

CRANFIELD UNIVERSITY

UCHENNA DANIEL ANI

IMPROVING CYBER SECURITY IN INDUSTRIAL CONTROL
SYSTEM ENVIRONMENT

SCHOOL OF AEROSPACE, TRANSPORT AND MANUFACTURING

PHD THESIS
Academic Year: 2015 - 2018

Supervisor: Dr. Hongmei He & Prof. Ashutosh Tiwari
February 2018

CRANFIELD UNIVERSITY

School of Aerospace, Transport and Manufacturing

PHD THESIS

Academic Year 2015 - 2018

UCHENNA DANIEL ANI

Improving Cyber Security in Industrial Control System Environment

Supervisor: Dr. Hongmei He & Prof. Ashutosh Tiwari
February 2018

This thesis is submitted in partial fulfilment of the requirements for
the degree of Doctor of Philosophy

© Cranfield University 2018. All rights reserved. No part of this
publication may be reproduced without the written permission of the
copyright owner.

ABSTRACT

Integrating industrial control system (ICS) with information technology (IT) and internet technologies has made industrial control system environments (ICSEs) more vulnerable to cyber-attacks. Increased connectivity has brought about increased security threats, vulnerabilities, and risks in both technology and people (human) constituents of the ICSE. Regardless of existing security solutions which are chiefly tailored towards technical dimensions, cyber-attacks on ICSEs continue to increase with a proportionate level of consequences and impacts. These consequences include system failures or breakdowns, likewise affecting the operations of dependent systems. Impacts often include; marring physical safety, triggering loss of lives, causing huge economic damages, and thwarting the vital missions of productions and businesses.

This thesis addresses uncharted solution paths to the above challenges by investigating both technical and human-factor security evaluations to improve cyber security in the ICSE. An ICS testbed, scenario-based, and expert opinion approaches are used to demonstrate and validate cyber-attack feasibility scenarios. To improve security of ICSs, the research provides: (i) an adaptive operational security metrics generation (OSMG) framework for generating suitable security metrics for security evaluations in ICSEs, and a list of good security metrics methodology characteristics (scope-definitive, objective-oriented, reliable, simple, adaptable, and repeatable), (ii) a technical multi-attribute vulnerability (and impact) assessment (MAVCA) methodology that considers and combines dynamic metrics (temporal and environmental) attributes of vulnerabilities with the functional dependency relationship attributes of the vulnerability host components, to achieve a better representation of exploitation impacts on ICSE networks, (iii) a quantitative human-factor security (capability and vulnerability) evaluation model based on human-agent security knowledge and skills, used to identify the most vulnerable human elements, identify the least security aspects of the general workforce, and prioritise security enhancement efforts, and (iv) security risk reduction through critical impact point assessment (S2R-CIPA) process model that demonstrates the combination of technical and human-factor security evaluations to mitigate risks and achieve ICSE-wide security enhancements.

The approaches or models of cyber-attack feasibility testing, adaptive security metrication, multi-attribute impact analysis, and workforce security capability evaluations can support security auditors, analysts, managers, and system owners of ICSs to create security strategies and improve cyber incidence response, and thus effectively reduce security risk.

Keywords:

Industrial Cyber Security, Cyber-Physical System Security, Cyber Security Evaluation, Security Impact Analysis, Operational Security Metrics; Human-factor Security, Functional Dependency Analysis; Security Criticality Analysis, Security Risk Assessment.

ACKNOWLEDGEMENTS

I want to thank God Almighty for giving me the grace and direction to complete this research project and thesis. I thank God for His immeasurable blessings on me and my family all through the period of this study. My gratitude goes to my dear lovely wife Mrs. Nneka C. Daniel who stood by me, encouraged, and supported me with ideas, suggestions, checks, and prayers throughout the period of my studies. I love you baby. My thanks also go to my parents, siblings, in-laws, and friends for their utmost support and reassurances.

My profound gratitude to my esteemed supervisors: Dr. Hongmei (Mary) He, and Professor Ashutosh Tiwari for their relentless guidance, correction, redirections, and supervision throughout all the stages of my research work at Cranfield University. I remain indebted to you for your patience, tolerance, and confidence you accorded me.

My sincere appreciation to Tertiary Education Trustfund (TETFUND) Nigeria and Federal University Lokoja for giving me the opportunity to study and further my career to a PhD level. My deepest thanks to Professor Abdulmumini Rafindadi, Professor Sunday Eric Adewumi, and all other great mind in FUL for believing in me and supporting my course to advance my career.

I want to specially thank Holding Forth Christian Centre, Cranfield Christian Fellowship, and other church fellowships that provided the spiritual enrichment for me to accomplish this research. I thank my precious friends and office colleagues for their friendship, support, and kindness during my studies. With you all, it was a great family.

As you have supported me to achieve this accomplishment, God will surely bless and establish you with success in all your endeavours in Jesus Name. Amen.

Uchenna Daniel Ani

LIST OF PUBLICATIONS

Journal Paper

1. **Uchenna P. Daniel Ani**, Hongmei (Mary) He & Ashutosh Tiwari (2017) *Review of Cybersecurity issues in Industrial Critical Infrastructure: Manufacturing in perspective*, Journal of Cyber Security Technology, 1:1, 32-74, DOI: 10.1080/23742917.2016.1252211.
2. **Uchenna P. Daniel Ani**, Hongmei He & Ashutosh Tiwari (2017). A *Framework for Operational Security Metrics Development for Industrial Control Environment*. **Submitted** to Journal of Cyber Security Technology – Taylor & Francis Publishers
3. **Uchenna P. Daniel Ani**, Hongmei He & Ashutosh Tiwari (2017). *Evaluation of Cyber Security Capacity of the Industrial Workforce*. **Submitted** to Journal of Systems and Information Technology - EmeraldInsight Publishers.
4. **Uchenna P. Daniel Ani**, Hongmei He & Ashutosh Tiwari (2017). *Security Vulnerability Impact Analysis for Industrial Control System Reliability Improvement*. **Submitted** to IEEE Transactions on Reliability.
5. **Uchenna P. Daniel Ani**, Hongmei He & Ashutosh Tiwari. Multi-Element Security Risk Reduction Methodology for Industrial Control System Operational Environment. **To be submitted to** Journal of Systems and Information Technology - EmeraldInsight Publishers

Conference Book Chapter (Published)

1. Uchenna P. Daniel Ani, Hongmei He & Ashutosh Tiwari, "Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure," *Advances in Human Factors in Cyber Security (Springer): Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA*, vol. 501, D. Nicholson, Ed. Florida: Springer International Publishing, 2016, pp. 169–182.

TABLE OF CONTENTS

ABSTRACT	i
ACKNOWLEDGEMENTS.....	iii
LIST OF PUBLICATIONS.....	iv
LIST OF FIGURES.....	xi
LIST OF TABLES	xiii
LIST OF ABBREVIATIONS	xiv
1 INTRODUCTION	1
1.1 Research Background	3
1.1.1 Evolution of Industrial Control Systems (ICSs).....	3
1.1.2 Industrial Control System Security Vulnerability and Attack Trends	4
1.1.3 Industrial Control System Security Enablers and Operational Efficiency.....	6
1.2 Research Gap.....	9
1.3 Research Aim and Objectives.....	12
1.4 Research Scope and Limitation	13
1.5 Research Justification.....	19
1.6 Thesis Structure.....	21
2 RESEARCH METHODOLOGY	22
2.1 Introduction	22
2.2 Work Package 1: - Understanding the Contexts, and Issues of Cyber Security in Industrial Control System Environments (ICSE).....	22
2.2.1 Cyber-Attack Demonstration	23
2.3 Work Package 2: Security Metrication Framework and Security Criticality Evaluation Models	28
2.4 Work Package 3: Security Risk Reduction via Security Risk Reduction through Critical Impact Point Assessment(S2R-CIPA) Process Plan.	31
3 LITERATURE REVIEW	32
3.1 Industrial Control System Environment Security	32
3.1.1 ICS Security Threats	34
3.1.2 ICS Security Vulnerabilities	34
3.1.3 ICS Security Attack Patterns and Impacts.....	35
3.1.4 ICS Cyber Incident Analysis.....	36
3.2 Categorised Methodologies for ICSE Security	39
3.3 Existing Works Related to Research Objectives	40
3.3.1 Cyber-Attack Simulation in ICSE.....	40
3.3.2 Security Metrics Generation Methods	42
3.3.3 Technology Vulnerability Impact Analysis Techniques.....	45
3.3.4 Human-factor Cyber Security Evaluations.....	50
3.3.5 Security Risk Assessment and Reduction Approaches.....	57

3.4 Chapter Summary.....	59
4 INDUSTRIAL CONTROL SYSTEM TESTBED DEVELOPMENT AND CYBER-ATTACKS DEMONSTRATION.....	61
4.1 Introduction	61
4.2 Construction of the Testbed.....	61
4.2.1 The Hardware of ICS-CS	62
4.2.2 The Testbed Process	63
4.3 Cyber-Attack Demonstration.....	64
4.3.1 Initial Assumptions	65
4.3.2 Reconnaissance.....	65
4.3.3 Target Exploitation	68
4.4 Discussion and Conclusions	75
5 SECURITY METRICS GENERATION FRAMEWORK.....	79
5.1 Introduction	79
5.2 The Framework for Operational Security Metrics Generation (OSMG)...	79
5.2.1 Target Definition (Phase 1)	82
5.2.2 Objective Definition (Phase 2).....	85
5.2.3 Metrics Synthesis	86
5.2.4 Structural Flow and Review.....	89
5.3 Implementation and Application of the Framework	90
5.3.1 Validation of the OSMG Framework.....	91
5.4 Chapter Summary.....	106
6 MODEL-BASED TECHNOLOGY VULNERABILITY IMPACT ANALYSIS ..	107
6.1 Introduction	107
6.2 Theoretical Concept for Technical Vulnerability Impact Analysis	107
6.3 Multi-Attribute Vulnerability Criticality Analysis (MAVCA) Model Development Analysis and Presentation	109
6.3.1 Criticality Index Estimation	111
6.3.2 Vulnerability Exploit Potential (β).....	112
6.4 Case Study	122
6.4.1 Network Structure and Vulnerability Scan	123
6.4.2 Graph Structure for Functional Dependencies	124
6.4.3 Results	124
6.4.4 Analysis and Discussion.....	131
6.5 Chapter Summary.....	138
7 MODEL-BASED HUMAN (WORKFORCE) CYBER SECURITY CAPABILITY EVALUATION.....	139
7.1 Background.....	139
7.2 The Evaluation Model for User-Centred Security Capability	139
7.2.1 Model Formulation	141
7.3 Scenario-Based Model Testing (Validation).....	149
7.4 Chapter Summary.....	163

8 SECURITY RISK REDUCTION THROUGH SECURITY RISK REDUCTION THROUGH CRITICAL IMPACT POINT ASSESSMENTPROCESS	164
8.1 Background.....	164
8.2 Proposed Security Risk Reduction through Critical Impact Point Analysis (S2R-CIPA).....	164
8.2.1 Overview of S2R-CIPA Process Plan.....	165
8.2.2 S2R-CIPA Concept Descriptions.....	166
8.2.3 S2R-CIPA Process-flow and Steps Descriptions	169
8.3 Evaluation: Case Study Results and Discussions.....	175
8.3.1 S2R-CIPA Steps 1, 2, and 3.....	176
8.3.2 S2R-CIPA Step 4	177
8.3.3 S2R-CIPA Step 5	178
8.3.4 S2R-CIPA Steps 6 and 7.....	181
8.3.5 Analysis and Summary.....	183
9 DISCUSSIONS AND CONCLUSIONS	185
9.1 Appraising ICSE Cyber Security Landscape.....	185
9.1.1 Security Metrics Framework Development.....	185
9.1.2 Technical Vulnerability Impact Analysis	187
9.1.3 Human (Workforce) Cyber Security Capability and Vulnerability Evaluation	188
9.1.4 Security Risk Reduction through Vulnerability Analysis and Critical Impact Point Process	189
9.2 Key Research Contributions	191
9.2.1 A list of good characteristics for security metric frameworks	192
9.2.2 A framework to guide a holistic generation of security metrics	193
9.2.3 A novel approach for evaluating and prioritising technical security criticality impacts	193
9.2.4 A novel approach to evaluate and prioritise human cyber security capabilities.	194
9.2.5 A novel approach for security risk reduction.....	194
9.3 Research Limitations	195
9.4 Conclusions	199
9.5 Future Work	202
REFERENCES.....	206
APPENDICES	234
Appendix A: Tables.....	234
Table A-1: Reviewed Cybersecurity Principles Relative to ICS.....	234
Table A-2: Network Components of Industrial Control System Conveyor Testbed Setup.....	237
Table A-3: CVSS 2.0 Standard Metrics Scoring Values [77]	239

Table A-4: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (1)	240
Table A-5: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (1)	241
Table A-6: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (2)	242
Table A-7: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (3)	243
Table A-8: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (1).....	244
Table A-9: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (2).....	245
Table A-10: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (3).....	246
Table A-11: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (4).....	247
Table A-12: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (5).....	248
Table A-13: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (6).....	249
Table B-14: Testbed Vulnerability - Risk Reduction (Technology and People Assets)	250
Table A-15: Complete (37-Member) Workforce Capability Evaluation Results	251
Table A-16: Common Industrial Control Systems Protocols.....	252
Table A-17: IT and ICS Specific Security Standards, and Guidelines	253
Table A-18: Technology Vulnerability Analysis and Resolution Results..	254
Table A-19: Current State Vulnerability Impact Point Analysis Results...	255
Table A-20: Enhanced State Vulnerability Impact Point Analysis Results	255
Table A-21: ICS Cyber Incidents in History	256
Table A-22: Analysed Incident Classification based on Security Principles Targeted	258
Table A-23: Cyber Security Methodologies relative to ICS Critical Infrastructure	260
Table A-24: Comparative Review of ICS Security Risk Management (Assessment and Reduction) Methods	263
Table A-25: A Sample Collection Security Metrics from selected literature	266
Appendix B: Figures	270
Figure B-1: Demonstrator System Testbed Setup (Screenshots)	270
Figure B-2:Wiring Schematics for ICS-CS Conveyor Testbed Setup	271

Figure B-3: Totally Integrated Portal ICS-CS Testbed Topology and Network Configurations.....	272
Figure B-4: Totally Integrated Portal ICS-CS Testbed Device and Network Configurations.....	273
Figure B-5: Ladder Logic Programme for Conveyor Testbed Process Control (1)	274
Figure B-6: Ladder Logic Programme for Conveyor Testbed Process Control (2)	275
Figure B-7: Ladder Logic Programme for Conveyor Testbed Process Control (3)	276
Figure B-8: ICS-CS Testbed Network Live Host Scan Results (Nmap) ..	277
Figure B-9: ICS-CS Testbed Network Port Scan Results (Nmap).....	277
Figure B-10: ICS-CS Testbed Network Host Reachability Scan Results (Fping).....	278
Figure B-11: ICS-CS Host Vulnerability Scan Summary (NESSUS)	278
Figure B-12 : ICS-CS Testbed Network Vulnerability Scan (NESSUS)...	279
Figure B-13: ICS-CS Testbed Network Control Workstation Privilege Escalation Attack Scenario – Windows Login Attempt	281
Figure B-14: ICS-CS Testbed Network Control Workstation Privilege Escalation Attack Scenario – TIA Portal Access	281
Figure B-15: PLC Denial-of-Service Attack Scenario: Hping3 Flood Instance.....	282
Figure B-16: PLC Denial-of-Service Attack Scenario: Packet Flood Analysis – 1 (Wireshark)	282
Figure B-17: PLC Denial-of-Service Attack Scenario: Packet Flood Analysis – 2 (Wireshark)	283
Figure B-18: PLC Denial-of-Service Attack Scenario: SMOD Utility Attack (1).....	283
Figure B-19: PLC Denial-of-Service Attack Scenario: SMOD Utility Attack (2).....	284
Figure B-20 : PLC Denial-of-Service Attack Scenario: SMOD Attack Impact (1).....	284
Figure B-21 : PLC Denial-of-Service Attack Scenario: SMOD Attack Impact (2).....	285
Figure B-22 : PLC Denial-of-Service Attack Scenario: SMOD Attack Impact (3).....	285
Figure B-23: Nexpose Vulnerability Scanner Start-up from Metasploit Framework in Kali Linux.....	286
Figure B-24: Nexpose Vulnerability Scanner – Host IP Scanning Parameter Setup	286
Figure B-25: Nexpose Vulnerability Scanner – Vulnerability Scan Results	287

Figure B-26: Nexpose Vulnerability Scanner –Vulnerability Description Results	287
Figure B-27: Complete (37-Member) Workforce Capability Chart.....	288
Figure B-28: Complete Chart Representation of Cumulative Capability Ratings (CCR).....	289
Figure B-29: Testbed Control Network Components integration	290
Appendix C: Questionnaires and Ethics Approvals.....	293
Figure C-1: Framework Validation Questionnaire (Tool)	293
Figure C-2: Ethics Approval for Framework Validation Questionnaire (Tool).....	298
Figure C-3: Ethics Approval for Workforce Cyber Security Capability Test-based Questionnaire	299
Figure C-4: Cyber Security Capability Questionnaire	300

LIST OF FIGURES

Figure 1-1: Layered Architecture of a Typical Industrial Control System (<i>Source: Author</i>)	2
Figure 1-2: Increasing Number of ICS Vulnerabilities	5
Figure 1-3: Increasing Number of ICS Attacks	5
Figure 1-4: The ICS Cyber Security Trend (<i>Source: Author</i>)	8
Figure 1-5: Three Functional Elements of Industrial Control System Environment	9
Figure 2-1: Overview of Applied Research Methods	24
Figure 3-1: Sampled ICS Cyber Incidents	38
Figure 3-2: Distribution of Security Violations for ICS Cyber Incidents	39
Figure 4-1: ICS-CS Network Diagram	63
Figure 4-2: Scenario Demonstration Attack-plan	65
Figure 4-3: ICS-CS Testbed Process Flow Diagram	67
Figure 4-4: Metasploit and Hping Attack Execution Screens	72
Figure 4-5: SMOD DoS Utility Attack Execution Screen	73
Figure 4-6: Attack Scenario Impacts and Cascade Illustration	76
Figure 5-1: Operational Security Metrics Generation (OSMG) Framework	83
Figure 5-2: Workforce Capability Visualisation Chart	97
Figure 5-3: Relevance Mappings of Framework Characteristics	102
Figure 5-4: Criteria Representation Maps	104
Figure 6-1: Multi-Attribute Vulnerability Criticality Analysis (MAVCA) Process flow	110
Figure 6-2: ICS Emulator Network Architecture for Test Scenario and Vulnerability Mapping	129
Figure 6-3: Functional Dependency and Cascading Impact Graph Representation	129
Figure 6-4: Vulnerability Exploit & Impact Potentials	130
Figure 6-5: Criticality Index Estimation	130
Figure 6-6: Criticality Index Rationing	131
Figure 7-1: Human Workforce Security Capability Evaluation Scheme	143
Figure 7-2: Capability Representation Formats	148

Figure 7-3: Workforce Capability Evaluation Placement Chart (37-User Classification)	155
Figure 7-4: 15 Lowest Capability Workforce Representation (Kc, Sc, and PSC Contributions)	156
Figure 7-5: The Least 15 cumulative capability rating (CCR)	157
Figure 8-1: S2R-CIPA Flow Diagram	167
Figure 8-2: Component-Level Vulnerability Reductions	180
Figure 8-3: Aggregate-Level Vulnerability Criticality Reductions	181
Figure 8-4: Workforce Entity-Level Vulnerability Reduction	182
Figure 8-5: Workforce Aggregate-Level Vulnerability Reductions	182

LIST OF TABLES

Table 3-1: Functional Properties Classification of ICS Vulnerabilities	35
Table 4-1: ICS-CS Testbed Components Mapping to NIST Standard.....	62
Table 4-2: Attack Scenarios Characterisation	69
Table 4-3: Attack Scenario - Security Violation Relationship.....	69
Table 5-1: Metrics Profile Description for Human Capability Evaluation.....	95
Table 5-2: Capability Evaluation Results	97
Table 5-3: Context - Response Mapping Groups	100
Table 5-4: Good Metrics Characteristics Evaluation Results.....	102
Table 5-5: Framework Validation Mapping Results	103
Table 6-1: <i>k</i>₂ Vulnerability Impact Evaluation	126
Table 6-2: Testbed Vulnerability Results	128
Table 6-3: Severity Estimation Results.....	128
Table 6-4: Severity Estimation and Prioritisation Results	131
Table 7-1: Capability-to-Priority Classifications	147
Table 7-2: Scenario Baseline Definitions.....	152
Table 7-3: Capability-Priority Classification for Test Scenario	154
Table 7-4: Priority Ranking for the 15 workforce members with the least security capacities.....	155
Table 7-5: The Least 10 Skills Cumulative Capability Ratings (CCR)	157
Table 7-6: The Least 5 Knowledge Cumulative Capability Ratings (CCR)	158
Table 7-7: Statistical Crosstab for Security Capability by Priority Ranking	159
Table 7-8: Statistical Crosstab for Workforce Group by Priority Ranking	159
Table 8-1: HACCP to S2R-CIPA Translation.....	166
Table 8-2: Summarised Technology Risk Reductions	179
Table 8-3: S2R-CIPA Mapping to Objective Questions	184

LIST OF ABBREVIATIONS

ADT	Attack and Defence Trees
AGA	American Gas Association
ARP	Address Resolution Protocol
BIOS	Basic Input Output System
BSC	Balanced Scorecard
BYOD	Bring Your Own Device
CCR	Cumulative Capability Rating
CIA	Confidentiality Integrity Availability
COTS	Commercial-Off-the-shelf
CPNI	Centre for the Protection of National Infrastructure
CPS	Cyber-Physical System
CVE	Common Vulnerability and Exposure
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
DIACAP	Defence Information Assurance Certification and Accreditation Process
DMZ	De-Militarised Zone
DNS	Domain Name System
DoC	Denial of Control
DoS	Denial-of-Service
DoV	Denial of View
ENISA	European Network and Information Security Agency
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
HACCP	Hazard Analysis Critical Control Point Process
HAG	Hybrid Attack Graph
HMI	Human-Machine-Interface
I/O	Input Output
ICCP	Impressed Current Cathodic Protection
ICS	Industrial Control System
ICS-CS	Industrial Control System Conveyor Setup
ICSE	Industrial Control System Environment
IDS	Intrusion Detection System
IOMS	Information Operations and Management Systems
IoT	Internet-of-Things
IP	Internet Protocol
ISO/IEC	International Standard Organisation and the International Electrotechnical Commission

IT	Information Technology
LAN	Local Area Network
LAN/WAN	Local Area Network/Wide Area Network
LLNs	Low-power Lossy Networks
LoC	Loss of Control
LoV	Loss of View
MAVCA	Multi-Attribute Vulnerability Criticality Analysis
MitM	Man-in-the-middle
MoC	Manipulation of Control
MoV	Manipulation of View
MTBDD	Multi-Terminal Binary Decision Diagrams
NERC CIP	Northern American Electricity Reliability Corporation Critical Infrastructure Protection OSCE
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSTB	National SCADA Testbed
NVD	National Vulnerability Database
OPC	OLE for Process Control
OS	Operating System
OSMG	Operational Security Development Framework
OT	Operational Technology
PCS	Process Control System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
R&D	Research and Development
RPL	Routing Protocol
RTU	Remote Terminal Unit
Sbl	Security by Inclusion
SCADA	Supervisory Control and Data Acquisition
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TC	Trusted Computing
TCP	Transmission Control Protocol
TEK	Traditional Ecological Knowledge
TFTP	Trivial File Transfer Protocol
TPM	Trusted Platform Module
USB	Universal Serial Bus
S2R-CIPA	Vulnerability Analysis Critical Impact Point
VPN	Virtual Private Network

1 INTRODUCTION

Industrial Control System (ICS) is an all-purpose (common) term used to describe various types of automated industrial systems that control, monitor, and manage industrial processes (Macaulay and Singer, 2012; Stouffer *et al.*, 2015). The name 'Industrial Control System' was coined in 2008 by National Institute of Standards and Technology (NIST) publication NIST 800-82: Guide to Industrial Control System Security. It was used to refer to several types of control systems including; Supervisory Control and Data Acquisition (SCADA) systems (Shaw, 2006; Radack, 2011), Process Control Systems (PCS), Distributed Control Systems (DCS) (Kisner *et al.*, 2010; Karnouskos, 2011; Radack, 2011; ICSJWG, 2013), which are often found in industrial and critical infrastructure sectors such as manufacturing, transport, electric power, energy generation and distribution, water and wastewater management, chemical and petrochemical operations, for handling production, processing, coordination, and distribution services (Radack, 2011; Lu *et al.*, 2014). Essentially, an ICS comprises of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that collaboratively operate to realise an industrial objective (Stouffer *et al.*, 2015).

The basic functions of ICS involve: sensor measurements, hardware control for actuators (breakers, switches, monitors), human-machine interfacing, and remote diagnostics and maintenance utilities (Amin and Sastry, 2015) (Nicholson *et al.*, 2012b). These are enabled using a collection of network protocols at varying levels. The control system may be designed to operate open-loop, closed-loop, and (or) manual mode. In an open-loop, predefined settings control the system's output. In closed-loop, the control system output has an influence on the input to sustain the desired objective. The manual mode describes the outright control of the system by humans solely (Stouffer *et al.*, 2015). Figure 1-1 shows the architecture of a typical ICS comprising of the core components and connection to IT networks. These include the supervisory control centre, the field control, and physical process, all connected via a communications gateway.

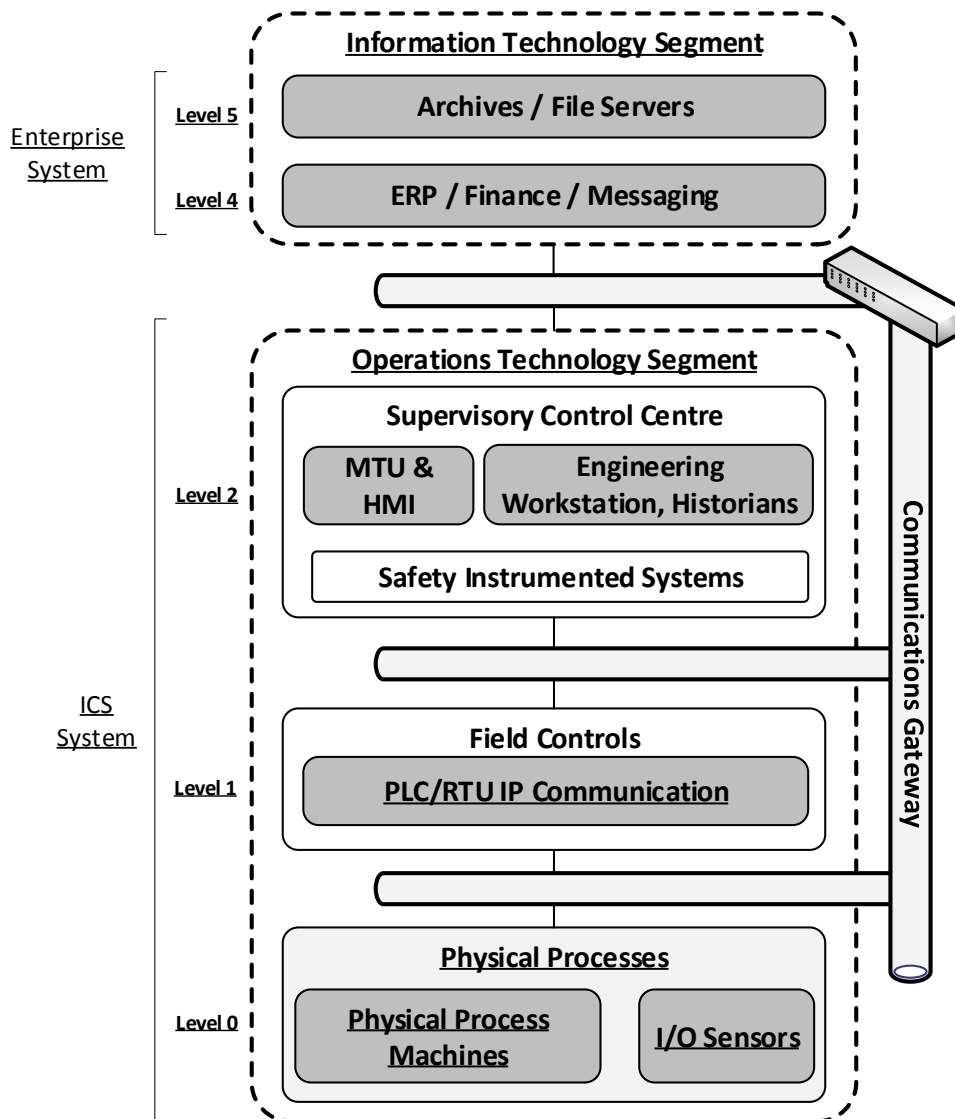


Figure 1-1: Layered Architecture of a Typical Industrial Control System (Source: Author)

The supervisory control comprises of industrial components that handle control initiations and monitoring such as master terminal units (MTU), human-machine-interface (HMI) device, engineering workstations, historians, plus safety instrumented devices.

The field devices include programmable logic controller (PLC) and other control maintenance components used to automate control functions through the network. Physical process comprises of machine, actuators, sensors and I/O ports connected to physical equipment to accomplish input and output processes. The communication gateway comprises of local/wide area network components, routers, switches, satellite, etc, through which communication exchange is facilitated amongst the network

components. This is the bridge, allowing the OT system to communicate with IT systems, which include ERP, finance, and administration, file servers, messaging, and archives.

An Industrial Control System Environment (ICSE) refers to a domain where industrial control operations and processes are performed. ICSE is comprised of a collection of entities that function, operate, interact, and collaborate towards achieving a set of industrial objectives(s). These entities often involve collection of technology assets that interact over a network, a set of humans (operators, designers, developers, user, etc.) that use and interact with the technology assets by supplying inputs commands or responding to output instructions, and an array of processes enabled by the integration of the functions, operations, and interactions between human and technology assets.

1.1 Research Background

1.1.1 Evolution of Industrial Control Systems (ICSs)

In the past, Industrial Control Systems (ICSs) were operated in secluded setups in a process technically referred to as '*Air-gapping*' (Gold, 2009; Neg *et al.*, 2016). ICS system and networks used only trademark protocols and were totally isolated from other networks (Dumont, 2010). The components in use were typically designed without security considerations. Design and development priorities were rather focused on performance, productivity, reliability, flexibility, and safety (Honeywell, 2011; Stouffer, Falco and Scarfone, 2011).

However, the desire to automate manual functionalities in control of industrial processes brought about the increased use of computers, networks, and the internet to leverage high performance efficiencies (Wells *et al.*, 2014). The ill-fate is that the potentials for misuse came inclusive in the new convergence between IT and traditional ICS (Alcaraz and Zeadally, 2015; Bartman and Carson, 2017). The manufacturing ICSE is one of such notable areas where cyber security threats and vulnerabilities are growing issues. Clearly, a threat in cyberspace implies a threat to all that rely on cyberspace for normal operations. Hence, implementers of ICS in the cyber domain are now seeking ways of ensuring security and safety while remaining operational.

In this research thesis, 'Cyber security' and 'Security' are used interchangeably with the same meaning. From NIST's Glossary of Key Information Security Terms (NIST, 2013a), 'Cyber security' is defined as "*the ability to protect or defend the use of cyberspace from cyber-attacks*". Modern (ethernet/cyber-enabled) ICS infrastructures need to be protected to ensure that they are not rendered unworkable by the nefarious activities of malicious attackers, who have continued to show that no system is beyond reach or impenetrable. Every prospective disruption or damage ensuing from a cyber-attack on an ICS asset may well be as significant as the loss of revenue, or damage to brand reputations. The targets and numbers are evident.

1.1.2 Industrial Control System Security Vulnerability and Attack Trends

The first popular attack incident against an ICS infrastructure termed a '*logic bomb*' targeted the Supervisory Control and Data Acquisition (SCADA) system of a Russian Gas Company. This caused a massive explosion and damage to the Tran-Siberian gas pipeline (Dickman, 2009). More recently (2010), 'Stuxnet' worm targeted and successfully infected Programmable Logic Controller (PLC) systems in an Iranian nuclear plant. Stuxnet caused centrifuges to spin faster and out of control while evading monitoring and alert system controls. This damaged one-fifth of the overall working centrifuges; putting them out of use in a time earlier than expected, and setting back the Iranian nuclear program (Sadeghi, Wachsmann and Waidner, 2015). The 'Shamoon' Saudi Aramco spear-phishing attack compromised over 30,000 computers (Leyden, 2012). The combined 'spear phishing and social engineering' attacks on a German Steel factory (Paul, 2014) aided the compromise of production network devices and damaged factory equipment.

These exploit and compromise phenomena seem to be increasing as vulnerabilities increase with time and technology evolutions (Andreeva *et al.*, 2016a). Figure 1-2 indicates a steady increase in the number of ICS vulnerabilities from less than 10 in 2003 to over 170 in 2015. Similarly, recent security survey reports (IBM Security, 2015; McMillen, 2016) summarised in Figure 1-3 indicates a steady increase in the number of attacks against ICSs from about 600 in 2013 to nearly 2700 in 2016. The 2014-2015 Computer Science Corporation, Global CIO Survey (CSC, 2014), reported that 76% of the manufacturing ICS respondents noted that emerging innovative technologies such as 'Industrial Internet-of-Things' (IIoT) were of critical priority following the increasing

enthusiasm by manufacturers to interact with real-time production and consumption data. With IIoT, more industrial infrastructures are continually being connected to the Internet; establishing presence in the cyberspace.

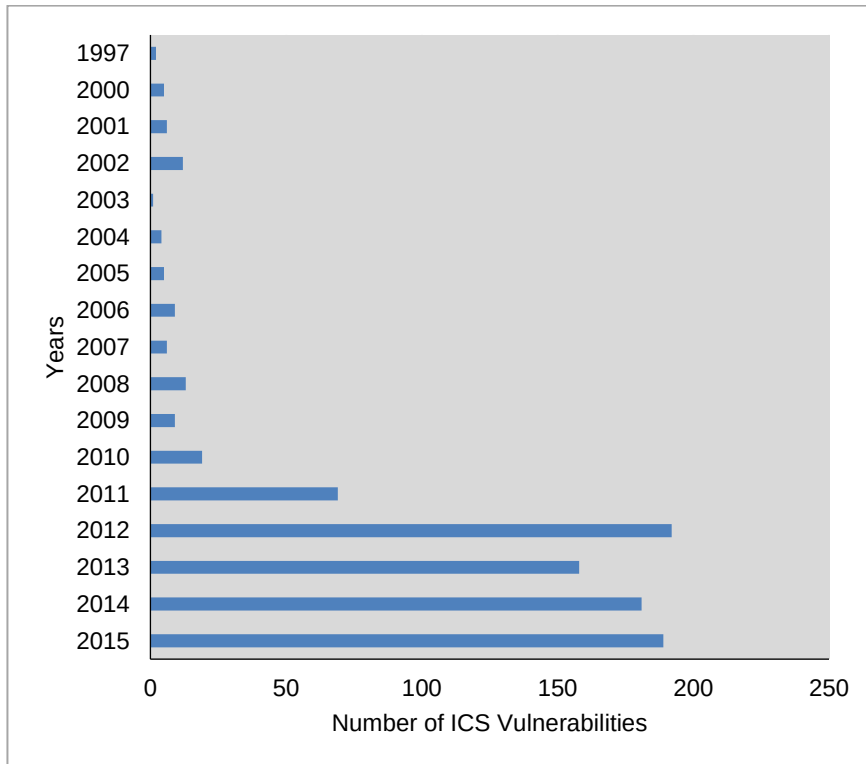


Figure 1-2: Increasing Number of ICS Vulnerabilities

Source: (Andreeva et al., 2016a)

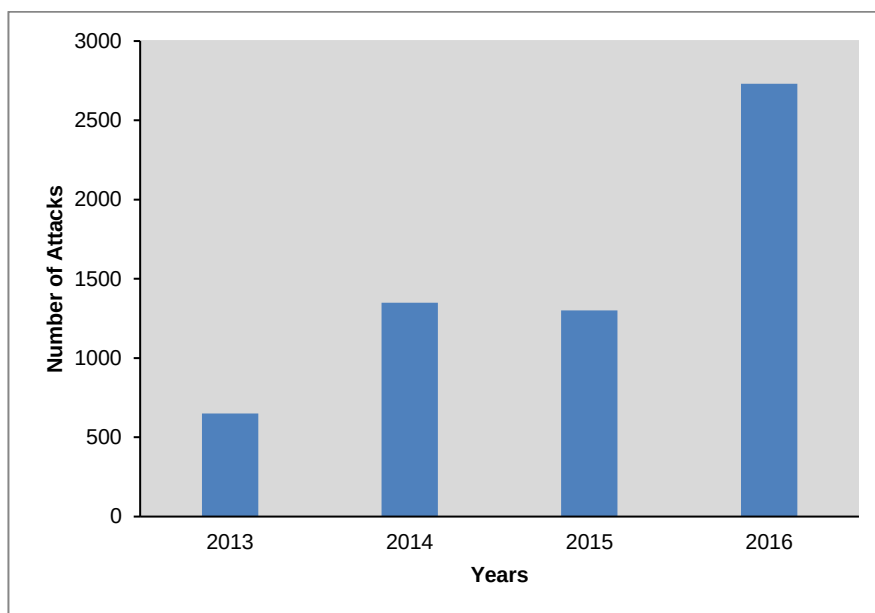


Figure 1-3: Increasing Number of ICS Attacks

Source: (IBM Security, 2015; McMillen, 2016)

As interconnectivity and convergence continue to grow, insecurity seem to follow similar trend, and projections are that malicious activities will likely follow the same growth trend while attack feasibilities may dwindle (Wells et al., 2014). Virtualisation, Bring-Your-Own-Device (BYOD), Mobile Computing, along with other emerging IT trends and technologies, while beneficial, have unlocked numerous security vulnerabilities and risks that make ICSEs easily exploitable by cyber-attackers (Radack, 2011; Rautmare, 2011; Brenner, 2013).

According to Wells *et al* (2014), what is more worrisome is that as the number of cyber-attacks grow, the attack visibility potentially declines, while their damaging capacities increase. Generally, trends suggest that increasing connectivity and integration of traditional ICSE (assets, protocols, and networks) with IT capabilities appears to increase security vulnerabilities and risks within the ICSE. Although performance, productivity, reliability, high-tech monitoring, and maintainability are improved by the ICS-IT connectivity and integration, the resultant system often yield vulnerable and insecure configurations. Figure 1-4 shows the evolution of ICS from its original state of being solely isolated from external networks, to a state of convergence with IT to improve operational and service performances, but also introducing security vulnerabilities.

1.1.3 Industrial Control System Security Enablers and Operational Efficiency

Following from the current trend, cyber security has become a fundamental requirement for ICSEs to function and operate safely. Implementing security for this system also comes with tough challenges. Computing and IT security control measures are fairly developed and standardised. However, IT security controls and measures cannot be totally and directly applied to ICSEs without some form of modifications. This is due to several differences between the two which bordered on security and operational requirements and prioritisation (Macaulay and Singer, 2012). The authors (Macaulay and Singer, 2012) argued that nearly all ICS security compromises have associated physical consequences and impacts. These are often more severe and abrupt than in the IT domain.

The main reasons for the difficulty of ensuring the security of ICSE include: vastly dispersed assets with frequent compulsory remote access requirements, traditional IT

security applications such as antiviruses and firewalls may not be suitable for compatibility issues, and when possible, application could affect system availability which is not acceptable for ICS as a high-availability system. Older ICS systems are often not open to patching or upgrades (Macaulay and Singer, 2012; Drias, Serhrouchni and Vogel, 2015). Cyber security threats to ICS encompass threat vectors like non-typical network protocols and instruction sets that cannot be blocked, as they were not designed with the concerns of security.

Technical control may be easily subverted by intelligent adversaries, who can easily deceive unaware, unskilled, and unsuspecting ICS operators and users into undertaking actions and activities that can grant the attackers easy access and high privilege capacities to execute their malicious intents. These are often also undetectable by security alert systems until serious damages and anomalies begin to emerge (Johansson, Sommestad and Ekstedt, 2009; Fan *et al.*, 2015).

The above issues in ICS require the development and adoption of domain-specific security approaches to ensure and improve cyber security in the industrial domain. Enhanced and tailored efforts need to be built on the knowledge and understanding of emerging security threats, vulnerabilities, attack patterns, impacts, security methods, areas of weaknesses and non-conformities, which may require modifications and improvements.

To achieve and sustain a more secure and safe operational ICSE, *People, Process* and *Technology* (Figure 1-5) key system collaborating elements should be considered (King-Turner, 2014), since they are prime to the 'success' of every operational electronic IT/ICS system, from Business development (King-Turner, 2014), to Operations and Performance Efficiency (Emerson Network Power, 2013). Success in this case implies effective operations that bring about the attainment of desired or predefined system and(or) service objectives without any form of undesirable impediments, interruptions, or modifications.

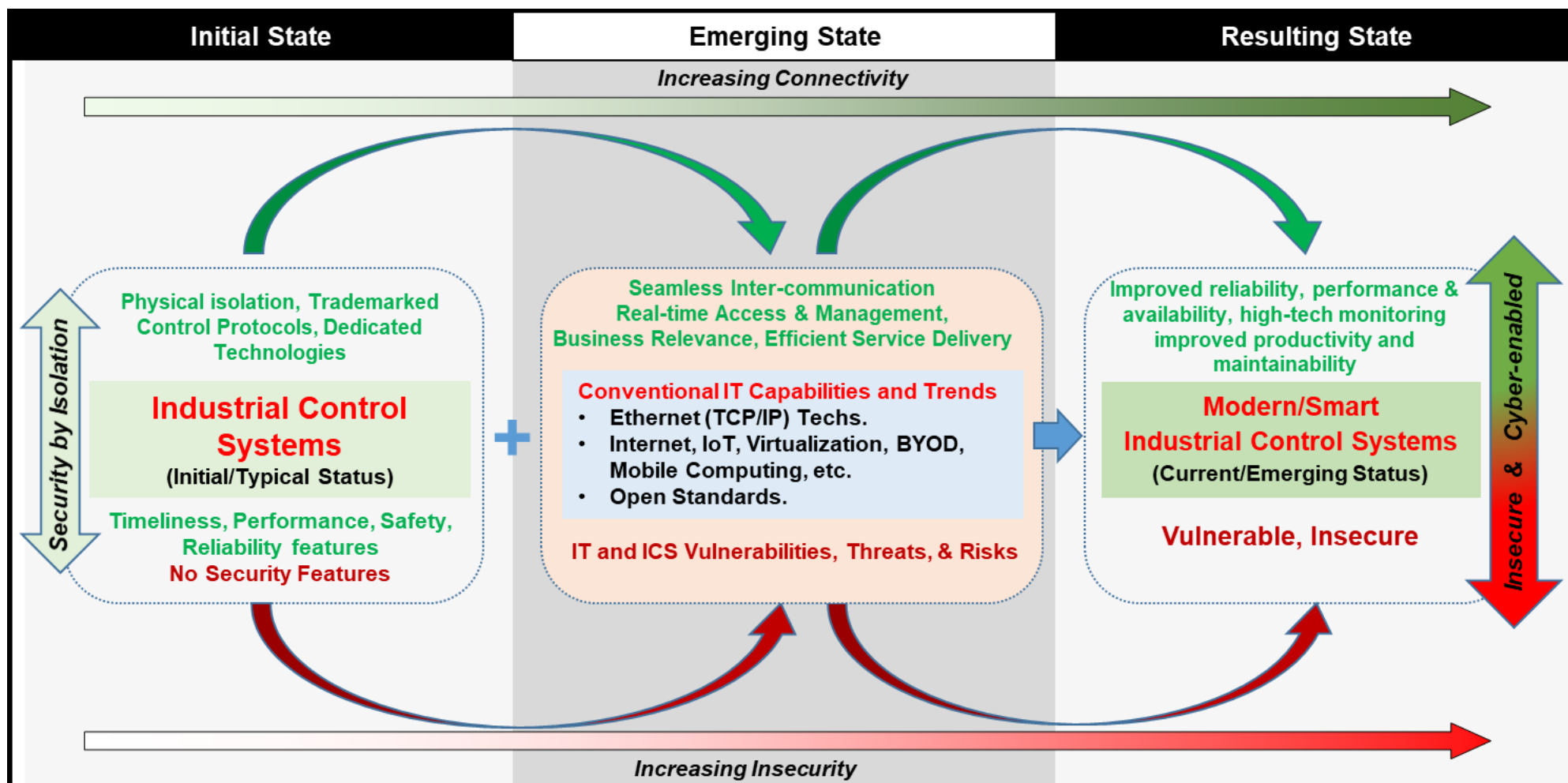


Figure 1-4: The ICS Cyber Security Trend (Source: Author)

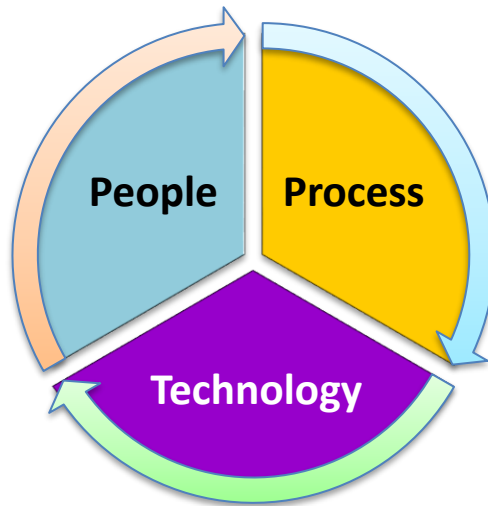


Figure 1-5: Three Functional Elements of Industrial Control System Environment

1.2 Research Gap

The industrial control system environment has become more attractive targets to cyber-attacks across the three collaborating elements: people, technology, and process (Ani, *et al.* 2016). Generally, the convergence of varied initially separated technologies and protocols into modern ICS has introduced more functional complexities which have also impelled the pressure from security and privacy legislations to obtain necessary justifications for security features and solutions (Savola, 2009). Evidence to support such security justifications can easily be obtained from the application of systematic security analysis and evaluation guided by effective metrics development approaches. This research addresses some of the gaps identified from reviews of existing security solutions for ICSEs. The gaps are quite related in that they seek to address different aspects of ICSE security vulnerability and impact evaluations, which can collectively contribute to engaging a more strategic security control implementation. From the point of using domain-specific security metrics methodology to generate appropriate metrics, to the point of applying quantitative evaluation of vulnerability, capability and impact from both technical and human-factor dimensions to support more precise and effective risk mitigations in ICSEs. The specific research gaps addressed in this study include:

- i. Currently lacking and needed is an ICS-specific security metrics methodology for metrics generation that considers the multi-entity nature of ICSEs – including people, process, and technology elements and attributes (Fruehwirth *et al.*,

2010). Metric attributes related the target system segment, applicable security objectives and control capability direction, and measurement formats need to be well clarified when deciding on an appropriate metric for understanding certain security contexts. This will provide ICS security auditors with options and capabilities to derive metrics and measures for wider or narrowed security evaluations, and which aligns with relevant standards such as the NIST SP 800-82 (Stouffer et al., 2015).

Existing metrics generation methods are more inclined towards IT applications and cannot be directly adopted for ICS due to differences in the prioritisation of security objectives. There is the need for methods which can guide organisations that run ICSs in the unambiguous outline of their security objectives, identification of appropriate metric quantities for evaluating their desired cyber malicious attributes (Fruehwirth *et al.*, 2010; Barabanov *et al.*, 2011). For example, the method with nearest relevance to the contexts mentioned is the technical-centric security metrics development model for SCADA (TSMM SCADA) (M. P. Azuwa *et al.*, 2012). However, TSMM SCADA focuses on metrics for technical security controls alone, and does not consider people and(or) process security control metrics. This falls short in that it ignores the crucial aspects of human-factor and process security metrication which are very crucial and contribute to an overarching assessment of vulnerability and security within an ICSE. There is a limitation to use such existing approach for security metrics development specified for ICSEs.

- ii. From a technical security perspective, vulnerability analysis is a common method used to quantitatively evaluate and rank security severities and determine suitable countermeasures. However, there is the need to effectively address a further issue resulting from the above, which involves more precisely resolving the uncertainties in severity prioritisation; enabled by the multiplicity of the same vulnerability in different technology assets, and the same severity ratings for different vulnerabilities within the same system. This problem seem to be caused by the use of single and static severity ratings and attributes alone for vulnerabilities, without considering the effects of environmental factors and other external influences such as functional dependencies and impact cascades (Kheir

et al., 2010; Wells *et al.*, 2014). Here, 'effective' implies an ability to consider multiple dynamic attributes of security vulnerabilities especially in relations to their lifecycle and host environment changes while undertaking an impact analysis. In ICSE, considering multiple and dynamic vulnerability attributes such as functional dependency index during security analysis can help provide a much more precise quantification of severities to resolve the uncertainties and improve decision-making for countermeasures.

- iii. The need to quantitatively assess the security capabilities of the human-agents (workforce) within an ICS operational environment can proffer a much more precise indication of security adeptness in a way that is new and shifts from the typical qualitative approach. This implies an ability to analyse human-related security vulnerabilities in the ICSE such as skills and knowledge, and quantitatively estimate users' security capacities for appropriate response and control and identifying the most vulnerable users within a group. This can also simplify the process of engaging strategic security measures and controls related to human-related vulnerabilities. This measure is significant contributory towards achieving efficient workforce security consciousness and characterisation, as well as support overall organisational security posture enhancement (Navarro, 2007; Beautelement *et al.*, 2016). While the gap in (i) addresses the issue of security metrics methodology development with scope covering people, process and technology aspects of ICSE, this gap more specifically focuses on the application process for quantifying security knowledge and skills human-factor attributes of the workforce to support decision-making.
- iv. There is the need for an operational security risk assessment and mitigation approach that considers and combines both technical and human-factor attributes into a single and purposeful ICSE security risk control (Cherdantseva *et al.*, 2016). Again, this differs from the gap in (i) in that it focuses on risk reductions methods that considers technical and human risk factors, to provide a wider and more precise view of security risk evaluations and the analysis of the extent of control capacities achieved post implementation.

This study adopts a socio-technical, risk-based, metrics-driven security improvement approach in line with NIST SP 800-82 v2 (Stouffer et al., 2015) recommendations for effective ICS security. This approach will contribute an in-depth security analysis procedure with the compliance of NIST ICS security. The NIST guideline recommends that industries running ICSs must develop risk evaluation models and processes that can adapt to their operations and business objectives, and effectively resolve identified security risks based on organisational priorities that account for both internal and external constraints and dynamics. Security risk assessment processes and models should be interactive and iterative in response to the evolutionary nature of cyber threats in ICSE.

