. Participant C2P1 stated that "there is a constant battle between IT and engineers. IT wants to lock everything down … but we want everything opened up and talking to each other." C2P1's comment is consistent with Ashibani and Mahmoud's (2017) findings that

system availability takes precedence over confidentiality and manufacturing integrity. Gurtov et al. (2016) identified the gap between controls engineers and IT professionals as a challenge for the IIoT; it follows that a collaborative working relationship between these groups is beneficial for success. A need for a collaborative working relationship is well noted in the literature. The theme is also in alignment with GST, the conceptual framework for this study.

When viewing a manufacturing environment through the lens of GST, having a collaborative working environment will have an overall benefit to the organization. Eyers and Potter (2017) identified manufacturing as a system of systems that resides within organizational systems. As such, the electrical controls engineers and IT professionals can be viewed as individual systems, but each is also a subsystem of the overall organization or system. According to von Bertalanffy (1972), systems are interrelated and work to achieve common system goals. It could appear to some that electrical controls engineers and IT professionals have competing priorities. However, when viewed holistically via the GST perspective, each has its function that supports the overall system's goals and objectives. Systems also have clearly defined boundaries (von Bertalaffny, 1972). C1P2 confirmed this when stating, "We work on projects together, and we kind of say this is my part, this is your part, let's define our interface." When viewing this phenomenon through the lens of GST, findings from this study indicate that one strategy electrical controls engineers can use to securely implement IoT in manufacturing environments is to have a collaborative work environment. Other theories

considered as the conceptual framework for this study do have some relevancy to the theme of a collaborative work environment.

System dynamics and complexity theory are two other theories considered as a basis for this study and can serve to inform at least one component of the theme of a collaborative work environment. In the GST, all systems eventually reach an equilibrium state where each system performs its function (von Bertalanffy, 1972). However, as stated previously, one of the drivers for the theme of collaborative work environment is the changing landscape of manufacturing; this seems counter to the GST. While both are founded on the GST, system dynamics and complexity theory have significant differences from GST. They share that systems are ever-evolving, and this difference aligns with the changing landscape of manufacturing. Next follows a discussion of the second theme discovered in the data: employ existing cybersecurity practices.

**Theme 2: Employ Existing Cybersecurity Practices**

The second theme exposed during data analysis is the need to employ existing cybersecurity practices. All participants and four organizational documents referred to the need to engage standard cybersecurity practices such as network segmentation, confidentiality and authentication techniques, data backups, and virtualization technologies. These and other standard cybersecurity practices must be engaged as a minimum to securely implement IoT devices in manufacturing environments. Table 2 contains a listing of the number of references in the data to this theme.

**Table 2**

*References to Employ Existing Cybersecurity Practices*

| Major theme | Participant | | Document | |
|---|---|---|---|---|
| | Count | References | Count | References |
| Employ existing cybersecurity practices | 8 | 180 | 4 | 29 |

There is a minimum level of existing cybersecurity practices that must be employed. All participants discussed different cybersecurity practices throughout the interview. Ethernet network segmentation between the machine level network and the business network was a priority for all cases. Network segmentation was accomplished using managed switches or multiple ethernet network cards. For example, C1P2 stated, "I try to physically segment the network [with two network cards]. Another reason why I try to keep my stuff to limit my surface of exposure to their network because that adds another layer of defense." C2P1 said this about network segmentation "we have two networks, a local network, and a plant network and we have that as a separate isolated physical network on its own dedicated switches, its own dedicated copper wire." All eight participants identified the use of passwords and user/group policies to control access to technology. Four participants across two cases mentioned the use of firewalls to limit access. Seven of the participants discussed the use of policy and procedure to establish cybersecurity guidelines; all four of the organizational documents referenced above are examples of this. Five of the participants referred to data backup to ensure the availability of data in the case of loss. The need to employ a minimum level of existing

cybersecurity practices was prevalent in the data. Each case employed other existing cybersecurity practices.

All three cases had implemented a few more additional cybersecurity practices that are perhaps less common. None of the cases allow remote access to the machine network from offsite. Also, none of the cases allow access to the local machine via any wireless network. Finally, excluding limited use of RFID, none of the cases are using wireless devices in their control systems; C2P2 points to a lack of trust "wireless in industry, there's just not too many things in the short term that people are just going to go out there and trust. They don't trust things wirelessly". Case #1 and #3 had implemented virtual machines to keep a secure host environment. C3P3 describes the architecture: "they [IT] did give us a virtual machine that has all of our programming software…and we have admin over those, but that's the only part of the machine we have admin over is the virtual machines." Case #1 had implemented plant-wide intrusion detection and backup system for all the machine control devices that compared current data with daily snapshots for changes. The data demonstrate that existing cybersecurity practices must be employed to securely implement IoT devices in manufacturing environments. Existing literature supports this theme as well.

Theme #2 is well represented in the literature. According to Lezzi et al. (2018), some manufacturers are creating flat, unsegmented networks for their ICS. An unsegmented network had been the situation for Case #3, as C3P3 explains:

> that's [the network has] evolved a little bit since I've been here as we introduced more IoT devices…everything previously was on the same plant network. We had

> office computers, machines, program files access. All that stuff was on the same network. As we started introducing more IoT devices, the IT department then created a separate machine network for us; and installed a couple of switches so that we had our own network, so we didn't have all that traffic going on the same network. We segregated that out. That was kind of step one of the process.

A segmented network is the first line of defense as it prevents attack propagation and simplifies system monitoring (Corbo et al., 2018; Gurtov et al., 2016). Boiko et al. (2019) recently purported an adequately segmented network is necessary lest the network is easily exposed. Kobara (2016) identifies mandatory countermeasures for ICS LAN that include network segmentation, physical separation, limiting remote access, authentication, and intrusion detection systems. All three cases implemented many of these countermeasures as part of their IoT implementation. About whether there is network monitoring occurring on the ICS LAN, C1P1 noted,

> they [IT] know what's on every port, on every one of those switches routers. So if I go in and they got 20 ports on one of these cisco switches, if I plug in a laptop, I get a call in 10 minutes and saying hey, why did you do that? They're [IT is] watching all of the switches.

The theme of employing existing cybersecurity practices is common in the literature. This theme also aligns with the GST, as detailed in the next paragraph.

The GST lens supports the theme that employing existing cybersecurity practices is a strategy to securely implement IoT devices in manufacturing environments. In the GST, each phenomenon can be modeled as a system that is a subsystem of larger systems

with clearly identified boundaries (von Bertalaffny, 1972). Segmenting networks, as all cases in the study have completed, creates smaller network systems that are part of the overall network; more recent literature confirms that network segmentation simplifies information security for each individual network (Mhaskar et al., 2021). The GST also states that each system has inputs, outputs, and states (von Bertalaffny, 1972). When viewing the study's data in this manner, the individual IoT devices themselves have a state and are both inputs and outputs of the network segments in which they interact; however, when viewed more holistically by applying GST, the IoT devices and network segments, are subsystems within the manufacturing environment and employing existing cybersecurity practices enhances each component of the system. Employing existing cybersecurity practices aligns with the GST. The following section details how the SRP might add insight to the theme to employ existing cybersecurity practices.

The SRP is another theory I had considered for this study. I decided not to use this theory in part due to its limited scope. The GST allowed me to conduct the study with a holistic view; networks, network segments, and IoT devices have been identified as systems and subsystems. The SRP is a process model that might evaluate these systems and provide a strategy to employ existing cybersecurity practices to each of the systems. Another theme identified by this is study is that adequate resources must exist to maintain security.

**Theme 3: Adequate Resources Must Exist to Maintain Security.**

The next theme to emerge during data analysis was that adequate resources must exist to maintain security. The participant's discussed resources primarily in terms of

personnel or people and technical resources. Adequate resources in both areas must exist to securely implement IoT in manufacturing environments. Table 3 highlights the number of references to the theme that adequate resources must exist to maintain security.

