RISK ASSESSMENT OF CYBER INFRASTRUCTURE AND INTERDEPENDENT SYSTEMS: A DYNAMIC MODELLING APPROACH

A thesis submitted to the
Department of Business Development and Technology
School of Business and Social Sciences
Aarhus University, Denmark

In the partial fulfilment of requirements for the degree of

Doctor of Philosophy

Samuel Tweneboah-Koduah

CTIF Global Capsule
Department of Business Development and Technology
School of Business and Social Sciences
Aarhus University, Herning, Denmark

Ph. D. Supervisor:	Professor Ramjee Prasad CTIF Global Capsule (CGC), Department of Business Development and Technology, Aarhus University, Herning, Denmark
Ph. D. Co-Supervisor I:	Professor Peter Lindgren CTIF Global Capsule (CGC), Department of Business Development and Technology, Aarhus University, Herning, Denmark
Ph. D. Co-Supervisor II:	Professor Knud Erik Skouby Center for Communication, Media and Information technologies Aalborg University- Copenhagen, Denmark
Ph. D. Committee:	Professor Albena D. Mihovska, Aarhus University (**Chairperson**) Professor Christian Damsgaard Jensen, Technical University of Denmark (**Member**) Executive Vice President, Dr Lim Woo Lip, Ensign infosecurity (**Member**)
Ph. D. Series:	Risk Assessment of Cyber Infrastructure and Interdependent Systems: A Dynamic Modelling Approach, Department of Business Development and Technology (BTECH), School of Business and Social Sciences, Aarhus University, Herning, Denmark

Dedication:

To my late Grandma*:* ***Nana Abenaa Bronya***

CV

Samuel received his BSc. degree in Computer Science from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana (2001), MSc. in Information Systems from University of Westminster, London, United-Kingdom (2006) and a Graduate Certificate in Cybersecurity and Leadership from University of Washington, Seattle, USA (2015).

Samuel prior to starting the Ph. D. program worked as a full-time lecturer at the Computer Science department, and a department head at the School of Technology, Ghana Institute of Management and Public Administration (GIMPA), Accra, Ghana. Samuel was once a visiting Lecturer to the Centre of Media and Information Technology, Aalborg University, Copenhagen, Denmark, and a Visiting Scholar to the University of Washington, Seattle and Northern Kentucky University in the United States.

Samuel has a number of peer-reviewed journal publications to his credit and has presented a couple of peer-reviewed papers at a number of international conferences. As a lecturer and a scholar, Samuel has been involved in a number of projects, both at the national and international levels. Currently, Samuel is the Ministry of Health appointed Governing Chairperson of Twifu-Praso Nursing and Midwifery Training College, Twifu-Praso, Ghana. Samuel's research interest and expertise are in the areas of Cybersecurity and risk assurance, digital forensics and e-discovery, network-centric innovations and applications (cloud, IoT, M2M, intelligent systems), data mining, systems thinking and dynamic modelling, project management and IT integration.

English Abstract

Over the years, the rise of Internet technologies such as cloud computing, Internet of Things, etc. has led to an increasing rate of technology adoption among start-ups, private enterprises and public service institutions. The trend has seen many institutions providing critical services such as energy (electricity, oil, and gas), transportation, healthcare delivery, education, water supply, etc. outsource some of their IT resources to Cloud Service Providers (CSPs), delegating to them the management of critical information resources, which traditionally used to be managed in-house. Moreover, the digitization of modern infrastructure developments and their integration with information and communication technologies have also created complex networks of infrastructure interdependencies. This system of systems interdependencies has become the new cyber infrastructure platform supporting institutions in need of budget, but large-scale computing resources.

Particularly, the industrial controlled environments are witnessing massive scales of control systems development being integrated with intelligent systems utilise a two-way Internet and network communications. While the advancement has improved the efficiency and performance of operational technologies supporting systems operation, it has also exposed critical systems to countless forms of cyber-related threats that were not present in the hard-wired analogue systems. Dropper, Shamoon, Rootkits, Trojan horse, Worms, Night Dragon, Ransomware, Havex, Web Compromises, Phishing and Spear Phishing are the few examples of cyber attacks which have been reported to have targeted industrial control systems in recent times. Besides, the rapid system of systems integration in modern infrastructure development is adding to the complexities associated with critical infrastructure setups, making the systems and their structural characteristics even more difficult to predict, understand, analyse, and to model.

Extensive studies have shown that interdependent systems add to systems' structural, functional and algorithmic complexities. The

interdependency induced complexities pose further challenges to integrated systems in terms of operations, reliability, and efficiency.

The claims that cybersecurity risks associated with cyber-based infrastructure systems need to be properly investigated so that the technology's adoption is pursued with the total understanding of its inherent risks. It further claims that, in the institutional cybersecurity assessment context, both tangible and intangible risks are introduced along with the functionality and benefits provided by cloud-based applications. In the preliminary stages, two major trends have been observed in terms of an attack. Firstly, the targets are shifting from individual systems to chains of integrated systems. Secondly, the dynamics of attackers have shifted from script kiddies to advanced persistent threats, with the latter being much more specialised and coordinated.

The aim of the thesis is to present a way of identifying cybersecurity risks in a cloud infrastructure setup, investigate adversaries which could exploit such weaknesses and develop a framework to assess the impact of such exploitation. It begins by developing the understanding of cyber infrastructure risks sources and their impacts on interdependent systems from failure cases. Following that, infrastructure interdependency models are developed to assess systems' structural characteristics and then incorporate the modelling into a simulator, which simulates the behaviour of systems' interdependencies. Finally, a dynamic risk assessment framework is developed as a new approach to assessing the risks in interdependent infrastructure systems. Empirical studies of infrastructure interdependencies between cyber infrastructure and Industrial Control Systems-Systems Control and Data Acquisition (ICS-SCADA) have been carried out to demonstrate the modelling approach, the applicability and the validity of the methods.

Concluding, this study provides a valuable meaning into the process of studying and understand the cybersecurity dynamics of critical infrastructure systems; to serve as an input to a proactive critical infrastructure risks assessment and an overall policy framework for infrastructure protection management.

Resumé

I de senere år har fremvoksende internetteknologier såsom cloud computing, Internet of Things osv. ført til en accelererende teknologianvendelse i nystartede virksomheder, private virksomheder og offentlige serviceinstitutioner. Der er en tendens til at mange institutioner, der leverer kritiske tjenester såsom energi (elektricitet, olie og gas), transport, sundhedsydelser, uddannelse, vandforsyning osv. outsourcer nogle af deres IT aktiviteter til Cloud Service Providers (CSPs) og uddelegerer styring af følsomme informationer, som traditionelt er blevet administreret internt. Desuden har digitaliseringen af den moderne infrastrukturudvikling og dens integration med informations- og kommunikationsteknologier skabt komplekse net med indbyrdes infrastrukturafhængighed. Dette system af systemer, der er indbyrdes afhængige, er blevet den nye platform for en cyber-infrastruktur, der understøtter institutioner, der har brug for prisbillige, men omfattende IT-ressourcer.

Især ses i industrimiljøer massiv udvikling af kontrolsystemer, der integreres med intelligente systemer, der bruger tovejs internet- og netværkskommunikation. Mens denne udvikling har forbedret effektivitet og ydeevne i operationelle teknologier, der understøtter systemdrift, har den også udsat vitale systemer for utallige nye former for angreb. Dropper, Shamoon, Rootkits, Trojan horse, Worms, Night Dragon, Ransomware, Havex, Web Compromises, Phishing og Spear Phishing er eksempler på cyberangreb, der er rapporteret at have angrebet industrielle kontrolsystemer i de senere år. Desuden øger det hurtige system af systemers integration i moderne infrastrukturudvikling kompleksiteten forbundet med kritisk infrastrukturopsætning, hvilket gør det endnu sværere at forudsige, forstå, analysere og modellere systemernes strukturelle egenskaber.

Omfattende undersøgelser har vist, at indbyrdes afhængige systemer øger systemernes strukturelle, funktionelle og algoritmiske kompleksitet. Denne kompleksitet skabt af indbyrdes afhængigheder giver yderligere udfordringer til integrerede systemer, hvad angår funktionalitet, pålidelighed og effektivitet.

Resumé

I denne afhandling argumenteres for, at cybersikkerhedsrisici forbundet med cyberbaserede infrastruktursystemer skal undersøges indgående, så teknologien introduceres med fuld forståelse for de iboende sikkerhedsrisici. Det fremføres endvidere, at i den institutionelle vurdering af forholdene omkring cybersikkerhed bør både håndgribelige og immaterielle risici betragtes sammen med funktionaliteter og fordele ved cloud-baserede applikationer. I de indledende faser observeres to hovedtendenser i cyberangreb. For det første ændres målene fra individuelle systemer til kæder af integrerede systemer. For det andet ændres dynamikken i angrebene fra at være script-kiddies til avancerede vedvarende trusler, hvor sidstnævnte er meget mere specialiserede og koordinerede.

Formålet med afhandlingen er at præsentere en måde at identificere cybersikkerhedsrisici ved opsætning af cloud-infrastruktur, at undersøge modstandere, der kan udnytte sådanne risici og udvikle en ramme til vurdering af virkningen af en sådan udnyttelse. Den lægger ud med at fremme forståelse for risikokilder i cyberinfrastruktur og deres indvirkning på indbyrdes afhængige systemer ud fra fejl-cases. Derefter udvikles modeller af indbyrdes afhængige infrastrukturer med henblik på at vurdere systemers strukturelle egenskaber. Efterfølgende indsættes modellerne i en simulator, der viser, hvordan indbyrdes afhængige systemer opfører sig. Endelig udvikles en ramme for dynamisk risikovurdering, der er en ny tilgang til vurdering af risici i indbyrdes afhængige infrastruktursystemer. Empiriske studier af indbyrdes afhængige infrastrukturer - mellem cloud-strukturer og SCADA (Supervisory Control and Data Acquisition) - er blevet udført for at demonstrere anvendelighed og gyldighed af modelleringsmetoden.

Konkluderende, giver dette studie en god basis til at forstå cybersecurity-dynamikken i kritiske infrastruktursystemer. Det kan tjene som input i en proaktiv, kritisk infrastruktur risikovurdering samt i formulering af en overordnet ramme for, hvordan infrastrukturbeskyttelse styres.

Acknowledgements

"I know nothing because I know too much, and understand not, nearly enough and never will."

- Anne Rice

To begin with, I would like to remember and thank the Almighty God who gave me the strength, patience and courage that kept me going throughout this rutted journey of PhD. I sincerely want to express my acknowledgement to all those who in various ways contributed to the success of this study. It has been very challenging, but you have been with me.

First of all, I would wish to express my heartfelt appreciation to a great Scholar, Scientist, Mentor, Coach, and Supervisor Professor Ramjee Prasad; who when it seems all was lost, decided to give me the confidence and hope to carry on. Throughout my time with him, he has been an inspirational force through his great supervisory, mentoring and coaching role. I am and will remain very grateful to him for giving me the opportunity to work with him to complete my PhD.

It is also a great honour and privilege to get to know and work with Professor Knud Erik Skouby and Peter Lindgren; my co-supervisors. I am very grateful for their efforts, comments, contributions, suggestions and criticisms in shaping the thesis. Their smiles, supports, efforts, and contributions motivated me to carry on at the most critical times. My special gratitude also goes to my former supervisor (Professor Reza Tadayoni) at the Centre for Communications, Media and Information Technologies (CMI) of Electronic Systems, Aalborg University for his immense support, guidelines, and directions during the period of my stay. It is also my pleasure and with gratitude to mention Professor Henning Olesen for his wonderful review work at some stages of the thesis. I am also grateful for the support and reviews received from other professors in the department and other senior PhD Fellows most importantly Dr

Anthony Tsetse of Northern Kentucky University, Dr Ruth Ayanful Torgby at the Nuguchi Memorial Institute, Legon, Accra, Ghana and Dr Williams Idongesit of CMI, Copenhagen, Denmark for keeping me on my toes from the beginning of the process until the end.

My best experience during the PhD study was the time at the iSchool, University of Washington, Seattle, USA. This, however, couldn't have been possible without the efforts of Professor Barbara Endicott-Popovsky and the husband (Dr. Viatcheslav Popovsky - Slava). Barbara, having the opportunity to know you, is God's gift and blessing. I will forever be grateful. I am especially grateful for the various supports, directions and most importantly the love, motivation, and encouragement you and your Slava gave me.
My PhD study was partly supported by the Ghana Institute of Management and Public Administration (GIMPA). On this basis, I would like to extend my sincere gratitude to the management especially Deputy Rector (Professor Philip Osei) and the Director of Finance (Mr Darko) for granting me the study leave with fully paid salary. I couldn't have finished this study without your support.

Many thanks also go to Mr M. K. Hamilton of Critical Informatics Inc., Bremerton and the Seattle Chapter of Cloud Security Alliance (CSA) for the daily feeds you pushed to me on cybersecurity and related issues regarding critical infrastructure systems. I am also thankful for the technical support received from Bryan and Mike at the CISO's office, City of Seattle, USA during my 6-month research internship. My special appreciation also goes to the Microsoft Research Centre, Redmond, for introducing me to Microsoft Azure and the exposure on Microsoft Datacentre.

Last but not least, I would like to thank all those who in the very diverse ways contributed to the success of this thesis. Surely, this work would not have been completed without the encouragement, motivation, financial, emotional and spiritual support of my family and friends (most especially those in Copenhagen and Herning). To you all, I am most grateful.

Publications

Journal

i. **Tweneboah-Koduah S**., Francis Atsu and Ramjee Prasad (2020). "The reaction of Stock Volatility to Data Breach: An Event Study" *Journal of Cyber Security and Mobility*, vol. 9, no. 3

ii. **Tweneboah-Koduah S**. and Ramjee Prasad (2020). "Threats of Obsolete Infrastructures to Smart Grid Protection" *Wireless Personal Communications*, 1-19

iii. **Tweneboah-Koduah S.** and Ramjee Prasad (2020). Quantitative Estimate of Cyber Infrastructure and Interdependency Systems (under review)

iv. **Tweneboah-Koduah S.**, F. Atsu, and W. Buchanan, "Impact of Cyberattacks on Stock Performance: A Comparative Study," *Inf. Computer. Security.* vol. 26, no. 5, Oct. 2018.

v. **Tweneboah-Koduah S.** and W. J. Buchanan, "Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study," *Computer. Journal*, vol. 61, 2018.

vi. **Tweneboah-Koduah S.**, K. E. Skouby, and R. Tadayoni, "Cybersecurity threats to IoT applications and service domains," *Wireless. Pers. Communication.*, vol. 95, no. 1, pp. 169–185, 2017.

vii. **Tweneboah-Koduah S.**, A. K. Tsetse, J. Azasoo, and B. Endicott-Popovsky, "Evaluation of Cybersecurity Threats on Smart Metering System," in *Information Technology-New Generations*, Springer, 2018, pp. 199–207 – Book Chapter

viii. **Tweneboah-Koduah S**, B. Endicott-Popovsky, and A. Tsetse, "Barriers to government cloud adoption," *International Journal of Management Information Technology*, vol. 6, no. 3, pp. 1–16, 2014.

ix. A. Tsetse, P. Appiah-Kubi, A. Loukili, and **Tweneboah-Koduah S.**, "Performance Evaluation of a Multipurpose Bare PC Gateway," *Int. J. Appl. Eng. Res.*, vol. 10, no. 15, pp. 35488–35495, 2015.

Conference

i. Tsetse, et al. (2018). Performance Study of the Impact of Security on 802.11ac Networks. Conference Proceedings, ITNG, 2018, Las Vegas, USA. April 16 – 18, 2018

ii. **Tweneboah-Koduah S.** and Philip Osei. Accessing Online Education in an Offline Environment. Conference Proceedings: International Conference on Distance Education, Toronto, Canada. October 16 -19, 2017

iii. **Tweneboah-Koduah S.**, et al, (2016), Evaluation of cybersecurity threats on Smart Metering System (Conference Proceedings, ITNG, 2017, Las Vegas, USA. April 10 – 12, 2017

iv. **Tweneboah-Koduah S.** (2013). Unleashing the Potential of Cloud Computing: What is it and what does it mean for public organizations in Ghana – Presented at "The International Conference on Applications of Mobile communications in Africa: Prospects and Challenges", Accra-Ghana. June 16-17, 2013

v. **Tweneboah-Koduah S.** (2012). Knowledge Management, Critical Factor for Successful Implementation of e-Government projects: presented at "The 12th European Conference on e-Government", Barcelona, Spain. June 12-14, 2012

List of Figures

List of Tables

List of Acronyms

1:1	One-to-One
1:M	One-to-Many
ALE	Annualized Loss Expectancy
API	Application Program Interface
APT	Advanced Persistent Threat
AWS	Amazon Web Service
BCP	Business Continuity Plan
BLI	Breach Level Index
BPDS	Bulk Power Distribution Systems
CAS	Complex Adaptive System
CDPD	Cellular Digital Packet Data
CERT	Computer Emergency and Response Team
CII	Critical Infrastructure Interdependency
CIS	Cloud Infrastructure Stack
CISO	Certified Information Security Officer
CLD	Causal Loop Diagram
CRC	Cycle Redundancy Check
CSA	Cloud Security Alliance
CSC	Cloud Service Consumer
CSP	Cloud Service Provider
CVE	Common Vulnerability Exposure
CVSS	Common Vulnerability Scoring Score
CWE	Common Weakness Enumerator
DCS	Distributed Control Systems
DDoS/DoS	Distributed Denial of Service
DNP3	Distributed Network Protocol version 3
DHS	Department of Homeland Security
DNS	Domain Name Services
DRP	Disaster Recovery Plan
ECG	Electricity Company of Ghana
FCC	Federal Communication Commission
FERC	Federal Energy Regulatory Commission
FIRST	Forum of Incident Response and Security Teams
FTA	Fault Tree Analysis
GOI	Graphic Operator Interface

GRIDCo	Ghana Grid Company
HMI	Human Machine Interface
HTTPS	Secure Hypertext Transmission Protocol
IA	Impact Assessment
IaaS	Infrastructure-as-a-Service
ICCP	Inter-Control Centre Communications Protocol
IEC	(or 60870-6/TASE.2)
ICMS	Industrial Control Monitoring Systems
ICS	Industrial Control Systems
IED	Intelligent Electronic Devices
IoT	Internet of Things
ISID	Industrial Security Incident Database
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
L2TP	Layer 2 Tunnelling Protocol
M: M	Many-to-Many
M2M	Machine-to-Machines
MTU	Master Terminal Units
NERC	America Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology, Special Publication
NSTB	National SCADA Test Bed
NVD	National Vulnerability Database
OT	Operation Technology
OWASP	Open Web Application Security Project
PaaS	Platform-as-a-Service
PCCIP	Presidential Commission on Critical Infrastructure Protection
PRS	Physical Resources Set
PSE	Puget Sound Energy
RCC	Regulation Control Command
ReST	Representational State Transfer
RTU	Remote Terminal Units
SaaS	Software-as-a-Service
SCADA	Supervisory Control and Data Acquisition

SCP	Secure Copy Program
SCPS	Supervisory Control Protocol Services
SD	System Dynamics
SDDC	Simple Device Control Command
SLA	Service Level Agreement
SLA	Service Level Agreement
SME	Subject Matter Experts
SIS	Safety Instrumentation Systems
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service-Oriented Computing
SQL	Structured Query Language
TCCP	Trusted Cloud Computing Platform
TCP/IP	Transmission Control Protocol/Internet Protocol
TVP	Threats, Vulnerability Pair
VFD	Variable Frequency Drives
VMM	Virtual Machine Monitor
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VRA	Volta River Authority
VRS	Virtual Resources Set
WoT	Web of Things
XSS	Cross Site Scripting
ZDT	Zero-Day Threats

Summary of Research Contributions

The primary objective of the study is to answer the question - *"security risks in cloud (as a cyber-infrastructure) setup and their impact on interconnected critical infrastructure systems, and the methods of such assessment"*. Five major observations (regarding infrastructure interdependencies from the risk assessment perspective), were found to have influenced systems overall risk exposure. The observations made are:

i. Vulnerabilities inherent within the host as the independent system and ISC-SCADA as the dependent system contributes to the security risk exposure of other interdependent systems.
ii. Critical infrastructure systems are under constant cyber-attack due to the 'richness' of their resources.
iii. Infrastructure interdependency increases systems complexity which then increases the systems' security risk exposure.
iv. The value of the system is statistically significant to the impact of a threat attack.
v. The presence (and absence of) control mechanisms influence the likelihood of threats attack.

One major challenge encountered in addressing these challenges was the method of identifying, clarifying and predicting interdependencies induced complexities; this is where this study is even more useful. An equally important discovery is the lack of an acceptable method to quantify the value of critical infrastructure systems (and their criticality thereof). This makes the proposition and the development of new methodology even more relevant.

Having considered how the thesis's results correspond to its objectives, the paragraphs below look at how the key research questions have been discussed.

Question 1: *What are the vulnerabilities, which are inherent in cyber infrastructure systems and the potential threats capable of exploiting these vulnerabilities?* The answer to the question is presented in

chapter four; over here, data (both primary and secondary) was collected, analyzed, results presented and explanation provided. In relations to the thesis's objectives, the outcome from this question is also used as the basis for the model design and the simulation procedure in chapter seven.

Question 2: *How to assess the interdependencies in critical infrastructure systems?* The answer to this question is captured in chapter five; in this context, Bendell model is adopted to compute the interdependency efficiency ratio between two interdependent infrastructure systems. The results show that in an interconnected system, the behaviour of one system has a direct impact on other systems due to the feedback effect. In reference to the thesis objectives, the outcome from this question feeds into the modelling design and analysis; a useful guide in tracing causes of systems' behaviour and source of failure.

Question 3: *How to capture and predict the complex behaviour of infrastructure interdependencies?* The answer to this question is captured in chapters six and seven. In this context, a model-based design (from the perspective of system thinking) is adopted to model infrastructure interdependencies. From that, structural analysis of interdependent systems is performed using causal loop diagrams. This helps to determine the causes and effects of system behaviour.

Question 4: How to assess cybersecurity risks in interdependent critical infrastructure systems? The answer to this question is represented by the development of the thesis's proposed dynamic modelling framework. It follows the gaps identified in the literature and in practice, and the development of the dynamics model and simulations. To support the use of the framework, guidelines are provided to support its implementation, especially at the industrial level. On this basis, it can be concluded that the thesis has sufficiently answered the research questions. This does not necessarily mean the thesis has addressed every concern raised due to the implications of other unidentified but relevant concerns the thesis might have unsuccessful captured.

Table of Contents

Chapter 1: Introduction

> *"Is your control system accessible directly from the Internet? Do you use remote access tools to log into your control system network? Are you unsure of the security measures that protect your remote access services? If your answer was yes to any or all of these questions: You are at increased risk of cyber attacks including scanning, probes, brute force attempts and unauthorised access to your control environment"*
>
> *ICS-CERT*[1]

Over the past few years, security challenges from cyber ecosystem have become a major global epidemic to both private and public institutions, whose activities or operations depend on cyber infrastructure systems. Thus, the increasing rate of global digital migration coupled with the technological convergence, have brought new forms of security risks, which were relatively unknown in traditional hard-wired solo systems. The cybersecurity challenges have become global cyber warfare, which attention is a concern to all actors in the cyber ecosystem.

The quotation above (from ICS-CERT) sets the tone for the argument presented by this research, claiming, 'interdependent critical infrastructure systems, which are connected to public networks are under constant threats from cyber adversaries, and a method of assessing the risks is worth an academic exercise'. The findings from the study provide the basis to develop and test the appropriate methods and models to assess security-related risks associated with critical cyber infrastructure systems and their interdependencies.

In its broader sense, the study attempts to assess the interdependencies between cloud as a cyber infrastructure and its interdependent systems and the security risks the interdependency introduces. The other controlled variable the thesis considers is

[1] Industrial Control Systems Cyber Emergency Response Team

Industrial Control Systems-Supervisory Control and Data Acquisition (ICS-SCADA)[2]. The primary objective is to explore the interdependencies induced complexities, and how the behavioural characteristics of such independency influence the overall performance of the unified systems, and the risks, associated with such integration.

SCADA is a member of the family of operational technologies (tools) supporting industrial control processes in a controlled environment. SCADA is defined by Robles and Kim as a set of a system comprising of "computers, controllers, instruments; actuators, networks, and interfaces which manage the control of automated industrial processes" allowing the analysis of the "processes through internally generated data" [1]. In recent times, technological advancement in industrial automation has witnessed the integration of controlled systems with public networks (i.e. the Internet). While the integration has improved systems performance, the integration, however, has also exposed industrial control systems to various forms of threats. Moreover, the integration and the use of computerised applications to control, monitor and view critical infrastructural systems have further made systems even more interconnected and complex in terms of design, deployment, and management. This convergence of system of systems has become a new managerial totem; a major concern for the management of critical infrastructure systems.

Over the years, numerous security assessment methods targeting infrastructural systems have been proposed, developed and implemented. Notwithstanding, very few of such methods have focused on Cyber Infrastructure (CPI) and its dependent systems. There is, therefore, the need to develop different methods to assess the current wave of cybersecurity risks against critical infrastructure systems, since there is no universal 'all-in-all silver bullet solution' to any particular problem.

The rest of the chapter is structured as follows: The next section provides a general background of the thesis and follows with the research objectives in section 1.2. Section 1.3 articulates the research

[2]In this study, ICS-SCADA will be referred to as SCADA for clarity of purpose

problem which is followed by the objectives of the thesis in section 1.3. The research approach and the methodology are the contents of sections 1.4 and 1.5 respectively. Section 1.6 concludes this chapter.

1.1 Background

The emergence of Internet-based technologies has witnessed a rapid rate of technology adoption among both private and public institutions. The trend has led to the situation where both institutions providing critical services (i.e. energy distribution, transportation, healthcare, water and sewerage system, etc.) outsource some of their Information Technology (IT) and Operational Technology (OT) resources to Cloud Service Providers (CSPs). In this context, cloud computing has become the new cyber infrastructure platform, upon which institutions in need of budget but large-scale computing resources fall on. However, the richness of resources available in the cloud environment has made the environment very attractive to different forms of threats from cyber adversaries.

Furthermore, the advancements in modern infrastructure development integrated with computing technologies, have created complex networks of interconnected infrastructure systems (referred here as critical cyber infrastructure), making the infrastructure resources more interdependent. The interdependency between critical infrastructure and cloud infrastructure is termed here as Cloud Infrastructure Interdependency (CII). CII is considered as a member of Infrastructure Interdependencies (II) that was first proposed by [2]. According to the authors, infrastructure interdependencies have a significant impact on the services the infrastructures support [2]. On this basis, it is argued, such an impact needs to be explored, and the method of such an assessment is worth a research effort.

In this thesis, it is claimed, critical infrastructure systems need to be protected at all time so that they can operate at their optimum level. Ensuring that interdependent systems achieve their optimum performance requires planned systems integration so that security risks associated with the systems interdependency are properly explored and their integration is pursued with the total understanding of its inherent risks. Paquette et al. further argue that from the context

of institutional technology adoption that, both "tangible and intangible risks are introduced; along with the functionality and the benefits provided" by the technology" [3]. Therefore, institutions adopting cloud computing must understand the security challenges such adoption presents to existing infrastructure and develop strategies to respond to any unwanted consequences and even greater problems from infrastructure service providers. Furthermore, the study argues, the ability of infrastructure owners, asset managers and administrators to manage the security risks, is fundamental to the success to be derived from the planned technology adoption and use.

1.2 Research Motivation

Critical infrastructure is defined as the "systems and assets, physical or virtual, so vital to the Nation that the incapacity, unavailability and destruction of such systems have a very unbearable impact on national safety, economic security, public health, or any combination of those matters" [4]. These systems are the foundation upon which societies thrive. Whether operational or informational, critical infrastructure resources require industrial control technologies to operate. Nevertheless, technology advances in programmable logic control (PLC) design in industrial control systems has made modern controlled systems inherently automated, interconnected and complex in terms of design, application and management. Additionally, the introduction of advanced network technologies such as Internet-facing cloud computing has pushed many infrastructure owners, administrators and managers to integrate part of their control operations to the cloud space. From transportation networks to heating, ventilation and air-conditions (HVAC), water and sewerage systems, energy distribution, elevators, smart grid and smart meters, etc., controlled systems are found in almost any critical infrastructure operations. This system of systems integration apart from its immense benefits has also introduced new forms of security risks, which must concern all stakeholders who depend on these critical resources.

For instance, Chen et al argue that the system of systems infrastructure integration has made "critical infrastructure systems independently complex", making it difficult to predict any form of

security risk impact" [5]. In a related study, Bodungen et al claimed that in recent times, "assets owners have driven demand towards greater visibility and platform standardization" [6]. At the same time, vendors are also seeking "ways to lower production costs, given that a lot of protocols, such as ControlNet, DeviceNet, Profibus, and Serial Modbus, Windows OS and Ethernet are on the production line" [6]. With this convergence, [6], posits "asset owners are now faced with managing both Information Technology (IT) and Operational Technology Networks (OT)" to manage enterprise records and systems operations [6]. According to Bodungen et al, this convergence is not only mutual but also established [6]. Undoubtedly, the convergence has introduced different security concerns that were relatively unknown in the pre-industrial automation hard-wired analogue systems. While the focus has been on the benefits, little do infrastructure owners think of their inherent risks and attack impact, until some major crises highlight the inherent vulnerabilities within the technology setup.

Accordingly, the notion of "critical infrastructures is highly interconnected and mutually dependent in some complex ways, both physically and virtually, through a host of information and communications technologies, is more than just an abstract theoretical concept" [7]. Consequently, some questions that come up include; why are Internet-dependent systems are becoming increasingly vulnerable to cyber-attacks? What are the potential threats capable of exploiting these vulnerabilities? What is the potential impact should threat agents succeeded in attacking these systems? These and other questions set up in the thesis necessitate the need for this research.

In the era of Internet-based technologies, multiple solutions are being developed to control and monitor critical infrastructure systems. Regrettably, not many studies in the past have focused on exploring challenges relating to systems interdependencies. This thesis, therefore, seeks to explore the cybersecurity challenges associated with cyber infrastructure convergence and examine how the convergence impacts the behaviour of the interdependent systems.

The author is also motivated by the quest to understand the cyber-related threats, industrial control systems are exposed to when integrated with Internet-facing applications; and how such events impact systems' performance. The discoveries made from the assessment will support the design and the development of a new risk assessment framework.

One primary objective of every research activity is the benefit to the end-user, in this regard, the author considers Ghana as the key beneficiary of this study. In the last couple of years, Ghana has been going through a lot of challenges relating to power distribution and delivery. One of the major challenges according to the operators is the issue of infrastructure obsolesce and the general lack of proper risk management strategies in the energy sector. It is a personal motivation to present and share the ideas gained with some of the key players in the energy sector in Ghana.

Perhaps, the most significant part of every academic exercise is the contribution to the body of knowledge; in this case, the author is motivated by the idea that the study's discoveries, will make significant contribution to the existing body of knowledge in the cybersecurity security and risk assurance landscape, especially in the area of cyber infrastructure protection.

1.3 Problem Articulation

The recent high profile cyber attacks on critical systems worldwide have become a wake-up call to infrastructure managers, administrators, asset owners, Governments and even individuals whose day-to-day activities depend on these infrastructure systems. The global economic powers run on critical infrastructure network systems such as transportation, power distribution, and water and sewerage. It is critical that these systems and their subsystems are available and reliable. Furthermore, the advancement in digital technology landscape of critical infrastructures in recent times has significantly contributed to the modernization of industrial control automation, which provides computational power, large-scale as well as low-cost storage facilities. This transformation of control automation has contributed to improved systems inter-

communication and operational processes. Nonetheless, the convergence has also made the systems highly interdependent and complex, exposing them to different forms of threats that were relatively unknown in the hard-wired analogue systems of the past. Thus, the new structural setup presents its own opportunities as well as its inherent risks.

While the advances have improved systems' efficiency and performance, they have also exposed systems to countless security risks. Shamoon, Dropper, Rootkits, Worms, Night Dragon, Trojan Horse, Ransomware, Watering Hole, Havex, Black Energy, and Sandworm are few examples of malware, which have targeted industrial control and other distributed systems in recent times. Moreover, in the energy sector, technologies such as Advanced Metering Infrastructure (AMI) [8] have also been introduced to new functional areas, through which potential threat actors could launch an attack on the energy grid. This convergence in the critical infrastructure systems has become common, and in most cases complex to analyse and to model. Complexity adaptive theorists argue that the interdependency induced complexity in systems can influence systems operations, reliability, efficiency, and modelling [9]. The challenge to researchers as well as systems administrators and managers is how to assess the cybersecurity risks associated with the interdependent complex infrastructure systems.

According to global energy report, in the energy sector, two new trends of cyberattack have recently emerged [10]. First, "targets are shifting from individual systems to chains of integrated systems". Secondly, "components of attackers have also shifted from script kiddies to criminal groups" and state-sponsored adversaries, with the latter becoming more sophisticated and coordinated [10]. Studies by Kundur et al, also provide statistics on various cyber attacks against critical infrastructure systems [11,12]. From the above discussions, this thesis attempts to assess the cybersecurity risks in the cyber infrastructure setup (e.g. cloud computing) and how such events impact interdependent critical infrastructure systems. To address this problem, the thesis explores the following questions:

i. What are the vulnerabilities, which are inherent in cyber infrastructure systems and the potential threats capable of

exploiting these vulnerabilities?

ii. How to assess the interdependencies in critical infrastructure systems?

iii. How to capture and predict the complex behaviour of infrastructure interdependencies?

iv. How to assess cybersecurity risks in interdependent critical infrastructure systems?

1.4 Research Objectives

As stated earlier, over the past couple of years, critical infrastructures, in general, have become very sophisticated and complex in terms of design and applications. Both cloud infrastructure and industrial controls systems are but few examples of such complex systems. To achieve stability and operational efficiency, complex systems and their subsystems require all sections to perform at their optimal levels [13]. Tackling complexities (e.g. multi-tenancy) in cyber infrastructure set up is a major challenge, not only to the service provider but also to the cloud service users and other stakeholders in the environment. In addition to the challenge of defining system boundaries, there is also the need to understand how a malfunction in one part of the system affects the performance of interconnected systems.

Many controlled automated systems have been designed to self-recover, nonetheless, large-scale disruptions do occur and sometimes occur unexpectedly. Though the frequencies of occurrences may be low, the overall impact of such distractions could be high. Planned or unplanned threats against critical infrastructure systems are inevitable. The author, therefore, claims that threats exist in the cyberspace, and a method of assessing such risks is worth an academic exercise. In this context, cyber insurance also comes mind. Notwithstanding, if cyber risks can be transferred like a portfolio and brokered like investments, the concern will be the method of an assessment. Even then, the argument will be the level of risks to be accepted, transferred or mitigated.

The study, therefore, presents a way of identifying potential vulnerabilities in cyber infrastructure setup, investigate adversaries

which could exploit such vulnerabilities and then develop a method to assess the impact such exploitation could have on interdependent critical systems. It begins by developing the understanding of cyber infrastructure risks sources and their impacts on infrastructure dependencies from failure cases. Following that, infrastructure interdependencies models are built to assess successful threat impact, and then incorporate the interdependencies modelling into a critical infrastructures simulator for interdependency simulation.

Specifically, the study is structured along with the following objectives:

i. To capture and predict the complex behaviour of infrastructure interdependencies
ii. To assess threats and vulnerabilities in interdependent critical infrastructure setup
iii. To estimate the efficiency of infrastructure interdependencies systems
iv. To develop a system-based framework to assess cybersecurity risks in critical infrastructure setup

1.5 Research Approach

The first objective is to explore the causal factors in the understanding of threat and vulnerability vectors in critical infrastructure systems and their propagation patterns on interdependent systems. The knowledge of cloud infrastructure as a controlled variable is developed using relevant literature and proprietary materials from secondary sources. Observatory studies were conducted at three independent cloud service providers. Cloud adoption cases covering over thirty-four public institutions in major cities in the North-West Pacific, USA were reviewed. In addition, some primary data were collected through unstructured interviews with individuals considered to be Subject Matter Experts (SMEs).

To accomplish the second objective, a database of current and hypothetical vulnerabilities is built together with a catalogue of threat events, which are considered common to critical infrastructure

setups[3]. Using threats and vulnerability catalogues; a quantitative impact assessment model is built to measure the cybersecurity induced risk.

To accomplish the third and fourth objectives, system-specific simulation models are then built to formalise infrastructure interdependencies and their representations. In this context, a set of empirical functions are set up as datasets to build functional dynamic models. From the functions, the relationship between infrastructure inputs to the corresponding output of the dependent systems (SCADA) is established. The information used to construct these empirical functions is collected from interviews with asset owners as well as infrastructure operators. Other sources include infrastructure failure reports from service providers and other secondary sources.

1.6 Methodological Overview

There are two approaches to the study design. The first approach deals with assessing cybersecurity risks in interdependent critical infrastructure systems. The second part focuses on the development and the implementation strategy of the thesis's proposed systems dynamics risk assessment framework. In the first instance, data (both primary and secondary) is collected, analysed and results interpreted. Following that, systems dynamic models are developed to observe the structural characteristics of interdependent systems. And then using the results from the data analysis, simulations are run to test if model development produces the expected results. In the second approach, the gaps (i.e. from the literature and theoretical reviews), results from data analysis and the modelling process are used as requirements to design and develop a system dynamic framework for the assessment of risks in critical infrastructure systems.

[3] Current vulnerabilities list known vulnerabilities to cloud infrastructure systems. Hypothetical vulnerabilities involve vulnerabilities that are listed in the secondary vulnerability databases but were not verified by the SMEs as significantly relevant to be exploited by threat agents in the cloud environment.

1.7 Thesis Structure

Figure 1-1 (termed as SLAVA Model[4]) depicts the key stages of the research process with an emphasis on the correlations between the chapters. The main research activities (i.e. chapters) are shown in the rectangular boxes. Other activities are considered auxiliary and are shown with the light green background. Auxiliary activities are considered external to the core thesis's activities, but a useful share of the overall research process. Besides the preliminary activity, there are two main auxiliary activities (i.e. connected world and Knowledge dissemination). In the first instance, a postdoctoral researcher is expected to use the learning experience to build networks with both research and the industrial communities. The second activity involves using both local and international platforms to share one's acquired knowledge and at the same time making an impact on the global world through further research and learning. Activities in the shadow boxes are considered iterative (shown by the interconnected broken lines). The thesis is organised into eight main chapters. The sections below provide a brief of each of the chapters.

Chapter one introduces the study and discusses research motivation, problems articulation, objectives, and methodology. Chapter two looks at the state-of-the-art of the subject matter. The chapter focuses on the general overview of institutional risk assessment processes and follows up with a detailed discussion on cloud computing; with an emphasis on cloud-specific risks. Other topics discussed in this chapter include critical infrastructure systems and ICS-SCADA[5] systems. The chapter is concluded with the analysis of the gaps identified in the literature. A theoretical review is the focus of discussion in chapter 3. In this context, three main and two subsidiary theories were reviewed; system theory, network theory, complexity adaptive theory, the theory of structures and theory of dynamic complexity.

---

[4] The model is named after Dr. Viatcheslav Popovsky – Slava at the University of Idaho, USA who walked me through the Russian approach of research method. The model is based on the Russian teaching pedagogy, that states "if you understand something, you must be able to present your ideas by drawing"

[5] Industrial Control System-Supervisory Control and Data Acquisition

Chapter four looks at the research approach; emphasising on the data collection strategy and the characterization of cybersecurity risk assessment processes. Among the metrics discussed are threat types, types of system vulnerabilities, control mechanisms and the impact of cyberattacks. Data (results) analysis and discussions are presented in chapter five. In chapter six, system dynamics as the instrument for constructing dynamic models and simulation design were introduced. Topical areas discussed here include principles of modelling, the modelling process and an overview of general system thinking.

In chapter seven, models construction and simulation design are discussed. The proposed dynamic risk assessment framework and the guidelines (to use) were also presented in chapter seven. The thesis is concluded in chapter eight; where the summary of the thesis's findings, theoretical and practical implications, limitations and the future research scope are presented.