1.3 Research Aim and Objectives

The aim of this research is to develop a security risk reduction framework that incorporates dynamic technical and human-factor vulnerability attributes and metrics to support a more precise prioritisation of controls based on ranked estimates of impacts, and improvement of cyber security in Industrial Control Systems Environment (ICSE). In order to reach the aim, this research will achieve the following objectives:

- i. To learn the current state-of-the-art in cyber security risks (threats, vulnerabilities, attacks, impacts and control techniques) of industry control systems environments (ICSEs), identify current research gaps, and demonstrate the feasibility of performing denial of service and privilege escalation attacks on an ICS network.
- ii. To develop an ICS-specific security metrics development framework that considers technology, people, and process elements of ICSEs to support the generation of suitable metric quantities for security assessment.
- iii. To develop a quantitative vulnerability impact estimation method that combines multiple vulnerability attributes (dynamic severity, attack probability, and host component dependency) to resolve the uncertainties in prioritising security control measures in an ICS network.
- iv. To develop a quantitative method for evaluating industrial workforce (human) cyber security capacity based on security knowledge and skills to identify the least capable workforce and the security area(s) needing improvement.

- v. To propose a security risk reduction framework that integrates both technical and human-factor attributes and evaluations to improve security in ICSE.

1.4 Research Scope and Limitation

The research is to address the operational cyber security of industry control system environments (ICSEs) in regard of measurement, governance, and reduction of cyber risks. The ISO/IEC standard 27000-4 (ISO/IEC, 2018) and NIST's security metric guide (Chew et al., 2008) provide general qualitative models that describe variables/concepts in the security domain and how these concepts relate to each other. They defined how an organisation should develop and maintain a measurement program for information security management, but do not define the actual measurements that can be made quantitatively and/or qualitatively in terms of various security scenarios. These two documents provide the theory framework for this research on the operational cyber security of ICSEs exploring improved security vulnerability and risk reduction approaches.

In particular, the underpinning theory guiding the study is built on the submission that; while in security evaluation, considering and combining vulnerability-related attributes of ICSE technical and human elements can yield a criticality and impact estimation that will be a much more precise representation of the dynamics of security risk, and to support effective prioritisation and application of security controls. Examples of vulnerability of interest include: buffer overflows due to low processing power, vulnerable operating system platform (e.g. Microsoft Windows), weak authentication bypass, and improper input validation in technology elements (Yusta, Correa and Lacal-Aránegui, 2011; Ani, He and Tiwari, 2017). Others include; a lack or low security awareness, lack or low security response skills in human elements in ICSEs. These vulnerabilities are noted to be more widespread in ICS components and networks (Andreeva et al., 2016a), and represent the most typical and common concerns in the study domain (Pasqualetti, Dorfler and Bullo, 2015). The research is not designed to cover other ICS vulnerabilities such as cleartext transmission of sensitive information, SQL injections, Use of Hard-coded credentials, cross-site scripting, malware (e.g. Stuxnet) injections, and unrestricted file uploads. Aspects related to intrusion detection, and protocol security analysis are also not covered within the scope of this study because of time constraints of the research.

The study covers security metrics framework development which considers technology, people and process elements of ICSE, and necessary for generating relevant security metric quantities for security evaluation. It also covers security risk assessment and mitigation via technical and human-factor (people) vulnerability and impact analysis.” The results could be used by security analysts, security auditors, security risk assessors to identify and use the appropriate metric quantities that suite their unique security assessment needs. The model achieves this by providing the factors and guiding principles to consider in the metrics generation process to yield outputs that relate to desired security contexts. This will in turn support efficient security monitoring, prediction, and decision-support for risk managers and top management executives as they strive to improve security in their ICSEs.

The technical aspect focuses the quantitative analysis and estimation of security criticalities of identified vulnerabilities and based on dynamic attributes and scores from the Common Vulnerability Scoring Scheme (CVSS) (Franklin, Wergin and Booth, 2014), attack probability and vulnerability host component dependency values. These factors and details obtained from a testbed allows for the testing and study of cascading impacts due to the exploitation of technical vulnerabilities and determining associated security control measures.” The testbed is representative of a small machine shop product/item conveyor control system comprising of actual industrial-grade control hardware, software, and services in the form they are configured in practice. It captures the basic architectural components of ICS and reflects the basic control functions and processes inherent such system. The physical process component is represented using a toy conveyor system robot with sensors and actuators which is representative of the functions of actual physical conveyor machine system.

The aspect of human-factor (people) covers the quantitative assessment of the security capability and vulnerability of human agents (workforce) in an ICSE based on their security knowledge and skills attributes and in line with prescribed policy(ies) and standard(s). In this study, the NIST SP 800-82 v2 (Stouffer et al., 2015) standard, and the UK ‘10 steps to Cybersecurity’ good practice guide (UK-Cabinet-Office, 2012) were used. A method for achieving the evaluation based on these factors, policy and standard is explored. The process element is only considered from the perspective of the interactions between the people and technology elements. The direct assessment of

process element attributes is not in the research scope. Implicitly, improving security capacities in technologies and people could help improve security capacity of the physical processes.

In the industrial facilities and setups of a small machine shop product/item conveyor control system and the security guidelines in NIST SP 800-82 v2 and the UK '10 steps to Cybersecurity' guide, this is particularly important, for example, a shop floor automation engineer typically interacts with control system workstation to programme sensing and actuation control on a PLC to drive processes on conveying machines. The engineer also interacts with HMI to monitor ongoing processes as the run. Such engineer's inability to timely recognise security anomalies related to unsolicited emails, credential requests, access to workstations, patches and updates to PLCs, or control activation or deactivation on HMIs, can cause the engineer to act inappropriately away from precautionary or reporting actions that can deter any maliciousness. However, efficient and timely recognition and actions against the compromises mentioned would depend on security knowledge and skills. Drawing lessons from the popular security breach against Target Corporation, it is noted that Target's security technology detected the breach, but the human agents who should have applied security responses to control the attack impacts, lacked the necessary skills and knowledge (Hershberger, 2014). Thus, the characteristics of the interactions between the people and technology elements are shown in these types of scenarios that open-up vulnerabilities, and where human actions or inactions as part of a security or operational process on the small machine control system can make or mar cyber-attacks.

The study involved critical reviews of cyber security issues in ICSEs covering; evolving security threats, vulnerabilities and attack patterns, security metrics methodologies, vulnerability-driven impact assessment, human-centred capability/vulnerability evaluation techniques, and security risk mitigation. Critical reviews of existing security analysis techniques covering architectural design, attack detection, attack modelling, attack categorisation, and strategy implementation were also carried out.

The study also includes attack simulations on a developed ICS testbed, and is representative of the attack modelling technique. The testbed approach is used as a medium for testing and validating the outcomes of the research." Literature suggests that the importance of simulating attacks such as: denial-of-service (disrupting

communications), deception attacks (controller hijack or manipulation), replay attacks, protocol forgery attacks, and firewall exploitation attacks for a machine shop product/item conveyor control system and security guidelines such as NIST SP 800-82 v2 and the UK '10 steps to Cybersecurity' guide, can support understanding how vulnerabilities can negatively impact on normal functionality and operations, affect productivity and other potential consequences. The testbed is designed with the top 2 scenarios of the attack list.

The testbed design is demonstrative of a small machine product/item control-based conveyor belt system/network covering the control centre, the communication architecture, the field devices and the physical process, which form the basic architectural characteristics of a typical ICS network as defined in NIST SP 800-82 Revision 2 (Stouffer et al., 2015). This is characteristic of the basic technology-oriented functionalities that can be found in an ICS and chosen because it represents a sectional process in manufacturing. Manufacturing is one of the most targeted sectors for cyber-attacks, especially in the UK (DeSmit et al., 2016; Chapman, 2018). Thus, the testbed design chosen provides a good platform for investigating security vulnerabilities and attacks related to a part of manufacturing, and to come up with solutions that can address (reduce) the prevailing security issues in this and other sub-sectors of manufacturing.

The testbed is designed to be able to address specific types of attacks limited to: (i) denial-of-service (DoS) via traffic flooding (buffer overflows) of field device components such as the programmable logic controller (PLC) and extended (input/output) module devices, and (ii) deception attacks such as process hijacking via the direct compromise and escalation of privileges on control centre computer/workstation. They are chosen for two reasons: (i) to capture the two dimensions of attacks feasible on ICSEs, i.e., insider attack and outsider attack. DoS attack represents an outsider attack, while the process hijack is viewed as a form of insider attack. (ii) because they represent the most frequent and common concerns in the ICSE in relations to the damaging impacts they cause (Pasqualetti, Dorfler and Bullo, 2015; Andreeva et al., 2016b). Hence, demonstrating these attacks can lead to insights into how attackers act, and help ICSE security managers and administrators to understand how to proactively control or mitigate the attacks.

The DoS attack aims to target and exploit any vulnerability on the designed testbed PLC or Network Switch related to Resource Exhaustion via a vulnerable network port, for example Port 80. The process hijacking attack aims to target and exploit any vulnerability on the testbed related to backdoors and design flaws in control system software which can enable unauthorised access to the affected system and allow for the lock-out of authorised users and alteration of preconfigured processes and operations on the testbed. Although emerging design policies and updates are being put forward to shut identified backdoors, however, these are vendor-specific and are often not included in former products and burden of implementation are left on the users. Again, patches or updates have been seen to open up new flaws, and even corrupt ICS components (Leyden, 2018). Thus, it is important to test ICS components and networks for available flaws even after implementing certain updates or security policies to find out if other/newer flaws exist, and how to fix them.

The general understanding of the two testbed scenarios such as the aspect of target profiling, tools for vulnerability assessment, tools and techniques for exploitation are quite published and are known knowledge particularly in the IT domain. However, in employing these attack simulation scenarios, the study aims to use the outcomes to investigate an aspect of security impact assessment which has not been considered. This aspect involves finding out how the topological link amongst components within an ICS network and their functional dependency attributes can affect the impact estimates of vulnerabilities. Also, to explore how such information when obtained can help to achieve better prioritisation vulnerability controls based on evaluated cascading impacts to improve security decision-making. Thus, the information gathered from these attack scenarios can help the development of appropriate impacts assessment and security reduction methods for ICSEs. The testbed operations and attack (DoS and deception) scenarios only addresses technical vulnerability attributes and do not include any human-technology interaction attributes. Human-factor vulnerabilities are not directly considered in the testbed. These are derived from the evaluation of data collected from sample ICS workforce respondents.

The results from initial reviews and cyber-attack demonstration both provided insights that guided the development of security frameworks and methodologies to support the enhancement of cyber security in ICSE. The testbed also provided the platform for testing and validating the technical vulnerability and impact estimation method proposed. A use case scenario and data from sample ICSE workforce was used to test and validate the human-factor security capability evaluation model. This is further consolidated by expert opinions. The results from these studies will be beneficial to security auditors, assessors, analysts, and managers. It will improve the process of analysing and prioritising both technical and human-level security-related vulnerabilities and impacts and increase their confidence in adopting the appropriate security controls to achieve the best possible security improvements in ICSEs.

Other human-factor attributes such as security culture, attitude, behaviours are not considered within this scope of work. This is because of the difficulty of deriving direct human adeptness from these factors, and the time constraint to handle the qualitative research activities that may be involved. The study does not include translating developed framework and evaluation methodologies into automated (online) software tools. The analysis and improvement of business-wide economic security impact is not within the scope of this study too.

The results of this study will benefit both the academic and industrial communities. ICS academic research community will benefit from the understanding that changing technologies and attack trends means that security risks are no longer confined to technical vulnerabilities alone. But includes vulnerabilities from human agents. Thus, this research will spur developments of new security techniques and approaches (architectures and protocol developments) that consider both technology and human risks to enhance security. This will bring and keep the academic community in-tune with security trends and developments in modern ICS domain.

With the results of this research, ICSE security practitioner community (security analysts, assessors, administrators and managers) will be better informed about how multiple technical and human-factor attributes can be used to evaluate and address security vulnerabilities and impacts. These workforce group will be furnished with the information that will enable them to make the right decisions about the metrics methodologies to adopt, the security metrics of importance, the security risks to address

to achieve highest possible security based on prioritised scale of impacts on industrial operations. This way, the cost of security risk management can be significantly reduced, and implementation also reduced. This is against the typical all-inclusive security management approach being adopted in the industrial environments. It will motivate and influence the change/modifications of viewpoints and policies in organisations where emphasis have been more on technology security. It will provide the motivation to include both technical and human-factor aspects in security risk assessments for better security outcomes.

1.5 Research Justification

Cyber security has become a critical goal of ICSE, as required by Industry 4.0. Although security control efforts have been made to mitigate cyber threats to ICSE, cyber incidents are still happening. There is a need for new methodologies for security evaluations to mitigate cyber-threats and improve security in ICSE. This study is motivated by the need to improve the security of ICSEs where industrial organisations run advanced ICSs enabled by IoT for improving performance and productivity and increasing the global competitiveness. The research will be furthered by providing details about existing security control approaches and their limitations towards achieving effective security.

A testbed is a suitable approach for this because; it provides a way for evaluating the performance or behavioural degradation of ICSs while undergoing cyber-attacks (Candell Jr., Zimmerman and Stouffer, 2015). A testbed provides an easier and more valid understanding of cyber-attack feasibilities and their implications on control system networks/processes, thus guide the development and implementation of effective security countermeasures (Candell Jr., Zimmerman and Stouffer, 2015; H. Holm *et al.*, 2015; Kavak *et al.*, 2016). It also provides a strong path towards validating the output of the research since it mirrors the realism of industrial control environments, providing a high level of results credibility (Stouffer *et al.*, 2015). Therefore, a small machine shop conveyor industry control system is developed as a testbed. The basic operations of ICS networks to simulate include; sensing, actuation, control, and monitoring operations in line with NIST SP 800-82 Rev 2 (Stouffer *et al.*, 2015). The values of the testbed include: firstly, testing the feasibility of attack scenarios to demonstrate the importance of this research; secondly, it will support the analysis of security risk attributes, such as

vulnerability severities and impacts, and validate the research on vulnerability impact analysis; thirdly, the testbed will also provide a practical use case for exploring the new theories and knowledge in the combination of multiple dynamic attributes related to security vulnerabilities and their host assets to achieve a better estimation of security criticalities and impacts. This helps to identify the most critical technology assets, and proffer basis for prioritising security efforts based on the estimated impact magnitudes of vulnerabilities.

Other validation mediums employed in this research include: scenario-based formative decomposition (Frechtling, 2002), and expert opinions (Perumal, 2014). These are used to validate the research on framework for security metrics generation. The scenario-based formative decomposition helps to test the applicability and effectiveness of the research outcome to guide the generation of appropriate security metrics in ICSEs contexts. This is further consolidated by expert-based opinions on the suitability, usability and workability (Dodig-Crnkovic, 2002; Freitas, 2009) of the research outcome. These validations will help support new concepts and associated value in clarifying the security dimensions, segments, target constituents, security requirements, control capabilities, and measurement formats, in metrics generation to obtain appropriate security metric quantities. They also underscore the significance of considering good metrics framework characteristics.

A test-based approach (Gilbert, 2008; Robson and McCartan, 2015) involving cross-sectional data collection (Perumal, 2014) is also used in this research to validate the research on human-factor security capability evaluation. This is explored through collection and analysis of data from actual human subjects with work affiliates to ICSEs. This will provide data which is representative of the scenario/condition that may be found in the ICSE, and which can be used to demonstrate the application and impact of the methodology adopted. Thus, this brings to light the significance and contribution of human security knowledge and skills capability/vulnerability evaluations to the overarching goal of improving security in ICSEs.

The outcome of these validations put together are used to further the research and validation of the work on security risk reduction in ICSE. By identifying vulnerabilities in both technology and human-elements of ICS, analysing associated severities and

impacts, applying suitable controls to reduce the vulnerabilities and impacts; security can be significantly improved.

1.6 Thesis Structure

Chapter 1 presents a background and generalised overview of security vulnerability and control issues in ICSE. The chapter outlines the research aims and objectives along with the scope and justifications.

Chapter 2 presents the methodology for this research and justification in relations to the defined research aim and objectives.

Chapter 3 presents a review of literatures related to ICS security risks (threats, vulnerabilities, attacks, and impacts), security control solutions in relations to metrics development methodologies, vulnerability impact analysis, and security capability evaluation of human elements.

Chapter 4 addresses the development of the PLC-based assembly-line testbed, with which, vulnerability analysis, and penetration testing using attack scenarios was carried out, and the outcomes of such attacks on the testbed were assessed.

Chapter 5 focuses on the development framework of security metrics in relations to ICSE to fill the identified gaps in existing methodologies, and the framework validation.

Chapter 6 provides an evaluation model to assess technical vulnerability, criticality, and impact in an ICS, and demonstrates the usability of the evaluation model on the developed testbed from chapter 4.

Chapter 7 presents the work on human-factored cyber security capability evaluation, and a test scenario for verifying the usability and suitability of the proposed approach.

Chapter 8 provides an ICS Security Risk Reductions framework, with the description of concepts, structures, attributes and validation of the framework.

Chapter 9 summarises the contribution of the research to knowledge, research limitations, and future work.

2 RESEARCH METHODOLOGY

2.1 Introduction

The successful attainment of the research aim and objectives relies on appropriate and well-designed scientific research methodology. This chapter presents a justification of the selected research methods, and discusses aspects covering research purpose, design, strategy, and data collections in relations to adopted research aim and objectives

To achieve the research objectives, the research was structured into three work packages: (i) Understanding the Contexts, and Issues of Cyber Security in Industrial Control System Environments (ICSE), (ii) Security Metrication Framework and Security Criticality Evaluation Models (Reviews, Analysis, Development, and Validation), and (iii) Security Risk Reduction via Security Risk Reduction through Critical Impact Point Assessment (S2R-CIPA) Process Plan. These are structured in line with defined research objectives. Each objective was achieved following the initial review of context, research gap identification, solution development, validation, and the presentation of conclusive results. Figure 2-1 presents the work package indicating the work flow of the methods adopted.

2.2 Work Package 1: - Understanding the Contexts, and Issues of Cyber Security in Industrial Control System Environments (ICSE).

This addresses research objective 1 which involved reviewing the current state-of-the-art in open cyber security issues and demonstrating the feasibility of identifying and exploiting security vulnerabilities in an ICS network to identify research gaps and objectives (Creswell, 2014). This was achieved through a comprehensive critical review (Ani, et. al. 2017) of ICSE security issues and risks.

At this stage, relevant numerous resources materials (journal and conference papers, textbooks, trusted website articles, and security standards, etc.) on ICSE security were reviewed. Key search terms included: cyber-physical security, industrial control system security, SCADA security, ICS cyber-attacks, industrial control system cyber-attacks, ICS security metrics development, ICS/SCADA vulnerability analysis, human-factor security, security risk assessment, etc. Interactions with experts were also engaged to

understand ICSE security state-of-the-art. Information acquired from this were analysed critically based on the scale of suitability ICSEs, and responsiveness to the dynamics such as changes in attack directions and operational requirements.

Initial review of literatures is used to uncover research issues and gaps in previous studies within the same research area (Creswell, 2014). In this study context, it enabled insights into issues surrounding ICSE security, such as; the lack of ICS-tailored security metrics methodologies, lack of human-factor security evaluation methods, elements, and the lack of baseline for understanding and prioritising the control of vulnerabilities from a severity rating perspective. It also provided the necessary background to support the understanding the research context and guided the pathway for the choice of research techniques employed in the succeeding stages of the research.

2.2.1 Cyber-Attack Demonstration

2.2.1.1 Testbed Design Approach

The foundational part of the research design involved the development of an ICS testbed. This was to support the achievement of the second part of objective 1 which involved demonstrating the feasibility of identifying and exploiting security vulnerabilities in an ICS network.

Typically, the best approach would be to use actual (real) ICS networks and environments for the test as this will produce realistic results and insights to support exploring other research objectives. However, significant operational risks exist that make technical security audits such as penetration testing impracticable on real ICS networks (H. Holm *et al.*, 2015). ICS infrastructures are quite weak in withstanding even the most basic vulnerability enumeration tools. Simple probing can crash ICS components such as PLCs (Luders, 2006) within an operational industrial environment. Therefore, applying security research and test activities directly on real ICS is too risky, as the outcomes may well tamper with real industrial/ business processes and operational continuity, or even damage infrastructure. It is safe to consider that the type and scale of negative impacts may be better managed and coped with within a controlled simulation network environment such as a testbed than within a real ICS network operational environment. Thus, environmental replication via testbeds provides a more viable alternative for this type of research (H. Holm *et al.*, 2015).

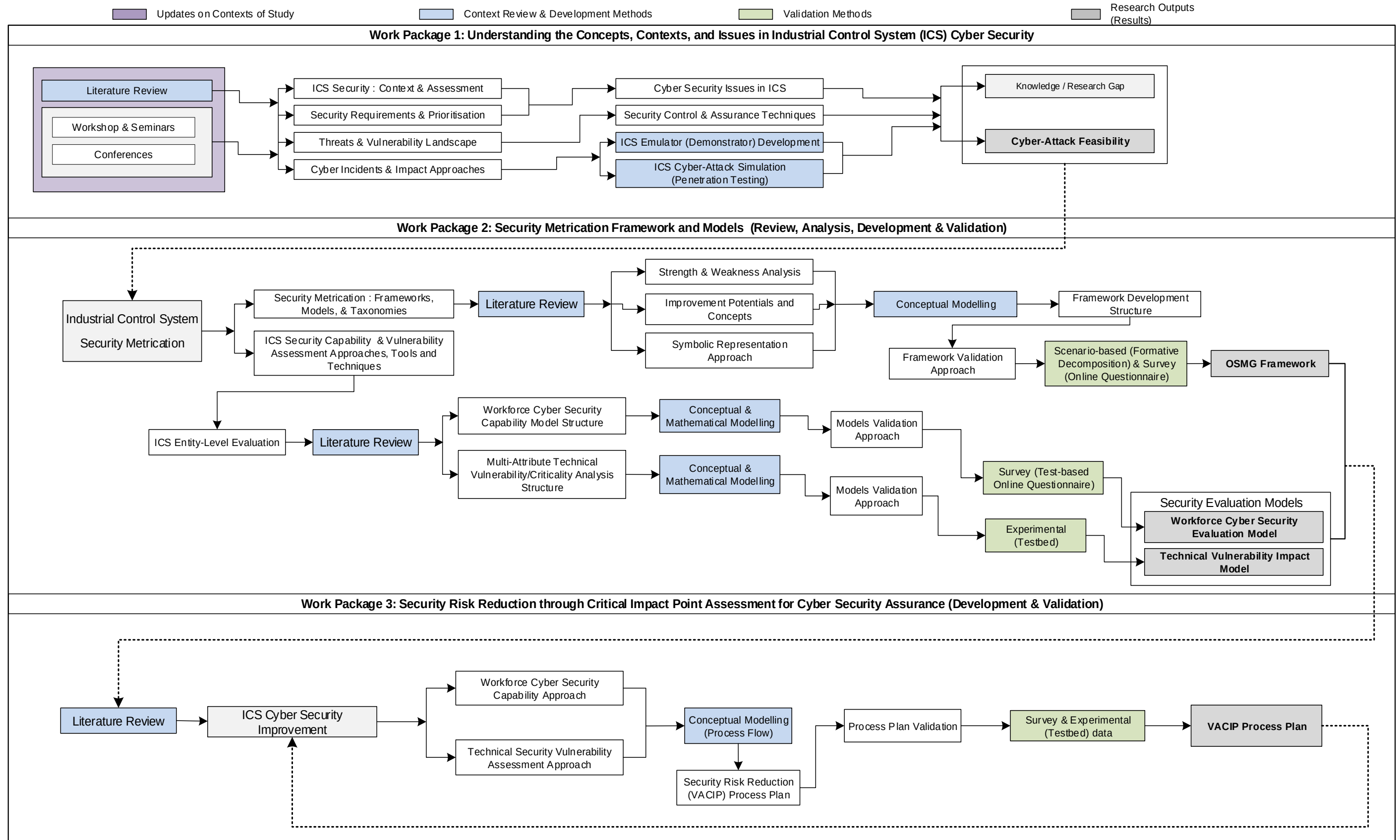


Figure 2-1: Overview of Applied Research Methods

Similar researches (Soupionis and Benoist, 2015; Ahmed *et al.*, 2016; Mathur and Tippenhauer, 2016; Tekeoglu and Tosun, 2017) related to ICS have also used the testbed approach to explore security-related research phenomena, solutions, and improvements. This adoption have been chiefly influenced by constraints related to a non-availability of realistic ICS data and environments (Hurst *et al.*, 2016; Korkmaz *et al.*, 2016).

2.2.1.2 Testbed Design Requirements and Credibility

The negative implications of using actual ICS networks and references to the works and outcomes of prior similar studies informed the choice of research design to include the testbed approach. This involved building an experiment platform of a small-scale shop-floor control system comprising of actual industrial grade hardware, software, and services in the form they are configured in practice. It is developed following appropriate and commonly acceptable testbed structure and characteristics, and against which cyber-attack scenarios can be executed, impacts observed and analysed. Again, the attack scenarios are adopted to represent some past, current, and used to evaluate potential future states. This can go a long way in emphasising the validity and credibility of results.

For research works using ICS testbeds, it is a common requirement that the testbed infrastructure setup should capture the basic functionalities and processes of an ICS, and clearly capturing the four component-level architectural characteristics of: (i) *control centre*, (ii) *communication architecture*, (iii) *field devices*, and (iv) *physical process segments/levels*; over a range of temporal and dynamic time scale (Stouffer *et al.*, 2015) as indicated in section 1.4. To achieve this in the design, it was ensured that for each of the four segments of ICS, an associated device/component was incorporated in the testbed network. Each of the basic processes associated to each segment was also replicated in the testbed process design and configuration using the Siemens' Totally Integrated Automation (TIA) Portal Software tool on available devices, as used in actual environments. Typical ICS functional characteristics of sensing, communication and actuation were be captured as required in commonly acceptable ICS design prescription (Candell, Zimmerman and Stouffer, 2015). Proximity and photoelectric sensors were used on capture and transmit signals on Fischertechnik robots for both movement and punching of objects as a physical process. These signals are received and processed for actuation by a field device PLC with extended I/O modules. The setup and configuration of network

and process behaviour is performed on the Windows-based Control Workstation and monitored by the human-machine-interface (HMI). The exchange of data (information flow) amongst these devices is enabled via a communication architecture enabled by a network switch and cable connectors.

The development of a framework for ICSE security metrics generation (objective 2) was furthered following the understanding of gaps in existing methodologies obtained from literature review (objective 1). Conceptual modelling with block diagrams is used to develop and represent the structure and interrelationships amongst components of an improved framework. Conceptual modelling provides a theoretical method for building representations of tangible or intangible real-world features for the purpose of investigating certain phenomenon (Freitas, 2009; The Open University, 2016). It can be used to develop methodologies, construct logic and semantic models, and to reason about process, procedures, and programs to prove their usability, workability, and correctness (Dodig-Crnkovic, 2002; Freitas, 2009).

For the research on technical vulnerability impact analysis (objective 3) and human-factor capability evaluation (objective 4), conceptual modelling is combined with mathematical modelling (Freitas, 2009) in both cases. For research on vulnerability impact analysis, relevant vulnerability attributes such as severity and probability of attack are often represented in numeric formats. These are used to explore extended modelling while incorporating new attributes like functional dependencies to help derive a more precise estimate of impact and criticality.

For human-factor evaluation research, relevant human-factor security capability factors (knowledge and skills) are drawn from literatures, and mathematical modelling technique is employed for modelling the relationship between them. The models on technical vulnerability impact analysis and human-factor security capability evaluation both combine to form the basis for creating the security risk reduction methodology (objective 5).

Another aspect considered relates to the validity and credibility of experimental design, tests, and outcomes. Key credibility requirements supported by a testbed approach include: *fidelity, repeatability, measurement accuracy, and safe execution of tests* (H. Holm *et al.*, 2015; Kavak *et al.*, 2016). These credibility characteristics were considered and

captured in the testbed design process to strengthen the argument for the testbed's suitability for the research.

Fidelity emphasises the level of correlation between the security simulation model or test predictions and the actual world observations. It relates to the design/model validation method adopted which can include: validation against other simulations designs, validation against expert opinion, or validation against test data (Muessig, Laack and Wroblewski, 2001; H. Holm *et al.*, 2015; Kavak *et al.*, 2016). The testbed in this study adopts the first approach, i.e., in line with prior security simulation designs works, NIST SP 800-82 Rev 2 recommended guide to industrial control system security (Stouffer *et al.*, 2015), and the NIST'S Industrial Control System Cybersecurity Performance documentation (Candell, Zimmerman and Stouffer, 2015). The basic component-level architecture of ICS was captured each with a representative device and process configurations as described earlier in paragraph 2 of this section.

Besides gaining realistic setup and results, *repeatability* is also crucial which refers to the characteristics of ensuring that replicated security test scenarios produce identical or statistically consistent results. To test this feature, 4 experiments comprising of control process activation and network vulnerability assessment were performed at different time intervals (3 days) using 'NESSUS HOME' Vulnerability Scanner. This was done ensuring that all hardware and network configuration parameters were the same. The analysis of the results of these tests on the testbed indicated that the component ID, network, and vulnerability details were the same. Further theoretical analysis and evaluation of impacts depend on these data. However, a significant variation in results was noticed while using NEXPOSE vulnerability scanner, where fewer number of vulnerabilities were discovered. This phenomenon reflects the issue of vulnerability updates in database, which is perhaps less regular in NEXPOSE (being entirely open source) than in NESSUS (being a commercial tool).

Measurement accuracy emphasises an ability to ensure that the process of testing or replicating cyber security test scenarios do not interfere with corresponding outputs. In the testbed use case, it relates to validating the measurement tools used in the attack scenarios. To demonstrate this, testbed network profiling was performed using *Nmap* and *Fping* security tools to scan the network for live hosts and open ports on each host (See

Appendices B-8 to B-12). Result statistics related to *component IP addresses, MAC addresses, component label and device type, and active hosts (hosts that are up)* were gathered and compared to the measurements of network profile data obtained from *NESSUS*. The result was that all the tools provided the same information. Similarly, the vulnerability results discovered in both *NESSUS* and *NEXPOSE* were also compared in terms of their host information, severity ratings and CVSS scores. The results also appeared to be the same.

2.3 Work Package 2: Security Metrication Framework and Security Criticality Evaluation Models

The results from 2.2: work package 1 served as a foundation to the initiation of this second work package. This package encompassed three key research activities: (i) the development of a framework to guide the generation of cyber security metrics for ICSE, (ii) the development of a technology (technical) vulnerability impact analysis model, and (iii) the development of a workforce (people) cyber security capability and vulnerability evaluation process model. Each of these activities are contained in objectives 2, 3, and 4 respectively.

2.3.1 Security Metrics Development Framework

From the review of existing security metrics methodologies, application gaps were identified that made the each of the current methodologies directly unsuitable to be applied to ICS domain contexts. There was a need for an improved security metrics development methodology that would address some of the limitations of existing methods. A conceptual modelling (block diagrams) was used to develop and represent the structure and interrelationships amongst ICS-specific components of an improved framework. These included the analysis of the interplay amongst metrics development stages such as target and objective definitions, as well as how they can translate to the actual metric quantities and their specifications.

In this framework development task, block diagrammatical structures are used for the ease of representation and understanding of interrelationships amongst typical entities and attributes required for security metric development. With reference to ICSE, this supported a simplified analysis and justification of each component of the intending framework. The conceptual development of the framework comprised of the process of clearly indicating

the target ICSE scope and segment for which security metrics are required. Guides to relevant security objectives, metric control capabilities, specific metric quantity selection were presented. Validating the proposed framework involves demonstrating its usability, workability, and correctness (Dodig-Crnkovic, 2002; Freitas, 2009) in relations to an applicable use case. For this, a scenario-based case study that adopted a formative decomposition approach was adopted. It was used to demonstrate the application and validity of the framework to effectively guide the generation of suitable security metrics in the ICSE within any initially defined context.

A second way of demonstrating validity adopted involved gaining analytical feedbacks about perceived validity levels of the framework from multiple experts other than the framework developer. A survey (web-based questionnaire) evaluation approach was used to gain the opinion of security experts and professionals. The questions related to the improved framework's ability to meet the state-of-the-art needs of security metrics generation in the ICSE. Statistical Package for the Social Sciences (SPSS) (IBM, 2013) analysis tool was used to analyse and present acquired data. Degrees of relevance were evaluated based on the framework validity criteria such as scope-delineations, consistency, understandability, ease of use, tailorability, and verifiability, recommended by Beecham et al., (2005), using the data from expert responses. This research also provided an outline of recommended 'good security metrics framework' characteristics.

2.3.2 Technical Vulnerability Impact Analysis

For the technical impact analysis, a multi-attribute vulnerability criticality analysis model was developed. A conceptual model was developed to represent the interplay amongst the metric quantities that encompassed the criticality evaluation process. A graphical model was developed to illustrate how each of the primary components of an ICS contributes to the derivation of numeric values attributed to each component that could be hacked. Using the testbed as a validation platform, vulnerability analysis technique (Johansen *et al.*, 2016) was used to characterise initial severities of vulnerabilities emerging from the ICS testbed. Vulnerability frequencies were used to evaluate associated probabilities of attack, and graph-based theoretical approach (Conte de Leon *et al.*, 2002; Kundur *et al.*, 2010) was used to model the functional dependency of the components in the testbed system. These were combined into the computation for estimating criticality of vulnerabilities. The

proposed model was applied (validated) on the PLC-based assembly-line control system testbed as a case study to demonstrate the model's feasibility and usability.

2.3.3 Human-factor Cyber Security Capability Evaluation

The development of the workforce (people) cyber security capability evaluation process model was also furthered following existing research limitations in human-factor security approaches identified from literature review – see 3.4.4 The need for a quantitative security capability assessment of the human elements within an ICSE is justified by a need to be able to quantify the security states of industrial workers, identify weak links, and use such information to drive effective security control enhancements (Beautement *et al.*, 2016). Relevant human-factor security capability factors that reflect human adeptness such as security skills and security knowledge were drawn from literatures, and the relationship between these factors was identified and modelled. The computational model was incorporated into a larger conceptual process model approach (Freitas, 2009) for workforce cyber security capability and vulnerability evaluations.

The conceptual model was evaluated using a test-based approach using questionnaire-style online tool (Gilbert, 2008; Robson and McCartan, 2015) on real ICSE workforce (personnel) as respondents. A cross-sectional approach (Perumal, 2014) involves data collection from a sample of ICSE workforce, exploration of the behaviour of the model to evaluate security capabilities of the samples, and the use of results to learn about the larger population.

A web-based questionnaire-style test tool was considered more appropriate for the acquiring respondents feedback data to be used to computed for security capabilities. Web-based style was used to resolve accessibility issues by respondents spanning different geographical areas. Test-based dimension was adopted, aligning with the study context, which focuses on evaluating the security abilities of human subjects based on a specific measurable security situation and baseline. The specific scenario relates to the assessment of a subject's security knowledge, and capacity to demonstrate this security knowledge in the form of skills to resolve security situation(s).

Since the validation involved verifying how the proposed model works in relations to evaluating workforce members in the ICSE, security-related data of actual industrial workers (workforce) were obtained and used. The acquired data was fed into the proposed

evaluation model to estimate security capabilities and identify potential human weak-links, as well as potential weak security areas.

2.4 Work Package 3: Security Risk Reduction via Security Risk Reduction through Critical Impact Point Assessment(S2R-CIPA) Process Plan.

The third stage of the study involved adopting a structured security risk reduction process plan that can be followed to achieve improved security in the ICSE. The process plan characterises a combination of technical vulnerability impact analysis and workforce security capability evaluation. Process-flow modelling approach was used to develop vulnerability analysis and critical impact point process. Conceptual analysis was used to demonstrate how the process plan can be used to reduce security risk. The process plan was evaluated using data acquired from phases 1 and 2, to demonstrate the usefulness of the process plan to support the reduction of security risks and improvement of security in the ICSE. A multi-level evaluation process was developed to demonstrate the validity of risk reduction, where reductions in security vulnerabilities and severities were observed from subsequent evaluations.

3 LITERATURE REVIEW

This chapter presents a review of existing literatures that relate to ICSE cyber security improvement, and which specifically proffers resources and knowledge of the state of the art, and open research gaps. This literature review is presented after the methodology to show the review results as satisfying the requirements of the research objective 1. This also provides basis for exploring subsequent research objectives.

3.1 Industrial Control System Environment Security

ICS is typically an operation-critical system that places critical requirements for continuous, uninterrupted, and unmodified functioning of collaborating components and assets. Thus, the priority of IT security requirements (triangle) are reversed to *Availability, Integrity, and Confidentiality - AIC* (Larkin *et al.*, 2014). These are further supplemented with some secondary security principles such as Non-repudiations, Timeliness, Graceful Degradation (Zhu *et al.*, Joseph and Sastry, 2011), etc. Appendix A-1 presents a summary description of ICS security principles.

Safety is also a critically requirement in ICSE (ENISA, 2011). This requirement can also be easily deduced from the definition of ‘*security*’ from NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security (Stouffer *et al.*, 2015). Here, security is defined as: “*freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment*”.

Safety is prior to security in the modern ICSE. Any security measure(s) that weaken(s) safety is unacceptable (Stouffer *et al.*, 2015). Cyber security guards ICSs, and keeps industrial processes and operations running safely and efficiently. It ensures that data and process instructions remain uncompromised, communication flows and exchanges uninterrupted, and malicious codes and applications barred from infecting control systems and networks or upsetting control and processes.

The security risks in ICSE are characterised by threats, vulnerabilities, attacks, and impacts from both technical, and socio-economic dimensions. Targets and victims often range from industrial technologies (equipment, components, services), people (operational workforce, suppliers, customers), and processes (controls, sensing, actuation). Effective

security response lies in an adequate understanding of the array of risk features of ICS in relations to threats, vulnerabilities, and attacks (agents and patterns).

A key issue in ICS security is that industrial network protocols typically do not undergo widespread security testing for robustness before being adopted. Research records show that it is quite easy to crash ICS networks just by simply establishing connection to TCP ports on a functional ICS device (Austin, 2017; Gibbs, 2017; Symantec, 2017). Some common ICS protocols are described in Appendix A-16.

Additionally, most ICSE components devices are now supporting web-enabled capabilities, and yet do not come with strong authentication beyond passwords. Even passwords on defaults are usually very weak and could be easily broken. Thus, current ICS authentication methods are not seen to be commensurate to the criticality level of the system. In most cases, there are very minimal access controls between the corporate network and the control system (Stouffer, Falco and Scarfone, 2011), and an attacker only needs to compromise the corporate network to get to the control system network segment. For instance; Modbus was formerly developed for serial line communication, today; Modbus/TCP implementations are commonly used in ICSs. Modbus and DNP3 protocols currently do not support direct authentication, integrity checking, authorization, or encryption. As a result, design flaws in the core protocols render ICS networks insecure (Byres *et al.*, 2007; Gervais, 2012).

Open standards and technologies of vulnerabilities and exploitation modes can be easily employed by intelligent malicious cyber actors. Secondly, insecure technologies and protocols are being introduced into today's chaotic cyber domain without well-thought prior security solutions in place. This indicates that ICSE users and operators have moved on to a new insecure environment, but retained their age-long misconceptions that they are yet isolated from other networks, and thus inaccessible by cyber attackers (Ilgure, Laughter and Williams, 2006). This group are yet to grasp and acknowledge that so long as there are the likes of gateways, some form of connection to the outside world (dial ups, or internet), commercially-off-the-shelf devices, open standards or protocols, and human operators/actors, determined attacks will always find vulnerable points from these to achieve any targeted compromise on the ICSE infrastructure (Ilgure, Laughter and Williams, 2006).

3.1.1 ICS Security Threats

The security threats to the functionality of ICSE infrastructure typically engage attacks in forms of illicit access to sensitive industrial information, disruption of the functions of industrial infrastructure, physical damage to systems, and(or) harm to human operators (Chandrika, 2011; CPNI, 2014). Threat agents include: direct external attackers, bot-network operators, criminal groups, foreign intelligence services, insiders, phishers, spammers, spyware/malware authors, terrorists, and industrial spies (Stouffer, Falco and Scarfone, 2011).

3.1.2 ICS Security Vulnerabilities

A security vulnerability is a flaw that could allow an attacker to compromise the data, functionality, or operations of a system. With respect to ICSE, adversaries are exploiting organisations whose business models depend on the availability of digital infrastructures and content (Roland-Berger, 2015). Therefore, it is important that all industrial actors become aware of the cyber-attack threats and the full extent of their consequences (Wells *et al.*, 2014).

Macaulay and Singer (2012) present a classification of ICS vulnerabilities which is based on the illustration of functional characteristics. They argue that waiting to recognise the patterns of exploitation impacts before initiating responses is by far less ideal and not an option. Thus, ICSE vulnerability analysis can start with considering ICS control devices to include a combination of two distinct communication interfaces – Internet Protocol (IP) and Input/Output (I/O) communication interfaces. Thus, given the feasibility of logically accessing ICS devices, the exploitation options for security vulnerabilities would neatly fall into the following 6 categories: (i) Denial of view (DoV), (ii) Loss of view (LoV), (iii) Manipulation of view (MoV), (iv) Denial of control (DoC), (v) Loss of control (LoC), and (vi) Manipulation of control (MoC). Table 3-1 presents a summary of the impacts of exploiting each of the vulnerability forms articulated in this section. The researcher asserts that classifying technical security vulnerabilities from the viewpoint of functionality allows for the investigation of previous known failures or unknown ICSE vulnerabilities. They argue an instance that, an understanding of *LoV* and *MoV* vulnerabilities can support the access to the potentials for erroneous or manipulated view of a current system state (Macaulay and Singer, 2012). More specific technology-oriented vulnerabilities more common in ICS

networks include: buffer overflows, authentication bypass, improper input validation, cleartext transmission of sensitive information, and SQL injections.

Table 3-1: Functional Properties Classification of ICS Vulnerabilities

	Denial (Temporary)	Loss (Sustained)	Manipulation
View	DoV	LoV	MoV
Control	DoC	LoC	MoC
White	<ul style="list-style-type: none"> - View is Disrupted - Disruption to reporting and Operator awareness - Risks to infrastructure and production if left undetected or unchecked for a long period of time 		
Grey	<ul style="list-style-type: none"> - Control is Disrupted - Impacts (temporary or sustained) can cause erratic communication - Control interface and logics typically stable and intact - Risk vary widely with the process under control 		
Black	<ul style="list-style-type: none"> - View and/or control unrecoverable automatically or remotely - Damage potentials through delivery of wrong information to control room personnel or production infrastructure - Risk is highest 		
<i>DoV – Denial of View</i> <i>LoV – Loss of View</i> <i>MoV – Manipulation of View</i>		<i>DoC – Denial of Control</i> <i>LoC – Loss of Control</i> <i>MoC – Manipulation of Control</i>	

Source: (Macaulay and Singer, 2012)

3.1.3 ICS Security Attack Patterns and Impacts

Cyber-attacks on ICSE could be executed in various forms or modes. The more trending techniques that often target human vectors include: phishing and other social engineering attack methods (CLOUDMARK, 2016). More technology-oriented attack modes include the compromise of domain controllers, attack on exposed servers, attack on ICS clients, session hijacking, piggybacking on the system's virtual private network (VPN), exploiting firewall and other gateway vulnerabilities, misconfiguration of firewalls, forged Internet Protocol addresses, circumventing the network security, and Sneaker net techniques (Maize, 2014). Other authors (Pasqualetti, Dorfler and Bullo, 2015) have categorized ICS cyber-attacks into four, these include; deception attacks, denial-of-service attacks, replay attacks and covert attacks.

The impacts of cyber-attacks on ICS could be instant and obvious, or dormant and(or) subtle over a prolonged period. The degrees of damage can range from inconvenient downtime for ICS inputs, outputs, control, and enterprise system equipment, to life-threatening devastations of critical infrastructures (CACI International Inc., 2010). Choo (2011a) highlights that cyber-attack impacts can yield either short or long-term effects. Short term impacts would typically characterise effects on the daily activities of individual end-users (workforce) and (or) systems (e.g. upsetting the ability to receive up-to-date information), and the routine activities of businesses, companies, and governments. The Long-term impacts could include: loss of intellect property, which can upset long-term competitiveness, spur social discontent and unrests (e.g. loss of public confidence in products or services), and potentially national security breaches (Choo, 2011).

With respect to manufacturing environments, specific impacts could appear in varying forms including: disruption of normal operations, equipment damage, delayed or lost productions and products launch (Honeywell, 2011), loss of customer trust, brand value and competitive advantage, loss of revenue, loss or injury to human life (Nicholson *et al.*, 2012b; CPNI, 2014; Wells *et al.*, 2014).

3.1.4 ICS Cyber Incident Analysis

A non-exhaustive survey study of the impact of recorded real attacks on ICSE or related systems spanning 1982 to 2016 was carried out. Details about the incidents are presented in Appendix A-21. As shown in Figure 3-1, results indicated a gradual increase in the occurrence of popular cyber-attacks targeting the ICSE. These demonstrate proof that the ICSE is being targeted and at rising frequency. It also drives the motivation for engaging necessary solution actions.

The study also included a careful contextual study and analysis the of recorded information and description for each incident, with focus on the malicious actions or activities engaged, the attack vectors, corresponding effects, and the extent of cascading impacts. Special attention was given towards identifying popular keywords and phrases that represent similar descriptive meanings with already known and established security violation principles. The incidents were grouped according to recorded and(or) perceived violation of one or more of the primary security principles: availability, integrity, and(or) confidentiality. Analysing cyber incidents in the light of reported, documented, or publicised

details about the actors, targets, vectors, execution mode, and impacts facilitated the clearer identification of the specific security principles violated. Most of the studied incidents present obvious indications of the security principles violated. For example, the German Steel Mill cyber-attack (Lee, Assante and Conway, 2014) can be viewed to have targeted the violation of system *availability*. Attack outcome reported “*an accumulation of breakdowns of individual components of the control system or of entire facilities*” such that “*the furnace was then unable to be shut down properly which resulted in unexpected conditions and physical damage to the system*” (Lee, Assante and Conway, 2014). In this study, breakdown of control system components meant that the affected control system components became unavailable for use, thus violating the *availability* of those components and connecting facilities. The overall impact, also indicated a “*physical damage*” which took systems/components out of use at least for some time, thus affirming the *availability* violation.

Another purpose for this systematic analysis was to corroborate or refute earlier submissions on the emerging most widely targeted/violated security principle by attackers in ICSE. Thus, provide justification to lending strong voice to the accent on security prioritisation, and the adoption of security measures for mitigating the damages posed by such most frequent violations. Figure 3-2 presents a set distribution of the reviewed incidents based on perceived potential violations. From the records, a total of 32 cyber incidents were sampled. 3 cyber incidents targeted the violation of all three security principles. 2 cyber incidents target the violations of integrity alone, 3 incidents target confidentiality violation alone, and 9 cyber incidents were thought to have targeted the violation of availability alone.

Marked with the *asterisk* (*) symbol, some of the cyber incidents in Appendix A-22 led to the violation of at least 2 of the three security principles: 6 incidents targeted both availability and integrity, while 9 incidents targeted both integrity and confidentiality. Generally, out of the 32 sampled incidents, only 2 were experimental, while 30 were essentially real-life incidents that successfully targeted actual industrial control systems infrastructures with varied degrees of successes. The experimental incidents reviewed involved live and public demonstrations of the exploitation of identified vulnerabilities in ICS networks, which enabled the manipulation of the system to behave in ways other than initially designed.

From the distribution in Figure 3-2, it can be observed that a bulk of the cyber incidents against ICS infrastructures offered sole or contributory potentials towards the violation of availability with the typical aim of disrupting routine industrial functions and operations as evidenced in the attack and impact description. Therefore, it is reasonable that ‘*availability*’ is accorded the highest priority amongst the three primary security requirements, and the *availability* of ICS considered of utmost concern. The two experiments demonstrated that attacks on the ICSE are feasible from the technology and process perspectives. The records of real incidents also demonstrate that similar domain attacks via exploiting the human-factor (people) vulnerabilities are also feasible. Both aspects show that successful cyber-attacks on ICSE bears enormous consequences and impacts that cannot be ignored. Cyber security awareness still needs to be improved to forestall the growing situation when lessons are learnt, and solutions sought after incidents and impacts have occurred. New, improved, and proactive solution approaches are required if conventional solutions become ineffective.

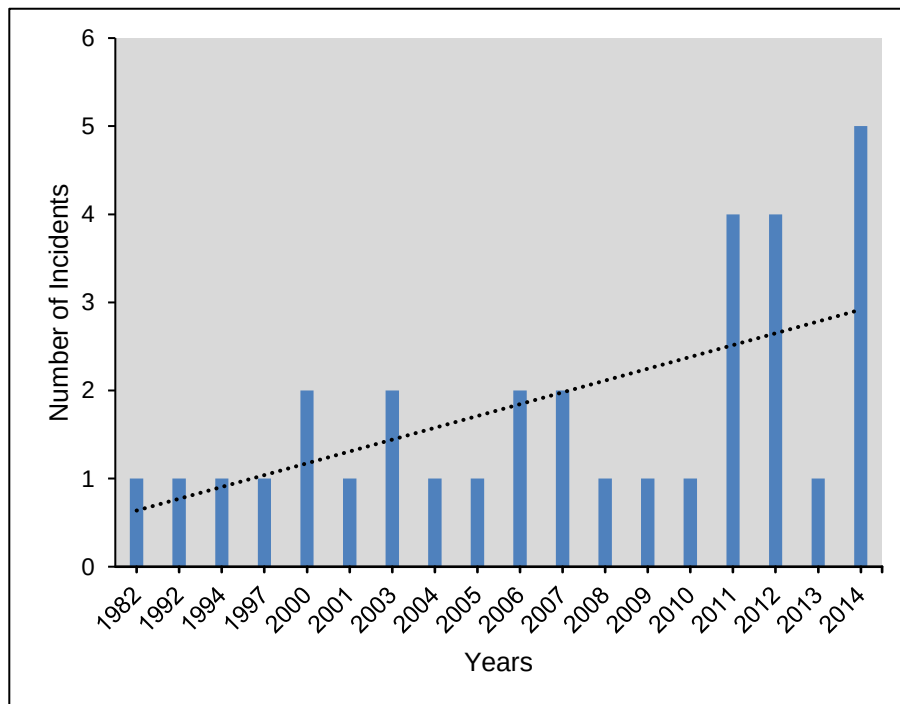


Figure 3-1: Sampled ICS Cyber Incidents

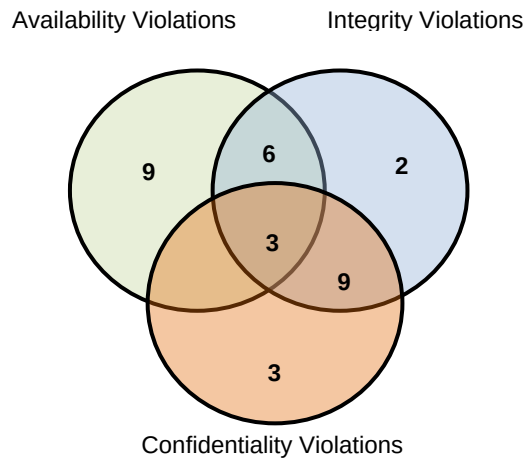


Figure 3-2: Distribution of Security Violations for ICS Cyber Incidents

3.2 Categorised Methodologies for ICSE Security

Different researchers have proffered different techniques and pathways towards achieving security in the ICSE. These methods can be broadly classified into: architectural design, strategy implementation, attack modelling, attack detection, and attack categorisation approaches.