**Table 3**

*References to Adequate Resources Must Exist*

| Major theme | Participant | | Document | |
|---|---|---|---|---|
| | Count | References | Count | References |
| Adequate resources must exist | 8 | 157 | 4 | 34 |

The data supports that adequate personnel resources must exist to maintain security. All eight of the participants commented on the need to have sufficient resources to maintain security. Six participants, across all three cases, commented on the need to have an adequate number of trained and qualified people to implement and maintain IoT in manufacturing. When asked about IoT implementation projects that did not go well and why, C1P1 stated, “my opinion is the problem is that the knowledge and the motivation, the typical maintenance person is not skilled enough to support this rapid advancement of technology,” referring to a lack of an adequate number of electrical controls engineers available for projects. C3P3 stated that having enough personnel resources to design and engineer IoT implementations allows for improved system simplicity. Five participants across all three cases stated that system simplicity is a primary factor in their design considerations because simplicity improves reliability and ease of maintenance. Six participants spanning all cases acknowledged the need for external personnel resources such as contractors, vendors, and consultants in many IoT implementations. Participant C1P2 stated about using external personnel resources: “let

the experts do their part and then figure out how best to work together." Organization documents C2D2 and C3D1 identify desired skillsets of sought-after external personnel resources. The need for adequate personnel resources to maintain security is represented in the data from this study.

Technological resources were another necessity identified by the participants to maintain security. C1P3 stated IoT system availability is limited by the resources in the IoT device itself: "usually the first thing we'll run into is you'll exceed the number of packets per second that a network card or something in our racks [IoT device] will handle." C3P1 stated that IoT device resources limit the solutions that the technology can provide. Five participants spanning all cases noted that IoT systems generally fail due to the inability to process the desired amount of data in the expected timeframes. The IoT systems that fail lack the necessary technical resources; either the devices themselves are too limited, or the entire system is under-engineered with fewer technical resources than is necessary. Organizational documents C1D2, C2D3, and C3D1 provide further evidence by providing technical performance specifications (storage, data traffic, network allocation) for IoT projects. The literature contains data that aligns with the theme of having adequate resources.

The theme of having adequate resources is a must to maintain security is well represented in the literature. Gurtov et al. (2016) proposed two types of resources, personnel, and equipment necessary for the successful integration of industrial and business systems. Many recent researchers, including Alaba et al.(2017), Amaran et al. (2018), Khan and Salah (2018), Lin and Bergmann (2016), and Randhawa et al. (2019),

identify the lack of resources in the IoT is a security concern. Gupta and Quamara (2020) build on previous work to provide a taxonomy of challenges related to lack of resources in the IoT; additionally, Gupta and Quamara (2020) provide further discussion on the device, architectural, and protocol challenges related to IoT's inadequate resources. The literature contains data on the significance and importance of adequate resources in the IoT. The next section demonstrates that Theme 3 aligns with the GST.

The theme of having adequate resources is a must to maintain security aligns with the GST, the conceptual framework for this study. A key tenet for GST is that a system is only functioning at its highest efficiency when all individual parts of the system are operating properly (von Bertalannffy, 1972). If a part of the system lacks adequate resources to perform its function, that system does not function efficiently as a whole. C3P2 highlighted an implementation where the ethernet nodes could not handle all the required network traffic; in that case, they segmented the network to accommodate the limited bandwidth of the IoT networked devices. Personnel can be modeled as a resource. For example, Oesterreich and Teuteberg (2018) included customers and suppliers in their GST founded study building information management systems. For this study, I viewed both personnel and technical resources as components of the manufacturing systems; a lack of resources impacts the system's overall ability to complete its goals and objectives. The theme of adequate resources is a must to maintain security aligns with existing literature. System dynamics theory provides some understanding of this theme as well.

System dynamics is another theory I considered as a conceptual framework for this study. One role of system dynamics is to understand a complex system's behavior to

simulate the system with a model (Hjorth & Bagheri, 2006); two of the five properties of a system according to Hjorth Bagheri (2006), are limited certainty and predictability. When a system does not have adequate resources, the certainty that it will perform predictably is compromised. Thus, when the IoT is implemented without adequate resources, it becomes difficult to model and simulate as it is not reliable, and therefore security is diminished. System dynamics can provide further insight into the challenges of not having enough resources and how security is impacted. The final theme to emerge during data analysis is learning and education.

**Theme 4: Learning and Education**

The final theme to be exposed during data analysis is the need for continued learning and education to securely implement IoT devices in manufacturing environments. All eight participants discussed the need for continued learning and education to keep pace with changing and evolving technologies and threats. Table 4 illustrates the number of references to the theme of learning and education.

**Table 4**

*References to Learning and Education*

| Major theme | Participant | | Document | |
|---|---|---|---|---|
| | Count | References | Count | References |
| Learning and education | 8 | 71 | 5 | 26 |

Organizational proffered learning and education was in the data as an essential factor to securely implement IoT devices in manufacturing environments. All eight participants made references to learning and education during their interviews. Three participants mentioned the importance of understanding how IoT devices respond to or

interact with the industrial controls hardware. C3P3 stated one implementation suffered from “install personnel not understanding the importance of separating the IoT network cables from power … there were some ghosts that we were chasing as far as intermittent signals dropping out or devices not changing state”. As a result, all maintenance and electrical control engineers were required to complete a curriculum identified in C3D2 to learn more about network susceptibility. C1P1, C2P1, and C2P3 mentioned the importance of mentoring younger engineers to learn from their experience. C2P1 stated, “I train and mentor my group and bring them up to speed … on what is the best method for that application.” Four participants spanning all three cases, each with more than a decade of electrical controls engineering experience, stressed the importance of life-long learning to understand and implement new technology in manufacturing environments. The data supports that organizational-sponsored learning and education are necessary to securely implement IoT devices in manufacturing environments. Learning and education beyond internal resources are of value as well.

It surfaced that learning and education that originates from external resources is a valuable component of this theme. Three participants mentioned the value of vendor or external training in learning about new IoT devices and technology. C3P1 appreciated learning from a vendor: “We did have training through our vendor … also gives more of an in-depth knowledge of it [IoT camera] because there’s a lot of different tools you can use that you’re not aware of.” C2P2 also identified the lack of ubiquitous higher educational opportunities for industrial controls engineering as a hindrance to implementing IoT devices in manufacturing environments. Notably, only two of the

participants had academic degrees explicitly related to industrial controls; all other participants had degrees in tangential engineering disciplines. Due to the number of references in the data and its relevance significance, learning and education surfaced as the fourth theme for this study. Learning and education are apparent in the existing literature.

Learning and education to stay knowledgeable of manufacturing and IoT is well represented as significant in academic literature. All eight participants discussed the continuously changing environment in industrial controls and the IoT and the need for learning and education to address the environmental changes. C1P2 specifically discussed an evolution from simple controls to IoT devices' addition to detect pH levels as part of the organization's legal compliance activities as an example of how industrial controls have evolved. The notion of a continuously changing environment is widely represented in the literature. For example, Baskaran et al. (2019), Griffy-Brown et al. (2019), and Tuptuk and Hailes (2018) each identified IoT as an emerging technology that is rapidly changing and evolving. The rapid growth and evolution of the IoT have been identified as a security risk (Abomhara & Geir, 2015); this is later confirmed in a more recent study by Gupta and Quamara (2020). A recent study by Ryan and Watson (2017) recommended further education to stay abreast of the changing IoT. The need for learning and education regarding rapidly changing manufacturing and IoT is a necessity for learning and education for increased information security posture.