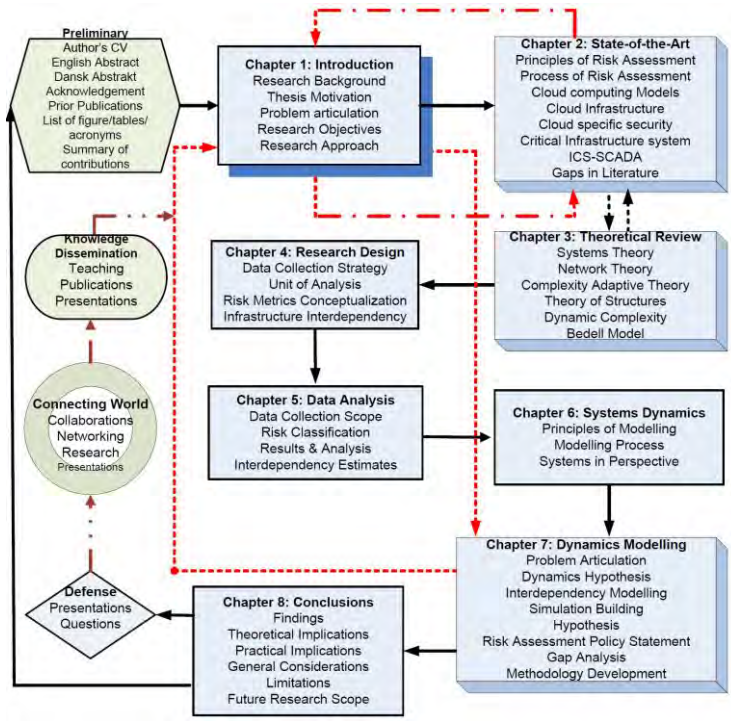


Figure 1- 1: The Research process (SLAVA Model)

1.7 Conclusions

The issue of cybersecurity has become a global epidemic and a major concern to everyone in the digital ecosystem. For private organisations and state-owned agencies, the threats from the cyberspace are even more alarming. While the practitioners (i.e. industrialists) are doing everything possible to protect cyber infrastructure systems, the responsibilities of researchers and academics are to lead and proactively develop theories and guidelines to support institutional risk assessment processes in the area of cyber infrastructure protection. And in this context, this thesis sets the tone for an academic discourse; as it explores the dynamics in the subject matter.

This chapter has looked at the general overview and in particular the major components of the thesis. Among the key topics discussed are the research objectives, problem articulation, the research approach and the research methodology. In the next chapter, the state-of-the-art of the subject matter is examined by reviewing extant work on the subject.

Chapter 2: State-of-the-Art

"Protecting the nation's electricity grid from cyber attack is a critical national security issue. Evidence collected by the Department of Homeland Security (DHS), suggests that cyberattack on key energy infrastructure and electricity system, in particular, is increasing, both in frequency and sophistication. These trends are alarming because the potential consequences of a successful large-scale cyber attack or combined cyber and physical attack on the power sector are difficult to overstate"

BPC Electric Grid Cybersecurity Initiative

Note: Few contents of this chapter have been published in a journal [14]. However, any content found in this thesis has been duly referenced. The paper as published in the journal provides a general overview of the security and risk assessment in the cyber ecosystem. This chapter, however, provides comprehensive literature on the state of the art of critical infrastructure systems and their interdependencies with special emphasis on industrial control SCADA systems. The narratives provided in this chapter are also extensive as compared to the content of the publication in the journal paper. Significantly, there was some mathematical misinterpretation of two equations in the publication, which have also been addressed in the thesis (i.e. equations 2.3 and 2.4).

This chapter looks at the state-of-the-art of the subject matter; providing a comprehensive literature review on some of the contextual aspects of the thesis. Among the issues discussed in this chapter is the principle of risk assessment, an overview of cloud computing, cyber infrastructure setup, security risks specific to cloud computing and infrastructure interdependency systems. The chapter is concluded with the discussion of knowledge gaps identified in the literature.

2.1 Principles of Risk Assessment

In the context of risk assessment, there seems not to be a commonly accepted definition of the subject 'risk'. This ambiguity "is a fairly common roadblock to truly understanding risk" and related concepts [15]. It is claimed;

> *"…it is safe to say that there have been many discussions about risk but there have been very few definitions provided or accepted. Of the definitions that we do have, the only thing that they share in common is the very fact that they share so little in common"*
>
> ***Talabis and Martin***

This claim by Talabis and Martin does not suggest, there is no definition of risk, and neither do experts disagree on the true meaning of risk. This discourse, however, highlights how different researchers have perceived the concept of risks. Consequently, the differences in opinion may also be attributed to the variations in perception (psychometric) and context (communication).

The word "risk" originates from the Italian word "risco" (danger) or "rischiare" (run into danger) [3]. The NIST[6] SP-30 framework defines risk as the "impact resulted from an action on an entity, and the potential consequences of that action" [16]. Accordingly, Paquette et al, argue that "risk should not be defined or classified by the size of the risk, but by the balance of expected and unexpected consequences" [3], which is considered as the impact of loss. The problem with the existing institutional risk assessment processes is the difficulty in conceptualizing the various constructs embodied in the existing models due to the lack of uniformity in their applications. For instance, how does one estimate the true value of a critical infrastructure system (e.g. virtual PLC) in the face of quantitative analysis? It is further argued that in such a situation, many institutions become "susceptible to engaging in high-risk activities which yield short-term benefits at the expense of future uncertainties" [17]. This and other related reasons rationalise the quest for the development of a new assessment method that focuses on the infrastructure interdependency system.

Kaplan and Garrick have proposed a quantitative risk assessment concept based on the following three factors ("the set of triplets") [18];

[6] National Institute of Standards and Technology

i. "What can happen"?
ii. "How likely is that to happen"?
iii. "What is the consequence should it happen (i.e. Impact)"?

This leads to Kaplan's first-level definition of risk; presented as a mathematical function and presented as

$$R = \{< T_i, L_i, I_i >\} \quad (2.1)$$

where T_i represents the *i*th risk event, L_i as the likelihood of the event; and I_i is the resulting impact. It is from this basis risk is defined. Per their definition, the risk is defined as to the likelihood of an event or entity moving from one state to another (i.e. as a function of time 't' and completeness 'c') [18]. This exposition by Kaplan and Garrick redefines Risk (R) as;

$$R = \{< T_i, L_i, I_i >\}_c \quad (2.2)$$

One significant gap identified in Kaplan and Garrick's model is the lack of the underlying entity (object) upon which an impact is estimated. Consequently, Tweneboah-Koduah and Buchanan extended this definition and remodelled equation (2.2) to denote the likelihood of an event happening and its consequence (impact) [14]. They refer to this as the Asset ('A') and argued that threats are inactive unless there is the presence of vulnerabilities. Subsequently, threat ('T') is introduced as a function of vulnerabilities ('V') in equation (2.3):

$$R = \{<T_i(V), L_i, I_i(A) >\}_c \quad (2.3)$$

The introduction of an Asset (A) and Vulnerability (V) in (2.3) makes the definition of risk even more useful in the discussion of institutional risk assessment. From equation (2.3), the authors proposed a new risk assessment model as a function of likelihood (L) of a Threat (T) event exploiting systems vulnerability (V), and its severity, measured by the outcome of its impact (I) on asset (A). The following metrics are subsequently identified:

i. Asset (A)
ii. Threat
iii. Vulnerability
iv. Likelihood (L)
v. Impact (I)

These lead to a new risk equation as

$$R = \{< (V(T_i)\, L_i,\, A\,(I_i))_t >\}_c \qquad (2.4)$$

2.2 Risk Assessment in Context

Security or risk management are both academic and business disciplines with numerous extant studies; yet, the subject continues to generate interest across various academic disciplines. Nonetheless, experts have failed to clarify or distinguish clearly the relationship between the two concepts. Security and risk as subjects are in most cases treated with the same meaning or are interchanged in many discussions. For instance, in the information security context, the terms cybersecurity, cybercrime, cyber-risk, cyberattack, security threats and more recently data breach, have, in most cases been used to either refer to security or risk in the cyberspace. Perhaps, just a confusing phrase to blur the purported audience. It is therefore stated here that the challenges relating to security and/or risk assessment can be addressed if the two concepts are situated in their proper context.

Traditionally, security practices in our social settings or environment have revolved around the 3Gs (‘guns’ ‘guards’ ‘gates’). Researchers over the years have adopted several theories (from behavioural sciences to qualitative risk scenarios and econometric theories) to assimilate investment decisions and security governance [19]. This behavioural approach to risk; acknowledges the importance of behavioural factors in risk management. In that case, behavioural risks should be separated from technical risks. Along with this behavioural discourse comes with a challenge as to how risk should be measured. In the behavioural sciences, the risk is treated as subjective or perceived, rather than quantitative. In this study, the risk assessment process is approached quantitatively, by modelling risk metrics using arithmetic embedded process. The assumption is that information resources like all other assets, have values and their values must be quantifiable so as to express their real worth in terms of assessing the impact of attacks.

A study by Pieters suggests that “traditional implicit philosophy of the protection of information” resources is “based on the notion of containment and creating physical boundaries around assets,

compartments or perimeters that need protection" [20]. However, in a network-centric and interdependent critical infrastructure ecosystem, the notion of the 'inside' versus the 'outside' is non-existing; making it difficult to draw a line between "insiders and outsiders" [21]. In recent times, cyber infrastructure systems by their design have become highly interconnected and complex, in such environments, it is not always clear where a systems' boundaries lie, making it difficult to implement traditional perimeter defence systems ('loosely termed security'). Not only has information and communication technologies as well as systems integration introduced new security concerns but also changed the way these resources can be secured and protected by the traditional security methods. 'This is a paradigm shift in the management and protection of our critical infrastructure resources'.

Though the terms 'Security' and 'Risk' have been used interchangeably, it is stated here that the relationship between the two is more than just a linguistic pair. For instance, Borodzicz argues that the theoretical approach to security should aim at "identifying losses in order to establish the appropriate security procedures" [22]. In a related study, Talbot and Jakeman claim that security is the condition of being protected against danger or loss" [23]. This proposition does not differ from the quantitative risk approach that aims at estimating losses and their impact stated in equation (2.3). One model that appears to support this assertion is the Manunta's Assets, Protection and Threats (APT) model [24]. The model defines security as the function of Assets, Protection and Threats:

$$S = F(A, P, T)S_i \tag{2.5}$$

Comparing S in (2.5) to R in (2.4) implies $S \neq R$. Inference, security and risk though related, exhibit different functional characteristics, which do not support mathematical equality as previous studies have suggested. However, the security definition by Manunta also provides a significant analogy to the discussion of risk in [22]. Furthermore, it is emphasised here that in a situation of security and risk communications, several realities exist, which must be considered in any contextual discussion. Such contextualization is necessary for reducing security and risk problems down to their basic components.

This helps to clarify their true meaning under the context in which they are being applied. Indeed, security and risk variables (as presented in equations (2.4) and (2.5) are likely to be defined or perhaps interpreted differently depending on who is defining them, and where they are being applied.

Talbot and Jakeman on their part, define security risk as "an event that could result in the compromise of organizational assets" [23]. Furthermore, the authors describe security risk as "unauthorized use, loss, damage, disclosure, or modification of organizational assets for profit, personal interest, and political interests or activities of individuals, groups, or other entities which compromise the safety of organizational assets" [23]. For the avoidance of doubt, this thesis defines 'security risk' as the principles of '*risk'* as established in equation (2.4), incorporating terminologies such as cybersecurity, cyberattack, cyber-threat, and data breach as part of the discussions.

2.3 Risk Assessment Process

Institutional risk assessments process is a standard practice by which institutions operationalise their privacy, security, and compliance with other policies to protect their assets against potential loss [25]. The study by Kaliski et al, proposes five metrics to be associated with any institutional risk assessments process. These are 1) "system characterization"; 2) "threat analysis"; 3) "vulnerability assessment"; 4) "impact analysis", and 5) "risk determination" [25]. This argument is supported by [26], and NIST[7] SP800-30 framework which provides similar guidelines on institutional information security risk assessment. The constructs in the above studies corroborate with the metrics identified in equation (2.4). The approach in this thesis is based on the risk assessment model proposed by Talabis and Martin [14]. In this context, this thesis introduces three additional metrics to the assessment process. These are Threat/Vulnerability Pair (TVP), Risk Modelling, and Policy Evaluation (figure 2-1). The thesis's proposal is based on a dynamic modelling approach, which is built on quantitative method.

[7] National Institute of Standards and Technology

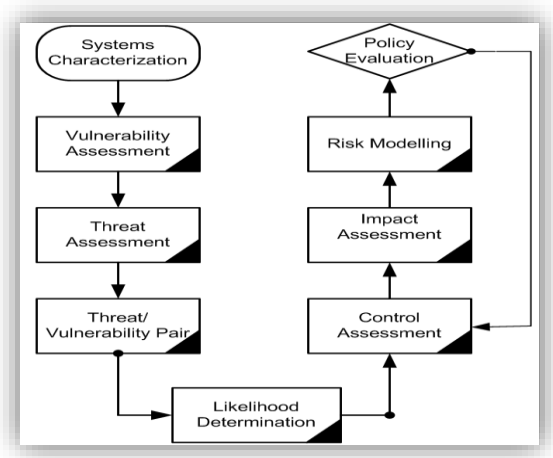


Figure 2- 1: Risk Assessment Framework

2.3.1 Risk Metrics

This section is a summary of the risk assessment framework presented in [14] and described in details in the sections below.

2.3.1.1 System Characterization

System characterization is part of an environmental risk assessment process, which seeks to explore the space or the environment in which the assessment is to be conducted. Thus, the entire information system environment should be characterized in terms of assets (for information flow), operations, procedures and policies. When a risk assessment is pursued as project management, system characterization becomes part of the requirement gathering activity.

2.3.1.2 Assets

Assets are the cyber infrastructure systems supporting business operations. The primary objective of the assessment process is "to identify and define the critical assets to protect, their value, container and the custodians" [14]. Ozier defines assets as both tangible and

intangible resources upon which institutions survive [28]. In relation to cyber infrastructure, assets are defined as the embodiment of an organization's resources, needed to conduct or transact day-to-day business operations. Accordingly, Henderson and Peirson claim that it is the service potential and economic benefits to be derived, and not the physical form of an asset, which is relevant in assessing whether an asset exists [29]. In a related study, Manunta argues that an information asset exists only when a proprietor deems it worthy of protection in [24].

2.3.1.3 Cyber Threats

A threat is defined here as an event (i.e. action or inaction), which are capable of exploiting systems vulnerabilities. Threats could either be external or internal to the system. It is also important to identify threats to their source (i.e. actor and method). In a related study, Touhill and Touhill identified top five cybersecurity threats to any cyber infrastructure system [30]. In a controlled environment, there are multiple threat agents, which could be identified. These include (but are not limited to) "the act of human error, technical hardware failure, technical obsolescence, quality of services deviation from standard services, application/protocol attack, deliberate act of sabotage or vandalism, deliberate act of information extortion, DDoS, Botnets, web interface attack, and advance persistent or state-sponsored threats" [31-33]. Other threats specific to SCADA systems include "Ransomware, Water Hole attack, Dropper, Rootkits, Spyware, Worms, Trojan Horses, Phishing and Spear Phishing" [14].

2.3.1.4 Systems Vulnerabilities

Vulnerability as a security concept has also been discussed in many extant studies; its true meaning is often not clear. In this context, Weichselgartner describes vulnerability as "a system overall susceptibility to loss due to undesirable events" [34]. Vulnerability analysis in an interdependency system is considered as systems susceptibility to its threat exposure (global perspective) and the susceptibility to its internal components (local perspective) [35]. Vulnerability also connotes the weaknesses (within) or factors which increase the probability of threat agents being successful in their

attack [14]. For the purpose of analysis, two different considerations are made with respect to infrastructure vulnerabilities (i.e. current and hypothetical vulnerabilities). Current vulnerabilities are the known vulnerabilities identified in a signature list. Hypothetical vulnerabilities are vulnerabilities that are listed in the secondary vulnerability databases.

2.3.1.5 Controls Mechanisms

The study defines security controls (i.e. countermeasures) as both technical and administrative procedures implemented by institutions (i.e. asset owners and administrators) to protect, prevent, detect and recover from adversaries against threat vectors and systems vulnerabilities. It is assumed that the presence of control mechanisms reduce the likelihood of threat actors exploiting systems vulnerability. Whitman and Mattord propose a control cycle (figure 2-2) to evaluate the effectiveness of existing security control mechanisms [36]. According to Whitman and Mattord, an effective security control mechanism must take into consideration the specific asset it is to protect, the level of risk that can be accepted or otherwise [36]. Accordingly, they identify an asset to protect to be directly linked to the effectiveness of the control mechanism. Additionally, the authors argue that the effectiveness of security control to an asset is proportional to the vulnerabilities the asset is exposed to [36].

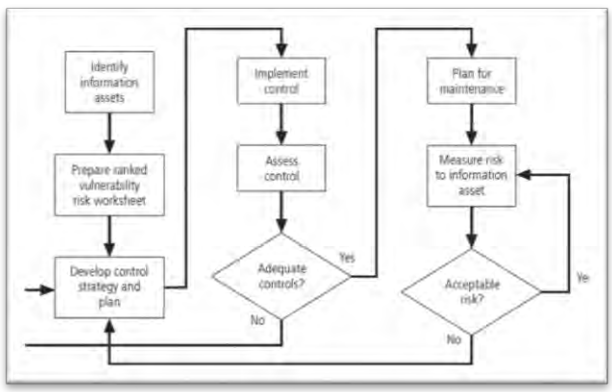


Figure 2- 2: Risk Control Cycle [36]

2.3.1.6 Threat-Vulnerability Pair (TVP)

Whether known or unknown, critical infrastructure systems and their interdependencies face both internal and external threats; it is the vulnerability inherent in the system that makes the system susceptible to threat attacks. TVP is introduced here as the matching between potential threats and vulnerabilities [14]. The authors propose the following TVP score (see table 2-1) as a quantitative measure for any quantitative risk assessment process.

From table 2-1, a matching scale of less than 1 (i.e. per year), denotes a very weak TVE pair; meaning there is near zero chance of threat exploiting system vulnerability. Thus, the higher the rate of TVE pair, the greater the chance of threat agent exploiting system vulnerability.

Table 2- 1: Threat-Vulnerability Event (TVE) Score [15]

Description	Scale	TVE Score
>100 times per year	Very likely	1.0
>=50 <100 per year	Likely	0.8
>=10 < 50 per year	Somehow likely	0.6
>=1 <10 per year	Not Likely	0.4
<1	No Chance	0.1

2.3.1.7 Likelihood Estimation

This is the probability of a threat vector (i.e. agent, method) exploiting systems vulnerability (as a function of time *'t'*). "It is defined as a quantitative measure of the probability of a threat vector exploiting system's vulnerabilities (TVP), measured as the function of the available control mechanism" [14]:

$$L_t = [(A(V) * T)/C)]^{8} \quad (2.6)$$

[8] For quantitative analysis, the values for likelihood determination are scaled from 1 (being very low) to 10 to (the most likely possibility)

2.3.1.8 Impact Assessment

Impact assessment as part of the security assessment process is the determination of the extent of a loss to an asset due to a successful threat attack, measured by the value (cost) at loss and effect. According to Miller, an impact assessment activity should focus on the Annual Loss Expectancy (ALE) [37]. Chen, on the other hand, argues that impact analysis is the factor of the "likelihood of the threat occurring"; the loss resulting from the attack; and the rate of occurrence. For example, the impact of Shamoon virus attack (which disabled over 30,000 workstations on Saudi Aramco large national Oil and Gas company) in August 2012, that led to the disconnection of their IT system, brought both tangible and intangible losses to the company [38]. There have also been reported instances of industrial control failures where the severity of impacts has resulted in human fatalities. Two such cases can be found in [39-40].

2.3.1.9 Risk Modelling

The primary dimension of the risk assessment process as defined in this thesis is to map out the potential future scenarios and consider the way such outcomes should be regarded; as desirable or undesirable [41]. The subjectivity associated with predicting future scenarios in the assessment process is very critical. The modelling approach is introduced as a solution to map out future scenarios in the assessment process. The insights gained from the assessment are then mapped to inform decisions about whether to accept the current situation (e.g. an existing system or a proposed design) or whether the systems should be changed or redesigned.

2.3.1.10 Risk Decision and Policy Evaluation

Quantitative risk[9] factor as defined here is obtained by multiplying the impact of attack (i.e. the value at lost) by the likelihood of the threat event; given as: $(R = L * I)$. It is argued, when future events become unpredictable, risk determination becomes subjective; giving credence to a qualitative measure of low, medium and high risks

[9] See Appendix 8 for the Risk Metrix Score

interpretations. It is on the basis of unpredictable future risk events that the introduction of systems modelling is even more useful in the risk assessment process. The process is also useful in the complex and network-centric systems where it is difficult to predict the behaviour of threat vectors. The outcome of the risk estimation and the discovery made from the assessment process necessitate the need for asset owners to evaluate systems security risk exposure through policy evaluations. Policy evaluation should, therefore, address issues relating to space where systems reside, systems' vulnerabilities (i.e. internal weaknesses), threat actors and their methods, control mechanisms, contingency planning, incidence response, disaster recovery, business continuity planning and business impact analysis.

2.4 Overview of Cloud Computing

Since its conception (ca 2005), cloud computing has been interpreted differently by both researchers and practitioners, and the debate is likely to continue. A study by Wang et al, argue that "There is still no generally accepted definition for cloud computing, albeit the practice attracting increasing popularity and greater attention" [42]. Accordingly, Jamsa also claims that for years, both system developers and network administrators have represented the Internet as a cloud [43]. An assertion this study agrees and references as such. Moreover, there are many who argue, there is nothing new in the cloud; 'just old wine in a new bottle' [44]. This is because, the core technologies supporting cloud computing (i.e. virtualization, data centre, grid computing, distributed computing and Service Oriented Architecture (SOA), have all been available, before the 'birth' of cloud computing. If the above claim holds, then, it can be concluded that it is the combination of these technologies to the realisation of cloud models that have changed or shaped how Information Technology (IT) and its related services are deployed, accessed and paid for. Whichever way one looks at it, the basic concept behind cloud computing is that 'anything' that can be done using the power of computing (from portable tablet to a corporate data centre) could be shifted to the cloud [45].

In its general interpretation, cloud computing means different things to different people and the concept encompasses a whole range of IT

services which can be hosted on a variety of platforms. To an individual, cloud computing means accessing an email, using Instagram, Twitter or Facebook. For organizations, it means the ability to outsource computing resources and services as a utility, rather than having to invest a massive amount of resources to host all the necessary large-scale data centres to provide a given level of IT services. And for governments, Wyld claims *"the value proposition of cloud computing is especially appealing, given both changing demands for IT and challenging economic conditions"* [46]. A study by Vaquero identifies over twenty-two different definitions and interpretation of cloud computing [44]. Similarly, in a review of fifty-three cloud definitions, there were thirty-two different definitions and interpretations of the concept, with the remaining twenty-one authors aligning to the definition proposed by the National Institute of Standards and Technology (NIST). It is, therefore, fair to say, cloud paradigm is still evolving and the integration of Internet of Things (IoT), Web of Things (WoT) and Machine-to-Machine technologies is likely to make the cloud platform, even more, wider and complex in terms of design, deployment, and management. This argument is supported by Vaquero who emphasises that "looking for a common denominator for cloud would lead us to no definition as no single feature is proposed by all definitions" [44].

2.4.1 The Proposed Definition

In this study, cloud computing is defined as: 'a public network infrastructure which integrates large-scale data centre resources, virtualization and hypervisor technologies for the provision of computing and IT services (i.e. computational, storage and communication) as a utility'. Unless otherwise stated, the term cloud in this study is used in its general sense, incorporating the Internet as public network services. This composition is useful for the conceptualization of the technology for academic discourse. Supporting this argument, Gong argues that with multiple definitions and interpretations of cloud concept, the definition itself is unimportant for academic discussions without the understanding of cloud core characteristics [47].

2.4.2 Cloud Service Models

Cloud computing is classified based on how cloud services are provisioned; generally termed as "X-as a service" (XaaS) models. There are multiple "X-as-a-Services' clouds; the three common ones discussed in this study are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) generally known as the SPI models (figure 2-3).

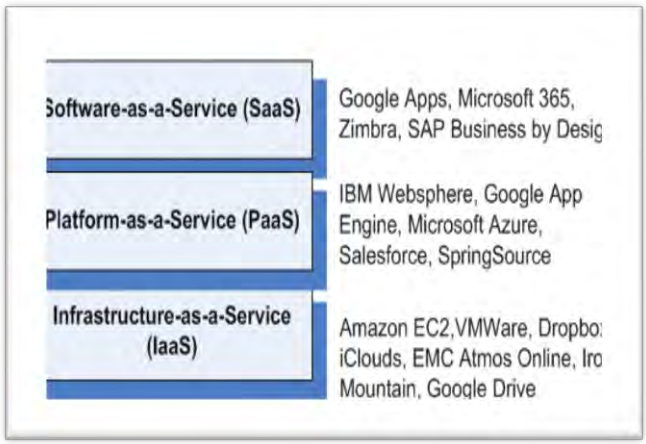


Figure 2- 3: Cloud Offerings Hierarchy

2.4.2.1 Software-as-a-Service (SaaS)

SaaS model provides the functionalities of a traditional software application through Web-enabled protocols. Per the structure, a cloud service provider (CSP) runs software applications on top of cloud infrastructure, provided by a third-party infrastructure service provider (usually invisible to the service consumer). Examples of well-known SaaS applications include Google Docs, Google Calendar, Google mail, Google Forms, Office 365, Microsoft OneNote, and Business SAP.

2.4.2.2 Platform-as-a-Service (PaaS)

According to Hilley, PaaS cloud provides an enabling platform for the development of software and applications [48]. The model offers a unified stand for systems and application developers to build custom applications, running on clouds infrastructure support, utilising the cloud ability to scale up resources (automatically). Per this structure, the management of the underlying infrastructure is the responsibility of the infrastructure providers while users control the deployed applications and, their configurations [49]. Some of the well-known PaaS solutions include IBM Websphere, Saleforce.com, SpringSource, Morphlabs, Google App Engine, Microsoft Azure, and Amazon Elastic Beanstalk.

2.4.2.3 Infrastructure-as-a-Service (IaaS)

Cloud IaaS provides infrastructural resources as a service to the higher-level cloud layers, which is then used to construct new cloud applications [50]. Example of IaaS deployment services includes Web-service hosting, Google Drive, Amazon Web Service (AWS), Google Compute Engine, Microsoft Azure, etc. Other structural functions of cloud IaaS involve making resources such as a hypervisor, virtual machines, network and storage servers, CPU, memory, storage instances and other hardware components more readily available and accessible as a utility (users paid use of resources). It is the inherent structure of the IaaS stack coupled with its complexities that make the IaaS susceptible to cyber adversaries. This is because an attack on the infrastructure stack does not only destabilise the entire cloud structure but other dependent resources. These inherent risks make security prioritisation of IaaS worth exploring.

2.4.3 Deployment Models

Cloud deployment describes how cloud services are deployed to consumers. It explains the ownership composition of cloud services. Generally, the offering structure is categorised as Private, Public, Hybrid and Community Clouds as explained below.

2.4.3.1 Private Cloud

This is an ownership arrangement whereby individual organization owns the cloud infrastructure resources. Thus, cloud resources are within the confines of the agency's firewall, managed by its IT team [51]. Private cloud is suitable for institutions with sensitive data where a resource sharing presents a potential danger (e.g. GovCloud) or where security policies do not permit data to be hosted offsite.

2.4.3.2 Public Cloud

Per this arrangement, a private cloud provider offers computing resources to the public as a utility (i.e. pay-per-used). In this case, the infrastructure resource is owned and managed by the cloud service provider (CSP) or its third-party agent, who owns and manages the infrastructure. While security, privacy, and trust remain the argument against public cloud adoption, its greatest merit is the superior cost savings, due to demand aggregation, bulk purchasing and large-scale resources, as well as reduced per-unit costs. Some public cloud providers occasionally offer some of their services for free as an enticement for new customers and also as a tool to lock-in existing ones. Facebook, Instagram, Google, Microsoft, IBM, Amazon, Alibaba, are few popular public cloud service providers.

2.4.3.3 Hybrid Cloud

A hybrid cloud combines the ownership structure of a public and a private cloud. Per this structure and ownership arrangement, the owner may decide to host some services (e.g. computation, network and storage), in a public cloud environment while other processes get hosted in a private cloud platform.

2.4.3.4 Community Cloud

This is a cloud service arrangement in which the ownership structure is made up by a group of 'community' members with an agreement to share cloud infrastructures resources. Per this arrangement, two or more institutions (as a community) may decide to jointly construct and share computing infrastructure (for the benefits of large-scale/ high capacity computing resources). The size and number of

organizations are among the factors which determine the scale of demand and cost savings that can be obtained from the community cloud arrangement. Based on the agreed principles, certain resources could be hosted by a third-party infrastructure service provider or one of the organizations within the community [52]. The focus of the thesis is on cloud infrastructures (IaaS) setup. Notwithstanding, an overview of other models is provided.

2.5 Cloud Infrastructure Stack

Cloud infrastructure stack consists of cloud infrastructure layers. There are two main types of infrastructure stack: Physical Resource Set (PRS) and the Virtual Resource Set (VRS). Above them is the cloud functional layer which is made up of the computational compartment e.g. MapReduce [53]; storage compartment e.g. GoogleFS [54]; and communication (networking) compartment e.g. OpenFlow [55]. Functionally, cloud infrastructure stack involves starting up and shutting down active resources, managing processes, establishing network topology, capacity configuration, and memory management. Others functions include resource scalability, heterogeneity and accessibility.

2.5.1 Physical Resource Set

The physical resource set is made up of the physical resources, which support data centre infrastructures and service-oriented architecture (SOA). Unlike virtual resource set, the physical resource set is hardware dependent and therefore vendor-specific. They include large-scale data centre (for storage), physical memory and multi-purpose processors (for computation). Examples of cloud PRS are Ethernet cards, SCSI/IDE, Huawei U2000 for networks and fibre infrastructure, CloudStack from Apache, Microsoft Cloud Fabric and HP Site Scope Multiview.

2.5.2 Large-Scale Data Centre

Data centre infrastructures (figure 2-4) consists of the core physical cloud infrastructure setup. They are usually built to contain a massive amount of storage resources, multiprocessors as well as some high-

speed fibre optic data network facilities. The architecture of a traditional data centre includes the data centre power generator (for backup power), Integrated Datacentre Solution (IDS) systems, network infrastructure services, Site Scope Multiviews (SSM), topology view and other system monitors. Other physical resources set making up the centres include security monitors, backup generators (i.e. power), human-machine interface (HMI), coolers, Security Infrastructure Systems (SIS). The main features of a large-scale data centre are scalability, load balancing, instrumentation monitors, and infrastructure enhancement management.

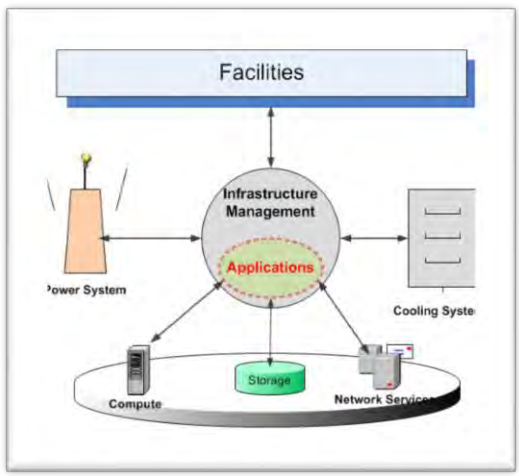


Figure 2- 4: Data Centre Structure

2.5.3 Virtual Resource Set

Cloud virtualization presents an abstraction that separates the physical resource set (i.e. the hardware) from the underlying systems and application software (see figures 2-5 and 2-6). Thus, virtualization decouples the higher-level cloud applications (PaaS and SaaS) from the underlying infrastructure systems (IaaS). The abstraction layer is termed as the hypervisor or virtual machine monitor (VMM). VMM is a piece of software which manages the sharing of resources among multiple tenants [56]. Some example of

VMMs includes Xen (figure 2-6) and KVM (close sourced VM), VMWare and HyperV (open sourced VM).

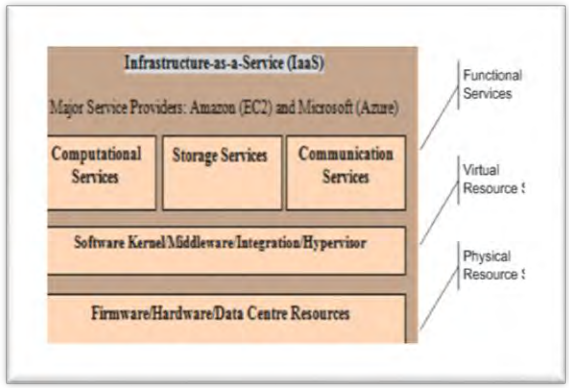


Figure 2- 5: Cloud Infrastructure Stack

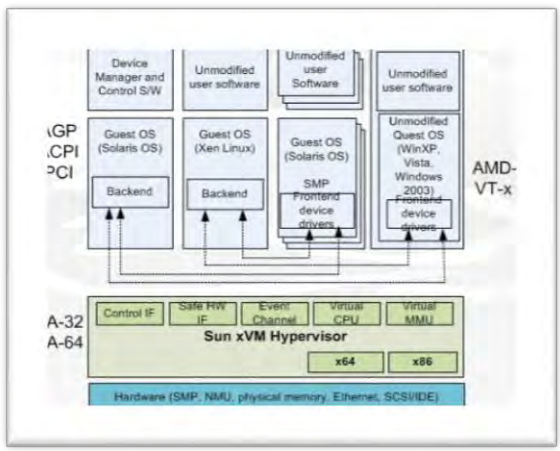


Figure 2- 6: Sun xVM Architecture

Cloud VMs are categorised based on the virtualization process. These are Storage, Hardware, Application, Operating Systems (vOS) and Para virtualizations. Each of these sets presents unique structural characteristics. Above the PRS and VRS layers lies cloud Functional Resources Set (FRS), which consist of high-level computational services e.g. MapReduce, ([53], storage set e.g. GoogleFS [54], and network services e.g. OpenFlow [55] (figure 2-5). On top of the FRS is cloud-induced Application Program Interface (API) (figure 2-7), which allows cloud service consumers (CSCs) to provide their applications on PaaS. Cloud API enables users' application to communicate with the cloud platform. For example, Amazon ECS, Microsoft Azure, and GoGrid provide a platform for their users to provision computational, storage and networking services.

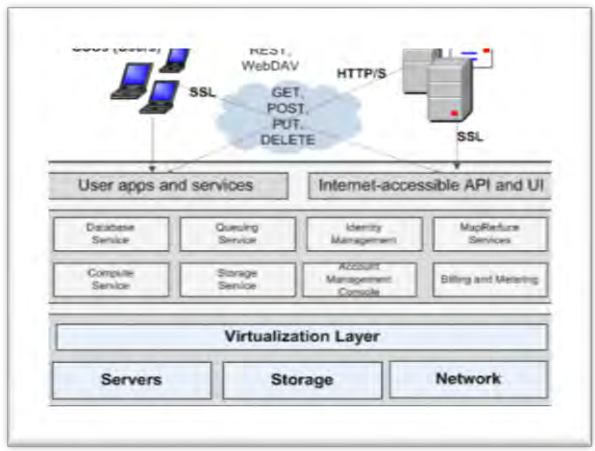


Figure 2- 7: Cloud Induced API

2.6 Cloud Specific Risks

The thought of hosting data resources in the cloud environment is very concerning to many information resource custodians. The primary concern of data custodians and asset owners is the safety of their data. To the cloud users, secured cloud service means that any potential risk factor is thoroughly reviewed so as to provide a

comprehensive understanding of the situation, and to ensure that any unexpected consequences are averted. The primary responsibility of the cloud provider is to ensure the confidentiality, integrity, accessibility, accountability, traceability and auditability of data stored in the cloud.

Security challenges specific to the cloud and controlled environments include network, storage, virtualization and system's application [57].

2.6.1 Network Level Security

Understanding network-level security of cloud infrastructure is very significant to customers who adopt the technology because of the changes to the security requirements to the internal network topology. Customers and asset owners must, therefore, review how local network infrastructure interacts with the cloud infrastructure providers. In adopting cloud services, two security concerns do exhibit. First, service providers must ensure the security and safety of data-in-transit and then guarantee that the resources would be available when and where they are needed. Furthermore, cloud service providers must also address the issue of multi-tenancy abuse. Thus, service providers must ensure that a customer resource is assigned to the rightful owner or the user has been assigned to the right organization per the conditions of the Service Level Agreement (SLA).

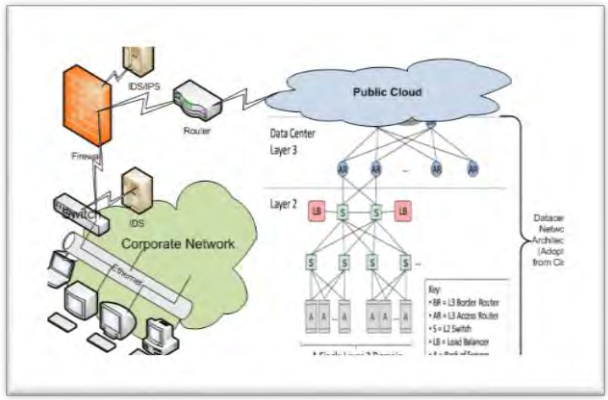


Figure 2- 8: Public Cloud & LAN Integration

Figure 2-8 is a modified Cisco data centre Network structure depicting a corporate WAN network that is integrated with cloud infrastructure using a layer 2/3 router. The architecture above involves a local network service (LAN) that is connected to the public cloud (built on the provider's data centre networks) where data communications occur between the provider and the customer's networks.

This setup has become the standard for most corporate cloud users. These types of setups are known to have vulnerabilities, which expose the setup to network induced threats. Other known threats are DoS, DDoS, and DNS cache poisoning. Thus, threats, which are common in the traditional network systems, become apparent when a local corporate network is connected to public cloud infrastructure systems. One proposed solution is the use of HTTPS; notwithstanding, the HTTPS protocol has not been standardized. Indeed, many cloud platforms are still accessible via HTTP. Other recommended solutions include network tunnel hardening using encryption (SSL, IPSec), IDS and IPS). Whilst these solutions have been in existence for years, they have not been proven to prevent attacks on network-centric systems.

In response to these and other related cloud threats, FIPS[10]' recommends State-owned institutions in the USA to adopt Government clouds known as GovCloud. On this basis, Amazon has implemented a virtual private cloud (VPC) on public cloud platforms specifically for State-owned institutions. According to Amazon, the VPN architecture provides a point-to-point encrypted tunnel between their servers and clients' resources using L2TP and PPTP. Amazon assurance is that the use of VPC protocols in cloud provisioning does increase security controls, and protect government information resources from network-related attacks. Nonetheless, VPN itself is a point-to-point protocol and cannot guarantee secure point-to-point-traffic.

2.5.2 Storage Level Security

Cloud infrastructure providers allow service users to deploy database applications on virtual data servers, which are virtual machines with pre-installed and pre-configured storage systems. There are two types of datasets in the storage area; transactional and analytical data [58]. Security risks associated with cloud storage environment include shared storage resources due to multi-tenancy and geo-distribution of storage servers. For instance, both Microsoft and Amazon have the options, which allows customers to choose the preferred regional server location (for storage services). However, due to fail-over and load balancing, data stores in the cloud are replicated across remote server farms, which locations, are usually unknown to the users. Additionally, multi-tenancy arrangement in cloud environment raises serious data integrity issues such as resource abuse by co-tenants, service hijacking and nefarious use of resources by co-tenants.