- i. **Architectural design approaches** include the works (Cruz *et al.*, 2014; Dong *et al.*, 2015) that explore security establishment through a description of potentially secure designs - integrating ICS hardware and software into a structured setup to enable a protection capacity. Such design setups are orchestrated to make it difficult for cyber-attacks to happen. Examples (methods and authors) of the architectural design approaches to ICSE security are presented in Appendix A-23.
- ii. **Strategy implementation approaches** include the researches (Northcutt, 2014; Lu *et al.*, 2015), which explore security enablement through applying scope analysis, organisational policies, procedures, and technologies, to address security threats, vulnerabilities, and potential attack patterns. Examples (methods and authors) of the strategy design approaches to ICSE security are presented in Appendix A-23.
- iii. **Attack detection approaches** refer to works (Chen and Abdelwahed, 2014; Nourian and Madnick, 2014) built on the popular technique of using Intrusion Detection and Prevention System (IDPS) to enable a capacity to secure ICSEs from cyber-attacks. This approach typical focuses on uncovering of attacks from functional and operational

faults, anomaly, malfunction signatures, patterns, and behaviours, and proffering isolation and recovery controls.

In ICSE platforms like manufacturing, anomalous conditions would encompass a range of minor or major process disruptions that would require interventions by human operators (workforce) to correct problems which the control systems cannot handle. Often, a challenge involves the precise and accurate identification of the sources for process misbehaviours to allow for appropriate remediation measures (Krotofil and Gollmann, 2013). Examples (methods and authors) of the attack detection approaches to ICSE security are presented in Appendix A-23.

- iv. **Attack modelling approaches** include research works (Srivastava *et al.*, 2013; Pasqualetti, Dorfler and Bullo, 2015) that explore ICSE security through the replication of cyber-attack events in simulation, emulation, real environments. It involves the study of vulnerability patterns, direct effects, and impacts of exploiting the vulnerabilities, and using observed and evaluated results to bring about effective security solutions. Examples (methods and authors) of the attack modelling approaches to ICSE security are presented in Appendix A-23.
- v. **Attack categorisation approaches** include the researches (H. Zhang *et al.*, 2013; Yuan *et al.*, 2013), that explore security enablement through the classification of cyber-attacks based on exploit modes for attacking ICS systems, and engaging specific controls to meet specific attack modes. Examples (methods and authors) of the attack categorisation approaches to ICSE security are presented in Appendix A-23.

3.3 Existing Works Related to Research Objectives

In the light of adopted research objectives, a review of related works is presented. Research works were reviewed in relations to techniques for demonstrating cyber-attack feasibilities, methodologies for security metrics development, technical vulnerability impact analysis, human-factor cyber security capability evaluations, and security risk reductions in ICSE.

3.3.1 Cyber-Attack Simulation in ICSE.

As earlier pointed, practical (experimental) security audits impact negatively on real industrial operational environments, hence, the use of simulation techniques as suited alternatives for ICSE security studies.

Most previous works have used testbed simulation demonstrators, often conducted on computers or laboratory control environments to show the techniques, consequences, impacts of attacks, as well as the potential ways of ensuring or improving security. Several works have leveraged on testbed capacities and setups for exploring varied aspects of cyber security relative to ICSE and Critical Industrial Infrastructures (CII).

The National SCADA Testbed (NSTB) (U.S. Department of Energy, 2009) was developed using real physical components to investigate vulnerabilities and security assessment methods in electric and power grid. The authors argued that a better understanding of how to safeguard SCADA systems could only be achievable via adequate test-bed approach for vulnerability assessment and development of appropriate security mechanisms. Wells *et al* (2014) used a testbed to investigate user-level diagnostic capabilities. The work demonstrated a clear scenario of compromising a production system, and the unaware state of future manufacturing engineers to the cyber-security threats and trends in modern manufacturing control systems.

Korkmaz *et al* (2016) used a testbed approach to study the impacts of cyber-attacks on a SCADA system. The cyber-physical testbed was based on power generations and emulated the typical technologies that are seen functional in a critical infrastructure setup. Cyber-attack patterns demonstrated included; Man-in-the-middle (MitM), Denial-of-Service (DoS), and Malicious software injections. Similar Cyber-physical testbeds were used by Soupionis *et al* (2015) for evaluating the impact of DoS attacks in power distribution networks, and Hurst *et al* (2016) for replicating the scenario of a water distribution plant and investing attacks that can affect critical infrastructures.

One general view shared by all these research is that the testbed approach supports cyber-security research purposes, and the testing of new experimental methods for improving the level of security in cyber-critical systems. The reviewed works also suggest that testbeds involving real components offer a more viable and credible approach for conducting cyber security demonstrations and researches in the ICSEs since they are able to emulate industrial assets (H. Holm *et al.*, 2015), and deliver the type of data and information that can assist in a research analysis attributable to the actual industrial environment. Testbeds have the potential to support several aspects of ICSE cyber security research: threats and vulnerability research, impact and cascade/dependency

analysis, controls and mitigations research, cyber-physical security metrics, data and security model development, security validation, interoperability, cyber-forensics, and operator training, etc., (Hahn *et al.*, 2013).

3.3.2 Security Metrics Generation Methods

To understand the security capability or vulnerability state of an ICSE or its varied entities, security metrics are required and used to measure relative attributes of the system or components. However, generating and adopting relevant and good security metrics needs to be guided by carefully planned and effectively designed approach, which should be feasible, flexible, and adaptive to a wide range of ICS audience and use case security scenarios; including technical and non-technical audience (Collier *et al.*, 2016).

The effectiveness of a security metric lies in its ability to specify the degree to which security objectives are being met, and to drive actions towards improving the security state of an organisation or system (Cybenko and Cybenko, 2014). The need to clearly articulate the characteristics of a metric development approach is ever crucial. Characteristics that can guide security metrics formulation - give basis, relevance, and acceptability to designed approaches, and their usefulness towards improving security. Essentially, a good security metric is more likely a product of a good metric generation or development approach.

Metrics generation approach can adopt a customised or compliance-based adoption process. In either case, directional process-adoption methods like top-down or bottom-up are considered when determining desirable assessment metrics (Payne, 2006). With the top-down approach such as the Balanced Scorecard (BSC) (R. M. Savola and Abie, 2009; Nguyen, 2012), security objectives are first defined, processes worked down to identify specific security metric quantities that meet the objectives, and the measurements needed to generate the security metrics. In the bottom-up approach, a reverse process, categorising existing, easy-to-obtain data as a starting point for outlining the metric quantities, and working up to the security objectives of a target system accordingly (Stoddard *et al.*, 2005; Payne, 2006).

Savola and Abie (2009) also present the enhanced version of an earlier security metrics development approach. This revised model provides an iterative process for metric

generation aimed at achieving balanced and comprehensive security metrics taxonomy for any given system. Jonsson and Pirzadeh (2011) presented a security metrics development framework based on operational system attributes that may be applied to an ICSE. The model combines the concepts of security and dependability, studying operational system's interaction with its environment via the system boundaries concepts. The model regroups conventional security and dependability attributes into 3 attributes: protective, behavioural, and correctness. The model provides capabilities for generating at least two possible types of security metrics: protective, which relates to the system input, and behavioural, which relates to the system output. The researchers explained correctness to mean a possible template state considered desirable of the system, and against which measures of actual deviation can be deduced. This template state can be viewed as an ideal state suggested in (McQueen *et al.*, 2008), and describing the state of metric quantities that is representative of the best and desirable security state of the system or entity being evaluated. This ideal-driven concept essentially addresses the gaps of the operational system model as described in (Jonsson and Pirzadeh, 2011).

An Adversary View Security Evaluation (ADVISE) model-based security metrics approach is presented in (LeMay *et al.*, 2011). The approach tried to create an executable model that combines system information, adversary information, and desired security metrics to produce quantitative metrics data. The resulting metrics generated by ADVISE indicate the measurements recorded from discrete-event simulation and are used to assess the probability of compromise within a specific period. The metrics also give insight to the speed of compromise, and possible attack steps.

A technical-centric security metrics development model for SCADA (TSMM SCADA) systems is presented in (M. P. Azuwa *et al.*, 2012). This guides the generation of metrics used to measure the effectiveness of network security management controls and services such as firewalls, and Intrusion detection prevention systems (IDPS) in the protection of SCADA systems. The model adopts a four-step process of: Plan, Do, Check, and Act (PDCA), and the resultant metrics are basically targeted at meeting compliance requirements of ISO/IEC 27001 Information Security Management System (ISMA) standards.

A resilience-centric approach to security metrics development for cyber infrastructure was presented in (Linkov *et al.*, 2013). A matrix framework (Linkov *et al.*, 2013) was used to develop and organise effective resilience metrics for improving cyber security in cyber systems. The metrics formulation approach is such that policy goals are linked to certain system measures, translating resource allocation decisions into actionable interventions and investments. The developed matrix of resilience metrics combines the four stages of system event management cycle for resilience by the National Academy of Science (NAS) (Plan/Prepare, Absorb, Recover, Adapt), and the Network-Centric Warfare doctrine's situational awareness and decentralised decision-making domains (Physical, Information, Cognitive, and Social) (Linkov *et al.*, 2013). These strategies collectively integrate actual data, technical judgement, literature-based measures to assess system resilience across physical, information, cognitive, and social domains of a cyber system (Linkov *et al.*, 2013).

An ASPIRE (Aim, Select, Prepare, Introduce, Report, Establish) IT-centric metric development approach was presented in (Chandrakumar *et al.*, 2013) which slightly addressed metrics related to the industrial environment. The steps of the metrics model include: define the aim and objectives of a metric program, select the metrics to be generated in line with business goals, prepare strategies for generating the metrics, introduce measurable performance targets, report the plan for metrics, establish the implementation plan, review, and refine the plan as necessary. These steps provide organisations with an defense-in-depth approach to managing and mitigating operational risks through the deployment of business information security program. A key advantage of ASPIRE is that it can be utilised in security programme formulation yet without upsetting existing system setups or processes.

In reviewing existing security metrics generation methods, there appears to be some challenge in achieving adaptive security metrics approaches despite the exponential control and security efforts of organisations. This difficulty is further exacerbated by the non-linear efforts adopted by attackers, even where enterprises and organisations are required to put in exponential efforts on security (Bellovin, 2006). Security metrics developers should think themselves as pioneers, and be prepared to fine-tune their approaches as circumstances and experiences dictate (Stouffer *et al.*, 2015). Another notable gap is that existing ICSE-specific methods lag in providing sufficient security metrics generation guides to ICS organisations along widely accepted security frameworks

requirements such as NIST SP 800-82 (Stouffer *et al.*, 2015), NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2014), and Security of Industrial Control System Good Practice Guide (CPNI, 2009). It is noteworthy that current methods are more inclined to ISO/IEC 27001 IT security metrics developments guidelines (Fruehwirth *et al.*, 2010; Barabanov, Kowalski and Yngstrom, 2011; M. . Azuwa *et al.*, 2012; ISO/IEC, 2013).

This situation reveals a need for an improved method that would be clearer - proffering an inclusive, concise step-wise methods for developing cyber security metrics that would be aligned to prevailing trends and features. Reviewed metrics development models do not appear to be very suitable to meet the dynamic nature of security in the ICS domain. Especially, the ability to eliminate ambiguities in the outline of relevant metrics generation attributes. A methodology that allows for the clear definition of system security scope and objectives, allow for measurements and comparisons, refinements, and predictions to guard against potential future harms.

3.3.3 Technology Vulnerability Impact Analysis Techniques

Technical vulnerability analysis provides a way of investigating and identifying flaws that can be exploited to violate or compromise security with a technology entity. One of the most common model for evaluating vulnerabilities is the Common Vulnerability Scoring System - CVSS (Wang *et al.*, 2016).

CVSS is an open industry standard for assessing the security of system vulnerability by attempting to establish a measure of concern attributable to a vulnerability in comparison to other known vulnerabilities, to influence proper prioritisation of security efforts (Singhal and Ou, 2011; Chejara, Garg and Singh, 2013). It allocates a discrete 'score' to each vulnerability on a scale of 0 to 10 where higher values indicate greater severity and is generally composed of three metric groups: *Base*, *Temporal*, and *Environmental*. Each of these metrics also consist of a set of sub-metrics. The Base group embodies the basic characteristics of a vulnerability that are invariable over time and user environments. These include: access vector, access complexity, authentications, confidentiality impact, integrity impact, and availability impact.

The temporal groups represent the features of a vulnerability that vary over time but not amid user environments. These include: exploitability, remediation level, and report confidence. The environmental groups represent characteristics of a vulnerability that are related and exclusive to a user's environment, these include: collateral damage potential, target distribution, confidentiality requirement, integrity requirement, and availability requirement (FIRST, no date). Standards vulnerability scoring schemes like CVSS helps organisations to normalise vulnerability ratings across all its technology platform (hardware and software) and use same to leverage a single vulnerability management policy. It provides an easy understanding of the individual characteristics used to derive vulnerability score, and offers a way to achieve prioritisation of vulnerabilities in relations to the dynamics of the environment (FIRST, no date).

Abraham and Nair (2014a) explored a cyber situational awareness means for improving the understandability of cyber-attack impacts on networks and systems. They applied stochastic modelling (absorbing Markov chain) and simulation techniques using attack graphs to outline a complementary suite of quantitative metrics to aid security engineers in visualising current and future security status of a network. They used CVSS exploitability definition to estimate the transition probabilities of the absorbing Markov chain through a normalisation approach. In another work (Abraham and Nair, 2014b), the same researchers explored the use of non-homogenous Markov models that consider a vulnerability's age integrated into Frei's model (Frei, 2009) to derive vulnerability temporal weight scores from attack graphs, rather than adopting conventional CVSS scoring scheme. Three key metric quantities were proposed for achieving this goal: expected path length, probabilistic path, and expected impact.

Jaganathan, Cherurveetil and Sivashanmugam (2015) proposed a mathematical model for predicting the impact of an attack. They adopted a multiple regression approach to help predict the potential impact of a vulnerability well before the host IT application is released for usage. The aim was to reduce impact through adequate cost and resource allocations for prioritised vulnerabilities resolutions. They also used the CVSS score of vulnerabilities as the dependent factor to derive the environmental and system characteristic of the target host application.

Another study (Yang *et al.*, 2016), also adopted CVSS combined with Hierarchical assessment model and Grey Clustering Algorithm (GCA) to effectively evaluate vulnerability risk assessment in Electric Cyber Physical Systems. The work focused specifically on Electric Power Information Network (EPIN). The approach was verified using 4 typical EPIN vulnerabilities, and the results showed an improved vulnerability risk method over conventional approaches for electric CPS cyber space. In another study (Keramati, Akbari and Keramati, 2013), the CVSS framework was combined with attack graphs to derive some security metrics that supported the measurement of attack impact indicated or represented on an attack graph. Their work tries to resolve the non-consideration of interrelations between vulnerabilities. It supported the quantitative evaluation of network security through attack graphs analysis, and the determination of the most critical vulnerability in the network.

A VEA-bility quantitative metrics were proposed and used for measuring the desirability of varied network configurations (Tupper and Zincir-Heywood, 2008). The researchers modelled VEA-bility as a function of the security scores along three dimensions: vulnerability, exploitability, and attackability. The vulnerability dimension is accounted for using the CVSS impact score and temporal score for a known vulnerability.

Younis *et al* (2016) proposed a model for evaluating the exploitability of a vulnerability in a software system based on the existence of a function call connecting attack surface entry point to a vulnerability location within the software. Their approach demonstrated the feasibility of using systematic evaluation rather than subjective judgements in the assessment of system security. The authors proposed a new metric: structural severity, which is based on software properties name: attack entry points, vulnerability location, dangerous system calls, availability and reachability. These sub-metrics are derivable objectively from attack surface analysis, vulnerability analysis, and exploitation analysis.

A static graph-theoretic approach has been used to consider smart grid topological information for vulnerability analysis (Conte de Leon *et al.*, 2002). Researchers (Dudenhoeffer *et al.*, 2007; Rozel *et al.*, 2008; Hadjsaid *et al.*, 2009) adopted experimental approaches to gain realistic details in power system simulations. They used reliability metrics to assess impacts of cyber-attacks. A cyber-physical leakage approach (Tang and McMillin, 2008; McMillin, 2009) was used to study the voltage measurement confidentiality

of a power system cyber network for the purpose of learning cyber protocol activity. Mechanistic approaches (Mander *et al.*, 2007; Sheng *et al.*, 2007) involving cyber protocols, algorithms, and architectures have also been used to examine change impacts in power systems

In (MacDermott *et al.*, 2012), critical infrastructure cascading failure is simulated using a virtual smart city. The simulation assessed failed telecommunication and demonstrated how failure in one infrastructure can cause impact in another. Similarly, other researchers (Sgouras, Birda and Labridis, 2014) evaluated the impact of denial-of-service attacks on a simulated smart metering infrastructure servers, which was noted to have caused severe communication disruptions. The researchers also investigated the impacts of cyber-attacks on power systems wide-area frequency control applications. The outcomes reveal a significant impact on system stability in the form of severe drops in system frequency due to cyber-attacks. A graph-based model is proposed by Kundur *et al.* (2010) for evaluating the effect of control loops on physical processes, and used to measure the impacts of cyber-attacks on electric power generation.

Kotenko and Chechulin (2013) proposed a cyber-attack modelling and impact assessment component (CAMIAC) framework. The framework emphasises the representation of malefactor's behaviour, attack graph generation, security metrics calculations, and risk analysis, as the common approach to attack modelling and impact assessment. The framework optimises attack graph and security evaluation using anytime algorithm with different timeliness and accuracy.

A holistic criticality assessment methodology that considered existing security plans and risk assessment of critical infrastructure is presented (Theoharidou, Kotzanikolaou and Gritzalis, 2010), where a layered approach was adopted for modelling the needs and requirements for criticality assessment, but the layers are categorised as operator, sector, and intra-sector/national layer.

Cascading impact is described in the context of functional/operational failures (Kotzanikolaou, Theoharidou and Gritzalis, 2013). The researchers assert that a cascading failure ensues when a disruption in one infrastructure impacts one or more components in another infrastructure, which sequentially causes a partial or complete unavailability or non-functionality of the second infrastructure. Earlier works by the same researchers

(Theoharidou, Kotzanikolaou and Gritzalis, 2010) adopted a layered approach underscoring the interdependence across layers to evaluate security risk and criticality. The work based on a much earlier suggestion that risks ought be analysed on multiple levels of hierarchy corresponding to the objectives and requirements of the respective decision makers (Haimes *et al.*, 2007). Analysis ought to aim at underscoring how micro-level dependencies affect macro-level impacts in systems. The above suggestions and recommendations also provide motivations for researching this context.

Reviewed literatures show that standard CVSS is a widely accepted scheme and method for evaluating and rating the severities and risks of technical vulnerabilities. Some researchers have used the CVSS base score metric to characterise and demonstrate these severities within a network. Others have used the CVSS temporal or environmental metrics scores, or some selected decomposable attributes or sub-metrics to demonstrate similar severities considering the dynamic changes of the vulnerabilities in relation to their host environment or components.

Even more, some researchers have combined CVSS metric attributes with other security evaluation methods like attack graphs, Bayesian and Dynamic Bayesian Networks, Stochastic and Non-homogenous Markov models, and Statistical approaches to demonstrate better assessment approaches, schemes, and outcomes for technical security severities and impacts. By this, they indicate that combining multiple attributes of a security vulnerability in a security assessment, can yield better views, insights, and outcomes about derivable security states.

Reviewed works also suggest that understanding the dependency relationship amongst system collaborating components (cyber-physical) is key to achieving effective modelling of cascading impacts. Graph-theoretical approaches (static or dynamic) appear to offer good ways of representing dependencies and impacts within complex cyber-physical systems. In relations to ICS, graphs enable a tighter coupling between cyber and physical domains, and induce overall system status dynamism, allowing for convenient representation of cascading effects (Kundur *et al.*, 2010).

Despite the usefulness of current works on cascading impact analysis, a key drawback observed is that of the use of static severity attributes and ratings for vulnerabilities without considering the effect of environment and other external influences. Most existing solutions

proffered are domain-dependent and chiefly focus on power systems, their applications to the manufacturing domain are hardly feasible. Although CVSS base score metric can provide a foundational understanding of the potential severity of a vulnerability, it does so with the limitation of not considering the changes in the vulnerability properties or the environment they reside.

This work suggests that a better valuation of such severities can be achieved while considering temporal and environmental factors surrounding the vulnerabilities and their hosts. Researchers (Ridley, Young and Carroll, 2004) have portrayed similar disposition, asserting that *“prioritizing of vulnerabilities based on such measures should be used with caution”*. The actual impact of security incidents have been shown to vary significantly among varied types of users, organisations, and businesses (Ishiguro *et al.*, 2006; Telang and Wattal, 2007), which also necessitates varied prioritised mitigation modes (Lai and Hsia, 2007). Hence, introducing the CVSS temporal and environmental metrics in a security evaluation process bears the potential to account for the variations in prioritised mitigation, and support improvement, since the reflection of actual impact of vulnerabilities in specific organisations are better achieved (Frühwirth and Männistö, 2009).

Also, since the amount of CVSS information also potentially influences the effective modelling of security (Holm, Ekstedt and Andersson, 2012), again it is suggested that combining the varied sub-metrics characterised in the temporal and environmental score metrics bear the potential to yield outcomes that are closer to the precise about the severity state of a vulnerability. Analysing the distribution of CVSS environmental score showed that the quantitative estimation of the impact of environmental metrics on vulnerability severities was feasible. It further demonstrated that if such estimation is achieved, it could offer high-level view of vulnerability severities, and thus support the prioritisation of the vulnerabilities for responses, and appropriate application of controls to ensure improved security (Li, Xi and Zhao, 2015)

3.3.4 Human-factor Cyber Security Evaluations

3.3.4.1 Security Issues and Requirements

As cyber-attacks continue to evolve, businesses and organisations are prone to security concerns that threaten their business and operational relevance within the currently

competitive business domain (Ralston, Graham and Hieb, 2007; Mirashe and Kalyankar, 2010). Many organisations keep upgrading technology assets equipped with defensive capacities to protect automation processes from cyber intrusions or breaches. Notwithstanding, cyber-attacks and incidents on industrial control environments have continued to rise, chiefly due to changes in the direction of targeted attacks (Knowles *et al.*, 2015). While organisation continue to invest heavily in technology-oriented security, attackers have strategically side-tracked attack concentration from technology to people (human) assets (IRM, 2015).

Recorded cyber-attack events clearly demonstrate that the analytical proficiencies of the human constituents through the exploitation of cognitive capacities are still crucial for effective security in ICSE (Chen *et al.*, 2012; Gonzalez *et al.*, 2014; Ben-Asher and Gonzalez, 2015). This is made possible by the existence and expression of easily exploited human weakness in the system process interaction loop.

For instance, in 2013 Target Corporations network was breached. The most popular theory describing the initial infection mode for the breach involved the compromise of a third-party vendor via phishing attempt. This was viewed successful due to poor security training of the third party, enabling an easy exploitation of the third party's access to Target's network to get into Target's Ariba external billing system (business network), collected and exfiltrated customer card details (including card numbers) (Shu *et al.*, 2017). Further analysis of the Target Corporation breach showed that Target's security technology was capable of detecting the breach, but the people (leaders and general employees) who should be able to take appropriate responses to control the attack impacts, lacked the necessary skills and knowledge (Hershberger, 2014). The attack caused a disaster that cost Target about \$148 million, and other financial institutions about \$200 million (Tobias, 2014). Target could have benefitted more from a proactive evaluation of its workforce cyber security capability, which may have unveiled cybersecure weak links in the workforce, and the areas affected. The organisation may could have responded better and earlier with such understanding of the potential security knowledge and skills strengths and weaknesses of its workforce. It is believed that such understanding may have spurred the corporation into engaging capacity improvement efforts in the direction of the weaknesses observed.

From other works, weak cyber security knowledge and skills in the workforce and leadership have become apparent to top the list of several human vulnerabilities in the minds of corporate decision makers, governments, and academic researchers (Adams and Makramalla, 2015). These have been quite dominant in the list of successful attack drivers targeting industrial control system environments such as manufacturing and energy (Ani, H. He and Tiwari, 2016). In one research, respondents believed that inadvertent human error, lack of staff awareness, and weakness in vetting individuals contributed 48%, 33%, and 17% respectively to the single worst security breaches, suffered by organisations (HM Government, 2015). Similarly, UK businesses have identified human error as the most single factor that they consider to have led to their most disruptive breach (Klahr *et al.*, 2016). Such precarious situations continue to press on industries and organisations due to inadequate or complete lack of understanding of the security capacities of operational workforce, and failure to provide operational staff (humans) with effective and up-to-date cyber security knowledge and skills capability to defend against cyber-attacks (Ashford, 2016).

These suggest that despite any huge investments in technology-based security solutions to safeguard the ICSEs, human-factor security characteristics still play very significant roles towards achieving a holistic cyber security capacity and assurance. Security knowledge and skills characteristics are still important. The statistics further suggest that the value of an organisation's chief security asset is more in its people – human constituents (workforce), than in technologies or laws and regulations (Navarro, 2007). It also points to human actors being potentially the weakest links (Kaspersky-Labs, 2015) in the ICSE operation chain. The success of any security venture would often depend on the human element – people are both the most significant resource and potentially the major threats to security (PA Consulting Group, 2015).

3.3.4.2 Human-factored Security Evaluation

The assessment of workforce's cyber security capability is quite instrumental towards achieving an efficient workforce security consciousness (Navarro, 2007). Some researchers have emphasised and suggested schemes for assessing cyber security postures from the workforce perspectives.

Wang (2013), explored an assessment of cyber security knowledge and behaviour using anti-phishing scenario. The study investigated the relationship between the evaluation of user's knowledge of cyber security risks and solutions (in relations to phishing), and their attitude and intention towards adopting and using cyber security solution. Important findings indicated a positive correlation between direct assessment answers and self-assessment responses.

Other works have considered the impacts of human perception (Bulgurcu, Cavusoglu and Benbasat, 2010; Siponen, Adam Mahmood and Pahnla, 2014), attitudes, and behaviour (Parsons *et al.*, 2014; Evans *et al.*, 2016) to organisational security capacities, and policy implementations. These works have emphasised the relevance of social human attributes to effective security performances. While these attributes are quite relevant and influential in deriving security conclusions in terms of capacities and controls, the security knowledge and skill levels of individuals can influence the outcome of each attribute. Thus, it is rational to consider the primary influencing factors and how they impact resulting security capacities and controls.

Beautement *et al* (2016) argued that effective security management requires that security managers are able to evaluate the effectiveness of prescribed policies, as well as the impact of employee behaviour. They proposed a Productive Security (ProdSec) methodology for aggregating huge datasets on employee behaviour and attitudes using scenario-based surveys. The approach involved the use of scenario-based surveys and was designed to ensure repeatable and scalable data collection, from which better insights can be deduced about security-related issues facing employees, their response behaviours, and attitudes. The outcome of statistical analysis of collected data showed that business area, age, and geographical location, all provide axis of differentiating response maturity levels of employees, as well as intra-population group of employees. Details as these can influence efficient planning of future trainings, communications, and policy-making. It can also support proactive interventions (remediation) on specific employees, which can save from inclusions in non-targeted interventions and reduce the expense on employee compliance budgets (Beautement, Sasse and Wonham, 2009).

Generally, the work by Beautement *et al* (2016) advances a concept to employee security analysis using group-level employee maturity evaluations. In contrast, this study

emphasises individual-level security capability evaluations. It is submitted that group-level evaluation alone does not support efficient individual attribution of security states within a group. Rather, it ascribes group capabilities to all individuals within a group, which might not exactly be true for all group members. Better interventions can be achieved if individual security capacities of employees are derived and used to drive decision policies.

Also, Beaument et al (2016), focused on evaluating security behaviours and attitudes of employees to derive security response maturities. The focus is on different human-factor attributes: knowledge and skills and use these to derive security capabilities of employee. While attitudes and behaviours are relevant human-factor security attributes, they can easily be influenced by knowledge and skill levels. Thus, logical relationship exists amongst the attributes. Thus, to effectively evaluate the security capabilities and performance of employees, their knowledge and skill attributes are quite relevant and important.

Individuals with varied levels of knowledge and experience in cyber security potentially demonstrate different perceptions of cyber security. Typically, higher security proficiencies imply better capability as experience can influence decision-making capability levels (Asgharpour, Liu and Camp, 2007). Advanced knowledge and previous experience could enhance the sensitivity to security threats and the performance of incident response.

The researchers in (Goodall, Lutters and Komlodi, 2009) highlighted that domain knowledge in information and network security, as well as, situated environmental knowledge grounded in an analyst's unique environment; are required to boost the expertise for effective intrusion detection by an analyst. The domain knowledge includes: theoretical knowledge acquired through formal education, training, or certification (Chi, 2006), and practical knowledge cultured through hands-on practice and experience with tools, methods of operation, and work- flows. The situated environmental knowledge is acquired through continued interactions with a specific operating environment (Goodall, Lutters and Komlodi, 2004). Researchers have used interviews and questionnaires to drive easy understanding of both mental models and security workforce workflows (D'Amico and Whitley, 2008; Paul and Whitley, 2013).

Ben-Asher and Gonzalez (2015) investigated the security capacity disparities between security experts and novices. They focused on evaluating the expertise of cyber security

analysts with specific interests in intrusion detection, and the use of intrusion detection systems (IDS). The outcome suggested theoretical knowledge as being completely independent of practical knowledge. Generally, the use of quantitative tools and measures of performance relating to intrusion detection scenarios provided an effective means of evaluating and characterising security control capacities of the expert groups as desired (Ben-Asher and Gonzalez, 2015).

While this research bears close similarity with the work by Ben-Asher and Gonzalez (2015), this work differs in the scope of security subjects covered. Rather than focus strictly on security experts and their performance level characterisations, this study covers the entire spectrum of ICS workforce, including IT security analysts (experts or novices), and non-IT-oriented workforce (environment end-users) such as, operators, technicians, engineers, supervisors, enterprise system users, etc. It is believed that the security performances of all these workforce members can contribute to an overall security capability of an industrial organisation. Also, based on security threshold definitions, this study tends towards the identification of potential weak-links in the workforce, as well as, potential weak themes (areas or aspects) of security performance. The intended evaluation approach would be based on prescribed standards and covers multiple security focus areas, rather than single security focus area adopted in previous work. The latter does not effectively capture the entire spectrum of security that may be of interest or relevant for optimum organisation security.

Security capabilities can be evaluated through interviews (structured and semi-structured) (D'Amico *et al.*, 2005), questionnaires (Botta *et al.*, 2007), observations and gamifications (Paul and Whitley, 2013; Adams and Makramalla, 2015; Ben-Asher and Gonzalez, 2015), penetrations testing (Aloul, 2012), etc.

While some methods have been developed for evaluating workforce cyber security capabilities, there is little research that has proffered a clear quantitative scheme for representing the security capacity of an individual or the entire organisation according to cyber security policies and/or standards in a specific environment. The Cybersecurity Capability Maturity Model (CCMM) (Christopher *et al.*, 2014) focuses on organisation-wide dispositions rather than workforce-focused dispositions. Reviewed researches in security performance evaluation of human constituents within organisations typically focused on

comparative analysis of security perceptions, and most often emphasises on the security staff (analysts) typically responsible for securing systems.

From the review of related works, it can be deduced that fewer researches have explored non-IT security operational workforce and their security-related dispositions, as well as contributions to overall system security. It is gradually being acknowledged that; user-centred evaluation of security capabilities, individual-level security capability evaluation, and identification of security-capable weak links are quite important and supportive of overall organisational security analysis and control prioritisation. However, approaches and methods that explore these areas have not been widely researched. This work explores a potential solution that fill the research gap.

Cyber security knowledge and practical security response skills are two direct attributes of workforce security capability, considered invaluable for achieving an improved secure industrial operating environment. However, the effective input of security knowledge and skills should be built on; a clear understanding of existing measures of capability, and the identification of capability shortfalls that reveal user vulnerabilities (weaknesses) to cyber attackers. This can only be achieved through evaluations.

A human-factor security approach is required to supplement existing technical-based security approaches towards an overall cyber security assurance. This is necessary to improve the capabilities of the operational technology human constituents, so that they can appropriately recognise and respond to cyber intrusion events within the ICSE environment.

Quantitative analysis can provide an easy approach to evaluating the security capability of a user in relations to cyber-attacks, as it can help both senior managers and general infrastructure users to intuitively understand the status of their cyber security capability. A quantitative approach also simplifies result presentation and interpretations. Essentially, quantitative approaches allow for consistent results, the production of trend interpolations and forecasts, quicker situational understanding for decision-making, and the further representation of results in better understood in formats like charts, graphs, and tables for time-critical decision-making. These are necessary to improve security capacity and assurance within the industrial operating environment, and without which top management

is unable to retain high degrees of confidence about the security of their industrial asset (Evans *et al.*, 2016).

3.3.5 Security Risk Assessment and Reduction Approaches

Cyber incidents that have occurred within the ICSE demonstrate how much susceptibility has been enabled due to the vulnerabilities, and the interaction between technology and people entities that constitute the environment. The adoption of technical security controls only provides a part of the overall solution, since human-factor vulnerabilities are often not considered. Any effective security management process requires considering both human and technology factors. Such security approach must focus on high-value targets in both entity classifications, so that no potential vulnerability is overlooked in a security management strategy. Security vulnerabilities in both technologies and people entities translate to security risks when related to likelihood and impacts. In the ICSE, security risk assessment offers a good method for controlling the impact of security threats, vulnerabilities, and impacts on technologies and human assets

There have been studies (Ralston *et al.*, 2007; Cherdantseva *et al.*, 2016) on security risk assessment approaches relative to the ICSE. In the approaches, varied schemes have been proposed for identifying threats, determining vulnerabilities, evaluating impacts of the vulnerabilities, and determining effective applications of security controls. To be able to ensure or improve security within the ICSE, all assets that function within the environment require to be protected. This can be achieved through analysing asset-level vulnerabilities which can pose significant security threats and estimate their impacts. Then, appropriate security policies, procedures, and tools can be applied to address the situations and reduce security risks. Risk assessment is quite a vast area, as such, many methods and tools have been proposed for assessing risk. A summary of the security risk assessment/management approaches reviewed are presented in Appendix A-24, however, these do not reflect an exhaustive outline, but only represent some selected methods that relate to this study.

From the reviews, security risk reduction through an assessment process proffers an invaluable means for improving security within ICSEs. Achieving this is characterised by some security analysis processes, which must account for all possible vulnerabilities within the asset that constitute the system and domain, especially the tangible active and

interacting components. System-interacting components include both technical (technology hardware and software) and non-technical (human and organisational) assets. It is necessary to understand the potential magnitude or severity of impacts that may be attributed to the successful exploitation of asset vulnerabilities. This can be effectively determined if the likelihood of attacks can be derived, along with a dependency modelling of data/communication flows amongst the system components. Dependency modelling is a key feature of a goal-oriented approach to risk management, which is proposed as an alternative to the reviewed failure-oriented approaches, and can proffer a better means towards achieving a more substantial understanding of ICSEs and their security risk factors (The Open Group, 2012). As against the hardly practicable failure-oriented mode of foreseeing all possible failure-modes and estimating likelihoods from cause-related logic trees alone, goal-oriented approach requires identifying elements and dependencies required to keep a domain (e.g. ICSE) and system operational, safe, and secure (The Open Group, 2012). This can support understanding the extent of impacts that may be enabled if a certain vulnerability is exploited. Such knowledge in relations to other vulnerabilities presents a good platform for deriving informed decisions about security control approaches that can be effective to address existing security risks.

From the reviewed ICSE-related security risk assessment method and frameworks, technology (hardware and software) asset form a huge and most tangible part of typical ICSEs, and the part that has enjoyed significant attention in terms of security management efforts and research. A contextual analysis of the risk management (assessment and reduction) methods indicate a general focus on technology-oriented security risks. Most of the studies that clearly address their contexts are observed to be limited to characterising or evaluating technology components, systems, and network configurations. Thus, only security risks associated to IT and OT components of an ICS are considered by the security risk management (assessment/reduction) methods. Other non-technology aspects that can attract security risks are not considered. 12 out of the 13 risk management (assessment/reduction) approaches reviewed centred on technology-oriented aspects. 10 out of the 13 risk management (assessment/reduction) approaches reviewed centred on technology-oriented aspects alone. Only 3 methodologies considered non-technical aspects of security. Notwithstanding, none of the 3 methodologies considered human-factor quantitative security capability and vulnerability evaluations from defender points of

view. Also, other non-technical factors like knowledge, skills, and culture are not considered.

Although beneficial, recent developments in security threats and vulnerabilities have made the technology-centred security risk assessment approach insufficient to provide an effective measure of security for ICSE assets. Both technical and non-technical (e.g. human factors) attributes are not typically included into a security risk evaluation and reduction method or framework. Human actors play significant roles in ensuring and improving overall domain-level security even from a risk management perspective. Cherdantseva (2016) stated that a clear and purposeful inclusion of human-factor security vulnerability analysis can help to characterise overall security states and prevent human-influenced compromises in the ICSE. Morgan (2013) also argues that monitoring and evaluation of human-factors can support the prevention of human-errors which may bring about unintended internal and external cyber compromises or intrusions.

When cyber security threats, vulnerabilities, and attack patterns are adapting both technical and non-technical dimensions, security risk management (assessment/reduction) methods and frameworks are required to adapt and cover both outlooks. Risk reductions should consider both technical and non-technical factors to achieve an all-encompassing view of security risks, controls, and improvements. An effective and responsive security risk assessment and reduction method should benefit from an in-depth understanding of an ICSE, including its components, interdependencies between components, and non-technical factors affecting the industrial environment. New risk assessment/reduction methods may draw from more precise accounts of human-factors such as end-user knowledge, skills, organisational security culture, and business processes (Cherdantseva et al., 2016). A holistic sense of security can be better gained when both technical and precisely human-factor attributes are considered and combined in a risk evaluation process and model.

3.4 Chapter Summary

The growing trends in ICSE security requires that effective security response depends on an adequate understanding of the security issues and risks that plague the industrial domain. Some of these issues include: security and safety implications of integrating open IT with proprietary ICS protocols and components, inadequately educating human-

elements about their capability/vulnerability states and impact on organisational security, adoption of appropriate tailored security standards and best practices, and weak or imprecise metrics development approaches.

A revealed need is for an enhanced method that would provide clearer, encompassing, and structured approach for generating security metrics that would be aligned to prevailing trends in the security landscape. It is noted that dependency relationship modelling of ICSE components using methods such as graph theory can help improve the process of vulnerability and impact analysis in ICSE. In addition, it is worth noting that regardless of any deployment of technical security in ICSE, human-factor security remains crucial and complementary towards achieving overall environment security. One way of achieving this complementing security is through user or workforce-centred security assessment, such that individual-level security capacities and vulnerabilities are characterised, as well as dominant weak security areas. These can support effective security response prioritisation. Combining both technical and human-factor security assessments can support a better assessment and reduction of risk within the ICSE.

4 INDUSTRIAL CONTROL SYSTEM TESTBED DEVELOPMENT AND CYBER-ATTACKS DEMONSTRATION

4.1 Introduction

In order to gain first hand insight into the security landscape of ICSE and explore the feasibility for determining and exploiting security vulnerabilities in an ICS, a real ICS environment is needed for a case study. A common approach is to use a testbed as an alternative to mirror the functionalities and processes of a real ICSE (H. Holm *et al.*, 2015; Soupionis and Benoist, 2015). A testbed approach can be used to support research in several areas of cyber-physical system or ICSE security such as; vulnerability research, impact analysis, mitigations research, cyber-physical metrics, data and model development, security validation, interoperability, cyber-forensics, and operator training (Hahn *et al.*, 2013). Hence, a testbed is constructed to provide data and information that can support research and analysis and bring about findings that can be attributed to the real ICSE.

This chapter focuses on the development of an ICS testbed, and the exploration of the potentials for identifying and exploiting technical vulnerabilities to compromise pre-configured functionalities and processes on the testbed network. Attack demonstration and insights related to vulnerabilities, attack patterns, and impacts dependencies are acquired, and analysed to provide a basis for other research objectives.

4.2 Construction of the Testbed

In NIST SP 800-82, an ICS testbed architecture include: *the control centre, the communication architecture, the field devices* and the *physical process*. The Control Centre relates to the computing servers and operator workstations used to remotely monitor and control field devices, such as Master Terminal Units (MTUs), Human-machine-interface (HMI), Engineering workstations, and data historians. The Communication Architecture comprises components that facilitate communication within the ICS network. Components in this category include; routers, switches and modems. Field Devices refer to the components that connect the physical domain to the digital or logical environment. Example of devices in this category include Programmable Logic Controllers (PLC), or other Remote Terminal Units (RTU). Scope of Testbed Representation and Description. A

small PLC-based product assembly and conveying system, denoted as ‘ICS-CS’, can replicate the assembly control process operation, and is representative of a small shop-floor control system setup.

4.2.1 The Hardware of ICS-CS

The ICS-CS testbed is built over local area network (LAN) using real-time Profinet industrial protocol for the communication between the field device controller and the physical process devices. Ethernet-based IP protocol-enabled communications devices were used to facilitate real-time deterministic data exchanges between the control centre and the field devices. The ICS-CS meets the minimum acceptable component requirements for ICS testbeds from NIST SP 800-82 standard. Thus, it can replicate control system configurations with specific applications for operational control of discrete event processes by reflecting the components of *ICS* control centre, communication, field devices and physical process (See Table 4-1). Complete descriptions of the components are presented in Appendix A-2. Screenshots of the physical testbed are presented in Appendix B-1.

Table 4-1: ICS-CS Testbed Components Mapping to NIST Standard

ICS Testbed Component Categories	Components in ICS-CS	Manufacturer
Control Centre	Control Workstation	Lenovo PC
	Human-Machine-Interface (HMI)	Siemens
Communication Architecture	Industrial Switch	Moxa
	Profinet Cable	Generic
Field Devices	Programmable Logic Controller (PLC) - with Extended I/O Modules	Siemens
Physical Process Devices	3D Robot Arm	Fischertechnik
	Conveyor belt and Punching Robot	

The testbed development included processes of technology (hardware and software) integrations, configurations, programming, vulnerability assessment, and exploitation. The ICS-CS components were assembled following the network wiring schematics presented in Appendix B-2. System configurations and automation programming of discrete event processes were implemented on the Siemens Totally Integrated Automation (TIA) portal installed on the control workstation. Appendices B-3 and B-4 present screenshots of the configurations performed. The PLC controls the conveyor/punching machine. The PLC and I/O Module share a direct communication connection on the Profinet network and makes

provisions for any extended devices to be added in the network. The HMI provides visual updates of processes running in the system. The HMI, PLC, and Control workstation are connected via the Industrial Switch which serves as the central communication hub of the network. Appendix B-29 and Appendix B-30 present the screenshots of the implemented network ICS-CS testbed in line with the network diagram.

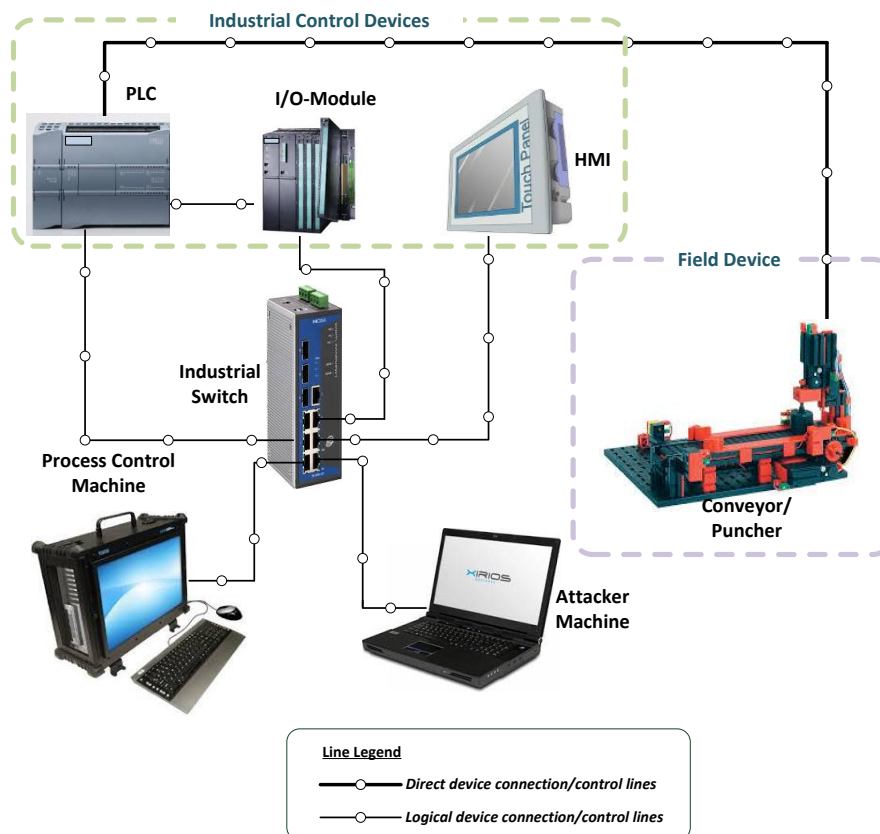


Figure 4-1: ICS-CS Network Diagram

4.2.2 The Testbed Process

The automated process replicated in the process flow in Figure 4-3 describes the flow of the activity for sensors detecting dropped items, and automatically actuating movement of the sensed product on a conveyor belt system. The conveyor system upon detection of item; moves the item to a punching position on the conveyor system, where upon a puncher arm is let down, which punches (labels) the item appropriately. When punching is completed, the punching arm is retracted back to its initial position, while the punched item is conveyed back to its source position. Because the process describes a simulation, a process loop is introduced to cause the item to be conveyed back to the puncher position

upon detection again. Each time the loop is executed the item conveyed assumes the position of a new item. The loop is introduced to keep the process running continuously as cyber-attack events are attempted. The aim is to observe the impacts in a continuous ICS automated process in the event of attacks. The ladder logic automation programming for the described process is presented in Appendices B-5, B-6, and B-7.

4.3 Cyber-Attack Demonstration

This section presents the demonstration of cyber-attacks on the ICS-CS testbed. Using real industrial components as indicated in Table 4-1, the aim of the cyber-attack demonstration was to explore practical potentials for identifying real vulnerabilities in varied components of the testbed and exploiting some of the vulnerabilities to disrupt pre-configured (normal) operations of the testbed system. This represented one of the potential ICS cyber security objectives feasible using testbeds (Candell, Stouffer and Anand, 2014).

Generally, ICS cyber-attack incidents and scenarios (past and present) tended towards exploiting one or more of six key broad vulnerability areas in the system. These include: weak authentication for ICS protocols, low processing power for ICS hardware, weak file integrity checks, weak user authentication in legacy control systems, vulnerable operating system platform (e.g. Microsoft Windows), and undocumented third-party relationships (Yusta, Correa and Lacal-Aránategui, 2011; Ani, He and Tiwari, 2017). For example, the German steel mill attack exploited weak user authentications (Lee, Assante and Conway, 2014; Harp and Gregory-Brown, 2016). Attack scenarios were adopted to exploit vulnerabilities in one or more of the above-mentioned vulnerability areas. The study demonstrates security vulnerabilities that are representatives in an ICS. However, the identification of vulnerabilities relied upon the outcome of a vulnerability analysis process in line with common Penetration Testing Execution Standard (PTES) (Johansen *et al.*, 2016) and security testing methodology. To achieve this, openly available and recommended security audit tools were used.

Key steps of PTES adopted included: (i) Reconnaissance (intelligence gathering), which is characterised by network/device profiling and vulnerability assessment, (ii) Target exploitation; also characterised by target selection and exploitation, and (iii) Result documentation; characterised by exploit outcomes and impact enumeration. Figure 4-2 presents the methodical flow described.

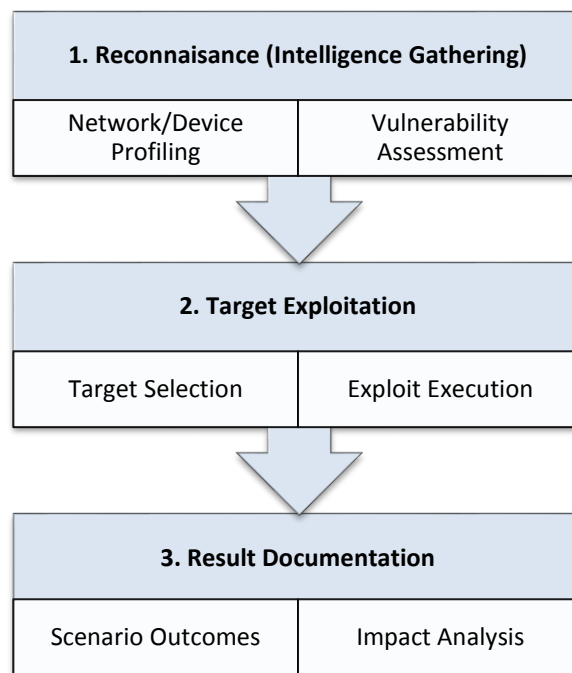


Figure 4-2: Scenario Demonstration Attack-plan

4.3.1 Initial Assumptions

To effectively demonstrate attack scenarios, some assumptions were made to satisfy initial testbed requirements and architecture, as well as provide sufficient justification for engaging the selected scenarios. The assumptions made include;

- The attacker is not part of the system development team
- An insider approach is adopted, where the attacker has access to the ICS-CS network.
- The insider attacker is actively connected to the ICS-CS network (LAN) as shown in the network diagram (Figure 4-1).
- Security features like firewalls, IDP, antivirus and other security capacities are not enabled in the system. This is in a bid to capture the potential states of traditional ICS network segments prior to the proliferation of insecurity trends.

4.3.2 Reconnaissance

For intelligence gathering about vulnerabilities on the testbed, *NESSUS*, an open source vulnerability Scanner (Tenable, 2017), was used. The tool was used to profile the network to discover functional IP-enabled assets, alongside open ports and running services on the network. Nessus was also used to scan each of the discovered devices, ports, and services

for vulnerabilities. *Nmap* and *Fping* utility tools were also used to scan the network for live hosts and open ports on each host. Nmap is a free and open source application software for network discovery and security auditing. It adopts a command-line interface (CLI) for executing security audit processes. Fping is a network utility program for probing active or live network components by sending ICMP echo probes to multiple network hosts. The results obtained from these tools were used to validate the results from the *NESSUS* scan to see where necessary resolve inconsistencies. The screenshot of the Nessus Scan results is presented in Appendices B-11 and B-12. Nmap scan results are presented in Appendices B-8 and B-9, while Fping scan results are presented in Appendix B-10.