The concept of education to increase information security posture is contained in the literature as well. Boutwell (2019) identified a security training program is vital to

protect critical infrastructure systems. Bryan (2020) recently confirmed the importance of information security training as an effective strategy for security. Similarly, Griffin (2017) identified security awareness as a strategy to prevent data breaches by mobile devices. The theme of education and learning aligns with data in the literature. The following section demonstrates that theme #4 aligns with the study's conceptual framework, GST.

When viewed through the lens of GST, learning and education are an intricate part of the manufacturing ecosystem. Like Theme 1, I viewed personnel as subsystems that are part of the overall manufacturing system. It behooves organizations to invest in their personnel resources, as evidenced by Theme 3, and adequate resources must exist to maintain security. Additionally, a recent study finds that employee training fosters better continuous improvement, and enhanced continuous improvement leads to greater efficiencies (van Assen, 2020); according to Duan et al. (2018), improved production efficiency is one goal of the IIoT. Additionally, Mira and Odeh (2019) found that employee training enhances employee satisfaction and, subsequently, performance. The GST defines systems as having inputs and outputs (van Bertalaffy, 1972). When viewing learning and education with a GST perspective, learning and education become inputs, and improved efficiencies and employee performance become outputs. The theme of learning and education is in alignment with the GST. The TAM theory may expand the theme of learning and education.

Using the TAM might provide an opportunity to employ the theme of learning and education. As previously stated, none of the cases are using wireless networks in any

significant way in their ICS; C2P2 offered a lack of trust in wireless technology as an explanation. Also, none of the cases allow remote access to the ICS from off-site. C1P2 agrees that disallowing is remote access is more secure, but "it makes work more difficult. I remember spending two or three hours on the phone because it just takes longer to walk people through things when you can't see what they see. Access is an issue." The TAM states that technology is dependent on the perceived ease of use and perceived usefulness of that technology (Davis, 1986). Conceivably, with proper learning and education curricula, the perceived ease of use of wireless technology in a secure manner would allow the electrical controls engineers to employ wireless technology solutions comfortably. With proper learning and education, IT might allow remote access to the ICS if they fully understood the usefulness of remote access for the electrical controls engineers. TAM helps speculate how learning and education might further enhance capabilities in manufacturing environments. The next section details how these themes apply to professional practice.

## Applications to Professional Practice

The specific IT problem I sought to research with this study is the perceived lack of strategies electrical controls engineers can use to securely implement IoT in manufacturing environments. While the participating organizations in this study included three manufacturers from the Midwest region of the United States, the strategies uncovered by the study may be more broadly applicable to manufacturers in the other areas of the United States and perhaps even globally. The study participants were all very knowledgeable of industrial control systems, IoT, and their capabilities in the field of

information security; the strategies identified by the data they presented demonstrate there are strategies electrical controls engineers can use to securely implement IoT in manufacturing environments. Unsurprisingly, the strategies apply to both electrical controls and IT professionals.

The themes identified in this study apply to both electrical controls and IT professionals. Since much of the IoT in manufacturing stems from a convergence of manufacturing systems and business systems, the strategies apply to both professional disciplines. Electrical controls engineers maintain the manufacturing systems while the IT professionals maintain the business systems. Electrical controls engineers and IT professionals each have a role to properly use the strategies to improve the cybersecurity posture in manufacturing environments. Working together collaboratively, electrical controls engineers and IT professionals can employ existing cybersecurity practices and ensure adequate resources are made available to IoT in manufacturing environments. Finally, both electrical controls engineers and IT professionals should endeavor to achieve life-long learning and education to be effective practitioners of their respective disciplines. The strategies have the potential to support positive social change.

## Implications for Social Change

Employing the strategies in this study can elicit positive social change by increasing manufacturing company's profits in two significant ways. First, the average cost of a single data breach is $3.86 million as of 2020 (IBM, 2020). If manufacturers experience data breaches, then their profits will be diminished. Second, manufacturers are implementing IoT devices to increase efficiencies. If production efficiency is improved,

then manufacturing costs decline and profits increase. Socially responsible manufacturing companies will provide more community support and increased wages and benefits to their employees as profits rise. When employees have increased wages and benefits, their spending power increases, and economic growth occurs. Additionally, employees with economic means will increase donations to nonprofit social agencies. Increased manufacturing profits can provide positive social change; implementing IoT securely in manufacturing environments has the potential to produce a physically safer work environment.

Ensuring that IoT is implemented securely in manufacturing environments can enhance the physical safety of personnel and equipment. One attribute of ICS, or cyber-physical system, is that they control real-world devices and equipment (Ashibani & Mahmoud, 2017). If the security of these systems is compromised and a bad actor gains access or control of the ICS, then that actor may be able to cause significant damage to the equipment or even jeopardize the safety of personnel. Strategies identified in this study can create positive social change by enhancing the physical safety of personnel and equipment. Some actions can be taken to ensure maximum advantage is achieved from the results of this study.

## Recommendations for Action

The findings of this study are useful for a variety of stakeholders. Engineering and IT managers might benefit from Theme 1, a collaborative work environment, as leaders directly impact the work environment and culture. The same managers should also heed the strategy of adequate resources must exist. Electrical controls engineers and IT

professionals are the individuals that would employ existing cybersecurity practices. Learning and education apply to all stakeholders. Each stakeholder group can evaluate the strategies, contextualize them to their environment, and implement them as applicable. Disseminating these findings is also something in which I will endeavor.

The findings from this study will be disseminated using several venues. First, the study will be published in the Proquest database. The publication will be available to other academic scholars and IT professionals for review. Second, the college where I work hosts the Advanced Manufacturing Consortium (AMC) for our region. The AMC has nearly 70 local manufacturers as its membership. Once the CAO has approved the study, I will conduct a four-part series with the AMC, present the study, and identify the strategies identified to their membership. Third, I will also create a two-page executive summary of the study and distribute it to the study participants for review. Finally, I will seek opportunities to present the material at various conferences that I attend each year as part of my work. While this study did identify strategies to securely implement IoT in manufacturing environments, more research is needed.

## Recommendations for Further Study

I, along with many examples in the literature, recommend continued research in IoT, IIoT, Industry 4.0, and the smart factory. These fields are emerging and evolving continually, and continued academic research is necessary to address the challenges presented by these technologies. I am interested in pursuing Theme 1, a collaborative work environment, further as I am interested in the human aspect of cybersecurity; I am also a student of leadership. There is a great opportunity to learn more about the

convergence of human behavior and the dichotomy of manufacturing: production efficiency and availability, and the need to adhere to cybersecurity practices. The technical aspects of IoT and manufacturing should also continue to be studied by academic scholars.

There are many examples in the literature that produce potential technical solutions for cybersecurity in the IoT. However, there is no one solution or even category of solutions that have been established as best practices. Researchers have attempted to address the limited resources in IoT by improved processes for encryption, authentication, and identification. Researchers have also been thoughtful in creating models and taxonomy for the IoT to simplify understanding and implementation of the IoT. One area of necessary research is to conduct a survey on the literature regarding IIoT, Industry 4.0, and the smart factory to create a central marshaling document with currently available solutions. Another needed study is a case study where solutions are implemented and tested in manufacturing environments to measure and report their effectiveness; a study of this nature would move past theory and practice. I have reflected on my experience with this study, and I have certainly grown and changed due to this process.

## Reflections

I have several reflections that manifested as a result of having performed this study. First, I have begun keeping a journal as part of my daily habit; I found the reflexive journal to be a powerful tool to enhance understanding and help concluding with little or no bias to steer my thinking in a specific direction. Second, theme #1, a

collaborative work environment, was a surprise to me because I experienced the exact opposite when I worked in manufacturing as an electrical controls engineer; I am pleased to learn that these two professions have begun working collaboratively to solve problems together. Themes 2-4 were not surprising to me and served to confirm initial thoughts based on my personal experience and the findings of themes in the literature review. Having performed this study has improved my daily work as a community college executive and an IT consultant in manufacturing.