Moreover, in the cloud storage platform, Secure Copy Program (SCP) is a standard copying protocol for copying data (via TCP/IP). In this case, data in transition becomes vulnerable to IP sniffing or IP hijacking, man-in-the-middle attack and other related threats. The solution to this problem is encryption and hashing. The challenge, however, is that transactional data needs to be decrypted before they can be processed, defeating the whole concept of encrypt-to-protect.

[10] Federal Information Processing Standards

One proposal instituted by Cloud Security Alliance (CSA) is to develop trust with their service providers. However, in the matter of data protection, trust has legal limitations against controls and governance.

2.6.3 Virtualization Level Security

According to Perez-Botero et al, there are three main vectors associated with the hypervisor: source, method and target [59]. At the virtualization level, the host VM contains a set of virtual CPUs (vCPUs) which are usually allocated to each of the guest VMs [60]. However, CSCs do not have access to this layer and its processes because the CSPs or their agents manage it. Attacks on both hypervisor and VMs have increased in recent times. A study by Vogl, for example, identifies three common threat vectors related to cloud virtualization. These are 1) covert channels, 2) resource monitoring and 3) single source of failure [61]. For example, in CVE-2010-4525[11], Perez-Botero et al, identified hypervisor memory contents disclosure (via vCPU registers) due to "incomplete initialization of vCPU data structures in which one of the padding fields was not zeroed-out" [59]. The authors argued, because virtualized memory allocation takes place in the kernel, the VM padding field ends up contaminating the information from data structures previously used by the hypervisor or the previous user if the memory cleaning process is compromised [59].

Cloud virtualization like all other resources requires protection against all possible threat actors because an attack on virtual resources compromises the integrity of the compartments of the vMMs. One example is the "Blue Pill attack" demonstrated by Joanna Rutkowska and Rafal Wojtczuk [62]. There is also an instance where a virtualization application initiated by system vulnerability enabled a remote attacker to execute sensitive Unix commands to corrupt virtualization resources (including recursive directory removal command (rm –r) [63].

[11] Common vulnerability exposure database (source: http://www.cvedetails.com/)

One of the core functionalities of the VMs is resource monitoring, which involves control actions such as (start, shutdown, pause, restart the VMs), and resources modification. Unfortunately, system administrators or an authorised user with control privileges can misuse this procedure. For example, Xen access [64] which is an authentication protocol, is capable of allowing sysadmins (procedure) to run a user-level process in Dom0. This procedure grants administrator access (during runtime) to the memory of a guest VM. This tool, which is available to most systems administrators could be manipulated and abused by an insider creating serious threats to customers' data. Besides, communications between guest and the host VMs occurs through the shared virtual network. In such a protocol, the host VMs can monitor and sniff network traffic [65]. Additionally, Kirch argues that shared network infrastructure enables an attacker to exploit some critical VMs information (e.g. shared clipboard) [66]. Two other threats known to hypervisor are hyper jacking and guest-hopping attack [43]. The former is referred to as the process of taking over the hypervisor and the later as an attack from one guest operating system on multi-vOS platforms [14].

2.6.4 Application Level Security Risks

At the application level, the inter-communication process between CSPs applications and that of CSCs takes place via a cloud induced Application Program Interface (API), which act as a communication link. Example of cloud-induced API is ReST, SOAP, HTTP/S and XML/JSON. Application-level security has vulnerabilities which are inherent in cloud induced APIs. According to SANS Institute, until 2007 very few attacks were perpetrated against vulnerable API. However, the openness in the program development infrastructure means that criminals intend to cause havoc are able to exploit systems vulnerabilities (from weak programming codes). In a related study, Dawoud et al detailed a well-known attack on protocols using "XML signature for authentication or integrity protection" which are executable on web services, consequently affecting interdependent resources [65]. In a related study, Jensen demonstrates how an attacker broke the security barrier between the cloud user browser and the service application using DNS spoofing [67]. Furthermore, at

the application level, there are multiple opened and closed source software implementations such as Eucalyptus and Nimbus, which interact with other cloud services. These applications have known vulnerabilities which expose systems application to threat attack. Each of these applications presents various security concerns, which require assessment. For example, the 'OWASP Top 10' contains the ten topmost application-level security threats in the web-based environment [68].

In addition to these specific threats, there are other disadvantages relating to hosting applications and data in the cloud environment. These include country-specific (or jurisdiction) data protection and other legal matters, malicious insiders, vendor lock-in and the risk of cloud provider folding up or going into administration. These and other security challenges show the extent of danger cloud infrastructures pose to critical infrastructure systems. Notwithstanding, cloud adoption among public service institutions keeps rising. According to IDC, "Worldwide Cloud IT infrastructure spending is forecast to grow 32% over in 2017, driven by public cloud data centre expansion" [69].

2.7 Critical Infrastructure Systems

Figure 2-9 provides a topographic structure of how a power grid is integrated with a public network infrastructure. The diagram depicts some of the key components contained in a typical power grid. The difference between the modern power grid and the old-analogue type is the convergence of the modern power grid with public networks. The convergence has opened up the grid to public networks, exposing the grid to various forms of cyber threats.

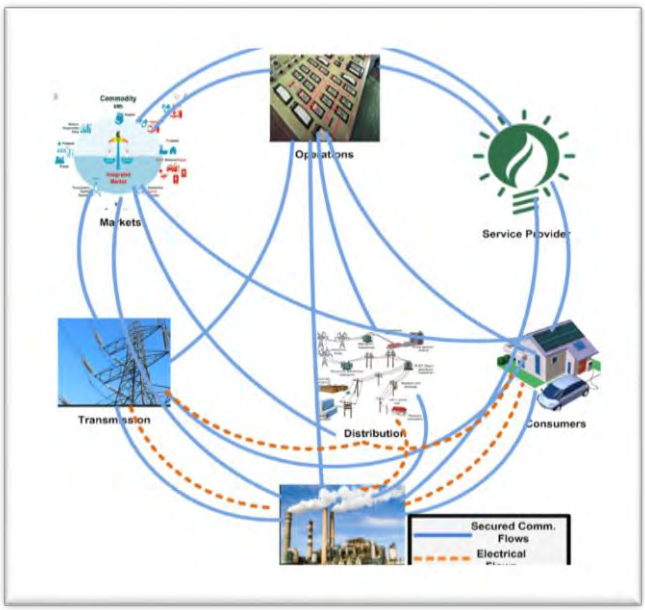


Figure 2- 9: Power Grid Conceptual Model

In the succeeding sections, the study reviews the core components of the critical infrastructure systems with much emphasis on downstream power distribution.

Critical infrastructure systems are loosely defined "as large-scale socio-technical assets" upon which societies thrive, and are essential for socio-economic living [70]. The USA President's Commission on Critical Infrastructure Protection (PCCIP) proposes eight categories of critical infrastructure systems. These are "Information and Communications, Electrical Power Systems, Gas and Oil Transportation and Storage, Banking and Finance, Transportation, Water Supply Systems, Emergency Services and Government Services". In a related study, Rinaldi et al argue that systems such as food and agriculture distribution, healthcare delivery, and educational system should also be included in the classification of critical infrastructure services [2].

Little further argues that it is the services of by the infrastructure provider which delivers real value to people and society as a whole [72]. Extending this argument, Hassel claims that the societal consequences of critical infrastructure breakdown depend not only on the extent and duration of the service disruption but also, how dependent the society as a whole is dependent on these services [41]. In recent times, critical infrastructure setups have undergone and continue to undergo considerable changes due to the advancement and integration of information and communication technologies. According to Zimmerman, "technological changes have improved the provision of services for transport, water, electricity, and communications [73]. These changes often transforming the way society thrives, subsequently increasing the fragility and vulnerability of critical infrastructure systems and the services they provide, making them more complex and interdependent" [73].

The interdependencies between critical infrastructure setup mean that any disruption in one system can cascade to others, "causing secondary, tertiary and even higher-order unexpected consequence", such that, the resultant effects can cascade back from where the disruption originated [41]. In this study, it is argued that any method of exploring security risks in systems interdependency, should consider the dynamic complexities resulting from systems interconnectivity. This is because the complexity associated with interconnected systems contributes to the understanding of the method of assessing their threats exposure. According to Haimes and Longstaff, it is not usually possible to fully understand the cascading effects of infrastructure interdependency due to systems interconnectivity [74]. Additionally, it is argued that the complexity of the interconnected system requires "systemic and quantitative risk modelling, assessment, and management efforts" [74, 75]. It is reasonable to say, there are different perspectives to how these systems are explored, and a method of such assessment is worth exploring. This argument is supported by Eusgeld et al who claim, "there is no single 'silver bullet solution' to the problems of assessing risks associated with critical infrastructures" [76].

Primarily, the focus of the thesis is on downstream energy sector infrastructure and related technologies. Some of the major functions

specific to these infrastructure systems include: "fabrication, refining, gas processing, raw gas purification systems, pump control and blow-out prevention, well-monitory manifolds management and net oil measurement. Other additional services are metering and billing, transportation tracking, storage monitoring, safety control operations, separation and burner management as well as services which support the distribution of energy to the final consumer" [14].

The recent advances in the industrial automation system, coupled with the increasing demand for high-level visibility from production lines have necessitated the quest for controlled automation in the energy sector. The convergence is supported by the integration of information and communication technologies in industrial control systems (ICS) and logic-based digital design [14]. As Bodungen et al put it "today, ICS and automation are found in nearly every aspect of our daily lives" [6]. HVAC[12], SCADA systems, sensor networks in substation automation and power grid transmission, and robotic controls are some of the few examples of how control systems have changed the dynamics of industrial control systems [6].

In addition to the general IT infrastructure systems, Enterprise Resource Applications (ERAs), Electronic Data Interchange (EDI), Database Management Systems (DBMS) and other controlled technologies are mostly integrated to serve as the Operations Technologies upon which critical infrastructure systems function [77]. This convergence between IT and OT in a controlled environment has created a new platform for a modern (digital) industrial automation process. Subsequently, the convergence has led to a situation whereby assets owners and systems administrators constantly deal with two interconnected network systems: "IT networks for business information" and "Operational Technologies (OT) for operations" [14]. "Today, this convergence is not only common, but prevalent, and business reasons often require that certain OT data be communicated through the IT networks" [6].

[12] Heating, Ventilation and Air-condition

2.7.1 Infrastructure Complexity

Technology integration, digital migration, interconnectivity and systems independencies have become the foundation upon which critical infrastructure systems are built. These characteristics have made critical infrastructure systems inherently complex. The term complex was first applied to critical infrastructures by [78,79] in the study of a complex adaptive system[13] (CAS). In a related study, Stapelberg argues that "characterising the structural properties" of critical infrastructure systems "is of fundamental importance to the understanding of systems dynamics" [80]. Contributing to the discussion, Strogatz provides the following as the factors which have contributed to the difficulty of understanding interdependent critical systems [81]:

i. "Structural complexity - increasing the number of component nodes and links between the nodes"
ii. "Network evolution – changing links between network nodes over time"
iii. "Connection diversity – links between nodes could have different weights, directions, and signs"
iv. "Dynamic complexity – in a network the state of each node can vary in time in multiple ways"
v. "Meta-complication – various meta-systems or outside network complications can influence each other"
vi. "Component diversity – components within a network may be of very different nature"

Complexity theorists agree with the perspective of system theory, suggesting that different components of a system are interconnected to the extent that changes in one component affect the other, causing second, third and n-tier dependency failure of interdependent systems [82]. Furthermore, Strogatz claimed, a unified framework is, therefore, "needed to develop a solid theoretical understanding of physical processes underlying the formation of complex infrastructure systems" [81].

[13] See Appendix 10 is the Complexity Adoptive Index

2.8 ICS-SCADA

SCADA system consists of a group of components, which support industrial control operations in a controlled environment. SCADA belongs to the family of Operational Technologies (OT) supporting critical infrastructure systems such as water and sewerage, power transmissions and gas pipelines, and other distribution network systems [77]. Some core features of SCADA include "Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) also known as controllers, Human Machine Interface (HMI), Safety Instrumentation Systems (SIS), and Variable Frequency Drives (VFD)" [14]. SCADA is found in almost every critical infrastructure systems and is used in all types of controlled and monitoring systems. Apart from supporting industrial automation process, SCADA systems are also used to gather real-time data, control industrial processes, monitor equipment and view systems from remote locations [6]. Some of the core OT functions include " acquiring data coming from the industrial processes (i.e. temperatures, pressures, valve positions, tank levels, human operators) and the direct control of electric, mechanical, hydraulic or pneumatic actuators" [77]. Characteristically, SCADA functions are described based on the underlying component and its operations [83]. Appendixes 3 and 4 describe ICS-SCADA functional architecture and the ISA/IEC-62443[14] SCADA reference model respectively.

2.8.1 SCADA Specific Threats

The digitization of industrial automation process presents various forms of risks to the industrial control space, which were not common in the hard-wired analogue platform[15]. According to Bodungen et al, most of the current protocols, such as "ControlNet, DeviceNet, Profibus, and Serial Modbus" are based on proprietary applications and have known vulnerabilities [6]. Furthermore, the efforts by system administrators to use open technologies such as Windows OS,

[14] Formerly ISA-99 is a series of standards and technical specifications which define procedures for implementing electronically secure industrial automation and control systems (IACS)

[15] Appendix 11: Top 10 SCADA Vulnerabilities

Linux, and ethernet protocols (i.e. IPs) to control, view and monitor controlled technologies have exposed the systems to various forms of threats that were relatively unknown in the legacy systems [14]. Consequently, the integration of OT with open public network technologies such as cloud computing has made the situation even more alarming. Examples of enterprise-wide operation technologies supporting controlled environment are Honeywell's Experion Process Knowledge System (PKS) (for Terminals), Huawei Tipping Point, Integrated DataCentre Solutions (Software), and Tank Inventory Systems (single-window interface for Tank Gauging Systems). Other related systems include Emerson Rosemount TankMaster WinOpi, Microcontrollers, Site Scope Multiviews (HP), Honeywell Enraf BPM, Smart Meter Management, Huawei M2000 (for monitoring), and Huawei U2000 (for network connectivity).

Pieters, further argues, the traditional implicit of the safety of critical systems have been on the general tolerance of creating physical boundaries around assets and their components and compartments (perimeter defence) [20]. Modern critical infrastructure systems by their structure, design and operations have become technology dependent and highly interconnected, making them more complex in design and deployment [14]. And it is not always clear in such space, to determine where an organization's boundary lies, "making it difficult to implement traditional perimeter defence systems" [14]. The security philosophy of the 'outside' versus the 'inside' is problematic in an interconnected controlled environment.

Cybersecurity risks relating to critical infrastructure systems include both physical and logical as well as technology defects in the infrastructure setup [14]. Furthermore, in a controlled environment, multiple threat sources exhibit including; human error, technical (physical or hardware) failure, equipment obsolescence, quality of services deviation and application/protocol attack [31, 32]. Other known threats are 'deliberate act of sabotage or vandalism', "deliberate act of information extortion, DDoS, Botnets, web interface attack, and advance persistent or state-sponsored threats" [31, 32]. Other specific ones are Ransomware, Water Hole attack, Dropper, Rootkits, Spyware, Worms, Trojan Horses, Phishing and Spear Phishing [31, 32]. Moreover, the convergence of controlled

systems with IoT, Web of Things, Machine-to-Machine and cloud computing has also exposed the former to IP-based attacks.

For example, in 2010, there was a reported case of hackers using STUXNET to attack industrial control systems globally [84]. This attack specifically targeted computers controlling oil refineries, gas pipelines, and power plants which seriously affected major energy companies worldwide [84]. According to Holla, hackers are using common tools such as: 'Metasploit' to hack anything from a small webcam to controlled technologies [85]. Per the 2015 Global State of Information Security Survey', the number of cyber incidents reported globally in the power & utility industries increased from 1,179 in 2013 to 7,391 in 2014 in [85]. Similarly, records from the Breach Level Index (BLI) indicates that since 2014, data breach against cyber infrastructure resources has more than doubled [86].

An analytical study of data breach disclosure shows that the technology industry and state-owned institutions are the greatest hit in terms of a data breach. Moreover, among the critical services, the energy industry seems to have become the most attractive targets for cyber adversaries due to its richness in resources and the severity of impact. According to the U.S. Department of Homeland Security (in a news file, published in April 2012), "American water and energy companies, deal with a constant barrage of cyber attacks on a daily basis". These incidents usually take the form of cyber espionage, Denial-of-Service (DoS) attacks against control systems. Moreover, Fernandez and Fernandez claim that modern industrial control systems have created more efficient and failsafe operating conditions, enabling systems' operators and asset owners to monitor, control and troubleshoot systems from remote locations in real-time [87]. However, monitoring and controlling these systems have become an enormous undertaking, requiring constant supervision. Any single point of failure can disrupt entire operations, potentially cause a catastrophic impact and perhaps bringing a nation to its knees [87].

Extant studies indicate that during the past few years, major critical installations around the world have in one way or the other witnessed carefully engineered and profoundly complex cyber attack using vectors such as BlackEnergy, HAVEX, Sandworm, 'Stuxnet', 'Night

Dragon' and 'Shamoon'. For instance, in 2015, an Automated Tank Gauge (ATG) (a device used to monitor the gasoline levels at refuelling) across the United States, was used to remotely access oil tanks leading to systems manipulation. This unexpected threat activity caused nation-wide destruction to a gas supply, which led to the shutting down of the flow of fuel to some parts of mainland USA and Canada [77]. Similarly, on September 10, 2012, Telvent[16] became a victim of a sophisticated Advanced Persistent attack [77].

2.9 Risk Assessment Framework

Security risks associated with critical infrastructure systems vary and depend on a wide range of factors including the sensitivity of the information assets, system architecture, operational functions, systems complexity, countermeasures, interdependent resources and existing security risk policies. To strengthen the safety and security of critical systems, both asset owners and system users need to perform a regular security assessment of their controlled environment [26]. Institutional security risk assessment processes have become the common standards by which institutions assess the strength of their cyberspace. Various assessment frameworks exist, both in practice and in literature, explaining how the security risk assessment processes have been conceptualised over the years.

A study by Tweneboah-Koduah and Buchanan provides a summary of six existing security risk assessment frameworks (see Table 2-2 appendix 5)[17]. Their involves Six (6) independent risk assessment frameworks. Among them are Three (3) governmental level frameworks and Three (3) enterprise-wide frameworks. According to the study, none of the existing risk management frameworks is focused on interdependent critical infrastructure systems.

[16] An IT and Industrial Automation Company specializing in SCADA, GIS and related IT systems for pipeline, energy, traffic, environmental monitoring

[17] Summary description of the models in Appendix 5

2.10 Gaps in the Literature

The review has provided a better understanding of the subject matter and reveals the lack of clarity among experts on the very important theories they have propounded. The ensuing confusion adds to the difficulty in defining and normalising existing security risk assessment processes as well as the clarification as to which method is apt for our discourse.

Furthermore, the review uncovers the lack of adequate research in the area of critical infrastructure protection. It also confirms the thesis's accession that research in the area of infrastructure interdependency (in the perspective of protection) is developing. Moreover, the very few discussion on the subject in the existing literature, appear to be skewed towards metrics identifications, with little (or no) emphasis on conceptualization as approached by this study. Certainly, the 'identification' approach as observed from extant literature conflicts with the risks assessment process, which incorporates systems dynamics and policy evaluation proposed by this thesis.

What also appear missing in the current discussions (but introduced in this study) are systems characterization (i.e. environmental assessment), assets valuation and Threats and Vulnerability Pair (TVP). Thus, most of the extant studies on the subject have so far failed to discuss these constructs as part of the security assessment process and in particular reference to industrial controlled environments.

As stated earlier, cyberattacks on critical installations are increasing globally. A successful attack on critical infrastructure systems could cripple an entire nation. Any institutional risk assessment process on such systems must, therefore, identify and quantify the value of cyber assets; it is only then, risks impact can be quantitatively assessed. It is further argued that quantitative risk assessment without asset valuation is a challenge for evaluators, and more problematic for risk assessors [14].

Finally, none of the existing risk assessment framework (so far reviewed) has looked at critical infrastructure systems from the dynamic modelling perspective. The very few studies on the concept,

have approached from the point of metrics identification. This identification process, while useful for management discourse, is problematic to operationalize, as, it does very little to predict the behavioural characteristics of critical infrastructure systems and their interdependency. This is where the dynamic modelling approach proposed in this study is even more relevant.

2.11 Conclusions

Critical infrastructure systems for centuries have been the backbone of every human society across the globe. In modern times, the convergence of these resources with computing technologies has transformed the infrastructural landscape in terms of design, operations, maintenance, and more importantly their protection. Moreover, the reliability, performance, continuous operations and safety of these critical infrastructure systems is a fundamental requirement to their protections.

In a controlled environment, one of the important applications to control and monitor controlled automation (e.g. critical infrastructure) has been SCADA. As established, in the era of Internet technologies such as cloud computing, Internet of Things, Web of Things and Machine-to-Machine communications, modern industrial control systems have evolved to be big, complex and highly distributed. The convergence and complexity have not only made the infrastructure and their supporting systems difficult to operate and manage but also exposed the systems to numerous forms of threats, which were relatively unknown in the traditional analogue setup. As important these national assets are, their vulnerability to attacks and protection becomes a significant issue for the citizenry and the nation as a whole.

This chapter has examined the current states of cyber infrastructure interdependency systems, their operational characteristics and some of their safety mechanisms. The next chapter further reviews theories, which are considered very significant to support the thesis's proposition.

Chapter 3: Theoretical Review

This chapter reviews the theories that are necessary to understand the research approach; upon which the study's proposition is developed. Three major theories are reviewed: systems theory (also known as general system thinking), complexity adaptive theory and network theory. Two other sub-theories, relating to systems dynamics and relevant to this study are also reviewed. These are the theory of structure and dynamic complexity (connecting to the technical aspect of modelling) as well as the mental model (connecting to the soft aspect of modelling).

Theoretical review in research is considered functional in the understanding of the research question as well as the development of the research outcome. In this case, the theoretical epistemology is applied to conceptualise how various variables in critical infrastructure setups coordinate to form a unified system of systems of which they are part. Thus, through modelling and simulations, we are able to determine how an attack on a subsystem of a major system could propagate to impact the structure of an interdependent system. Perhaps, the major contribution of the thesis is the modelling and the simulation of security risk assessment of interdependent critical infrastructure systems where systems thinking and network theories are even more functional.

3.1 Systems Theory

The history of system theory dates back to the contributions from influential thinkers such as Alfred North Whitehead, Ludwig von Bertalanffy, Anatol Rapoport, Kenneth Boulding, Paul A. Weiss, Ralph Gerard, Kurt Lewin, Roy R. Grinker, William Gray, Nicolas Rizzo, Karl Menninger, Silvano. The theory has been applied in many disciplines. They include cybernetics [88], sociology [89], network analysis and synthesis [90], physiology [91], electric energy systems

[92], developmental systems [93], management science [94] and system dynamics by [95].

The word system is defined in Webster's Dictionary as "a group of elements that interact and function together as a whole" (pg. 685). In its early development, the Biologist and one of the forefathers of the systems movement, Bertalanffy, defines a system as "an entity that maintains its existence through the mutual interaction of its parts" in [96]. In a related study, Laszlo and Krippner describe a system as a "complex interaction of components together with the relationships among them, which permit the identification of a boundary-maintaining entity or process" [97]. Moreover, Macy defines a system as a group of interacting components which conserve some identifiable set of relations with the sum of their components plus their relations. In its broadest sense, system connotes a complex interacting of entities together with the relationships among their parts, which defines and maintains their uniqueness in identification [97].

Grounded from systems thinking and dynamic complexity, the thesis describes cyber infrastructure and its interdependent systems as a complex 'system of systems' with interconnected subsystems, which work together to achieve the objectives of the unified system. The epistemic deduction leads to the identification of three key constructs from the systems theory: Interactions, Components and Relations (figure 3-1).

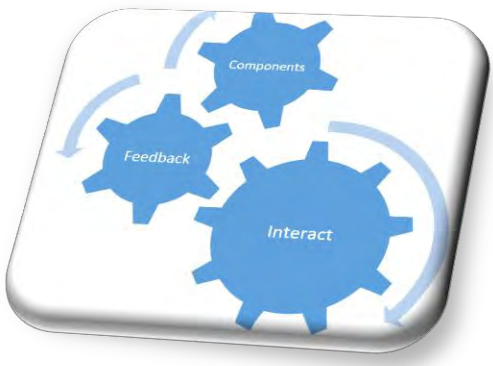


Figure 3- 1: Constructs of System Theory

Component: representing individual entities, which are an embodiment of a system. They are unique albeit interdependent, relating to each other for a system's overall functions. Per this trait, a loss or breakdown of a components affects the functionality of the whole [13].

Interaction: depicts the communication (or coordination) among the components. By interacting with other components, the interrelating part exhibits effects on the rest of the system and its subsystems. This referential property (hereby called feedback) establishes a relationship between a component (subsystem) and the rest of the system leading to the third property (i.e. relations).

Relations: denotes the association among individual components. Chen defines relationships among the system's entities as the association among individual subsystems belonging to a complete system [98]. In entity-relationship models, three main relationships are exemplified; one-to-one (1:1), one-to-many (1: M) or many-to-many (M: M). Inference, relationships among elements within a system can be one-to-one, one-to-many, or many-to-many.

It is argued, therefore, that the understanding of these constructs is critical to the epistemological applications of systems thinking. This

proposition is shared by Ackoff who applied system theory in the area of management science. In his study, Ackoff defines a system as a set of two or more interconnected entities with the following attributes [99]:

i. "Each element has an effect on the functioning of the whole" (interdependency).
ii. "Each element is affected by at least one other element in the system" (1: M relationship).
iii. "All possible subgroups of elements also have the first two properties" (frame of reference).

Inference, a system (as used in this study), pertains to a unit (which is also part of a major unit) of any kind (in this case critical infrastructure systems), "whether formal (e.g., mathematics, semantic), existential (e.g., 'real-world'), or affective (e.g., aesthetic, emotional, imaginative)" [97]. In which case, a "whole" is made up of interdependent components (i.e. subsystems), which interact to form a unit termed as a system. Accordingly, Ackoff posits that the idea of a system infers that "the relationships between its parts strongly influence its overall behaviour" [99]. In a related study, Laszlo and Krippner claim, the usefulness of systems theory is "its potential to provide a trans-disciplinary framework for a simultaneously critical and normative exploration of the relationship between perceptions and conceptions and the worlds they purport to represent" [97]. Furthermore, Laszlo and Krippner claim that system theory is useful in modelling complex entities because it helps in observing the behaviour of the interactive components. In such perspective, the characteristics of individual components can be abstracted from the details of their internal structure by "concentrating on the dynamics which define the characteristic functions, properties, and relationships that are internal or external to the system" [97]. This theoretical interpretation provides the grounds upon which the research problem is defined. Furthermore, the theoretical constructs per their definitions provide further exposition to the understanding of systems behaviour and their functional traits.

The theoretical application of dynamic systems starts from the 'problem' to be solved (i.e. the undesirable state of the system); this problem is then processed (identified, diagnosed and corrected) to

produce the desired system state (output). The output is either fed back into the system (figure 3-2) or taken out of the system. This is synonymous with the feedback model (as defined in cybernetics), which organises information flow into the modelling and simulation of interdependent systems.

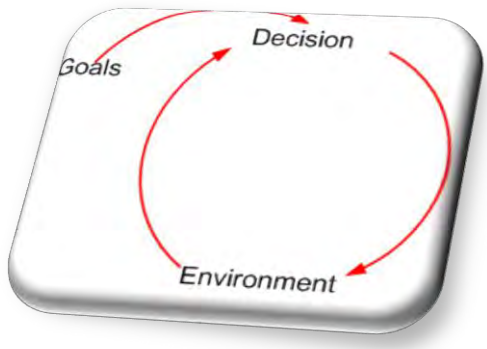


Figure 3- 2: Feedback Loops

The feedback structure represents instances where a decision causes changes, which in turn influence further decisions and reaction. This suggests the degree to which the behaviour of critical infrastructural systems influences the structural and functional characteristics of its interdependencies. On this point, Sterman argues that "intervening is a way of causing a chaos" [100]. Bertalanffy on his part hypothesises that "one cannot sum up the behaviour of the whole from the isolated parts; you have to take into account the relations between the various subordinate systems which are superordinated to them in order to understand the behaviour of the parts" in [100]

3.2 Systems Thinking

System thinking is based on the fundamental principles of system theory as discussed above and is defined as a thematic concept that embodies the idea of a set of elements connected together to form a whole and showing properties, which are an embodiment of the whole rather than properties of its component parts. The phrase

systems thinking implies "thinking about the world outside ourselves, and doing so by means of the concept system" [101]

According to Linnéusson, systems thinking acknowledges a holistic perspective on the studied question [102]. Thus, applying a system dynamics concept to risk assessment processes or critical infrastructure projects requires taking a holistic perspective on the studied problem. The approach influences the qualitative or quantitative interpretations of any explorative research. Consequently, it limits the possibilities to perform multiple tests, otherwise common when studying a defined subject that generates results, which are built on some quantitative data. Therefore, the study aims at answering the research question by interpreting systems behaviour through model designs and simulations, instead of supporting a hypothesis through satisfying data samples.

3.3 Complexity Adaptive Theory

Dodder and Dare argue that "Complex Adaptive Systems" (CAS) as a school of thought gained prominence in the mid-1980s with the formation of the Santa Fe Institute, a New Mexico think tank formed in part by former members of the nearby Los Alamos National Laboratory [103]. The primary aim of the birth of CAS is to cross traditional disciplinary boundaries. Thus, CAS was to provide an alternative to the linear, reductionist thinking that has ruled scientific thought since the time of Newton [103]. CAS has since been distinguished by extensive use of computer simulation as a research tool. In a related study, Waldrop and Gleick indicated that (like systems thinking), the common framework for complexity was built upon an interdisciplinary concept in the fields of neural networks, ecology, economics, artificial intelligence, chaos theory and cybernetics [104].

Waldrop further claimed, prior to the birth of CAS, the Belgian Nobel laureate, Ilya Priggogine's effort to explore sources of order and structure in the world, observed that "atoms and molecules are exposed to energy and material flowing from the outside, partially reversing the decay required by the second law of thermodynamics" [104]. Subsequently, systems and their subsystems are able to

instinctively organize themselves into a series of complex structures [103]. In a related study, Chan suggests that many natural systems (i.e. brains, immune systems, ecologies, societies) and artificial systems (i.e. parallel and distributed computing, artificial intelligence, artificial neural networks, and evolutionary programs) are characterized by their complex behaviour [79]. They have emerged as a result of often nonlinear Spatio-temporal interactions among a large number of systems and their subsystems at different levels of organization [79]. These systems, according to Chan are the embodiments of CAS.

A review of CAS reveals a couple of traits about the theory. The most commonly repeated ones noted in literature include:

i. Adoptive systems are "balanced between order and anarchy, at the edge of chaos" [103]. And as Waldrop put it, "...frozen systems can always do better by loosening up a bit, and turbulent systems can always do better by getting themselves a little more organized" [104]. Wardrop posits that "if a system isn't on the edge of chaos already, you'd expect learning and evolution to push it in that direction...to make the edge of chaos stable, the natural place for complex, adaptive systems to be" [104].
ii. "System co-evolves with its environment" [79]
iii. "Adaptive systems are composed of a network of many agents gathering information, learning and acting in parallel in an environment produced by the interactions of these agents" [105].
iv. "Order is emergent, instead of pre-determined, always unfolding and always in transition" (perpetual novelty) [106].
v. "Adaptive systems tend to exist in many levels of organization in the sense that agents at one level are the building blocks for agents at the next level" [107].
vi. Finally, "CAS, by their nature, have a future that is hard to predict" [103].

3.4 Theory of Structure

The theory of structure reached its mature level in 1968 and is still useful today. For instance, Forrester argued that, in contrast to other disciplines and bodies of knowledge, which provide philosophies of structure in systems, system dynamics provides with the sharpest definition and the most rigorous application of structure [108].

The theory of structure presents four core constructs, which are useful for systems modelling (figure 3-3):

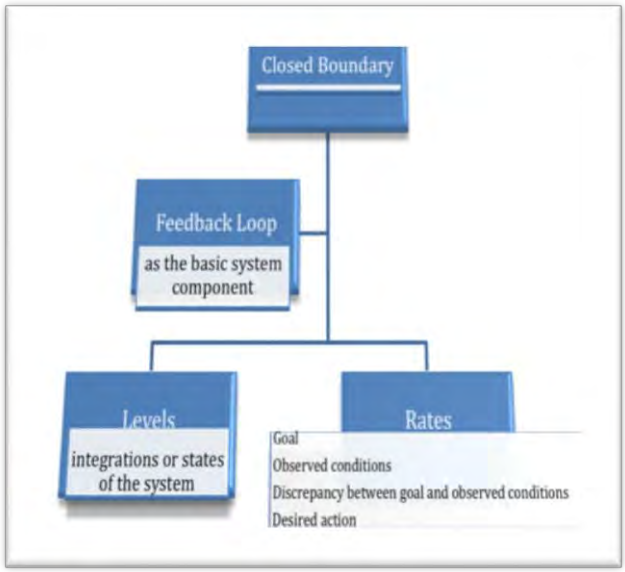


Figure 3- 3: Constructs of the theory of structure

The closed boundary: This represents a philosophical view of the structure (feedback thinking). It connotes the assumption that what crosses a boundary from outside has no effect on the system behaviour [108]. Thus, the line of boundary strictly depends on the modelled problem and not it outside [102]

The feedback loop: represents the basic component of a decision-making process [102]. Thus, a decision making depends on our perception of the present situation, and any decided change give rise for a new condition which subsequently influences our next decision [102].

Levels and Rates: they are two basic variables of dynamics modelling. "Level equations are integrations which accumulate the effects of the rates" [109]. Levels describe the present condition of a system under investigation. The levels further "carry the system's continuity from the past to the present and are the source of information to rate equations" [102].

Rates: Rates flows into or out from the levels, for instance, investment in infrastructure system (flow into) or resource erosion (flow out from). Under the rate, the following sub-constructs are observed within the policy substructure: "goals, observed conditions', 'discrepancy between goals and observed conditions', and 'desired action" [102].

The goal: According to Linnéusson, goals are the desired state of a system" [102]. To every system, there may be several conflicting goals. An observed condition "is the apparent state, the available information of the system at that time, and the information for decision (the true state of a system may be delayed or distorted by conditions in the system)" [102]. The discrepancy between a goal and observed conditions is the variance between the desired goal and the observed conditions [102]. The desired action, on the other hand, is to close the gap of the desired state [102].

3.5 Dynamic Complexity

The notion of dynamic complexity arises from the principles of both systems thinking and complexity theory. While systems thinking has been well explained in the literature, Dodder and Dare appear to suggest that, research in the field has so far failed to agree on a common definition for complexity [103]. For the avoidance of doubt, some researchers have attempted to provide certain characteristics, which describe complex systems. According to Dodder and Dare, there are a wide variety of factors that come up to make a system

complex. Dodder and Dare categorize the factors into the following: static complexity, dynamic complexity and informational complexity [103]. Beyond the general identification of complexities in systems, researchers, engineers and scientists have raised a fundamental question of the exact measure of complexity….asking 'how complex is a system'?

In a related study, Teisman and Klijn provide two broad insights into complex phenomena; first, they are more dynamic than most scientific methods have previously assumed [110]. Secondly, complex systems do not develop only by their external forces imposed upon them but their internal structures [110]. A study by Walby theorises the intersection between systems and complexity theory and defines complexity as a lax collection of work that addresses the basic questions on the nature of systems and their interactions with their internal and external environments [111]. In his assessment of hierarchy, Simon described a complex system as a system made up of large subparts, with many interactions [112].

Organization theorists, assert that complex organizations exhibit nonlinear characteristics. They describe complexity as a structural variable that characterizes both organizations and their environments [82]. On that basis, Daft et al, equate "complexity with the number of activities within the organization, noting that complexity can be measured along three dimensions; vertical, horizontal and spatial" [113]. In a related study, Galbraith posits that organization designers always try to match the complexity of an organization's structure with its environment and technology [114].

Linnéusson (2009) argues that reality is dynamically complex, and the methodology of system dynamics "is developed in order to capture these kinds of dynamics" [102]. Inference, system dynamics is a language of dynamic systems. This description supports the importance of using system dynamics to deal with the dynamic complexity in critical infrastructure systems. According to Linnéusson, there are multiple reasons behind the rise of dynamic complexity; including dynamism, tightly coupled, by feedback and nonlinearity [102]. Others reasons are history-dependent, self-organizing adaptive and counterintuitive [102].

3.6 Network Theory

Balthrop et al. define a network as a graph consisting of vertices (or nodes) connected by edges (or lines). Network theory (part of applied mathematics) takes its fundamental conception from graph theory [115]. The theory presents the relationships between discrete objects as either symmetric or asymmetric. This is where the theory is found to be useful in the analysis of interdependent critical infrastructure setup. Characteristically, a graph is made up of various vertices, connected by their edges. In computational networks, vertices and edges are known as nodes and links respectively. They are referred here as components and relations respectively. Balthrop et al, further argue that the particular interest of focus in the study of network theory is the "scale-free networks, in which the degree distribution follows a power law, where the fraction p_k of vertices with degree k falls off with increasing k as $k^{-\alpha}$ for some constant α" [115]. The following studies provide evidence of significant applications of network theory in the study of interdependent systems [34,116-117]. Notwithstanding, not many of these studies have focused on cyber infrastructures and their interdependent systems.

3.6.1 Types of Networks

The following sections look at the various types of network;

3.6.1.1 Socio-Economic Networks

Social and Economic networks consist of people and groups of people intertwined with other social artefacts (businesses, organizations, institutions) with some pattern of contacts or common interests among them (e.g. Facebook, LinkedIn, friendship networks, a network of classmates, business relations between companies, unions, a family tree or generational linkages).

3.6.1.2 Information Networks

This is made up of networks with links to information objects such as citations between academic papers, the Internet, semantics (how concepts or ideas are interlinked), etc. For example, in the labour market, Rees identifies two forms of information networks: "formal and informal networks" [118]. Rees considered formal information

networks to include "state employment services, private fee-charging employment agencies, newspaper advertisements, union hiring halls, and school or college placement bureaus" [118]. And informal sources to include "referrals from employees, other employers, and miscellaneous sources, and walk-ins or hiring at the gate" [118].

3.6.1.3 Biological Networks

Some common example of biological networks includes Neural Networks, Protection Interaction Network, and Metabolic Pathway Networks.

3.6.1.4 Technological Networks

According to Balthrop et al, technological networks include the Internet and the World Wide Web [115]. In this study, the classification is extended to include critical infrastructure systems such as power grid, transportation networks and communication networks. Other application areas are sensors networks, ad hoc networks, machine to machine (M2M) communications, Internet-of-Things (IoT) and cloud computing. For example, Xie et al argue that "for many technological networks, the network structures and the traffic taking place on them mutually interact" [119]. Furthermore, Xie et al, claim any increment in network traffic "spurs the evolution and growth of the networks to maintain their balancing" [119].

3.6.2 Characteristics of a Network

The study argues that interdependent critical infrastructure systems exhibit the characteristics of a network[18] (as a graph). Thus, each network structure is made up of multiple nodes and different types of edge. Figures 3-4(a-c) depict different types of graphs (detailed descriptions are provided in Appendix 6).