20 documented vulnerabilities were discovered from the *NESSUS* scan with varied levels of severities. 1 vulnerability with 'critical' severity, 3 vulnerabilities with 'high' severities, 14 vulnerabilities with 'medium' severities, and 2 vulnerabilities with 'low' severities. In addition, 1 undocumented vulnerability with presumed 'critical' severity was discovered from extended research. Further analysis was focused on the critical, high, and medium severity vulnerabilities because they presumably posed more significant security risks to the network. The vulnerability with highest 'critical' severity of 10.0 was on the Engineering Control workstation and indicated a lack of security update for Microsoft Windows SMB Server. Exploiting this vulnerability could enable the total hijack of the affected asset and its dependencies. The three vulnerabilities with 'high' severities are the PLC, I/O module, and Ethernet Switch. This meant that exploiting any of these could pose potentially significant impact on the testbed. Also, 13 of the total vulnerabilities were found in the Engineering workstation, 6 in the ethernet switch, and 1 each in the PLC and its I/O module. This gives insight into the components where greater security evaluation and control are necessary to block a large proportion of security vulnerabilities on a modern ICS testbed. In this use case, directions point towards the Engineering workstation and the Ethernet switch. The outline of vulnerabilities and impact enumerations are presented in Appendices A-8 to A-13.

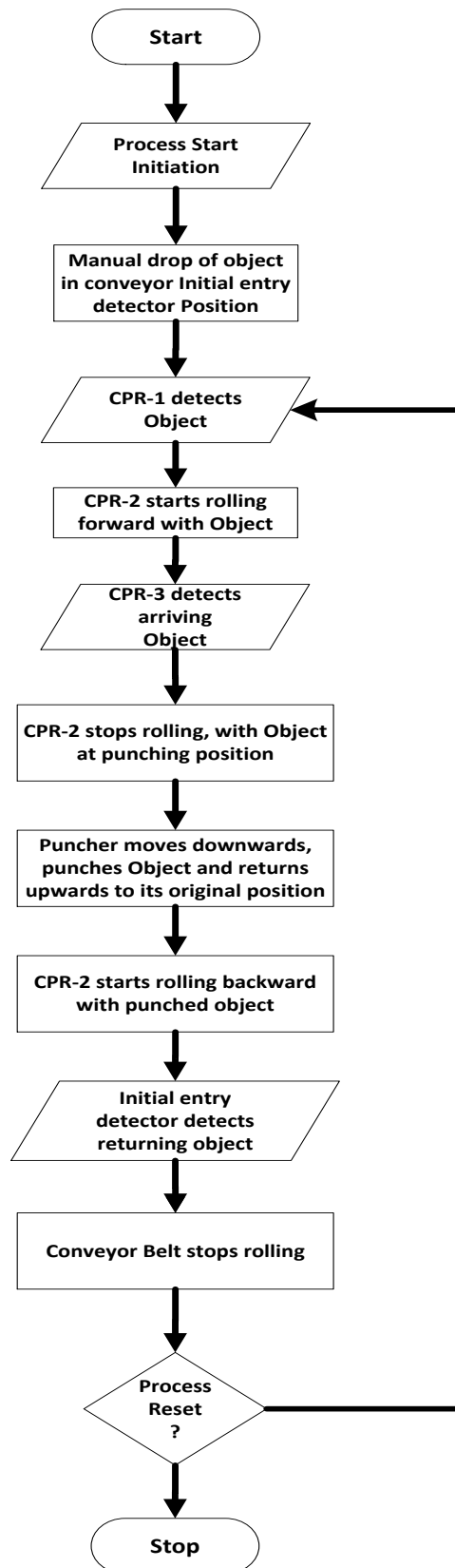


Figure 4-3: ICS-CS Testbed Process Flow Diagram

4.3.3 Target Exploitation

The target exploitation stage comprised simplistic attack scenarios involving both insider and outsider threat agents. The scenarios are adopted from a white box testing perspective (Johansen *et al.*, 2016), given prior knowledge of the internal and underlying technologies used in the testbed. The scenarios are aimed at testing how feasible it was to accomplish such attacks on the testbed type network. This would be different if the details of the network were completely unknown, for which a black box testing approach would have been used for scenario selection. The scenarios also represent the more common attack types used against real industrial system networks (Klahr *et al.*, 2016).

From the insider threat perspective, physical access privilege escalation was attempted on the Engineering Control Workstation based on the operating system (Windows 7) design flaw vulnerability discovered from extended research. Privilege escalation attack targets the violation of system integrity and confidentiality and may further enable the violation of availability. From the insider/outsider threat perspective, a denial-of-service (DoS) attack was performed on the PLC component of the testbed to exploit a potential resource exhaustion vulnerability discovered from analysis results. DoS influences the violation of availability on any targeted component and is often considered one of the key attack forms that greatly threaten the functionalities of ICSEs. More so, availability is considered a topmost priority in the ICSE. Using open source DoS execution tools such as Hping3, Metasploit framework, and SMOD (SCADA and Modbus DoS penetration testing tool), attacks were initiated against the PLC. In Table 4-2, the characteristics of the attack scenarios are presented for better understanding of the objectives targeted by each scenario. In Table 4-3, the attack scenarios and their target objectives are mapped to relevant security principle violations.

Table 4-2: Attack Scenarios Characterisation

Address	Device	Vulnerability	Description	Attack potential	Prospective outcome
192.168.1.11	Control Workstation (Computer)	Presumed design flaw in Operating system	Vulnerability inherent in systems (including servers) that run on Windows OS through which access is granted using a “KL live” instance.	Windows backdoor for file access and modification	Privilege escalation attack
				Privilege escalation	Administrative access
192.168.1.2	PLC	RESOURCE EXHAUSTION: Unauthenticated users to cause a denial of service (reboot) - Port 502	Modbus protocol port that listens to and accepts connection establishment requests	SYN flood attempt	Denial of service attack Privilege Escalation Cross-site scripting

Table 4-3: Attack Scenario - Security Violation Relationship

Threat	Vulnerability/Asset	Attack Direction	Attack Pattern	Violated Security Principle
Insider	Control Workstation Operating System	Physical	Privilege Escalation, Data Exfiltration, System Hijack	Integrity Confidentiality Availability
Insider or Outsider	PLC Modus Protocol Communication	Logical (Network)	Denial-of-Service	Availability

4.3.3.1 Scenario 1: Control Workstation Exploitation through Privilege Escalation Attack

From information gathered at the reconnaissance stage, a computer system exists with an IP address 192.168.1.11 and a computer name ‘XXX’. NESSUS operating system (OS) scan indicated that the system is running a ‘*Microsoft Windows 7 Enterprise*’. A further research on security vulnerabilities attributed to this OS platform indicates the possibility of a design flaw for service pack 1 distributions for computers running with default BIOS settings. Following an insider attacker threat agent who has access to the control system network and its components, the intent is to access the computer and steal data, and possibly change administrative credentials to block other valid administrators or users from accessing the system in the future. The exploit procedure included locating the system and using available tools or techniques to obtain escalated level access to the system. Initial assumption is that the physical security setups for protecting the target asset have been bypassed or compromised. A ‘bootable Kali live USB’ is used to attempt to gain access to

the computer and bypass the windows administrative login requirement that has been setup on the control workstation. The procedure for this exploitation is described as follows:

A. System Access and Modifications:

A bootable Kali Linux Live USB is used to gain access to the target system files and configurations. From systems32 folder of the 'Windows' partition, the file 'cmd.exe' is accessed renamed to 'sethc.exe', while the original 'sethc.exe' file is deleted. On restart, this procedure causes the Windows platform to launch a 'sethc.exe' file name with 'cmd.exe' executable instructions, which prompts and accessibility option to the computer.

B. New User Creation and Escalation of Privilege:

On windows platform, the 'Shift' key on the keyboard is pressed 5 times successively to call-up the command prompt where a new user credentials can be created with upgraded access privileges to Administrator.

The complete step-by-step procedure and screenshots for the above exploitation is presented in Appendix B-31

4.3.3.2 Scenario 1 Results - Privilege Escalation Attack Impacts

Following a successful login attempt after the exploit procedures, access was established to the target system (control workstation). The entire system resources; files, folders, programmes, etc., were successfully viewed and moved to the USB drive. Assuming a further intent of altering existence process functions in the system, the process-flow control automation program (TIA portal) and file can be accessed and reconfigured to manipulate the PLC into causing the conveyor machine to run in one direction alone, and not perform the earlier designed activity process. It is also possible to covertly plant any malicious virus/malware that could be used for executing future malicious activities on the system.

The elevated privilege enables the installation of new programs, modification of existing programs configurations, deletion of files, folders and programs, and the execution of any intending programs with malicious capabilities. Details and stored data of all other account holders/users in the system also become accessible and modifiable.

4.3.3.3 Scenario 2: PLC Denial-of-Service Attacks

A denial-of-service (DoS) attack is a type of attack that affects the disrupts or blocks the availability of a system, functionality, or service. DoS aims to put the target component services in an inaccessible state, and away from the desired or pre-planned objective state of the component. Generally, DoS attacks pose very significant threats to ICSE technology infrastructures due to the strict high-availability requirements of the system (Hahn *et al.*, 2013). In this scenario, potential impact of a DoS attack against the PLC component of the ICS-CS is explored. From the position of an outsider attacker threat agent, the PLC interface is flooded with massive volume of arbitrary data packets to overwhelm its response capacity and cause a disruption of genuine communications and functionalities. It is anticipated that the functions and operations of any component connected to the PLC will be impaired when the PLC becomes overly unresponsive to the component thereby disrupting designed system functionality. Flooding the PLC may be able to constrain its ability to transmit control traffic/data to other connected devices such as extended I/O module, HMI, and conveyor /punching device, which all rely on the PLC's data to execute their individual functionalities properly.

To execute this objective, two DoS attack patterns were adopted. The first included a TCP Syn-Flood attack using the *tcp-synflood auxiliary module* of the Metasploit Framework from a Kali Linux box, and the *Hping3* network enumeration utility also from Kali Linux. One instance of the Metasploit syn flood attack was combined with four instances of the Hping3 tcp syn flood attack. This generated huge number of packets directed at the PLC interface IP address 192.168.1.2. The attack was sustained for 25 minutes to help establish the stability of effects and impacts. Figure 4-4 presents the screenshot of the combined instances of the DoS attack. The screenshots of other exploit activities and outcomes are presented in Appendices B-15, B-16, and B-17.

A second DoS attack was executed using a freely available python modular framework programme called 'smod'. Smod is a full Modbus protocol diagnostic and offensive application designed to run on the Linux platform. It can be used for vulnerability analysis of a Modbus protocol. The smod module '*modbus/dos/galilRIO*' was used to initiate the DoS attack on the PLC interface IP address 192.168.1.2 as the remote host 'RHOSTS'. The attack was executed on port 502, which is the default port for Modbus protocol, and using 24 concurrent threads. The attack duration was 25 minutes. Figure 4-5 shows the

exploit execution module interface. The screenshots of other exploit activities and outcomes are presented in Appendices B-18 to B-22.

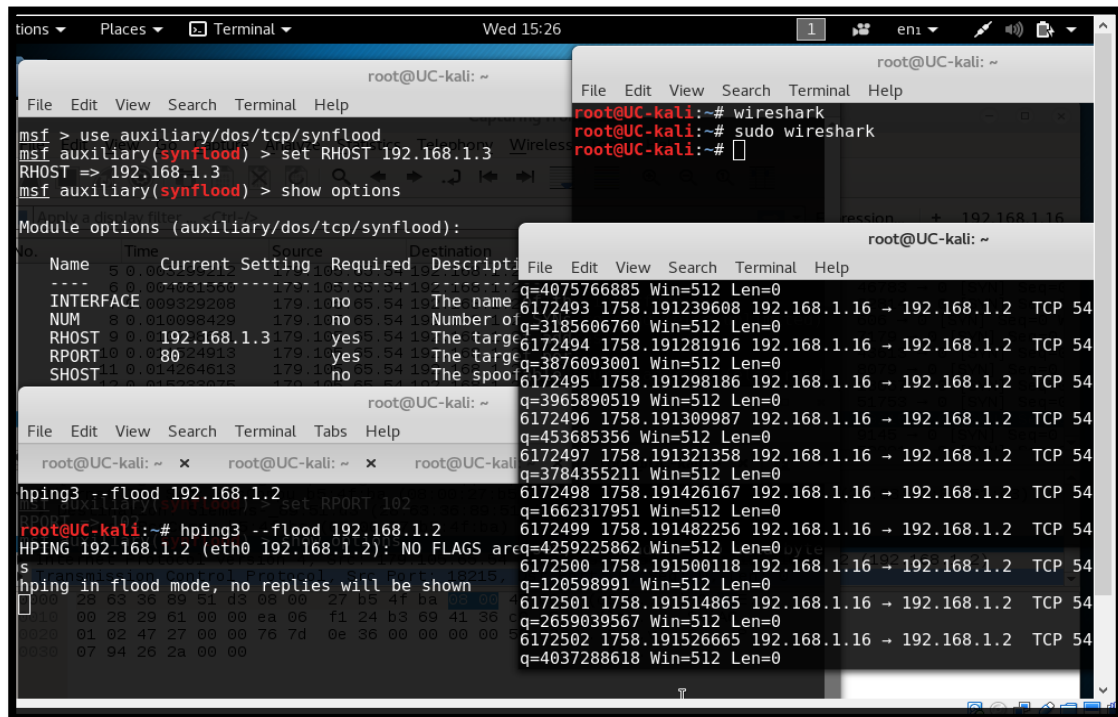


Figure 4-4: Metasploit and Hping Attack Execution Screens

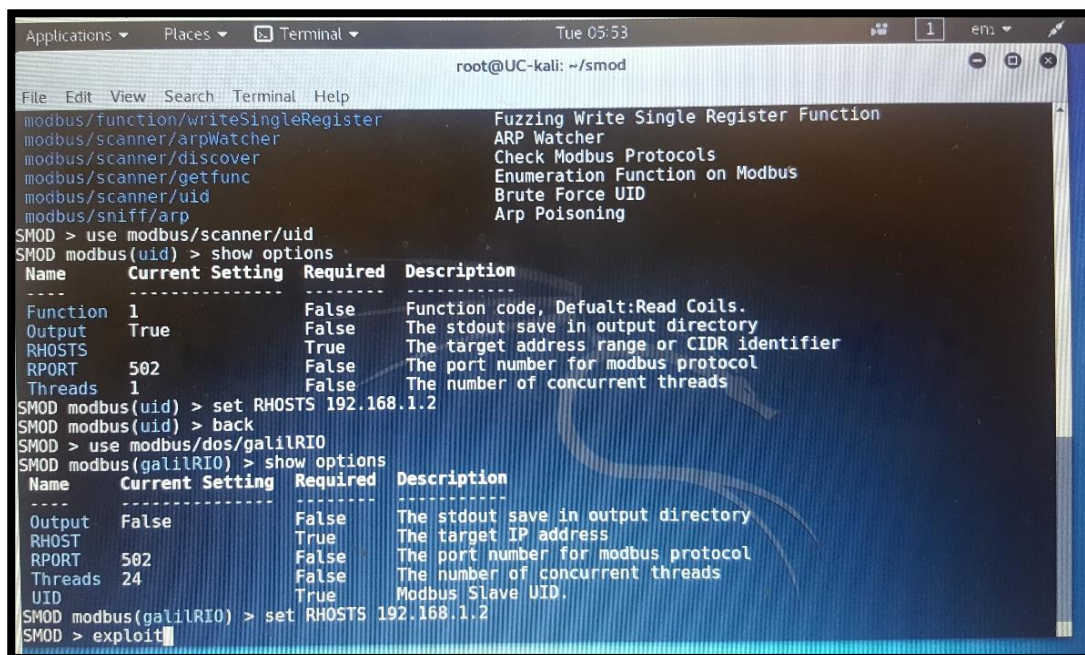
4.3.3.4 DoS Attack Results and Impacts

The impact of the two DoS attacks on the PLC are expressed by observing the physical and behavioural changes in the PLC, which may present a deviation from the predefined and preconfigured behaviours of the PLC. The statistics from the Hping3 syn-flood indicates that a minimum of 8,000,000 arbitrary packets were transmitted by each instance of the 4 syn flood attacks. The Metasploit syn flood framework module also transmitted about 6,000,000 arbitrary data packets to the PLC (from Wireshark packet analysis). These transmissions happened simultaneously, constituting a massive volume of packet that were hitting the PLC interface at the same time.

One of the direct effects of the floods on the PLC was an inability to maintain a connection and communication to with the HMI for gaining updates on the status functions in the PLC logic. This meant that the PLC only received partial and delayed data packets from the conveyor/punching equipment and transmitted in like manner to the HMI. Seamless flow

of data was being affected by the floods hitting the PLC and constraining it from giving full attention to the its (PLC) communication to the conveyor/puncher and the HMI.

Prior to the attack, all communications were normal with diagnostic and communication light indicator all 'green' on the PLC. However, during the attack, an error led (red light) appeared and kept blinking on the PLC as the floods continued. A similar red error led (RN light) was also blinking on the extended I/O module interface. This impact consequence signified an impairment on availability of the PLC, which also affected the functionalities of the extended I/O module and HMI interface devices. The configured processes handled and controlled by these devices (PLC, I/O Module, and HMI) were interfered with and stopped.



```
root@UC-kali: ~/smod
File Edit View Search Terminal Help
modbus/function/writeSingleRegister      Fuzzing Write Single Register Function
modbus/scanner/arpWatcher                ARP Watcher
modbus/scanner/discover                  Check Modbus Protocols
modbus/scanner/getfunc                   Enumeration Function on Modbus
modbus/scanner/uid                       Brute Force UID
modbus/sniff/arp                         Arp Poisoning
SMOD > use modbus/scanner/uid
SMOD modbus(uid) > show options
-----
Name      Current Setting  Required  Description
-----
Function  1                False     Function code, Default:Read Coils.
Output    True             False     The stdout save in output directory
RHOSTS    True             True      The target address range or CIDR identifier
RPORT     502              False     The port number for modbus protocol
Threads   1                False     The number of concurrent threads
SMOD modbus(uid) > set RHOSTS 192.168.1.2
SMOD modbus(uid) > back
SMOD > use modbus/dos/galilRIO
SMOD modbus(galilRIO) > show options
-----
Name      Current Setting  Required  Description
-----
Output    False            False     The stdout save in output directory
RHOST     True             True      The target IP address
RPORT     502              False     The port number for modbus protocol
Threads   24               False     The number of concurrent threads
UID        True             True      Modbus Slave UID.
SMOD modbus(galilRIO) > set RHOSTS 192.168.1.2
SMOD > exploit
```

Figure 4-5: SMOD DoS Utility Attack Execution Screen

A significant behavioural anomaly observed involved the HMI kept disconnecting and attempting reconnection to the PLC via the configured profinet network, which continued all through the attack duration. The blinking 'RED' error led indicates an error caused by a communication disruption or failure between a PLC and a connected component. Since the error was non-existent prior to the attack, it was certain that the error could only have occurred due to the attack that influenced a disturbance in the PLC. It implied that the DoS

attack on the PLC caused some disruption in communications between the PLC and extended I/O module and created a malfunction in both components. This malfunction in form of delayed or partial data reception and transmission affected the sensing and actuation in the field equipment connected to the PLC by halting PLC control functions.

The continuous disconnection of the HMI link to the PLC implies that the HMI was intermittently losing communication with the PLC, and every reconnection attempt also failed. This rendered the HMI unusable since it was not able to provide status update on the processes running in the control system during the attack period. The error lights on the PLC and extended I/O module, as well as the HMI disconnection-reconnection loop all stopped as soon as the DoS attack instances were terminated.

The impact of the DoS attack using the smod framework presented similar effects as already described. Blinking error led (lights) were observed on the PLC and the extended I/O module, which represented a faulty communication link between the two components. However, the effect seemed rather more severe as the faulty communication led remained even after the attack was stopped. This represented a permanent communication error on both devices and prompted the suspicion for a more severe impact needing investigation.

While investigating the error codes implication and possible resolution approaches from the Control workstation software terminal (TIA portal), it was discovered that the initial component and profinet network configurations had been wiped clean. An IP configuration 'RESET' had occurred on the PLC and extended I/O module. The profinet network was non-existent. This implied that the PLC was no longer having any link to any of the other components, i.e., no communication. This further explains and justified the reason for the permanent communication error led (red light) left on the components even after the Smod DoS attack was terminated. The only feasible resolution involved calling up any backup control configuration and reloading the configurations on all devices. In worst cases where backup configurations are not available for immediate restoration, it required a fresh reconfiguration process for the entire system including profinet connections. The system would have to remain un-operational until the reconfiguration is completed. This impact reflected a complete and permanent loss of system availability until a restoration is achieved.

4.4 Discussion and Conclusions

The outcomes of the attack scenarios indicated a strong feasibility for cyber-attacks on ICSE technology infrastructures. These attacks can take both physical and logical dimensions. The insider mostly relates to the attacks perpetrated by or with the support of insiders with knowledge and(or) access to the ICSE infrastructure. While logical attacks include both insider and outsider attack threat agents. The violation of system or service availability poses a most significant threat to the ICSE due to the requirement of the system to support high-availability and operational continuity. In real life situations, this physical attack often involves the process of accessing and enabling elevated privileges on target system for some other malicious intents. This type of exploitation and attack requires knowledge of the internal structure and network of a target control system environment, and(or) with some valid access credentials. Adequate system and target profiling is necessary to learn the system that retains the desired data or information and vulnerability. Nonetheless, key targets of this type of attack within ICSE include Central Controllers, SCADA Servers, Web servers, data historians, which run Microsoft Windows OSs in their default configuration states. Also, these systems often contain details about other potential systems or process targets and used to control other industrial equipment.

Attacks on availability from the DoS perspective can also have varied levels of impacts on an ICSE depending on the complexity and target objectives of the exploit, attack techniques, and tools. Most often, a DoS attack targets a specific component within the network, but by attacking a certain component, network bandwidth, seamless communication and data/packet exchange, and component functionalities are potentially going to be limited or inhibited. Non-targeted component may well share in the consequences of a DoS attack either directly or from a cascade point of view. DoS attacks on ICSE networks can cause temporal loss of availability, which can often be restored when the attack is isolated or eliminated. However, there are extreme peculiar situations where DoS attacks can also cause permanent losses of availability that often require a significant amount of resources and time to restore availability for affected components. Learning these varied vulnerability, attack, and impact potentials can help ICSE owners and security expert to engage or adopt the appropriate measures and strategies for protecting their ICS technologies and processes from malicious attacks. An illustration of

the potential direct and cascade impacts (both observed and projected) of executed attack scenarios is presented in Figure 4-6.

These attack scenarios and outcomes highlight that security vulnerabilities can be in any ICS-CS setup. If these vulnerabilities are exploited, the consequences could bring about severe destructive impacts in relations to the violation of very crucial security requirements of the system and environment. The benefit of using this attack simulation design is that it becomes easy to observe the direct impacts of exploiting certain vulnerable components of a larger ICS network. With this it becomes easy to estimate the scale of impact and determine the most appropriate measure of security and control required. The disadvantage is that in large networks where components from several manufacturers are in use, the knowledge of a vulnerability in one proprietary component may not be the same in a similar component from a different manufacturer.

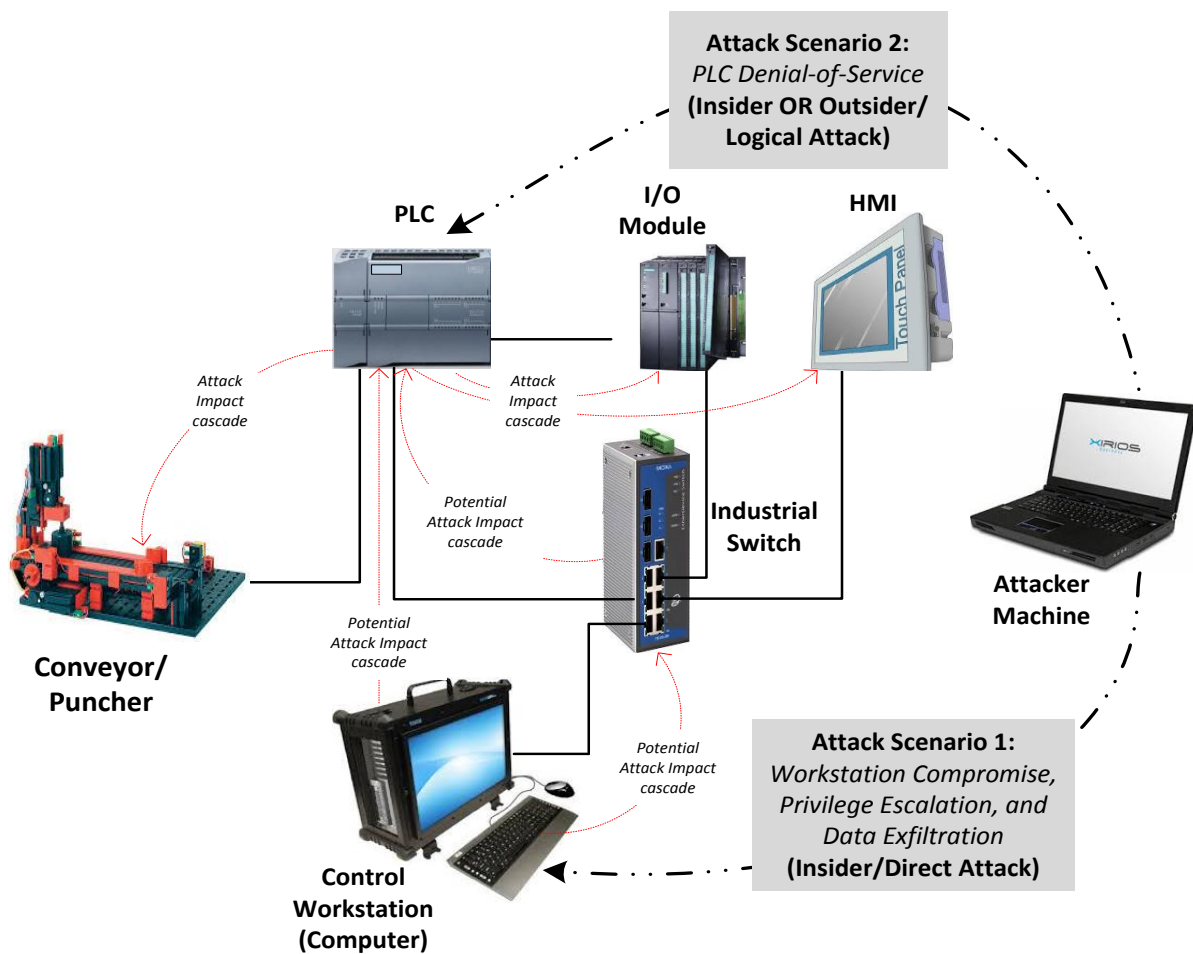


Figure 4-6: Attack Scenario Impacts and Cascade Illustration

Thus, since a one-size fits all knowledge about vulnerabilities in components may not be feasible, nevertheless, such knowledge in one manufacturer infrastructure offers insights about potential security audit lookouts in others and may well speed up audit processes overall.

The impacts observed from the scenarios in this study can be related to potential impacts in a real environment. For example, for the DoS scenario on the PLC, a successful attack brought about the disruption of discrete event process control and monitoring. Communication transfer to the Physical process equipment (conveyor robot) was also inhibited. This demonstrates the interruption of interaction between the target PLC and other devices linked to it, causing the process of moving and punching items enabled by the interactions to be affected. In a real ICS environment, similar attack might not be restricted to a single device target but can expand to other process control network infrastructure depending on the damage objectives of the perpetrator(s). In extreme cases, operational activities can be hindered, causing significant loss of operational downtime, production losses, and additional recovery costs. Brand reputations and customer satisfactions can also be affected.

Another point worth noting is that viable attack potentials might not require high skills and expertise to accomplish. A low or medium knowledge and skill in hacking and intrusions can as well do the job. This suggests that with the proliferation of free (open source) exploitation tools and handy online guides, any system users that is highly motivated even without expert hacking skills and knowledge but determined to sabotage such a system can achieve their desired malicious objective(s) against any target ICS-CS critical infrastructure. Not much training or difficulty is required to accomplish basic attacks on typical industrial networks such as the ICS-CS network. Therefore, a capability is enabled that empowers every potential cyber attacker; proving that a measure of capability for a cyber-attack is genuinely a function of some measure of knowledge, and skills.

This work suggests that only a similar capability from a defensive (protective) perspective would be able to nib these potential cyber coercions in the bud and bring about the potentials of a more cyber-secure ICSE. It emphasises the need for improved security criticality analysis, estimation of impacts, and prioritisation of controls, since it may be infeasible to resolve all discovered vulnerabilities at once. More so, it may not be necessary

to treat some vulnerabilities given their low severity and impact estimates. The attack results also cast emphasis on the need for proper ICS-specific cyber-security threats and vulnerabilities awareness, the building or enhancement of cyber-security skills of the industrial, and all that depend on it. This can be considered the most reasonable measure for amplifying protective capabilities within the industrial/manufacturing environment.

In addition, the attack results also provide a means for verifying the testbed design and implementation. For example, from initial testbed design and implementation, the PLC is configured from the Engineering control workstation to control sensing and actuation events on the conveyor robot. The control flow is enabled through the Ethernet switch, and these events are monitored from the HMI. Under unperturbed conditions, the discrete event process execution remains unchanged and considered correct as desired. The results of the DoS attack scenario can be used to verify this implementation. The flood of spurious data packets to the PLC causes it to lag in its interaction with the conveyor robot and inhibit updates to the HMI. This effect proves that there were prior connections and interactions amongst these testbed components from design, which are altered by the DoS action. Results also indicate that communications are restored to normal once the DoS events were stopped. It is safe to conclude validity about the design and implementation of the testbed as attack results can show a difference between the desired unperturbed design and its altered state.

5 SECURITY METRICS GENERATION FRAMEWORK

5.1 Introduction

The growing increase in targeted cyber-attacks and successful incidences on ICSEs have stirred up the quest for improving capacities and investments in securing critical industrial infrastructure platforms and setups. Security objectives in an industry control environment can be chiefly achieved through regularly checking the performance of systems and the environment guided by security metrics derived from the security objectives (Savola, 2009).

Here, security metrics are defined as *‘a collection of measurable properties of an ICS constituent elements and attributes that enumerate the degree to which ICS cyber security assurance are achieved’*. Security metrics can be viewed as a system of related dimensions (matched to a standard) that allow for evaluating the degree of freedom from possibility of suffering damage or loss from malicious cyber-attacks, or to which the system or network objectives are achieved (Reichert et al., 2007; Collier et al., 2016). They are often designed to arrive at measures that facilitate decision-making, and improve performance and accountability through evaluations (collection, analysis, and reporting) of relevant system status (Chaula, Yngström and Kowalski, 2004). They are also supportive for predicting system security states and determining security assurance level (Savola, 2007; Beres et al., 2009).

From an economic perspective, security metrics can be used to illustrate the business impacts of security, thus enabling the integration of security functions into the overall business process (Chandrakumar et al., 2013). However, precise and efficient security metrics are feasible from a well-defined semantic process of identification and selection, which helps to ensure that selected metric quantities and their outputs are relevant and fit for purpose or use (Homer et al., 2013).

5.2 The Framework for Operational Security Metrics Generation (OSMG)

The OSMG framework aims to overcome the weakness of a lack of clarity and methodical guidance for producing security metrics in response to clearly defined security objectives by organisations (Jansen, 2009). It should account for varied security scopes, dimensions,

and attributes definitions, thus, to provide a step-wise guideline to relevant component/attribute considerations in the selection and adoption of security metric quantities. It can be used be use at the planning stages of security audits and analysis by industrial security analysts, developers and system owners.

The framework illustration presented in Figure 5-1 defines the semantics for ensuring that the output of a metrics generation process has clear relevance and meaning with respect to certain pre-conceived objectives and resulting inputs. The inputs represent the factors for consideration at varied phases towards arriving at desired security metric quantities from a pool or collection of security metrics available. It seeks to clarify answers on if the security metric quantities adopted is representative of the security objective(s) and dimension(s) of interest and evaluated. To address the limitations in existing models, the OSMG framework combines the features of existing security metrics development frameworks, and best practice standards and guidelines, such as NIST SP 800-53 (NIST, 2013b), NIST SP 800-82 (Stouffer *et al.*, 2015), NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.0. (NIST, 2014).

The OSMG framework extended the model for aggregating technical security metrics by Holmer *et al* (2013) to capture other key areas beyond technical security metrics dimensions for. It includes both process and people (human-factor) security metric dimensions. All three dimensions of People, Technology and process are considered necessarily in every metric selection process to capture the entire spectrum of an ICSE. The uniqueness and strength of the OSMG framework is that it assembles several framework characteristics into its structure by logically harnessing varied strengths of existing approaches and producing an improved approach for security metrics generation from a wider/large collection of metrics. For example, it integrated the merits from: top-down and bottom-up concepts (Stoddard *et al.*, 2005; Payne, 2006), ideal-driven model (McQueen *et al.*, 2008), adaptive capability concept (Nguyen, 2012; Linkov, D. . Eisenberg, *et al.*, 2013; Savola and Abie, 2013), hierarchical interdependency model (CIS, 2010), review and refinement concept (Payne, 2006), control and compliance-driven models in TSMM (M. P. Azuwa *et al.*, 2012), and defense-in-depth strategy (Chandrakumar *et al.*, 2013). Security analysts and experts within industrial organisations can use the OSMG framework to guide the selection of appropriate security metric quantities relative to defined security audit objectives of interest.

The main differences between OSMG framework and other frameworks and methods lie in that the OSMG framework provides (i) a broader view of relevant factors necessary to be considered in the processing of selecting security metrics, (ii) a decomposition of associated sub-factors that whose consideration can simplify the process of understanding and identifying necessary security metrics in line with desired objectives, (iii) a structure flow for input and outputs in the security metrics generation process, and (iv) a two-way approach for accomplish security metrics generation following guided formats.

A good metrics development approach should have some essential characteristics such as: *scope-definitive*, *objective-oriented*, *reliable*, *simple*, *adaptable*, and *repeatable* (SORSAR). ‘*Scope-definitive*’ property of a security metrics development framework should make for the specification of scopes and constraints in relation to the dimension of security (offensive or defensive) for which metrics are required. It should also allow for the articulation of target network segment (enterprise or industrial control), and the precise system constituents (people, processes, technologies) to be measured. ‘*Objective-oriented*’ characteristic provisions for the precise articulation of security objectives targeted by the metrics. These could include both the primary (safety, availability, integrity, confidentiality, and accountability) and secondary (decomposed) security objectives, and the articulation of the violation principles being considered.

The ‘*Reliable*’ property outlines the requirement of a development framework to yield desired and consistent metrics in line with consistent objectives and scope. ‘*Simple*’ emphasises the characteristic of framework to be easy to understand and straightforward to employ or use. ‘*Adaptable*’ defines the requirement of a development framework to be easily bent or tractable. A good framework should be adaptable to different security scenarios, objectives, and tweaked to suite varied dimensional changes. ‘*Repeatable*’ emphasises the need for a development framework to allow for the repetition of process and procedures where necessary; in response to the need for modifications and improvements in metric quantities of measurements. The concept of iterations is a necessary to keep pace with the dynamisms that might emerge.

The development of the framework of ICSE security metrics, following the SORSAR properties, could contribute to creating strong and fit-for-use security metrics that can meet the ever-dynamic changes in the current security landscape. As represented in Figure 5-1,

the OSMG framework includes three phases: (i) Target definition, (ii) Objective definition, and (iii) Metrics Synthesis.

5.2.1 Target Definition (Phase 1)

This involves describing the attributes that give clear information about the target system or environment for which security metrics are being generated. It includes defining the measurement scope, the target segment, and the specific constituent(s) from which metrics will be derived.

5.2.1.1 Security Dimension (L1 Scoping)

This outlines the potential perspectives through which security can be rationalised. Traditionally, security can be construed from 2 outlooks: (i) Capability, and (ii) Vulnerability. The security state of a system can be measured based on how strong or weak the system can be to circumvention. It is, therefore, important to articulate the dimension of security especially at the beginning of every security metrics development process. This concept presents a high level-1 (L1) scope definition that signifies the beginning of defining a clear direction for the security metrics development process.

i. Capability

Security capability characterises the strength to uphold a protected state, and is measured by how difficult it is (or will be) to circumvent inherent protected capacities (Schechter, 2004). Metrics for evaluating security capability or strength should include the measurement of time, effort, and other resources necessary to breach a system's protections. These metrics can be observed when taking the perspective of an attacker or adversary. Attack graphs, attack trees, and other security analysis paradigms (Kotenko and Chechulin, 2013; Wang and Liu, 2014) can be used to characterise potential attacker actions in the light of a system's scope or configuration in the security capacity.

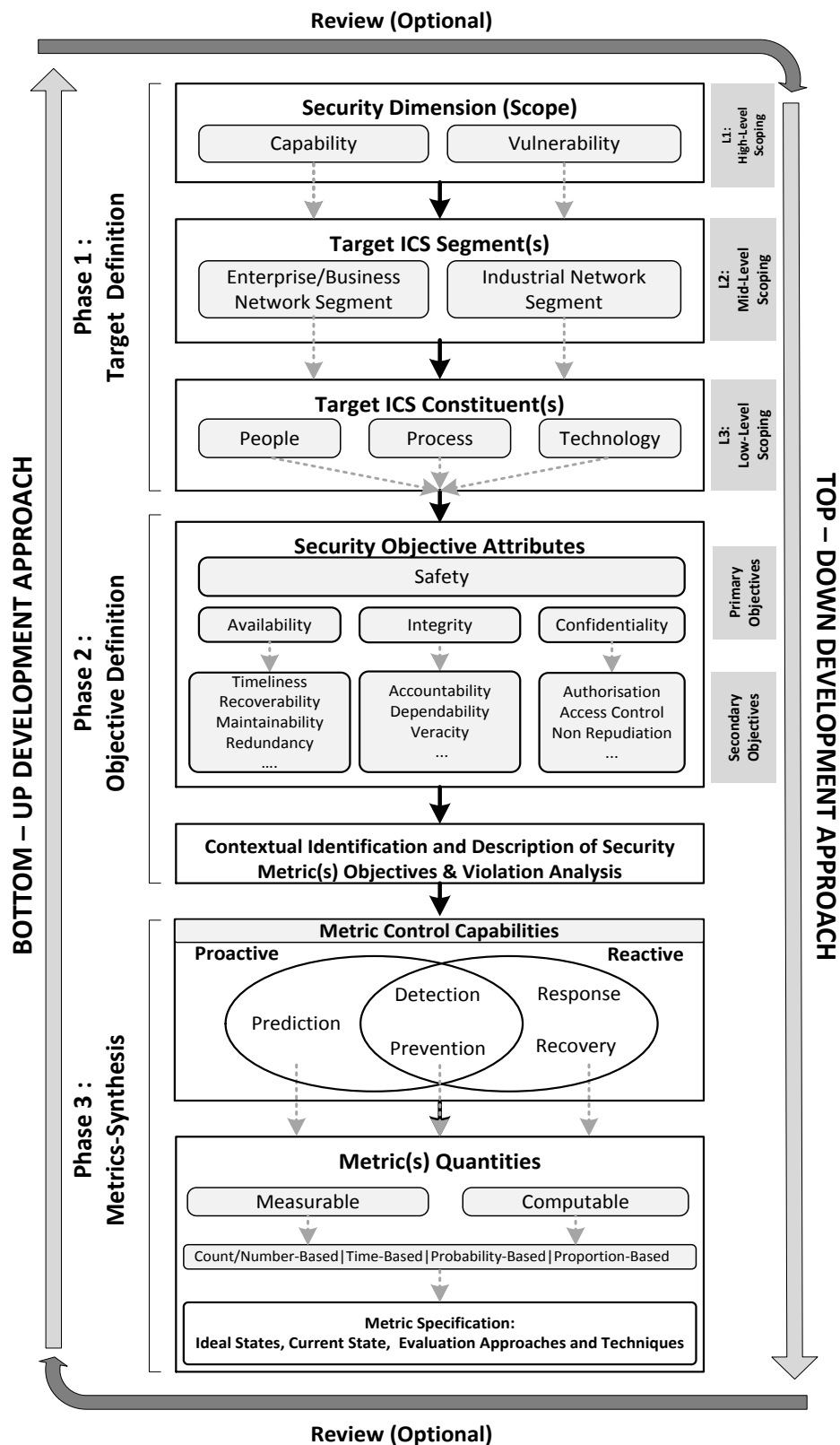


Figure 5-1: Operational Security Metrics Generation (OSMG) Framework

ii. Vulnerability

Vulnerability is the flip-side of security capability and emphasises the inability to achieve or sustain a certain (normal or protected) state. Technically, vulnerability outlines the ease of rupturing a system's normal or security state observed from a defensive point of view. Many methods have been used to derive metric values from representing system susceptibilities to potential threats and attacks, such as defense trees (Bistarelli, Fioravanti and Peretti, 2006; Bistarelli *et al.*, 2012), the CVSS paradigm (Abraham and Nair, 2014a; Keramati and Keramati, 2014; FIRST, 2015), and the change-point detection evaluation approach (Lei *et al.*, 2016), etc.

5.2.1.2 Network Segmentation (L2 Scoping)

Typically, modern ICSE architectures encompass a wide area network (WAN) integrating industrial operational technology (OT) networks with enterprise information technology (IT) networks (Stouffer *et al.*, 2015). The two networks are different in technologies and protocols, and most times require different approaches, metric quantities, and policy priorities for evaluating security features and states. System segment could also be based on assets or system functionality, configurations, or security requirement (Defence Signals Directorate, 2012). Hence, a level-2 (L2) scope definition is provided to specify a large ICSE network architecture to which security evaluation is focused.

5.2.1.3 System Constituent (L3 Scoping)

With a clearly defined security dimension, and an understanding of the target segment of a security metrics development process, it is also necessary to specify the constituent of the segment of interest/focus. A network segment is a sub-system that would basically be made up of several interacting constituents or entities. The IT and OT segments of an ICSE are made up three inter-operating, value provisioning, structural constituents: *technology*, *people*, and *process*. Every emergent metric quantity should measure characteristics of one or more of the three constituents, and express corresponding capabilities. It would be better to have a constituent-oriented metric development. This will help simplify the task of generating and analysing metric quantities, and generally speed-up the development process.

5.2.2 Objective Definition (Phase 2)

Metric quantities should typically provide information that guide towards the attainment of pre-defined or pre-conceived security goal and objectives. Such goal-oriented security metrics require defining security objectives first.

5.2.2.1 Primary and Secondary Objectives

In the ICSE, safety seem more important than security and should be considered a necessary critical objective. Safety seeks to preserve from death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (Stouffer *et al.*, 2015), while security emphasises the protection of technologies, processes, and data from malicious compromise in the contexts of the AIC triads as discussed in section 3.1. The scope of this work does not extend in-depth to the concept of safety but focuses on security.

For clarity in development process and results, it is necessary to decompose the primary security objectives into corresponding secondary security objectives. This should be in line with business/operational objectives, and the envisaged security violations that potentially threaten the actualisation of the desired business/operational objectives.

The secondary objectives specify deeper actionable security principles targeted in the metrics development process. For example, availability objectives could be decomposed into timeliness, recoverability, redundancy, maintainability, etc. Integrity objective could be decomposed into accountability, authentication, non-repudiation, dependability, veracity, etc., while confidentiality objective could be decomposed to authorisation, access control, etc., (NIST, 2013b; Stouffer *et al.*, 2015).

5.2.2.2 Contextual Description

The objective definition phase is concluded with a contextual description of the target state of the security objective desired by resultant metrics, and the analysis of violation concepts. A descriptive statement should plainly states the objective end of the metrics selection and measurements (Payne, 2006) in line with pre-defined security objectives. For instance, a contextual security objective description could read '*to provide security metrics that plainly and easily communicate the degree to which system technologies can effectively control security threats, vulnerabilities, and attacks, to guard against operational disruptions*'.

Here, primary objectives include ‘availability’ and ‘integrity’, and a secondary objective could include ‘redundancy, reliability, veracity, dependability, and access control’. Contextual security objective descriptions should be clear enough to enable the derivation of prospective action plans for the attainment of prescribed security objectives. Contextual description could be guided by relevant security standards such as NIST SP 800-53 (NIST, 2013b), NIST SP 800-82 (Stouffer *et al.*, 2015), and NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.0. (NIST, 2014), etc.

5.2.3 Metrics Synthesis

In this phase, the focus of security controls is defined, appropriate metric quantities that satisfy objective criteria are selected from the collection of available metrics. The criteria considered include; control capability direction, related metric quantities, and metrics specification.

5.2.3.1 Control Capabilities

Existing security control efforts and implementations basically take-on one of two broad control capabilities: proactivity or reactivity (Lin, Wang and Huang, 2013; Kwon and Johnson, 2015). Thus, security metrics should mirror similar disposition. Security metrics can adopt proactive capability direction, where measures are derived to give perspectives about future security or vulnerability states. Proactive capability directions can also help guard against potential future security threats and risks (Abraham and Nair, 2015b).

Control capability sub-direction attributes within the proactive context include: prediction, detection, and prevention. Security control efforts can also assume reactive dispositions, in which case metric derivations are obtained to give outlooks about current security states (Musliner *et al.*, 2014), or indicate what is required to control or counteract the effects and impacts of security compromises that already occurred. Control capabilities in this regard include detection, prevention, response, and recovery. Furthermore, security metrics could combine both capabilities into what is termed a ‘*hybrid*’ capability. This yield measures and metrics that capture the perspectives of both proactivity and reactivity. The occurrence of detections and preventions in both directions indicates their importance and relevance in any security metrics development process. Any security metric taxonomy should capture among other features; quantities that articulate capacities for both detection and prevention.

5.2.3.2 Metric Quantities

With a clear definition of desired metrics control directions, it becomes easier to generate or select specific metric quantities and specify their attributes. Prior works (McQueen *et al.*, 2008) indicate that security metric quantities can be derived computationally; applying mathematical concepts, or via measurements using scales and instruments. The outcomes can be as a single measurable attribute that is representative of the state of a system or security phenomenon, e.g., security evaluation deficiency count, known vulnerability days, and password crack time metrics (Homeland Security, 2009). However, metrics can also be derived from the combination of two or more disparate attributes, from which a single quantity emerges and is representative of the security perspective desired. This is referred to as '*composite metrics*' (NSA, 2010). Metric quantities can be further defined based on the unit or base for measurement, and accordingly; can be count or number-based, time-based (McQueen *et al.*, 2008; Abraham and Nair, 2015b), probability-based (O'Neill, 2013; Keramati and Keramati, 2014), proportion-based (Abbadi, 2006), or cost-based (Peuhkurinen, 2008; Aissa *et al.*, 2014). It is appropriate to clearly clarify these units in relation to each metric quantity in the taxonomy to be generated, and to understand the interpretation of each metric in relation to pre-defined security objectives of the system.

5.2.3.3 Metric Specification

A metric specification profile is required for every metric quantity generated during the development process. A metric specification refers to the identification and description of the attributes and development procedure that embody the structure and totality of a metric quantity. A metric specification is described as a function of a metric's current state/value (quantitative or qualitative), an ideal state, and an evaluation technique for obtaining the metric measures. These are relevant in describing a metric since consistency (expressed by the gain of repeatable results in measurement technique) is a characteristic of good metrics (Chandrakumar *et al.*, 2013), and is considered of higher priority than the decision of measurement subjectivity or objectivity (Henning *et al.*, 2002). Since the goal of any measurement is to determine if a system constituent meets its security objective as defined in the metrics profile description, such descriptions help proffer quicker and clearer understanding and interpretation of each metric, and the corresponding implications in relations to targeted objectives.

i. Symbolic Representation of Specification

Symbolic representations offer an easy way to capture and visibly demonstrate concepts, ideas, and attributes by showing the various features that encompass their relationship structure. It is considered a suitable approach for gauging and representing plans comprising of sequences of actions in a continuous, low-level domain or perspective (Konidaris, Kaelbling and Lozano-Perez, 2014). For better understanding, the OSMG framework can be represented symbolically as a *septenary set* comprising seven state vectors, namely **{D, S, d, PO, SO, CC, M}** based on the relationship among the three (3) development phases and their corresponding sub-phases as shown in Figure 5-1. The symbolic septenary relationship is described in detail as follows:

D : {Cap, Vul} is a set of all security dimension for metrics development, where Cap and Vul represent capabilities and vulnerabilities respectively.

S : {Entr, Indr} is a set of all target network segments within the ICS network for which security metrics are required. Entr and Indr represent Enterprise and Industrial Network segments respectively.

d : {d = 1, 2, 3, ..., n} is a set of all system constituents or devices for a target network segment.

PO : {A, I, C} is a set of all primary security objectives targeted by the metrics development approach, where A, I, and C represent availability, integrity, and confidentiality respectively.

SO : {so_i|i=1...n, so_i → A ∪ I ∪ C} is a set of all secondary security objectives related to a targeted primary objective.

CC : {Prd, Det, Prv, Rsp, Rcv} is a set of all control capability directions, where Prd, Det, Prv, Rsp, and Rcv represent Prediction, Detection, Prevention, Response, and Recovery respectively.

M_d : {m_j | j=1, 2, ..., n} is a set of all metric quantities deducible from constituent d.

With this, a metric specification (as described in subsection 5.2.3.3) for a resulting metric quantity can also be represented using a quinary set comprising of five state vectors, namely {M_d, d, I, C, E}, such that:

$$(M_d) = f(I_d, C_d, E_d)$$

where:

$I_d : \{s_1, s_2, s_3, \dots, s_n\}$ is the set of all respective ideal state values for the metric quantities M_d . The value of I is defined based on acceptable security states of M_d from prescribed security requirements.

$C_d : \{c_1, c_2, c_3, \dots, c_n\}$ is the set of all respective current state values for the metric quantities M_d . The value of C is derived via measurements or computationally.

$E_d : \{e_1, e_2, e_3, \dots, e_n\}$ is the set of all respective evaluation techniques (approaches) for the metric quantities M_d .

The above variable definitions and criteria provide basis for identifying and selecting corresponding metric quantities for an available pool. A non-exhaustive collection of security metrics from prior works is presented in Appendix A-25. This pool of security metrics is used as a sample collection to validate the usability of the proposed OSMG framework.

5.2.4 Structural Flow and Review

The proposed model supports the top-bottom approach of metrics development. Nonetheless, it can as well adapt to a bottom-up approach. The top-bottom approach describes the scenario of starting the metrics generation process from the definition of target system and follow down to the point of achieving metrics specification profile. The bottom-up approach describes the reverse process involving when generation may commence from identifying a metric of importance and then working up the metric characterisation process. These two approaches are captured by the two directional arrows (one directing up and the other directing down) surrounding the framework structures. It is suggested that the choice of direction should be entirely dependent on organisational convenience, expertise, and the perception of a most suiting approach towards achieving targeted goals. However, for easy, better structured, and most appropriate synthesis of security metrics, the top-down approach is recommended. Because, it might be better that the security metrics development should follow the system development life cycle, where the system provides a broad concept of security metrics for industry control environment. it may be a better approach to obtain metric quantities following a holistic understanding of what the metrics are meant to target, measure, and resolve.