My ability to perform my duties and responsibilities as a community college executive and IT consultant have been enhanced by completing this study. Admittedly, a doctoral degree in and of itself does not garner respect; however, I find it is easier to connect with faculty now that I have conducted a study with the full academic rigor of terminal degree research. Now, there is a bit of a shared experience in which the faculty and I can draw upon to better relate to each other, strengthening our relationship. Another way this study has helped me is the enhanced ability to perform data triangulation and thematic analysis. I recently conducted 31 interviews with college personnel as part of a strategic planning effort; these interviews provided 106 individual thoughts on goals for next year. I was able to garner four themes from these ideas using thematic analysis. Finally, as an IT consultant, I can speak confidently on cybersecurity strategies employed in manufacturing environments.

## Summary and Study Conclusions

The ability to securely implement IoT in manufacturing environments does not come with a straightforward strategy or a small subset of stakeholders. The IoT and

manufacturing environments are ever-changing, and securely implementing IoT requires diligence for continued solutions development and effort by many stakeholders. Technology leaders, both engineering and IT, must be committed to cybersecurity in their manufacturing environment to create a collaborative work environment and the employment of other strategies discovered by this study. However, this work is worthwhile as it enhances the effectiveness and efficiency of manufacturing processes, thereby creating a safer and more beneficial experience for all involved.

# References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa*, *19*(1), 66-98. https://doi.org/https://doi.org/10.13058/raep.2018.v19n1.578

Abdmeziem, M. R., & Tandjaoui, D. (2015). An end-to-end secure key management protocol for e-health applications. *Computers and Electrical Engineering*, *44*, 184–197. https://doi.org/10.1016/j.compeleceng.2015.03.030

Abomhara, M., & Geir, K. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders, and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Abubakar, A. M., Elrehail, H., Alatailat, M. A., & Elçi, A. (2017). Knowledge management, decision-making style and organizational performance. *Journal of Innovation & Knowledge*, *4*(2), 104-114. https://doi.org/10.1016/j.jik.2017.07.003

Ahmed, W., Ashraf, M. S., Khan, S. A., Kusi-Sarpong, S., Arhin, F. K., Kusi-Sarpong, H., & Najmi, A. (2020). Analyzing the impact of environmental collaboration among supply chain stakeholders on a firm's sustainable performance. *Operations Management Research*, 1-18. https://doi.org/10.1007/s12063-020-00152-1

Alaba, F., Othman, M., Hashem, I., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Alcaraz, C. (2019). Secure interconnection of IT-OT networks in industry 4.0. In *Critical*

*infrastructure security and resilience* (pp. 201-217). Springer, Cham. https://doi.org/10.1007/978-3-030-00024-0_11

Aldiabat, K. M., & Le Navenec, C. -L. (2018). Data saturation: The mysterious step in grounded theory method. *The Qualitative Report*, *23*(1), 245-261. https://doi.org/10.46743/2160-3715/2018.2994

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). AL-FA-Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communication Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.5752/P.2316-9451.2013v1n2p78

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*(May), 56–65. https://doi.org/10.1016/j.cose.2014.01.005

Almomani, I., Al-Kasasbeh, B., & Al-Akhras, M. (2016). WSN-DS: A dataset for Intrusion Detection Systems in Wireless Sensor Networks. *Journal of Sensors, 2016*. https://doi.org/10.1155/2016/4731953

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23*(3), 121-127. http://tuckerpub.com/jcd.htm

Amaran, M. H., Rohmad, M. S., Adnan, L. H., Mohamed, N. N., & Hashim, H. (2018). Lightweight security for MQTT-SN. *International Journal of Engineering and*

*Technology, 7*(4), 223–226. https://doi.org/10.14419/ijet.v7i4.11.20811

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in Internet of Things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2), 99–109. https://doi.org/10.1109/TMSCS.2015.2498605

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers and Security, 68*, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report, 22*(6), 1607-1621. https://doi.org/10.46743/2160-3715/2017.2674

Azevedo, B. B., & Saurin, T. A. (2018). Losses in water distribution systems: A complexity theory perspective. *Water Resources Management, 32*(9), 2919–2936. https://doi.org/10.1007/s11269-018-1976-7

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5

Barnaghi, P., Wang, W., Henson, C., & Taylor, K. (2012). Semantics for the Internet of Things. *International Journal on Semantic Web and Information Systems, 8*(1), 1–21. https://doi.org/10.4018/jswis.2012010101

Basile, G., Kaufmann, H. R., & Savastano, M. (2018). Revisiting complexity theory to achieve strategic intelligence. *International Journal of Foresight and Innovation Policy, 13*(1–2), 57–70. https://doi.org/10.1504/IJFIP.2018.095858

Baskarada, S. (2014). Qualitative case study guidelines. *The Qualitative Report, 19*(40), 1-18. https://doi.org/10.46743/2160-3715/2014.1008

Baskaran, S. B. M., Arumugam, S., & Prasad, A. R. (2019). Internet of Things security. *Journal of ICT Standardization*, *7*(1), 21–42. https://doi.org/10.13052/jicts2245-800X.712

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLOS ONE*, *11*(9), 1-33. https://doi.org/10.1371/journal.pone.0163050

Bi, Z., Da Xu, L., & Wang, C. (2014). Internet of Things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics, 10*(2), 1537–1546. https://doi.org/10.1109/TII.2014.2300338

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Computer Science, 149*, 65-70. https://doi.org/ 10.1016/j.procs.2019.01.108

Bolbot, V., Theotokatos, G., Bujorianu, L. M., Boulougouris, E., & Vassalos, D. (2019). Vulnerabilities and safety assurance methods in cyber-physical systems: A comprehensive review. *Reliability Engineering and System Safety, 182*(March 2018), 179–193. https://doi.org/10.1016/j.ress.2018.09.004

Boutwell, M. (2019). *Exploring industry cybersecurity strategy in protecting critical infrastructure* [Doctoral Study]. Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/7965/

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*(March), 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Bridgen, S. (2017). Using systems theory to understand the identity of academic advising: A case study. *NACADA Journal*, *37*(2), 9–20. https://doi.org/10.12930/NACADA-15-038

Brinzer, B., Banerjee, A., & Hauth, M. (2017). Complexity thinking and cyber-physical systems. *International Journal of Industrial Engineering*, *4*(1), 14–20. https://doi.org/10.14445/23499362/ijie-v4i1p103

Bristowe, K., Selman, L., & Murtagh, F. (2015). Qualitative research methods in renal medicine: An introduction. *Nephrology Dialysis Transplantation*, *30*(9), 1424–1431, https://doi.org/10.1093/ndt/gfu410

Broks, A. (2016). Systems theory of systems thinking: General and particular within modern science and technology education. *Journal of Baltic Science Education*, *15*(4), 408–410. http://www.scientiasocialis.lt/jbse/files/pdf/vol15/408-410.Broks_JBSE_Vol.15_No.4.pdf

Bryan, L. L. (2020). Effective information security strategies for small business. *International Journal of Cyber Criminology*, *14*(1), 341-360. https://doi.org/10.5281/zenodo.3760328

Burg, A., Chattopadhyay, A., & Lam, K. Y. (2017). Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. *Proceedings of the IEEE*, *106*(1), 38-60.

https://doi.org/10.1109/JPROC.2017.2780172

Cairney, P. (2012). Complexity Theory in political science and public policy. *Political Studies Review, 10*(3), 346–358. https://doi.org/10.1111/j.1478-9302.2012.00270.x

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. *IT Professional*, 18(2), 22–30. https://doi.org/10.1109/MITP.2016.27

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*(5), 811-830. https://nsuworks.nova.edu/tqr/vol21/iss5/2

Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., & Yin, B. (2017). Smart factory of industry 4.0: Key technologies, application case, and challenges. *IEEE Access*, *6*, 6505–6519. https://doi.org/10.1109/ACCESS.2017.2783682

Chen, H. C., You, I., Weng, C. E., Cheng, C. H., & Huang, Y. F. (2016). A security gateway application for End-to-End M2M communications. *Computer Standards and Interfaces*, *44*, 85–93. https://doi.org/10.1016/j.csi.2015.09.001

Connelly, L. M. (2016). Trustworthiness in qualitative research. *MEDSURG Nursing, 25*(6), 435–436.