[18] Types of networks (a: unidirectional network with a single edge and vertex; b: unidirectional network with different types of vertices and edges; c: directional network with types of vertices)

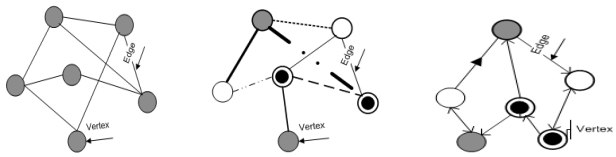


Figure 3- 4:Types of network

3.6.3 Network Resilience

Network resilience measures the strength of a network to the removal of its vertices. In relation to interdependent systems, it is the measure of the strength of the system to an external 'attack' on its nodes (assumption: when vertices are attacked (i.e. removed from a network), the length of their paths increases. When this happens, the interconnection between vertex pairs breaks down, disrupting any communication between the pair. Depending on the environment, network systems exhibit different characteristics for the removal of vertices. Characteristically, different networks systems show varying degrees of resilience. For instance, the removal of vertices with the highest degree affects the entire network structure. For example, in computer networks, an attack on a proxy server affects all the interconnected nodes leading to DDoS. Besides, while security controls (e.g. firewall) can make Internet resilient to random failure of a node, the setup can be vulnerable to a deliberate attack on its highest-degree nodes (i.e. network server). Network resilience relates to the conceptual assumption that network structure affects its performance; an observation very useful in the assessment of security risks in interdependent critical infrastructure systems. It is argued that measuring network performance of different attack scenarios provide a useful measure in protecting a network-centric system.

The analytical approach to the study of network theory is to establish the statistical properties that characterise the structure and the functions of network systems and ways to measure their behavioural characteristics [120]. This approach provides a better understanding of the process of modelling and the measurement of cybersecurity risks in network-centric systems. And it is also significant in

predicting and analysing systems structural and functional characteristics.

3.7 Bedell Model

Bedell method is a "set of procedures for the evaluation of information systems" [121]. The method involves measuring the effectiveness of existing IT practices, "data-sharing strategy planning, development resource allocation and project cost management" [122]. The fundamental notion of underpinning Bedell's model is the rankings of critical services based on their importance to an organization or society [121]. The model assumes, if a system is critical, it must support strategic operational functions, such that an attack on such a system (i.e. breakdown or unavailability) leads to unintended consequence [121]. Thus, if there is criticality in designing and implementing a system, the system effectiveness to serve the intended purpose must be equally high [122].

Using Bedell index (see Appendix 7), effectiveness estimation is conducted by measuring the following characteristics of the intended systems and/or services [121]:

i. The importance of the system's function (activity)
ii. The importance of the information systems in supporting the activity and
iii. The quality of the information systems in terms of effectiveness to support the activity.

Accordingly, the following five indices are considered useful in estimating the effectiveness index [121] (details in Appendix 3):

i. ISA – how Important a particular System is to the Activity it was built to support
ii. ESA – how Effective (quality) particular System is to the Activity it was built to support
iii. IAO – how Important the Activity in question is to an Organization
iv. ISO – how Important a particular System is to the Organization as a whole
v. EIO – how Effective (quality) Information system is to support the entire Organization

$ISO = ISA_i * IAO_i$ and $EIO = \sum_{i=1}^{n}(ESA_i * ISO_i)/\sum_i^n ISO_i)$; 1<=i<=n; where n is the total number of cyber activities within the institution (i.e., supporting energy generation and distribution services). This study estimates the 'effectiveness indices' at the institutional level[19]. For example, a power distributing company is an institution responsible for bulk power generation and distribution, which critical operations are dependent on SCADA systems.

3.8 Assumptions

There are a few important interests in the application of Bedell model to the study of information technology systems. First, the model was originally proposed for the assessment of behavioural information systems. At that time, cloud computing and digital automation systems were not part of information systems, therefore, there were not included in discussing the method. However, information systems and their applications have changed significantly over the years, making it relevant to extend the discussion to include the new changes. This study considers critical infrastructure systems to be part of the current cyber infrastructure ecosystems; which have become the core of industrial control automation. Furthermore, cyber infrastructure is no more an afterthought of institutional corporate strategy, rather, the driver for change for achieving institutional objectives. It is also assumed; information system's effectiveness (EIO Index) in the Bedell model is linked directly to the output of SCADA systems. This assumption is justified because, for many critical infrastructure systems, their operational technologies have become a key platform for operational efficiencies, rather than supporting tool. For example, when interacting with the experts, it was established that SCADA systems have gradually become Internet-facing, permitting remote monitoring, viewing and controls. Besides, the functions of most modern bulk power distribution systems have become information technology-dependent with enterprise resource applications.

[19] Institution as used here is the entity responsible for the provision of critical infrastructure services

3.9 Conclusions

This chapter has examined the corpus of theories that have been applied to investigate issues, concepts, models and phenomena related to the subject matter. In all, five different but interrelated theories have been examined. These are systems theory, complexity adaptive theory, the theory of structures, dynamic complexity and network theory. The review has helped to establish what theories already exist, their relationships to the subject, and to what extent have the selected theories been applied to examine a subject of this matter. Importantly, the review has also provided the opportunity to understand and to reveal that the chosen theories are adequate for explaining the problems raised by the thesis. Furthermore, the theoretical deduction provides the opportunity to re-examine the appropriateness of the existing knowledge in the subject matter due to gaps identified in the current argument. This is where the thesis proposal is even more relevant.

Chapter 4: Research Design

This chapter looks at the overview of the research strategy. As stated in chapter one, the primary research objective is to present a way of identifying potential vulnerabilities in cloud infrastructure setup, investigate the adversaries which could exploit such vulnerabilities and then develop a framework to assess the impact such exploitation could have on interdependent critical infrastructure systems. The objective is achieved by developing a strategy that recreates preconditions for assessing and estimating cybersecurity risks associated with public cloud infrastructure systems and their interdependencies. The strategy involves proposing and developing a cybersecurity risk assessment framework and gaining an understanding of the existing assessment processes. In the case of framework development, the study is concerned with how to design a method that meets certain specified criteria in the assessment of risks in critical infrastructure systems. In the application context, the study aims to make the assessment process suitable for the dynamics of interdependent infrastructure systems.

Among the thematic areas discussed in this chapter are the research strategy, vulnerability analysis, threat analysis, and quantitative estimates of infrastructure interdependencies. Other topics conversed here are infrastructure interdependency modelling and simulations.

4.1 Research Strategy

Research strategy provides the directions by which a study is conceived, designed and the appropriate data is collected to answer research questions. The strategy in this study (figure 4-1) follows a mixed-method approach defined in [123]. In an attempt to differentiate between quantitative and qualitative research methods, Berg and Lune suggest that “the notion of quality is essential to the nature of things” [123]. On the other hand, “quantity is elementally an amount of something” [123]. Thus, to understand ‘the why’, and

'the how' public institutions adopt cloud computing entails investigating what, how, when, where and the why of many things (i.e. their essence and ambience). According to Berg and Lune, this requires a qualitative approach. Similarly, to analyse the impact of a cyberattack on interdependent systems necessitates counting and the measurement of facts, the extent and the distributions of risk matrices; this involves a quantitative measure [123].

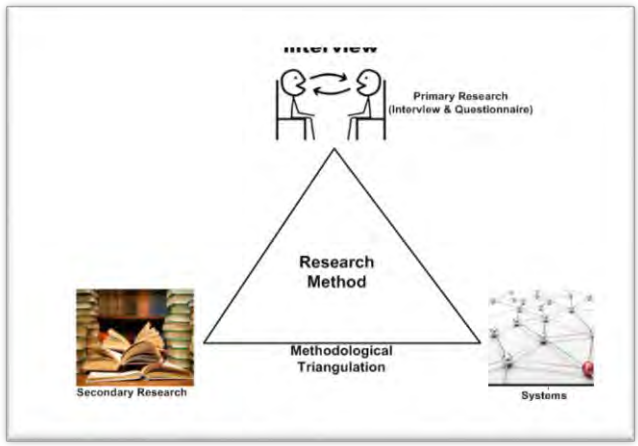


Figure 4- 1: Research Approach

4.1.1 Unit of Analysis

The unit of the analysis as presented here follows the risk assessment metrics developed in chapter 2.

4.1.1.1 Design Type

The study adopts two broad design types: exploratory approach and model development. In the first instance, data related to critical infrastructure cybersecurity risks are explored, collected, organized and summarized to gain the understanding of the subject matter. In the second phase, data is analysed as an input to the development of system dynamics models. This is then simulated to observe the behaviour of the interdependent systems and their subsystems when

subjected to cyber threat vectors. The exploratory study adopts a cross-sectional survey approach for data collection. The strategy involves administering questionnaires, interviews, and observations as well as documents analysis. A cross-sectional study provides the appropriate means by which a researcher gains sufficient information to make an informed generalisation on a subject. In a related study, Yin argues that a cross-sectional survey is convenient when attempting to answer questions such as: what is, where is, when, how much and how many [124].

4.1.1.2 Sampling Strategy

According to Berg and Lune, the logic of using sample subjects is to make inference about some larger population from a smaller one [123]. Such inference succeeds or fails depending on how well the sample represents the population. In line with the risk metrics, multiple sampling strategies are used (i.e. survey, interviews[20], observations, documents analysis, and focus group discussions). The survey approach involves interviewing (drawing samples[21]) selected members from three independent groups considered 'Subject Matter Experts' (SMEs). These groups are Washington State chapter of Association of IT Professionals, Washington State Members (Association) of CISOs and Deputy CISO, and members of the Seattle Chapter of Cloud Security Alliance (CSA). Data relating to data breach disclosure is collected from the Breach Level Index database. According to Pinsonneault and Kraemer (1993), a mixed-method sample strategy increases response rates [125].

4.1.1.3 Survey Distribution

The questionnaire[22] was administered using Google Forms[23]. It begins by creating an e-mail list of all recipients. A total of four

[20] Sample of the interview structure is provided in Appendix 2
[21] Variables (details in chapter 4) include SCADA vulnerabilities, threats vectors, system's failure (incidents) reports and security control practices
[22] See appendix 1 for the questionnaire composition
[23]See appendix 14 for the descriptive statistics & frequencies on the responses

hundred and eighty-two (482) emails were distributed, out of which two hundred and seventy-two responded[24] (representing 57.3%).

4.1.1.4 Interviews

Interviews[25] were used as a follow-up exercise from the questionnaire. All interviewees were considered either Subject Matter Experts (SMEs) or practitioners who have successfully implemented cloud-computing services at their various institutions. Three groups of participants were considered; CISOs (and Deputy CISOs) from Washington State were interviewed about public cloud initiatives at their counties. The second group involved administrators and managers of Industrial Control and Monitoring Systems (ICMS). The third group involved individuals with proven technical and security expertise specifically on cloud infrastructure security. This group includes technical administrators, programmers and facility managers from Microsoft Azure team in Redmond, Amazon, IBM, Intel and Google cloud service providers, Puget Sound Energy in Washington State and GRIDCo, Ghana. Some of the interviewees were contacted either in person, over the phone or through Skype. The interviews approach was semi-structured. In all, fifty-two (52) individuals with the position of either CISO or IT/Infrastructure Manager were interviewed. The purpose of the interview was not for analysis, but to gain a deeper understanding of the subject matter. For this reason, only in one instance, the outcome of the interview results is used in this thesis.

Furthermore, focus group discussions were held with some experts with a wide range of technical experience in the area of information security and risk assurance, cybersecurity, SCADA systems, cloud infrastructure, cloud services, records management, infrastructure and system design, and Internet of Things (IoT) and Web of Things (WoT). The following events provided the avenues for the focus group discussions:

i. Microsoft Azure eScience for Research[26]

[24] After data collation and cleaning, some selected responses were used for the analysis
[25] See appendix 2 for the interview guide
[26] April 29 -30, 2014: Microsoft Research Centre, Redmond, USA

ii. InterPARES Trust[27]
iii. Amazon AWS Government, Education, Non-Profit Symposium[28]
iv. 4th International Conference on the Internet of Things[29]
v. SecureWorld Expo 2014[30]
vi. Cloud Security Alliance (CSA, Seattle Chapter)

4.1.1.5 Observations

Data relating to systems vulnerabilities, Internet or web-based threats, network and application-level threats were observed as part of a six-month internship with the City of Seattle CISO's office and MK Hamilton and Associates Security Lab at Bremerton. The following proprietary network forensic tools were used for the monitoring, tracking, recording and analysing network traffic; Wireshark, FireEye, Snort, Infoblox, Websense and Norse. Furthermore, security-related studies on large-scale data centres were conducted at Microsoft Data Centre located at Chicago and Google Data Centre located in Douglas County, Georgia as well as Government (NITA) Data centre at Accra, Ghana. The observation of SCADA controllers and monitors supporting power generation and distribution processes was done at GRIDCo-Tema, Ghana.

4.1.1.6 Documents Study

Documents relating specifically to the study are reviewed. They include performance output report (and functionalities), events logs and contingency plan (incl. BCP, IA, IR). Other documents studied include security documents (relating access control and password policy), information technology acceptability use policies (ITAUP), Service Level Agreements (SLA), Software standard operating procedure, technical reports[31] on energy control systems and

[27] May 20-22, 2014: InterPARES Trust, North American Team Research Workshop, Vancouver, Canada
[28] June 24 – 26, 2014: Washington DC, USA
[29] October 3 – 8, 2014: MIT - Cambridge, USA
[30] November 11 – 12, 2014: Seattle Bellevue, USA
[31] Vulnerability analysis of energy delivery control systems (Idaho National Laboratory – www.inl.gov)

Government white paper on critical infrastructure developments (i.e. energy distribution and ICS). No specific structured text analysis method was adopted since in most cases where large documents were studied, it has only been a small part of the documents that were very informative to this study. From the document study, failure cases relating to critical infrastructure systems were also analysed and reported (see section 5.4.1).

4.1.1.7 Vulnerabilities and Threat Events Studies

Information relating specifically to cloud-based vulnerabilities was collected from CVE[32] and NVD[33] repositories. Cases of industrial incident failure report from two online incidence repositories and secondary (public) sources were also collected. The sources are ACM RISKS [126] and RISI [127]. Vulnerabilities relating specifically to SCADA systems were referenced from the NSTB[34] data repository [128]. Data breach records were collected from the Breach Level Index covering the period between January 1, 2013, and December June 2017.

4.1.2 Applications and Tools

The study uses various computer applications and tools for the analysis, modelling and simulations. For example, Mathlab, R-Studio, SPSS, and VB Access were mainly used for the data analysis. MS Visio has been used primarily for drawing diagrams. Dynamic systems modelling and related simulations were constructed using Vensim PLE workbench.

[32] CVE is a repository of publicly known information security vulnerabilities and threat exposure.
[33] NVD is an U.S. government repository of standards-based vulnerability management data represented which uses the Security Content Automation Protocol (SCAP). It includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.
[34] National SCADA Test Bed – see Appendix 11

4.2 Risk Metrics Operationalization

This section describes how the constructs of the proposed assessment framework have been operationalized. It involves identifying, characterising and operationalizing the assessment metrics. The metrics are described in the sections below.

4.2.1 System Characterization

This involves contextualizing risk metrics and their environment. The focus is on the environment in which the infrastructures operate. In the assessment process, the objective is to identify the asset to protect, its value in terms of impact and loss (on data, hardware, software, networks, processes and functions), the container and the custodian.

4.2.1.1 Vulnerability Assessment

Vulnerability assessment (VA) is defined as the process of investigating, identifying and categorizing the undesired states of a system, which make the system susceptible to threat attacks. The focus, in this case, is to identify vulnerabilities inherent in cloud infrastructure setup and the interdependent controlled (SCADA) systems. For assessment purpose, both current and hypothetical vulnerabilities were assessed. Current vulnerabilities list all known vulnerabilities in a vulnerability dictionary known to asset owners and systems administrators. Hypothetical vulnerabilities consider vulnerabilities that are listed in the secondary vulnerability databases but were not verified by systems administrators as significantly relevant to be exploited by threat agents.

4.2.1.2 Threat Assessment

This process identifies and evaluates the various threat vectors (agents and methods), which are capable of compromising the security and the safety of the system. A threat vector is observed by the actor's intent and the method deployed.

4.2.1.3 Likelihood Assessment

This is the process of measuring the possibility of threat agents exploiting systems vulnerability. In the context of institutional security risk assessment, determining the likelihood of a loss is the most difficult of the assessment process due to the difficulty in predicting a possible threat occurrence. As part of the assessment, the following metrics are considered:

i. Systems inherent vulnerability
ii. The effectiveness of existing security controls and
iii. Threat Event Frequency (TEF[35]).

For the purpose of analysis, the following TEF scales are proposed (table 4-1 and Appendix 3D).

Table 4-1: TEF Scale & Descriptions

Scale	Description	TEF Score
Very Likely (Very high)	>100 times per year	1.0
Likely (High)	Between 50 and 100 times per year	0.8
Somehow Likely (Moderate)	Between 10 and 50 times per year	0.6
Not Likely (Low)	Between 1 and 10 times per year	0.4
No change (Very Low)	Less than 1 per year	0.2

4.2.1.4 Control Assessment

Security Control (i.e. countermeasure) is defined as both technical and administrative procedure (including practices and policies), which are implemented, to detect, respond, protect, and recover from potential threat attacks and also to tighten internal vulnerabilities. It

[35] TEF is probable frequency, within a given timeframe that a threat agent will act against a system based on system's vulnerabilities [15]

is argued, the presence of control mechanisms reduce the likelihood of threats leveraging systems vulnerabilities.

In this context, the assessment process is focused on both technical (incl. physical) and operational controls in a controlled environment. The NIST SP 800-53 [129] framework provides guidance on the appropriate controls against cyber infrastructure systems. The study adopts SAN 20 Critical Security Controls (ver 5) as the basis of assessment (SANS Institute - CIS Critical Security Controls n.d.). In the simulation process (chapter seven), control values are scaled from 0.1 (i.e. very weak) to 1.0 (i.e. very strong)[36].

4.2.1.4 Impact Assessment

Treweek defines impact assessment as the "procedure to identify, quantify and evaluate the potential impacts of a threat action on systems and their subsystems" [131]. Extending the argument, Pagani argues, the impact of a threat attack on information resources depends on some uncertain factors [132]. Pagani likens these factors to the "likelihood of the threat occurring"; "the loss from a successful threat"; and "the frequency of recurrence of the threat" [132]. Traditionally, quantitative impact analysis tends to associate a financial cost to a successful threat event, called a Single Loss Expectancy (SLE) [133]. This is measured as the product of the likelihood of threat event occurring (measured as Annualized Loss Expectancy (ALE) and the likelihood of loss (measures as the Annualized Rate of Occurrence or ARO) [133]. The concept involves valuing information assets so as to quantify an attack impact (i.e. by cost and value). This procedure is adopted and modified in this study for the purpose of model design and simulation building.

NIST proposal (i.e. SP800-30) includes quantitative and semi-qualitative procedures. It is based on the following four-point metrics: 1) the harm to business operations; 2) the harm to assets; 3) the harm to individuals and 4) the harm to state-owned institutions.

This study extends the argument to include the impact on cyber infrastructure. Supporting this argument, Rinaldi posits that the

[36] See Appendix 9 for the control effectiveness index

digitization and the computerization of modern SCADA systems have led to "pervasive cyber interdependencies" which requires empirical assessment [134].

The approach in this study looks at the impact from the perspectives of critical systems and their interdependencies grounded on Bedell model [121,122]. It is assumed that a successful threat attack on cloud infrastructure systems will negatively impact on interdependent systems, thereby creating 2nd and 3rd order effect on the performance of interdependent systems. This requires assessing both structural and functional impact as a topological extraction of interdependent systems [135] grounded on network theory.

4.3 Interdependency Estimates

This section presents a set of quantitative estimates of critical infrastructure interdependencies. The result is useful for modelling and simulation of interdependency systems. The following studies [116-117,136] have shown that infrastructure interdependency can be modelled using quantitative estimates. Similarly, Rinaldi et al posit that systems interdependency is better understood when treated as a system of systems; which behavioural characteristics are unpredictable due to their individual uniqueness [2]. Rahman on his part argues, interdependency estimate is a "causality-based approach where critical infrastructure systems are viewed as a system of systems" [138].

As indicated earlier, the interdependency estimates in this context adopt Bedell model, where critical infrastructure systems are modelled as a causality-based function. It uses several functional attributes to describe infrastructure interdependencies in Bulk Power Distribution (BPD) systems. The approach is based on the analysis and the ranking of contributions from the different critical infrastructure services to SCADA functional outputs.

4.3.1 Infrastructure Interdependence Modelling

Critical infrastructure services include power grid, oil, natural gas production, transportation, water systems, transportation networks, etc. It is further argued that "the sheer complexity, magnitude, and

scope of the nation's critical infrastructures make modelling and simulation important elements of any analytic effort" [2]. Furthermore, Rinaldi et al, posits "modelling and simulation are important attributes in understanding the safety, reliability, and survivability of critical infrastructure systems" [2]. Notwithstanding, modelling of cyber interdependencies have not been well explored in terms of research, making it an important field to explore.

The thesis's modelling approach is based on dynamic complexity concept by Forrester. According to Forrester, systems are governed by feedback which generates "patterns of behaviour" [95]. Thus, to understand, predict and decode the behaviour of interdependent systems, require the understanding of their dynamic attributes. In a related study, Monga argues that dynamic modelling is a "fundamentally creative and intensive process" [139]. It requires collecting data, testing theories, developing hypotheses, making assumptions and testing them [139]. Subsequently, the relations between the measurable objectives and factors affecting their values require formalization [139]. These formalisations are known as the causalities. Using the causalities, dynamic models can then be developed, feed into a simulator; so as to examine the behavioural patterns of the systems being modelled.

4.4 Conclusions

This chapter provides a step-by-step plan of actions; directing the research approach and the efforts necessary and required to achieve the thesis's overall objectives. Specifically, the chapter has looked at the strategy for data collection, which discusses the scope, survey instruments, method of analysis and reporting. Following that, the operationalization of the assessment metrics in the proposed risk assessment framework has been comprehensively discussed. One of the key aspects of the thesis is the method of estimating the interdependency in critical infrastructure systems. In this case, Bedell interdependency model has been reviewed and adopted as the appropriate method to estimate the interdependency between cloud as a cyber infrastructure and industrial control systems. The next chapter provides a comprehensive data analysis, interpretations and data visualization.

Chapter 5: Data Analysis

"We are on the cusp of a historic transformation of our energy systems. The power network, from generation to transmission and distribution to consumption, will undergo the same kind of architectural transformation in the coming decades that computing and the communication networks have gone through in the last two. We envision a future network with hundreds of millions of distributed energy resources (DERs) such as solar panels, wind turbines, electric vehicles, energy storage devices, smart buildings, smart appliances, smart inverters and other power electronics. These intelligent endpoints will not be merely passive loads, as are most endpoints today, but endpoints that may generate sense, compute, communicate, and actuate. They will create a tremendous opportunity for greater efficiency, flexibility, and capacity in our generation and utilisation of electricity. They will also create severe risks because of potential cyber attack and other vulnerabilities".

Steven Low, Caltech, USA, 2015

In the previous chapter, the instruments for data collection were the main focus of discussion. This chapter comprehensively analyses the data and interpret the results. Among the key issues discussed are the scope of data collection, identification of risk assessment metrics, and quantitative estimates of infrastructure interdependency. The chapter is concluded with a quantitative analysis of interdependency in bulk power distributed systems.

5.1 Scope of Data Collection

The benchmark sample consists of both public and private institutions, providing utility services with an emphasis on downstream energy distributions systems. Institutions considered in the study are Department of Electricity Delivery and Energy Reliability (National SCADA Test Bed (NSTB-US), National Cybersecurity and Communications Integration Centre (NCCIC), Microsoft Azure and Amazon AWS (for cloud services). Additionally, data on incidence response, network analysis, and live cyber attack events and systems audit log files are obtained from the Department of Information Technology, City of Seattle. A case study of energy services is taken from Puget Sound Energy (PSE) - Washington State, USA, Ghana Grid Company Limited (GRIDCo), and Electricity Company of Ghana (ECG)[37].

Information relating to cloud-specific vulnerabilities is collected from CVE[38] [140] and NVD[39] (NVD - Search n.d.). Cases of industrial incident failure reports are collected mainly from two online incidence repositories (i.e. ACM RISKS[40] and RISI[41]). Vulnerabilities relating specifically to SCADA systems are obtained from the NSTB[42] repository [128]. And the data relating to data breach disclosure is collected from the Breach Level Index database.

5.2 Metrics Classification

This analysis is based on both primary and secondary data. Risk incident cases are also analysed.

---

[37] Any information recorded here are considered to be public records useful for the purpose of academic wok. No information is considered classified

[38] CVE is a repository of publicly known information security vulnerabilities and threat exposure.

[39] NVD is an U.S. government repository of standards-based vulnerability management data represented which uses the Security Content Automation Protocol (SCAP). It includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

[40] [126]

[41] The Repository of Industrial Security Incidents" n.d

[42] National SCADA Test Bed

5.2.1 Incidents Reports

The Critical Infrastructure Protection Standard (CIPS) document analysed here is based on the North American Electric Reliability Corporation (NERC) with the support of Federal Energy Regulatory Commission (FERC), a document, developed for the U.S. Federal Government. The standard highlights the safety and protection requirements for all critical infrastructure systems in the USA. The approach involves reclassification of critical infrastructure resources, implementation of acceptable security controls policies, designing of workable incident planning as well as data recovery plans [142]. Since its approval, the document has become a legal requirement for all infrastructure providers as well as asset owners. The document further requires providers and assets owners to submit all infrastructural failure reports to FCC[43]. The challenge for researchers is that outage report is only accessible to FCC officials and DHS[44]. This makes it difficult for researchers (outside the officialdom) to gain access to such data. The problem is further compounded by the unwillingness of both public and private infrastructure operators to share infrastructure failure information.

In the USA, FCC requires all infrastructure service providers to specify information about the state of their infrastructure resources, control parameters, input and output specifications, operating assumptions, backup facilities, management procedures and practices, and other physical and environmental constraints" [143]. In Ghana, none of the three institutions responsible for energy generation, distribution and delivery (VRA, GRIDCo, and ECG) has any reliable records on infrastructure failures or outages report for research purpose.

In 2008 Eric Byres and Mark Fabro began collaboration on a project to develop a Repository of Industrial Security Incidents with the goal of making the database available to the research community and industrial automation community. The taxonomy of their incidence database is based on five key parameters: attack type, event date (year), attack target (country/industry type), methods and failure

[43] Federal Communication Commission
[44] Department of Homeland Security

impact. This study, however, proposes a taxonomy based on attack method, target, impact and motivation.

The data collection approach involves systematically collecting cyberattack events cases on critical infrastructure systems. The events study period is between January 2010 and December 2014. Records on data breach disclosure are collected for the period between January 2013 and June 2017. On average, over five hundred and seventy-nine (579) cases of cybersecurity incidents relating to industrial control systems (ICS) were observed. In addition, a total of seven thousand, five hundred and three (7503) cases of reported breached events where analyzed.

For each incident, the following criteria are adopted:

i. V = Threat vector (cause)
ii. T = Target (SCADA)
iii. I = Potential Impact (low-highest)
iv. R = Reliability (report source, Date)

Each vector is further probed to ascertain its **origin** such as:

i. Source
ii. External or Internal attack
iii. Malware/Malicious Code
iv. Vendor or equipment

Case 5.1

> *"In 2013, the Dragonfly[45] group moved their focus into the U.S. and European energy firms. Dragonfly gains entry through these methods: 1) spear-phishing emails delivering malware 2) watering hole attacks that redirected visitors to energy industry-related websites hosting an exploit kit and 3) infecting legitimate software from three different ICS (industrial control systems) equipment manufacturers. With the growing dependencies on energy, if Dragonfly were to act with the information it has already been able to access,*

[45]Dragonfly is made up of cyber adversaries whose prime objectives is to target critical installations since least 2011

> *this group could do a lot of damage to the U.S. and Western Europe. A possible outcome from an attack on our utilities could cripple manufacturers that supply their armies with food and other crucial items"* [127]

In the above case, the identified threat agent is a malware (the method of attack is phishing) and the targetted system is SCADA. The impact is not observable (because the attack was not successful).

Case 5.2

> *"A spill from the trans-Alaska pipeline totalled about 5,000 barrels, making it the third-largest spill from the 800-mile pipeline. Alyeska Pipeline Services Co. kept the pipeline shut down for 3 days after discovering the spill at Pump Station 9 near Delta Junction. Alyeska was testing its fire command system when power at the pump station failed. Power was switched from the electrical grid to a battery system. The pipeline has relief valves that open to prevent pressure from increasing inside. They managed to open and oil flow into a partially filled tank. A control circuit in the battery system failed to close the relief valve and oil filled the tank and overflowed into the secondary containment area. The containment area is lined with an impermeable liner. No oil escaped from the area. The pipeline was shut down for 79 hours. About 5,000 barrels of oil spilt from the trans-Alaska pipeline. The disruption resulted in a loss of $45 million/day in North Slope production and about $13 million in state revenue"* [127].

In this case, the target system is gas pipelines (not SCADA). Such reports were reviewed but not analysed as part of the SCADA related incidents.

Case 5.3

> *"On 15 August 2012, Saudi Aramco, a large national oil, and gas company with global operations, announced that they had to disconnect their IT systems from the Internet while dealing with a serious disruption of their network.*

> *The disruption, which continued for two weeks, was the result of a cyber attack that used a computer virus to disable over 30,000 of the company's workstations. The virus, later named as "Shamoon", was the first significant cyber attack on a commercial target to cause real damage. It is also the most destructive attack, the private sector has experienced to date. Later in the same month Rasgas, the main player in the Qatari Liquid and Natural Gas scene, was also hit by the Shamoon (as per security experts) virus and consequently forced to bring their entire network offline*" [10].

In this case, the threat vector is a computer virus (malicious code) and the targeted system is computer workstations and network infrastructure (but not directly SCADA).

5.2.2 Data Breach

On average, over two million records get breached every single day. This represents only reported cases. There are many unreported cases of a data breach due to lack of enforcement and compliance in many countries. Table 5-1 contains year on year summary statistics

Figure 5- 1: Year-by-year Record Breached

Table 5- 1: Year on year Data breach summary statistics

	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
Yr_2013	1.000e+00	3.120e+02	2.290e+03	3.072e+06	1.471e+04	1.000e+09
Yr_2014	1.000e+00	2.000e+02	1.700e+03	2.909e+06	1.445e+04	1.200e+09
Yr_2015	1	200	1285	695389	8796	191337174
Yr_2016	1	500	2200	1522085	21000	412214295
Yr_2017	1.000e+00	6.000e+02	2.000e+03	2.841e+06	1.709e+04	1.340e+09

The report (figure 5-1) shows an increase in threat attack on critical systems globally. The year 2014 recorded the highest breach incident[46]. In the industry by industry statistics, Healthcare (figure 5-2) remains the most target industry followed by Government or state-owned institutions. Table 5-2 is the summary statistics of the four major hit industries

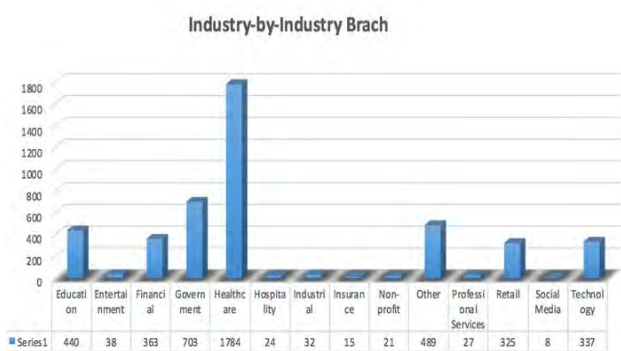


Figure 5- 2: Industry by Industry data breach

[46] The exact reason(s) behind this was not specifically explored by this study

Table 5- 2: Summary statistics of an industry-by-industry data breach

	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
Gov't	1	100	1598	1442659	17420	198000000
Technology	1	200	3.989e+04	1.188e+07	9.800e+05	1.200e+09
Health	1	571	1533	153771	6154	78800000
Education	1	154	1160	254075	6000	48600000

Generally, sources of cyberattack have been very diverse, with the motive of attack still unclear. From the database, malicious outsider remains the greatest source of data breach followed by accidental loss (figure 5-3).

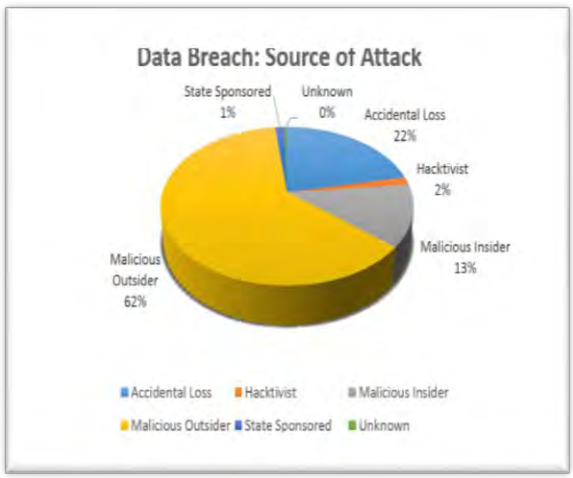


Figure 5- 3: Sources of Threats Attack

Moreover, the analysis of over 1000 data breach entries from BLI over the period of analysis identifies five (5) major types of a data breach (figure 5-4). These are identity theft, account access, financial access, existential data, and nuisance. The results put identity theft as a major type of data breach (61%). Table 5-3 is the corresponding summary statistics

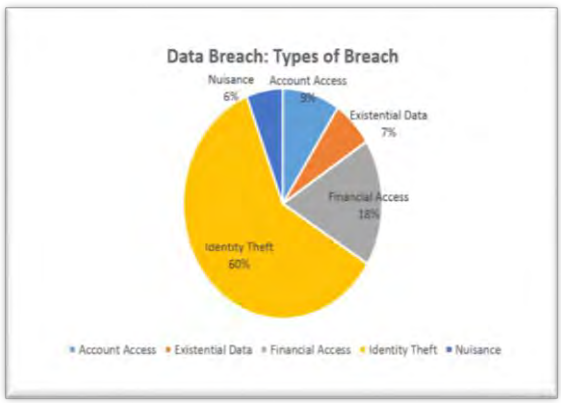


Figure 5- 4: Major types of data breach

Table 5- 3: Source/Types of Breach - Summary Statistics

	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
Mal. Outsider	1.000e+00	6.530e+02	2.709e+03	2.164e+06	2.300e+04	1.200e+09
Acc. Loss	1.000e+00	2.000e+02	1.168e+03	2.631e+06	9.000e+03	1.340e+09
Ident. Theft	1.000e+00	4.000e+02	1.654e+03	1.171e+06	1.000e+04	1.000e+09
Fin. Access	1	95	1000	1012697	12147 1	52000000

5.3 System Characterization

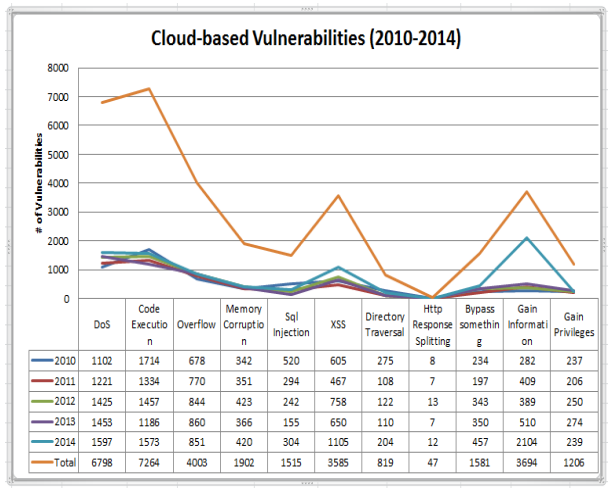
As indicated earlier, there are two primary systems under consideration: cloud computing as a cyber infrastructure system and ICS-SCADA as an interconnected system. Two factors considered necessary for the characterization of the latter were: (1) the value of the system (as an asset) and (2) the core system functionalities.

5.3.1 Vulnerabilities Assessment

According to NTSB, the most significant SCADA vulnerabilities are those, which allow for unauthorised access to physical controlled systems (hosts, applications, unsecured data and unauthorised manipulations by insiders) and impede information flow and critical

operations [144]. The assessment method is based on 'Common Vulnerability Scoring Systems (CVSS v2)'. The goal of the metrics is to provide "an open framework for communicating the characteristics and impacts of computer and information technology systems' vulnerabilities" [145]. The metrics[47] provide the standard by which systems vulnerabilities are prioritised according to their relative risks exposure. The categorization consists of three groups: i) Base, ii) Temporal and iii) Environmental. Each of the group according to FIRST, produces a numeric score ranging from 0 to 10; a vector, which is the textual representation of the values used to derive the CVSS score (see table 5-4). Appendix 4D contains further details on the CVSS ranking.

Figure 5-5 is the analysis of common vulnerabilities. During the period of assessment, the result shows code execution as the most exploited vulnerability. In all, a total of 19,035 vulnerability types were analysed.



	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges
2010	1102	1714	678	342	520	605	275	8	234	282	237
2011	1221	1334	770	351	294	467	108	7	197	409	206
2012	1425	1457	844	423	242	758	122	13	343	389	250
2013	1453	1186	860	366	155	650	110	7	350	510	274
2014	1597	1573	851	420	304	1105	204	12	457	2104	239
Total	6798	7264	4003	1902	1515	3585	819	47	1581	3694	1206

[47] FIRST (Forum of Incident Response and Security Teams) is the body responsible for CVSS ranking. It provides the following scoring scale (table 4.1) as a standard for vulnerability scoring.

Figure 5- 5: Common vulnerability exposure

5.3.1.1 Vulnerability Severity Raking

As indicated above, the vulnerability severity score is based on the CVSS ranking proposed by [146].

Table 5- 4: Vulnerability Severity Score

Rank	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Per the ranking, a base score of 4.0 has a severity rate of the medium. This provides a useful proposition for a quantitative risk assessment. Accordingly, the purpose of the CVSS score is to help organizations prioritize their security risk environment in terms of threat and vulnerability exposure (see case 5.4 below).

Case 5.4

Vulnerability (ID): CVE 2014-8966

Description: "Microsoft Internet Explorer 6 through 8 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, known as Internet Explorer Memory Corruption Vulnerability"

Source: nvd.nist.gov

Type: Executable Code Memory Corruption (DoS ECMC)

CVSS: 9.3

Product/Vendor: Internet Explorer/Microsoft

Date published: December 10, 2014

5.3.2 Threats Assessment

In this context, the strategy is to identify threat vectors and their motives. The analysis includes the frequency of attack as well as the likelihood of attack happening within a given period of time. The assessment is based on the administered questionnaires. For example, respondents were asked about the likelihood of potential threats attacking SCADA system within the next 12 months. The result suggests a "very likely" (see figure 5-6). Additionally, when respondents were asked if they suspect any threat attack against a computer and general IT systems within the next 12 months; the results show very likely (figure 5-7).

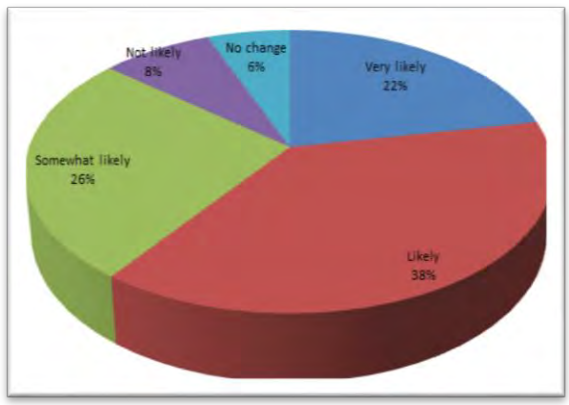


Figure 5- 6: Likelihood of cyberattack against Cyber Infrastructure in general[48]

[48] Based on 203 respondents

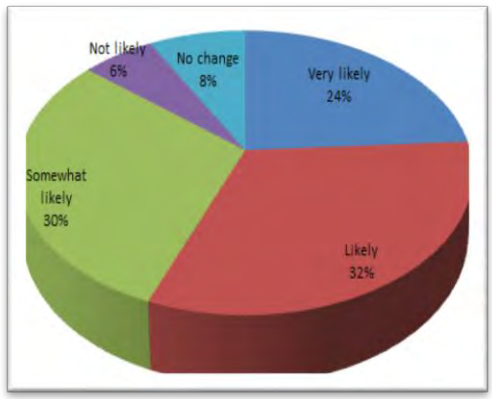


Figure 5- 7: Likelihood of cyberattack against SCADA systems[49]

5.4 Incident Assessment

Below are the results of the analysis of infrastructure risk incidence and related vulnerabilities.