It is also pertinent to engage formal reviews and reassessments of metrics taxonomy periodically, to check the relevance and appropriateness of current metrics taxonomy in relations to evolving security trends and the operational dynamics of the industrial environment. The two directional arrows at the top and bottom of the framework structure are used to capture review and reassessment requirements accordingly. It is crucial to resolve questions about continual relevance, accuracy and reliability of metrics, and their usefulness in determining new courses of actions for the overall attainment of pre-defined security objectives (Payne, 2006). The review will also help to assess the worth of efforts and techniques for generating metrics, and the reassessment of emergent external security metrics, standards, and best practices for improving existing internal metrics taxonomy. This study lends voice to the NIST SP 800-82 r2 ICS security standard (Stouffer *et al.*, 2015), which emphasises that as trends continue to emerge and evolve in security threats, vulnerabilities, breach patterns, techniques, and impacts, it is important for security metrics and their development approaches to take-on adaptive natures, adjusting to strategies as circumstances change.

5.3 Implementation and Application of the Framework

The OSMG framework can be implemented in various instances. The black-shaded phase and sub-phase transition arrows indicate mandatory transitions of implementation flow, while the grey-shaded sub-phase transition arrows indicate optional/selective transition inclusions. By these, it means that it is not in all cases that all phases and transition features will be reflected in a metrics generation process. Rather, the application environment's target security objective(s), desired security dimension, and control capabilities of interest determine the phase and sub-phase transition to be followed. This will also determine the varied security metric quantities that can emerge. For example, for an environment whose security improvement focus is on the people (human) perspectives, the security metric quantities that would be derived using the approach would clearly differ from the environment with focus on technology security perspectives. Similarly, an organisation that desires to evaluate security capability of its system via a combined technology and process perspective, would most often use different security metric measures from the organisation that desires to learn organisational security vulnerability of technology, process, and people dimensions.

The proposed framework presents an open approach to the enumeration of key dimensions, objectives, and control capabilities that can be considered in a security metrics development process. Security Capability and Vulnerability both represent different viewpoints through which security evaluations can be explored. Such evaluations can focus on either the business network or the industrial operations network, or both. Similarly, technologies, people, and process, all represent distinct constituents where security evaluations can be focused. In some cases, security evaluations may include any combination of the three. Regardless of the dimensions and control capabilities, the proposed framework emphasises adherence to a structured analysis process. This allows for the consideration of all possible security dimensions, objectives, and control capabilities to influence the correct identification and appropriate generation of security metric quantities that suit specific environments and situations. The key end goal is to ensure that suitable security metric quantities that suite every case scenario and(or) objectives be achieved using the prescribed framework in its totality or in parts. This also portrays the flexibility and adaptability properties earlier emphasised.

5.3.1 Validation of the OSMG Framework

A two-level validation approach was adopted for evaluating the proposed OSMG framework. The first level validation adopted a theoretical case study that explored the practical application of the proposed framework for selective security metrics aggregation. A scenario-based simulation and application of the processes is developed to show how the framework can be used, and to assess its effectiveness for guiding a cyber security metrics generation process. The second level validation involved the use of expert intuitions/opinions undertaken using an online questionnaire tool which was targeted at experts and researchers in ICS security.

5.3.1.1 Scenario-based Validation

The case study is conducted to particularly target the workforce end-users (human constituents) of the system. The employees within industrial environments are viewed to be the weakest links in both the operations and supply chain (Kaspersky-Labs, 2015), and potentially the most vulnerable vectors of industry-targeted cyber-attacks.

i. Scenario 1 Description

An industrial organisation has been a victim of several cyber compromises of systems in the industrial network segment. Initial investigation shows that most of the attacks targeted and exploited human elements in the system. The organisation's attention is drawn to the vulnerabilities in its human elements, and desires to do something to improve the situation. The organisation intends to learn the security capacities of the case study environment workforce (people), and further characterise the security capability attributes of each workforce individual and use same to influence security improvement decisions. Assuming the organisation has access to a pool of security metrics quantities in Appendix A-25, and desires to identify and select the metrics quantities that are most relevant towards achieving its desired security inference and target improvements.

ii. Framework Process Application

The motivation for identifying and aggregating cyber security metrics in relation to the evaluation of human security capabilities is to learn the security levels of human weak-links by determining their security capacities. This will support engaging the necessary guided control efforts on security to enhance security assurance of enterprises. Essentially, it is a formative decomposition validation technique for the proposed framework. The succeeding sub-sections will demonstrate how the framework may be applied towards achieving the prescribe scenario goals. Note that, the collection of security metrics in Appendix A-25 are used as sample collection for demonstrating the application of the framework.

a. Phase 1: Target Definition

In line with phase 1 of the proposed framework, this section demonstrates the process of deriving outputs after feeding in the scenario description as input into the proposed framework to support generating security metrics that are appropriate for the objectives targeted:

- i. Security Dimension (L1 Scoping):* From the scenario description, desired security metrics are intended to provide understanding “security capacities”, which conforms to a ‘**capability**’ security dimension at the L1: high-level scoping process of the framework. A weakest link objective describes a limitation status that can be obtained through comparing evaluated multiple capabilities. At this point, several metric quantities in technology, process, and people-oriented scopes that have the ‘**Cap**’

attribute in their characterisation all satisfy this criterion and are considered eligible for adoption. From the metric list in Appendix A-25, 38 out of 53 technology-oriented metrics are eligible, 10 out of 15 process-oriented metrics are eligible, and 7 out of 8 people-oriented metrics are also eligible.

- ii. **Target ICS Segment:** Based on the scenario description, this points to the **Industrial Network Segment**, which defines the working domain where cyber compromises have been prevalent. At this point, the metric quantities in the L1: high-level scoping also satisfy this criterion, because they can all be applied to obtained value measurements relative to the industrial network segment.
- iii. **Target ICS Constituent:** From the scenario description, not all the elements of the industrial network segment are the focus of attention. The focus of evaluation is on the **‘people’ (human elements)**, noted to be chiefly being exploited by attacks. At this point, the narrowed focus on people or human-elements allows for the elimination of other adopted metrics within the technology and people scopes. This leaves an output of only 7 eligible security metrics focused on the human capability of the industrial network segment. These include: *Number of Personnel Needing Security Training, Number of successful human-facilitated attacks, Number of thwarted human-facilitated attacks, Number of incidents caused by terminated personnel, Number of Technology Abuse Incidents, Personnel Security Knowledge Rating, Personnel Security Skill Rating, and Harmonised Personnel Security Rating.*

b. **Phase 2: Objective Definition**

Safety is not the focus of this study. In terms of security, the organisation desire to learn workforce capabilities in relations to the primary and secondary security objectives; availability, integrity, and confidentiality. The secondary requirement associated to these objectives are automatically adopted. Furthermore, the contextual identification and description of metric objectives in line with phase 2 of the framework, can be represented as thus:

‘Understand industrial segment corporate cyber security state through from the evaluation of individual workforce’s ability to pre-empt and respond appropriately to certain cyber-

attack patterns, and determine the weakest-link amongst the workforce needing capability security improvement'

c. **Phase 3: Metrics Synthesis**

From the contextual description derived from the scenario's objective definition, the grouped control capabilities of the desired metrics can be used for further decomposition or selective adoption of appropriate security metrics. As shown in Figure 5-1, grouped classification can include measures tailored towards proactive or reactive controls. The ability to both **"pre-empt and respond"** to cyber-attack events reflect both proactive and reactive control requirements, thus, security metrics within the selected 7 that do not satisfy both criteria are eliminated, leaving resulting metrics as eligible for adoption. Accordingly, 6 metric quantities are selected.

Again, the scenario descriptions assert a need to *"characterise the security capability attributes of each workforce individual"*. It is noted that all 6 metrics selected do not characterise individual workforce capabilities, hence the need to further refine the set by eliminating the metrics that do not satisfy the 'individuality ability' criteria. For example, the security metric: **Number of Personnel Needing Security Training** does not reflect an individualised measure, rather it reflects a corporate or generalised measure, likewise: **Number of thwarted human-facilitated attacks**. It is believed that those that satisfy the 'individuality ability' such as; **Personnel Security Skill Rating**, are more appropriate for the scenario description and evaluation objectives.

Accordingly, 3 metric quantities emerge as the final outputs of the selective generation process that reasonably satisfy the scenario description. These include: (i) *Personnel Security Knowledge Rating (K_c)*, (ii) *Personnel Security Skill Rating (S_c)*, and (iii) *Harmonised Personnel Security Rating (CR_p)*. The profile specification for these metrics can be drawn from the literature (Ani, H. M. He and Tiwari, 2016) where the metrics were presented. *Personnel Security Knowledge Rating* metric is used to evaluate the measure of awareness and theoretical understanding about recurrent cyber threats, vulnerabilities, attack patterns and impacts to the target system that a user, employee or operator has while working in an ICSE. *Personnel Security Skill Rating* metric is used to evaluate the measure of practical ability to use accrued knowledge either from experience or training to spot cyber-attack attempts, patterns and techniques, and the degree to which the user can

respond, prevent or recover timely with appropriate countermeasures. The Harmonised Personnel Security Rating metric is used to represent a balanced security capability potential for each individual workforce, obtained from the harmonisation of K_c and S_c metrics for respective workforce members into a set $W = \{CR_1, \dots, CR_n\}$, and the identification of the least value in W , which is the *weakest-link* CR_p . Therefore, $CR_p = \min(W) = \min(CR_1, \dots, CR_n)$, $CR_p \in W$, n = number of workforce members under evaluation (Ani, H. M. He and Tiwari, 2016).

K_c and S_c are **computable** as **count-based** quantities that are dependent on the specific evaluation techniques, i.e., their measures are discrete values derived based on the nature and type of evaluation (questionnaire, survey, gamification, etc) approach adopted. Their respective maximum values represent their ideal states. CR_p is thus a **composite metric** since it requires the combination of two metric quantities. The metrics specification profiles of the three-metrics taxonomy for workforce cyber security capability are presented in Table 5-1 in line with the symbolic representation structure described in 5.2.3.3. The *ideal situation* is the desirable state of every workforce member, while the *current state* would indicate the *actual state* of each workforce member after the questionnaire application, statistical analysis, and weakest-link analysis evaluation steps have been employed. These, aid the accomplishment of the initial security objectives, and towards attaining the pre-defined security aim of obtaining the metrics measures.

Table 5-1: Metrics Profile Description for Human Capability Evaluation

Metric No.	Name	Symbol	Metric Specification $f(I_d, C_d, E_d)$
Ppl6	Personnel Security Knowledge Rating	(K_c)	$SP(K_c) = f(KC_{max}, KC_p, QA)$
Ppl7	Personnel Security Skill Rating	(S_c)	$SP(S_c) = f(SC_{max}, SC_p, QA)$
Ppl8	Harmonised Personnel Security Rating	(CR_p)	$SP(CR) = f(CR_{max}, \min(W), WLA)$
I = Ideal State, C = Current State, E = Evaluation Approach, QA = Questionnaire Analysis, WLA = Weakest Link Analysis			

d. Application and Result Analysis

The generated workforce (people-oriented) security metrics outlined in Table 5-1 were further applied to a six-member team of postgraduate students undertaking a research project for the development of a similar physical demonstrator of cyber security in manufacturing. The team's objective was to develop and keep operational a physical

prototype manufacturing SCADA infrastructure and explore the potentials for executing cyber-attacks on the prototyped systems with impact observations and recommendations for enhancing cyber security.

In this scenario, it is assumed that the goal of '*keeping operational*', '*executing cyber-attack*', and making '*impact observations and recommendations*' all depend on the security knowledge and skills capabilities of the team members. This in turn describes the team members' knowledge and skills in actualising the primary and secondary security objectives. Hence, prior to the team's evaluation, the following extended assumptions were made; (i) the team represents a small-scale industrial (manufacturing) workforce, (ii) all the members of the team had equal action potentials to ensure the attainment of prescribed objectives of the project. For this metrication scenario, an online (web-based) evaluation tool (questionnaire) was developed guided by the UK's '*10 steps to cyber security*' guidelines (UK-Cabinet-Office, 2012). The questionnaire comprised of 40 security capability test questions (20 for knowledge, and 20 for skills). Appropriate research ethics approval was obtained prior to administering the workforce evaluation. This is shown in Appendix C-3. The evaluation tool was administered to each team member and responses analysed using the workforce capability evaluation approach. The corresponding knowledge and skills capability ratings were derived using the appropriate evaluation functions (Ani, H. M. He and Tiwari, 2016). Accordingly, the capability priority rankings include: $20.00 \leq h \leq 33.33$ for *high*, $33.33 < m \leq 66.67$ for *moderate*, and $66.67 < l \leq 100.00$ for *low*. The *low* priority range of scores represented the '*Ideal state*' *I* of the metric quantities. The result of the evaluation of capabilities is presented in Table 5-2. The questionnaire evaluation tool is presented in Appendix C-4.

The evaluation yielded different levels of capabilities for knowledge, skills, and normalised capability ratings for the team members. The evaluation provided quantitative value reflections of the team members security capabilities, from which the weakest link can be identified (indicated in Table 5-2 and Figure 5-2). No other work has been found to provide this type of quantitative, human-level tailored security evaluation and characterisation. Identifying the human weak links reveal to organisations their most vulnerable human elements in the face of human targeted attacks, since attacks typically target such most vulnerable points of an organisation or enterprise. This requires organisations to improve their security from these points. Otherwise, if a malicious person identifies such weakest

links, then it potentially provides the easiest means for compromising the organisation. In this scenario, the weakest link capability is attributed to the team member ID *WF03* ($K_c = 23$, and $S_c = 48$) with a normalised capability rating $CR = 33.23$. Therefore, organisations or enterprises need to ensure that the weakest link will be as strong as possible against cyber-attacks.

Table 5-2: Capability Evaluation Results

Member ID	K_c	S_c	CR	Priority
WF01	42	39	40.47	Moderate
WF02	38	32	34.87	Moderate
WF03	23	48	33.23	Moderate
WF04	70	72	70.99	Low
WF05	53	73	62.20	Low
WF06	56	49	52.38	Low

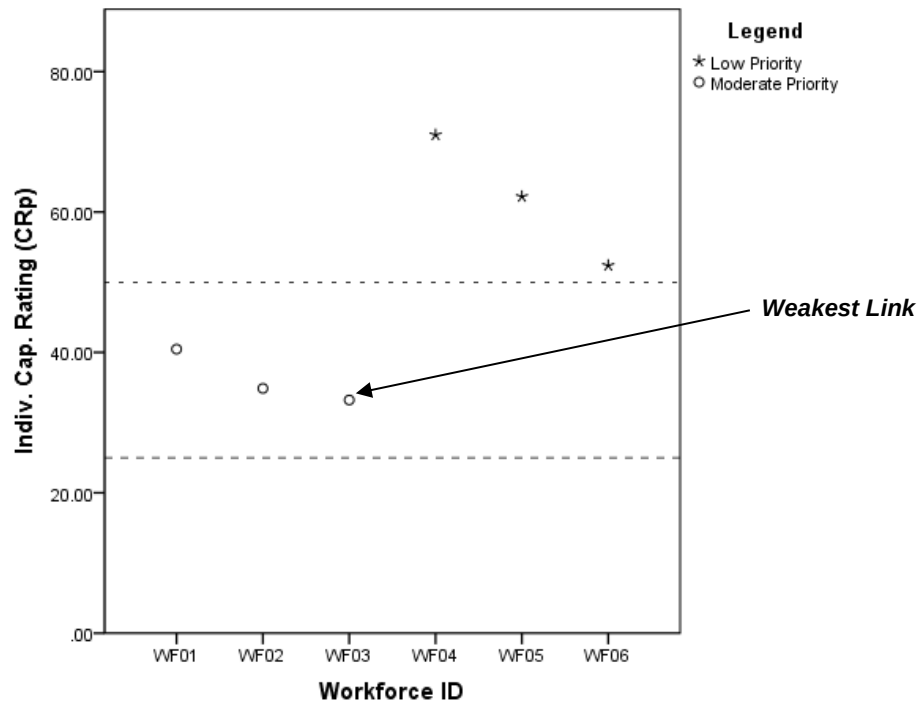


Figure 5-2: Workforce Capability Visualisation Chart

5.3.1.2 Expert-based Validation

The second level validation adopted an approach for validating improvement structures, frameworks, and measurement mechanisms by eliciting a group of experts to complete a detailed questionnaire or respond to oral structured interviews. The online questionnaire approach offers ample time and opportunity for completion to the experts, while allowing for flexibility of preferred times and places. Experts could also pause and return to the

questionnaire at their convenience. This method enables experts to view the model framework and consider the validity of its output based on practical implementations in their localised environment or theoretic analysis of feasible from inherent experiences in security metrication.

i. Validation Questionnaire Design

The questionnaire tool was designed with the evaluation characteristics in mind. Evaluations were undertaken to determine the relevance of the suggested good metrics framework characteristics (i.e., scope-definitive, objective-definitive, reliable, simple, adaptable, and repeatable - SORSAR), and against six other recommended framework validation criteria which include: scope-delineation, consistency, understandability, ease of use, tailorability, and verifiability (Beecham *et al.*, 2005).

Scope-delineation advocates the importance to know the scope of the framework. *Consistency* emphasised the need for a common language, and the description of processes at similar granular levels at each stage of the framework. *Understandability* emphasised the importance to ensure clear definitions that allow all users of the framework to have a shared understanding of the process, especially when needing improvements. *Ease of Use* property advocates that frameworks and models should be decomposed to a level that is simple to grasp and follow. *Tailorability* advocates that a framework should be responsive to the need for changes, it should be structured such that can be extended and tailored to specific development environments. *Verifiability* emphasises the need for a framework to provide for re-tests and re-measurements on how well the framework satisfies its objectives, and what quality magnitudes are achieved.

This is to help affirm confidence and usefulness in the design and(or) implementation structure of the model (Kitchenham *et al.*, 2005). Other characteristics evaluated included: *industrial and academic usefulness*, and *applicability of the framework for yielding desirable security metrics* relative to industrial operations scenarios. The layout and sequence of the questions was such that a first array of questions linked a one-to-one relationship with the characteristics, and then a similar approach was used to present the second round of questions. This was to ensure that no characteristic had two related questions in succession to control the potentials for cheap response consistencies due to question proximities. Closed-ended questions were used, and the questionnaire

(presented in Appendix C-1) was contextually structured in three sections (A, B, and C) to capture all aspects of the study work.

Section A (consisting of 3 questions) covers the demographic details of experts. This was aimed at determining how long and level of experience in cyber security capabilities of the experts, and their scope engagements. This information is necessary to support and justify eventual views asserted by each expert, and to lend credence to the validation process and result. Section B (consisting of 1 question with 6 attribute queries) gains expert views concerning the proposed characteristics of good metrics development framework. This was aimed at gauging professional views about how relevant or unrelated the prescribed good metric framework characteristics are to contemporary security metrics development needs. This way, any characteristic widely viewed to be irrelevant or redundant in the group could be removed or discarded, to allow for the identification of relevant foundational requirements for developing and(or) adopting effective security metrics development frameworks and models. Section C (consisting of 14 questions) also obtains expert views of how and if proposed framework satisfies the initial criteria for its development in relations to the needs of different users and environments. Thus, the framework is validated in this context as recommended in Sargent (2010), to demonstrate that its constituents and attributes possess an acceptable range of correctness consistent with the proposed application of the framework. The overall purpose was to investigate whether the essentially generic framework meets the initial criteria for its development in the first place, with reasonable emphasis on satisfying the need of individual users.

Appropriate Ethics Approval was obtained before the validation tool was released and shared for access by respondents (See Appendix C-2 for Ethics Approval).

ii. Response and Feedback Mapping

Eleven (11) cyber security experts from both industry and academic environment took part in the survey. For the characteristics of good metrics framework (*scope-definitive, objective-definitive, reliable, simple, adaptable, and repeatable*), each attempted mapping to a criterion was characterised as either a 'Strong Relevance', 'Average Relevance', or 'Weak Relevance'. A 'Strong Relevance' included the combination of clearly affirmative responses (high and very high) and indicated that such attribute characteristic should be

considered as reasonably required and be an incorporated feature in any ICSE security metrics framework. An 'Average Relevance' encompassed only the 'moderate' responses which indicated a fair significance for a characteristic as requirement feature in ICSE security metrics frameworks. Hence, could be considered. A 'Weak Relevance' included the cumulative of less affirmative expert responses (low and very low), indicative of the attribute characteristic being barely important for consideration and representation in an ICSE security metrics framework, thus, should be negligible. The mappings are clearly outlined in Table 5-3.

Table 5-3: Context - Response Mapping Groups

Contexts	Response Map	Cumulative Mapping Group Selections
Characteristics Relevance	Strong Relevance	<i>High + Very High</i>
	Average Relevance	<i>Moderate</i>
	Weak Relevance	<i>Low + Very Low</i>
Framework Validity	Strongly Represented	<i>Consistent + Strongly Consistent</i>
		<i>Little + Very Little</i>
		<i>Appropriate + Strongly Appropriate</i>
		<i>Agree + Strongly Agree</i>
		<i>Realistic + Strongly Realistic</i>
		<i>Easy + Strongly Easy</i>
		<i>Useful + Strongly Useful</i>
		<i>Applicable + Strongly Applicable</i>
	Weakly Represented	<i>Inconsistent + Strongly Inconsistent</i>
		<i>Much + Very Much</i>
		<i>Inappropriate + Strongly Inappropriate</i>
		<i>Disagree + Strongly Disagree</i>
		<i>Unrealistic + Strongly Unrealistic</i>
		<i>Uneasy + Strongly Uneasy</i>
		<i>Not Useful + Strongly Not Useful</i>
		<i>Not Applicable + Strongly Not Applicable</i>
	Not Represented	<i>No Opinion/Don't Know</i>

Similarly, a second mapping of expert responses was performed for the validity of the framework against earlier outlined criteria (*scope-delineation, consistency, understandability, ease of use, tailorability, verifiability*). Each attempted mapping was characterised as 'Strongly Represented', 'Weakly Represented' or 'Not Represented'. A

‘Strongly Represented’ map encompassed the cumulative of the two most affirmative experts’ responses and indicated a higher representation or expression of the criteria in the proposed framework (see Table 5-3). A ‘Weakly Represented’ map encompassed the cumulative of the two least affirmative experts’ responses and indicated a feeble and faint representation or expression of the criterion in the proposed framework. Possible sets of cumulative responses and their context groupings are shown in Table 5-3.

iii. Results and Analysis of Response Mappings

Prior to the analysis of the contexts and response mappings as enumerated in Table 5-3, the work and capability demographics of 9 experts (that responded to the question) in this evaluation indicated a mean work experience of 4 years in operational security aspect of the industry environments. It is observed that 2 experts did not indicate their years of work experience, however, these 2 rated themselves ‘*very high*’ in knowledge, skill, experience, and expertise in cyber/information security, metrics development and assessment. More than half (54.54%) of the experts indicated to have worked for at least 2 years in the industrial/operational security. It is notable that 90.91% (10) of the experts accented to ‘*both security knowledge and skill capability*’ classification, which suggests that most of the experts were reasonably equipped with adequate information (knowledge) and technical know-how in ICSE cyber security enough to enable them lend judgements as professionals in the validation process. This is supported further by the security capability rating mean value of 3.36, with 81.81% (9) of the sample indicating at least ‘*moderate*’ security capability. Most of the experts admit to having a relatively good knowledge, skills, experience, and(or) expertise in industrial cyber security and metrication.

a. Good Security Metrics Framework Characteristics Results

After mapping expert responses to corresponding cumulative mapping groups to evaluate their views on the degree of relevance of each of the good security metric framework characteristics proposed, analysis showed that for all the characteristics, considerably large fractions (70.00%) of the relevance attribute mapped to ‘*Strong Relevance*’. It is particularly noteworthy that there was a general unanimity amongst all the experts with 100.00% ‘*Strong Relevance*’ of the ‘*scope-definitive*’ characteristic. This was followed by a 90.90% ‘*Strong Relevance*’ on the ‘*Reliable*’ characteristic. ‘*Simple*’ and ‘*Repeatable*’ characteristics had the least valuations (72.70% each), although both reflected a ‘*Strong*

Relevance’ mapping as well. The responses of experts did not indicate any ‘*Weak Relevance*’ fractional map on any of the characteristics but had minimal fraction values on ‘*Average Relevance*’ as shown in Table 5-4. The Chart representation of the three classes of ‘relevance’ maps is presented in Figure 5-3.

Table 5-4: Good Metrics Characteristics Evaluation Results

Characteristics	Strong Relevance	Average Relevance	Weak Relevance	Total
<i>Scope-definitive</i>	100.00%	0.00%	0.00%	100.00%
<i>Reliable</i>	90.90%	9.10%	0.00%	100.00%
<i>Objective-definitive</i>	81.80%	18.20%	0.00%	100.00%
<i>Adaptable</i>	81.80%	18.20%	0.00%	100.00%
<i>Simple</i>	72.70%	27.30%	0.00%	100.00%
<i>Repeatable</i>	72.70%	27.30%	0.00%	100.00%

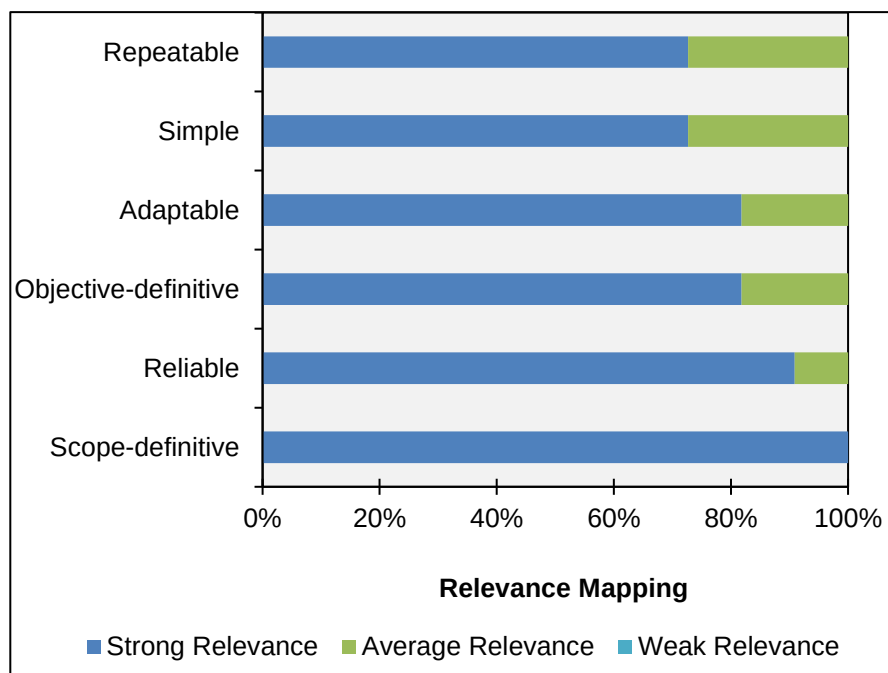


Figure 5-3: Relevance Mappings of Framework Characteristics

b. Analysis of Framework Validity Characteristic Mappings

To assess the validity of the proposed security metrics development framework, the questions covering validity contexts were further mapped to corresponding validation criteria, according to earlier mapped and grouped/cumulative response selections as represented in Table 5-5. This was done to relate expert responses to corresponding evaluation criteria, and to help simplify the process of evaluation through taking the

statistical mean (average) of multiple mapping results that are related or attributed to a single criterion. In this section, some of the questions were unanswered by some experts in the group, which resulted that some questions had a total count response record of 11, while some had lower total count of 9. These were aptly considered in the analysis of overall mapping results for each criterion and used to evaluate the cumulative records as presented in Table 5-5.

Table 5-5: Framework Validation Mapping Results

Questions Nos	Criteria Mapping	Evaluations Recorded		Weakly Represented Map		Strongly Represented Map		Average
		TC	%	TC	%	TC	%	Percent
C.Q1	Scope-Delineation	11	100.00%	1	9.10%	10	90.90%	95.45%
C.Q7		9	100.00%	-	-	9	100.00%	
C.Q2	Consistency	11	100.00%	-	-	11	100.00%	100.00%
C.Q8		9	100.00%	-	-	9	100.00%	
C.Q3	Understandability	11	100.00%	1	9.10%	10	90.90%	95.45%
C.Q9		9	100.00%	-	-	9	100.00%	
C.Q4	Ease of Use	11	100.00%	6	54.50%	5	45.45%	72.73%
C.Q10		9	100.00%	-	-	9	100.00%	
C.Q5	Tailorability	11	100.00%	2	18.20%	9	81.80%	90.91%
C.Q11		9	100.00%	-	-	9	100.00%	
C.Q6	Verifiability	11	100.00%	1	9.10%	10	90.90%	90.90%
C.Q12	Usefulness to Industry	9	100.00%	-	-	9	100.00%	100.00%
C.Q13	Usefulness to Academy	9	100.00%	-	-	9	100.00%	100.00%
C.Q14	Applicability	9	100.00%	-	-	9	100.00%	100.00%
TC = Total Count, % = Percentage equivalence								

The results of individual questions and related average mapping values for multiple questions were used to evaluate the degree of representation or expression of the corresponding criteria in the proposed security metrics development framework. This helped to determine whether, and to what opinionated extent the criteria outlined were reasonably captured or satisfied in the proposed framework. For example, two questions (C.Q1 and C.Q7) mapped to ‘*scope-delineation*’, and while C.Q1 had a total count of 11, C.Q7 had a total count of 9. It implied that two experts did not respond to C.Q7. As shown in Table 5-5, all the other criteria followed a similar pattern in outcomes for number of questions mapping, and the total count values. However, only one question mapped to ‘*verifiability*’ property of the validation criteria. This had a total count of 11. Each of the total counts was aggregated to a 100.00%.

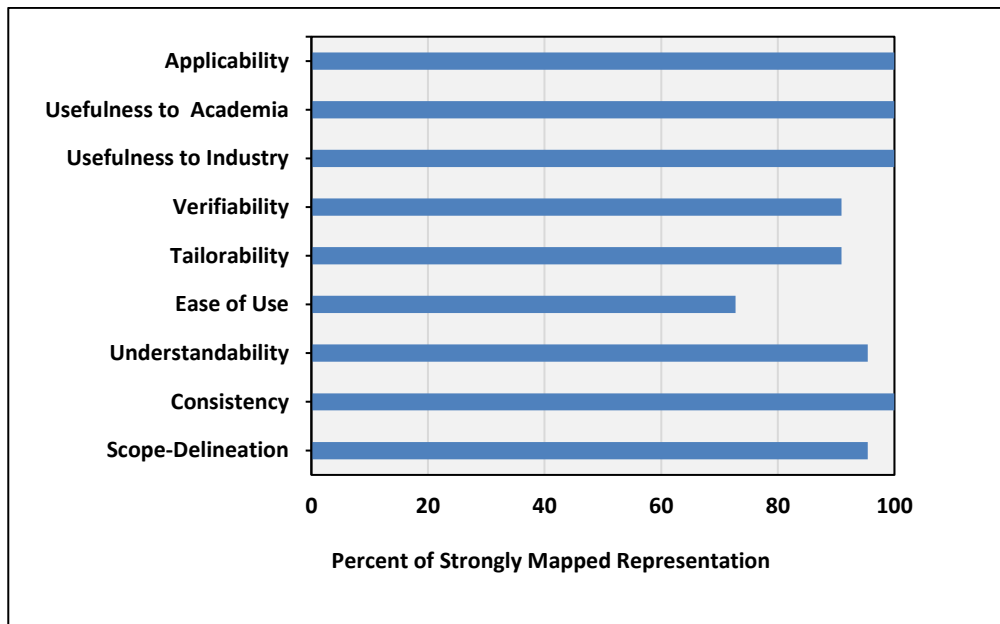


Figure 5-4: Criteria Representation Maps

Results also show that both 90.90% (10) for C.Q1 and 100.00% (9) for C.Q7 all mapped to ‘*scope-delineation*’ were in the ‘*Strongly Represented*’ map. These had a mean percent count of 95.45%. A result in like manner was replicated in the ‘*understandability*’ criteria as presented in Table 5-5. In a similar but slightly diminished pattern, the ‘*tailorability*’ property had an 18.18% (2) ‘*Weakly Represented*’ fractional response for one of its questions (C.Q5) but had an overall mean of 90.91%. The ‘*verifiability*’ property had a single question mapped to it with 90.90% ‘*Strongly Represented*’ and 9.10% ‘*Weakly Represented*’ response maps. The questions C.Q2 and C.Q8 that mapped to ‘*consistency*’ criterion each yielded a 100.00% map in ‘*Strongly Represented*’ mapping response. However, a slight variation from others is observed with the ‘*ease of use*’ validation criteria. The question (C.Q4) that had a total response count of 11 showed a 45.45% (5) ‘*Strongly Represented*’ fractional map response, and a 54.54 (6) ‘*Weakly Represented*’ fractional map response. The second question (C.Q10) that mapped to ‘*ease of use*’ yielded a 100.00% ‘*Strongly Represented*’ map, which introduced some inconsistency in the behaviours or patterns of the results. This required further analysis towards uncovering possible influences on the variations observed. The supplementary validation criteria: *usefulness to industry*, *usefulness to academic R&D*, and *applicability* evaluated, each yielded a 100% ‘*Strongly Represented*’ mapping as shown in Table 5-5. Figure 5-4 shows the ‘average representation’ values accordingly.

From the case study verification (level 1), it is observed that the outcome of a security metric development can be dependent on the clear and concise articulation of system scope, and target security objectives. Primary security attributes (e.g. availability) might vary in meaning. Supplementary secondary objectives can depend on the constituent of the target systems and environments, and the context of security definition. Adopting the proposed OSMG-developed security metrics together with the evaluation model to the test scenario helped the identification and understanding of the capability of each workforce member with respect to cyber security knowledge and skills. It also aided the identification of the security weakest-link amongst the workforce. Derived metric quantities can also be reviewed as deemed necessary, especially when in response to changes, which weaken or nullify the reliability of the outcomes expected. The nature of the development model also allows for the development of security metrics that focus on other ICSEs, segments, and constituents of control processes, which are expected to yield varied lists of security metrics quantities depending on the security objectives.

From the expert validation (level 2), results from the framework characteristics evaluation suggest a wide affirmation and acknowledgement of relevance of the prescribed '*characteristics of good security metrics framework*'. Based on the '*Strong Relevance*' mapping cumulative values obtained, '*scope-definitive*' criteria topped the list of affirmations by the experts. This was followed by '*reliable*', '*objective-definitive*', and '*adaptable*' criteria. The last two in the order included; '*simple*' and '*repeatable*' criteria. Accordingly, this suggests that for an effective security metrics development framework, being *definitive in scope, objectives, reliable, and adaptable*, were viewed as considerably more prioritised characteristics than being *simple* and *repeatable* in situations where preferences became necessary during process or methodology design and developments.

The framework validation result also shows that five (5) of the framework validation criteria (*scope-delineation, consistency, understandability, tailorability and verifiability*) showed a consistently '*Strong Representation*' in the proposed OSMG framework. It implied that that these criteria were considerably characterised and expressible in the proposed framework. However, for the criteria (*ease of use*) that showed a slight variance with others, the question labelled C.Q4 sought expert feedbacks on the perceived scale of previous knowledge of security metrication required to interpret the proposed framework. A further analysis of the results revealed that 3 out of the 6 experts whose responses resulted to the

'Weakly Represented' (Much + Very Much) response had at least four years work experience in industrial/operational security; with good security knowledge and skills. Their probable elongated and diverse experience might influence and justify a supposed more profound insight they presumed to have about understanding the *'ease of use'* shortcomings. This limitation might not have been noticed by the less experienced experts. 2 other experts did not indicate their number of years of experience in the cyber security field. However, the nearly half (45.45%) *'Strongly Represented'* responses suggests that the framework had some significant degree of *'ease of use'*. Clearly grasping this seem to depend on the measure and diversity of security metrication experience and knowledge at the disposal of a user or developer. This view is backed by the 100% count for *'Strongly Represented'* map of the matching part question (C.Q10), which does suggest that very significant *'ease of use'* property in the proposed framework, indicating that the framework was considerably realistic for industrial organisations to use to guide the security metrics selection and aggregation processes.

5.4 Chapter Summary

In this chapter, a new framework for Operational Security Metrics Generation (OSMG) with focus on industrial environment application is presented. The framework offers new insights to security metrics adopter experts on how to resolve the issue of choosing and using appropriate security metrics with added process capability improvements in the aspects of adaptability and repeatability. The framework supports industrial organisations that desire to develop security metrics for measuring certain security contexts within their environment, by providing a structure approach for considering the necessary processes, attributes, and dimensions required. It will support efficient security monitoring, prediction, and decision-support for risk managers and top management executives as they work to improve security in their ICSEs. Through formative decomposition and expert-based validation approaches, the framework demonstrates capability and usability for security metrics generation in the ICSE. In addition, an outline of good characteristic of metrics generation methodologies is presented. These include: scope-definitive, objective-definitive, reliable, simple, adaptable, and repeatable.

6 MODEL-BASED TECHNOLOGY VULNERABILITY IMPACT ANALYSIS

6.1 Introduction

A system or network is often as strong as its weakest link (PWC, 2013). The weakest link refers to the frailest attack point on a system or component. From a security perspective, vulnerability impact analysis offers a way of identifying and resolving the security weak links in technology components. However, system-level evaluation of vulnerabilities is often less informative despite assuming that all vulnerabilities do not have equal exploit and impact likelihoods, thus, do not affect the system in the same way when exploited. Thus, it is crucial to assess the exploit and impact likelihoods of each vulnerability separately, and then determine the vulnerability that potentially amasses the greatest impact criticality.

The Common Vulnerability Scoring Scheme (CVSS) (Franklin, Wergin and Booth, 2014) is more commonly used to achieve analysis of technical vulnerabilities and their severities. The CVSS Base Score metric is more commonly used to support response prioritisation in cases where similar vulnerabilities do not occur with a system under study (Allodi, Woohyun Shim and Massacci, 2013). However, this is hardly feasible since similar technologies and development approaches often characterise the components of digital computing systems. Repeated design flaws often bring about reoccurring vulnerabilities in different components. This of course unveils a security control problem that needs to be resolved to achieve improved security. Besides, vulnerability states have been shown to be quite dynamic, and often change over a life cycle period (Frei, 2009), it is important for analysis approaches to consider the subsequent state transformations of security vulnerabilities. *How can one select and prioritise technical vulnerabilities resolution, such that optimised outcome is achieved?*

6.2 Theoretical Concept for Technical Vulnerability Impact Analysis

This study explores an attempt to answer the above questions by providing an improved methodology for evaluating the functional consequences and cascading impacts of exploiting vulnerabilities in ICSE technology components. It also provides a priority-based approach to implementing strategic and efficient vulnerability controls. Considering and

integrating system components dependency attributes with component vulnerability analysis can help achieve a more precise quantification of security criticalities that is closer to the actual. Understanding and utilising the dynamic state attributes of a vulnerability can provide a more realistic estimation of impact criticalities than using the typical non-dynamic vulnerability attributes. It is believed that a more precise criticality and cascading impact valuation can support speedy and productive engagement of proactive and reactive responses to cyber incidences in the ICSE.

Therefore, a probabilistic Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model for estimating the dynamic severity and impact states of vulnerabilities within ICSE networks is proposed. The purpose of the model is to provide a means of resolving vulnerability management uncertainties with considering the potential to achieve the highest possible impact control per response time. The MAVCA model can also support prioritising vulnerability controls and resolutions based on quantitative attributions of impacts. The MAVCA model will come useful to security analysts, administrator and auditors during security and vulnerability analysis of industrial system and networks. Industrial organisations can use the model for understanding, estimating, and managing security vulnerabilities and potential impacts in their operational networks.

The MAVCA approach contributes knowledge and novelty by leveraging on three key attributes to quantify potential impacts of exploiting security vulnerabilities in ICSE networks. These include: (i) vulnerability severities influenced by environmental factors, (ii) attack probabilities relative to the vulnerabilities, and (iii) vulnerability host's functional dependencies. These factors have been shown (in chapter 3) to support security vulnerability, criticality and impact analysis (Abraham and Nair, 2015a; Wang *et al.*, 2016; Yang *et al.*, 2016). Here, criticality refers to the magnitude of negative consequences resulting from a successful exploitation of a vulnerability. The three factors are modelled into two main network vulnerability metric dimensions: *Vulnerability Exploit Potential (VEP)*, and *Vulnerability Impact Potential (VIP)*. An overall *Criticality Index* probability score value in the range [0,1] is proposed as a function of the two metric dimensions. Priority for the response and resolution of security vulnerabilities is performed by ordering the criticalities indices in descending order. Priority is given to the vulnerability with the highest criticality index probability values in the ordered arrangement. Given that it is hardly feasible to accurately determine the impact of any exploitable vulnerability on a network without full

details about both attacker and defender (or user), a probabilistic approach offers a viable solution path. Also, it is more reasonable to consider security analysis from perspectives that are known (e.g., the user and network characteristics and capabilities), rather than the unknown (defender's side).

6.3 Multi-Attribute Vulnerability Criticality Analysis (MAVCA) Model Development Analysis and Presentation

In this work, it is proposed that a reasonable understanding of cyber-attack impacts is a function of the vulnerabilities in the ICSE technology infrastructure, the likelihood of exploiting the vulnerabilities, and the functional dependency relationship amongst technology components that make up the ICSE infrastructure. These are integrated into a Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model for ICSE technical security impact estimation presented in Figure 6-1. The arrows show the process and output transitions from one evaluation stage to a succeeding stage.

Since an impact is only feasible if an attempted attack successfully exploits a vulnerability in the network, then an impact scale or '*criticality index*' (m) of the vulnerability is also practicable. This can be determined if the characteristics of any such vulnerability is known in a way that reflects its severity, its probability of attracting interests by malicious persons, and the functional dependency relationship and interaction with other components that enable a cascading function or impact flow and transfer.

The Criticality Index (m) is conceived as a probabilistic security metric defined to capture several factors which influence the security of a network. This is proposed to be a function of security scores from two broad security metric dimensions: vulnerability exploit potential (VEP), and vulnerability impact potential (VIP). For simplicity, the VEP and VIP scores will be represented in equations as β and γ respectively. Each of the two-dimension scores yields a numeric value in the range [0,1]. The m probabilistic metric uses data from 3 sources: scores assigned from standard CVSS, functional dependency modelling structure, and probabilistic frequency of vulnerabilities evaluations. Typically, this m metric would yield an array of index values associated to vulnerabilities from which a weakest link can be determined. The weakest link identifies the host that bears the vulnerability with the highest m value in each array. Since a network is potentially as strong as its weakest link

technology component, the two key security dimensions (β and γ) proposed are defined as functions for each network vulnerability retained by a host technology component.

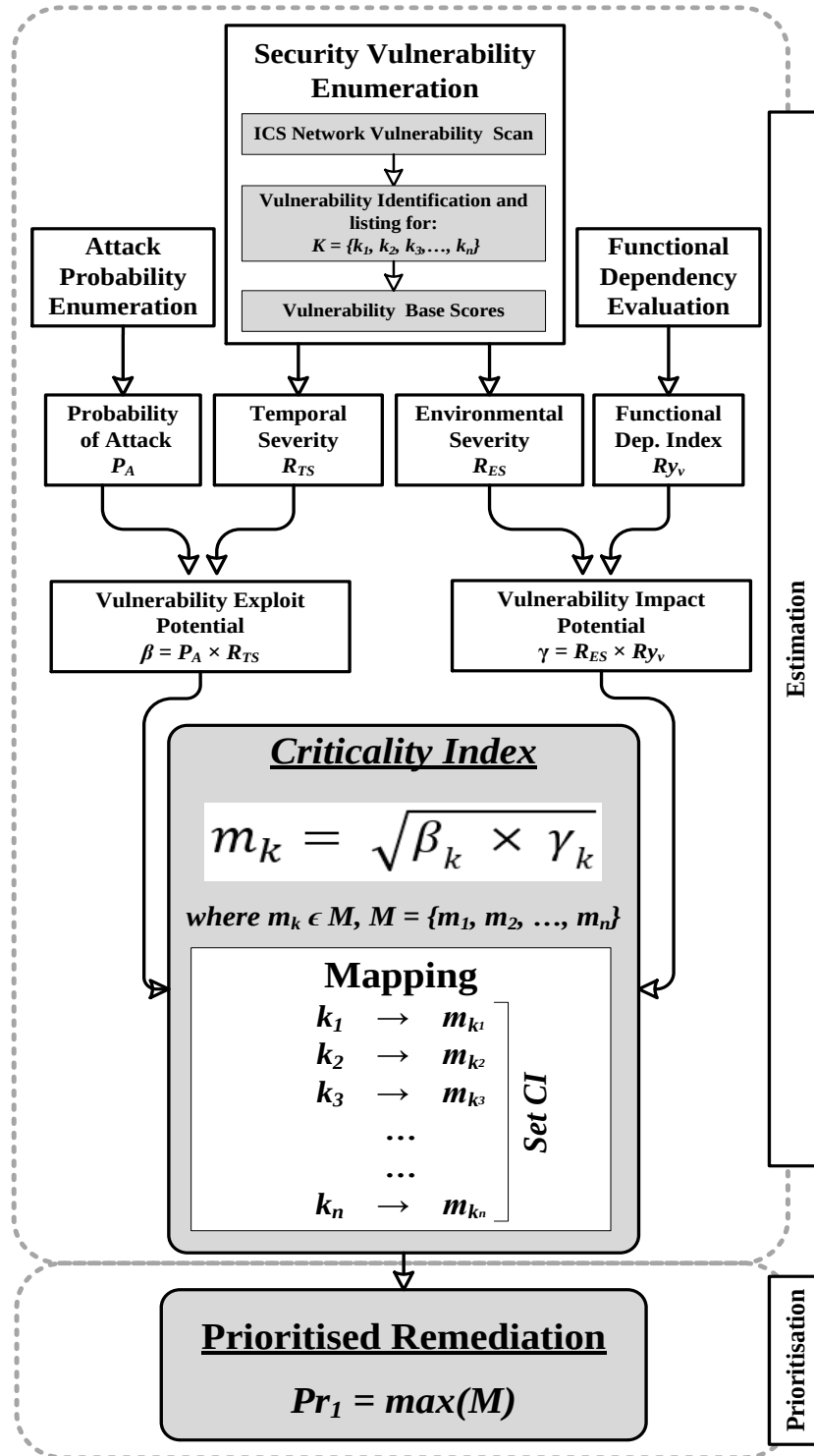


Figure 6-1: Multi-Attribute Vulnerability Criticality Analysis (MAVCA) Process flow

6.3.1 Criticality Index Estimation

It is important to understand the extent to which a potential impact can ripple down a network topology when a certain vulnerability is exploited. Such episteme can offer insight into the scale of probable damage that can be incurred if a specific attack on a specific node is successful. Evaluating the criticality level of cascading impacts is crucial as it can support the identification of the key infrastructure resources that need to be protected, based on a cost–benefit process (Stewart, 2010). Such information will further guide easy and speedy placement and engagement of mitigation controls, and the prioritisation of measures in the face of multiple exploitable nodes. It is believed that more profound measure for the prioritisation of vulnerabilities can be easily derived based on the impact and attack potentials to yield a *criticality Index* (m) that outlines the potential magnitude of effects (consequences) amassable from the successful exploitation of a vulnerability within a system/network. Thus, the criticality index (m) of a vulnerability (k) can be represented as a function of the vulnerability's exploit potential (β) and vulnerability impact potential (γ), and derived by determining the absolute or positive square root of the product of the two variables as Equation (6-1). The exploit potential of a vulnerability (β) can be determined with respect to the *Vulnerability's Probability of Attack*; P_A , and its *Temporal Severity Ratio* (R_{TS}), while the impact potential of a vulnerability (γ) can be determined with respect to the vulnerability host's *Functional Dependency Ratio*; (γ_v) and its *Environmental Severity Ratio* (R_{ES}).

$$m_k = f(\beta_k, \gamma_k) = \sqrt{\beta_k \times \gamma_k} \quad (6-1)$$

In a given ICS network with multiple vulnerabilities, Equation (6-1) can be used to obtain a set of Criticality Indices $M = \{m_1, m_2, \dots, m_n\}$ for the corresponding set of discovered vulnerabilities $K = \{k_1, k_2, k_3, \dots, k_n\}$, such that every k in K has a corresponding m in M , and n imply the total number of elements in the vulnerability and criticality sets.

Thus, from Equation (6-1), and the set of estimated *criticality Indices* (M) for exploiting a set K of discovered vulnerabilities, effective security response requires that control measures be engaged that can enable the control of the vulnerability(ies) with the greatest *criticality index*. This corresponds to resolving the highest possible technical/functional impact estimation attributable to a vulnerability on the ICSE network. It then translates to

enabling a highest possible security remediation and improvement per response time. Since a decision is often required for the choice of a ‘*first priority*’ response, this study suggests that such priority be set based on the magnitude of functional effects amassable by a vulnerability if successfully exploited.

This can easily be achieved following the *criticality index* (m) probabilistic values derived. Since each discrete element in M describes a potential technical or functional impact scale for a corresponding vulnerability in K , a suiting prioritised response would involve giving priority Pr_1 position to the highest value in M per remediation time. The highest value in M , which takes on the *priority* Pr_1 position is also considered as the weakest link. This means that each time a remediation effort is required, the vulnerability with the highest m value, also considered as the weakest link, should be treated first. The cumulative of all elements in M could imply the summed scale of criticalities for all vulnerabilities in the network and remediating the highest value in the set per time is equivalent to plugging-in on the widest possible critical security impact per time. The derivation of priority Pr_1 is represented in Equation (6-2).

$$Pr_1 = \max(M) \quad (6-2)$$

This impact estimation approach can help efficient security information gathering, and the resolve of potential queries if a final attack state is reached from a cyber-attack. Some of these questions include: Which node or vulnerability if exploited can cause the widest, cascading, and devastating effects on the control system infrastructure? What is the estimated likelihood attributed to attacking each vulnerability? How far down or through the network can the effect in the final attach state be felt? It will also guide effective decisions related to the best set of actions and capabilities that can be employed to reduce (to as low as practicably possible) the impact magnitude of a specific attack.

6.3.2 Vulnerability Exploit Potential (β)

This attribute is used to indicate the measure of likelihood for exploiting a vulnerability based on its dynamic characteristics that make it an attractive attack option over other vulnerabilities. In this work, the exploit potential of a vulnerability (β) can be derived by the probability of an attack that exploits a vulnerability P_A , given its temporal severity ratio R_{TS} within a network at any given evaluation time.

This is conceived based on the phenomenon that the slightest malicious pressure, exertion, or probe on an ICSE network or any given open vulnerability is capable of greatly causing significant impact on the systems with respect to security and safety. The assumption here is that the likelihood that a vulnerability will attract interest for exploitation would depend on the ease with which the vulnerability can be exploited. Since the availability of an exploit with varied levels and requirements for modifications, availability of patches on official or third-party levels for remediation, and attack potential of the vulnerability within the system also termed its report confidence, are all viewed to contribute to a vulnerability temporal score metric (Mell, Scarfone and Romanosky, 2007). These also contribute to determining the attack severity potential β . It is viewed that a more reflective view of attack probability for any vulnerability can be derived in relations to other vulnerabilities that are both internal and external the network. This probability can be derived using Equation **Error! Reference source not found.**). The derivation of PA and (R_{TS}) are discussed in the following sub-sections.

$$\beta = P_A \times R_{TS} \quad (6-3)$$

6.3.2.1 Temporal Severity Ratio

To capture this exploitation dependency factor, the CVSS temporal score attributes: *Exploitability (Ex)*, *Remediation Level (RL)*, and *Report Confidence (RC)* are adopted as notable influencing attributes, and, because of their wide acknowledgement and adoption. Exploitability evaluates the likelihood of a vulnerability being attacked and is usually dependent on the current state of exploit techniques or exploit code availability.