Cook, D. A., Kuper, A., Hatala, R., & Ginsburg, S. (2016). When assessment data are words: validity evidence for qualitative educational assessments. *Academic Medicine*, *91*(10), 1359-1369. https://doi.org/ 10.1097/ACM.0000000000001175

Corbo, G., Foglietta, C., Palazzo, C., & Panzieri, S. (2018). Smart Behavioural Filter for

Industrial Internet of Things: A Security Extension for PLC. *Mobile Networks and Applications*, *23*(4), 809–816. https://doi.org/10.1007/s11036-017-0882-1

Da Mota Pedrosa, A., Naslund, D., & Jasmand, C. (2012). Logistics case study based research: Towards higher quality. *International Journal of Physical Distribution & Logistics Management*, *42*, 275-295. https://doi.org/10.1108/09600031211225963

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end- user information systems: Theory and results* [Doctoral Dissertation]. Massachusetts Institute of Technology).

Demetis, D. S., & Lee, A. S. (2016). Crafting theory to satisfy the requirements of systems science. *Information and Organization*, *26*(4), 116–126. https://doi.org/10.1016/j.infoandorg.2016.09.002

Demetis, D. S., & Lee, A. S. (2017). Taking the first step with systems theorizing in information systems: A response. *Information and Organization*, *27*(3), 163-170. https://doi.org/10.1016/j.infoandorg.2017.06.003

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods.* New York, NY: McGraw-Hill.

Dinculeana, D., & Cheng, X. (2019). Vulnerabilities and limitations of MQTT protocol used between IoT devices. *Applied Sciences (Switzerland)*, *9*(5). https://doi.org/10.3390/app9050848

Dolezal, O., & Tomaskova, H. (2019). Czech cyber security systems from a view of system dynamics. *Journal of Cyber Security and Mobility*, *8*(2), 241–260.

https://doi.org/10.13052/jcsm2245-1439.824

Domenech Rodriguez, M. M., Corralejo, S. M., Vouvalis, N., & Mirly, A. K. (2017). Institutional review board: Ally not adversary. *Psi Chi Journal Of Psychological Research*, *22*(2), 76-84. https://doi.org/10.24839/2325-7342.JN22.2.76

Drack, M., & Schwarz, G. (2010). Recent developments in general system theory. *Systems Research and Behavioral Science*, 27, 601-610. https://doi.org/10.1002/sres.1013

Draper, J. (2015). Ethnography: Principles, practice and potential. *Nursing Standard*, *29*(36), 36– 41. https://doi.org/10.7748/ns.29.36.36.e8937

Duan, Y., Luo, Y., Li, W., Pace, P., Aloi, G., & Fortino, G. (2018). A collaborative task-oriented scheduling driven routing approach for industrial IoT based on mobile devices. Ad Hoc Networks, 81, 86-99. https://doi.org/10.1016/j.adhoc.2018.07.022

El Hussein, M., Jakubec, S. L., & Osuji, J. (2015). The FACTS: A mnemonic for the rapid assessment of rigor in qualitative research studies. *The Qualitative Report*, *20*, 1182–1184. https://doi.org/10.3928/01484834-20151214-15

Emblemsvag, J. (2020). Risk and complexity – on complex risk management. *Journal of Risk Finance, 21*(1), 37–54. https://doi.org/10.1108/JRF-09-2019-0165

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4. https://doi.org/ 10.11648/j.ajtas.20160501.11

Eyers, D. R., & Potter, A. T. (2017). Industrial additive manufacturing: A manufacturing

systems perspective. *Computers in Industry, 92–93,* 208–218. https://doi.org/10.1016/j.compind.2017.08.002

Farooq, M., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7), 1–6. https://doi.org/10.5120/19547-1280

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management and Computer Security*, *22*(5), 410–430. https://doi.org/ 10.1108/IMCS-07-2013-0053

Forrester, J. W. (1961). *Industrial dynamics*. Cambridge, MA, MIT Press.

Forrester, J. W. (2007). System dynamics - the next fifty years. *System Dynamics Review, 23*(August), 1–15. https://doi.org/10.1002/sdr.381

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408–1416. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss9/3

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report, 20*(11), 1772–789. https://nsuworks.nova.edu/tqr/vol20/iss11/5

Gentles, S. J., & Vilches, S. L. (2017). Calling for a shared understanding of sampling terminology in qualitative research: Proposed clarifications derived from critical analysis of a methods overview by McCrae and Purssell. *International Journal of Qualitative Methods*, *16*(1), https://doi.org/10.1177/1609406917725678

Gill, M. J. (2014). The possibilities of phenomenology for organizational research.

*Organizational Research Methods*, *17*(2), 118–137. https://doi.org/10.1177/1094428113518348

Granjal, J., & Pedroso, A. (2018). An intrusion detection and prevention framework for internet-integrated CoAP WSN. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/1753897

Griffin, T. (2017). *Strategies to prevent security breaches caused by mobile devices.* [Doctoral Study]. Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/4628/

Griffy-Brown, C., Lazarikos, D., & Chun, M. (2019). Emerging technologies and cyber risk: How do we secure the Internet of Things (IoT) environment? *Journal of Applied Business and Economics*, *21*(2), 70–79. https://doi.org/10.33423/jabe.v21i1.1455

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and computation: Practice and experience, 32(21), e4946. https://doi.org/10.1002/cpe.4946

Gurtov, A., Liyanage, M., & Korzun, D. (2016). Secure communication and data processing challenges in the industrial internet. *Baltic Journal of Modern Computing*, *4*(4), 1058–1073. https://doi.org/10.22364/bjmc.2016.4.4.28

Haimes, Y., Horowitz, B., Guo, Z., Andrijcic, E., & Bogdanor, J. (2015). Assessing

systemic risk to cloud-computing technology as complex interconnected systems of systems. *Systems engineering, 18*(3), 284-299. https://doi.org/10.1002/sys.21303

Hammond, D. (2010). *Science of synthesis: Exploring the social implications of general systems theory*. Boulder, CO: University Press of Colorado

Harvey, L. (2015). Beyond member checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, 38, 23-38. https://doi.org/10.1080/1743727X.2014.914487

Hernandez Ramos, S., Villalba, M. T., & Lacuesta, R. (2018). MQTT Security: A novel fuzzing approach. *Wireless Communications and Mobile Computing*, *2018*, 1–11. https://doi.org/10.1155/2018/8261746

Hjorth, P., & Bagheri, A. (2006). Navigating towards sustainable development: A system dynamics approach. *Futures*, *38*(1), 74–92. https://doi.org/10.1016/j.futures.2005.04.005

Homer, J. (2007). System dynamics review. *System Dynamics Review*, *23*(4), 465–467. https://doi.org/10.1002/sdr.388

Hou, J. L., & Yeh, K. H. (2015). Novel authentication schemes for IoT based healthcare Systems. *International Journal of Distributed Sensor Networks*, *2015*, 1–9. https://doi.org/10.1155/2015/183659

Houghton, C., Murphy, K., Meehan, B., Thomas, J., Brooker, D., & Casey, D. (2016). From screening to synthesis: using Nvivo to enhance transparency in qualitative evidence synthesis. *Journal of clinical nursing*, *26*(5-6), 873-881.

https://doi.org/10.1111/jocn.13443

Huberman, B. (2016). Ensuring trust and security in the industrial IoT: the internet of things. *Ubiquity*, *291*(January), 1–7. https://doi.org/10.1145/2822883

IBM (2020). *Cost of a data breach report.* https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

ISO 27005 (2013). *Information technology – security techniques - security risk management*.