5.4.1 Scope

Figure 5-8 shows the statistics of the sources of data for the incident reports (based on their contribution ratio). A total of five hundred and seventy-nine (579) incidents were reviewed. The "other" section includes sources that had contributed less than 6%. ACM RISKS forum provided the largest ratio (being the only academically peer-reviewed source among the lot).

[49] Based on 52 interview respondents

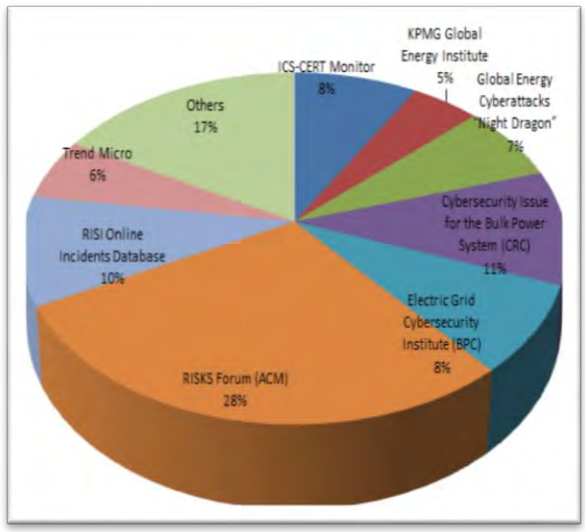


Figure 5- 8: Sources of ICS-Incidents

It is observed that before 2009, apart from state-owned institutions, very few independent institutions were recording cybersecurity issues relating to SCADA systems. Besides, most of the reports on the subject were published in local and international (electronic) media, which were not peer-reviewed. In fact, the Breach Level Index database had no records on breach disclosure until 2013.

While there was a downward trend of reported cases between 2010 and 2011, the result (figure 5-9) shows a surge in reported failure cases from 2011.

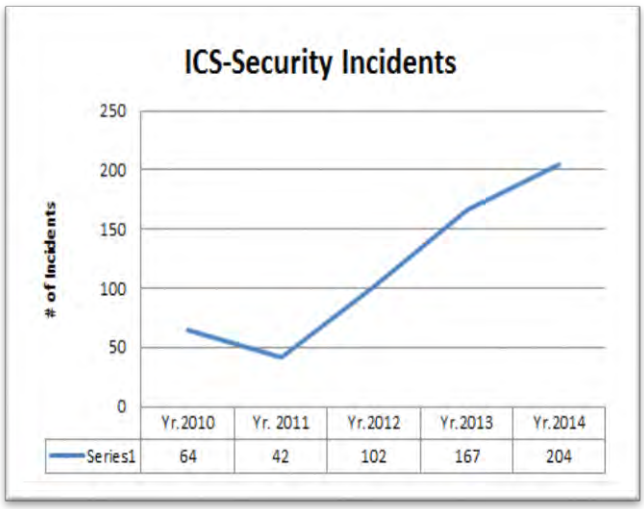


Figure 5- 9: ICS Incidents report trend

5.4.2 SCADA Vulnerabilities

This involves identifying vulnerabilities specific to SCADA systems. The assessment references NSTB top 10 most critical ICS vulnerabilities (see appendix 11). The vulnerability assessment matrix is ranked using the Common Weakness Enumeration (CWE) based on CVSS v2 metrics. According to NSTB, exposure rate and security requirements for each metrics can be adjusted for individual ICS installations [144].

Accordingly, the NSTB documentation on standards provides four core ICS functionality assessment metrics: Level1- Local or Basic Control; Level 2: Supervisory Control; Level3: Operations Management and Level 4: Enterprise Systems [144]. Figure 5-10 shows the vulnerability assessment of ICS-SCADA systems based on their functions. The result shows that ICCP[50] Services and Protocol

[50] Inter-Control Center Communications Protocol

stack, as well as Supervisory Control Protocol Services, are the two most vulnerable SCADA functional sets.

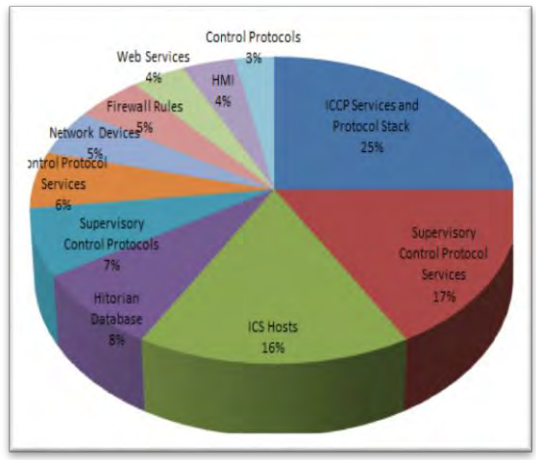


Figure 5- 10: Common SCADA Vulnerabilities

5.4.2.1 Cloud-Based Vulnerability

Figure 5-11 shows the most common application vulnerabilities (i.e. by type). The result shows Code Execution is the most exploited vulnerability.

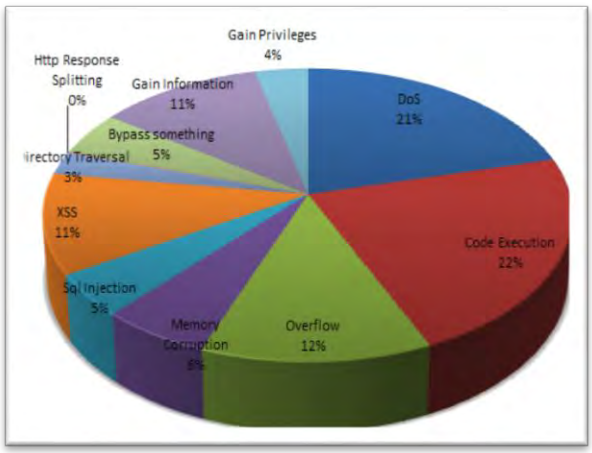


Figure 5- 11: web-induced vulnerabilities by type

5.4.2.2 Coordinated Vulnerabilities

Following the two results (figures 5-10 and 5-11), a comparative analysis of cloud-based vulnerabilities and SCADA-based vulnerabilities was performed (see table 5-5). The analysis shows that in most cases there is more than one match.

Table 5- 5: ICS Application Vulnerability matrix

Common ICS Vulnerabilities		Vulnerability Matching	Common Web-based Vulnerabilities	
1	Unpatched Publish Vulnerabilities	A, B, J	DoS	A
2	Use of Vulnerable Remote Display Protocols	A, B, I	Code Execution	B
3	Web HMI Vulnerabilities	B, F, H, J	Buffer Overflow	C
4	Buffer Overflows in ICS services	A, B, C, F, I	Memory Corruption	D
5	Improper Authentication	A, B, I, J, K	SQL Injection	E
6	Improper Access Control (Authorization)	A, B, I, J, K	XSS	F
7	Use of Standard IT Protocols with Clear-Text Authentication	I, J, K	Directory Traversal	G
8	Unprotected Transport of ICS Application Credentials	I	HTTP Traverse Splitting	H
9	ICS Data and Command Message Manipulation and Injection	B, E, I, J	Bypass Something	I
10	SQL Injection	B, E, I, J	Gain Information	J
		A, B, E	Gain Privileges	K

5.4.3 SCADA-Targeted Threats

The key factors considered in the assessment process are threat actors (figure 5-12) as well as their methods. While insecure web applications pose the greatest threat to controlled systems, insider threat remains the second most common threat recorded in the last 24 months (figure 5-12). Moreover, social engineering and phishing are

the two common methods of exploits against controlled systems during the assessment window (figure 5-13). The most identified malware against controlled systems includes Dropper, Rootkits, viruses (including adware and spyware) and Worms. Other identified malware are Trojan Horses, Ransomware, Water Hole, Phishing and Spear Phishing.

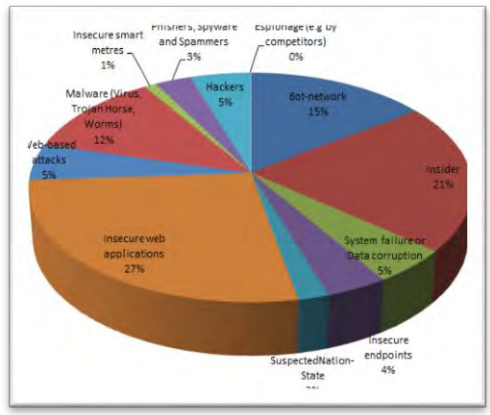


Figure 5- 12: Common Threat Actors against ICS systems[51]

[51] Results based on 213 respondents (see appendix 4B)

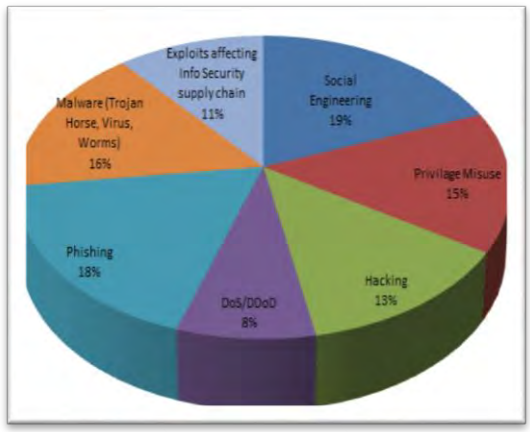


Figure 5- 13: Common method (threat exploits) [52]

5.4.3.1 Attackers Motives

Attack motivation varies from case to case (see case 5.5). The result (as shown in figure 5-14) shows that destruction of critical services, compromising computerised systems, as well as IP theft, remains the most common attack motives on SCADA system respectively.

[52] Results based on 209 respondents

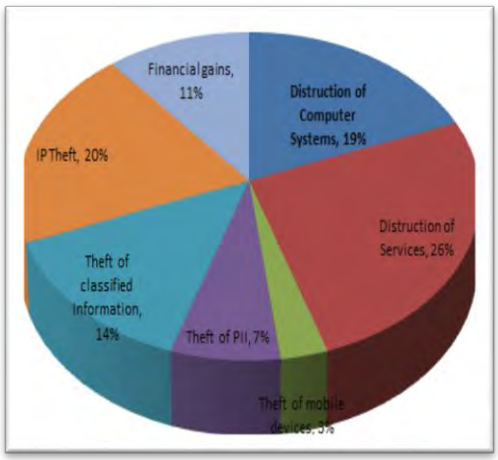


Figure 5- 14: Attackers motivation[53]

Case 5.5

> *"On 15 August 2012, Saudi Aramco, a large national oil and gas company with global operations, had to disconnect their IT systems from the Internet while dealing with a serious disruption of their network. The disruption, which continued for two weeks, was the result of a cyber attack caused by a computer virus, which disabled over 30,000 of the company's workstations. The virus ("Shamoon"), was the first significant cyberattack on a commercial target to cause that significant damage. It is also the most destructive attack the private sector had experienced to date". Source:* [147]

5.4.4 Controls Assessment

This involves determining for each known vulnerability and threat vector, the control measures, which can be deployed to counteract them. The objective is to assess the mechanism that can be deployed

[53] Results based on 231 respondents (see Appendix 14)

to protect infrastructure systems. Table 5-6 shows the level of respondents'[54] awareness of existing implemented controls.

Table 5- 6: Security Controls against known vulnerabilities and threats[55]

ICS-Induced Vulnerabilities	Yes (%)	No (%)	Threats	Yes (%)	No (%)
DDoS/DoS	53.8	31.9	Bot-network	48.7	38.6
Code Execution	72.6	20.3	Malicious Insider	23.6	57.6
Buffer Overflow	62.6	31.8	System failure or Data corruption	66.6	18.1
Memory Corruption	57.7	33.1	Insecure endpoints	72.6	23.7
XSS	81.2	6.6	Suspected Nation-States	7.8	55.7
Improper Access Control (Authorization)	57.5	31.1	Insecure web applications	78.5	13.3
HTTP Traverse Splitting	67.3	16.6	Web-based attacks	89.3	4.6
ICS Data and Command Message Manipulation and Injection	62.3	28.6	Malware (Virus, Trojan Horse, Worms)	92.8	1.2
SQL Injection	67.8	27.6	Insecure smart metres	15.6	17.4
Unprotected Transport of ICS	48.3	28.8	Phishers, Spyware,	88.21	3.1

[54] Details of individual institutional security controls were not specifically identified
[55] based on 221 respondents (see appendix 14)

Application Credentials			and Spammers		
Improper Authentication	56.6	28.1	Hackers Attempts	48.8	31.8
Directory Traversal	34.3	16.7	Espionage (e.g by competitors)	7.8	12.2

5.5 Impact Assessment (Interdependency Systems)

This section presents a set of quantitative estimates of infrastructure interdependencies using Bedell model. According to Buschle and Quartel, quantitative estimate of systems interdependencies is well represented using mathematical functions [148]. Other extant studies have also shown that infrastructure interdependency can be modelled using quantitative estimates.

5.5.1 Infrastructure Interdependency Estimates

Infrastructure interdependency function is defined in this study as the cloud infrastructure (CI) interdependency function. It represents a linear model of dependency on the output of SCADA systems to cloud infrastructure inputs. Interdependence effectiveness of two systems is determined by Bedell's effectiveness index (EIO). From the function, an EIO index is normalized by a factor of 10. For instance, when SCADA operation (x) is dependent on the services of cloud infrastructure systems, the interdependency function (output) is expressed as:

$$f(x) = \left(1 - \frac{EIO}{10}\right) + \left(\frac{EIO}{10}\right)x;\ 0 \leq x \leq 1 \qquad (5.1)$$

where x is CI services feed and f(x) is the output from SCADA functions (activities).

In the example below (figure 32), the CI (x-axis) represents cloud services while the y-axis represents SCADA output. The EIO index is the slope of CI interdependency; where a higher slope value implies a stronger coupling between two interdependent systems. The result

(EIO index) of 9.0[56] signifies a strong association between the two dependent systems. This suggests that an attack on one system has a direct impact on the interdependent system. This relation supports the earlier argument (on system thinking) that the behaviour of a subsystem has a direct impact on the whole system. The assumption of linearity implies a reasonable approximation observed from the failure cases. Thus, an attack on any part of the system would most likely lead to a decrease in the system's performance. This argument is corroborated by findings in [5, 149 -150].

5.5.2 Quantitative Estimate of Infrastructure Interdependency

This section estimates the interdependency between SCADA functions and cloud as cyber infrastructure services using Bedell efficiency index (see table 5-7). In doing so, the functional properties of a SCADA were observed and the numeric ranking index was assigned and computed for the purpose of analysis. These functions[57] include communication, control, monitoring, data processing and computation. Furthermore, communication networks, remote controllers, remote terminals, storage servers and computational tools were considered to be the supporting cyber infrastructure systems. For example, in table 10, communication networks were considered a strategic factor (ISA=10[58]), highly effective (ESA=10) and strategic activity (IAO=8) respectively to SCADA communication functions. Similarly, in the same example (in table 10), communication networks were considered a major supporting factor (ISA=5), moderately effective (ESA=5) and a contributing activity (IAO=6) respectively to SCADA communication functions. As indicated earlier, an IEO of 9.0 signifies a very strong coupling between cloud services and that of SCADA functions.

[56] Based on the 52 interview respondents – see Appendix 2
[57] Based on the 52 interview respondents – see appendix 2
[58] ISA, ESA, and IAO values used here were applied for codification and clarification purposes (actual data values may vary)

Table 5- 7: CI-SCADA Effectiveness Index

Activity	Systems	ISA	ESA	IAO	$ISO = ISA * IAO$	IEO = ESA * ISO
Communication	Communication Network	10	10	8	80	800
Control	Remote Controllers	10	10	8	80	800
Monitoring	Remote Terminals	10	10	8	80	800
Data processing	Storage servers	5	5	6	30	150
Computation.	Computational tools	5	5	6	30	150
Total					300	2700
EIO Index for SCADA Systems					2700/300 = 9.0	

It is argued that the integration of Internet and network technologies, as well as the advancement of Smart Grid, has contributed to the merging of cloud computing services and that of SCADA operations. For example, it was observed, in some circumstances, systems administrators could monitor and control some SCADA operations remotely via dedicated LANs and VLANs. These operations were carried out jointly via the RTU and MTU in the hard-wired analogue environment which is susceptible to wire-tapping. Additionally, it was also observed that the intercommunication process between MTU and RTUs is automated by SCADA administrators, which enable them to administer the process remotely. Historical events logs have shown that malfunctioning of any of these critical services has a major impact on power distribution operations. Although most critical systems were designed with security and efficiency in mind, previous failure cases have shown that occasional breakdown of these critical systems is unavoidable. For example, a software flaw in a software upgrade caused a nation-wide power outage at one of the

facilities studies. This led to a total nationwide blackout (e.g. in case 5.5).

5.5.3 Infrastructure Interdependency in Bulk Power Distribution Systems

The following analysis is based on an event study conducted at GRIDCo power distribution company in Ghana. GRIDCo deploys SCADA systems to facilitate power distribution across many parts of Ghana. The example below presents four key cyber infrastructure services, which were found to impact the BPD operations. Table 5-8 (figure 5-15) shows the interdependency function between selected BPD operations and the corresponding cyber infrastructure services. The BPD operations considered are tank monitoring, emission control, communication and procurement. The corresponding services are end-user applications, distributed generation, smart grid and supply chain. The EIO[59] index (8.08) depicts a strong interdependency ratio between BPD activities and the corresponding cyber infrastructure services collaborated by the linear relationship between them. The linear graph (figure 5-15) shows that the two systems are strongly interrelated and that the performance of cyber infrastructure systems has a direct impact on the BPD operations. Implying, an attack on cyber infrastructure systems (in this case cloud services) will have a direct impact on the interdependent system (in this case the BPD system).

[59] ISA, ESA, and IAO values used here were applied for the purpose of codification

Table 5- 8: CI-BDPS Effectiveness Index

Activity	Systems	ESA	ISA	IAO	$ISO = ISA * IAO$	$IEO = ESA * ISO$
Tank Monitoring	End-User Applications	10	10	8	80	800
Emission Control	Distributed Generation	10	5	8	40	400
Communication	Smart Grid	5	10	5	50	250
Procurement	Supply Chain	5	5	5	25	125
Total					195	1575
EIO Index for BPD systems					1575/195 = 8.08	

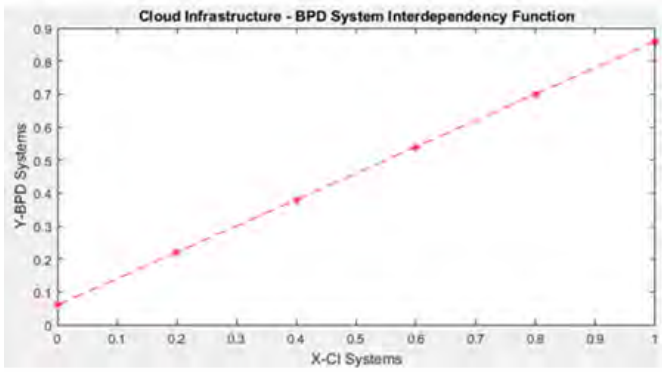


Figure 5- 15: ICS-SCADA and BPDS Interdependency function

5.6 Conclusions

The data analysis and reporting as discussed in this chapter can be considered as those aspects necessary for generating a fundamental understanding of the thesis's overall objectives. The findings from the data analysis further confirm the thesis's claim of the risks confronting critical infrastructure systems in their digital operating environment. As part of the discussion, the thesis characterises risk assessment process into six core components (i.e. systems classification, threats, vulnerabilities, threats-vulnerability pair, controls and impacts). These are considered to be the fundamental

principles needed to understand and operationalize cybersecurity risk assessment in critical infrastructure systems. This accession is supported by the results of the data analysis.

Following that, the effectiveness of systems interdependency has been quantitatively measured using Bendell interdependency effectiveness index. In this context, a working sample of quantitative estimates of infrastructure interdependency in the BPD system was computed. The outcome from this chapter is used as the inputs for the development of the system dynamics modelling and simulations discussed in chapters Six and Seven.

Chapter 6: Systems Dynamics

The preceding chapters can be considered as those aspects necessary for generating the fundamental understanding of the thesis's objectives. Beginning with this chapter, the next three chapters can be categorised as those aspects important for the contribution of the thesis, putting modelling and systems thinking in the wider perspectives of dynamism. Among the topics discussed in this chapter are principles of modelling, systems dynamic behaviour, and simulation approach.

6.1 Principles of Modelling

As explained earlier, critical infrastructure systems (and as defined in this thesis) include power grid, oil and natural gas production, energy distribution, transportation networks, water and sewerage systems, networks, etc. Rinaldi et al, argues that "*the sheer complexity, magnitude, and scope of a nation's critical infrastructures make modelling and simulating security risks exposure of critical infrastructure systems important element of any analytic effort*" [2]. In a related study, Stapelberg (2008) claims that the modelling process is "*critical in the general understanding of system interdependencies*" [80].

It is therefore justified to argue that the modelling approach is also useful in the assessment of the security and safety of critical infrastructure systems. The assessment approach involves exploring the complexities, which are introduced by systems integration and the associated security risks, which are induced due to interdependencies. The use of modelling, in this case, is to examine the causal characteristics of each interdependent system so as to simulate the behaviour of the individual subsystems. Thus, to compare present situations to future scenarios. In this case, the core functions of ICS-SCADA systems are examined, and their risks metrics empirically assessed.

6.1.1 Modelling Building Blocks

Building blocks are the basic entities, which make up a model under construction (figure 6-1). The structure of building blocks in modelling shows hierarchies in the theory of structures. A model comprises of '*Levels'* and '*Rates'* (details in the next section). Sterman (2002a) defines dynamics modelling as a process of gaining *"insight into situations of dynamic complexity and policy resistance"* [151]. In this study, it is argued, the dynamic process provides a systematic approach to understand the behavioural characteristics of systems interdependencies. Thus, interdependent systems are inherently dynamic, and their complexities are inborn from their structures and operations. According to complexity adaptive theorist, the dynamics of interdependent systems "*rise from their feedback processes, either positive (*for Reinforcing – represented in the modelling process as *'R') or negative (for Balancing* - represented in the modelling process as *'B')*" (as shown in figure 6-2) [151].

Inference; an increase in systems' vulnerabilities increases systems' threats exposure, which in turn increases existing vulnerabilities. This is a reinforcing loop (represented in the modelling process *as '+ve*') indicating a positive effect on the underlying variable. Similarly, an increase in threat vectors leads to an increased in controls measures, which in turn decrease threats exploitations. This is a balancing loop (*re*presented as '*-ve'* in the modelling process) with a negative effect.

6.1.1.1 Stocks, Flows, Levels, Rates and Auxiliary

Stocks (also known as Levels) and Flows (also known as Rates) are fundamental building blocks in a modelling construction process (see figure 6-1). Stocks are used in defining the behaviour of a system and its subsystems. Flow influences stock dynamics and is represented in a mathematical expression (e.g. equation 6.1). As indicated above, a model comprises of Levels and Rates. Levels can only be affected by its connected Rates. Rates are controlled either by another Rate or by the Rate's equation. Rate equations comprised of Auxiliaries and Constants. Another fundament component in the block building is 'Time' and 'Sizes of Time Step' a simulation is programmed to run. This is subjective to the problem being modelled.

$$\text{Stock (t)} = \text{Stock}\,(\,l_o\,) + \int[(\text{inflow(t)} - \text{Outflow (t)}]\,dt. \qquad (6.1)$$

$$\text{Rate} = \frac{\text{Desired Action}}{\text{Delay}} = \frac{\text{Discrepancy between Goal and Observed Condition}}{\text{Delay}} = \frac{\text{Goal}-\text{Level}}{\text{Delay}} \qquad (6.2)$$

Equations (6.1) and (6.2) are Level and Rate equations respectively. Combining the two equations results in feedback between the parameters (i.e. being modelled). The "B" in figure 36 means balancing feedback that governs the loop; the counter arrows show its directions. The building blocks (stock and flows), described by figure 6-2 and explained in equations (6.1) and (6.2) are the tools to map the feedback loops. Feedback loops are the structural elements of systems [108]. They are considered as the fundamental building blocks for learning and making decisions. In the simulation process, stocks and flows patterns are observed at a different time interval by assigning different numeric values to each vector. Similarly, in the construction of the simulation; stocks and flows are the determinants of the model's behavioural patterns. Occasionally, auxiliary variables are introduced in the modelling construction to better explain the models' behavioural (e.g. figure 6-2). Figure 6-3 shows a model behaviour graph.

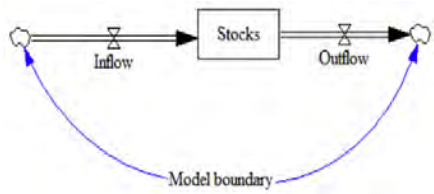


Figure 6- 1: Stock and flow diagrams

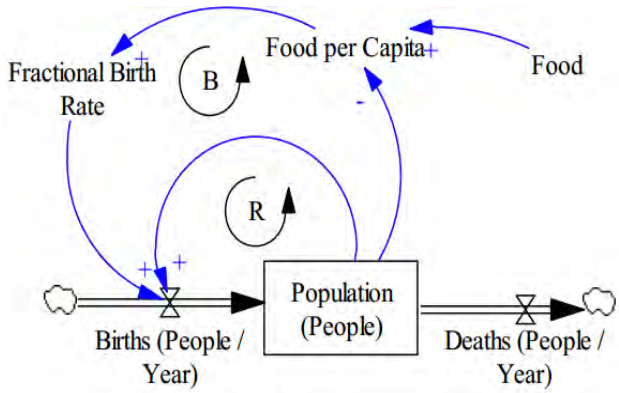


Figure 6- 2: Stock and flow diagram with Auxiliaries

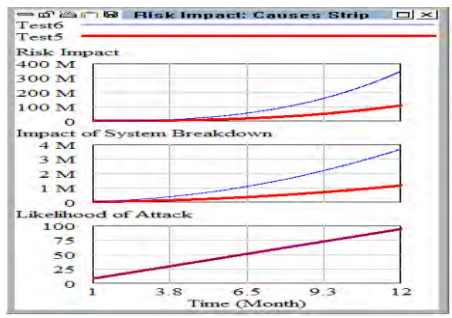


Figure 6- 3: 34: Behaviour graph

6.1.3 Systems Dynamic Behaviour

Dynamic systems have been identified to exhibit three different fundamental characteristics. These are exponential growth[60] (figure

[60] *"Exponential growth is exhibited when the rate of change (i.e. the change per instant or unit of time) of the value of a mathematical function is proportional to the function's current value, resulting in its value at any time being an exponential function of time, i.e., a function in which the time value is the exponent. In the case of a discrete domain of definition with equal intervals, it is also called geometric growth or geometric decay, the function values forming a geometric progression. In either exponential growth or exponential decay, the ratio of the rate of change of the quantity to its current size remains constant over time. The formula for exponential growth of a variable x at the growth rate is*

6-4a), goal-seeking[61] (figure 6-4b) and oscillation[62] (figure 6-4c). The aim of the behavioural examination in the assessment process is to identify how the dominant (dependent) system functions and its impact on the interdependent systems.

a b c

Figure 6- 4: System Dynamic Behaviour (a, b, c)

6.1.4 Causal Loop Diagrams

Causal loop diagrams (figure 6-5c) are a block of diagrams designed to depict 'causes' and 'relationships' as well as patterns of systems' behaviour. Each link of the diagram has a causal interpretation. For example, an arrow moving from point 'X' to point 'Y' means X causes Y (i.e. the actions of X influences Y's action). For instance, in figure 6-5c; "Work to Do" increases resources requirements, which then increases the chances of introducing substandard tools. When this happens, the standards required will be reduced leading to the reduction in the job done.

The dynamic process (section 6.2) discussed in this study is built using Vensim PLE[63]. Two categories of Vensim PLE tools are utilised: structural analytics and dataset analytics tools. The structural analysis tools are used to investigate models' structure while dataset analysis tools are used to analyse the simulation datasets, which assist in determining the variables' behaviour.

$$X_t = X_0(1+r)^t$$

r, as time t goes on in discrete intervals (that is, at integer times 0, 1, 2, 3, ...), is where x_0 is the value of x at time 0 [152]*"*

[61] Goal seeking: the process of reverse computation to get an input to influence an output/outcome

[62] Oscillation: Repetitive variation to measure event in time *'t'*

[63] http://vensim.com/vensim-software/#ple

a b c

Figure 6- 5: Causal Loop Diagrams (A, B, B)

6.1.5 Simulation Approach

Simulation construction is mathematically iterative. There are three stages in the construction process (i.e. Create, Integrate and Evaluate (figures 6-6).

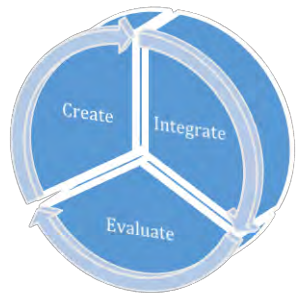


Figure 6- 6: Stages in a simulation construction

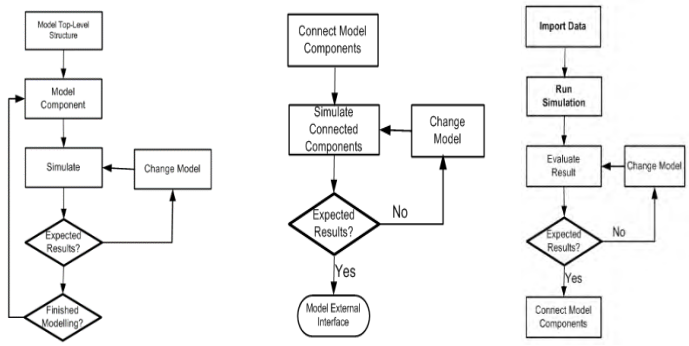
6.1.5.1 Stages in a simulation construction

i. **Create**: this stage involves constructing the individual models and their sub-components. Figure 6-7a is a flowchart that depicts the stages and movement in the construction flow

ii. **Integrate**: this is the process of connecting individual components or subsystems, so as to simulate their behaviour and to observe their responses over time. Figure 6-7b is the integration process flowchart. It shows the flow and the logic in the integration process

iii. **Evaluate**: this is the process of assessing the simulation

results to determine if the present outcomes match predetermined expectations. Figure 6-7c is the evaluation process flowchart that shows the steps and the logic in the evaluation process.



A: Model Creation B: Models Integration C: Models Evaluation

Figure 6- 7: Figure 38: Model Development Flowcharts (A, B, C)

6.1.6 Qualitative and Quantitative Modelling

Both qualitative and quantitative modelling has been used in system dynamics for a very long time [108,153]. The qualitative procedure (also known as *systems thinking)* was popularised by [154,155] and has been used since the late 1970s. The guidelines on whether to apply qualitative or quantitative modelling are identified as a problem to be addressed. That is "when to map and when to model" [153]. On the basis of the thesis's objectives, a quantitative modelling technique is considered. This is to enable the quantification of information systems assets (part of the risk assessment process). Secondly, the quantification provides the opportunity to simulate the behaviour of dynamic interdependent systems on the principles of formal (mathematical) reasoning. Importantly, it is argued, without simulation, it is near impossible to understand, estimate and to predict systems' nonlinear dynamics behaviour.

According to Linnéusson, both qualitative and quantitative modelling techniques are based on fundamental principles of causes and feedback loops [102]. Furthermore, Linnéusson claims that

quantitative modelling brings:

i. Variable characteristics: "*which describes the interrelatedness of systems components (stocks, flows, and constants) in the form of equations"* [102] and
ii. Enables simulations through computations and provide an experimental model*"* [102].

According to Sterman and in [156], system dynamics provide a dynamic presentation of the modelled system; facilitating understanding of problem causes [151] and the possibility to experiment on different scenarios in order to explore how to perform change [156,157]. In a related study, Torres claims that quantitative modelling provides a better analysis of systems of dynamic nature [158]. Furthermore, Torres asserts that simulation brings a better chance to test if uncertainty affects systems, and that simulation facilitates judging if enough data exists to reach correct conclusions [158].

6.2 Modelling Approach

Monga describes the modelling process as a *"fundamentally creative, intensive"* and iterative exercise [139]. Figure 6-8 depicts the processes of dynamic modelling [151] from the work "System Dynamics: Systems Thinking and Modelling for a Complex World" [159]. The original work itself is grounded on a methodology proposed by [159]. The modelling process is built on two fundamental principles: structural analysis and dataset analysis. The former involves assessing the structure of the model while the latter explores the various underlying datasets, which are useful to the model design process. There are five (5) stages in the modelling process. The succeeding sections provide a detailed explanation of these processes.

6.2.1 Problem Articulation

It is the process of identifying the purpose of modelling as well as the scope (i.e. problem to be addressed, what needs to be done, the expected outcome, and how to measure the outcome). Following from the thesis objectives, the problem articulation process guides the

modeller to articulate the issues concerning systems complexities, control assessment, existence (or otherwise) of security policy, contingency plans, impact assessment and security risk decision metrics. Two sets of tools are useful in this case: Reference Modes and Time Horizon. Reference Modes are annotated diagrams, which are used to represent the dynamic problems over a period of time. Time Horizon establishes the periods within which problems are investigated and articulated.

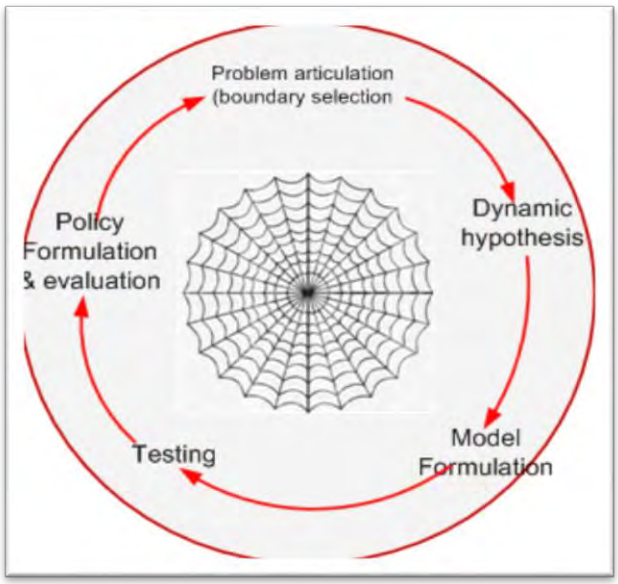


Figure 6- 8: Dynamic Modelling Process

6.2.2 Dynamic Hypothesis

A dynamic hypothesis is the examination of the interdependent system and its subsystems. The aim is to establish how each subsystem relates to a unified system of which they are part. This stage investigates how the behaviour of an individual system (and the underlying variables) influences the system of which it is part. In the

case of SCADA, it involves establishing how the behaviour or an operational function (i.e. PCL, SCADA, DCS, SIS and HMI) impacts the safety of the entire controlled system[64]. For accuracy, a scientific data collection method is required to develop an appropriate hypothesis to explain the underlying problem. This does not contradict the earlier arguments put forward by pioneer authors.

A dynamic hypothesis assumes that a controlled system exists in a state of equilibrium which is affected not only by its endogenous variables but the exogenous variables. The simulation process as proposed in this study tests the following hypothesis:

i. Integrating industrial control systems with cyber infrastructure systems increases systems complexity
ii. Systems complexity increases systems' risk exposure
iii. Interdependency between cloud infrastructure and ICS-SCADA systems increases the later's risk exposure due to inherent risks induced by the former
iv. There is a correlation between threats and vulnerabilities (which is either reinforcing or balancing)
v. Lack of controls mechanisms increase the likelihood of threat actors exploiting systems vulnerabilities
vi. A rise in threat attacks increases attack impact (conditioned on the value of the target assets)

6.2.3 Model Formulation

This requires setting up system models. The setting up process implies that the model under construction is coded with algorithms (i.e. embedded with mathematical expressions or equations), and supported by underlying theories, assumptions, and sets of conditions. The process includes the analysis of systems complexities, vulnerability, threat events, security controls and the impact of threat attacks.

[64] Due to security concerns and policy restrictions, a live assessment test was not performed in any controlled environment

6.2.4 Testing and Validation

Model validation involves examining and testing the model to assess whether it replicates the behaviour of the system it represents. This gives the modeller the opportunity to examine the validity or otherwise of the simulation process and the method used (based on the datasets collected and the results generated). Results generated from the simulation processes are then tested to validate the robustness of the existing methods and processes.

6.2.4.1 Validation Methods

Barlas proposes a three tests validation method. These are [160]:

i. **Direct structure test:** This approach does not depend on simulation results. It rather compares the model's output with knowledge about the real system.
ii. **Structure-oriented behaviour test:** This uses simulation results to study the model's behaviour as the means to assess the weakness in the system.
iii. **Behaviour pattern test:** this is the measure of model accuracy in reproducing the behaviour patterns found in the real system.

6.2.5 Policy Design and Evaluation

After the dynamic processes have been tested and proven, dynamic policies and procedures are then designed to guide the 'Dos' and 'Don'ts' in the risk assessment process. In terms of the institutional risk assessment process, one common policy document that guides the process is the IT Acceptable Use Policy (ITAUP). The ITAUP in many environments acts as the blueprint or a checklist for the institutional risk strategy. In the security risk assessment process, policy formulation and evaluation, form part of the vulnerability and threats assessment process. The policy statement, in this case, indicates in clear terms the do(s) and don't(s), so as to protect the system and ensure users' safety. According to Sterman, *"all too often, a well-intentioned effort to solve pressing problems creates unanticipated side effects"* [100]. An evaluation process provides the opportunity to address the issue of 'side effect'. Policy evaluation is

part of the overall systems audit (i.e. validating guidelines against standards and acceptable procedures). Furthermore, policy evaluation acts as a checklist, which ensures compliance, self-checks and acceptance.

A dynamic process, according to Forrester, has minimal effect, unless an approach changes the way situations are perceived [108]. Forrester, further argues that dynamic models provide the meaning that "*links the past to the present"* by explaining "*how present conditions arose*", and how to project present values into alternatives expectations "under a variety of scenarios determined by policy alternatives" [108]. A model-based policy formulation involves the use of modelling as an investigative tool in assessing the effect and impact of a policy on systems' behaviour [139]. This requires formulating new policies to determine the impact of systems' behaviour in different conditions. Supporting this argument, Monga claims that for a policy to be considered useful and effective, its development and evaluation need to be tested and implement so as to gain stakeholders' confidence [139].

6.3 Systems in Perspective

This section describes a system as defined by the thesis. The definition considers the system as the primary cyber infrastructure to protect and its environment. In the modelling process, this definition is extended to include the processes relating to the institutional risk assessment within the scope of industrial control systems as an integrated component of cyber-infrastructure. Figure 6-9 depicts the relationship between the system and its subsystems. Table 6-1 explains the variables within the system and its environment.

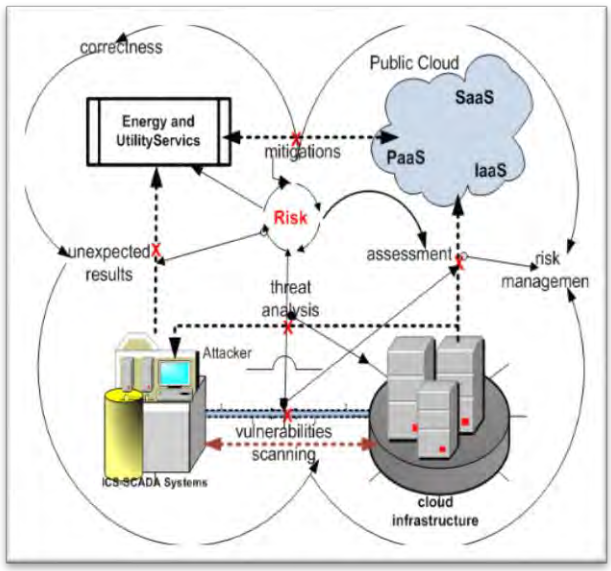


Figure 6- 9: System Causal Map

6.3.2 Subsystems

Figure 6-9 depicts the interactions between the system under discussion and its environment (i.e. systems characterization). It is made of the system and its subsystems referred here as variables (nodes), and the links (edges) connecting them, which depict the connection among the variables. The key variables (i.e. subsystems) include the controlled environment (i.e. space) and the infrastructure (as the technology) supporting them. Other variables include cloud services as cyber infrastructure as well as the risk metrics, which form the basis of the assessment process. As identified in chapter two, some of the core-controlled variables in the ICS-SCADA

system include HMI[65], SIS[66], DCS[67], VFD[68] and PLC[69] and other operations' technologies, which support energy distribution. The interaction between cloud infrastructure and ICS-SCADA systems provides the basis for the development of the assessment framework.