From CVSS, current state options of exploit techniques include being: *Unproven*, *Proof-of-concept*, *Functional*, *High*, or *Not-defined*. Remediation level evaluates the present state of control application reflecting the urgency of remediation. Remediation levels options include having: *Official fix*, *Temporary fix*, *Workaround*, *Unavailable* or *Not-defined*. Report confidence evaluates the degree of confidence in the existence of the vulnerability and the credibility of known technical details with options of *Unknown*, *Reasonable*, *Confirmed* and *Not-defined*.

All three attributes are viewed to contribute to a resultant temporal severity of a vulnerability. For example, a vulnerability that has available and easily accessible exploit

is most likely to be targeted than that without. The availability or accessibility of an exploit implies easy handiness for the required weapon for perpetrating an attack. An attacker with this type of weapon in hand is more likely to attack a respective vulnerability, rather than seeking or developing newer exploits (weapons) to target other vulnerabilities whose exploits are not readily available or accessible publicly or privately. More so, considering the case of an advanced or intelligent adversary, it would be easier for such persons to execute attacks targeting vulnerabilities with known or available exploits.

In extended cases, intelligent adversaries are likely to desire to modify or reconfigure existing exploit to suit a certain attack target or vulnerability than initiate a fresh exploit development process. Hence, they are more likely to first attack vulnerabilities whose exploits they can easily access, or through the less stressful approach of tweaking existing exploits. It is only when these options do not apply that attackers revert to attacking vulnerabilities which require fresh exploit development. The CVSS severity rating scale [0,10] is used; 0 indicating a no/low severity and 10 indicating a critical severity to represent standard static base scores (BS) of vulnerabilities. The temporal severity ratio (R_{TS}) of a vulnerability can be evaluated using Equation (6-4). A temporal score (TS) value can be derived from the combination of Ex , RL , RC , and BS attributes using Equation (6-5). Appendix B-3 presents the standard metric values used for deriving the current CVSS version 3.0 evaluation score.

$$R_{TS} = \frac{TS}{10} \quad (6-4)$$

where;

$$TS = round(BS \times Ex \times RL \times RC \times 10)/10 \quad (6-5)$$

6.3.2.2 Probability of Attack

Furthermore, it is typical for a component or asset to have multiple vulnerabilities, each with potentially multiple attack paths. In this case, it is hardly feasible to determine which of the paths is more vulnerable using a CVSS alone, since CVSS only gives a single machine vulnerability score, and multiple occurrence of such vulnerability need to be calculated separately. CVSS temporal score alone might not sufficiently fulfil completely and appropriately the predisposition for the probability of attack. A more realistic measure

of likelihood can be obtained if multiple occurrence features of a vulnerability is factored into the evaluation of attack probability. This study suggests that multiple paths towards the exploitation of a single vulnerability widens the attack space and potentially amplifies the likelihood of attracting the interest of attackers, since attackers would typically have numerous paths to follow towards exploiting a target vulnerability. The likelihood of exploiting a vulnerability in this sense would be in relation to the cumulative number of attack paths for all discovered vulnerabilities on the system. To derive quantitative dispositions for these, a proportionality concept is adopted that involves taking the ratio of the occurrence of attack paths to individual vulnerabilities against their cumulative in the entire network. This yields the probability P_A of attacking a specific vulnerability amidst a collection of vulnerabilities inherent the analysed system. One way of deriving this probability is through path analysis using attack graphs (Chejara, Garg and Singh, 2013), and the modelling of causal relationship amongst vulnerabilities (Wang *et al.*, 2008a). The frequency of occurrence of a vulnerability directly along an attack path can be determined considering inputs (e.g. vulnerability information) from the system and its environment (Shandilya, Simmons and Shiva, 2014).

In this study we consider the *Access Vector* description of vulnerabilities from CVSS scheme, which defines how a vulnerability can be exploited using value attributes of '*local*', '*network*', or '*adjacent network*' accesses (Mell, Scarfone and Romanosky, 2007). Through these details about discovered vulnerabilities, all possible paths to the exploitation of each vulnerability is developed accordingly considering each vulnerability's host asset topological positioning on the network, and its ease of access. The path outcomes give an idea of the amount of work or effort required by an attacker to successfully exploit a vulnerability and contribute to understanding the attack impacts on the network. Several methodologies (Sheyner *et al.*, 2002; Ou, Govindavajhala and Appel, 2005; Jajodia and Noel, 2010) and tools (*MulVal*, *NetSPA*, *TVA*, *Attack Graph Toolkit*) (Yi *et al.*, 2013) can be used to generate the attack graphs, and subsequently used to derive the probability value. In this work, the advanced cyber-attack modelling and analysis approach (Jajodia and Noel, 2010) was used. This work also assumes that the knowledge and application of attack graph tools for network analysis are disposed to users. The measure of effort greatly influences an attacker's choice of attack with respect to vulnerabilities and the further paths to take, since attack efforts are reliant on capability expressed by the availability of

sufficient resources (Ingoldsby, 2013). It is suggested that understanding the various scales of efforts (expressed in probabilistic forms) towards breaching vulnerabilities can contribute to the decision on target vulnerability, and by extension; the plausible impacts of exploiting such targets. For example, if k_1 is a vulnerability in an ICS network that can be exploited, and the path to k_1 appears n number of times in the set of N cumulative attack paths for all vulnerabilities discovered in the network, then it is feasible to ascertain the probability of exploiting k_1 amidst other vulnerabilities. The probability P_{k_1} can represent P_A , *i.e. probability of attack*, as shown in Equation (6-6). This can be evaluated as the ratio of attack paths having direct link to vulnerability k_1 denoted as n_{k_1} , and the total number of attack paths in the network denoted as N_K .

$$P_A = P_{k_1} = \frac{n_{k_1}}{N_K} \quad (6-6)$$

In the case where it is impossible to attack a vulnerability directly but requires following an attack path from another vulnerability k_2 , before being able to access the target vulnerability k_1 , then a conditional probability $P_{k_1|k_2}$ of occurrence of the two vulnerabilities in succession is evaluated. A similar concept is presented in (Chejara, Garg and Singh, 2013), and is computed as the ratio of attack paths having k_2 and k_1 in succession, and the ratio of the total number of attack paths in the network. The probability of k_2 and k_1 in succession can be represented as $P_{k_1 \cap k_2}$. The conditional probability $P_{k_1|k_2}$ is represented in Equation (6-7). The extended derivatives are presented in Equations (6-8) and (6-9).

$$P_A = P_{k_1} = P_{k_1|k_2} = \frac{P_{k_1 \cap k_2}}{P_{k_2}} \quad (6-7)$$

where:

$$P_{k_1 \cap k_2} = \frac{\text{Total attack paths with } k_2 \text{ and } k_1 \text{ in succession}}{\text{Total Number of attack paths}} \quad (6-8)$$

And generally, for $k_1 \dots k_n$,

$$P_{k_1 \cap k_2 \cap \dots \cap k_{n-1} \cap k_n} = \frac{\text{Total attack paths with } k_n, k_{n-1}, \dots, k_2, k_1 \text{ in succession}}{\text{Total Number of attack paths}} \quad (6-9)$$

6.3.2.3 Vulnerability Impact Potential (γ)

In order to provide an easy approach for analysing vulnerability impacts and how they cascade (Kotzanikolaou, Theoharidou and Gritzalis, 2013) through an ICS network structure, and guide the development of a cyber security plan, a conceptual functional dependency modelling approach relating topological layering of devices in a typical ICS network infrastructure (Haimes *et al.*, 2007; Theoharidou, Kotzanikolaou and Gritzalis, 2010) is proposed, from which an impact dependency ratio attribute can be derived. It focuses on the scope of impacts and consequences on the system. A dependency modelling approach to cyber-attack impact analysis bears great potentials to be effective in the ICSE, since it necessitates relating the attacks on one device or operational infrastructure to its corresponding functional/operational impact on another device(s) that interact with the attacked device. A cascading impact systems paradigm provides an easy method to model the impact-flow relationship between an affected device and its underlying connected device(s). It ultimately relates them to the extent of the overall operational impact. It can guide the development of a strategic countermeasure for significantly reducing if not eliminating potential impacts. The quantities derived can also be used as metric inputs in a larger security risk management goal.

The key interest here is to determine the vulnerabilities and host components which when attacked bear the potential to amass a wider scope of ripple effects in terms of failures or malfunction on the entire system. This work underscores the functionalities of the ICSE structured and layered classes as defined in the Purdue Enterprise Reference Architecture (PERA) (Macaulay and Singer, 2012). These layered architecture classes include: *Field Execution*, *Data and Process Execution and Monitoring*, *Data and Process Control*, *Gateway Communications*, and *Network-Based Defence Mechanism/Setup*. This work underscores the concept of learning their interrelationships and interactions with respect to dependencies and using same to conjecture and represent cascading impacts. The ICS network is broken down into operational functions consisting of nodes with similar function but with relatively distinct operations depending on the environment. The connection amongst nodes across multiple layers suggests a form of layered interaction and dependency structure. For example, a PLC is dependent on the normal functions of an engineering workstation to manipulate field sensors and actuators. Similarly, it is viewed that a disturbing impact on the engineering workstation has the potential to cascade down

to the PLC with significant effects, which also bear the potential to cascading further down to the sensors and actuators. Since nodes are the pivots of activities on the ICS network, it is typical for an attack on an ICSE to target a technology (infrastructure) node in some way, and potentially affect the status availability, integrity, confidentiality, or any combination of these for any connected downward-route-dependent nodes. To model node dependency in relation to impact cascade, it is necessary to capture the component-link relationship of an ICS network, which indicates the likely rippling of adverse impacts on the ICS. This can help the appropriation of controls and countermeasures.

Environmental severity ratio (R_{ES}) measure enables the customisation of standardised environment severity scores depending on the importance of affected asset to the attainment of function and operational objectives. The attributes considered are measured in relations to the availability of complementary/alternative security controls for attaining availability, integrity, and confidentiality. Since different environment setups can yield different severity potentials, the environment metric is considered the modified equivalence of the base metric, and assigned values based on the status of the environment. The impact dependency ratio R_{y_v} derived from the functional dependency index y_v also presents an attribute that relates to the environment with respect to impact, since the position placement of nodes affects direct and indirect relationship interactions with other nodes. Thus, this work proposes that a more profound impact potential of a device relative to a known vulnerability is derivable using the device's functional dependency index and its environment metric score obtained from standard CVSS ratings.

These two quantitative metric values can be multiplied to yield a more reflective dependency impact potential (γ) for a device v with a known vulnerability and its environmental severity, and represented mathematically in Equation (6-10). The environmental severity and impact dependency ratio derivatives are explained in the following sub-sections.

$$\gamma = R_{ES} \times R_{y_v} \quad (6-10)$$

6.3.2.4 Functional Dependency Modelling

In the functional dependency modelling, a relationship structure is defined based on the connectivity of components in a network and the configuration of the network. A

dependency is inferred if a specific node j is linked (physically or logically) to an upper-layer component i and relies on the link from i for the receipt or processing of signal or data streams to carry out its own basic functions. A directed arrow from i to j ($i \rightarrow j$) indicates the established connection for the flow or exchange of data streams between the two nodes (components). It can also be used to represent a potential transfer of attack impact from an originating component i to a dependent component j . Any form of impairment due to cyber-attack on component i , the impact is presumed to potentially ripple down to component j , altering its functionality or operations as well. In a multi-order dependency structure, the impact could cascade from a single component to others in multiple layers. To clearly articulate the dependency status of a given component or asset in the network, it is necessary to provide answers to questions like: Does an asset have one or more asset(s) depending on it for data or instruction set to accomplish a desirable process? Does it depend on any node(s) to accomplish its set operation in the system? Is it connected to an industrial LAN/WAN? Does it have a known exploitable vulnerability? and Does its function contribute to the actualisation of a set of system operations? Providing answers to these questions can guide the correct mapping of node dependencies in the ICS network.

A typical ICSE network consists of a set of connected components, thus, can be represented using a directed graph G as an ordered pair (V, E) composed of a finite set of vertices V , and a binary relation E on V . The elements of E are referred to as edges (arrows) and represent the '*impact link*' that cascades along successive edges. These arrows form an ordered pair $e = (v_i, v_j)$, where $v_i, v_j \in V$ represent components in the network, and e represents the dependency impact link from an originating component v_i to a destination component v_j .

To develop a functional dependency and impact model, every component (physical execution, logical execution and monitoring, control and workflow management, and boundary-based devices) is mapped to a *vertex* and every dependency impact link to an *arrow* in a graph. This graph-based structure can be used to model the topological dependencies in ICSE network and used to capture attack impacts. On a typical directed graph structure, this corresponds to the sum of the number of directed edges e going out of a source node v_i , and that of the target destination node(s) v_j . However, the impact of an

attack starts from a source node, so that the determination of a dependency impact captures all possible impact points on the graph or network.

For every vulnerability attributed to a component v on the network, a corresponding functional dependency impact index $y = f(v)$ is proposed as the cumulative dependency links across the component from the vertex v inclusive. When a component is attacked, the functional dependency index is conceived to as the number of components that are included along a path following the arrows from the originating component. Depending on the existence or otherwise of a functional dependency link, initial impact(s) of the attack is typically expressed in the origin v_i , and flows downward to any connected node v_j along the same path. A logical switch function is used to represent this conditional existence of a functional dependency link between any two nodes on the network. A logical 0 (*FALSE*) implies a '*non-dependency link*', i.e., connection not configured, and a '1' (*TRUE*) implies a '*dependency link*', i.e., connection configured. A switch function is defined as Equation (6-11).

$$\varphi(v) = \begin{cases} 1 & \rightarrow \text{connection configured} \\ 0 & \rightarrow \text{connection not configured} \end{cases} \quad (6-11)$$

For a structural tree network, a component's functional dependency index (denoted as y_v) can be construed as the sum of functional dependency indices of components connected to component v , and it is formulated with Equation (6-12).

$$y_v = \sum_{u \in T_v} (y_u \times \varphi(v)) \quad (6-12)$$

where, T_v is the subset of components that can be reached directly from v .

The ratio of impact dependency may be derived in relations to the highest possible dependency; representing the widest or worse case impact of an attack. This can be assumed to involve cases where a dependency runs through all the devices on the network, such that all are affected when a certain vulnerability is exploited. This should typically yield an impact dependency ratio of 1. A zero (0) would mean no device is affected. From Equation (6-12), let the highest possible functional dependency index be represented as $\max(y_v)$, so that the *impact dependency ratio*, (R_{y_v}) can be represented as the degree/proportion of dependency impact amassable from the exploit of a certain

vulnerability in relations to the *widest* or *worst-case* dependency impact. This is represented mathematically in Equation (6-13).

$$R_{y_v} = \frac{y_v}{\max(y_v)} \quad (6-13)$$

It is noted that, for a non-tree network; the components to which component v links may be reachable from component u . Therefore, Equation (6-12) may not be suitable for this case. The algorithm for determining reachable vertices from a vertex v in a digraph G can be applied to search components that a component v can reach to. Both depth-first and breadth-first search algorithms for digraph can be used for this purpose. Addressing these algorithms is not within the scope this work.

6.3.2.5 Environmental Severity Ratio

Cyber-attack impacts in ICSE are typically demonstrated in the physical environment, hence, additional factors viewed to affect the impact of an attack in relation to the environment are considered. These also contribute to an overall impact potential, and are highlighted in the light of vulnerability environmental (severity) metrics defined by standard CVSS severity scores (Mell, Scarfone and Romanosky, 2007). In traditional IT security analysis, CVSS environmental score are often considered optional, however, this study emphasises that with regards to the attainment of realistic impact estimates for vulnerabilities and attacks in ICSE, environmental scores should be considered important and necessary. The environmental metric domain is characterised by: *collateral damage* potential of a vulnerability, its *target distribution*, and its *target security requirement violation* all with respect to the target operational environment (Chejara, Garg and Singh, 2013). These allow scoring analysts to incorporate attributes for potential losses, the proportion of such losses, and affected asset importance. It further allows for the integration of security controls which may lessen any consequences, as well as promote or relegate the importance of a vulnerable system according to functional/operational objectives and risks (Mell, Scarfone and Romanosky, 2007). ES is used to denote the *vulnerability environmental severity* while adopting the standard CVSS formula prescriptions as presented in Equation (6-14). For this, the CVSS 2.0 is used because it retains a larger base record for existing vulnerabilities. The newer CVSS 3.0 rating scheme is still being updated, some vulnerabilities do not yet have CVSS 3.0 scores. Notwithstanding, this evaluation approach can be applied to CVSS 3.0 environmental severity metric function in

scenarios where all discovered vulnerabilities have CVSS 3.0 scores. It further provides a background guide for the adoption of any future changes to standard vulnerability rating scheme functions. To preserve the consistency of CVSS2.0, the values of all relevant formula are rounded to 1 decimal. Similarly, using the CVSS severity rating scale [0,10]; 0 indicating a 'no severity' and 10 indicating a 'critical severity' to represent standard static base scores (BS) of vulnerabilities, the environmental Severity Ratio (ES_r) can be derived using Equation (6-15). This is derived using the environment score (ES) function represented as Equation (6-14).

$$ES = \text{round}((AT + (10 - AT) \times CDP) \times TD \times 10)/10 \quad (6-14)$$

$$R_{ES} = \frac{ES}{10} \quad (6-15)$$

where:

$$AT = \text{round}(AI \times Ex \times RL \times RC \times 10)/10$$

$$AI = \min(10, 10.41(1 - (1 - C \times CR) \times (1 - I \times IR) \times (1 - A \times AR)))$$

And:

AT = Adjusted Temporal, CDP = Collateral Damage Potential, TD = Target Distribution, AI = Adjusted Impact, Ex = Exploitability, RL = Remediation Level, RC = Report Confidence, C = Confidentiality Impact, I = Integrity Impact, A = Availability Impact, CR = Confidentiality Requirements, IR = Integrity Requirements, AR = Availability Requirements

6.4 Case Study

To test the realistic application of the proposed approach and evaluate its suitability in the context proposed, a case study scenario was adopted involving the ICS-CS network testbed developed in chapter 0. The testbed design satisfies standard ICS testbed requirements and guidelines in NIST SP 800-82 r2 (Stouffer *et al.*, 2015) for ICS security and NISTIR 8089 (Candell Jr., Zimmerman and Stouffer, 2015) for ICS cybersecurity analysis. The four basic ICS network architecture components: *the control centre*, *the communication architecture*, *the field devices* and *the physical process*, are represented using one or more associated devices prescribed by Holm *et al* (2015).

As indicated in chapter 4, the testbed adopts a PLC-based product assembly and conveying system referred to as 'ICS-CS' developed over LAN with real-time profinet protocols for ICS components communications, and ethernet-based IP protocol-enabled communications IT asset communications. This is to simulate the basic functionalities of sensing and moving of items. A second field device; 3-dimensional Robot Arm was added to the network and connected to the extended I/O module interface. This does not affect the representativeness of the testbed as multiple field equipment and processes can be enabled within a single ICS network (Candell Jr., Zimmerman and Stouffer, 2015). The proposed MAVCA model was applied to the testbed for determining technical vulnerabilities on the configured ICS components, estimate vulnerability severities, impacts, and prioritisation of controls. This scenario is adopted as a simplistic representation to demonstrate the application of the approach proposed, since it not feasible to apply the approach on an actual industrial network for the reason of avoiding the damaging functional impacts that may be incurred in the process.

6.4.1 Network Structure and Vulnerability Scan

To recap the testbed network structure including the new field equipment added, the network consists of a PLC with extended Input/Output Modules, HMI, Industrial Switch, Control Workstation, and two miniature field devices (Conveyor/Punching Machine and 3D Robot Arm machine). In line with the assumption presented earlier, a computer representing the attacker's machine is also included in the Network. Table 6-2 presents the modified network architecture of the testbed. The 3-D robot and conveyor/punching machines represent field equipment controlled by the PLC along with the extended I-O module. The external I/O module, the HMI, and process control machine are connected via the Industrial Switch, which serves as the central hub for the PROFINET network. The PLC is linked to the same hub, sharing a direct communication connection on the PROFINET network.

The test explored the application of the proposed methodology to estimate failure criticalities and prioritise potential impacts of inherent vulnerabilities. Hence, the prescribed procedures in the MAVCA methodology were followed starting with a network vulnerability scan and analysis. This was performed using *Nexpose* (Rapid7, 2017) automated vulnerability analysis tool to scan the network for possible vulnerabilities. The screenshots are presented in Appendices B-23, B-24, B-25 and B-26. The results of the vulnerability

scan are summarised in Appendices A-5, A-6, and A-7. For each discovered vulnerability on the network, its corresponding severity base score (*BS*) was documented. For this test, the CVSS/CWE 2.0 base score of the vulnerabilities were used. Though there is currently a new and more updated CVSS 3.0 scheme for evaluating vulnerabilities, some of the discovered vulnerabilities did not have updated and documented CVSS 3.0 scores. But all vulnerabilities had CVSS 2.0 severity ratings.

6.4.2 Graph Structure for Functional Dependencies

As described in 6.3.2.4, a graph-based structure is used to model the functional dependencies among components in ICSE network. This helps to capture the potential rippling impacts of disrupted or distorted functions. We use functional dependencies to represent the influence of a component's (mal)functions on the functions of other components on the network. For example, from Table 6-2, the conveyor/punching machine's functions solely depends on the normal functions of the PLC component it connects. Similarly, based on connections and configurations, the PLC, its extended I/O module, and the HMI are all linked to the industrial switch. Hence, the unimpaired functions of these three components would depend on the unimpaired function of the switch. It means that if the switch is impaired, such impairment could cause a resulting impairment on the PLC, which in turn can cause extended impairment on the conveyor/punching machine. The functional dependency directed graph in Table 6-3 represents the various functional relationships amongst the components in the network architecture. Same can be used to infer functional dependency values for each component using Equation (6-12) accordingly.

6.4.3 Results

From the testbed vulnerability scan, 11 vulnerabilities were discovered on the assets that made up the system. It was particularly observed that some of the assets had multiple vulnerabilities each with different base scores as indicated in Table 6-2. For example, two vulnerabilities: k_2 and k_5 were found in the programmable logic controller (PLC) with severity CVSS 2.0 base scores of 10.0 and 8.0 respectively. Similarly, the Ethernet switch had four vulnerabilities, while the interface module and control workstation had two vulnerabilities each. Only the HMI had a single vulnerability. Using appropriate equations, the corresponding temporal and environment score ratios of each vulnerability were

evaluated. Functional dependency index was evaluated for each component that had a vulnerability, and the probability of attack determined accordingly. These were done in line with the attack path analysis concept earlier discussed in the proposed approach (6.2.2.4).

For example, analysing the PLC vulnerabilities, vulnerability k_2 on the PLC indicated a “Default or guessable SNMP community names: public” vulnerability discovered in 1999 as observed by the vulnerability number. The vulnerability is expressed as a weak authentication mechanism in the PLC as a network device through the use of unencrypted ‘community string’ (Gary A, 2000). Exploiting this, attackers can acquire a lot of details about a network including system information, routing table, and tcp connections, with which remote access, reconfiguration, and shut down of devices were possible. This indicates a breach and threat to availability, integrity, and confidentiality of the PLC. The enormous magnitude of damage that is opened-up to an attacker, and even worse; that the attacks can be perpetrated unnoticed explains why a CVSS 2.0 base score (BS) of 10.0 is assigned to this vulnerability. However, this only accounts for the intrinsic features of the vulnerability. This work further shows how the dynamic feature values can be derived using the documented guide in Appendix A-3, and how respective metric quantities were computed for each vulnerability. The dynamic feature values were derived following the vulnerability descriptions from vulnerability analysis report and extended research about the vulnerability in relations to the test network’s design, structure, and attributes. Table 6-1 presents the dynamic feature variables and values of k_2 vulnerability as derived. The complete evaluation data are presented in Appendices A-3 and A-4.

Note:

The impact dependency ratio, $R_{y_v} = 7$, implies worst case dependency impact feasible on the ICSE testbed network from design architecture (it represents the case where a vulnerability on the industrial switch is exploited, and whose functional impact can ripple down the entire network of components). The calculation of dynamic metric features is presented as follows:

Table 6-1: k_2 Vulnerability Impact Evaluation

Vulnerability Number: CVE-1999-0254		
Description: - Default or guessable SNMP community names: public		
Affected Device: - PLC		
Label: - k_2		
Base Score (BS): - 10.0 (CVSS 2.0 score from Vulnerability Scanning)		
Metric	Metric Value	Numeric Value
Exploitability (Ex)	Functional	0.95
Remediation Level (RL)	Workaround	0.95
Report Confidence (RC)	Confirmed	1.00
Collateral Damage Potential (CDP)	Medium-high	0.4
Target Distribution (TD)	Medium	0.75
Confidentiality Requirement (CR)	Medium	1.0
Integrity Requirement (IR)	High	1.51
Availability Requirement (AR)	High	1.51
Confidentiality Impact (C)	Complete	0.660
Integrity Impact (I)	Complete	0.660
Availability Impact (A)	Complete	0.660

$y_v = 4$ (i.e. Total number of devices that are connected and depend on the PLC)

$$AI = \min(10, 10.41(1 - (1 - 0.660 \times 1.0) \times (1 - 0.660 \times 1.0) \times (1 - 0.660 \times 1.0)))$$

$$AI = \min(10, 9.9999607)$$

$$AI = 9.9999607$$

$$AT = \text{round}(9.9999607 \times 0.95 \times 0.95 \times 1.00 \times 10)/10$$

$$AT = 9.1$$

$$ES = \text{round}((9.1 + (10 - 9.1) \times 0.4) \times 0.75 \times 10)/10 = 7.1$$

$$R_{ES} = \frac{7.1}{10} = 0.71$$

$$\gamma = 0.57 \times 0.71$$

$$\gamma \cong 0.41$$

$$TS = \text{round}(10.0 \times 0.95 \times 0.95 \times 1.00 \times 10)/10$$

$$R_{TS} = \frac{9.1}{10} = 0.91$$

$$Pa = P(k_2) = \frac{n_{k_2}}{N_K}, \text{ where } n_{k_2} = 8, \text{ and } N_K = 15,$$

$$Pa = P(k_2) = \frac{8}{15} = 0.533$$

$$\beta = 0.91 \times 0.533$$

$$\beta \cong 0.48$$

$$CI(k_2) = m_{k_2} = 0.48 \times 0.41$$

$$m_{k_2} = 0.1969$$

The computed temporal score (TS) of k_2 is 9.1, and a temporary score ratio (TSr) of 0.91. Its environmental score (ES) is 7.1, and a corresponding environmental score ratio (ESr) of 0.71. The PLC being the host asset of k_2 had a functional dependency index $y_v = 4$ because it had a self-inclusive dependency link with four devices, the maximum dependency expression on the network is 7. This yields a dependency impact ratio $R(y_v)$ of 0.57. Analysing the attack paths to all the 11 vulnerabilities on the system, a total of 15 attack paths were derived, and 8 of those paths had k_2 in their path enumeration; yielding a 0.53 probability of k_2 being exploited in the network. Accordingly, the overall exploit potential of k_2 was computed at ≈ 0.49 , its impact potential was 0.41, while the generalised criticality index m_{k_2} was ≈ 0.44 . Adopting the same approach for evaluating quantities for k_5 also in the PLC yielded temporal score of 7.6, temporary score ratio of 0.76, environmental score of 7.3, environmental score ratio of 0.73, vulnerability exploit potential of ≈ 0.41 , impact potential of 0.42, and a criticality index $m_{k_5} \approx 0.41$. Full details of all vulnerability valuations are contained in Table 6-2. Severity Estimation results are presented in Table 6-3, and prioritisation results presented in Table 6-4. Accordingly, corresponding graphical illustration of the vulnerability attributes are indicated in Figure 6-4, Figure 6-5, and Figure 6-6.

Table 6-2: Testbed Vulnerability Results

Vulnerability Number	Description	Label	Devices Affected	Base Score
CVE-1999-0254	Default or guessable SNMP community names: public	k_1	Ethernet Switch	10.0
		k_2	PLC	10.0
		k_3	I/O Module	10.0
CWE-319	SNMP credentials transmitted in clear text	k_4	Ethernet Switch	8.0
		k_5	PLC	8.0
		k_6	I/O Module	8.0
Unnumbered	Reset Password Backdoor Vulnerability in Windows 7	k_7	Control Workstation	7.9
CVE-2015-6465	Resource Exhaustion: authenticated users to cause a denial of service (reboot) - Port 80	k_8	Ethernet Switch	6.8
CVE-1999-0524	ICMP timestamp response	k_9	Control Workstation	0.0
		k_{10}	Ethernet Switch	0.0
		k_{11}	HMI	0.0

Table 6-3: Severity Estimation Results

Vul. Label	Devices Affected	TS	R_{TS}	ES	R_{ES}	y_v	R_{y_v}	P_A
k_1	Ethernet Switch	9.1	0.91	9.5	0.95	7	1.00	0.80
k_2	PLC	9.1	0.91	7.1	0.71	4	0.57	0.53
k_3	I/O Module	9.1	0.91	2.4	0.24	2	0.29	0.27
k_4	Ethernet Switch	7.6	0.76	9.7	0.97	7	1.00	0.80
k_5	PLC	7.6	0.76	7.3	0.73	4	0.57	0.53
k_6	I/O Module	7.6	0.76	2.5	0.25	2	0.29	0.27
k_7	Control Workstation	6.5	0.65	9.1	0.91	6	0.86	0.67
k_8	Ethernet Switch	6.0	0.60	9.4	0.94	7	1.00	0.80
k_9	Control Workstation	0.0	0.00	Null	Null	6	0.86	0.67
k_{10}	Ethernet Switch	0.0	0.00	Null	Null	7	1.00	0.80
k_{11}	HMI	0.0	0.00	Null	Null	1	0.14	0.07

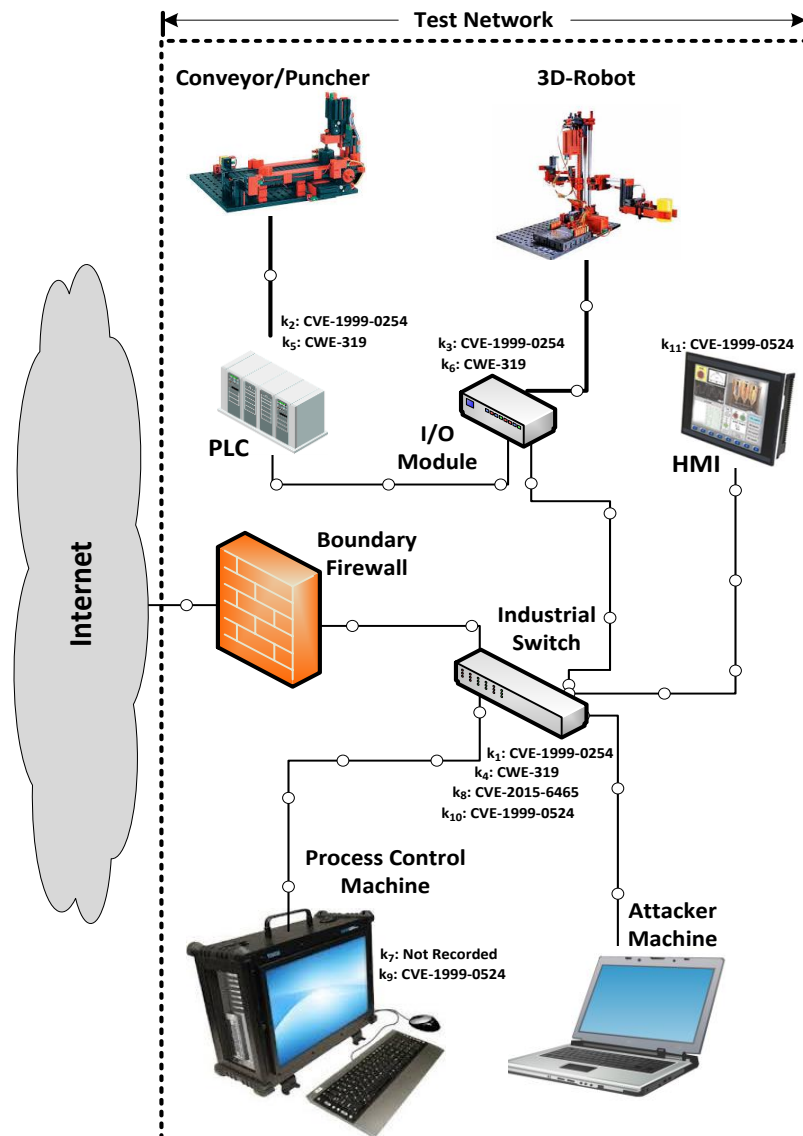


Figure 6-2: ICS Emulator Network Architecture for Test Scenario and Vulnerability Mapping

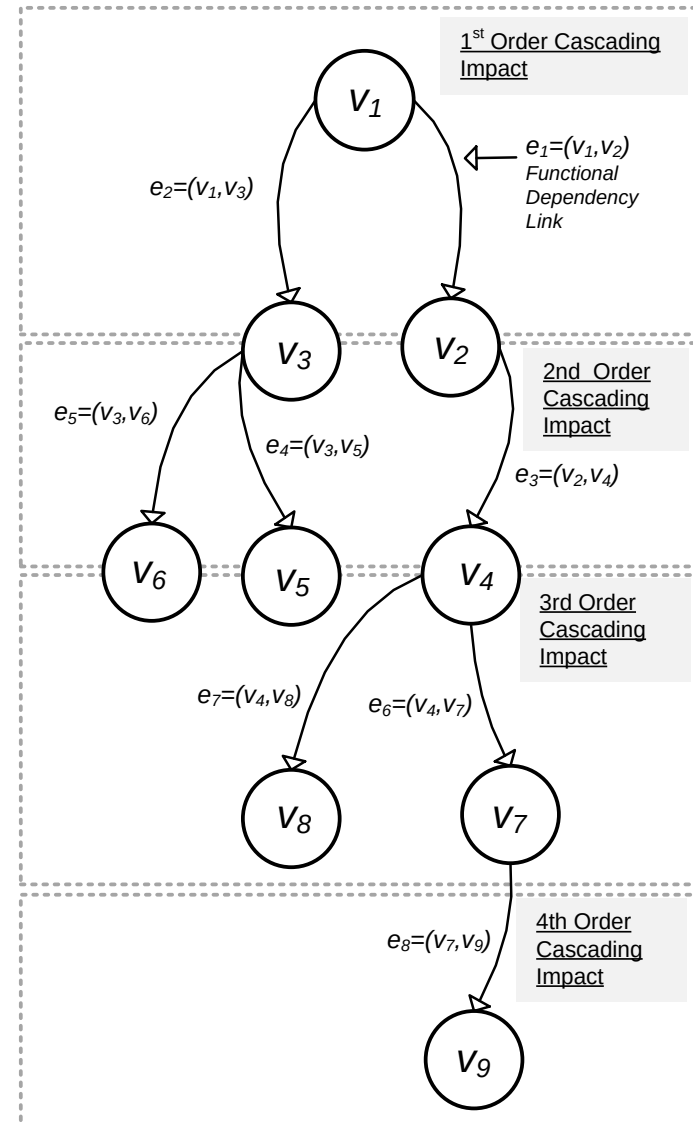


Figure 6-3: Functional Dependency and Cascading Impact Graph Representation

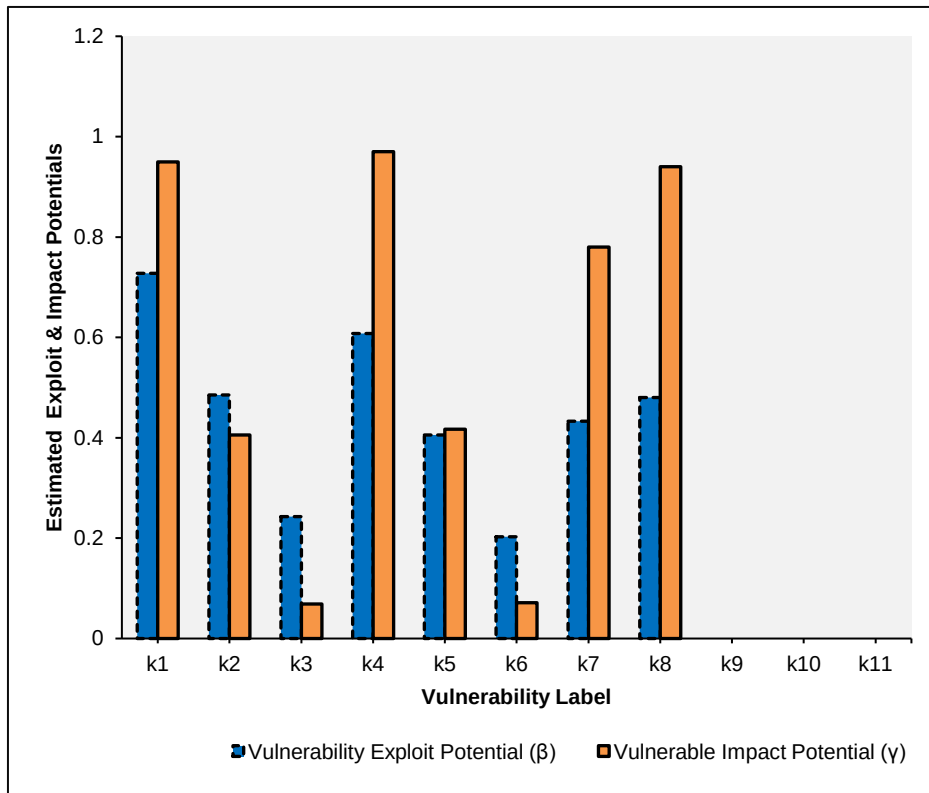


Figure 6-4: Vulnerability Exploit & Impact Potentials

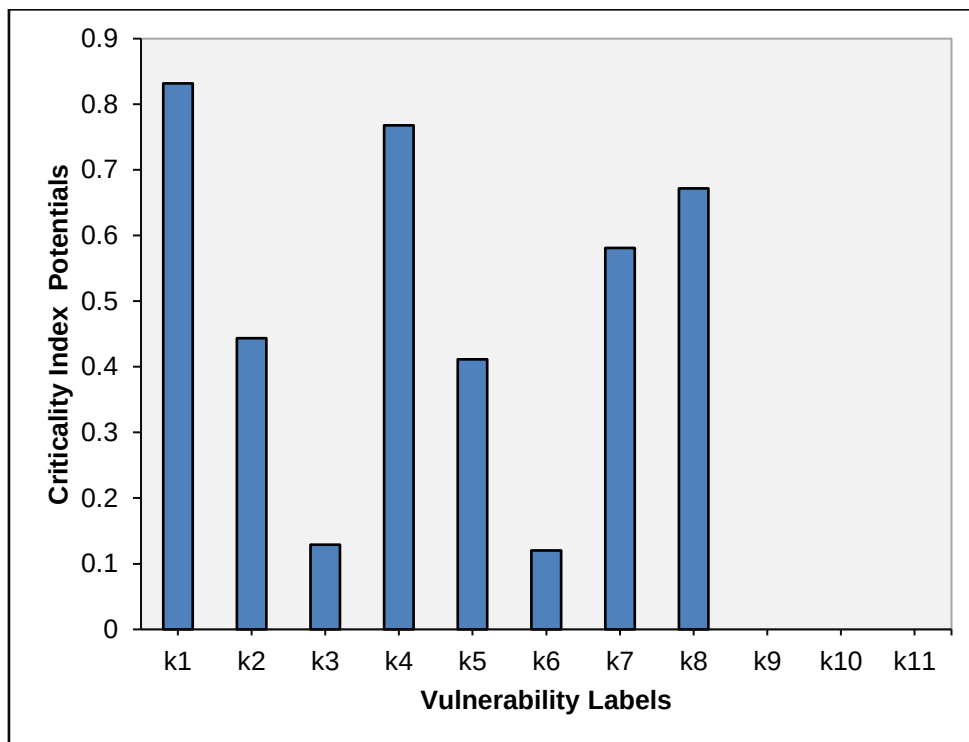


Figure 6-5: Criticality Index Estimation

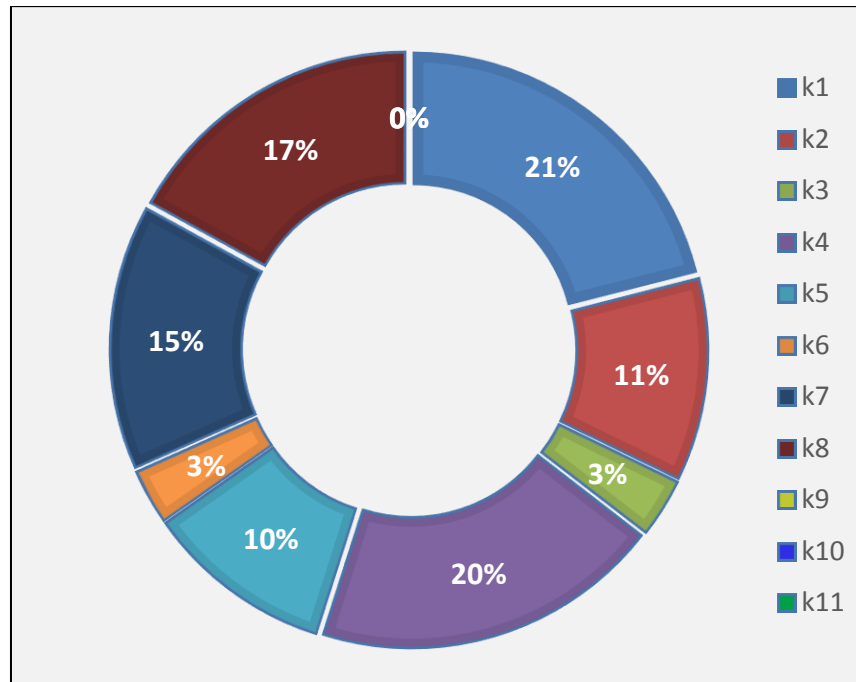


Figure 6-6: Criticality Index Rationing

Table 6-4: Severity Estimation and Prioritisation Results

Vulnerability Label	Vulnerability Impact Potential	Vulnerability Exploit Potential	Criticality Index	Prioritisation on Index
	γ	β		
k_1	0.950	0.728	0.8316	Pr_1
k_4	0.970	0.608	0.7679	Pr_2
k_8	0.940	0.480	0.6717	Pr_3
k_7	0.780	0.433	0.5813	Pr_4
k_2	0.410	0.485	0.4437	Pr_5
k_5	0.420	0.405	0.4111	Pr_6
k_3	0.070	0.243	0.1289	Pr_7
k_6	0.071	0.203	0.1203	Pr_8
k_{10}	Null	0	Null	Pr_9
k_9	Null	0	Null	Pr_{10}
k_{11}	Null	0	Null	Pr_{11}

6.4.4 Analysis and Discussion

From the results of initial vulnerability scan indicated in Table 6-2, 11 vulnerabilities exist on the testbed network. However, there are multiple occurrences of the same vulnerability with the same CVSS base score ratings in multiple assets (CVE-1999-0254 in Ethernet switch, PLC, and I/O module, CWE-319 also in Ethernet switch, PLC, and I/O module,

and CVE-1999-0524 in control workstation, Ethernet switch, and HMI), and occurrence of different vulnerabilities in a single ICS asset distribution (k_1 , k_4 , k_8 , and k_{10} in the Ethernet switch; k_2 , and k_5 in the PLC, k_3 and k_6 in the I/O module, k_7 and k_9 in the control workstation). Normally, using the standard approaches that use vulnerability CVSS base scores alone for impact analysis would not provide suitable solutions due to the presence of uncertainties. It is directly unclear which vulnerability can have the greatest impact on the ICSE network. Having multiple occurrences of the same vulnerability in disparate assets at the same time also introduces another uncertainty as to the specific host assets bearing the vulnerability capable of the greatest impact.

Similarly, approaches that combine base score metrics and attack probabilities do not account for environmental dynamics such as the position of the vulnerability host or the impact on the number of components that depend on such vulnerable host. Thus, might not provide sufficient representation of vulnerability impact. MAVCA model attempts to address both limitations. It introduces additional vulnerability factors and metrics such CVSS temporal metric and probability of attack to resolve uncertainties in vulnerabilities. It also combines CVSS environmental metric with vulnerability host functional dependency metric to account for environmental dynamics that support estimation of impact. Resolving these uncertainties and accounting for environmental influences demonstrate the reliability of MAVCA to support new insight into vulnerability and impact analysis, as well as support control prioritisation in a way that contributes solutions to the limitation of existing approaches.

From the results of severity/impact estimations and prioritisation, the proposed MAVCA model can support strategic and effective security control response in a multilateral insecurity domain. Strategic effectiveness relates to the capacity to resolve the largest possible critical vulnerability per response time. Clearly, the CVSS base score metric values of the vulnerabilities alone could not have been enough to support this type of solution approach, since the score ranges presented similar standard scores for multiple vulnerability occurrences. At this level, multiple vulnerabilities are considered to have the same severity and impact magnitudes, which might not be true considering the testbed network environment and the positions of the vulnerabilities. Further engagement of procedures in proposed method potentially leads closer to the realistic state of severity and impacts desired.

Lower temporal score values are observed in comparison with respective base score for all discovered vulnerabilities. Although the values for environment scores are slightly higher than temporal scores, they are still lower than the base scores of all discovered vulnerabilities. For example, as shown in

Table 6-3, k_1 , k_2 , and k_3 all had a uniform severity base scores of 10.0, which were reduced to a uniform severity temporal score of 9.1, temporal score ratios of 0.91, but different severity environment score of 9.5, 7.1, and 2.4, and environmental score ratios of 0.95, 0.71, and 0.24 respectively. The derivation of temporal and environmental scores and ratios elucidate further and deeper considerations of dynamic features and criteria more specific to the vulnerability, and in relation to its immediate host asset and environment. It is learnt that a vulnerability life transformation demonstrated as changes in the characteristics of vulnerabilities; for example, a remediation level change from 'unavailable' to 'temporal-fix' or 'official-fix', a collateral damage potential change from 'high' to 'low', indicates a more valid updated state of the vulnerability than its initial base state.

Essentially, this implies a shift from initial vulnerability severity characterisation from a global viewpoint to a more localised viewpoint, thus, gaining more realism about the vulnerability. This initial result indicate that standard vulnerability base scores represent severity globally (i.e. in relations to external factors). However, a realistic measure of severity can be estimated with corresponding magnitude ratios using the temporal score, and even more using the environment score. It suggests that although a vulnerability can have a generalised view of severity scale, the frequency of the vulnerability, the topological positioning of the vulnerability's host asset within the localised system, the availability of a known remediation measure, and exploit at varied modification requirements, all contribute to a more realistic and better measures of severity. Based on these combined criteria, the vulnerability with the highest severity environmental score is k_4 , with $ES = 9.7$, and $ES_r = 0.97$ (*SNMP credentials transmitted in clear text*) on the Ethernet switch. However, the functional dependence of the component bearing the k_4 vulnerability has not been considered yet. The magnitude of impact on other functional components dependent on the ethernet switch is yet to be considered, which makes the current severity consideration insufficient for resolving functional impact prioritisation of the vulnerabilities. More so, three vulnerabilities (k_9 , k_{10} , and k_{11}) do not have

environmental scores because their base score are 0.0; implying a no severity status. Since both temporal and environmental scores are considered better precise representations of vulnerability severities (base scores) that depend on the base scores in relations to the dynamic changes in the local network environment, it is reasonable to arrive at null scores for the two dynamic quantities.

With varied functional dependency ratios and attack path probabilities, each vulnerability in the list yields a different vulnerability attack potential. Although different vulnerabilities in a single asset as in the case of (k_1 , k_4 , k_8 , and k_{10}) can have similar attack path probabilities (0.8), overall individual vulnerability attack potential can vary based on each vulnerability's exploit modification requirement, and availability of remediation capabilities all integrated into a temporal metric score. These account for the varied vulnerability exploit potentials β ; ($\beta_{k1} = 0.728$, $\beta_{k4} = 0.608$, $\beta_{k8} = 0.480$, and $\beta_{k10} = 0.000$) for the respective vulnerabilities in the industrial ethernet switch. Higher values for vulnerability exploit potential indicates a higher likelihood of a vulnerability being attacked, and lower values indicate less likelihoods. The results also indicate that multiple vulnerabilities in a single asset or system can have different attack potentials that informs of the likelihoods of each vulnerability to attract exploitation interest in relation to other vulnerabilities in the system.

From Table 6-4, the vulnerability with the highest exploit potential is k_1 , $\beta_{k1}=0.728$ (*Default or guessable SNMP community names: public*) on the Ethernet switch. Valuations for vulnerability impact potential is also derived with the least quantifiable impact potential γ of 0.070 for k_3 vulnerability on the extended I/O module, and the highest to be 0.970 for k_4 vulnerability on the ethernet switch as shown in Figure 6-4. These probabilistic values indicate a quantitative interpretation and representation of the potential scale of ripple effects attributed to the exploitation of corresponding vulnerabilities on specific host assets based on the presented architecture. Accordingly, vulnerabilities with no temporal scores and ratios do not have computable vulnerability impact potentials. The *Criticality index* (m) is derived based on the vulnerability exploit potential (β) and the vulnerability impacts potential as indicated in Equation (6-1). The prioritisation of vulnerability control is performed on the set M of criticality indices obtained using Equation (6-2).

From Figure 6-5 and Figure 6-6, and applying Equation (6-2) for determining 'first priority' response, k_1 with the highest criticality index of 0.8316 takes-on the first priority position

(Pr_1), thus, should be resolved first. This is followed by k_4 ($m_{k_4} = 0.7679$), k_8 ($m_{k_8} = 0.6717$), k_7 ($m_{k_7} = 0.5813$), etc, in that order. Analytically, the k_1 vulnerability is resident on the industrial switch that serves as the central communication medium for all other IP-enabled devices (PLC, Extended IO, Control Workstation, and HMI) on the test network, hence, all these devices alongside their connected field equipment all depend on the correct functioning of the switch. Any malfunction of the switch can cause all other components that depend on it to also malfunction.

From CVSS description, the k_1 vulnerability on the switch allows for unauthorised disclosure of information; unauthorised modification, and disruption of services. It can be exploited via a network medium and does not require any form of authentication to be accomplished. The attack path from this vulnerability to other devices are more numerous than any other device on the network. Attackers can gain view and gain access to information like login details of PLC, HMI, Control workstation perusing the network switch, and use same to illegally access and control the devices. This imply that if any of the described violations is accomplished via k_1 vulnerability on the industrial switch, all other connected devices stand the risk of also being victims of attacks like Man-in-the-middle, denial-of-service, session hijack, etc. Attacks like these can cause the manipulation of processes into forms other than the required, and the disruption of industrial processes from the PLC or Control workstation points. Access details of operational devices means that the devices can easily be misconfigured or stopped from being operational illegally.