Jacob, S. A., & Furgerson, S. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report, 17*(42), 1-10. https://nsuworks.nova.edu/tqr/vol17/iss42/3

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jansen, W. (2009). *Directions in security metrics research* (NISTIR 7564). https://doi.org/10.6028/NIST.IR.7564

Jiang, W., Wang, Y., Jiang, Y., Xu, Y., Chen, J., Tan, L., & Liang, G. (2019). Mobile internet mobile agent system dynamic trust model for cloud computing. *Computers, Materials & Continua*, *61*(3), 123–136. https://doi.org/10.32604/cmc.2020.05933

Kamin, D. (2017). *Exploring security, privacy, and reliability strategies to enable the adoption of IoT*. [Doctoral Study]. Walden Dissertations and Doctoral Studies.

https://scholarworks.waldenu.edu/4382/

Kern, F. G. (2018). The trials and tribulations of applied triangulation: Weighing different data sources. *Journal of Mixed Methods Research*, *12*(2), 166–181. https://doi.org/10.1177/1558689816651032

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *2012 10th International Conference on Frontiers of Information Technology (FIT)* (pp. 257–260). https://doi.org/10.1109/FIT.2012.53

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. Future Generation Computer Systems, 100, 144–164. https://doi.org/10.1016/j.future.2019.04.038

Kobara, K. (2016). Cyber physical security for industrial control systems and IoT. *IEICE Transactions on Information and Systems*, *E99D*(4), 787–795. https://doi.org/10.1587/transinf.2015ICI0001

Kocakulak, M., & Butun, I. (2017). An overview of Wireless Sensor Networks towards internet of things. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017* (pp. 1–6). IEEE. https://doi.org/10.1109/CCWC.2017.7868374

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2018). Towards the

development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779–796. https://doi.org/10.1016/j.future.2019.05.041

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology. *Journal of Parapsychology*, *79*(2), 219–233. http://www.rhine.org/what-we-do/journal-of-parapsychology.html

Lee, J., Bagheri, B., & Kao, H. A. (2015). A Cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson.

Leusin, M., Frazzon, E., Uriona Maldonado, M., Kuck, M., & Freitag, M. (2018). Solving the Job-Shop Scheduling Problem in the Industry 4.0 Era. *Technologies*, *6*(4), 107. https://doi.org/10.3390/technologies6040107

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Li, K., Ma, T., Wei, G., Zhang, Y., & Feng, X. (2019). Urban industrial water supply and demand: System dynamic model and simulation based on Cobb-Douglas function. *Sustainability (Switzerland)*, *11*(21), 1–18. https://doi.org/10.3390/su11215893

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information (Switzerland)*, *7*(3).

https://doi.org/10.3390/info7030044

Liu, J., Chang, Q., Xiao, G., & Biller, S. (2012). The costs of downtime incidents in serial multistage manufacturing systems. *Journal of Manufacturing Science and Engineering*, *134*(2), 21016. https://doi.org/10.1115/1.4005789

Lloret-Climent, M., Nescolarde-Selva, J. A., Alonso-Stenberg, K., & Selva-Barthelemy, M. A. (2019). Causal analysis of the spanish industrial sector through Smarta. *IEEE Access*, *7*, 33556–33564. https://doi.org/10.1109/ACCESS.2019.2904242

Lowell, K. R. (2016). An application of complexity theory for guiding organizational change. *Psychologist-Manager Journal*, *19*(3–4), 148–181. https://doi.org/10.1037/mgr0000044

Mabila, T. t. (2017). Postgraduate students understanding of mixed methods research design at the proposal stage. *South African Journal Of Higher Education*, *31*(5), 136-153. https://doi.org/10.28535/31-5-1498

Malina, M. A., Norreklit, H. S. O., & Selto, F. H. (2011). Lessons learned: Advantages and disadvantages of mixed method research. *Qualitative Research in Accounting and Management*, *8*(1), 59-71. https://doi.org/10.1108/11766091111124702

Mannay, D., & Morgan, M. (2015). Doing ethnography or applying a qualitative technique? Reflections from the 'waiting field.' *Qualitative Research*, *15*(2), 166–182. https://doi.org/10.1177/1468794113517391

Manson, S. M. (2001). Simplifying complexity: A review of complexity theory. *Geoforum*, *32*(3), 405–414. https://doi.org/10.1016/S0016-7185(00)00035-X

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed

methods and choice based on the research. *Perfusion*, 30, 537-542. https://doi.org/10.1177/0267659114559116

McDermott, C., Isaacs, J., & Petrovski, A. (2019). Evaluating awareness and perception of botnet activity within consumer Internet of Things (IoT) Networks. *Informatics*, *6*(1), 8. https://doi.org/10.3390/informatics6010008

Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B. G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems*, *83*, 619–628. https://doi.org/10.1016/j.future.2017.04.039

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security*, *103*, 102162. https://doi.org/10.1016/j.cose.2020.102162

Mingers, J. (2017). Back to the future: A critique of Demetis and Lee's "Crafting theory to satisfy the requirements of systems science." *Information and Organization*, *27*(1), 67–71. https://doi.org/10.1016/j.infoandorg.2017.01.003

Mira, M., & Odeh, K. (2019). The mediating role of authentic leadership between the relationship of employee training and employee performance. Management Science Letters, 9(3), 381-388. https://doi.org/ 10.5267/j.msl.2018.12.011

Moore, T., McKee, K., & McCoughlin, P. (2015). Online focus groups and qualitative research in the social sciences: their merits and limitations in a study of housing and youth. *People, Place and Policy Online*, *9*(1), 17–28. https://doi.org/10.3351/ppp.0009.0001.0002

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*, 1212–1222. https://doi.org/10.1177/1049732315588501

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis, *European Journal of General Practice*, 24:1, 9-18, https://doi.org/ 10.1080/13814788.2017.1375091

Mourtzis, D., Vlachou, E., & Milas, N. (2016). Industrial big data as a result of IoT adoption in manufacturing. *Procedia CIRP*, 55, 290–295. https://doi.org/10.1016/j.procir.2016.07.038

Mukherjee, A. (2015). Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. In *Proceedings of the IEEE* (Vol. 103, pp. 1747–1761). IEEE. https://doi.org/10.1109/JPROC.2015.2466548

Nastase, L. (2017). Security in the Internet of Things: A survey on application layer protocols. *Proceedings - 2017 21st International Conference on Control Systems and Computer, CSCS 2017*, 659–666. https://doi.org/10.1109/CSCS.2017.101

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research.*, Washington, DC: U.S. Department of Health and Human Services. Retrieved from https://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

National Institute of Standards and Technology. (2012). *Guide for Conducting Risk*

*Assessments*. Gaithersburg, MD: Author.