Table 6- 1: System Causal Map – key variables

Variables	Description
Enterprise Operation	All over the world, agencies exist to provide services in which the Act establishing their existence mandates them to do. Agencies' operations define their identity and existence. The focus of this study is on energy (electricity) distribution as the core operations of GRIDCo (Ghana) and Puget Sound Energy (WA, USA) (electricity and natural gas).
Institutional Technical Infrastructure (ICS-SCADA)	The process of security risk assessment requires that systems' operators, administrators, asset owners and other stakeholders have a full understanding of the criticality of the systems under their care and to exercise a duty of responsibility and care. These resources include both physical and soft technologies. In the controlled environment, while the focus is on operational technology, the assessment process is extended to other informational technologies. NIST SP800-53 framework provides a checklist for most information technologies (tools) required in controlled environments.

[65] Human Machine Interface
[66] Safety Instrumented System
[67] Distributed Control System
[68] Variable Frequency Drives
[69] Programmable Logic Control

Cloud Environment	This relates specifically to cloud services and the underlying infrastructure available for adoption. In the system's characterization, the objective is to establish the environment in which critical (core) infrastructure is situated and its characteristics. This is useful in identifying threat sources and their propagation pattern. At the application service level, it is assumed institutional operations (which are cloud-dependent) interact with cloud services creating service interdependencies.
Cloud Infrastructure Set (Core)	As institutions adopt cloud, the cloud infrastructure interacts with the institution's information (technical) resources; this interaction creates infrastructure interdependency, increasing systems complexities. In the assessment process, it is assumed, any attack on the cloud infrastructure setup causes cascading effects on dependent systems due to the induced interdependencies.
Risk Metrics	The risk metrics provide the arithmetic datasets as well as algorithmic constraints for model construction. They include the assets (as the system to protect) vulnerabilities, threats vectors, the likelihood of an attack, impact assessment, controls (as countermeasures) and the dynamic modelling.

6.4 Conclusions

System dynamics is a systemic approach to understanding systems' behaviour and their complexities. According to Forester, the study of the dynamism of systems is to explain the "universal structure of social and physical systems" [159] and provide guidance for the construct of models. This makes it suitable for the analysis of risks in interdependent critical infrastructure systems, a focus of this thesis. It also supports the use of quantitative modelling in the study of dynamic systems. Because it provides a tool that is able to dynamically present the modelled systems' behaviour [102].

As established, assessing risks in interdependent infrastructure systems requires the understanding of their dynamics as well as the interplay among the interconnected systems and their subsystems. It is assumed, the simulation approach will enable systems designers to emulate the behaviour of interdependent systems under severe conditions (e.g. systematic cyberattack). In the simulation process, systems and their subsystems are presented as the underlying variables (i.e. cause diagrams, graphs and patterns), as the means to observe systems behavioural patterns in real-world situations. This is significant in a controlled environment where the criticality of systems' operations makes it difficult to conduct a real-live risk assessment.

The next chapter conceptualises the modelling processes, making a case for the construction of the thesis's proposed dynamic risk assessment framework.

Chapter 7: Dynamics Modelling

"What happens to one infrastructure can, directly and indirectly, affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy……. And the sheer complexity, magnitude, and scope of the nation's critical infrastructure systems make modelling and simulation important elements of any analytic effort"

Steven M. Rinaldi

In this chapter, a novel framework for dynamic risk assessment for critical infrastructure systems as well as the guidelines to use is presented. It begins with building an understanding of the system to assess and its environment. Following that, a dynamic modelling process is initiated to model the system to reveal its structural characteristics. Using the constructed model, simulations are run to test if the model outcomes meet its objectives, and test results matched the expected outcomes. Finally, the proposed thesis's framework is presented along with the guidelines to use.

7.1 Problem Articulation

The model design as discussed in this chapter is grounded on the thesis's problem statement. As stated earlier, critical infrastructure systems are the most vital resources of a country, without which the country's economic and social well-being suffers. And all over the world, these critical resources are required to be available, reliable

and sustainable to support the social and economic living of the citizenry. The availability, reliability and sustainability thereof, depends on how secured the resources are, in their operating environment.

According to Helbing, understanding systems complexities is necessary for the behavioural assessment of the "*systems' structural, dynamics, functional and algorithmic complexities*" [161]. Helbing further argues that the process of assessing risks in interdependent systems must equally analyse the systems' induced complexities [161], and a method of such assessment is worth an academic effort.

7.2 Dynamic Hypothesis

In the previous chapter, it was claimed, the behaviour of interdependent systems is influenced by their external and internal forces, which then impact how systems react to their environment. To support this accession, the thesis tests the following hypotheses:

i. Integrating industrial control systems with public cloud infrastructure systems increases systems complexity
ii. Systems complexity increases systems security risk exposure
iii. Interdependency between cloud infrastructure and SCADA systems increases the later's security risk exposure due to inherent risks induced by the former
iv. There is a correlation between threats and vulnerabilities (either reinforcing or balancing)
v. Lack of control mechanisms increase threats attack
vi. Increase in threat attack, significantly impact systems functions (negatively)

7.3 Infrastructure Interdependency Modelling

Complexity adaptive theorists describe critical infrastructure systems as complex interdependent systems [162]. Dynamic modelling process connects to the principles of feedback effect inherent in interdependent systems. This episteme is grounded on the philosophical position propounded by Forrester, who argues that "feedback structures in dynamic systems are responsible for the

systems' behavioural changes [163]. Thus, systems dynamic behaviour is a consequence of their inherent structure. Rinaldi modelled this concept (as shown in figure 7-1) to show how systems and their subsystems interact among themselves to create systems interdependency [134].

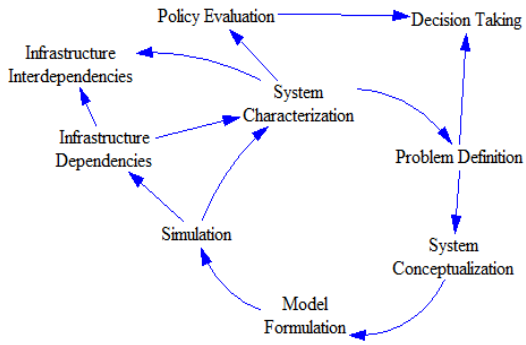


Figure 7- 1: Infrastructure Interdependency Structure [134]

7.4 Model-Based Design

This is defined as the process of developing a dynamic system (i.e. interdependent critical infrastructure). A model is an executable artefact (with attributes). System dynamic modelling is the centre of the development of model-based designs. After the model is developed, simulations are run to evaluate whether a designed model meets the requirements of the physical system it represents. Figure 7-2 is a system integration model that depicts a system and its subsystems. In the example below, the model is simulated to observe the system's interdependency and structural behaviour. In this context, the various subsystems making the complete system is observed as well as their structural characteristics (details in the sections below).

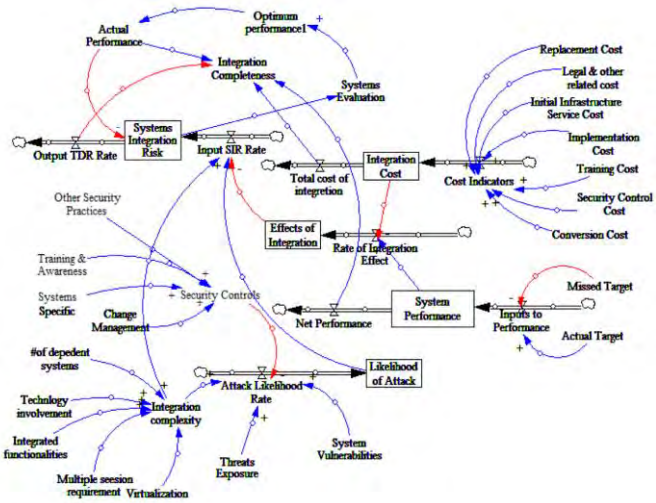


Figure 7- 2: System integration modelling

7.4.1 Structure Analysis of Infrastructure Interdependencies

This involves identifying and analysing the causal relationships among systems and their subsystems, and the extent of their interdependencies. This is based on the assumption that systems integration is complicated by other exogenous factors, which are introduced by the convergence with cyber infrastructure systems. Figure 7-3 represents an infrastructure interdependency model with systems variables and their causes within the model structure. The dynamic approach (as shown in figure 7-3) involves the analysis of the structure of the system by tracing through system's inherent make-ups in order to establish what causes a variable within the structure to change.

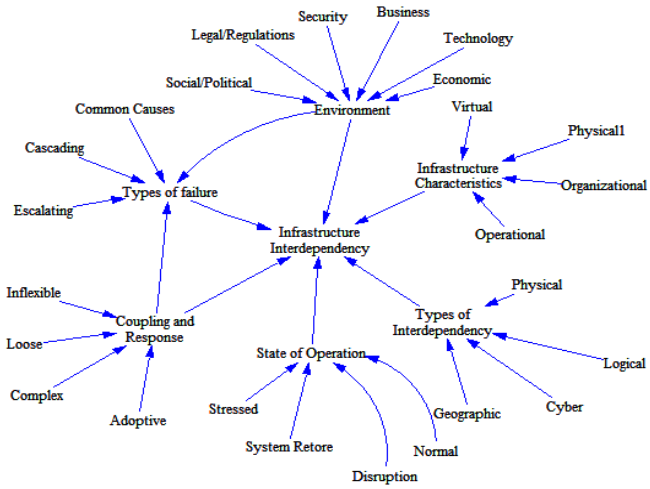


Figure 7- 3: Infrastructure Interdependencies model with exogenous factors

As shown in figure 7-3, some of the exogenous factors which impact infrastructure interdependency include the type of interdependency, state of operation, coupling and response, type of system failure as well as the environment in which the infrastructure is found. Each of these factors has its own sub-systems, which influence its existence and identity. For example, factors influencing 'coupling and 'response' include inflexibility, looseness, complexity, and adaptive. Similarly, factors considered to influence system environment include social/political, legal/regulations, technology, economic and business activities. Furthermore, the state of interdependency operations is a factor of stress, restore, disruption and normality.

7.4.2 Causal Analysis

Causal analysis is the process of tracing through the model's structure to establish what causes 'something' to change (i.e. systems' behavioural). It involves identifying the relationships among variables in interdependency systems and provides a logical base for assessing complexities associated with interdependent systems. The degree, to which interdependent systems and their

subsystems are coupled, is influenced by their inherent characteristics (figure 7-4). The relative flexibility of the characterisation determines how such systems respond to their new environment and the conditions that determine their internal weakness.

In the assessment process, the role of the assessor is to establish the root cause of a security event within the interdependent system. This helps to isolate the problem before it cascades and affect other interdependent systems.

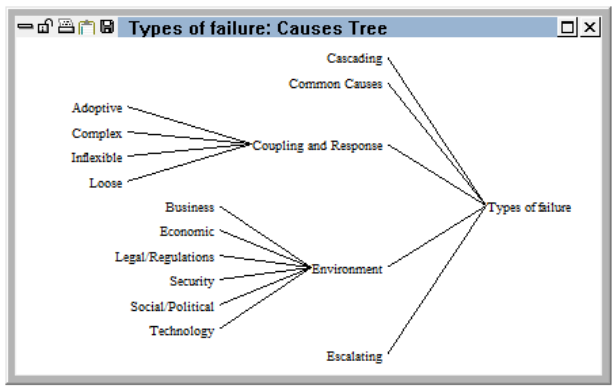


Figure 7- 4: Causal Diagram for Exogenous factors

7.4.3 Modelling Infrastructure Interdependencies

This subsection provides detailed descriptions of a model's behaviour and the relationships among its subsystems (figure 7-2). Figure 7-5 represents a modelling structure of infrastructure interdependency systems. The objective is to assess the behavioural patterns of the system and its subsystems, and how the modelling design influences simulation building.

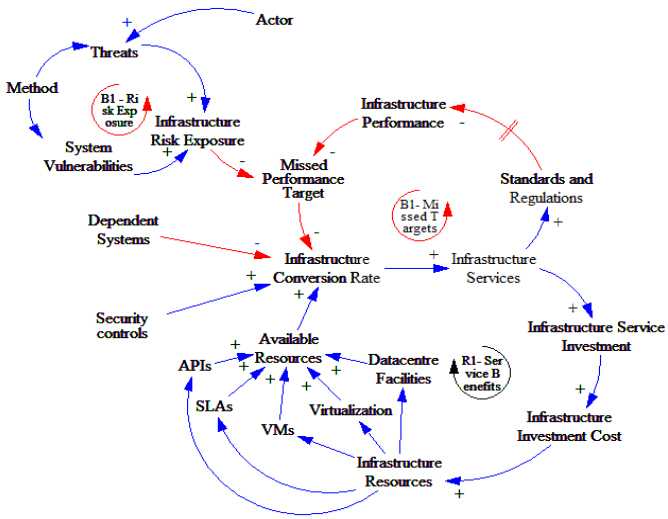


Figure 7- 5: CLD of Infrastructure Services

7.4.3.1 Causal Loop Diagram (Cyber Infrastructure)

Figure 7-5 depicts a CLD of cyber (cloud) infrastructure service with its subsystems. The model shows the interactions of various components of the cloud infrastructure setup; showing also the various possibilities in the risk assessment process. Key components are discussed below:

Threats and Vulnerabilities Pair (TVP): This is a matching of system's threat to its known vulnerabilities. Based on the diffused causal factors; the effect could either be negative or positive. The scenario is represented by a balancing loop (B1). As indicated earlier, the existence of security control mechanisms reduces the rate of risk exposure. All things being equal, this situation leads to an improvement in systems performances. Furthermore, an increase in infrastructure performance, will also lead to an increase in investment funding then increases investment in infrastructure systems; subsequently increasing resource availability. Such a situation increases the benefits derived from the system's overall performance. This is a positive affect, referred here as reinforcing

(i.e. R1-Services). Consequently, unregulated standards and unclear policy statements (in security investment) would also affect infrastructure services with negative effect (on performance targets). This negative scenario is known as balancing effect (e.g. missed target) represented by B1.

7.4.3.2 Causal Loop Diagram (Power Sector Infrastructure)

Figure 7-6 shows the dynamic modelling of energy infrastructure system and its subsystems. The objective is to assess the structural relationships between the interdependent systems. In this scenario, it is assumed energy supply rate is a function of local demand, and global demand and supply forces. The model depicts what is considered to be the operational activities relevant to energy generation and distribution, as well as the key supporting technologies. The determining parameters are SCADA technical functions, government as a regulator, generation technologies as well as capital investments.

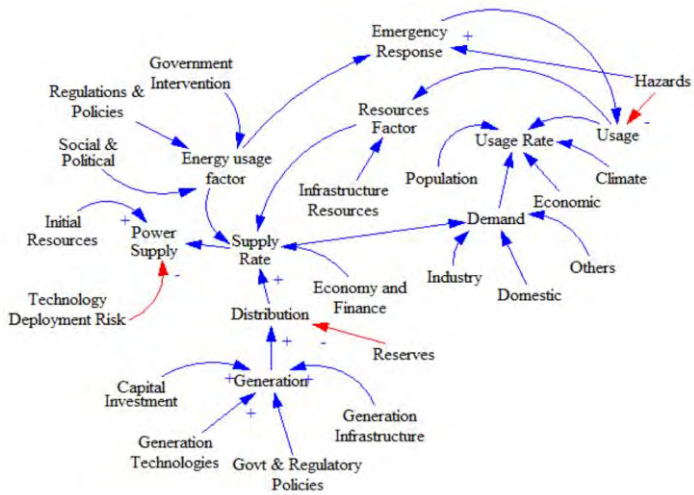


Figure 7- 6: CLD of Energy infrastructure system

7.4.3.3 Causal Loop Diagram (Infrastructure Interdependencies)

It is argued that energy supply rate is the function of distribution and generation (figure 7-7). Each of the subsystems has its own deterministic factors (sub-sub systems). For example, energy generation is the factor of capital investment, generation technologies, and government policies/regulations as well as available generation infrastructure. Additionally, the energy usage rate is a factor government intervention, policies and regulations and social and political atmosphere. Other factors are:

Determinants

i. *"Technology integration"*: The integration of cyber infrastructure services and SCADA systems forming infrastructure interdependencies.

ii. *"Integration risks"*: These are system-induced risks introduced due to systems interdependencies [14].

iii. *"Deployment risks*:" These are system-induced risks resulted from the technology deployment and use [14]. It is also assumed, as a new system is deployed, users and environmental forces will expose the new system to new risks. Deployment risk per the model is a function of the sum of the system's vulnerabilities, threats events, inherent complexities per available security controls, and security practices. It is further assumed that the availability of security controls reduces the rate of systems' overall risk exposure. Additionally, the system's environment and its risk exposure rate are statistically significant to technology integration (indicated by the balancing loop feedback effect (B3 likelihood) [14].

iv. *"System evaluation"*: This relates to the pre- and post-systems integration risk assessment strategy. The purpose is to establish the infrastructure requirements and how existing security control strategies and techniques protects critical infrastructure systems.

v. *"Technology integration performance":* This relates to the post-integration (performance) assessment measure. **Assumption**: System performance can either be positive (reinforcement) or negative (balance). This is also based on i) expected performance, ii) observed performance and iii) actual performance [14].

vi. *"R3 – System evaluation and findings"*: This is to observe and compare expected results with its actuals. Any identified gap, demands further assessment, which could affect the system's performance. This generates a feedback loop known as a positive reinforcement (represented as R1).

vii. *"B3 – Technology integration impact"*: It is assumed, technology integration has an effect on systems performance.

viii. *"B3 – Integration performance index"*: It is observed that technology integration leads to an improvement in the system's overall performance [14]. In an optimum performance level, the integration performance index is expected to lead to the reduction in infrastructure investment which in turn loops back and affects the system's overall performance [14]. This loopback effect is represented as B3 (i.e. a balancing loop)

ix. *"R3 – Integration benefit index"*: A poorly managed technology integration leads to unplanned shutdowns and prolongs systems' downtimes. This situation leads to a low-income generation, which in turn impacts future infrastructure investment (negatively).

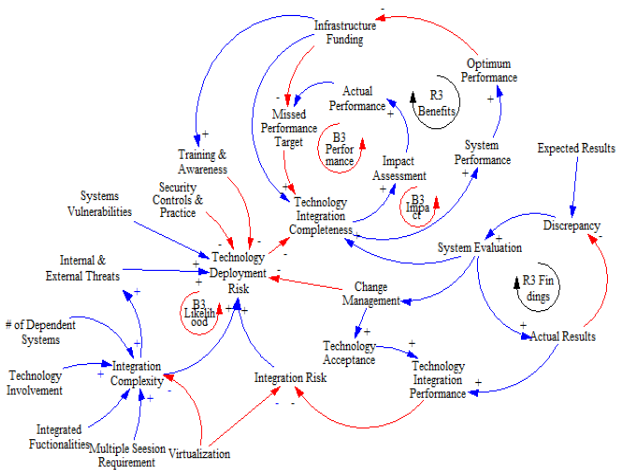


Figure 7- 7: Technology Integration Causal Loop Diagram

7.5 Simulations

This attempts to emulate and test the behaviour of the designed models. The objective is to assess future scenarios with the present situations. The following variables in the proposed risk assessment process are simulated and results presented below: i) likelihood of threat attack; ii) risk exposure and iii) the impact of threat attack.

7.5.1 Likelihood of Attack

Figure 7-8 is the simulation screenshot of the likelihood of an attack. A slider allows the system's user to manipulate the behaviour of a model at various adjustable inputs. Thus, the sliders act as the decision-making tools which control the input to the simulator. In this case, factors such as change management, multiple session requirements, etc. are constants, representing the system's performance indicators. Constants are defined as useful datasets which are set up prior to starting a simulator. For example, an Attack Likelihood Rate (ALR) signifies the probability of threat actor exploiting systems vulnerabilities (at a time *t*).

Determinants

Threat-Vulnerability Pair (TVP): As explained in section 7.3.3.1, TVP is a matching of system's threat with known vulnerabilities. It is assumed that an increase in TVP rate (either due to changes in threats exposure or system's vulnerabilities) changes the likelihood of an attack.

Complexity factors: They are parameters, which are considered to contribute to system complexity (as a result of infrastructure interdependencies). The following factors are considered to contribute to system's overall complexity: i) "*the number of dependent systems, ii) multiple session requirements, iii) integrated functionalities, iv) virtualization and v) the integrated technologies"* [14].

7.5.2 Controls Mechanisms

These are considered to be both technical and administrative procedures deployed to counteract threats exposure and subsequent impact. Per the model design, the rate of controls is a function of the existing security controls and practices. Control variables are measured in the scale of 0.1 (very weak) to 1.0 (very strong). This measurement has been adopted for the computational purpose.

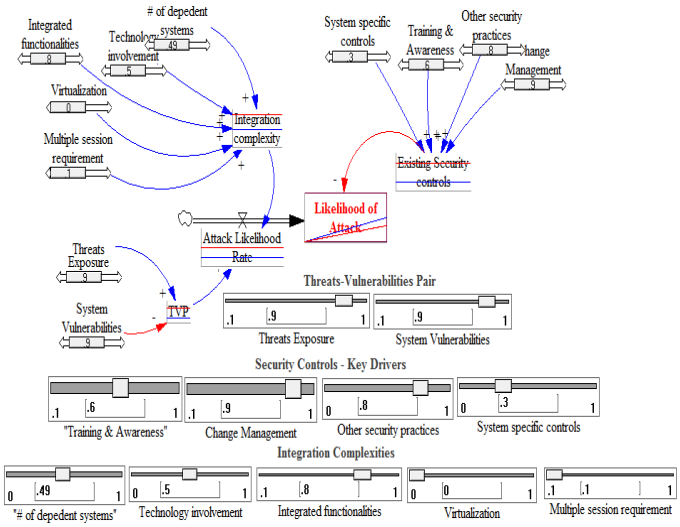


Figure 7- 8: Simulation Screenshot of Likelihood of Attack

7.5.3 Impact Assessment

The impact of a security breach is measured by the total loss of the system (i.e. value and effect). In determining the value of an asset, the following considerations are made: the cost of man-hours required to restore the system to an optimal level, the cost of rebuilding and reinstate, the cost of downtime and repair, legal fees and other administrative charges as well as the value of the output from the system.

Assumptions: The output of an interdependent system is the total sum of the outputs of the independent systems less any missed targets [14]. In the event of a security attack, the impact of such an event is in two folds – loss of performance (output) and the total cost to restore or to rebuild the system [14]. The simulator (figure 7-9) is run to monitor the behaviour of the system at different costs conditions.

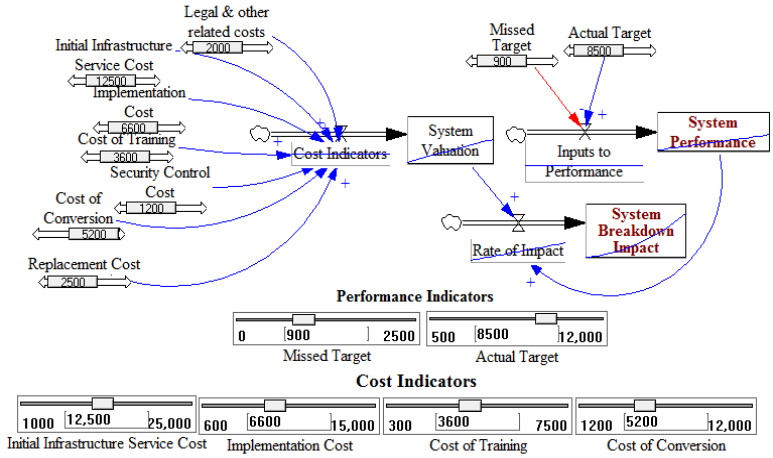


Figure 7- 9: Simulation Screenshot of the effects of an attack

7.5.4 Risk Exposure

Risk is defined here as the product of a likelihood of an attack and the corresponding impact ($R = L * I$) [14]. This definition is based on the risk function established in chapter 1. Figure 7-10 is the simulation screenshot of security risk assessment simulation. Figure 7-6 is the corresponding stock and flow diagram.

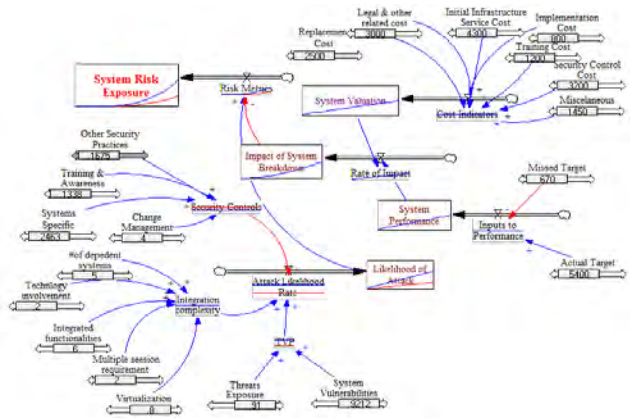


Figure 7- 10: Simulation Screenshot of Risk Exposure

7.6 Hypotheses

This section tests the proposition derived from the research questions. The hypothesis is built into the models designed to assess how the models replicate the dynamics of the system they represent. The objective is to assess the behaviour of systems (and their subsystems) when exposed to different threats conditions[70]. The following pre-conditions are tested for a likelihood of a threat attack:

i. *"High threat exposure levels, low vulnerability and weak security controls"*
ii. *"High threat exposure levels, high vulnerabilities and weak security controls"*
iii. *"High threat exposure levels, high vulnerabilities and strong security controls"*
iv. *"High threat exposure levels, low vulnerabilities and strong security controls"*

[70] The models as simulated here have not been implemented on any specific technology (or project) and for that matter all datasets were chosen to test the system based on experts' opinions. Parameters will have to be modified for specific projects in real time situation.

Table 7- 1: User-defined parameters for the likelihood of attack [15]

Test 1	High threat level	Low vulnerability level				Weak security controls			
	0.9	0.1				0.4			
Test2	High threat level	High vulnerabilities				Weak security controls			
	0.9	0.8				0.4			
Test3	High threat level	High vulnerabilities				Strong security controls			
	0.9	0.8				3.4			
Test4	High threat level	Low vulnerability level				Strong security controls			
	0.9	0.1				3.4			
Test5	Test2 + Low Asset Value	Asset 1	Asset 2	Asset 3	Asset 4	Asset5	Asset 6	Asset 7	Asset8
		100	100	100	100	100	100	100	640
Test6	Test2+High Asset Value	Asset 1	Asset 2	Asset 3	Asset 4	Asset5	Asset 6	Asset 7	Asset8
		7065	780	12430	1806	2018	11050	3957	4730

7.6.1 Test1: Likelihood of an attack

In this context, the simulation is run at two scenarios: when the vulnerability level is high and the control level is low and when the vulnerability level is high and the control level is high. In addition to values in table 7-1 The following timesteps were applied:

Initial time[71] = 1 month
Final time = 12 months
Timestep = 0.0078125 months

Observation: It is observed that (shown in figure 7-10) when vulnerability level is high and control mechanisms are low, the likelihood of threat attack is high. The situation is different when both threat and vulnerability levels are high and control mechanisms are high. In this case, the likelihood of an attack is relatively low.

7.6.2 Test 2: Increase in Vulnerability increases Threat attack

Following test 1, we test the likelihood of attack when system vulnerability increases. The following vulnerability conditions (rate) were made (at a constant threat rate of 0.8):

i. *"At a very low vulnerability rate (i.e. 0.2)":*
ii. *"At a relatively medium vulnerability rate (i.e. 0.5)"*
iii. *"At a high vulnerability rate (i.e. 0.8)"*

Observation: The simulation result (figure 7-10) shows that the likelihood of attack goes up irrespective of the level of security controls.

7.6.3 Test 3: Lack of risk controls increases the rate of Threat Attack

Observation: It is observed (figure 7-10) that when the rate of security controls is low, the rate of threat attack is high (even when the rate of vulnerability is low).

7.6.4 Test 4: Asset Value is proportional to the impact of an attack

The value of a system is proportional to the rate of its attack impact. This test is run by introducing two additional propositions:

i. Test V: "*when the value of the system is low"* and
ii. Test VI: "*when the value of the system high system"*.

[71] Measured in seconds

Assumption: It is assumed that the value of a system is the total cost of either building/acquiring a new system or restoring an existing one (breakdown due to threat attack) to its optimal level.

Observation: From the simulation result, it is observed that when the value of an asset is high, the impact of its attack is high and vice versa (figure 7-10).

7.6.4 Test 5: Interdependency increases risk exposure rate

Systems interdependencies increase systems complexity, which then increases the system's risk exposure rate. The following are considered to induce systems complexities:

i. "*Number of dependent systems"*
ii. *"Type of technology involvement"*
iii. *"Integrated functionalities"*
iv. *"Multiple session requirements" and*
v. *"Application virtualization"*

For each of the above variables, Tweneboah-Koduah and Buchanan propose a numeric scale of 0.1 (weak) to 1.0 (very strong) to signify the influence or otherwise of a particular variable. For example, 0.1 indicates a particular variable has a very weak or has no influence on system interdependency (e.g. application virtualization). Similarly, 1.0 indicates that a particular variable has a very strong influence on integrated system behaviour. The simulation results [of three possible scenarios i.e. (0.1 – weak); (0.5 – average); and (0.9 – strong influence].

Observation: It was observed that as the number of interconnectivity increases, the system's complexity rises and the rate of the system's risk exposure increases accordingly (figure 7-10).

7.7 Risk Assessment Policy Suggestions

As established in chapter 2, cyber infrastructure systems are beset with lots of threats. These include state-sponsored threats (APT), insecure web applications (e.g. XSS, SQLi, IP misconfigurations, etc.), insider threats, and malicious codes (i.e. worms, Trojan horses and ransomware). Notwithstanding, it is observed that the

deployment of effective control measures such as security training, awareness, and the existence of effective security policies are necessary to protect infrastructure systems against cyber adversaries. It is also claimed, the dynamics in the threat landscape coupled with the complexities of critical infrastructure systems necessitate the need to review existing security policies on infrastructural investment, systems protection and the overall infrastructure management. The objective is to encourage best practices that aim at protecting critical infrastructure systems. It has also been observed that infrastructure interdependencies increase system's complexities which in turn impacts systems security risk exposure [14]. The research concern is how (i.e. the method) to identify systems' complexity. In this case, the study proposes a complexity modelling architecture in interdependent systems using system dynamics modelling.

As established, the convergence of cyber infrastructure with critical infrastructure systems threatens the fundamental aspect of our society, it is essential to identify, design and implement adaptive methods to increase the worldwide defensive conditions to protect critical infrastructure systems in the most effective manner possible [164]. Additionally, Mori and Gato argue that the damages caused by cyberattacks are becoming larger, broader and more serious (when one includes the monetary losses as well as the loss of lifeline [165]. In a related study, Li et al, further argue that as computer and related technologies increase in volume and in complexity, malicious cyber-attacks are evolving, and as a result, society is facing enormous risks in the cyberspace more than ever before [166]. Bruijn and Janssen on their part posit cybersecurity has become a global phenomenon representing a complex socio-technical challenge for many institutions [167]. And it also one of the most important challenges faced by many governments today, yet, the visibility and public awareness remain limited [167]. Bruijn and Janssen further argue that the inability to frame cybersecurity methods to the needs of organizations has resulted in a failure to develop suitable policies to regulate the ecosystem [167].

Furthermore, Tweneboah-Koduah and Buchanan claim, system administrators, asset owners and managers must develop the

mechanism to identify both internal and external factors that are likely to increase systems complexity (unique to their own environment) so that their structural characteristics can be internally assessed [14]. This is because systems' structural characteristics provide clues in identifying causal relationships in interdependency systems [14]. Besides their usefulness in building simulations, they provide the basis for identifying threat actors, methods and their propagation patterns.

Another important policy statement that needs consideration is the valuation of an information asset. As established, the value of an asset is statistically significant to the impact of its threat attack. The challenge, however, is the lack of an acceptable method to value for critical infrastructure systems. Extant studies have so far failed to discuss or provide an acceptable method to quantitatively measure the value of critical infrastructure systems, especially in a controlled environment. The simulation method proposed in this study has attempted to address the gap[72]. Further studies, however, would be required to test and conceptualize the proposed approach.

7.8 Gap Analysis

The gap analysis provides the basis to outline the thesis's contribution, arguing on the need to support the application of system thinking and dynamic modelling to the institutional risks assessment process. It is argued, identifying the gap makes a case for the support of the adoption of a proposed assessment framework in the context of cyber infrastructure protection. The analysis is based on input from both literature and data collection from the field.

[72] The values used for estimation could be subjective and were used purposely for analysis and do not reflect open market conditions. Additionally, it is observed that controlled systems and for that matter, the power industry, in general, has one of the most complex networks of resources; assigning economic values to all these resources will require a complete shift is policy formulation from the stakeholders and policymakers point of view. Indeed, a method of such valuation is worth any academic effort.

7.8.1 Literature

Comprehensive gap analysis in literature is provided in section 2.9. The focus of this section specifically involves a review of systems thinking and dynamic modelling that have been reviewed in academic studies and theoretical discussions. The evidence available suggests that the discussion of systems dynamic modelling in infrastructure protection is very elementary. Similarly, the theoretical argument supporting existing studies are also outdated. There is, therefore, the need for academics, researchers and systems theorists to do more to bridge the existing gap.

7.8.2 Industry

This represents the requirements for the application of system dynamics in the context of a cybersecurity risk assessment. The industrial gap analysis provides the opportunity to assess the deployment of systems thinking approach in cyber infrastructure protection in order to gain an insight into the dynamic application at the industrial level. This is, however, dependent on the theoretical development that provides guidelines for development, deployment, adoption and use. The absence of guidelines is argued to be the primary reason behind the general lack of use of dynamic modelling in industrial risk assessment processes and for that matter cyber infrastructure protection.

The lack of use at the industrial level has been attributed to a number of factors and captured in literature. For example, Trochim et al identified eight different categories of challenges associated with systems dynamics implementation and the lack of use [168]. According to the authors, the categories of challenges include how to foster systems planning and evaluation, lack of awareness, lack of funding to implement systems dynamic projects, and the general lack of evidence to show the potential of systems approaches [168]. Other challenges include unavailability of new users, difficulties with implementing modelling project and limited support for system dynamic projects [163,171]. Furthermore, according to Linnéusson, the field of system dynamics has over the years produced quality results for practical use [102]. Notwithstanding, the lack of

theoretical frameworks to support how to implement dynamic projects has affected general acceptance and use [174]. This assertion is corroborated by Zock and Rautenberg who claim there is "no widely accepted and fully developed organizational intervention model for the use of the system dynamics methodology in an organizational context and also available in literature" [175].

Concluding, there is not enough evidence either in literature or in practice to suggest the immediate deployment and use of systems dynamic methods in infrastructure protection or in the general institutional risk assessment processes. Richmond argues that there is a long delay until the methodology can be fruitfully utilized in these disciplines [176]. This highlights improvement potentials in the concept: For the applications in infrastructure protection, the method acceptance could be aided by creating awareness, providing guidelines, and to support management to use the methodology. It is further argued that any proposed criteria supporting the systems dynamic method should include guidance on how to implement projects of dynamic nature.

7.9 Methodology Development

The analysis of data collected, the simulation results and the identified gap have necessitated the definition of a new criterion for methodology development. The methodology development is in line with the thesis' core objective that focuses on the development of a framework for assessing risks in critical cyber infrastructure systems. The aim of the new proposal is to bridge the gap between theory and practice. The guidelines as presented below look at the critical areas, which are useful for the development of the proposed framework. The approach can be divided into two procedures:

i. A systems dynamic risk assessment framework for critical cyber infrastructure protection and
ii. Detailed step-by-step instructions of use.

The aim of the first procedure is to provide ***guidelines*** to the user in the application of the framework in infrastructure protection. The second procedure provides the appropriate ***steps*** that need to be followed in the implementation of the framework.

7.9.1 Framework Development

The framework development is based on a model that was developed by Forrester [159]. The explanation of the stages in the framework is incorporated into the descriptions of the framework and discussed in the next section.

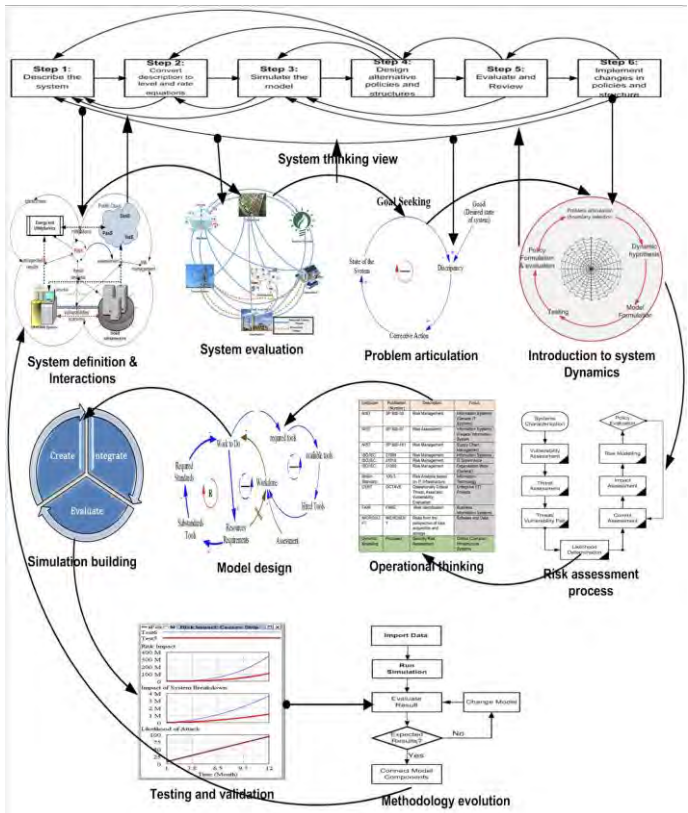


Figure 7- 11: System dynamics risk assessment framework

7.9.2 Description: Framework Constructs

Figure 7-11 is the annotated diagram of the proposed framework and its key constructs. Below is the description of the framework's construct:

1. *System thinking view:* this follows a proposition made by Forrester [159]. According to Forrester, *"system dynamics, systems thinking, and soft operations research aspire to the understanding and improvement of systems"* [159]. In its original work, *"the first step interprets the real world into descriptions"* [159]. The '*description'* provides the basis for the construction of model and simulation and provides the modeller with the opportunity to understand the dynamic behaviour of the system.

2. *System definition/interaction*: this defines the system to be assessed (and its subsystem). In this context, a system is characterized to reveal its identity, subsystems and characteristics, as well as their interrelations. This gives the assessor the opportunity to understand and acknowledge the problem at the start of the modelling process.

3. *System evaluation:* This sets up the time to assess the situational needs of the system and define its problem. It involves setting up a plan to define the statement of intent (objectives) that will characterize the model design. It is the stage that provides the opportunity to improve operational efficiency and effectiveness.

4. *Problem articulation:* At this stage, the system's problem is examined, including previous efforts that have been made to resolve it and the new proposals for its resolution. The aim is to understand the system's problem in order to diagnose the appropriateness of applying a system thinking approach. According to Forrester, it improves the idea of how to formalize a real-system into a model [163]. Furthermore, it is argued, *"the process of problem articulation impacts on model ownership"*, and for that matter, should be acknowledged explicitly so as to facilitate a successful

project [102].