However, similar direct attacks on this vulnerability but resident on the PLC and Extended IO module would only affect the target devices and the equipment connected to them, and not all other components. Hence, the impact in both cases would be much lower than that of the switch, because both devices (PLC and IO module) have fewer devices connected and dependent on them. Similarly, no other vulnerability on any other devices expresses as much impact characteristics like the k_1 vulnerability on the switch, which is why its criticality ratio is highest amongst all. Applying patch or any control fix on k_1 vulnerability on the switch will help block the potential to reach or attack all other devices connected to it, thus blocking the largest possible impact described. However, this must be done cautiously after such patches have been audited, to ensure that they do not affect existing configurations and functions of the industrial ethernet switch. Disabling the SNMP service on the switch if not in use also offers a good solution towards resolving this vulnerability,

and in cases where it is in use, the default community strings could be changed to private, or filtering should be applied to incoming UDP packets going to the affected port (41028). This way, access to details that can empower an attacker to exploit this vulnerability is denied.

In terms of asset-level prioritisation, just as it has been noted that k_1 , k_4 , and k_8 vulnerabilities all appear in the Ethernet switch, k_7 vulnerability appears in the Control workstation, k_2 and k_5 vulnerabilities appear in the PLC, etc. It can be inferred that the Ethernet switch as a single asset has the utmost number of vulnerabilities, and most critical cumulative valuations of impacts, thus should be considered the most critical asset of the testbed ICSE network considering its function, topological placement, and inherent vulnerability criticalities. With these, all known uncertainties that can impede selective prioritisation of vulnerabilities and impacts are potentially resolved. If using existing approaches that adopt CVSS base metric score to solve the same problem, it would be ambiguous and difficult to decide upon the order for resolving the vulnerabilities with a reasonable justification.

Clearly, analysed results indicate that MAVCA model contributes to knowledge by providing such missing basis and justification for the selection of vulnerabilities to be resolved per time and ensures that such selections are done strategically such that the highest possible solution is also engaged per resolution time. The effectiveness of the proposed approach relies on the ability to distinguish adequately and accurately between normal device/system functionalities and the outcome of a mal-functionality introduced by inherited perturbations from connected, trusted devices. It also relies on the understanding of known or identified vulnerabilities, their exploit potentials, and the dynamic nature of impacts due to control and environmental changes. This brings to light the value of expert knowledge and interpretations, which might be considered a limitation combined with the emphasis on known vulnerabilities, and without considerations for unknown or 'zero-day' vulnerabilities. These limitations are only introduced to the extent to which the model can be used for estimating exploitability impacts and the appropriation of remediation. The model is effective to the correct characterisation of the temporal and environmental attributes of vulnerabilities for which experience and expertise is required. Where this is in shortfall, the accuracy of results can also be affected. Again, the model may not be suitable for evaluating and characterising zero-day vulnerabilities since they would often

not have globally evaluated and assigned temporal and environmental attribute score. Although varied expert may allocate their own dynamic score based on knowledge of the vulnerability and documented dynamic attributes for similar vulnerabilities, the chances of inconsistency are high, which can raise the questions of accuracy of personalised scoring schemes.

It is a limitation that the proposed approach considers the security vulnerability and the impact of a domain environment solely from the context of technology security, it does not factor other system constituents like people and process security vulnerabilities, hence the sectoral view of security vulnerabilities and impacts, rather than an all-encompassing perspective.

Another limitation emerges from the reliance on only documented vulnerability scores, which makes the process unsuitable for estimating the impacts of undocumented vulnerabilities (vulnerabilities not contained or updated in the vulnerability analysis tool used). This is more constraining for ICSE networks as existing vulnerability databases currently do not support all the major ICS protocol applications and their vulnerabilities. This makes it infeasible for such vulnerability scanners to recognise vulnerabilities in proprietary ICS components. Thus, precision and cogency of outcomes are dependent on up-to-the-minute status of the vulnerability scanning/analysis database. Furthermore, any limitation(s) associated with an adopted vulnerability scoring protocol (e.g. CVSS 2.0 or 3.0) also typically affect the proposed approach. For instance, the subjectivity in the determination of temporal and environmental sub-group metrics in the CVSS scoring system introduces a limitation since there are potentials for variability of scores for the same vulnerability. The values would be dependent on the knowledge, expertise, and interpretation of the security assessors, which often vary. These could enable inconsistencies from multiple sources, especially due to uncertainties about software configurations.

With reference to the outcome of testbed vulnerability analysis using real vulnerability analysis tools and techniques, the proposed MAVCA model demonstrates value and novelty by combining ICSE component functional dependency attribute with CVSS environmental severity attribute, and Vulnerability attack probability with CVSS temporal severity attribute. Both combinations are used to derive two new metric quantities: vulnerability impact potential and vulnerability exploit potential respectively. These two are

also combined into an evaluation method that targets a near-accurate measure of function/technical impacts. This way, industrial organisations can consider and account for the unique attributes of their operational network environment (systems, network structure, components, and security controls), as well as, the changing state of vulnerabilities over time while undertaking a security impact assessment procedure. This presents a new contribution to prior works on vulnerability impact analysis which either adopted the static CVSS base metric characteristic of vulnerabilities, or a selection of few sub-metric attributes of the CVSS and no considerations for environmental attributes.

6.5 Chapter Summary

The proposed MAVCA model presents a scheme that improves technical security control implementation through impact estimation and prioritised remediation to address the issue related to the multiplicity of vulnerabilities, and dynamic environment factors. Asset prioritisation approach allows for the ranking of criticality significances for components relative to all other components of the network infrastructure, while vulnerability prioritisation enables ranking for security impact criticality based on individual vulnerabilities regardless of its host asset or frequency within the network. The criticality index metric proposed can support the assessment of a vulnerability's security impact such that can enable speedy decision making and response, thus to prevent potential damages. The security metrics derived from method can also be sub-metrics; proffering valuable inputs to a larger quantitative security metrics taxonomy. The proposed approach can also be integrated into a larger security risk assessment scheme of a larger distributed system. Another strength of the proposed approach is that it is flexible and easily adaptable to recurrent updates and changes. Although CVSS 2.0 scheme was adopted, the emerging CVSS 3.0 scheme can also be adapted into the approach to replace the CVSS 2.0 schemes for evaluating base, temporal, and environmental scores. That way, continual changes can be made appropriately to represent most current status of vulnerabilities and their corresponding impacts.

7 MODEL-BASED HUMAN (WORKFORCE) CYBER SECURITY CAPABILITY EVALUATION

7.1 Background

As cyber-attacks continue to grow, organisations have become concerned about how to react to security trends that threaten their business and operational relevance within the current highly-competitive business environment. Many recorded industrial cyber breaches have effectively beaten technological security solutions through exploiting human-factor limitations in knowledge and skills. These attack patterns have manipulated human elements into unintentionally conveying access to critical industrial assets.

Therefore, cyber security can be defined as the harmonisation of capabilities in people, processes, and(or) technologies to secure and control both authorised and/or unlawful access, disruption, destruction, or modification of electronic computing systems (hardware, software, and networks), the data and information they hold (Ani, H. M. He and Tiwari, 2016). Essentially, ICS can be viewed as a system of industrial technologies and infrastructures built and(or) operated by people (workforce) for the execution of processes towards attaining target products or services.

Probable motivations for these attacks may have stemmed from the perception that: (i) most ICSE workforce (personnel) are often unfamiliar with advanced digital (cyber) security concepts, and (ii) Information Technology security workforce are often unfamiliar with ICSE operational concepts. Updated security awareness and training can increase security capabilities, thus, presents a viable solution to this issue. However, engaging proper security capabilities hinges on an adequate understanding of recurrent security capacities of the workforce, and a clear outline of areas of weaknesses and strengths. Effectively improving security capacities of a workforce will typically require building strengths in the identified weak areas.

7.2 The Evaluation Model for User-Centred Security Capability

This work aims to provide a human-centred security capability and vulnerability evaluation method, which can be used to evaluate the security aptitude of human agents within ICSE. This evaluation approach provides a complement to traditional technical capability and vulnerability analysis, thus enables a wider view of vulnerability assessment of an

industrial environment where both technology and human agents are involved. More specifically, it explores how to understand and attribute quantitative ratings to security aptitudes of human agents in ICSE and use such information to drive a robust industrial cyber security responsiveness and resilience. The approach and measures can be useful to security auditors, analysts, managers and industrial system owners in carrying out human-level threats and vulnerabilities assessments, identify most vulnerable human agents, as well as the areas where security is low. Responding to these can significantly influence improvement of overall organisational security.

Workforce security capability is viewed from a normalised security proficiency for appropriate actions, reactions, or inactions of a human agent (user) for effective protection of operational systems. This is achieved by distinguishing between security knowledge and security skills drawing from previous researches (Reyes-García *et al.*, 2008; Kightley *et al.*, 2013). Familiarity with theoretical security concepts, procedures, and information about technology tools (software or hardware), process functionalities, scenarios, or projects, does not translate to an understanding of how to handle or respond (skills) to such tools, functionalities, or scenarios (Ryan and O'Connor, 2009). While knowledge emphasises a “know-that”, skills describes a “know-how” (Snowdon, 2004; Ryle, 2009), thus, should be evaluated separately (Beautement *et al.*, 2016). When necessary, the two constructs can be integrated to gain effective assessment of employee security capacities. A theoretical knowledge about security systems and phenomena (antivirus, IDS, firewalls, attack trends, etc), does not always translate to a practical ability to appropriately manage or respond to those systems and phenomena in the face of insecurity issues.

This study leans on the above distinction and explores the attainment of user-centred security capability measures by assessing and combining a user's security knowledge and skill characteristics. It addresses an open research for such security approach to support human actors in ICSE to fulfil operational and productivity objectives while maintaining security from multiple perspectives (Ben-Asher and Gonzalez, 2015; Beautement *et al.*, 2016). Security knowledge is conceived as ‘*theoretical know-that about ICS security landscape; covering threats, vulnerabilities, attack patterns, and control measures*’. Security skills is conceived as “*practical know-how for effective response or actions to curb or enforce the desired security*”. Security skills denote an ability to draw

from theoretical security knowledge to apply practical security actions to specific situations. Human actors in the ICSE such as IT experts, operations personnel, and OT personnel (field operators, automation engineers, SCADA and telemetry engineers, corporate management, etc) contribute directly and (or) indirectly, actively, or passively in control system process activities. Their corresponding individual security capabilities contribute directly and indirectly to the level of eventual organisational security capacity.

7.2.1 Model Formulation

In the model formulation, the '*weakest link*' attribute is introduced into the capability evaluation process where harmonised security capability ratings implicitly express measures of weakness or susceptibility to cyber-compromise. The collection of different values in a set of capability ratings is thus indicative of the varied, independent susceptibilities or weak status that can allow successful cyber-attacks. The multiplicity of capability values indicates the variety of potential attack surfaces corresponding to multiple human vulnerability weak-points for the success of cyber-attacks.

In a set of capability rating scores, higher values suggest higher defensive surfaces and lesser vulnerable surfaces in relations to a defined security baseline, and vice versa. Security defence and vulnerability baselines, and their representation quantitatively are used to support easy and clear identification, characterisation, and attribution of potential weak-links. The least capability value together with its corresponding vulnerability rating suggests the most vulnerable surface, and the highest likelihood of being targeted and becoming victim of cyber-attacks. Hence, it represents the weakest link. The new evaluation scheme presents a five-stage process: *definition*, *data collection*, *formulation*, *representation*, and *attribution* as presented in Figure 7-1. Each stage comprises of sub-stages that constitute an overall security capability evaluation of ICSE workforce.

7.2.1.1 Definition

This involves the definition of knowledge and skills security capability requirements, and the outline of desirable security capability baselines.

A. Security Requirements

Workforce security evaluation should be built upon defined security policies and requirements, compliant with relevant standards and best practices, and contextual

objectives of the specific operational environment. There exist several standards focusing on security in the ICSE, most of which are domain-specific, and do not cover all ICS types, security functionalities and requirements. For instance, the UK '10 Steps to Cyber Security' guideline (UK-Cabinet-Office, 2012), NIST SP 800-53 Revision 4 - guidance on security and privacy controls for systems and organisations (NIST, 2013b), NIST SP 800-82 Revision 2 - guide on industrial control system security, etc., all have sections that advise on requirements and guidelines regarding personnel security awareness and training. Combining recommendations from these standards can provide a better reference for situational security requirements to guide capability evaluations considering the specific features of the system/environment under consideration.

B. Security Baseline

Security baseline defines the desirable the status of the metrics/measures, representing varied capabilities and their corresponding attribute ratings from security requirements. It can be considered as the point of ideal capabilities of all workforce members. Any status lower than this ideal capability is considered a non-ideal capability.

In the proposed model, a capability ratio is introduced with value range of [0, 1]. Some standard recommendations FIPS 199 (NIST, 2004), (NIST, 2012) security categorisation recommendations are adopted to define three levels of capabilities: low, moderate, and high. The capability classification is applied to personalised security capability (*PSC*) metric and used to rank workforce security capability levels. However, the same priority classification can also be applied to knowledge and skills ratings.

7.2.1.2 Data Collection Methods and Tools

To determine the status of an entity in the light of prescribed security requirements, it is necessary to extract the information of the entity. It is pertinent for the workforce security capacity evaluation to aggregate the data of the response or reactions of ICSE workforce members to cyber threats, attacks and/or incidents through active and/or passive, direct and/or indirect security capability investigation. The investigation should reflect prescribed ICSE security policy guidelines, objectives, evaluation timeline, a targeted workforce size, and quality of expected feedback.

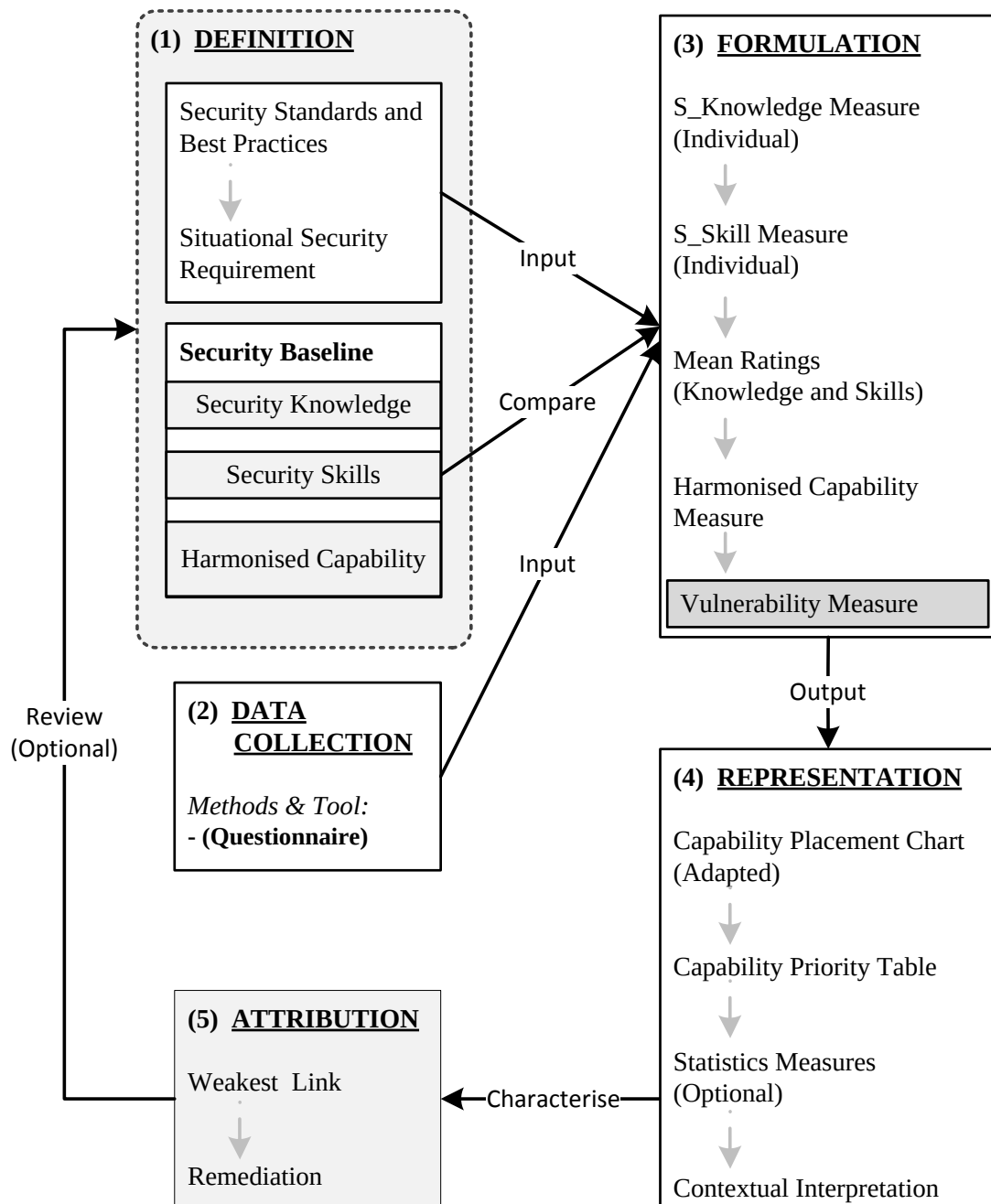


Figure 7-1: Human Workforce Security Capability Evaluation Scheme

For this evaluation, the test-based questionnaire tool is used for data collection following similar approaches observed in related literatures. This approach is typically used to determine if a tested subject qualifies in relations to certain prescribed standards as in this case; the *UK Cyber Security Essentials* (10 Steps to Cyber Security). Feedback data are collected and characterised to clearly represent attributes of individuals in the evaluated group. Score ratings are attributed based on the coded response/feedbacks in relations to the organisation's view of the security risk implications of each response to the security

objectives. These quantitative feedback data then serve as inputs to the computation stage of the evaluation model.

7.2.1.3 Formulation

Mathematical procedures are applied on collected data to evaluate workforce capability values. As described in 7.2, two groups of data corresponding to security knowledge and security skills evaluations are derived.

If p is an element in set P of ICSE workforce personnel, whose security capacity will be evaluated, and N denotes the total number of human agents in the set. Let $K = \{k_1, k_2, \dots, k_N\}$ represent the set of evaluation questions for knowledge capability. Every element in K has a multi-choice list of feedback/response options each having a corresponding score allocation based on expert judgment on the implications of the choice to an overall assurance of security of the ICSE. A response knowledge score allocation (x) with range of 1 to 5 is proposed. 1 implying a lower potential and 5 implying a higher potential of resistance to the prescribed security scenario. Each response/feedback to an element in K therefore has a value range: $\{x \mid 1 \leq x \leq 5\}$. The variety of feedbacks in K will yield varied occurrence of x during the data aggregation. Hence, it is necessary to obtain the cumulative knowledge capacity (CKC) for every $p \in P$ as the measure of the total quantitative security knowledge capability (Kc) scores of a single workforce member. This can be denoted using Equation (7-1).

$$Kc_p = CKC_p = \left[\sum_{x=1}^5 (x \cdot n_x) \right]_p, \forall p \in P \quad (7-1)$$

where n_x is the number of occurrences of respective response allocation x (i.e., 1-5)

Similarly, the cumulative skill capability (CSC) of $p \in P$ can also be derived from a set S of skills capability evaluation questions, using similar scheme and range for skill score (y) as in knowledge score (x), i.e. 1-5. The total quantitative skill capability (Sc) rating of a single workforce member p can be denoted using Equation (7-2).

$$Sc_p = CSC_p = \left[\sum_{y=1}^5 (y \cdot n_y) \right]_p, \forall p \in P \quad (7-2)$$

Equations (7-1) and (7-2) can be used to compute corresponding knowledge and skill capabilities of each workforce member p in the group P of the workforce under evaluation. The harmonisation of Kc and Sc values using a Geometric Mean (GM) function type shown in Equation (7-3), yields a Personalised Security Capability (PSC) metric. GM computational approach offers the strength of less submissiveness to the vast skewness influence of a very large values in a range of distribution (Manikandan, 2011), through normalising quantities to ensure that no singular measure (knowledge or skills) perpetually dominates the weighing of a final result. A set of PSCs will be generated, corresponding to all members, $p \in P$, and fed into the representation stage of the evaluation process.

$$PSC_p = (Kc_p \times Sc_p)^{1/2}, \forall p \in P \quad (7-3)$$

Since PSC_p represents the security capability of a specific user (workforce) within the ICSE, there exists a PSC_{min} and PSC_{max} that represent the minimum and maximum possible security capability scores respectively, which can be attributed to user p from evaluations. An incapability (vulnerability) potential of p can be inferred as the complement (fractional shortfall) $\overline{PSC_p}$ from the maximum security capability score. This can be quantitatively derived using Equation (7-4).

$$\overline{PSC_p} = PSC_{max} - PSC_p \quad (7-4)$$

$\overline{PSC_p}$ can be used to represent the security vulnerability of a user relative to prescribed security baseline requirements. Assuming that PSC_{max} is the security baseline, the workforce vulnerability impact magnitude (γ_p) can be derived as a proportion of the overall desirable capability score. This can be obtained using Equation (7-5). This variable can be used to represent the proportion of security severity that can be attributed to a specific user vulnerability.

$$\gamma_p = \frac{\overline{PSC_p}}{PSC_{max}} \quad (7-5)$$

It is assumed that the workforce vulnerability impacts are independent, i.e., a workforce member's vulnerability affects the system independently when exploited. Therefore, for a set P of users in an ICSE, the user (human-factor) security criticality index estimations of impact relate to the severity of inferred vulnerability as shown in Equation (7-6). This can

be used to reflect a user-oriented entity-level impact index, which can also imply a user-oriented risk impact h_p .

$$\gamma_p = h_p, \quad \forall p \in P \quad (7-6)$$

7.2.1.4 Representation

The visualisation of workforce security capacity can drive easy and speedy understanding of security perspectives, especially by top management and decision makers who are often less technically savvy. A capability placement chart (CPC), and a capability priority table (CPT) can be generated and used to represent the workforce security perspectives as shown in Figure 7-2 (a) and (b) respectively. A PSC score for an evaluated workforce member would fall between a minimum $\min(PSC)$ and maximum $\max(PSC)$ values, which respectively correspond to the least possible and highest possible harmonised capability scores that can be obtained from a security capability evaluation. Minimum and maximum values would typically depend on the number of questions, assessment or test cases in any evaluation category. As noted in 7.2.2.1.2, conventional information/cyber security risk level classifications of low, medium, and high (NIST, 2004, 2012) are used to categorise *PSC* scores, and further converted into corresponding priority ratings. A ratio 1:2:3 is used to implement the risk classifications. Fractional values: $1/3$, $2/3$, $3/3$, corresponding to respective ratios are used to derive the upper limit of each ratio. Each upper limit ratio also serves as the lower limit of the succeeding ratio in relations to the minimum and maximum scores.

For example, *High PSC* scores fall into ratio 3 with $3/3$ of the maximum score as upper limit. These indicate a relatively high harmonised *Knowledge (Kc)* and *Skills (Sc)* potentials, which suggest *high likelihoods* for appropriate security response and management of security events and incidents. This can be considered as a *Low Security Risk* potential, hence, a *Low Priority Rating*. Similarly, *Low PSC* scores fall into ratio 1 with $1/3$ of the maximum score as upper limit. Scores in this category indicate harmonised low *knowledge (Kc)* and *Skills (Sc)* potentials, suggesting *low likelihoods* for appropriate security response and management of events and incidents. This can also be considered as *High Security Risk* potentials, hence, a *High Priority Rating*. These three fractional upper limits (*Low, Moderate, and High*) are used to evaluate corresponding thresholds of

security capability depending on the number of questions or assessment cases in each group of measurement scale. An example implementation is shown in the section on validation. Table 7-1 presents a complete *capability-to-priority* classification accordingly.

Table 7-1: Capability-to-Priority Classifications

<i>PSC Scores</i>	<i>Ratio</i>	<i>Fractional Upper Limit</i>	<i>Capability Range</i>	<i>Risk Class.</i>	<i>Priority Rating</i>
Low (L)	1	$L_{up} = \left(\frac{1}{3}\right) \times \max(PSC)$	$\min(PSC) \leq PSC_p \leq L_{up}$	High	High
Moderate (M)	2	$M_{up} = \left(\frac{2}{3}\right) \times \max(PSC)$	$L_{up} < PSC_p \leq M_{up}$	Medium	Moderate
High (H)	3	$H_{up} = \left(\frac{3}{3}\right) \times \max(PSC) = \max(PSC)$	$M_{up} < PSC_p \leq \max(PSC)$	Low	Low

The capability placement chart portrays a scattered diagrammatic representation and placement of a set of *PSC* values between the potential minimum and maximum capability ratings for the workforce group. It depicts the status of personalised security capacity (*PSC*) for attribute workforce members.

A range of priorities assigned to each *PSC* indicates the degree of security attention that should be accorded to it in line with the capability-priority rating range outlined in Table 7-1. The priority order for security control effort is in the reverse order of security capacity. Workforce members who have high *PSC* values, suggestively retain a high degree of security awareness and practical proficiencies. This also suggests a high likelihood to respond appropriately to security incidents at least within the confines defined in the evaluation tool. *PSC* values that fall within the moderate capability ratings suggest a moderate priority rating. Those within the low capability rating suggest a high priority rating. The latter group particularly indicate low level security awareness and (or) skills, and thus require a higher need for security control measures that can improve their capacities to an acceptable level and within the prescription of the evaluation objectives.

The priority table presents *PSC* values alongside corresponding *Kc* and *Sc* values; helping to provide a holistic detail and comparative provisioning for the evaluation process. It provides a means of easily identifying both initial and successive weakest links in an array of *PSC* values. In the case where further or deeper insights are required about each metric or the harmonised format, capability priority table also provides a means for the optional analysis of derive measures using conventional statistical paradigms, such as measures

of central tendency and dispersion. It can also support test of hypothesis where necessary to compare or consolidate on findings and conclusion from initial evaluation results.

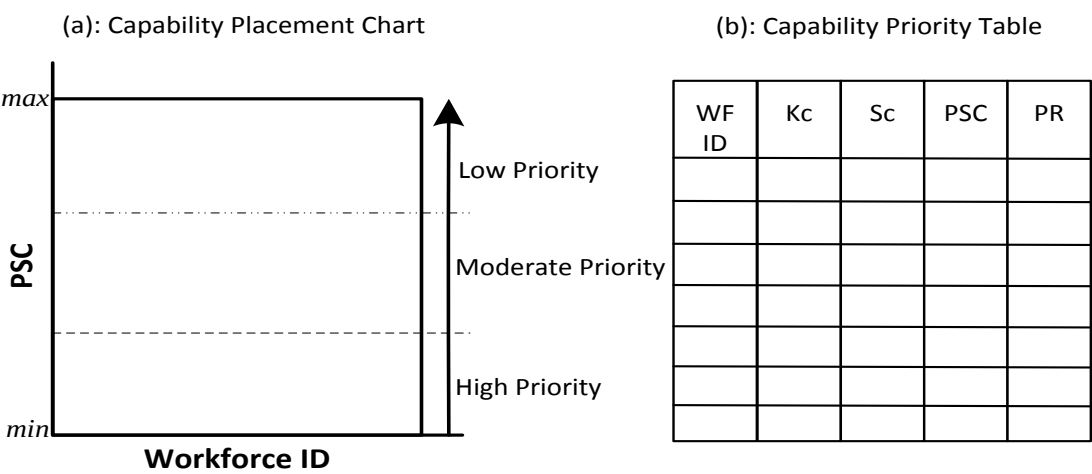


Figure 7-2: Capability Representation Formats

The interpretation of results contextualises the significances therein and attaches real and valuable meanings and implications to derived quantities and measures in both knowledge and skills evaluations in relations security threats, vulnerabilities, attacks capability gaps in the ICSE workforce. This makes it easy to identify high risks human agents (workforce), their risk levels and implications. It also supports understanding the capability requirements of high risk workforce members towards realising overall security of the ICSE.

7.2.1.5 Attribution

This involves the clear identification and binding of the weakest link attribute to a relative workforce member or group in line with a prescribed attribute function. In the approach proposed, the weakest link attribute implies the workforce or group with the least possible capability rating value and highest possible priority rating value in the capability priority table (CPT). The focus is typically on the *PSC* array, however, depending on the targeted objective, *Kc* and *Sc* arrays can also be used to attribute weakest link. Assuming *Z* represent the set of *PSC* values in the CPT, the weakest link (*WL*) attribute can be determined with simple mathematical minimum function using Equation (7-7).

$$WL = \min(Z) \tag{7-7}$$

The characterisation of weakest link also guides the process of determining the specific security vulnerability areas demonstrated by workforce members. It also supports determining potential control solutions as a means of remediating identified capability gaps. Results and inferences from the evaluation process give an understanding of the security incidence response and control measures that can be engaged. This is expected to incline towards security capability areas where workforce members demonstrate a low degree of knowledge and skills.

7.3 Scenario-Based Model Testing (Validation)

An online test-based questionnaire evaluation tool is adopted for scalable collection of evaluation data. The purpose was to assess if the proposed model can support efficient quantitative evaluations of ICSE workforce cyber security capability. The defined security objectives for this testing/assessment included: (i) evaluate the knowledge and skills security capability of the industrial workforce in relations to prescribed security guides, (ii) ascertain the weakest link from computed workforce personalised security capability values, and (iii) identify possible weak capability security themes and control areas in the workforce.

Online questionnaire approach was to efficiently reach large numbers of industrial workforce respondents while allowing for participation in the assessment from any geographical location. This way, the demand constraints for participation is reduced, and response rates likelihoods potentially increased. It was also meant to create more realistic unsupervised assessment scenarios that will yield realistic data collection. The assessment questionnaire was circulated via email links to forum members of the UK IoT Security Foundation. It was opened to those who shared concerns about human-factor security vulnerabilities, and who desired a way of determining specific security capabilities of respective workforce member within their industrial organisations, to support security decision-making. The emails contained brief description of the security capability evaluation questionnaire and its purpose.

7.3.1.1 Questionnaire Design

The questionnaire evaluation tool was developed using Qualtrics survey software for easy accessibility. The tool was administered via online medium to specific audiences, working directly or indirectly in an ICSE. The respondents assumed a sample industrial workforce

group, which may include general ICSE operation workforce personnel (control system operators, engineers, integrators, developers), enterprise and corporate business management personnel, and ICSE security specialists (security managers, analysts, architects, and incidence responders, etc.).

Direct response/feedback data were acquired from the sample respondents in relations to defined security requirements. These data were used to represent respondents' security capabilities and fed into the proposed capability evaluation model. These are in turn used to evaluate the varied security capacities of the respondents and determine the weakest link. In applying the model steps, it was hypothesised that (i) *the proposed approach can guide the identification of the security-oriented weakest link in industrial workforce*, (ii) *this approach can help identify predominant weak areas among a prescribed list of security control areas*; and (iii) *non-security-oriented work designations and experience will not allow the general operations workforce to make better judgement or demonstrate higher knowledge and skills capabilities than the Digital/Cyber Security designate professionals within an industry environment*.

In line with the model approach proposed, the evaluation was made following some recommended security control attributes and requirements for enabling cyber-attack defence, effective security within a digital system like ICSE, as contained in NIST SP 800-82 v2 (Stouffer *et al.*, 2015), and UK '10 steps to Cybersecurity' good practice guide (UK-Cabinet-Office, 2012). From these standards, specific security themes were deduced where human-factors can affect security states of an organisation, and where improved security capabilities can help avoid or control potential breaches. Two sets of evaluation questions - querying knowledge and skills (see Appendix C-4) were drawn using scenario-based formats to evaluate the level of respondents' capability from each of the security focus areas, and corresponding feedbacks to the questions were used to perform evaluations. Specific security themes considered include: *privacy and access control, system/network security monitoring, user awareness and training, secure configurations, removable media protection, personnel/credential security, home and mobile security, email security, malware protection, incident response, updates, and patch management*. These broad security themes also reflected similar security focus areas enumerated by Parson *et al* (2014) that provide valid themes for evaluating human aspect of information security.

Prior to issuing the evaluation questionnaire, appropriate research ethics approval was obtained (see Appendix C-3). It is also assumed that workforce members involved already have prior awareness and guidance on adherence to the prescribed security guides and essentials. Thus, the assessment was to determine the extent to which workforce members are holding up or improving on the security knowledge and skills already imparted by organisations. In structuring the questions, the design objectives included; to present seemingly realistic and familiar security scenarios to participants, and to proffer answer options that are seemingly realistic and familiar to the participants.

Each section of the questionnaire had 20 questions. Each question has 5 multiple optional answers with respective score allocations, corresponding to the perceived severity or implication of each answer to an overall cyber-attack susceptibility. The accompanying multi-choice answers is to represent varied security susceptibility levels (from high to low) for a respondent. The score allocation range is from 1 to 5, where an answer that implies a least security implication has a highest score of 5, while that with a highest implication has a least score of 1. A respondent's (knowledge or skills) capability is inferred from the selected answer to every question chosen by the respondent.

Response bias is a typical issue attributed to online surveys and questionnaires. It exemplifies a phenomenon where respondents provide answers they consider most acceptable, or expected from them, rather than a true expression of their personal views. To avert this, short and precise scenario-based questions with close-ended Likert-style answers were used to avoid potentials response biases that can emerge from too long and unclear questions. The interval scale (1-5) implied coding of responses was designed to help the acquisition of more accurate responses. The answer options were mostly structured into short and concise sentences to forestall the difficulty of evaluating their meanings by respondents. Response bias from incomplete set of answers was resolved through introducing answer options. For example, the answer option ***“Don’t Know”*** was used to cover other possible response options not included in the interval list, to avoid getting ‘false-positive’ answers due to the absence of desirable options. The complete questionnaire is presented in Appendix C-4.

7.3.1.2 Results and Analysis

Based on the described parameters of the scenario-based questionnaire, the summary of baseline definitions in line with earlier discussed capability classification ratios and groups is presented in Table 7-2, a minimum capability rating is feasible assuming that all responses for one workforce member have the same least allocation score of 1. A maximum capability rating is derivable if all the responses each have the highest allocation score of 5.

Table 7-2: Scenario Baseline Definitions

From Response Allocation Score, min = 20.00, and max = 100.00		
	Priority Class	Range
Capability Priority Rankings	<i>High Priority Range (h)</i>	$20.00 \leq h \leq 33.33$
	<i>Moderate Priority Range (m)</i>	$33.33 < m \leq 66.67$
	<i>Low Priority Range (l)</i>	$66.67 < l \leq 100.00$

A total of 37 industrial workforce respondents participated in the evaluation with everyone having a unique identifier. The feedback data were collected and used to compute the knowledge, skills, and personalised capabilities of corresponding workforce members using Equations (7-1), (7-2), and (7-3) respectively.

The ages of the respondents were grouped into three: Group 1 (20-35 years), Group 2 (36-50 years), and Group 1 (51-66 years). There were 18 respondents in Group 1, 18 in Group 2, and 1 respondent in Group 3. The average age of the respondents was 36. More than half of the respondents (workforce) were between ages 30 and 40. More precisely, 48.6% of the sample workforce were under 35 years of age, and over three quarters (91.9%) are under 45 years of age. These suggest that that most of workforce evaluated were mid-age range. There were more male (33) than female (4) respondents, which suggests that there are potentially eight times more male than female human workers in operational ICS domains. Similarly, there were more OT personnel (34) than IT personnel (3), which provides an indication that there are potentially more OT personnel than IT in the ICSE.

A summarised capability-priority classification of the results is presented in Table 7-3. Figure 7-3 presents the capability placement chart, Table 7-4 presents the capability priority table of the first 15 least capability (highest priority) ratings, while Figure 7-4 shows

a chart showing the *Kc*, *Sc*, and *PSC* representations of the 15 least capability (highest priority) Workforce members. The CPT for the 37 workforce is presented in Appendix B-28, while Appendix B-27 presents the CPC showing *Kc*, *Sc*, and *PSC* values of the 37 workforces. The complete workforce capability evaluation results are presented in Appendix A-15.

Initial validity and internal consistency reliability test of the measurement scale for knowledge capability (*Kc*) yielded Cronbach's $\alpha = 0.868$, which suggests a good measure of reliability. However, a good measure of reliability for the Skills capability (*Sc*) - Cronbach's $\alpha = 0.803$ was achieved in response to the need to remove the questions/assessment case Q35 item from the skills measurement scale. This item affected the reliability of the scale and needed to be excluded to achieve the minimum recommended level of reliability. The modified data was then used to analyse and derived further statistical insights. A Pearson's *r* data analysis revealed a low positive correlation, $r = 0.018$ between *PSC* and workforce *Age* with significantly high chances (0.914) of occurrence. This indicates a slight convergent validity and suggests that although workforce *PSC* and workforce *Age* were two separate constructs that measured distinct properties about the workforce, there existed high likelihood of slight increase in *PSC* as *Age* increases. This means that older industrial workforce personnel were more likely to be more knowledgeable and skilled in security response and incident management in the ICSE. Possible influences on this correlations relationship could be attributed to years of experience working within the ICS domain and the corresponding incidents that may be encountered, resolved, and learnt over the years. This outcome aligns with Beautelement *et al's* (2016) findings of a positive influence of *Age* on employee security maturity levels. Other measures that indicated slightly positive correlations to *PSC*, include: *Workforce Group* with $r = 0.130$, and *Capability Group* with $r = 0.416$. The likelihoods of occurrence for both measures were quite lower than that of *Age*. The results generally aligns with Wang's (Wang, 2013) conclusion of a positive correlations between directly evaluated (computational) and self-evaluated responses of workforce security evaluations. This suggest that measures derived from directly evaluating capabilities most often follows similar results pattern as measures from self-evaluated responses of the same workforce.

A. Direct Evaluation Results

Records indicated only 3 (8.1%) respondents from the '*security professional*' group, and 34 (91.9%) came from the '*general ICS operations group*'. This potentially reflects the typical rationing of workforce members in the industrial environment, where there is a greater proportion of the industrial workforce engaging in general process operations, and fewer workforce working for the maintenance of security. The result of the normalised individual security capability scoring of sampled respondents in line with the priority grouping ratios prescribed in the capability evaluation model, indicates that more than half of the respondents (23) representing 62.2% got categorised as '*low priority*' regarding their combined security knowledge and skills conforming to the prescribed security standards and best practices. 12 (32.4%) respondents fell onto the 'moderate priority', and 2 (5.4%) fell in the 'high priority' group. The latter group identifies the respondents with high-risk weaknesses in cyber security, and which needed a quite urgent attention in terms of education and security capacity-building. Contextually, the weakest link (WL) typically emerges from this group, and is attributed to the personnel with workforce ID **WF014** with an approximate harmonised capability rating *PSC* of 32.47 (*i.e.*, $WL = \min(Z) = \min(PSC_1 \dots PSC_n) = 32.47$). This workforce individual had a knowledge capability rating of 34, and a skill capability rating of 31.

Table 7-3: Capability-Priority Classification for Test Scenario

Cap.	Priority	Freq	Percent	Valid Percent	Cumm. Percent
Low	High	2	5.4	5.4	5.4
High	Low	23	62.2	62.2	67.6
Moderate	Moderate	12	32.4	32.4	100.0
	Total	37	100.0	100.0	

In assessing the areas of potential security weaknesses inherent the workforce evaluated, the cumulative capability rating (CCR) of each of the security questions was evaluated. The best-case scenario possible represents the maximum CCR ($CCR_{\max}$), with a value of 185, if the highest capability score of 5 is assigned by all workforce responses to a specific question. The CCR value for the specific question is the product of the uniform score and the number of respondents (*i.e.*, $5 \times 37 = 185$).

Table 7-4: Priority Ranking for the 15 workforce members with the least security capacities

WF ID	Kc	Sc	PSC	Priority Ratings
WF014	34	31	32.47	High
WF036	31	35	32.94	High
WF035	58	50	53.85	Moderate
WF023	64	48	55.43	Moderate
WF018	58	58	58.00	Moderate
WF037	60	60	60.00	Moderate
WF034	65	57	60.87	Moderate
WF019	66	57	61.34	Moderate
WF016	57	67	61.80	Moderate
WF032	71	54	61.92	Moderate
WF004	68	63	65.45	Moderate
WF028	70	62	65.88	Moderate
WF013	64	69	66.45	Moderate
WF002	59	75	66.52	Moderate
WF031	70	64	66.93	Low

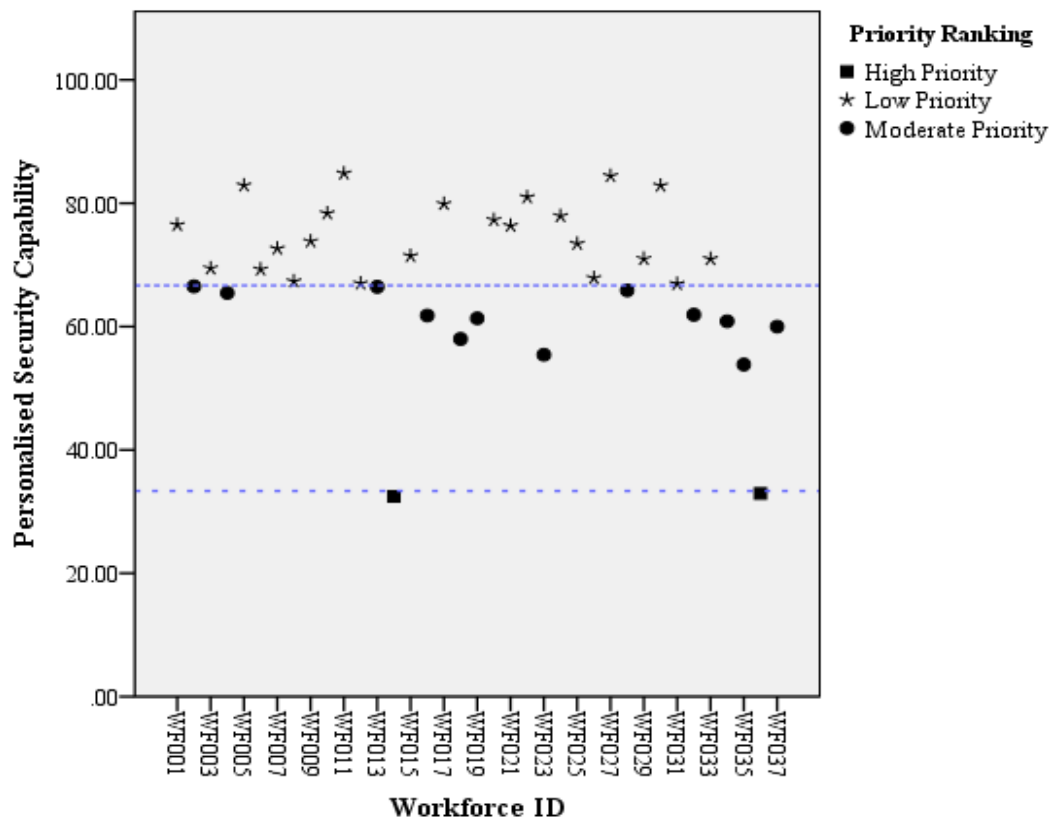


Figure 7-3: Workforce Capability Evaluation Placement Chart (37-User Classification)

The worst case possible represents the minimum CCR (CCRmin), which is 37 (i.e. representing the scenario where a uniform score of 1 is obtained by all responses to a specific question). The 15 least CCR values are presented in Figure 7-5. The records indicate that the first 3 least CCRs were from the skills evaluation questions, 10 (66.67%) of the least 15 CCRs compared came from the skills (Sc) evaluation questions (Table 7-5), and only 5 (33.33%) of the least 15 CCR values came from the knowledge (Kc) questions (Table 7-6).

Furthermore, the demographic details of WF014 workforce indicates an *age* of 29, no form of certification in information or cyber security, and self-rated assessment of security capability of 1, which corresponds to '*least capability*' rating. This suggests a relatively young age of work and perhaps experience, considering that three-quarters of the workforce were over 30 years. Self-rated assessment of security capability is likely to change as this personnel's age and experience in the ICSE environment increases.

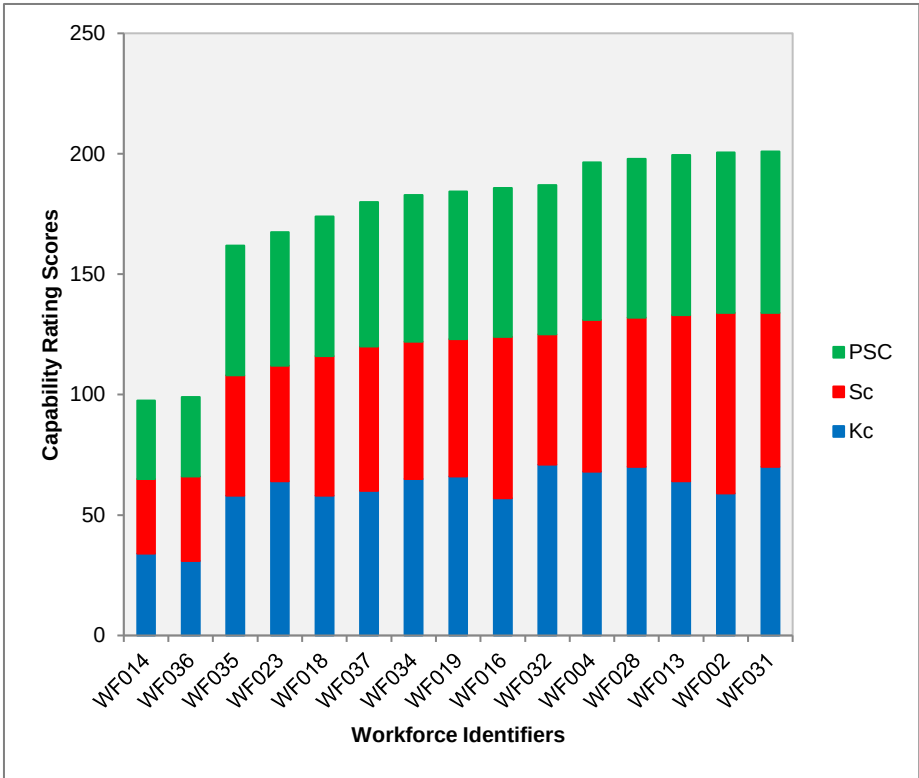


Figure 7-4: 15 Lowest Capability Workforce Representation (Kc, Sc, and PSC Contributions)

Table 7-5: The Least 10 Skills Cumulative Capability Ratings (CCR)

Skills Capability Weakness Areas	
Question_ID	Security Evaluation Areas
Q37	Credential (Password) Management Policies
Q27	Malware (Virus) Attack Response and Controls
Q23	Removable Media Protection
Q40	Malware (Virus) Attack detection
Q30	Credential Management and email security
Q22	Updates and patch management in ICS
Q28	Credential (password) security deployment
Q34	Email security (phishing) attack management
Q24	Incidence Response
Q29	Identity and Privacy Security

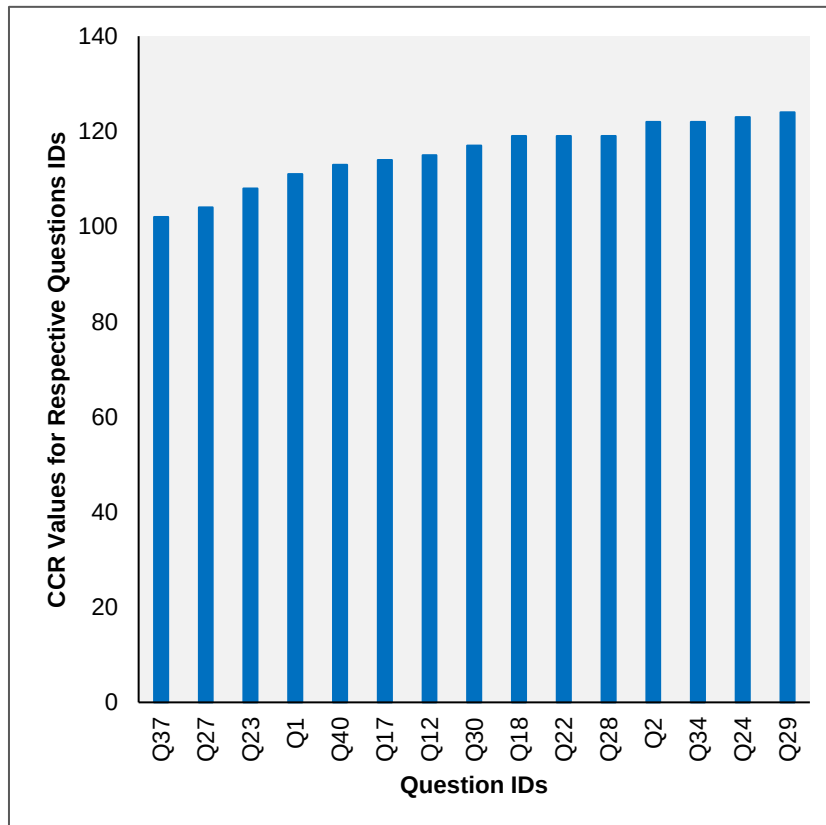


Figure 7-5: The Least 15 cumulative capability rating (CCR)

Table 7-6: The Least 5 Knowledge Cumulative Capability Ratings (CCR)

Knowledge Capability Weakness Areas	
<i>Question_ID</i>	<i>Security Evaluation Areas</i>
Q1	<i>Security Controls Availability</i>
Q17	<i>Proper Attribution of Security Responsibilities</i>
Q12	<i>Awareness of respective Roles in Security</i>
Q18	<i>Knowledge of Available security controls</i>
Q2	<i>Security Monitoring Frequency</i>

Other statistics results obtained include; the mean capability ratings for security knowledge and skills which are 69.43 and 62.97 respectively. The standard deviation for the security knowledge capability scores is 12.39, while that of the security skill capability score is 11.69. In relations to the security requirements adopted and evaluated, it implied that the workforce generally demonstrated higher theoretical knowledge than practical skills. It could also be because of the perceived lack of keenness for security skills in industrial workforce, who often assume that enforcing security should be solely left to the IT security specialists. The standard deviation values indicated that there were slightly more capability dispersions in security knowledge than security skill amongst the workforce. That is, most of the workforce had very closely the same level of practical skills in ICS security than they were closely levelled in awareness (knowledge) of ICS Security. The results generally suggest some measure of capability gaps amongst the workforce which may be influenced by their interactions, information sharing, personal capability enhancement engagements, and possibly organisational policies on security. Out of the 37 workforce members; 34 (91.9%) belonged to the General ICS operations class, 3 (8.1%) belong to ICS Security class. 36 (97.3%) did not have any security training or certificate, only 1 (2.7%) has a form of security training. This reflects the potential typical rationing of workforce members in the industrial environment. There is by far a greater proportion of the industrial workforce engaged with other industrial responsibilities other than the maintenance or assurance of security.

B. Self-Evaluation Results

In the aspect of self-evaluated capabilities, more than half (19 or 62.2%) rated themselves as '*low capability*' in ICS security proficiencies. This contrasts with the computed capability score class that showed 2 (5.4%) respondents under low capability. This suggest a

significant variation between individual and organisational views about security capability expectations, and further suggest that the respondents seem to have a higher capability rating disposition than that adopted by the organisation (used in the evaluation). To investigate and expound further on this capability variations, statistical hypothesis testing was applied with a Null assertion (A/H_0): *There is no difference in priority rating levels of the workforce amongst the self-rated security capability groups*. The self-rated security capability attributes used in the evaluation tool (questionnaire) included: 1= least capability, 2= low capability, 3 = moderate capability, 4 = high capability, and 5 = highest capability.