Nazir, S., Patel, S., & Patel, D. (2017). Autonomic computing architecture for SCADA cyber security. *International Journal of Cognitive Informatics and Natural Intelligence*, *11*(4), 66–79. https://doi.org/10.4018/IJCINI.2017100104

Ng, I. C. L., & Wakenshaw, S. Y. L. (2017). The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing*, *34*(1), 3–21. https://doi.org/10.1016/j.ijresmar.2016.11.003

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ICS-07-2016-0061

Oesterreich, T., & Teuteberg, F. (2018). Looking at the big picture of IS investment appraisal through the lens of systems theory: A System dynamics approach for understanding the economic impact of BIM. *Computers in Industry, 99*(3), 262–281. https://doi.org/10.1016/j.compind.2018.03.029

Okwir, S., Nudurupati, S. S., Ginieis, M., & Angelis, J. (2018). Performance measurement and management systems: A perspective from complexity theory. *International Journal of Management Reviews*, *20*(3), 731–754. https://doi.org/10.1111/ijmr.12184

Orange, A. (2016). Encouraging reflective practices in doctoral students through research journals. *The Qualitative Report, 21*(12), 2176–2190. https://nsuworks.nova.edu/tqr/vol21/iss12/2

Orlikowski, W. J., & Robey, D. (1991). Information technology and the structuring of

organizations. Information systems research, 2(2), 143-169. https://doi.org/10.1287/isre.2.2.143

Oztemel, E., & Gursev, S. (2018). Literature review of Industry 4.0 and related technologies. *Journal of Intelligent Manufacturing*, 1-56. https://doi.org/10.1007/s10845-018-1433-8

Palinkas, L., Horwitz, S., Green, C., Wisdom, J., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, *3*(10), 1–7. https://doi.org/10.15577/jmt.2016.03.01.1

Pasman, H. J., Knegtering, B., & Rogers, W. J. (2013). A holistic approach to control process safety risks: Possible ways forward. *Reliability Engineering and System Safety*, *117*, 21–29. https://doi.org/10.1016/j.ress.2013.03.010

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A Survey on systems security metrics. *ACM Computing Surveys*, *49*(4), 1–35. https://doi.org/10.1145/3005714

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, *13*, 1253–1260. https://doi.org/10.1016/j.promfg.2017.09.047

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. *Nurse Researcher (2014+), 22*(4), 6. https://doi.org/10.7748/nr.22.4.6.s2

Peticca-Harris, A., deGama, N., & Elias, S. R. S. T. A. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods, 19*(3), 376–401. https://doi.org/10.1177/1094428116629218

Pirbhulal, S., Zhang, H., Alahi, M. E. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y. T., & Wu, W. (2017). A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors*, *17*(1), 1–19. https://doi.org/10.3390/s17010069

Porambage, P., Braeken, A., Schmitt, C., Gurtov, A., Ylianttila, M., & Stiller, B. (2015). Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications. *IEEE Access*, *3*, 1503–1511. https://doi.org/10.1109/ACCESS.2015.2474705

Randhawa, R. H., Hameed, A., & Mian, A. N. (2019). Energy efficient cross-layer approach for object security of CoAP for IoT devices. *Ad Hoc Networks, 92*(November). https://doi.org/10.1016/j.adhoc.2018.09.006

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Razzaq, M., Gill, S., Qureshi, M., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6), 383–388.

https://doi.org/10.14569/ijacsa.2017.080650

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*(2018), 173–190. https://doi.org/10.1016/j.future.2018.05.046

Rimando, M., Brace, A. M., Namageyo-Funa, A., Parr, T. L., Sealy, D. A., Davis, T., Martinez, L., & Christiana, R. (2015). Data collection challenges and recommendations for early career researchers. *Qualitative Report*, *20*(12), 2025–2036. https://nsuworks.nova.edu/tqr/vol20/iss12/8

Rinke, C. R., & Mawhinney, L. (2014). Reconsidering rapport with urban teachers: Negotiating shifting boundaries and legitimizing support. *International Journal of Research and Method in Education*, *37*(1), 3–16. https://doi.org/10.1080/1743727X.2012.708924

Robey, D., & Abdalla Mikhaeil, C. (2016). Déjà Vu or art nouveau? A comment on Demetis and Lee's "Crafting theory to satisfy the requirements of systems science." *Information and Organization*, *26*(4), 127–130. https://doi.org/10.1016/j.infoandorg.2016.10.001

Rogers, E. (2003). *Diffusion of Innovations*. Fifth edition. Free Press: New York.

Rosenberg, J. M., & Koehler, M. J. (2015). Context and technological pedagogical content knowledge (TPACK): A systematic review. *Journal of Research on Technology in Education, 47*(3), 186–210. https://doi.org/10.1080/15391523.2015.1052663

Roulston, K., & Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative

research methods. *Qualitative Inquiry*, *21*(4), 332-342. https://doi.org/10.1177/1077800414563803

Ryan, P., & Watson, R. (2017). Research challenges for the Internet of Things: What role can OR play? *Systems* (Vol. 5). https://doi.org/10.3390/systems5010024

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*, 1375-1384. https://doi.org/10.1109/ACCESS.2016.2549047

Santaniello, T. P. (2018). *Active parental involvement and college and career readiness: A qualitative study* (dissertation). Rowan University. https://rdw.rowan.edu/cgi/viewcontent.cgi?article=3536&context=etd

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality and Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Schoenung, B., & Dikova, D. (2016). Reflections on organizational team diversity research : In search of a logical support to an assumption. *Equality, diversity And inclusion: An International Journal*, (3), 221. https://doi.org/10.1108/EDI-11-2015-0095

Schultze, U. (2017). What kind of world do we want to help make with our theories? *Information and Organization*, *27*(1), 60–66. https://doi.org/10.1016/j.infoandorg.2017.01.002

Seitz, S. (2016). Pixilated partnerships, overcoming obstacles in qualitative interviews via

Skype: A research note. *Qualitative Research, 16*(2), 229-235. https://doi.org/10.1177/1468794115577011

Sengupta, J., Ruj, S., & Das Bit, S. (2019). A Comprehensive survey on attacks, Security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications, 149*(April 2019), 102481. https://doi.org/10.1016/j.jnca.2019.102481

Shin, D., & Konrad, A. M. (2017). Causality between high-performance work systems and organizational performance. *Journal of Management*, *43*(4), 973–997. https://doi.org/10.1177/0149206314544746

Siddiqi, M. A., Mugheri, A. A., & Khoso, M. (2018). Analysis on security methods of Wireless Sensor Network (WSN). *Sukkur IBA Journal of Computing and Mathematical Sciences*, *2*(1), 52-60 http://journal.iba-suk.edu.pk:8089/SIBAJournals/index.php/sjcms

Sivabalan, S., & Radcliffe, P. J. (2017). Detecting IoT zombie attacks on web servers. In *27th International Telecommunication Networks and Applications Conference*, 1–3. https://doi.org/10.1109/ATNAC.2017.8215358

Slayton, R. (2016). What is the cyber offense-defense balance? *International Security, 41*(3), 72–109. https://doi.org/10.1162/ISEC_a_00267

Small, W., Maher, L., & Kerr, T. (2014). Institutional ethical review and ethnographic research involving injection drug users: a case study. *Social Science & Medicine, 104*, 157–162. https://doi.org/10.1016/j.socscimed.2013.12.010

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy

compliance model in organizations. *Computers and Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Soni, A., Upadhyay, R., & Kumar, A. (2019). Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging. *Physical Communication*, *33*, 249–258. https://doi.org/10.1016/j.phycom.2019.01.013

Stake, R. (1978). The case study method in social inquiry. *Educational Researcher*. https://doi.org/10.2307/1174340

Stanley, M., & Nayar, S. (2014). Methodological rigor: Ensuring quality in occupational therapy qualitative research. *New Zealand Journal of Occupational Therapy*, *61*(1), 6–12. https://doi.org/10.1080/14780887.2013.801543

Stockman, C. (2015). Achieving a doctorate through mixed methods research. *Electronic Journal Of Business Research Methods, 13*(2), 74-84. http://www.ejbrm.com/issue/download.html?idArticle=401

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22, 441-469. https://doi.org/10.2307/249551

Sullivan, J., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *Electricity Journal*, *30*(3), 30–35. https://doi.org/10.1016/j.tej.2017.02.006

Tan, L., & Wang, N. (2010). Future Internet: The Internet of Things. In *ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and*

*Engineering, Proceedings* (Vol. 5, pp. 376–380). IEEE. https://doi.org/10.1109/ICACTE.2010.5579543

Trafimow, D. (2014). Considering quantitative and qualitative issues together. *Qualitative Research in Psychology, 11*(1), 15-24. https://doi.org/10.1080/14780887.2012.743202

Trochim, W. M. K., & Donnelly, J. P. (2008). *The research methods knowledge base* (3rd ed.). Mason, OH: Cengage Learning.