5. *Introduction to system dynamics:* It is the basics of system thinking; describing the philosophy of feedbacks, causes and effects, and the building blocks of stocks and flows that are required for the modelling construction. This assists the modeller the opportunity to gain an understanding of the system [163]. Primary activities in this section include problem definition, dynamic hypothesis, model design, testing and policy formulation and evaluation [163].
6. Risk assessment process: this describes the key stages in the risk assessment process as proposed by the thesis. It is considered as the standard practice by which organizations operationalize privacy, security, and compliance with other policies to protect infrastructure systems against a loss.
7. *Operational thinking:* this involves formalizing the modelling process in order to represent the real system by the model design. The objective is to bring the model design in consonance to existing standards; making relevant the modelling process to the operational needs of the modeller.
8. *Model design:* this the formal process to start the model construction after the system has formally been analysed. It is the approach to understand the causal processes that shape the behaviour of the system and its subsystems [177].
9. *Simulations:* simulation uses data gathered to test modelling design; assessing if model design produces the expected outcome.
10. *Testing and validation:* This is to establish if a model's outcome (simulation results) is agreed by the modeller (and stakeholders). The testing guidelines must conform to the user requirements (captured during the requirements analysis stage).
11. Methodology evolution: this follows a feedback effect; i.e. the lessons learned and knowledge gained are documented to provide the basis for further assessment and system

improvement. A handbook of guidelines for using the framework must also contain both tacit and explicit knowledge to support method advancement.

7.10 Conclusions

Using Vensim PLE, this chapter has modelled and simulated risk assessment process in an interdependent system with the focus on critical energy infrastructure. The objective is to analyse systems' structural characteristics in order to observe the performances of their subsystems that make up the whole. The simulation results are based on identified problems, which were hypothesised and tested. The modelling development and simulation testing provide the foundation for the development of the thesis's proposed framework development.

The main idea with the framework development is to support the use of system dynamics (through system thinking) for institutional risk assessment. The development is based on the quest to establish the level of institutional support required to bridge the gap between literature (theory) and practice (industry). At its present stage, the framework has not been implemented and tested. To support its implementation and use, a handbook of guidelines is recommended.

Chapter 8: Conclusions and Future Scope

This chapter finalises the study. It begins with the summary of the thesis's findings then follows with the discussion of both theoretical and practical implications. It is concluded with the study's limitations and recommendations for future research scope.

"Problems are the results of past actions and are either eliminated by accurate measures or restrained by temporary solutions" [102]. Every research work sets out a mission to propose or to provide a solution to a problem defined by the researcher. The realization of the proposed solution (in theory or in practice) is the contribution to existing knowledge. The thesis has proposed a system dynamic modelling risk assessment framework from the lens of system thinking.

Systems dynamics is a methodology that uses the language of structural analysis and causes to understand systems' behaviour. While system thinking concept has been there for a relatively long time, its application in the area of infrastructure protection has not been well explored. And as established, none of the administrators, asset owners and staff interviewed as part of this study, indicated to have used or adopted a system thinking approach or a dynamic modelling as part of their risk management portfolios. Similarly, existing studies on the concept, appear to be outdated and less informational for the current discourse. Furthermore, current theories on the topic, have also failed to provide guidelines on their application. On this basis, the thesis's approach is novel; proposing a framework with guidelines to support the adopting of dynamic modelling through systems thinking in critical infrastructure protection.

From the thesis point of view, it sets out to explore the *"security risks in cloud computing (as cyber infrastructure setup) and its impact on interconnected critical infrastructure systems".* As established, cloud computing means different things to different people. In this thesis, an attempt has been made to define cloud computing for the purpose of academic discussion. As established, there has been a systematic

increase in cloud adoption among industrial controlled operators and systems administrators. And at the same time, greater integration of computing technologies and critical infrastructure systems. The thesis has looked at this convergence, specifically on infrastructural platforms in the power distribution sector with an emphasis on industrial controlled systems (SCADA). From the perspective of systems thinking, dynamic models were built together with simulations to demonstrate the impact of cyberattacks on the interdependent systems. For practical purpose, a dynamic modelling framework is developed and guidelines provided to support the implementation of the framework at the industrial level. The objective is to motivate both researchers and practitioners to apply a system thinking approach to critical infrastructure protection (both in theory and applied).

According to Stapelberg, the science of infrastructure interdependencies in complex systems is "*relatively immature*" in cybersecurity research [80]. Stapelberg argues further that "*developing a deeper understanding of such concept and their security implications will require a comprehensive research and development agenda, which encompass multiple disciplines ranging from engineering and complexity science to sociology, policy research and political science"* [80]. In this context, Stapelberg's claim has undoubtedly played a very significant role in framework development.

8.1 Summary of Findings

The primary objective of the study was to answer the question - *"what are the security risks in cloud computing (as a cyber-infrastructure) setup and the impact such risks have on interdependent critical infrastructure systems"?* Five major observations were made regarding infrastructure interdependencies, which were found to have influenced systems overall risk exposure and the corresponding risk impact.

The observations are:

i. Vulnerabilities inherent within the host as the independent system and ISC-SCADA as the dependent system

contributes to the systems' risk exposure.

ii. Critical infrastructure systems are under constant cyber attack due to the richness of the resources.

iii. Infrastructure interdependency increases systems complexity which then increases the rate of systems security risk exposure.

iv. The value of the system is statistically significant to the impact of a successful attack.

v. The presence (and absence of) security controls influence the rate of the likelihood of an attack.

One major challenge encountered in addressing these challenges was the method of identifying, clarifying and predicting interdependency induced complexities; this is where the thesis's approach is even more useful. An equally important discovery was the lack of an acceptable method to quantify the value of critical infrastructure systems as assets (and their criticality thereof). This makes the proposition and the development of new methodology more relevant.

Having considered how the thesis's results correspond to its objectives, the paragraphs below looks at how the thesis's questions have been answered.

Question 1: *What are the vulnerabilities, which are inherent in cyber infrastructure systems and the potential threats capable of exploiting these vulnerabilities?* The answer to the question is presented in chapter four; in this context, data (both primary and secondary) was collected, analyzed, results presented and explanation provided. In relations to the thesis's objectives, the outcome from this question was also used as the basis for the model design and the simulation procedure in chapter seven.

Question 2: *How to assess the interdependencies in critical infrastructure systems?* The answer to this question is captured in chapter five; in this context, Bendell model was used to compute the interdependency ratio between two interdependent infrastructure systems. The results obtained show that in an interconnected system, the behaviour of one system has a direct impact on other systems due to the feedback effect. In reference to the thesis objectives, the outcome from this question feeds into the modelling construction and

the simulation building.

Question 3: *How to capture and predict the complex behaviour of infrastructure interdependencies?* The answer to this question is captured in chapters six and seven. In this context, a model-based design was adopted to model infrastructure interdependencies. From that, structural analysis of interdependent systems was performed using causal loop diagrams. This helps to determine the causes and effects of system behaviour.

Question 4: How to assess cybersecurity risks in interdependent critical infrastructure systems? The answer to this question is represented by the development of the thesis's proposed systems dynamic modelling framework in chapter seven. It follows the gaps identified in the literature and in practice, and the subsequent development of models and simulations. To support the use of the framework, guidelines have been provided to support its implementation, especially at the industrial level. On this basis, it can be concluded that the thesis has sufficiently answered the key research questions. This does not necessarily mean, the thesis has addressed every concern it has raised due to the implications of other unidentified but relevant concerns the thesis might have failed to capture.

8.2 Theoretical Implications

The thesis presents multiple theoretical and practical implications from the application of systems thinking and dynamic modelling from the perspective of critical infrastructure protection. First, whilst existing studies on interdependency systems had focused on the system as in an individual entity, in this study, a system has been looked at as a unified entity. Thus, the thesis provides a better understanding of a system and its subsystems by way of explaining, the relationship between systems and their subsystems grounded on systems thinking (an extension to system theory).

Secondly, the study offers strong empirical evidence in the application of system theory in understanding the feedback effect on systems' performance. This is demonstrated in chapter seven, where system dynamic modelling is applied to show how actions of a

system's component can influence (either balancing or reinforcing) and impact changes in the interdependent systems. Similarly, infrastructure interdependency is defined as a system of systems; and argued that assessing their risks requires a causal understanding of their structural characteristics that make up the individual system. On this basis, it is claimed that one cannot (either in theory and in practice) deal with one component of a system without affecting the other part.

8.3 Practical Implications

This represents the requirements for the application of system dynamics in the context of a cybersecurity risk assessment. The gap analysis session provides the opportunity to assess the deployment of systems thinking approach in cyber infrastructure protection in order to gain an insight into the dynamic application at the industrial level. In this context, the significance of the thesis is with the proposal of a dynamic modelling methodology in the institutional risk assessment process, and the subsequent provision of guidelines to support the deployment and the use of the framework.

As established, infrastructure interdependencies increase the system's complexity, which subsequently intensifies the rate of systems security risk exposure. Thus, managers, administrators and asset owners must ensure that they understand the complexities induced by systems integration and develop new methods of capturing, simplifying and predicting the complex behaviour of infrastructure interdependencies. This will minimise the negative consequence introduced through systems integration. Furthermore, it is proposed here that, inasmuch it is necessary to strengthen systems' internal control mechanisms (both technical and operational), efforts must also be made to observe, analyse and manage systems' exogenous factors (such as security awareness programmes, training, investment in countermeasures, regulatory policies, government interventions, diligence in SLA, etc.) which are external to the systems but impact system's overall performance.

At the industrial level, the objective of the thesis is to produce results, which fill the existing knowledge gap and industrial needs. As

enumerated in the previous chapter, there are many challenges, which hinder the use of a system thinking approach at the industrial level. What is even more challenging is lack of understanding of system thinking approach due to insufficient guidelines from theories as well as lack of documentation on existing systems dynamic projects; offering little understanding to potential adopters. It is believed, the thesis's content and approach provide a user-friendly solution to industrial adopters.

8.4 Study Limitations

One major limitation of the study was the difficulty in acquiring primary data on ICS-SCADA systems in the assessment of the system's pre-and post-integration performances. Future studies should consider addressing this challenge.

Secondly, due to perceived security concerns and very restricted access management policies in most of the environments visited, there was a general reluctance by facility administrators and infrastructure managers to share critical security information such as log files, historic breakdown records, impact assessment reviews, control policies, vulnerability checklists, etc. For this reason, some of the analysis presented in the work were based on secondary data. For example, the entire data on web-based vulnerabilities were collected from secondary sources. While there is no doubt of the sources of the secondary data, using primary data and running live tests on controlled systems is believed would have provided better results.

One of the significant aspects of this study is the construction of the models and simulations in analysing security risks in critical infrastructure systems. As indicated earlier, two factors were observed in the assessment process: the impact of interdependency induced complexities as well as the economic value of systems resources. These observations need to be tested on a specific technology to make the findings practically significant. Future studies can test the approach on a specific technology to verify and validate the findings. Besides, because the cost estimation method that the thesis adopted to estimate the value of critical infrastructure resources was for the purpose of quantification; they are not reflective

of real market conditions. Neither did the thesis considered current or future economic conditions of the systems' resources. For practical applications, it is recommended that a proper costing model should be developed so that infrastructure cost assessments are reflective of real economic conditions (e.g. demand and supply).

Lastly, while the focus of the study was on the controlled technologies supporting the energy sector, the interdependency approach was specifically limited to the SCADA system. In a controlled environment, the performance of energy generation (upstream), transmission (midstream) and distribution (downstream) do not depend solely on SCADA as this study has suggested. Other supporting technologies such as HMI, SIS, PLC, VFD, DCS, ERP, SAP, etc., are embodiments of industrial control systems innovation development that this study did not consider. Future studies can consider these technologies and other integration factors, which can directly/indirectly influence the performance of energy generation, transmission and distribution.

8.5 General Considerations

Nations (and its economies) run on critical infrastructure services. These services include energy (power, oil and gas), utilities (water and sewerage), transportation and IT systems, etc. Modern critical infrastructure systems depend highly on Operational and Informational technologies. The failure and the subsequent impact of infrastructure failure could lead to serious environmental reactions and some cases the threat of human life. There is no doubt protecting critical infrastructure systems is a significant exercise for infrastructure sustainability, reliability and to ensure operational efficiencies. This thesis has shown that critical infrastructure systems face constant threats from both internal and external adversaries. Furthermore, integrating information and communication technologies with critical infrastructure systems structurally creates infrastructure interdependencies, which makes systems more complex in terms of design, operation and management. The complexity adds to the difficulty of understanding these systems, at the same time increasing their risk exposure. While systems owners and administrators in most cases provide control mechanisms to

protect systems against unintended consequences, existing methods have proven to be inadequate in addressing various risks specific to critical infrastructure systems.

It has also been established that the integration of network technologies with critical infrastructure systems has made the later more efficient leading to improvement in the overall operational performance and greater output. Nonetheless, it is also important that appropriate security assessment methodologies and control strategies are put in place to ensure systems protection, safety, availability and reliability. Over the years, there has been a sturdy increase in studies which seek out methods of assessing risks in critical infrastructure systems [134]. However, the advances in information and communication technologies, the emergence of new threats landscape, and advancement in the structural composition of critical infrastructure systems have increased systems complexities, leading to unpredictable behaviour of these infrastructure systems.

8.6 Future Research Scope

The application of system dynamics modelling in this study has set the stage for future research development focusing on providing a better understanding of interdependent critical infrastructure systems. While the study has examined infrastructure interdependencies with emphasis on industrial control systems, it will be interesting to extend the approach to other critical infrastructure systems such as transportation, water supply and sewerage systems. Furthermore, the study's approach has focused primarily on risk assessment, it makes a good policy case if future studies can extend the concept to include risk communication and implementation, in order to gain a holistic understanding of managing risks associated with interdependent critical infrastructure systems.

The modelling and simulations as developed in the study were not applied to a specific technology, it will be practically useful if the concept could be applied to a specific technology to assess how the method and results generated represent the real-world situation they were purported to represent. While mathematical modelling and simulations have so far failed to predict the motive behind threat

actors; one may ask why someone would attack systems which consequently lead to a loss of life and significant damage to social systems. Behavioural science is an obvious approach to address this concern. This is considered a psychological cyber-warfare against critical infrastructure systems, an area most assessment models, methods and studies have so far failed to consider.

Finally, the thesis provides several theoretical and practical considerations, offering a better understanding of security risks associated with interdependent critical infrastructure systems. It has also opened up some grey areas in the context of infrastructure interdependencies, which is worth further research.

References

[1] J. ROBLES and T. Kim, "Architecture of wireless supervisory control and data acquisition system," *Advances in Computational Intelligence, Man-Machine Systems and Cybernetics, Venezuela*, vol. 2, no. 3, pp. 241–244, 2010.

[2] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems, IEEE*, vol. 21, no. 6, pp. 11–25, 2001.

[3] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly*, vol. 27, no. 3, pp. 245–253, 2010.

[4] B. Obama, "Improving Critical Infrastructure Cybersecurity," The White House, Office of the Press Secretary, U.S.A, Press Release - An Executive Order, Feb. 2013.

[5] P. Chen, C. Scown, H. S. Matthews, J. H. Garrett Jr, and C. Hendrickson, "Managing critical infrastructure interdependence through economic input-output methods," *Journal of Infrastructure Systems*, vol. 15, no. 3, pp. 200–210, 2009.

[6] C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt, and K. Wilhoit, *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*. McGraw-Hill, Inc., 2016.

[7] J. P. Peerenboom and R. E. Fisher, "Analyzing cross-sector interdependencies," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 2007, pp. 112–112.

[8] S. Tweneboah-Koduah, A. K. Tsetse, J. Azasoo, and B. Endicott-Popovsky, "Evaluation of Cybersecurity Threats on Smart Metering System," in *Information Technology-New Generations*, Springer, 2018, pp. 199–207.

[9] J. Flum and M. Grohe, *Parameterized complexity theory*. Springer Science & Business Media, 2006.

[10] K. G. I. Energy, "Energy at Risk," KPMG Global Energy, Singapore, Study Report, 2013.

[11] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 244–249.

[12] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*, 2009, pp. 1–8.

[13] D. L. Kauffman, *Systems one: An introduction to systems thinking*. Future Systems Minneapolis, MN, 1980.

[14] S. Tweneboah-Koduah and W. J. Buchanan, "Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study," *The Computer Journal*, vol. 61, 2018, doi: 10.1093/comjnl/bxy002.

[15] M. Talabis and J. Martin, *Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis*. Newnes, 2012.

[16] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. risk management guide for information technology systems," 2002.

[17] M. Crouhy, D. Galai, and R. Mark, *The essentials of risk management*, vol. 1. McGraw-Hill New York, 2006.

[18] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk analysis*, vol. 1, no. 1, pp. 11–27, 1981.

[19] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *International journal of Internet and enterprise management*, vol. 6, no. 4, pp. 279–314, 2010.

[20] W. Pieters, "The (social) construction of information security," *The Information Society*, vol. 27, no. 5, pp. 326–335, 2011.

[21] N. Van Deursen, W. J. Buchanan, and A. Duff, "Monitoring information security risks within health care," *computers & security*, vol. 37, pp. 31–45, 2013.

[22] E. Borodzicz, *Risk, crisis and security management*. Wiley, 2005.

[23] J. Talbot and M. Jakeman, *Security Risk Management; Body of Knowledge*. New Jersey, USA: John Wiley & Sons, 2009.

[24] G. Manunta, "Defining security," *Diogenes Paper*, no. 1, pp. 48–52, 2000.

[25] B. S. Kaliski Jr and W. Pauley, "Toward Risk Assessment as a Service in Cloud Environments.," *HotCloud*, vol. 10, p. 13, 2010.

[26] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 1328–1334.

[27] W. P. Schuetze, "What is an Asset?," *Accounting Horizons*, vol. 7, no. 3, p. 66, 1993.

[28] W. Ozier, "A framework for an automated risk assessment tool," *Retrieved January*, vol. 25, p. 2007, 1999.

[29] S. Henderson, G. Peirson, K. Herbohn, T. Artiach, and B. Howieson, *Issues in financial accounting*. Pearson Higher Education AU, 2013.

[30] G. J. Touhill and J. C. Touhill, *Cybersecurity for Executives, A Practical Approach*. New Jersey, USA: John Wiley & Sons, 2014.

[31] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*, 2011, p. 12.

[32] Y.-M. Wei, Y. Fan, C. Lu, and H.-T. Tsai, "The assessment of vulnerability to natural disasters in China by using the DEA method," *Environmental Impact Assessment Review*, vol. 24, no. 4, pp. 427–439, 2004.

[33] J. Johansson, H. Hassel, and A. Cedergren, "Vulnerability analysis of interdependent critical infrastructures: case study

of the Swedish railway system," *International journal of critical infrastructures*, vol. 7, no. 4, pp. 289–316, 2011.

[34] J. Johansson, "Risk and vulnerability analysis of interdependent technical infrastructures," *Lund University, Dept. of Measurement Technology and Industrial Electrical Engineering*, 2010.

[35] G. E. Apostolakis and D. M. Lemon, "A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism," *Risk Analysis*, vol. 25, no. 2, pp. 361–376, 2005.

[36] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Fifth Edition. Canada: Course Technology, 2014.

[37] J. Miller, *Risk management for your web site. International risk management institute expert commentary*. 2002.

[38] C. Bronk and E. Tikk-Ringas, "The cyber attack on Saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81–96, 2013.

[39] "BBC NEWS | Europe | Danish capital loses power." [Online]. Available: http://news.bbc.co.uk/2/hi/europe/3132332.stm. [Accessed: 17-Jan-2017].

[40] N. Gibbs, "Blackout '03: Lights Out," *Time*, 25-Aug-2003.

[41] H. Hassel, *Risk and vulnerability analysis in society's proactive emergency management: Developing methods and improving practices*. Lund University, 2010.

[42] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific Cloud Computing: Early Definition and Experience.," in *HPCC*, 2008, vol. 8, pp. 825–830.

[43] K. Jamsa, *Cloud computing*. Jones & Bartlett Publishers, 2013.

[44] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2008.

[45] D. C. Wyld, "THE cloudy future of government IT: Cloud computing and the public sector around the world," *International Journal of Web & Semantic Technology*, vol. 1, no. 1, pp. 1–20, 2010.

[46] D. C. Wyld, *Moving to the cloud: An introduction to cloud computing in government*. IBM Center for the Business of Government, 2009.

[47] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The characteristics of cloud computing," in *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*, 2010, pp. 275–279.

[48] D. Hilley, "Cloud computing: A taxonomy of platform and infrastructure-level offerings," *Georgia Institute of Technology, Tech. Rep. GIT-CERCS-09-13*, 2009.

[49] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation computer systems*, vol. 25, no. 6, pp. 599–616, 2009.

[50] L. Youseff, M. Butrico, and D. Da Silva, "Toward a unified ontology of cloud computing," in *Grid Computing Environments Workshop, 2008. GCE'08*, 2008, pp. 1–10.

[51] M. A. Bamiah and S. N. Brohi, "Exploring the Cloud Deployment and Service Delivery Models," *International Journal of Research and Reviews in Information Sciences (IJRRIS)*, vol. 1, no. 3, 2011.

[52] T. Dillon, C. Wu, and E. Chang, "Cloud computing: issues and challenges," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 2010, pp. 27–33.

[53] J. Dean and S. Ghemawat, "MapReduce: simplified data processing on large clusters," *Communications of the ACM*, vol. 51, no. 1, pp. 107–113, 2008.

[54] S. Ghemawat, H. Gobioff, and S.-T. Leung, "The Google file system," in *ACM SIGOPS Operating Systems Review*, 2003, vol. 37, pp. 29–43.

[55] N. McKeown *et al.*, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[56] A. M. Azab, P. Ning, and X. Zhang, "Sice: a hardware-level strongly isolated computing environment for x86 multi-core

platforms," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 375–388.

[57] R. L. Krutz and R. Dean Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, 2010.

[58] D. J. Abadi, "Data Management in the Cloud: Limitations and Opportunities.," *IEEE Data Eng. Bull.*, vol. 32, no. 1, pp. 3–12, 2009.

[59] D. Perez-Botero, J. Szefer, and R. B. Lee, "Characterizing hypervisor vulnerabilities in cloud computing servers," in *Proceedings of the 2013 international workshop on Security in cloud computing*, 2013, pp. 3–10.

[60] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, First. Califonia, United States: O'Reilly Media, Inc, 2009.

[61] S. Vogl, "Secure hypervisors," in *Proceedings of 12th International Conference on Enterprise Information System*, 2010.

[62] R. Wojtczuk and J. Rutkowska, "Attacking Intel Trusted Execution Technology," Invisible Things Lab, Washington, DC, USA, Feb. 2009.

[63] "HyperVM - WHMCS Documentation." .

[64] B. D. Payne, M. D. P. De Carbone, and W. Lee, "Secure and flexible monitoring of virtual machines," in *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, 2007, pp. 385–397.

[65] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," in *Informatics and Systems (INFOS), 2010 The 7th International Conference on*, 2010, pp. 1–8.

[66] J. Kirch, "Virtual machine security guidelines," *The Center for Internet Security*, 2007.

[67] D. E. Jensen, "System-wide Performance Analysis for Virtualization," 2014.

[68] "OWASP Top 10 2013 vulnerabilities." [Online]. Available: https://www.ibm.com/developerworks/library/se-owasp-top10/. [Accessed: 20-Jan-2017].

[69] "IDC Cloud IT Infrastructure Forcast," *www.idc.com*. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS25946315. [Accessed: 20-Jan-2017].

[70] M. De Bruijne and M. Van Eeten, "Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment," *Journal of contingencies and crisis management*, vol. 15, no. 1, pp. 18–29, 2007.

[71] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems, IEEE*, vol. 21, no. 6, pp. 11–25, 2001.

[72] R. G. Little, "Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructures," *Journal of Urban Technology*, vol. 9, no. 1, pp. 109–123, 2002.

[73] R. Zimmerman, "Social implications of infrastructure network interactions," *Journal of Urban Technology*, vol. 8, no. 3, pp. 97–119, 2001.

[74] Y. Y. Haimes and T. Longstaff, "The role of risk analysis in the protection of critical infrastructures against terrorism," *Risk Analysis*, vol. 22, no. 3, pp. 439–444, 2002.

[75] Y. Y. Haimes and T. Longstaff, "The role of risk analysis in the protection of critical infrastructures against terrorism," *Risk Analysis*, vol. 22, no. 3, pp. 439–444, 2002.

[76] I. Eusgeld and C. Nan, "Creating a simulation environment for critical infrastructure interdependencies study," in *Industrial Engineering and Engineering Management, 2009. IEEM 2009. IEEE International Conference on*, 2009, pp. 2104–2108.

[77] A. Polyakov and M. Geli, "SAP Cybersecurity for Oil and Gas," ERPScan, Califonia, USA, Jun. 2012.

[78] M. Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*. Macmillan, 1995.

[79] S. Chan, "Complex adaptive systems," in *Research seminar in engineering systems*, 2001, vol. 31.

[80] R. F. Stapelberg, "Infrastructure systems interdependencies and risk informed decision making (RIDM): impact scenario analysis of infrastructure risks induced by natural,

technological and intentional hazards," *Journal of Systemics, Cybernetics and Informatics*, vol. 6, no. 5, pp. 21–27, 2008.

[81] S. H. Strogatz, "Exploring complex networks," *Nature*, vol. 410, no. 6825, pp. 268–276, 2001.

[82] P. Anderson, "Perspective: Complexity theory and organization science," *Organization science*, vol. 10, no. 3, pp. 216–232, 1999.

[83] S. C. Patel, G. D. Bhatt, and J. H. Graham, "Improving the cyber security of SCADA communication networks," *Communications of the ACM*, vol. 52, no. 7, pp. 139–142, 2009.

[84] N. Falliere, "Stuxnet introduces the first known rootkit for industrial control systems," *Published online at http://www. symantec. com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices. Last accessed on February*, vol. 10, 2011.

[85] A. Holla, "Cyber Risk for Energy/Power Industry," Aon Risk Solutions, Jan. 2016.

[86] Gemalto, "Data Breach Database," *Breach Level Index*. [Online]. Available: http://breachlevelindex.com. [Accessed: 05-Jul-2017].

[87] J. D. Fernandez and A. E. Fernandez, "SCADA systems: vulnerabilities and remediation," *Journal of Computing Sciences in Colleges*, vol. 20, no. 4, pp. 160–168, 2005.

[88] W. R. Ashby and others, *An introduction to cybernetics*, vol. 2. Chapman & Hall London, 1956.

[89] W. Buckley, "Sociology and modern systems theory.," 1967.

[90] B. D. Anderson and S. Vongpanitlerd, *Network analysis and synthesis: a modern systems theory approach*. Courier Dover Publications, 2006.

[91] E. Laszlo and A. Laszlo, "The contribution of the systems sciences to the humanities," *Systems Research and Behavioral Science*, vol. 14, no. 1, pp. 5–19, 1997.

[92] O. I. Elgerd and H. H. Happ, "Electric energy systems theory: an introduction," *Systems, Man and Cybernetics, IEEE Transactions on*, vol. 2, no. 2, 1972.

[93] D. H. Ford and R. M. Lerner, *Developmental systems theory: An integrative approach.* Sage Publications, Inc, 1992.

[94] P. M. Senge, *The fifth discipline: The art and practice of the learning organization*. Random House LLC, 2006.

[95] J. W. Forrester, "Designing the future," *Universidad de Sevilla*, vol. 15, 1998.

[96] F. E. Kast and J. E. Rosenzweig, "General systems theory: Applications for organization and management," *Academy of management journal*, vol. 15, no. 4, pp. 447–465, 1972.

[97] A. Laszlo and S. Krippner, "Systems theories: Their origins, foundations, and development," *ADVANCES IN PSYCHOLOGY-AMSTERDAM-*, vol. 126, pp. 47–76, 1998.

[98] P. P.-S. Chen, "The entity-relationship model—toward a unified view of data," *ACM Transactions on Database Systems (TODS)*, vol. 1, no. 1, pp. 9–36, 1976.

[99] R. L. Ackoff, "The art and science of mess management," *Interfaces*, vol. 11, no. 1, pp. 20–26, 1981.

[100] J. D. Sterman, "All models are wrong: reflections on becoming a systems scientist," *System Dynamics Review*, vol. 18, no. 4, pp. 501–531, 2002.

[101] P. B. Checkland, "Soft systems methodology," *Human systems management*, vol. 8, no. 4, pp. 273–289, 1989.

[102] G. Linnéusson, "On system dynamics as an approach for manufacturing systems development," PhD Thesis, Chalmers University of Technology, 2009.

[103] R. Dodder and R. Dare, "Complex adaptive systems and complexity theory: inter-related knowledge domains," in *ESD. 83: Research Seminar in Engineering Systems*, 2000.

[104] M. M. Waldrop and J. Gleick, "Teisman and Klijn," *info London: Viking, 1992*, 1992.

[105] S. F. Railsback, "Concepts from complex adaptive systems as a framework for individual-based modelling," *Ecological modelling*, vol. 139, no. 1, pp. 47–62, 2001.

[106] M. Couture and D. Valcartier, "Complexity and chaos-state-of-the-art; overview of theoretical concepts," *Minister of National Defence, Canada*, 2007.

[107] C. Mesjasz, "Complexity Studies and Security in the Complex World: An Epistemological Framework of Analysis," in *Unifying Themes in Complex Systems*, Springer, 2010, pp. 170–177.

[108] J. W. Forrester, "Lessons from system dynamics modeling," *System Dynamics Review*, vol. 3, no. 2, pp. 136–149, 1987.
[109] J. W. Forrester, "Industrial dynamics-after the first decade," *Management Science*, vol. 14, no. 7, pp. 398–415, 1968.
[110] G. R. Teisman and E.-H. Klijn, "Daft, Murphy, and Willmott 2010," *Public management review*, vol. 10, no. 3, pp. 287–297, 2008.
[111] S. Walby, "Complexity theory, systems theory, and multiple intersecting social inequalities," *Philosophy of the social sciences*, vol. 37, no. 4, pp. 449–470, 2007.
[112] H. A. Simon, *The sciences of the artificial*. MIT press, 2019.
[113] G. R. Teisman and E.-H. Klijn, "Complexity theory and public management: An introduction," *Public management review*, vol. 10, no. 3, pp. 287–297, 2008.
[114] J. Galbraith, "Designing complex organizations," 1973.
[115] J. Balthrop, S. Forrest, M. E. Newman, and M. M. Williamson, "Technological networks and the spread of computer viruses," *Science*, vol. 304, no. 5670, pp. 527–529, 2004.
[116] I. B. Utne, P. Hokstad, and J. Vatn, "A method for risk modeling of interdependencies in critical infrastructures," *Reliability Engineering & System Safety*, vol. 96, no. 6, pp. 671–678, 2011.
[117] G. H. Kjølle, I. B. Utne, and O. Gjerde, "Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies," *Reliability Engineering & System Safety*, vol. 105, pp. 80–89, 2012.
[118] A. Rees, "Information networks in labor markets," *The American Economic Review*, vol. 56, no. 1/2, pp. 559–566, 1966.
[119] Y.-B. Xie, W.-X. Wang, and B.-H. Wang, "Modeling the coevolution of topology and traffic on weighted technological networks," *Physical Review E*, vol. 75, no. 2, p. 026111, 2007.
[120] J. Johansson, *Risk and Vulnerability Analysis of Large Scale Technical Infrastructures-Electrical Distribution Systems*, vol. 1053. Dept. of Industrial Electrical Engineering and Automation, Lund Institute of Technology, 2007.

[121] E. F. Bedell, *Computer Solution: Strategies for Success in the Information Age*. McGraw-Hill, Inc., 1984.
[122] M. M. Lankhorst, D. A. Quartel, and M. W. Steen, "Architecture-Based IT Portfolio Valuation," in *Practice-Driven Research on Enterprise Transformation*, Springer, 2010, pp. 78–106.
[123] B. L. Berg and H. Lune, *Quantitative Research Methods for the Social Sciencens*, Eight. Pearson, 2012.
[124] R. K. Yin, *Applications of case study research*. Sage, 2011.
[125] A. Pinsonneault and K. L. Kraemer, "Survey research methodology in management information systems: an assessment," *Journal of management information systems*, pp. 75–105, 1993.
[126] P. G. Neumann, "The Risks Digest," *The Risks Digest*.
[127] "The Repository of Industrial Security Incidents." [Online]. Available: http://www.risidata.com/About. [Accessed: 23-Jan-2017].
[128] "National SCADA Test Bed | Department of Energy." .
[129] R. Ross *et al.*, "Recommended Security Controls for Federal Information Systems," National Institute of Standards and Technology, Gaithersburg, USA, Jun. 2005.
[130] "SANS Institute - CIS Critical Security Controls." [Online]. Available: https://www.sans.org/critical-security-controls. [Accessed: 23-Jan-2017].
[131] J. Treweek, *Ecological impact assessment*. John Wiley & Sons, 2009.
[132] M. Pagani, *Encyclopedia of Multimedia Technology and Networking*, vol. 3. IGI Global, 2008.
[133] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *Proceedings of the 2001 workshop on New security paradigms*, 2001, pp. 97–104.
[134] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in *System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on*, 2004, pp. 8–pp.
[135] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability

analysis," *Reliability Engineering & System Safety*, vol. 95, no. 12, pp. 1335–1344, 2010.

[136] S. Wang, L. Hong, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems: A methodological framework," *Physica A: Statistical Mechanics and its applications*, vol. 391, no. 11, pp. 3323–3335, 2012.

[137] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems, IEEE*, vol. 21, no. 6, pp. 11–25, 2001.

[138] H. M. Abdur Rahman, "Modelling and simulation of interdependencies between the communication and information technology infrastructure and other critical infrastructures," 2009.

[139] P. Monga, "A system dynamics model of the development of new technologies for ship systems," 2001.

[140] "CVE - Common Vulnerabilities and Exposures (CVE)." .

[141] "NVD - Search." .

[142] NERC Staff, "Reliability Considerations from the Integration of Smart Grid," North American Electric Reliability Corporation, New Jersey, USA, Dec. 2010.

[143] "NORS," *Federal Communications Commission*, 03-Dec-2015. [Online]. Available: https://www.fcc.gov/network-outage-reporting-system-nors. [Accessed: 24-Jan-2017].

[144] Idaho National Laboratory, "Vulnerability Analysis of Energy Delivery Control Systems," Idaho, USA, State Sponsored INL/EXT-10-18381, Sep. 2011.

[145] INL, "Vulnerability Analysis of Energy Delivery Control Systems," U. S. Department of Energy, Idaho, USA, State Sponsored, Sep. 2011.

[146] FIRST Global Initiative, "CVSS Specification Document," FIRST.org Inc, 2015.

[147] "World Energy Council," World Energy Counci, London, UK, 2016.

[148] M. Buschle and D. Quartel, "Extending the method of Bedell for Enterprise Architecture Valuation," in *Enterprise Distributed Object Computing Conference Workshops*

(EDOCW), 2011 15th IEEE International, 2011, pp. 370–379.

[149] I. Eusgeld, C. Nan, and S. Dietz, "'System-of-systems' approach for interdependent critical infrastructures," *Reliability Engineering & System Safety*, vol. 96, no. 6, pp. 679–686, 2011.

[150] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. Chen, "Cyber security and privacy issues in smart grids," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 4, pp. 981–997, 2012.

[151] J. D. Sterman, "System Dynamics: systems thinking and modeling for a complex world," in *Proceedings of the ESD Internal Symposium*, 2002.

[152] "Exponential growth," *Wikipedia*. 06-Nov-2018.

[153] G. P. Richardson and A. I. Pugh III, *Introduction to system dynamics modeling with DYNAMO*. Productivity Press Inc., 1981.

[154] A. T. Bahill and B. Gissing, "Re-evaluating systems engineering concepts using systems thinking," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 28, no. 4, pp. 516–527, 1998.

[155] D. H. Kim and P. M. Senge, "Putting systems thinking into practice," *System Dynamics Review*, vol. 10, no. 2–3, pp. 277–290, 1994.

[156] M. Kunc, "System Dynamics: A Behavioral Modeling Method," in *Proceedings of the 2016 Winter Simulation Conference*, Piscataway, NJ, USA, 2016, pp. 53–64.

[157] F. Aqlan and S. S. Lam, "Supply chain risk modelling and mitigation," *International Journal of Production Research*, vol. 53, no. 18, pp. 5640–5656, 2015.

[158] J. P. Torres, "System Dynamics Review and publications 1985–2017: analysis, synthesis and contributions," *System Dynamics Review*, vol. 35, no. 2, pp. 160–176, 2019, doi: 10.1002/sdr.1628.

[159] J. W. Forrester, "Industrial dynamics," *Journal of the Operational Research Society*, vol. 48, no. 10, pp. 1037–1041, 1997.

[160] Y. Barlas, "Formal aspects of model validity and validation in system dynamics," *System Dynamics Review*, vol. 12, no.

3, pp. 183–210, 1996, doi: 10.1002/(SICI)1099-1727(199623)12:3<183::AID-SDR103>3.0.CO;2-4.

[161] D. Helbing, "Globally networked risks and how to respond," *Nature*, vol. 497, no. 7447, pp. 51–59, 2013.

[162] H. Kloos, H. Baker, and T. Waltzer, "A mind with a mind of its own: How complexity theory can inform early science pedagogy," *Educational Psychology Review*, pp. 1–18, 2019.

[163] J. W. Forrester, "System dynamics, systems thinking, and soft OR," *System Dynamics Review*, vol. 10, no. 2–3, pp. 245–256, 1994.

[164] R. Montasari, A. Hosseinian-Far, and R. Hill, "Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments," in *Cyber Criminology*, Springer, 2018, pp. 71–93.

[165] S. Mori and A. Goto, "Review of National Cybersecurity Strategy Case Study: UK," p. 8, 2018.

[166] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *International Journal of Information Management*, vol. 45, pp. 13–24, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[167] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Government Information Quarterly*, vol. 34, no. 1, pp. 1–7, Jan. 2017, doi: 10.1016/j.giq.2017.02.007.

[168] W. M. Trochim, D. A. Cabrera, B. Milstein, R. S. Gallagher, and S. J. Leischow, "Practical Challenges of Systems Thinking and Modeling in Public Health," *Am J Public Health*, vol. 96, no. 3, pp. 538–546, Mar. 2006, doi: 10.2105/AJPH.2005.066001.

[169] B. Richmond, "Systems thinking/system dynamics: let's just get on with it," *System Dynamics Review*, vol. 10, no. 2–3, pp. 135–157, 1994.

[170] G. P. Richardson, "Problems for the future of system dynamics," *System Dynamics Review: The Journal of the System Dynamics Society*, vol. 12, no. 2, pp. 141–157, 1996.

[171] E. A. Rouwette and J. A. Vennix, "System dynamics and organizational interventions," *Systems Research and Behavioral Science: The Official Journal of the International Federation for Systems Research*, vol. 23, no. 4, pp. 451–466, 2006.

[172] P. S. Hovmand, "Group model building and community-based system dynamics process," in *Community Based System Dynamics*, Springer, 2014, pp. 17–30.

[173] K. A. Stave, "A system dynamics model to facilitate public understanding of water management options in Las Vegas, Nevada," *Journal of Environmental Management*, vol. 67, no. 4, pp. 303–313, 2003.

[174] A. Größler, "System dynamics projects that failed to make an impact," *System Dynamics Review*, vol. 23, no. 4, pp. 437–452, 2007.

[175] A. Zock and M. Rautenberg, "A critical review of the use of system dynamics for organizational consultation projects," in *Proceedings of the 22nd International Conference of the System Dynamics Society, Oxford*, 2004.

[176] B. Richmond, "Systems thinking/system dynamics: let's just get on with it," *System Dynamics Review*, vol. 10, no. 2–3, pp. 135–157, 1994.

[177] B. Hannon and M. Ruth, "Modeling Dynamic Biological Systems," in *Modeling Dynamic Biological Systems*, B. Hannon and M. Ruth, Eds. Cham: Springer International Publishing, 2014, pp. 3–28.

[178] R. F. Stapelberg, "Infrastructure systems interdependencies and risk informed decision making (RIDM): impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards," *Journal of systemics, Cybernetics and Informatics*, vol. 6, no. 5, pp. 21–27, 2008.