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems, 47*(February), 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007

Turner, J. R., & Baker, R. M. (2019). Complexity Theory: An Overview with potential applications for the social sciences. *Systems, 7*(1), 4. https://doi.org/10.3390/systems7010004

Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. *Wireless Personal Communications, 95*(1), 169–185. https://doi.org/10.1007/s11277-017-4434-6

Udo, G., Bagchi, K., & Kirs, P. (2018). Analysis of the growth of security breaches: A multi-growth model approach. *Issues in Information Systems, 19*(4), 176–186. https://www.iacis.org/iis/iis_articles.php

van Assen, M. F. (2020). Training, employee involvement and continuous improvement–the moderating effect of a common improvement method. *Production Planning & Control, 32*(2), 132-144. https://doi.org/10.1080/09537287.2020.1716405

van de Wiel, M. J. (2017). Examining expertise using interviews and verbal protocols. *Frontline Learning Research, 5*(3), 112-140. https://doi.org/10.14786/flr.v5i3.257

Vargo, S., Koskela-Huotari, K., Baron, S., Edvardsson, B., Reynoso, J., & Colurcio, M. (2017). A systems perspective on markets – toward a research agenda. *Journal of Business Research, 79*, 260–268. https://doi.org/10.1016/j.jbusres.2017.03.011

von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15*(4), 407–426. https://doi.org/10.2307/255139

von Bertalanffy, L., Juarrero, A., & Rubino, C. (2008). An outline of general system theory. *Emergence: Complexity & Organization, 10*, 103-123. http://www.isce.edu/index-2.html

Von Der Tann, L., Collins, B., & Metje, N. (2016). Predetermined? - Systems thinking for the urban subsurface. *Procedia Engineering*, *165*, 355–363. https://doi.org/10.1016/j.proeng.2016.11.710

Wallace, C. L. (2016). Overcoming barriers in care for the dying: Theoretical analysis of an innovative program model. *Social Work in Health Care*, *55*(7), 503–517. https://doi.org/10.1080/00981389.2016.1183552

Wan, J., Yang, J., Wang, Z., & Hua, Q. (2018). Artificial intelligence for cloud-assisted smart factory. *IEEE Access*, *6*, 55419–55430. https://doi.org/10.1109/ACCESS.2018.2871724

Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing smart factory of Industrie 4.0: An Outlook. *International Journal of Distributed Sensor Networks*, *2016*. https://doi.org/10.1155/2016/3159805

Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2016). Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination. *Computer Networks*, *101*, 158–168. https://doi.org/10.1016/j.comnet.2015.12.017

Wang, Y., Shi, S., Nevo, S., Li, S., & Chen, Y. (2015). The interaction effect of IT assets and IT management on firm performance: A systems perspective. *International Journal of Information Management*, *35*(5), 580–593. https://doi.org/10.1016/j.ijinfomgt.2015.06.006

Wolf, M., & Serpanos, D. (2018). Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*, *106*(1), 9–20. https://doi.org/10.1109/JPROC.2017.2781198

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS. ti and NVivo, 1994–2013. *Social Science Computer Review*, *34*(5), 597-617. https://doi.org/10.1177/0894439315596311

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering* (Vol. 5, pp. 484–487). https://doi.org/10.1109/ICACTE.2010.5579493

Yang, S. O. U., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling effective operational risk management in a financial institution: An action research study. *Journal of*

*Management of Information Systems*, *34*(3), 727–753. https://doi.org/10.1080/07421222.2017.1373006

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011). Study and application on the architecture and key technologies for IOT. In *2011 International Conference on Multimedia Technology, ICMT 2011* (pp. 747–751). IEEE. https://doi.org/10.1109/ICMT.2011.6002149

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions : epistemological , theoretical. *European Journal of Education*, *48*(2), 311–325. https://doi.org/10.1111/ejed.12014

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332. https://doi.org/10.1177/1356389013497081

Yin, R. K. (2014). *Case study research: Design and methods (5th ed.)*. Sage.

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13-15. https://doi.org/10.4314/mmj.v27i1.4

Zhang, D., Wan, J., Hsu, C. H., & Rayes, A. (2016). Industrial technologies and applications for the internet of things. *Computer Networks*, *101*, 1–4. https://doi.org/10.1016/j.comnet.2016.02.019

Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications*, 1–7. https://doi.org/10.1109/mwc.2019.1800455

Appendix A: Interview Protocol

| | | |
|---|---|---|
| Date and Time | | |
| Location | | |
| Participant ID | | |
| Preparation | Technology check and recording reminder for participant. | |
| Begin Conversation | State my name, Participant (ID) and date.<br>Have Participant (ID) confirm being provided with background information on this study including the purpose, reason for participation, benefits of participation, and approval for recording the audio portion of the interview and taking notes during this session. | |
| Review Confidentiality | Remind each participant:<br>~ Only the audio portion of video or phone call will be recorded.<br>~ Free to decline to answer any question or stop participating at any time; this is a completely voluntary session.<br>~ Free to decline to answer any individual questions or decline to provide any information not comfortable providing.<br>~ All information provide will be treated as strictly confidential and will not be disclosed to anyone, including employer.<br>~ Request avoid using organizational or individual names or any indicators that could be used to identify organization(s) or individual(s) in responses.<br>~ Names or comments that are mentioned in the interview will be removed from the transcripts and will not be included in the final report.<br>~ Request not discussing participation with anyone until the study concludes.<br>~ Any information provided in any form in the session will only be used for the purpose of this study, which will be presented in composite form with data from other participants in a doctoral study that may be published.<br>~ No responses will be presented in individual form.<br>~ Research records will be kept in an encrypted and password-protected format, locked in a safe for five years, after which time they will be destroyed.<br>~ Only I will have access to this data during that five-year period. | |

| | |
|---|---|
| Confirmation | Ask if any questions before continuing. |
| Interview | Semistructured interview about understanding participant(s) thoughts on the topic and questions. Questions outlined for which open and honest thoughts are appreciated. May ask for more thoughts or explanations on portions of your responses. Providing as much information on thoughts and perspective is greatly appreciated. |
| Semi structured Interview Questions | ~ Current role and how long in similar roles?<br>~ Worked in any other roles over during career in manufacturing? |
| Structured Interview Questions | ~ What strategies have you used to securely implement IoT devices in your manufacturing environment?<br>~ Which of those strategies worked well, and why?<br>~What issues or problems did you encounter?<br>~ How do you assess the effectiveness of the strategies used to securely implement IoT devices in your manufacturing environment?<br>~ How do the strategies fit or interact with other parts of the manufacturing environment?<br>~ What else would you like to add that might apply to the strategies you have used to securely implement IoT devices? |
| Collect Secondary Data | Conclude the interview portion of the meeting. Request any documents, multimedia presentations, or other information participant has agreed to provide. |
| Conclusion | Thank participant and to ensure interpreted responses are accurate discuss scheduling a follow-up interview and preferred method of communication for rescheduling? |

# Appendix B: Document Collection Protocol

| | |
|---|---|
| Name of document | |
| Date received | |
| Source | |
| Document type / format | |
| Description | |
| Key information | |

Appendix C: Training Certificate From the National Institute of Health Office of Extramural Research

**Certificate of Completion**

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Todd Hernandez** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 07/16/2016.

Certification Number: 2113426.