Appendix

Appendix 1: Assessment - Questionnaire

The purpose of this survey is to seek your expert opinion to assist research student in understanding cybersecurity and related activities in an industrial control environment with specific reference to IT resources. This is a simple checklist designed to identify and document the existence and status for a recommended basic set of cybersecurity activities as well as countermeasures in a controlled environment. Countermeasures are designed to reduce and/or eliminate the identified Threat/vulnerabilities that place an organization at risk.

Author: Samuel Tweneboah-Koduah (samueltk@uw.edu)
Advisor: Professor Ramjee Prasad (Ph.D.)
Interest: Doctoral (Ph.D) Dissertation
Thesis: Risk Assessment of Cyber Infrastructure and Interdependent Systems: A Dynamic Modelling Approach
Sponsor: Doctoral School, Department of Business Development and Technology, Aarhus University

General Security Assessment (For literature)

1. Which of the following security risk management standards has/have your organization adopted? (Tick all that apply)
    a. NIST-SP800-53
    b. ISO/IEC 27005:2003
    c. BS-77-2006
    d. OCTAVE
    e. FAIR
    f. Microsoft
    g. Others
2. Which of the following do you consider to be the greatest challenge facing your organization in ensuring security of your IT systems

   a. Evolving Technical Threats
   b. Employees' attitude
   c. Lack of funding for security control programs
   d. Lack of understanding at the C-Suite Level
   e. Inadequate review of risk prior to introduction of new technologies
3. Which of the following threat actors have exploited your environment in the past 12 months (Tick all that apply)
   a. Cybercriminals (Hackers)
   b. Hacktivists
   c. APT – State sponsored threats
   d. Malicious Insider
   e. Malicious Outsider
4. Approximately how many security incidents (SI) have you experience in your environment in the past 12 months?
   a. SI <=9
   b. 10 <=SI<=49
   c. 50 <= SI <= 99
   d. 100 <= SI <= 500
   e. SI = 500
5. What was the main method (s) used by the attackers?
   a. Hacking
   b. Physhing
   c. Exploits
   d. Privilage Abuse
   e. DoS/DDoS
   f. Malware
   g. Social Engineering
   h. SQL Injection
   i. Other
6. What do you consider to be the attackers motivation?
   a. Financial gains
   b. Destruction of IT equipment
   c. Destruction of critical services
   d. IP Theft
   e. Theft of classified Information
   f. Theft of PII
   g. Theft of mobile devices

7. How was your organization impacted by the security incidents (Tick all that apply)
    a. Complete system shut down
    b. Unavailability of some major services (e.g. email)
    c. Theft of IP and other corporate secretes
    d. Loss of customers
    e. Brand reputation compromised
    f. Financial losses (from sales and services)
    g. Financial losses (legal/regulatory/compliance charges)
8. Do you have controls against the following system vulnerabilities (Tick to signify Yes or leave blank to signify No)
    a. DDoS/DoS
    b. Code execution
    c. Buffer Overflow
    d. Memory corruption
    e. XSS
    f. Improper Access Control (Authorization)
    g. HTTP Traverse Splitting
    h. ICS Data Command Message Manipulation and Injection
    i. SQL Injection
    j. Unprotect Transport of ICS Application Credentials
    k. Directory Traversal
9. Do you have controls against the following Threat actors (Tick to signify Yes or leave blank to signify No)
    a. Bot-Network
    b. Malicious Insider
    c. Data corruption
    d. Insecure endpoints
    e. Suspected Nation-State
    f. Insecure Web Applications
    g. We-based Attack
    h. Malware (Virus, Trojan Horse, Worms)
    i. Insecure Smart Meters
    j. Phishers, Spyware and Spammers

   k. Espionage
10. Which of the following technical control measures do you have in place (Tick all that apply)?
    a. Firewalls, IDS/IPS
    b. Network/Remote Control Monitoring Systems
    c. Secure Network Transmission Control Systems
    d. Secure Remote Access (VPN)
    e. Data Encryption Systems
    f. Anti-Virus
    g. Other
11. Which of the following security controls you plan to deploy in the next 12 months (Check all that apply)?
    a. Firewalls
    b. Vulnerability scanning tools
    c. Enterprise Baseline Security Analyzers
    d. Automated Account Provisioning/De-provisioning
    e. IDS/IPS scanning tools
    f. Enterprise content management tools
    g. Code Analysis Tools
    h. Secure Access-Control Measure
    i. Behavioral Profiling and Monitoring (Background Checks)
    j. Others
12. Do you test your security controls?
    a. No
    b. No, but we are planning to do so
    c. No, but are developing some tests
    d. Yes, periodically (at least once a year)
    e. Yes, routinely (at least once every 3 months)
13. How effective are your security controls?
    a. Somewhat effective
    b. Average and predominantly reactive
    c. Good
    d. Very effective
14. Has your organization looked at cybersecurity insurance as a mechanism to cover cyberattacks, business interruptions, data theft, etc.?

a. Yes
b. No
c. We do not feel that be necessary
d. I do not know

15. What is your organization's top security initiatives for the last 12 months (Tick all that apply)?
    a. Information security regulation and legislative compliance
    b. Data protection
    c. Information security training and awareness programs
    d. Controls related to technology advancement
    e. Data Encryptions Solutions
    f. Identity and Access Control Management

General Security Assessment (Qualitative)	Yes	No
1. Do you have policies and procedures allowing authorized and limiting unauthorized physical access to electronic information systems and the facilities in which they are housed?		
2. Do your policies and procedures specify the methods used to control physical access to your secured areas, such as door locks, access control systems, security officers, or video monitoring?		
3. Is access to your computing area controlled (single point, reception or security desk, sign-in/sign-out log, temporary/visitor badges)?		
4. Are there procedures in place to prevent computers from being left in a logged-on the state, however briefly?		
5. Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
ACCOUNT AND PASSWORD MANAGEMENT	YES	NO

1. Do you have policies and standards covering electronic authentication, authorization, and access control of personnel and resources to your information systems, applications and data?		
2. Do you ensure that only authorized personnel have access to your computers?		
CONFIDENTIALITY OF SENSITIVE DATA	YES	NO
1. Do you classify your data, identifying sensitive data versus non-sensitive?		
2. Is the most valuable or sensitive data encrypted?		
3. Is there a process for creating retrievable backup and archival copies of critical information?		
4. Do your policies for disposing of old computer equipment protect against loss of data (e.g.. by reading old disks and hard drives)?		
5. Do your disposal procedures identify appropriate technologies and methods for making hardware and electronic media unusable and inaccessible (such as shredding CDs and DVDs, electronically wiping drives, burning tapes) etc.)?		
DISASTER RECOVERY	YES	NO
1. Do you have a current BCP?		
2. Is there a process for creating a retrievable backup and archival copies of critical information?		
3. Do you have an Emergency/Incident Response Plan?		
4. Does your plan identify who should be contacted, including contact		

information?		
5. Do you test your disaster plans on a regular basis?		
SECURITY AWARENESS AND EDUCATION	YES	NO
1. Are you providing information about computer security to your staff?		
2. Do you provide training on a regular recurring basis?		
3. Are employees taught to be alert to possible security breaches?		
4. Are your employees taught about keeping their passwords secure?		
COMPLIANCE AND AUDIT	YES	NO
1. Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?		
2. Do you audit your processes and procedures for compliance with established policies and standards?		

Cyber Security Threat/Vulnerability Assessment

A threat is a potential for a person or a thing to exercise (accidentally trigger or intentionally exploit) a flaw or weaknesses (vulnerability) within an organization. There are several types of threats that may occur within an information system or operating environment. The desired outcome of identifying and reviewing (assessing) threats and vulnerabilities is determining potential and actual risks to the organization. Risk is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organizations. Risk only exists when threats have the capability of triggering or exploiting vulnerabilities. The following formula is used to

determine a risk score: Risk = Impact X Likelihood
For this assessment, numeric rating scales are used to establish impact potential (0-6) and likelihood probability (0-5).

IMPACT SCALE	LIKELIHOOD SCALE
Impact is negligible	Unlikely to occur
Effect is minor, major agency operations are not affected	Likely to occur less than once per year
Organization operations are unavailable for a certain amount of time, costs are incurred. Public/customer confidence is minimally affected	Likely to occur once per year
Significant loss of operations, significant impact on pubic/customer confidence	Likely to occur once per month
Effect is disastrous, systems are down for an extended period of time, systems need to be rebuilt and data replaced	Likely to occur once per week
Effect is catastrophic, critical systems are offline for an extended period; data are lost or irreparably corrupted; public health and safety are affected	Likely to occur daily

Threats	Impact	Likelihood
Human Error	0 - 6	0 - 5
1. Accidental destruction, modification, disclosure, or incorrect classification of information		
2. Ignorance: inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge		
3. Incorrect system configuration		
4. Inadequate Security policy		
5. Unenforced Security policy		
6. Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information		
7. Attacks by "social engineering"		
8. Abuse of privileges/trust		
General Threats	0 - 6	0 - 5
1. Introduction of unauthorized software or hardware		
2. Time bombs: Software programmed to damage a system on a certain date		
3. Operating system design errors: Certain systems were not designed to be highly secure		

4. Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission		
5. Denial of service, due to ICMP bombing, TCP-SYN flooding, large PING packets, etc		
6. Logic bomb: Software programmed to damage a system under certain conditions		
7. Viruses in programs, documents, e-mail attachments		
Access Control Threats	0 - 6	0 - 5
1. Password cracking (access to password files, use of bad – blank, default, rarely changed – passwords)		
2. External access to password files, and sniffing of the networks		
3. Attack programs allowing external access to systems (back doors visible to external networks)		
4. Attack programs allowing internal access to systems (back doors visible to internal networks)		
5. Modems easily connected, allowing uncontrollable extension of the internal network		

6. Major natural disasters, fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power outages, etc		
7. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.		
8. Equipment failure from defective hardware, cabling, or communications system		
9. Sabotage: Malicious, deliberate damage of information or information processing functions		

Thank you very much for your time and information. All information will be given the necessary protection according to the State and Federal data and information protection laws. No personally identifiable information will be included in the final report or will be disclosed

Appendix 2: ICS-SCADA Interview Guide

General Information

1. Are you currently using any form of SCADA to monitor or control your controlled process/distribution system? –
2. Which of the following SCADA systems can you identify at your site (select more than one choice if applicable)? –
    a. Supervisory Computers
    b. Remote Terminal Unites

   c. Programmable Logic Controllers (PLC)
   d. Communication Infrastructure
   e. Human Machine Interface
   f. Security Instrumented Systems
   g. Variable Frequency Drives
3. Which of the following operating system platforms are used to run your SCADA software? (More than one answer may be selected –
   a. Windows
   b. Unix (e.g Linux, Fedora, SUSE, Ubuntu, etc.)
   c. MacOX
   d. Android
4. Which vendors manufacture the SCADA software program are you currently using? –
5. Which of the following systems (Systems which are connected with IT) do you use at your place? –
   a. Enfaf TM BOX
   b. Honeywell's Experion® Process Knowledge System (PKS) (For Terminals)
6. Which of the following Tank Inventory Systems (single-window interface for Tank Gauging Systems) do you use? –
   a. Emerson Rosemount TankMaster WinOpiyou
   b. Schneider-electric SimSci™
   c. Honeywell Enraf Entis Pro
   d. MHT's – VTW
7. Which of the following Tank Gauging Systems do you use (you may select more option if applicable)? -
   a. Honeywell Enraf BPM
   b. Saab, Varec, GSI, MTS, L&J
   c. Meter Management
   d. ControlLogic PLC
   e. SmartView
   f. Huawai U2000/U3000
8. Which of the following Meters/Gauges do you use (you may select more option if applicable)? -
   a. SmartRadar FlexLine
   b. ABB

c. Honeywell VIT
d. Enraf 854 ATG Servo Advanced Tank Level Gauge

Architecture

1. Does the Control & Monitoring system use Client/Server distributed processing?
2. Do you use the network to maximize the performance of the entire Control and Monitoring system?
3. If Yes, how do you use the network to maximize the performance of the entire Control and Monitoring system?
4. Can one make changes to the system without shutting down?
5. How do you exchange data with other applications?
6. Can other automation systems, like a DCS, communicate using industry standard Communication drivers like Modbus or DNP3? –
7. What external databases does the Control and Monitoring system support? –

Configuration –

1. How many applications do you require to configure a Control and Monitoring system?
2. Can you configure your system from any node?
3. How do you backup/archive your system configuration information?
4. How do you restore the system configuration and history in an event of data loss?
5. How do you set up communication with an I/O Device (PLC)?
6. Can you control how your system polls the I/O Devices (PLCs)?

Security Monitoring

1. Do you have security monitoring capabilities for your distribution system?
2. Are you using SCADA to monitor security system features within your distribution system?
3. Does your utility use an enterprise application for Blend Optimization and Emission Monitoring?

4. Does your utility use an enterprise application for loading and terminal automation?
5. Does your utility use an enterprise application for Truck loading, Gas-Pump Monitoring and POS?

Equipment Management

1. Does your SCADA system provide equipment status monitoring such as run-time, oil pressure, or temperature?
2. Is data collected from equipment sensors used for maintenance prediction or repair/replacement forecasting?

Data Management

1. Do you have remote access (other than your primary control interface) to your SCADA data?
2. What mode/modes of SCADA telemetry (data transmission) are used to transmit information from distribution system SCADA components to your SCADA system?
3. Which communication protocols (e.g., IEC 60870, Profinet, Hart) are being used to communicate within your SCADA system?
4. Do you have data storage and analysis system (Historian/ODMS) that stores data collected from sensors, water meters, or the like?
5. On average, how long is data collected by SCADA able to be stored before it is "dumped" or erased?

Process Control

1. Is your SCADA system used to remotely control physical processes (e.g., Pumps, valves, etc.) in the distribution system?
2. Are process control features of your SCADA system able to be accessed from locations other than the primary SCADA control interface?

Security Risk

1. Does any of your SCADA systems TCP/IP based? -
2. Do you believe cloud or Internet-based SCADA software/networks pose a serious security risk with respect to distribution operations?

3. Do you believe there is any security risk in allowing access to operational SCADA data over the Internet?
4. What is the likelihood of cyberattack on your SCADA systems (in the next 12 months)
    a. Very Likely
    b. Likely
    c. Somewhat likely
    d. Not Likely
    e. No Change
5. Do your SCADA systems have any security controls in place to protect the systems?
6. How effective do you consider your security control measures?
    a. Very effective
    b. Effective
    c. Somewhat effective
    d. Not effective
    e. I am not sure
7. Which of the following threat actors have you experienced in the last 24 months (select as many as applicable)
    a. Botnet
    b. Malicious Insider
    c. Systems failure/Data Corruption
    d. Insecure endpoints
    e. Suspected State sponsored
    f. Insecure Web Applications
    g. Web-based Attack
    h. Phishing, Spyware, Spammers
    i. Espionage
8. Which of the following methods to you consider to be the most common threat exploits?
    a. Social Engineering
    b. Privilege abuse
    c. Hacking
    d. DoS/DDoS
    e. Phishing
    f. Exploits affecting supply chain
    g. Malware

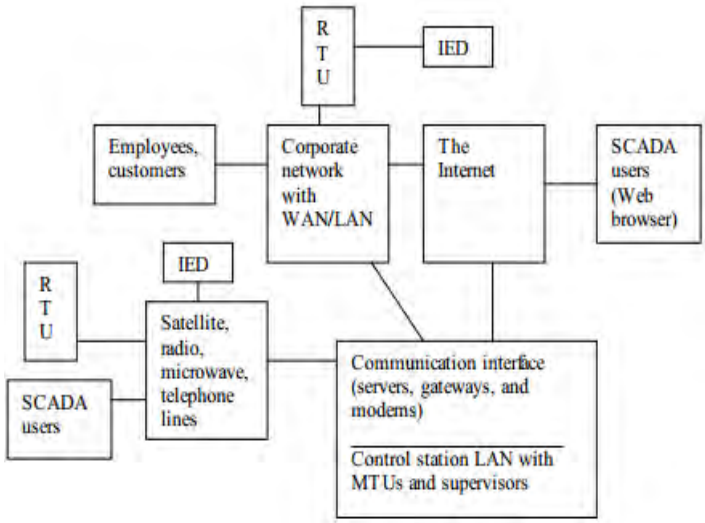
9. Please indicate Yes if you have Controls to counteract the vulnerability and No if not
    a. DDoS/DoS
    b. Code Execution
    c. Buffer Overflow
    d. Memory Corruption
    e. XSS
    f. Improper Access Control (Authorization)
    g. HTTP Traverse Splitting
    h. ICS Data and Command Message Manipulation and Injection
10. Please indicate Yes if you have Controls to counteract the vulnerability and No if not
    a. Bot-network
    b. Malicious Insider
    c. System failure or Data corruption
    d. Insecure endpoints
    e. Suspected Nation-States
    f. Insecure web applications
    g. Web-based attacks
    h. Web-based attacks
    i. Malware (Virus, Trojan Horse, Worms)

Service Ranking

1. Please rank the following SCADA processes in order of their importance to your operations with Five (5) being the most important. -
    a. Communication
    b. Control
    c. Monitoring
    d. Data Processing
    e. Computation
2. Please rank the following SCADA Tools in order of their importance to your operations with Five (5) being the most important.
    a. Communication Networks
    b. Remote Controllers
    c. Remote Terminals
    d. Storage Servers

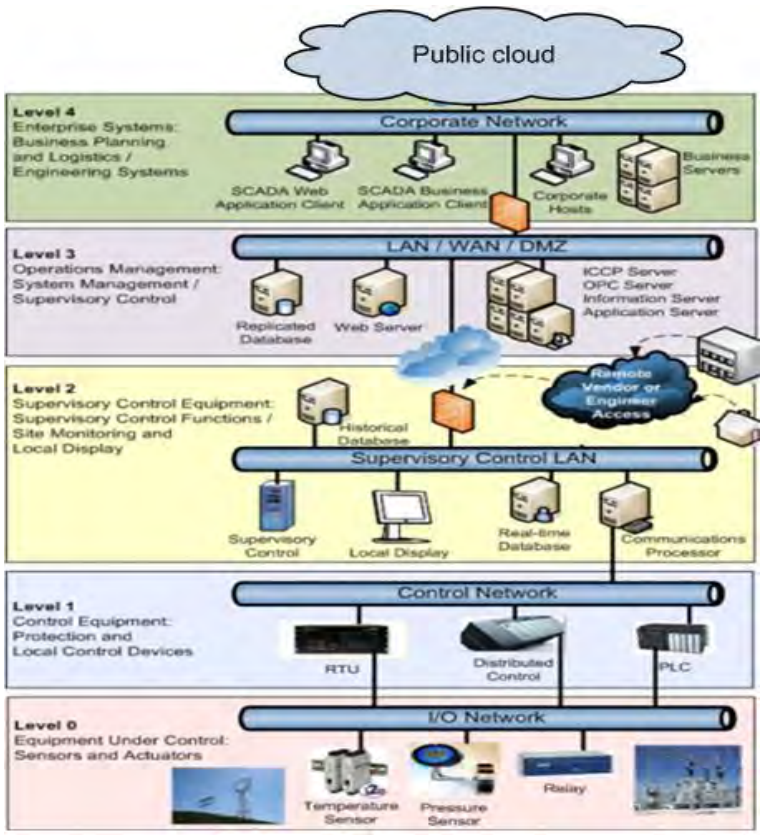
    e. Computational Tools
3. Please rank the following BPD activities in order of their importance with Four (4) being the most important
    a. Tank Monitoring
    b. Emission Control
    c. Data Communication
    d. Procurement
4. Please rank the following systems in the order of their importance in terms of BPD operations with Four (4) being the most important
    a. End-User Applications
    b. Distributed Generation
    c. Smart Grid
    d. Supply Chain

Appendix 3: ICS-SCADA Functional Structure



Structure of SCADA [83]

Appendix 4: ISA-99 (ICS-SCADA) Reference Model



ISA[73] -SCADA Functional Level Reference Model

[73] International Society of Automation Functional Structure

Appendix 5: Risk Assessment Standards

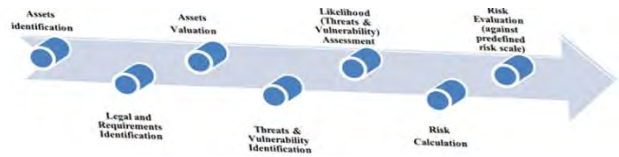
Table 2- 2: Summary of common Risk Assessment Frameworks [15]

Institution	Publication (Number)	Description	Focus
NIST	SP 800-30	Risk Management	Information Systems (General IT Systems)
NIST	SP 800-37	Risk Assessment	Information Systems (Federal Information System
NIST	SP 800-161	Risk Management	Supply Chain Management
ISO/IEC	27005	Risk Management	Information Systems
ISO/IEC	31010	Risk Management	IT Governance
ISO/IEC	31000	Risk Management	Organization Wide (General)
British Standard	100-3	Risk Analysis based on IT Infrastructure	Information Technology
CERT	OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation	Enterprise (IT) Projects
FAIR	FARE	Risk Identification	Business Information Systems
MICROSOFT	MICROSOFT	Risks from the perspective of data acquisition and storage	Software and Data
Dynamic Modelling	Proposed	Security Risk Assessment	Critical (Complex) Infrastructure Systems

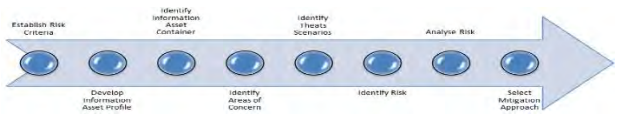
Appendix 5a*:* ***NIST SP800-30***

Appendix 5b: ISO/IEC

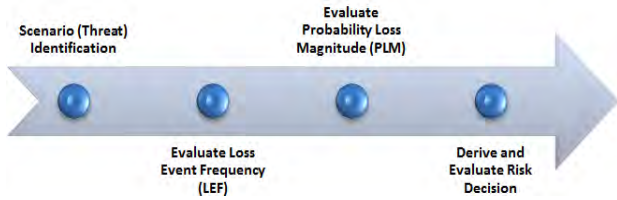
Appendix 5c: BS-7799-2006



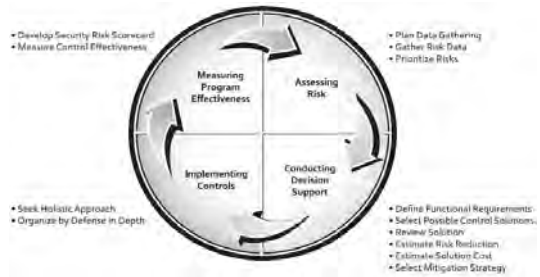
Appendix 5d: OCTAVE



Appendix 5e: FAIR



Appendix 5f: MICROSOFT



Appendix 6: Elements of Network Theory

A graph consists of vertices V, and edges E which together build graph $G\ (V, E)$. The number of vertices and edges are denoted as N and M respectively. Let $_i$ and $_j$ describe two vertices. The adjacent matrix A, describes the network A, where $A_{ij} = 1$, if there is an edge between them; i.e. $(i, j) \in E$, and $A_{ij} = 0$ if there is no edge between two vertices, i.e. $(i, j) \notin E$. An edge is said to be directed if it runs in single direction (figure 3.1c) and undirected if it runs in both directions (figure 3.1a and 3.1b). A directed graph has both an in-degree and an out-degree for each vertex, which are the numbers of incoming and out-going edges respectively.

A directed edge is also known as an arc. The number of edges connected to a vertex is termed as a degree. Vertices and edges can be assigned values; such graph is termed as weighted or a valued graph. It is also possible to have different types of vertices and edges as depicted in 3. 1b. A path starting in vertex, i, and ending in vertex j, with the smallest possible length is called a geodesic distance

between *i* and *j*. For an undirected graph *g*(V, E), the following are considered some of the basic properties of graph g;

Path (between node *i* and *j):* This is a sequence of edges *({i_1, i_2}, {i_2, i_3),……, (i_{k-1}, i_k}*) such that $i_1=i$ and $i_k=j$, and each node in the sequence i_1,…..,i_k is distinct. A path where no vertex appears twice is called an elementary path. It is also defined as a walk where there are no repeated nodes. A walk is the sequence of edges *{i_1, i_2}, {i_2, i_3},...., {i_{k-1}, i_k}.*

Length: This describes the number of edges in a path; (this is equal to the number of vertices in the path minus one).

Circuit: Also known as a circle, it is a path with a final edge to the initial node. A path that ends in the same vertex as it starts (i.e. edges with both endpoints at one vertex – self-loop). A circuit that consists of three edges is called a triangle. A graph without a circuit is called a tree if it is connected and a forest if not.

Connectivity and Components: A graph is connected if every two nodes in the network are connected by some path in the network and component of a network is the distinct maximally connected sub-graphs

The Shortest path (geodesic): Considered as an undirected network, where *l* is the geodesic distance between vertex pairs in a network:

$$l = \frac{1}{1/2n(n+1)} \sum_{i=j} d_{ij}$$

Where d_{ij} is the geodesic distance from vertex *i* to vertex *j*. In multi-component networks (e.g. Internet), there exist vertex pairs that have no connecting path. Conventionally when one assigns infinite geodesic distance to such pairs, the value of *l* becomes infinite. Infinite values of d_{ij} contribute nothing to the sum (this property becomes useful in problem diagnoses and resolutions in the network-centric system).

Equation (3.1) becomes;

$$l^{-1} = \frac{1}{1/2n(n+1)} d_{ij}^{-1}$$

Transitivity or Clustering Coefficient: (it measures the density of triangles in a network)$Cf = \frac{3*\text{number of triangles in the network}}{\text{number of connected triples of vertices}}$

Given a graph G with vertexes A, B and C; if A is connected to B and vertex B is connected to vertex C, then there is a probability that vertex A will be connected to vertex C.

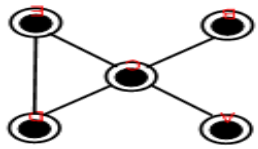


Figure: A-1

Clustering Coefficient (*Cf*): *Cf* measures the mean probability between two vertices which are network neighbours of the same vertex (assume the two will themselves be neighbours). Alternatively, Cf is defined as:

$$Cf_i = \frac{\text{number of vertices connected to vertex i}}{\text{number of triples centred on vertex i}}$$

For vertices with degree 0 or 1, for which both numerator and denominator are zero, $Cf_i = 0$. The clustering coefficient for the whole network becomes the average clustering coefficient which is;

$$Cl^{Avg}(g) = \frac{1}{n}\sum_i cf_i$$

Figure *A1* illustrates the definition of transitivity or clustering. Transitivity measures the extent to which "a friend of my friend is also my friend". Figure 3.2 has one triangle and eight connected triples. "Connected triple" means a single vertex with edges running to an unordered pair of the other.

The individual clustering coefficients for the nodes are 1, 1, 1/6, 0, and 0 with a mean *Cf* value of = 13/30 where *Cf* = 3*1/8 = 3/8

The degree of *k:* This is the number of edges connected to vertex *k*. *P(k)*is the fraction of vertices in the network that have degree *k.* If the graph *G* is directed, the distinction is made between the number of arcs coming into the vertex (in-degree), and a number of arcs coming out from the vertex (out-degree). The average degree of *k* is simply the arithmetic mean of the degree for all vertices, *k*, belonging to graph *G.*

Network Centrality: This is a micro-measure which captures the importance of the node's position in the network. Network centrality is classified as:

i. Degree Centrality (DC): for node *i, is* $d_i(g)/n-1$, where $d_i(g)$ is the degree of node *i*

ii. Closeness Centrality (CC): this tracks how close a given node is to any other node. For a given node *i*, closeness centrality is measured: $\mathrm{CC} = \mathrm{n} - 1/\sum_{\mathrm{j}\neq\mathrm{i}}^{\mathrm{n}} |(\mathrm{i},\mathrm{j})$, where |(*i, j*)is the distance between *i* and *j*.

iii. Betweenness Centrality (BC): It measures how well situated a node is in terms of paths that it lies on.

Appendix 7: Bedell Index

Bedell Index Values[74] [121]		
ESA Index	ISA Index	IAO Index
10 – "Highly Effective"	10 – "Strategic Factor"	10 – "Critically Strategic Activity"
5 – "Moderately Effective"	5 – "Major Support Factor"	8 – "Strategic Activity"
1 – "Ineffective"	1 – "Minor Support Factor"	6 – "Contribution Activity"
0 – "No Support"	0 – "Not Useful"	4 – "Support Activity"
		2 – "Overhead Activity"
		0 – "Detrimental Activity"

Appendix 8: Risk Metrics Scores and Specifications

Threats-Vulnerabilities Events - Score and Descriptions		
Scale	*Description*	*TVE Score*
Very Likely (Very high)	*>100 times per year*	*1.0*
Likely (High)	*Between 50 and 100 times per year*	*.8*

[74] Per the model, both ISA and ESA relate to the system level assessment, while the last three relate to institutional level. The indexes are scaled from 10 to 0. The method assigns specific index values for the first three factors based on their importance or effectiveness. The last two are obtained from the first three variables

Somehow Likely (Moderate)	*Between 10 and 50 times per year*	*.6*
Not Likely (Low)	*Between 1 and 10 times per year*	*.4*
No change (Very Low)	*Less than 1 per year*	*.2*

Appendix 9: Controls Effectiveness Index

CEI[75]	Description	Score
Default security controls No technical security controls No security training No security awareness program No cyber insurance	very weak controls	0.1
Default security controls technical security Controls No security training No security awareness programs No cyber insurance	average controls	0.5
Default security controls technical security Controls Security training Security awareness programs No cyber insurance	strong controls	0.8
Default security controls technical security Controls Security training Awareness programs Cyber insurance	very strong controls	1.0

[75] Control Effectiveness Index

Appendix 10: Complexities Adaptive Index

CAI[76]	Description	Score
<= 3 Interdependent system	Low level complexity	0.1
>= 3 Interdependent system Multiple session management Advanced Technology Integration	Average level Complexity	0.5
>= 3 Interdependent system Multiple session management Advanced Technology Integration Integrated functionalities	High-Level Complexity	0.8
>= 3 Interdependent system Multiple session management Advanced Technology Integration Integrated functionalities Virtualization and with IEDs[77]	Very Complex System	1.0

[76] Complexity Adaptive Index
[77] Intelligent Electronic Devices

Appendix 11: NSTB Top 10 SCADA Vulnerabilities

Table 4-2: NSTB Top 10 most critical ICS vulnerabilities [144]			
Rank	Vulnerability	Possible Consequences	CVSS Score
1	Unpatched published vulnerabilities	Compromise of ICS hosts and applications: This may allow DoS, Code execution, data loss, or security bypass	9.8
2	Use of Vulnerable Remote Display Protocols	Unauthorised access to ICS components: Possible unauthorised remote access to graphical supervisory control software, as well as any other functionality allowed to the remote user	9.8
3	Web HMI Vulnerabilities	Unauthorised access to Web HMI, Web server or other Web applications and functionalities: possible unauthorised remote access to graphical supervisory control software, as well as any other functionality built into the Web application or allowed to the Web server.	9.8
4	Buffer Overflows in ICS services	Unauthorized access to ICS components (from	9.3

		different security zones) and compromise of ICS hosts and applications	
5	Improper Authentication	Unauthorized access to ICS applications: Possible unauthorized remote access to supervisory control functionality	9.3
6	Improper Access Control (Authorization)	Unauthorized access to ICS functionality and security bypass (including information leaks, DoS, and arbitrary code execution)	9.1
7	Use of Standard IT Protocols with cleartext Authentication	Unauthorized access to ICS components: Possible unauthorized remote access to hosts with privileges to any functionality granted to the compromised remote user.	9.1
8	Unprotected Transport of ICS Application Credentials	Unauthorized access to ICS applications: Possible unauthorized remote access to supervisory control functionality	9.0
9	ICS Data and Command Message Manipulation and Injection	Exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or allowing execution of arbitrary code	8.8

10	SQL Injection	Data loss: Unauthorized read or write access to the database Security bypass: DoS of the database service or unauthorized access to the associated host Historical data exposure, loss or manipulation and possible attack path into the ICS network	8.6

Appendix 12: Co-author Statement

AARHUS BSS SCHOOL OF BUSINESS AND SOCIAL SCIENCES
AARHUS UNIVERSITY

Declaration of co-authorship*

Full name of the PhD student: **Samuel Tweneboah-Koduah**

This declaration concerns the following article/manuscript:

Title:	Barriers to government cloud adoption
Authors:	S. Tweneboah-Koduah B. Endicott-Popovsky, and A. Tsetse

The article/manuscript is: Published X☐ Accepted ☐ Submitted ☐ In preparation ☐

If published, state full reference: **S. Tweneboah-Koduah, B. Endicott-Popovsky, and A. Tsetse, "Barriers to government cloud adoption," *International Journal of Management Information Technology*, vol. 6, no. 3, pp. 1–16, 2014**

If accepted or submitted, state journal: ***International Journal of Management Information Technology***

Has the article/manuscript previously been used in other PhD or doctoral dissertations?

No X☐ Yes ☐ If yes, give details:

The PhD student has contributed to the elements of this article/manuscript as follows:

A. Has essentially done all the work
B. Major contribution
C. Equal contribution
D. Minor contribution
E. Not relevant

Element	Extent (A-E)
1. Formulation/identification of the scientific problem	B
2. Planning of the experiments/methodology design and development	B
3. Involvement in the experimental work/clinical studies/data collection	B
4. Interpretation of the results	B
5. Writing of the first draft of the manuscript	B
6. Finalization of the manuscript and submission	C

Signatures of the co-authors

Date	Name	Signature
15-01-2020	Anthony Tsetse	A.T. Tse
15-01-2020	B. Endicott-Popovsky	Barbara Endicott-Popovsky

In case of further co-authors please attach appendix

Date: **January 15, 2020**

Signature of the PhD student

*As per policy the co-author statement will be published with the dissertation.

AARHUS BSS | SCHOOL OF BUSINESS AND SOCIAL SCIENCES
AARHUS UNIVERSITY

Declaration of co-authorship*

Full name of the PhD student: **Samuel Tweneboah-Koduah**

This declaration concerns the following article/manuscript:

Title:	**Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study," *Computer. Journal*, vol. 61, 2018**
Authors:	**S. Tweneboah-Koduah and W. J. Buchanan**

The article/manuscript is: Published **X**☒ Accepted ☐ Submitted ☐ In preparation ☐

If published, state full reference: **S. Tweneboah-Koduah and W. J. Buchanan, "Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study," *Computer. Journal*, vol. 61, 2018**

If accepted or submitted, state journal: **Computer Journal**

Has the article/manuscript previously been used in other PhD or doctoral dissertations?

No **X**☒ Yes ☐ If yes, give details:

The PhD student has contributed to the elements of this article/manuscript as follows:

A. Has essentially done all the work
B. Major contribution
C. Equal contribution
D. Minor contribution
E. Not relevant

Element	Extent (A-E)
1. Formulation/identification of the scientific problem	**A**
2. Planning of the experiments/methodology design and development	**B**
3. Involvement in the experimental work/clinical studies/data collection	**A**
4. Interpretation of the results	**A**
5. Writing of the first draft of the manuscript	**B**
6. Finalization of the manuscript and submission	**C**

Signatures of the co-authors

Date	Name	Signature
15-01-2020	Samuel Tweneboah-Koduah	
15-01-2020	W. J. Buchanan	

In case of further co-authors please attach appendix

Date: **January 15, 2020**

Signature of the PhD student

*As per policy the co-author statement will be published with the dissertation.

Appendix 12: Co-author Statement

AARHUS BSS SCHOOL OF BUSINESS AND SOCIAL SCIENCES
AARHUS UNIVERSITY

Declaration of co-authorship*

Full name of the PhD student: **Samuel Tweneboah-Koduah**

This declaration concerns the following article/manuscript:

Title:	The reaction of Stock Volatility to Data Breach: An Event Study
Authors:	S. Tweneboah-Koduah, Ramjee Prasad

The article/manuscript is: Published ☐ Accepted ☐ Submitted **X** ☐ In preparation ☐

If published, state full reference: **N/A**

If accepted or submitted, state journal:

Has the article/manuscript previously been used in other PhD or doctoral dissertations?

No **X**☐ Yes ☐ If yes, give details:

The PhD student has contributed to the elements of this article/manuscript as follows:

A. Has essentially done all the work
B. Major contribution
C. Equal contribution
D. Minor contribution
E. Not relevant

Element	Extent (A-E)
1. Formulation/identification of the scientific problem	**B**
2. Planning of the experiments/methodology design and development	**B**
3. Involvement in the experimental work/clinical studies/data collection	**B**
4. Interpretation of the results	**B**
5. Writing of the first draft of the manuscript	**B**
6. Finalization of the manuscript and submission	**C**

Signatures of the co-authors

Date	Name	Signature
20-01-2020	Ramjee Prasad	Ramjee Prasad

In case of further co-authors please attach appendix

Date: **January 20, 2020**

Signature of the PhD student

*As per policy the co-author statement will be published with the dissertation.

Appendix 12: Co-author Statement

AARHUS BSS SCHOOL OF BUSINESS AND SOCIAL SCIENCES
AARHUS UNIVERSITY

Declaration of co-authorship*

Full name of the PhD student: **Samuel Tweneboah-Koduah**

This declaration concerns the following article/manuscript:

Title:	Threats of Obsolete Infrastructures to Smart Grid Protection
Authors:	S. Tweneboah-Koduah, Ramjee Prasad

The article/manuscript is: Published ☐ Accepted ☐ Submitted **X** ☐ In preparation ☐

If published, state full reference: **N/A**

If accepted or submitted, state journal:

Has the article/manuscript previously been used in other PhD or doctoral dissertations?

No **X**☐ Yes ☐ If yes, give details:

The PhD student has contributed to the elements of this article/manuscript as follows:

A. Has essentially done all the work
B. Major contribution
C. Equal contribution
D. Minor contribution
E. Not relevant

Element	Extent (A-E)
1. Formulation/identification of the scientific problem	**B**
2. Planning of the experiments/methodology design and development	**B**
3. Involvement in the experimental work/clinical studies/data collection	**B**
4. Interpretation of the results	**B**
5. Writing of the first draft of the manuscript	**B**
6. Finalization of the manuscript and submission	**C**

Signatures of the co-authors

Date	Name	Signature
20-01-2020	Ramjee Prasad	Ramjee Prasad

In case of further co-authors please attach appendix

Date: **January 20, 2020**

S. Tweneboah-Koduah

Signature of the PhD student

*As per policy the co-author statement will be published with the dissertation.

Appendix 12: Co-author Statement

AARHUS BSS SCHOOL OF BUSINESS AND SOCIAL SCIENCES
AARHUS UNIVERSITY

Declaration of co-authorship*

Full name of the PhD student: **Samuel Tweneboah-Koduah**

This declaration concerns the following article/manuscript:

Title:	Quantitative Estimate of Cyber Infrastructure and Interdependency Systems
Authors:	S. Tweneboah-Koduah, Ramjee Prasad

The article/manuscript is: Published ☐ Accepted ☐ Submitted **X** ☐ In preparation ☐

If published, state full reference: **N/A**

If accepted or submitted, state journal:

Has the article/manuscript previously been used in other PhD or doctoral dissertations?

No **X**☐ Yes ☐ If yes, give details:

The PhD student has contributed to the elements of this article/manuscript as follows:

A. Has essentially done all the work
B. Major contribution
C. Equal contribution
D. Minor contribution
E. Not relevant

Element	Extent (A-E)
1. Formulation/identification of the scientific problem	**B**
2. Planning of the experiments/methodology design and development	**B**
3. Involvement in the experimental work/clinical studies/data collection	**B**
4. Interpretation of the results	**B**
5. Writing of the first draft of the manuscript	**B**
6. Finalization of the manuscript and submission	**C**

Signatures of the co-authors

Date	Name	Signature
20-01-2020	Ramjee Prasad	

In case of further co-authors please attach appendix

Date: **January 30, 2020**

Signature of the PhD student

*As per policy the co-author statement will be published with the dissertation.