Table 7-7: Statistical Crosstab for Security Capability by Priority Ranking

Security Capability * Priority Ranking Crosstabulation						
			Priority Ranking			Total
			High Priority	Low Priority	Moderate Priority	
Security Capability	Least Capability	Count	2	1	1	4
		Expected Count	.2	2.5	1.3	4.0
	Low Capability	Count	0	12	7	19
		Expected Count	1.0	11.8	6.2	19.0
	Moderate Capability	Count	0	9	2	11
		Expected Count	.6	6.8	3.6	11.0
	Higher Capability	Count	0	1	2	3
		Expected Count	.2	1.9	1.0	3.0
Total		Count	2	23	12	37
		Expected Count	2.0	23.0	12.0	37.0

Table 7-8: Statistical Crosstab for Workforce Group by Priority Ranking

Workforce Group * Priority Ranking Crosstabulation						
			Priority Ranking			Total
			High Priority	Low Priority	Moderate Priority	
Workforce Group	General ICS Operations	Count	2	21	11	34
		Expected Count	1.8	21.1	11.0	34.0
	Security Professional	Count	0	2	1	3
		Expected Count	.2	1.9	1.0	3.0
Total		Count	2	23	12	37
		Expected Count	2.0	23.0	12.0	37.0

As observed in Table 7-7, 2 out of 37 workforce members are in the 'high priority' group. These same 2 workforces rated themselves as having 'least capability' in the self-evaluation section of data collection. Similarly, 23 of 37 workforce members are in 'low

priority', and of the 23, 9 self-rated themselves as having '*moderate capability*', 12 having '*low capability*', and 1 each having '*least*' and '*highest capabilities*'. Since this study focuses on the weakest link, focused analysis is undertaken on the '*least capability – high priority*' intersection. The row totals revealed 4 workforce members self-rated under least capability, the column total shows 2 workforce individuals on high priority ranking. A Pearson's chi-square (χ^2) value of 20.431 was obtained for these statistics with a 0.002 significance level. The crosstab statistics in Table 7-8 suggests that there is a rather large difference between the count and expected count in the sample if all self-rated least capability workforce reactively behaved in like manner of high priority as other grouped workforce members. However, a 0.002 significance level on the chi-square (χ^2) value implies; the possibility of rejecting the null hypothesis with only 0.2% chance of being wrong (i.e., less than 1 in 1000 chances of being wrong). The Null hypothesis could be rejected, and an alternative hypothesis (A/H_i): *There is a difference in priority rating levels of the workforce amongst the self-rated security capability groups* could be considered. It can thus be assumed that the workforce self-rated under least capability are more in high priority ranking group than in others. In the event of such variations, it becomes important to engage with, and determine the workforces' view about security capability expectations, and work towards updating and bringing-up the seemingly low-rated organisation security rating benchmark for personnel to a higher acceptable level.

Also, testing a second hypothesis (B/H_o) that: *There is no difference in priority ranking level between the general ICS operations and security professional workforce* yielded a Pearson's chi-square (χ^2) value of 0.188 with 0.910 significance level. The crosstab on Table 7-8 suggest very negligible difference between the real and expected priority ranking behaviours of the general ICS operations group. The security group also behaved in like manner. As expected, the results in the Table 7-8 crosstabs indicate that no security professional emerged in the high priority (low capability) group. Thus, a 0.910 significance suggests a 91% chance of being wrong if we reject the null hypothesis. This huge likelihood of being wrong informs our basis for not rejecting the null hypothesis that there is no difference in priority ranking level between the general ICS operations workforce and IT security professional workforce.

7.3.1.3 Discussion

The results suggest that irrespective of the number of high security-proficient cyber security professionals in the workforce members in an industrial control environment, the presence of other general operations ICSE workforce members with inherently low capabilities can decrease overall organisational human-factor security capacity. Circumstantially, this phenomenon supports that ICS workforce members with low security capability ratings are presumed to be more of the weak-links, since they pose more conspicuous targets of attacks.

If all the workforce evaluated all belong to the same organisation, then the workforce individual with identity number **WF014** represents the security capability of the organisation. Notwithstanding the security capability strengths of all other workforce members, the organisation may easily be compromised through the security and defence capability of **WF014** workforce individual. The organisation would be considered as weakly penetrable as the capability of ID **WF014**, who in this context and based on evaluation result is considered the weakest link. This represents the strawed portion of whatever security fences or capability enabled or imbibed in the entire workforce. Figuratively, a ‘*strawed*’ portion in a brick wall suggests the weakest and most vulnerable point of breach. This is a new approach to identifying security-oriented human weak links within an operational setting. Reactively or proactively raising the capability ratings of potential weakest link (via appropriate control measures) implies raising or strengthening organisational security capability. A low capability in both attributes suggests an even worse phenomenon. Basically, a workforce individual with high security knowledge and low security skill ratings indicate being abreast with evolving industrial cyber security landscape, but with a lack or gap in practical (responsive) proficiency to ensure security within his/her domain. A workforce in this state is nearly as weak as the workforce who is skilled in responding to primordial cyber security threats and attacks but does not constantly keep up with updates and changes in the security landscape. This is a possible scenario within ICS organisations that do not place adequate emphasis on human-factor cyber security controls and assurance.

A related phenomenon is seen to play out in the contrast between self-rated and computed capabilities of the workforce. The outcome indicate that more industrial workforce members were more aware of cyber-attack trends and issues than they have the skills to

respond appropriately to eventual incidences. Despite that, most of the workforce had not undergone any formal education and(or) training on security concepts, norms, and best practices, an information that would help them acquire appropriate knowledge and skills in the assurance of cyber security within their working environments. It suggests that while the organisation might feel comfortable about certain qualities and proficiency levels, personal workforce convictions might not represent the same opinion. This could result from a lack of updated details on emerging cyber security threat landscape on the part of the organisation, which is reflected in the test for seemingly old and widely known security capabilities. To avoid such precarious situations, organisations must continually keep abreast with the changing security trends, and updates evaluations in the light of those changes. Reviews and refinements of the security risk landscape should be continuous to capture any new or left out changes. Comparing the two results helps the balancing of security efforts between organisational view and workforce view about security capability.

The analysis of prime security-vulnerable areas reveals an interesting pattern inherent the workforce. The cumulative capability rating (CCR) of each of the security questions/parameters for all respondents can guide the identification of prime security knowledge and skill vulnerable areas. A lower CCR value indicate a gap or weakness in capability, and vice versa. It is therefore presumed that security weaknesses or vulnerabilities would typically widen or increase with decrease in CCR values. In the analysis of the least 15 CCR values selected, the first 3 least CCR values emerged from skill evaluation parameters, and 10 out of the least 15 CCR values also came from skill evaluation parameters. These suggest a potentially more incapacity and security gaps in skill than in knowledge of the workforce evaluated. This also presents a correlated perspective when compared with the overall knowledge and skill capability averages, which indicated a higher average security knowledge than security practical skill in the workforce.

Grouping the security areas of the least 10 skill CCRs into related family of security controls reveals that the workforce evaluated are basically practically weak in 4 broad areas of security control. These include: Credentials (Password) Management and Security, Malware (Virus) Detection and Management, Removable Media and Email Security, and Patch (update) management. The broad areas of theoretical knowledge weaknesses include; awareness of available security control measures, and knowledge

of self-duties and responsibilities towards overall system security. Most of the identified workforce vulnerability areas are in their weakest states in the security capability characterisation of the identified weakest link workforce individual (i.e., WF014). In this context, rather than engage all workforce members in practice training and awareness in all conceivable security areas, a strategic, cost, time, and resource-effective implementation of control measures for enhancing cyber security assurance would involve focussed awareness and practical training of selected purported weaker (more vulnerable) workforce members in the '*low capability*' areas enumerated. Security assurance improvement should involve inculcating security proficiencies (knowledge and skills) that are observed to be lacking, as it may be a waste of time, money, and other resource giving the workforce what they already have.

It is apparent that a single human-factor attribute such as security knowledge alone does not provide sufficient landscape and information to effectively characterise and represent a human agent's security aptitude. A better representation of security capability can be obtained by combining multiple human-factor attributes such as knowledge and skills as demonstrated in the results obtained. From the results, a low capability rating in any of knowledge or skills potentially upsets an eventual *PSC*, and by extension an organisational capability.

7.4 Chapter Summary

This chapter showed that the security capability and vulnerability of the human/people actors (workforce) is exigent and contribute to attaining an overall improved security in an ICSE. A single human-factor attribute alone provides an insufficient and skewed representation of a personnel's security rating. Combining multiple attributes such as security knowledge and security skills appear to provide results. These attributes both affect (can make or mar) overall ICSE security states. The presence of less knowledgeable and less skilled workforce member in relations to desired security requirements and policies significantly affects the security capabilities of an industrial organisation. The organisation's security capability is only as good as the capability of the least security capable workforce members. Being able to characterise each member's security capability in terms of knowledge and skills can support decision for a strategic, cost, time, and resource-effective security control implementation can be achieved.

8 SECURITY RISK REDUCTION THROUGH SECURITY RISK REDUCTION THROUGH CRITICAL IMPACT POINT ASSESSMENTPROCESS

8.1 Background

This attempts to build on prior similar theories and works (Markovic-Petrovic and Stojanovic, 2014; Woo and Kim, 2015; Cook *et al.*, 2017) which focus on technical risk assessment alone, and do not consider human-factor security assessments. These works provide the baseline for knowledge contribution explored in this study.

In this chapter, a structured security risk reduction framework is presented. The aim is to provide a risk assessment methodology that consider both technical and human-factor risk attributes, enabling the representation of a broader landscape of the ICSE. Risk assessment is explored in the context of vulnerability analysis and impact estimations. These can support better prioritisation of interventions based on the combined understanding of impact severities of technology and human agent vulnerabilities. This approach can be useful to industrial security auditors, managers, and system owners interested or engaging in security assessment of their operational environments.

8.2 Proposed Security Risk Reduction through Critical Impact Point Analysis (S2R-CIPA)

Cyber-attacks thrive on security vulnerabilities in technology and(or) people assets. As attacks become successful on ICSE assets, impacts are often enabled. Exploiting identified vulnerabilities in these assets can result in negative impacts that can greatly affect the ICSE. Often, these impacts are further propagated through the ICSE because of the system/network design interaction amongst the assets. For example, in social engineering attack modes, attackers often rely on the interaction between a user and a workstation (e.g. clicking on email hyperlinks or activating a program) to propagate their intended attacks and impacts through an operating environment. A significant control of impact would require building on earlier works (McQueen *et al.*, 2006) by considering both technology and human vulnerability risk reductions. This is achieved through a proposed Security Risk Reduction through Critical Impact Point Analysis (S2R-CIPA) process framework.

8.2.1 Overview of S2R-CIPA Process Plan

S2R-CIPA framework is proposed on the basis that security risk is related to the security impact caused by exploiting vulnerabilities in both technology and people elements. Reaching a risk level that is considered acceptable typically involves a process providing guide to the characterisation of vulnerabilities impacts and reducing the likelihoods of impacts by eliminating the vulnerabilities associated with high impacts. Traditional Hazard Analysis Critical Control Point (HACCP) (US-FDA, 2017) with its seven principles process structure; provides a suitable guiding process which can be adapted to the ICSE cyber security context. These principles follow an ordered consistent process whereby a system element is identified and characterised in terms of associated hazards that can ensue from its functionality or operation, the scale of tolerable impacts, and the control actions required guard against predicted impacts.

In this work, security risk is associated to the criticality indices of asset vulnerabilities where criticality is the magnitude of loss or impact that can occur from exploiting a vulnerability in relations to its likelihood (probability) (C'ardenas *et al.*, 2011). A structured, all-encompassing assessment of vulnerabilities can support a more precise and near-realistic estimation of failure and cascading impacts. This can also guide the adoption of appropriate security controls and risk mitigations. Adapting HACCP terminologies and process-flow structure into forming S2R-CIPA for ICSE offers an ideal by which appropriate inputs, outputs, and security response approaches can be engaged. Table 8.1 shows the translated HACCP principles to associated S2R-CIPA principles. The questions addressed by S2R-CIPA include:

- i. What Assets make up an Industrial Control System Environment?*
- ii. What security vulnerabilities exist in the assets of and ICSE?*
- iii. Which technology components retain the vulnerability if exploited can cause the highest impact on the ICSE?*
- iv. Which workforce member is most susceptible and more likely to fall victim to human-targeted attacks?*
- v. What security controls can be employed to resolve the most critical and impacting vulnerabilities in both technology and people components of the ICSE.*
- vi. What significant vulnerability and risk reductions can be achieved from applying identified security controls?*

8.2.2 S2R-CIPA Concept Descriptions

From Table 8-1, S2R-CIPA follows a seven-step process to guide both initiation and continuous adoption of ICSE security improvement; achieve through security risk reductions. The resulting outcomes can be used as basis for subsequent evaluations and control decision-making. At the core of S2R-CIPA include: (i) a variant of traditional HACCP tuned into a Critical Impact Point (CIP) vulnerability analysis process for the ICSE, and (ii) provisions for criticality index functions for evaluating individual-level, aggregate-level risks, and reduction values. These functions can derive their input data from standard *temporal* and *environmental* technology vulnerability (CVSS, NVD) scores, *functional dependency* mapping of vulnerability host assets, *people (workforce) vulnerability indices*, *probabilities of exploiting identified vulnerabilities* in the groups of ICSE assets. introducing human-factor security vulnerabilities and impacts assessment follows standard need and recommendations for achieving an organisation-wide security risk management.

Table 8-1: HACCP to S2R-CIPA Translation

HACCP Principles	S2R-CIPA Security Impact Steps
Principle 1: Perform a Hazard Analysis	Step1: Perform Asset (Technology and People) vulnerability Analysis
Principle 2: Identify Critical Control Points (CCPs) required to control identified hazards	Step 2: Identify Security Impact Points
Principle 3: Determine Critical Limits (CL) that must be met at each identified CCP	Step 3: Establish Critical Impact Point limits
Principles 4 and 5: Develop procedures to monitor CCPs. Establish Corrective Actions	Step 4: Implement Controls
	Step 5: Evaluate Reductions
Principle 6: Perform verifications procedures	Step 6: Periodic Verifications
Principle 7: Establish effective record-keeping systems	Step 7: Documentations

In the NIST SP 800-82 Rev 2 (Stouffer *et al.*, 2015), it is emphasised that the impacts on an ICS cannot be adequately determined by focusing only on technical parameters, as there are often non-technical factors that exist as weaknesses, and can enable or support the initiation or aggravation of security impacts. Including such non-technical factors can contribute to a better realistic view of ICSE security risks and help reduce negative impacts that an attack on ICSE might cause.

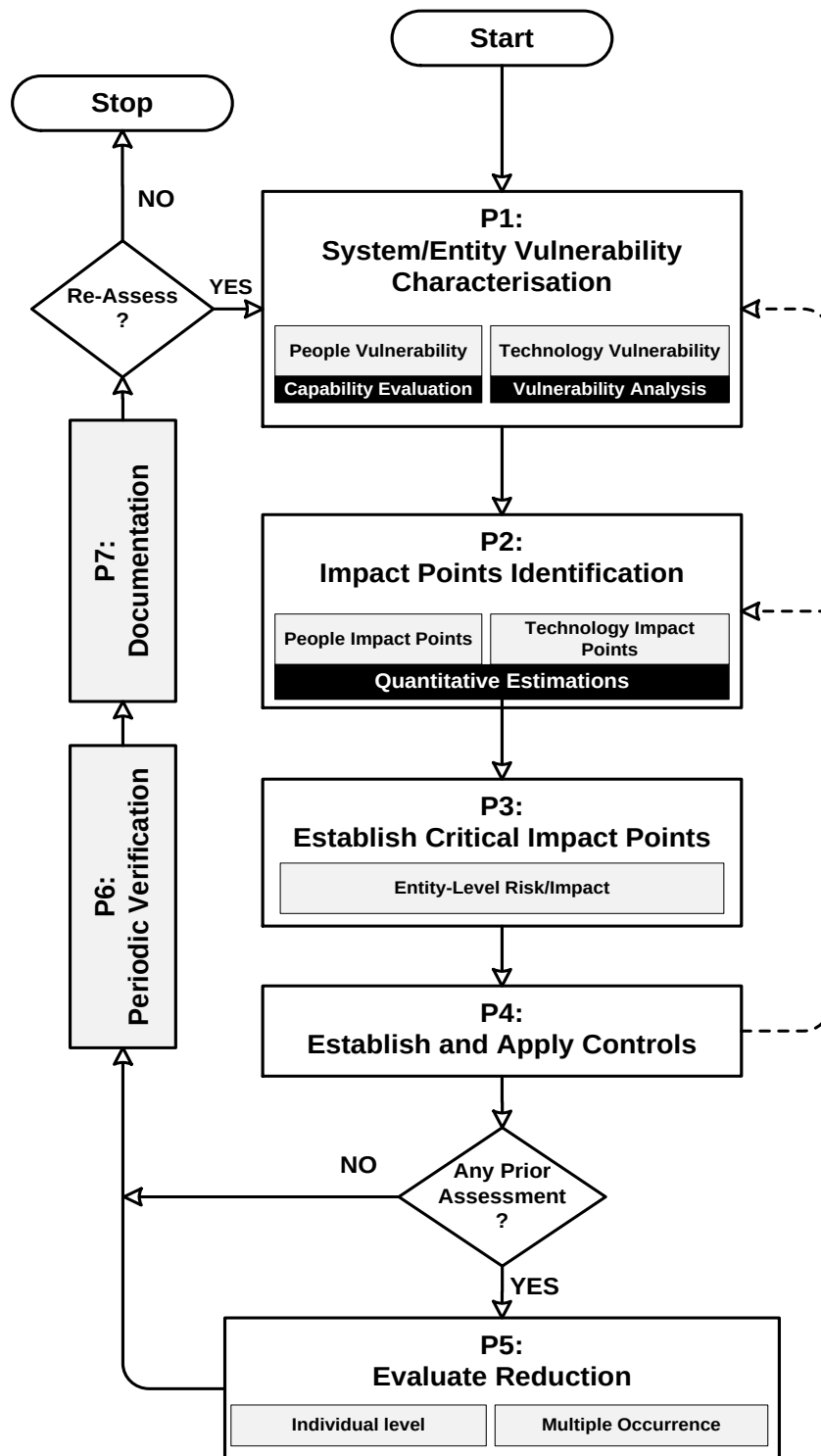


Figure 8-1: S2R-CIPA Flow Diagram

In ICSEs such as manufacturing, any stage of data exchange or electronic transactional process amongst operating assets (technology and human components) can have varied influential significances on the properties or outcomes of succeeding and(or) final processes, product(s), and service(s). This demonstrates a form of functional dependency

amongst the interacting components. An *impact point (IPt)* is used to refer to any asset (technology or user) whose malfunction or non-function can partially or wholly alter predefined process functionality, control, or monitoring, and resulting into a loss (operationally or financially). From a security point of view, the presence of vulnerabilities provides one way of identifying *IPts*. An *IPt* is considered 'critical' if the estimated criticality or risk of an associated vulnerability can significantly affect products, processes or services to an intolerable level. For example, if a technology asset s bears a vulnerability v_k , and v_k can be exploited by an attack a_k to effect changes in a defined process prc ($\Delta prc = prc_f - prc_i, f = final, i = initial$), such that Δprc results in an undesirable and intolerable state in the system, then, s is considered a '*critical impact point*'. A control action (CA) is used to define any activity or process that can either eliminate or reduce a known security vulnerability and its risk or prevent its further development. An *IPt*, which is critical to cyber security assurance is called a critical impact point (*CIPt*). It is necessary and crucial to precisely delineate value designation to *CIPt* to achieve an efficient and cost-effective deployment of security resources for controls and monitoring. While this might seem an overly complex task to achieve due to the occurrence of a variety of factors inherent an ICSE, such as temporal and environmental metric attributes, and architectural variations, which can cause possible misalignment of *CIPts* and ineffective outcomes, better *CIPt* assignments and security risk assessments can be achieved using a 'multi-attribute evaluation method' as a means of simplifying the security risk assessment process, while gaining wider characteristics view of the system under evaluation.

It is also possible to achieve extended classification of *CIPts* into *CIPt-1* and *CIPt-2*. *CIPt-1* is used to depict critical impact points whose corresponding security vulnerabilities and risks have '*assured security control(s)*'. Conversely, *CIPt-2* classes refer to critical impact points whose vulnerabilities and risks can only be minimised, and security controls cannot be utterly assured, i.e., '*non-assured security controls*'. However, since it is hardly feasible to achieve a state of absolute security or 'zero security risk' state, the emergence and stability of a *CIPt-1* is often unlikely. Instead, security trends, evolutions, and continuous developments in ICSE would be for continuous transition of *CIP-1s* to *CIPt-2s*, and sometimes vice versa. A *CIPt-U* class is also defined to account for unknown vulnerabilities and risks. Typically, a CA for this class would also be indeterminate, hence, *CIPt* values for such unknowns would usually be higher than the maximum known *CIPts*

in the evaluation system. In the S2R-CIPA process, technical vulnerability criticality index m_k and user (workforce) security vulnerability index m_p are used to represent impact point (*IPts*) for estimating corresponding risk reductions. *IPts* that go beyond a tolerable baseline definition are used to represent critical impact points (*CIPts*). This process helps to quantify and ascertain the most critical impact point, which can also be viewed as the weakest link. The S2R-CIPA steps are described in more details in the next sub-section.

8.2.3 S2R-CIPA Process-flow and Steps Descriptions

8.2.3.1 Step 1 - Perform Asset (Technology and People) Vulnerability Characterisation

The S2R-CIPA process starts with asset vulnerability analysis. Technology analysis is engaged where automated (public) vulnerability scanning tools/databases are used to determine the existence of vulnerabilities in technology assets and their severities analysed. The security severity ratings are then derived with respect to the uniqueness of each system and the continual changes that occur. This process can support the attainment of realistic measures of risk that represent a near-accurate security status of the technologies evaluated. Vulnerability analysis tools and repositories such as *NESSUS* (Tenable, 2017), *Nexpose* (Rapid7, 2017), and *SimaticScan* (Antrobus *et al.*, 2016) are examples of vulnerability databases and analysis engines that help with the enumeration of existing vulnerabilities in ICSE technology components. An example of the implementation of this process is demonstrated in chapter 6 section 6.4.

The human-factor (end-user) security vulnerability analysis methods that can help with the enumeration of potential security capability weaknesses (vulnerabilities) in ICSE human elements. For human-agent vulnerability analysis, a workforce cyber security capability evaluation method (Ani *et al.*, 2016) is adopted. A modified version of the concept and method is presented in chapter 7. The key requirement includes an ability to characterise security capability levels of individual end-users, derive quantitative values that correspond to specific capability levels, and infer or derive compliment attributes and values which may be considered as security vulnerability ratings. In the recommended approach in chapter 7, end-user security capability level may be derived from the quantitative evaluation of user-level security knowledge (K_c) and security skills (Sc) capabilities. The two metrics are combined to obtain an end-user's (p) personalised

security capability. Based on these, the vulnerability level of end-users (workforce set P) may be derived as the complement of respective end-user personalised security capabilities in relations to a defined baseline security capability requirement. This approach can support the process of analysing end-user security capability score of the ICSE workforce. A more precise estimation of environment-wide security vulnerability impacts and risk may be difficult to achieved without properly enumerating the constituting elements and their security vulnerabilities. Combining the two vulnerability aspects can provide a better estimate of an overall system security risk potential. Engaging security controls can affect the output of this process. This impact is represented by the dashed arrow lines coming into the P1 process block in Figure 8-1.

8.2.3.2 Step 2 - Identify Security Impact Points

This involves evaluating asset-level vulnerability potentials to cause negative or undesirable impacts within an ICSE. Recall that an *impact point (IPt)* refers to any technology or user that retains a vulnerability which if exploited can influence partial or complete disruption or destruction of industrial processes. Here, impact points evaluation is done quantitatively with the aim of attributing specific impacts in discrete or numerical terms to vulnerabilities in technology and people elements. All entity-vulnerabilities are then identified and characterised alongside their corresponding asset hosts. Impact point identification involves the estimation of criticality indices for all vulnerabilities identified.

The proposed Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model in Chapter 6 presents an approach for identifying impact points via a quantitative technical vulnerability impact analysis. The criticality index estimation subsection 6.3.1 describes a step-by-step approach for arriving at numerical impact values for discovered vulnerabilities. Impact values are derived considering; temporal and dynamic attributes of vulnerabilities from CVSS, probabilities of attack, and functional dependency attributes of vulnerability hosts (6.3.2). The evaluation process can help with the identification of technology vulnerabilities which when exploited can cause damaging impacts on the ICS domain. Similarly, the Workforce (Human) Security Capability Evaluations Model in Chapter 7 provides an approach for identifying potential impact points from human agent users' vulnerability-based impact analysis. The formulation subsection 7.2.1 describes how to infer corresponding vulnerability scores from derived workforce security capability scores. Corresponding equations (7-4 to 7-7) indicate how the vulnerability score of a

workforce member can be obtained considering both severity and probability attributes. The numeric outcome of the evaluation reflects a personalised impact index, which represents the potential impact scale of exploiting an associated user or workforce in the ICSE. Criticality indices values are derived to represent entity-level risks whereby higher criticality index values represent higher risk potentials. Typically, two sets of critical impacts indices: *G* and *H*, corresponding to technology and people risk potentials are generated. Each element within the two sets represents an impact point within the ICSE and is associated to the vulnerability inherent an asset. This step helps to guide the understanding of the possible impact and security risk attributed to all known vulnerabilities in the ICSE. The impact points can also be affected by existing or applied security controls. This is represented by the dashed arrow lines coming into the P1 process block in Figure 8-1.

8.2.3.3 Step 3 - Establish Critical Impact Point Limits

A critical impact point is a critical state for which security response/control is required to prevent or reduce security impacts to a tolerable or acceptable level. Recall that a critical impact point (*CIPs*) delineates a measure of damage that exceeds a predefined tolerable baseline. The tolerable baseline may not be static nor generic but can vary amongst organisations depending on operational objectives. A baseline definition would typically distinguish *IPts* from *CIPts*. The baseline limits are defined by system owners relative to the desired security functions and objectives of the assets, and the degree of failure of the functions and objectives. Hence, the baseline limits describe an organisation's conceived tolerable vulnerability, capability, or impact state.

Once the impact baseline limits have been established, the impact points are ordered according to the weight or index of impact from the highest to the least. Any *IPt* state, description or index that goes beyond the defined baseline limit is considered a *CIPt*. In a set of *CIPts* occurrences, the highest discrete *CIPt* indicates the vulnerability interaction points or potentials where the highest security impact and risk can occur. This should be accorded the topmost priority response for the two vulnerability classes of system elements. Engaging the above approach, the viewpoint is that both technology and people vulnerabilities are potential attack directions. Regardless of where the vulnerable element is within the system/network structure, their exploitations can cause a unique negative impact along the system chain from the point of initial influence. *CIPt* allows for identifying

the worst impacting entity vulnerabilities in the two asset groups to help in appropriately engaging strategic control interventions.

8.2.3.4 Step 4 - Implement Controls

When the impacts points of vulnerabilities, then security control are applied according to priorities. Security Controls provide safeguards that can help detect, reduce, or eliminate security impacts and risks. Essentially, for every vulnerability and associated *CIPt*, a control action (CA) is required to address the vulnerability state. It is important to identify a proper and deployable CA associated to a vulnerability or *CIPt*. CAs could include the implementation of single activities in technology and(or) people, or a collection of prioritised cyber security practices (technical and procedural) that culminate into a unified strength that add measures of security at the identified *CIPts*.

The dynamics in information/cyber security presupposes that there is hardly a widely acknowledged, single, static, and standard security control measure for ICSE security. Sustained effective security thrives better on continuous response to changing security landscape. Since ICSE comprise of legacy ICS devices, IT devices, and human users, security controls may involve aspects of policy, oversight supervisions, manual processes, actions by individuals, or automated mechanisms implemented by information systems, hardware and(or) software devices (Stouffer *et al.*, 2015).

Depending on the vulnerability and its potential impact, appropriate CAs may be adopted following two approaches: (1) Vulnerability analysis solution results – Vulnerability database tool (e.g. NESSUS), and (2) Recommended guidance from applicable standards – e.g. NIST SP 800-82 Rev 2 (Stouffer *et al.*, 2015), and NIST SP 800-53 *Appendix F* (NIST, 2013b). Vulnerability analysis solution results refer to the corresponding descriptive security control solution actions related to specific vulnerabilities discovered by vulnerability scanning and analysis tool, e.g. NESSUS. For example, the '*SNMP Agent Default Community Name (public)*' vulnerability on the testbed PLC has a suggested CA '*disable the SNMP service on the remote host if not in use*', or '*either filter incoming UDP packets going to the affected network port or change the default community string*'. Both CA descriptions offer some measure of enhanced security that addresses the vulnerability described. Recommended guidance from applicable standards like NIST SP 800-82 Rev 2 presents 18 family of security controls, which include: Access Control (AC), Awareness

and Training (AT), Audit and Accountability (AU), Security Assessment and Authorisation (CA), Contingency Planning (CP), Configuration Management (CM), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical and Environmental Protection (PE), Planning (PL), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), System and Information Integrity (SI), and Program Management (PM). One or more of these security control aspects may be engaged or combined to enable the suitable security capacity to be exerted on CIPTs. Each of these family of Security Controls describe a list of related security CAs and measure that may be adopted to address specific vulnerabilities and impacts. For example, Identification and Authentication control family includes potential CAs like password authentication, challenge/response authentication, physical token authentication, smart card authentication, and biometric authentication to be adoptable within ICSEs to enforce enhanced security.

The above control families and actions are based on the ISA-62443 (ISA99, no date) and the EPRI Report: SCADA system security guide (Mix, 2003). Other CAs related to privacy of Personally Identifiable Information (PII) are also described in *Appendix J* of NIST SP 800-53 Rev 4 (NIST, 2013b). Applying these security controls have been recorded to yield significant results (Pescatore, 2017). Depending on operational objectives and environment, other industrial security control guides may be adopted to ensure that the right measure of security improvements are achieved. Most often, a challenge encountered by industrial organisations involves adopting an appropriate set of security controls that can lessen or eliminate security *CIPTs* and risks. This becomes prominent in the bid to conform to standard security requirements and support realising operational and business objectives. The process described in this section can assist in resolving such challenge based on clear security risk information and predefined baseline security requirements.

8.2.3.5 Step 5 - Evaluate Reduction

To evaluate risk reduction, the approach used involves a time-dependent (current and enhanced) risk differentiation. At every point in evaluating security impacts, the records of current vulnerabilities and risk states are documented prior to applying controls. The enhanced states are also reviewed and documented to provide basis for comparisons. At the commencement of any security risk reduction activity in the ICSE (even in the case of

repetitive or multiple application of the process) the enhanced system risk attributes for a previous activity becomes the current risk attributes for a new activity. Thus, this enables a time-dependent differential evaluation of successive system interaction-level risk and the determination of the value of reduction. Essentially, a reduction is depicted by a positive outcome or value of the differential comparison of any successive (current and enhanced) security risk attributes relative to the occurrence of IPTs and CIPTs.

Assuming system security risk attribute is denoted by δ and t denotes the time for which δ is evaluated, δ_{t_1} will represent a current system risk outcome, and δ_{t_2} an enhanced system risk outcome. A generalised system risk reduction can be represented as a time-dependent change function $\Delta\delta$, and can be represented as $\Delta\delta = \delta_{t_2} - \delta_{t_1}$. The values for t_1 and t_2 is organisation-dependent, and may involve adhering to policy or standard guidelines, evolving trends, or incidence emergence that are internal or external to the organisation. Value ranges between t_1 and t_2 could be static or dynamic also depending on organisational requirements and objectives. Time-dependent risk change $\Delta\delta$ can be determined relative to security vulnerability occurrences, entity-level impacts, and aggregate-level evaluations. This approach helps to verify and validate genuine positive reductions of security risk within the ICSE. A positive reduction is not always absolute or certain since security and vulnerability landscapes are quite dynamic and uncontrollable. After a security risk change/reduction evaluation, it is possible to obtain negative reductions which imply a probable increase in risk. This should typically awake greater alertness and response to review current security standards and practices.

8.2.3.6 Step 6 - Periodic Security Verification of Controls

It is crucial to establish that applied methods, procedures, and tools for security monitoring and control action (CA) implementations at the *CIPTs* are adequate to control identified vulnerabilities, and as intended. Verification ensures that the control implementations deployed are in line with organisation's security policies, and emerging security solution trends. In the case of inconsistencies, the verification helps to determine specific areas of updates and improvements in response to security state-of-the-art. Responding to such improvement requirements may well include going through prior steps, which can pass as an enhance process. This process can be performed periodically by internal security auditors or external (third-party) auditors. Depending on the extent, cost implications, and

objectives, security verifications may not well be performed as often as the prior steps since the process can be quite extensive and expensive to accomplish.

8.2.3.7 Step 7: Documentations

This step emphasises the importance of historic data and record-keeping. Historic data about vulnerabilities, their likelihoods, impact and risk attributes, as well as control actions must be well documented. Records of verification procedures and outcomes must also be documented. This step can help demonstrate the effective application of the *CIPts*, and guide process of discovering any non-salient deviations or insights that can support better decision-making on the improvement of security. This step is always executed while engaging in other prior steps.

8.3 Evaluation: Case Study Results and Discussions

The proposed two-entity S2R-CIPA Process Plan was evaluated using the testbed system described in chapter 4. To recap, the testbed comprised of components integrated over an ethernet Local Area Network to mirror an industrial control system conveyors setup. The ICS conveyor system testbed components integrated include: PLC, extended I/O module, a HMI device, programming workstation computer, industrial ethernet switch, and conveyor belt equipment. The testbed also incorporated a six-member system management workforce consisting of postgraduate research students. These students presumably had some prior experience working in actual ICSEs.

The evaluation assumed the team of research students to constitute a small-scale ICSE workforce, they could manage and control the testbed process through interactions with the testbed technology assets. Together, the two asset groups: technology and people, were regarded as the small-scale ICS environment that was used to evaluate the risk reduction process plan. Similar exercise approaches have been used in the past for security evaluation of methods. ICSE testbed evaluation approach has been widely acknowledged and used (Beitel, Gertman and Plum, 2004; McQueen *et al.*, 2006; Markovic-Petrovic and Stojanovic, 2014) as a viable method for assessing security vulnerabilities. The steps of the proposed risk reduction process plan were followed while doing the evaluation of criticality impacts for both technology and people testbed assets. This was implemented in two stages corresponding to two different time-intervals: current (t_1) and enhanced (t_2) times. This is to reflect the time-dependent variations of risk levels

in the testbed environment and demonstrate the usability of the process plan for security risk reduction.

8.3.1 S2R-CIPA Steps 1, 2, and 3.

In *Step1: Assets Vulnerability Analysis*, NESSUS vulnerability scanning tool was used to scan the testbed network for vulnerabilities. A questionnaire workforce capability assessment tool was used to evaluate the vulnerabilities of the six-member workforce that were adopted as part of the testbed environment constituents. These were done in the context of security knowledge and security skills as described in chapter 7. Since there were available data from initial security capability evaluations of this workforce group from chapter 7, the data was used to represent the initial states (t_1) evaluations with no recourse to repeating the process.

In *Step 2: Impact Points (IPts) Identification*, quantitative attributes were determined for the identified security vulnerabilities. In technology assets, these referred to all severity score attributes of all the vulnerabilities identified during the vulnerability scanning stage. These were derived from the criticality impact computation of each vulnerability using dynamic severity scores, probability of attacks, and functional dependency attributes. In the people assets, it involved deriving the associated vulnerability attributes of each workforce member following the process of workforce cyber security capability evaluation. In both cases, numeric values were derived to represent the potential magnitude or impact of the vulnerabilities in the assets.

In *Step 3: Establishing Critical Impact Points (CIPTs)*, some baseline requirements were first set for both asset groups. Technology asset security baseline was set to Low. This relates to the outcome of severity ratings from vulnerability scanning. It implied the tolerable or acceptable severity level for technical vulnerabilities in the testbed environment. This was used to establish CIPTs for technical vulnerabilities. The CIPTs included any vulnerability whose severity rating was categorised as being above *low*, i.e., *medium*, *high*, and *critical* severities. For the workforce asset, the security baseline was set to low as well, so that any vulnerability rating that was above the low priority-ranking groups was considered a CIPT. This corresponds to the high security capability score grouping in workforce security evaluation. Critical Impact Points (CIPTs) were identified in relations to the prescribed security baselines in both asset groups.

8.3.2 S2R-CIPA Step 4

In Step 4: Implement Controls, the CIPts identified in step 3 were reviewed and available security control implementations were deployed to resolve some of the CIPts. For example, the PLC had a vulnerability 'V1' - "SNMP Agent Default Community Name (public)", which indicated a 'High' severity rating. This vulnerability could enable gaining of information about the PLC, sufficient to enable unauthorised changes to configurations in the PLC. NESSUS results also indicated that exploits for this vulnerability were available on the Metasploit Framework. Recommended correction approach for this vulnerability was followed. The default community string value for the SNMP Agent was changed from 'public' to 'private' through the device configurations 'totally integrated portal' (TIA). With the new settings, the SNMP Agent responds to the 'GETBulk' request with an error message, which eliminates the vulnerability at the enhanced state (t2) vulnerability scan of NESSUS. The extended I/O module also had vulnerability labelled 'V2', which was like the PLC vulnerability. The vulnerability had similar base severities, but different criticalities ratings. Control was established to address this vulnerability using similar approach as the PLC. Secure reconfiguration of the I/O module was done via the TIA portal settings platform. The vulnerability was also resolved. Appendix A-18 presents a summary of the security vulnerabilities discovered from NESSUS scan, and those that were resolved in the CIPt class as part of implementing step 4 of the S2R-CIPA risk reduction process plan.

For the people vulnerabilities, key vulnerability themes where the workforce expressed significant weaknesses in skills include: Credentials (Password) Management and Security, Malware (Virus) Detection and Management, Removable Media and Email Security, and Patch (update) management. Significant weak knowledge areas include; awareness of available security control measures, and knowledge of self-duties and responsibilities towards overall system security. To address the vulnerabilities in these areas, an informal security awareness in carried out in line with the UK "10 Steps to Cyber Security" (UK-Cabinet-Office, 2012) guide relative to the identified weak areas/themes. This was done from a capacity building point of view to help the workforce members understand better and improve in the areas identified. For example, in Removable Media Controls, the potentials for getting compromised via infected removal medias were outlined and explained. The security risk related to the lack of removable media control include: Loss of sensitive organisational information, introduction of malware into

organisation systems, and reputational damage. Specific risk control techniques such as: limiting the use of removal medias, scanning all media for malware on standalone system before connecting to organisation network, non-use of unofficial media, encrypting information held on media, and proper media reuse and disposal policies. The need to adopt proper media protection and management policies and adequate awareness of user responsibilities were discussed. In similar way, security risks and control techniques related to all other identified weak areas were discussed before the enhanced state evaluation of workforce capabilities was engaged. Appendix Table A-19 also presents the Impact Point enumerations of the current state evaluations based on the prescribed security baseline. Appendix A-20 presents the enhanced state enumeration after the application of control actions.

8.3.3 S2R-CIPA Step 5

In *Step 5: Evaluate Reduction*, the enhanced state evaluation process was initiated after step 4 of the current state process. This was necessary since there were no prior multi-state assessment and security data that could have been used for comparative analysis and the evaluation of reductions. To evaluate reduction, metric results derived from the enhanced state evaluation activities were contrasted against the metric results from the current state evaluation. The metrics data represented security states from which risk states can be derived. Appendix B-14 presents a summary of the evaluated testbed vulnerability reduction outcomes for both technology and people constituents.

For the technology group assets, there were reductions at component-level vulnerability occurrences. From Figure 8-2, there were reductions in the number of security vulnerabilities in most of the technology components at the enhanced evaluation stage, after associated controls were implemented. For example, the PLC had 1 vulnerability at the current t_1 state and 0 vulnerability at the enhanced t_2 state. The Control Workstation had 12 vulnerabilities at t_1 , and 8 vulnerabilities at t_2 . Similarly, the Ethernet switch had 6 vulnerabilities at t_1 and 4 vulnerabilities at t_2 . The differences in vulnerabilities between the two states t_1 and t_2 indicated the elimination of critical impacts that translate to the reduction of associated security risks.

From aggregate results perspectives in Figure 8-3, there was a 40% reduction in the total number of technology-based vulnerabilities. It is worth noting that the reduction of

vulnerabilities was on the bases of the ‘weakest-link-first’ approach. Hence, the 40% reduction included the potentially most impacting technology-based vulnerability based on derived vulnerability criticality impacts. In terms of the sum of criticality impacts at each evaluation stage, it is shown in Table 8-2 that there were reductions from 4.444 at t_1 to 2.493 at t_2 . This also corresponds to a 43.9% decrease in overall security criticality impacts. At t_1 , the weakest link was attributed to the control workstation component, which had a criticality impact of 0.403. However, at the enhanced state, the weakest link shifted to the ethernet switch with a lower impact criticality index of 0.364. This indicated weakest link reduction by 0.038 (9.5%). These statistics point to a reduction of potentially high-impacting security risks.

Table 8-2: Summarised Technology Risk Reductions

	Current (t ₁)		Enhanced (t ₂)	
Weakest link	Control Workstation	0.403	Ethernet Switch	0.364
Sum of Impact Criticalities for all devices	4.444		2.493	
Reduction	1.951 (43.91%)			

For the workforce group assets, reduction variations in individual vulnerability scores can be observed from Figure 8-4. Those that recorded significant reduction in vulnerabilities after control implementations were identified. These reductions translate to a corresponding improvement in security capabilities. For entity-level reductions, the number of impact points (*IPts*) remained steady for both current t_1 and enhanced t_2 states evaluations. Both states yielded 6 *IPts* each. The unchanged occurrence of *IPts* was because all the workforce members still expressed some measure of security susceptibilities. These vulnerabilities expressed some potentials that can still be exploited, thus, were considered impact points. However, for the *CIPts*, comparison against the defined baseline indicated a significant change. At the current t_1 , 3 (50%) of the workforce members were below the baseline. These had their security capability and vulnerability scores categorised in the ‘moderate’ groups. At the enhanced t_2 state, there was only 1 (16.7%) workforce member categorised under the ‘moderate’ capability and vulnerability groups. All the others were in the ‘high capability-low priority’ groups. This indicates an improvement in workforce security capabilities, also demonstrated by an increase in the number of ‘Non-*CIPts*’ from 3 to 5 (see Figure 8-5).

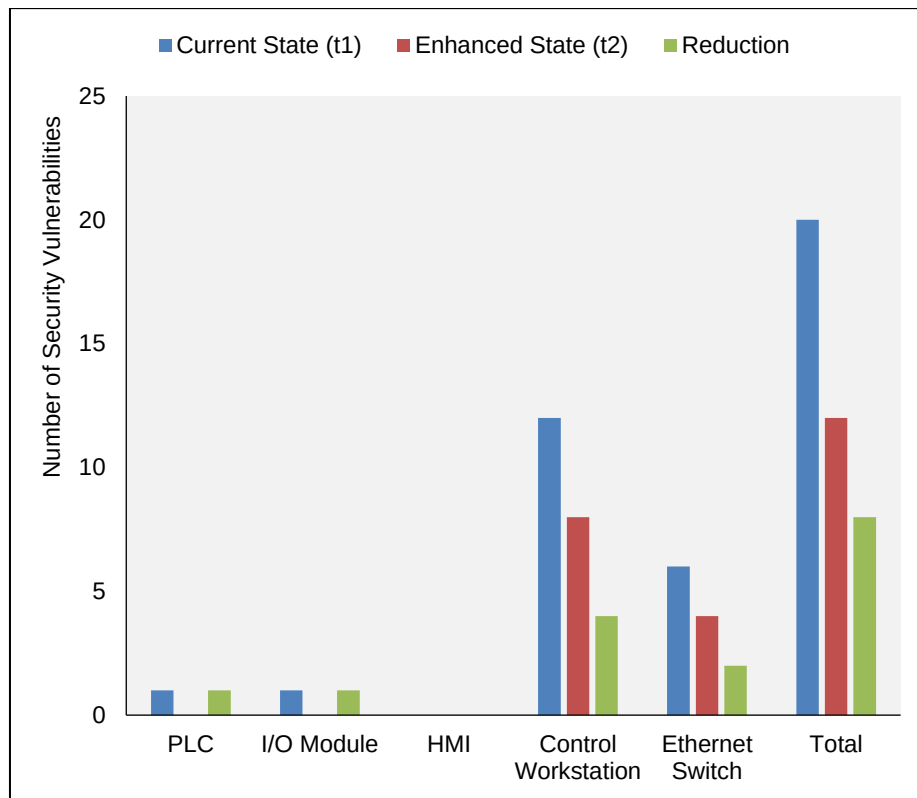


Figure 8-2: Component-Level Vulnerability Reductions

Workforce Individual-level reductions can also be observed as shown in Figure 3. For each of the workforce members, the associated vulnerability score in the enhanced state t_2 were lower than the score in the current state t_1 . This suggests that after the informal security awareness and training guide, all the workforce members improved in security capacity and correspondingly reduced their vulnerability levels. Comparing the weakest link attributes of the two evaluation states t_1 and t_2 , workforce with **ID WF03** was considered the weakest link with a vulnerability score criticality of 0.668 at the current state t_1 . At the enhanced state t_2 , the same workforce member (WF03) retained the weakest link position with a vulnerability score of 0.351. But as can be observed, the t_2 vulnerability score was much lower than the t_1 score. This represents a significant reduction in vulnerability potential of the workforce by 47.4% (0.316).

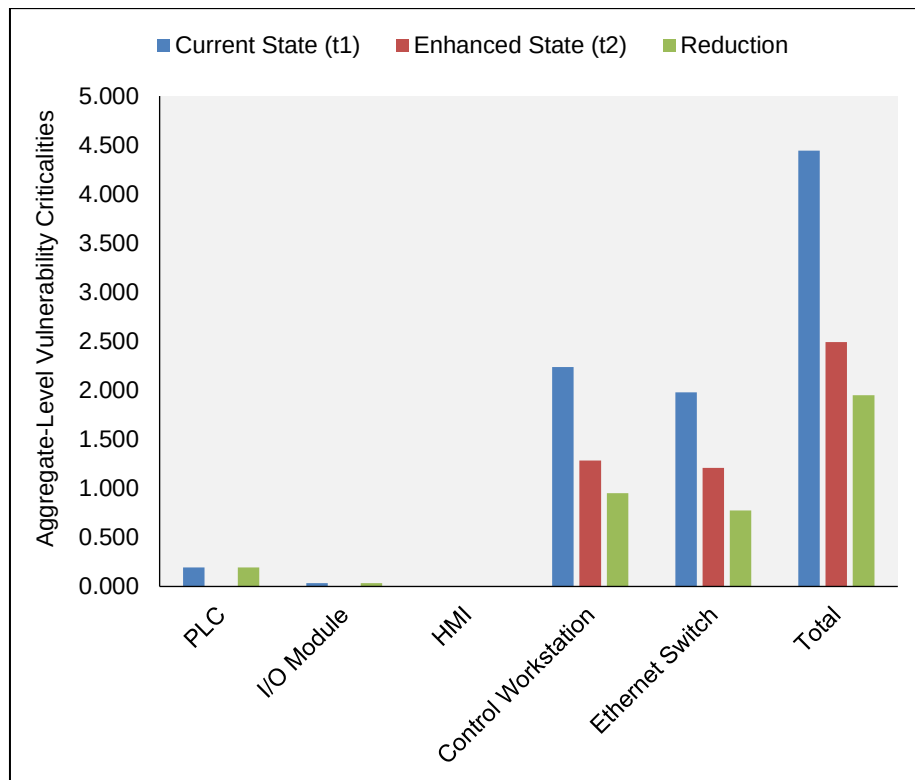


Figure 8-3: Aggregate-Level Vulnerability Criticality Reductions

8.3.4 S2R-CIPA Steps 6 and 7

Step 6 and Step 7 (Periodic Verification of Controls and Documentation) required that the security controls deployed to resolve the vulnerabilities in the PLC, Extended I/O Module, Control Workstation, and Ethernet Switches, all conformed with updated security trends. Since, the verification was done at about same time with prior processes, no inconsistencies were observed. The adopted security controls were still the recommended solutions as at when the verification was done, hence, there were no significant areas of updates required.

Step 7 involved the proper documentation of all the data obtained from the evaluation process. These included, current and enhanced states vulnerability records, their criticality attributes, the controls deployed, and the comparative analysis results of reductions. In the case of a future security evaluation. The results of the enhanced state evaluation would be used as the basis for comparative and risk reductions analysis.

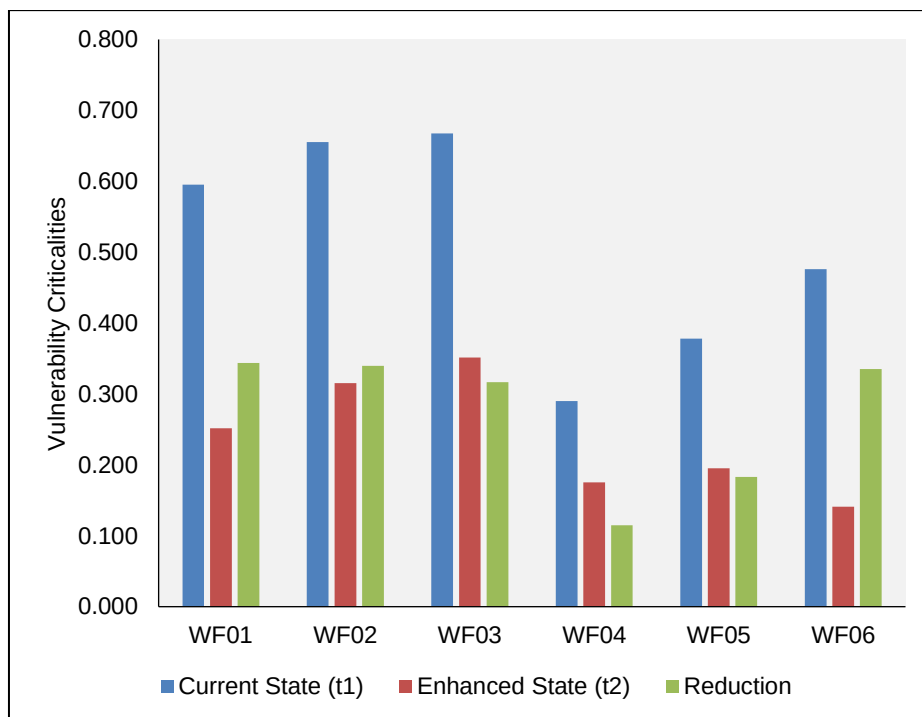


Figure 8-4: Workforce Entity-Level Vulnerability Reduction

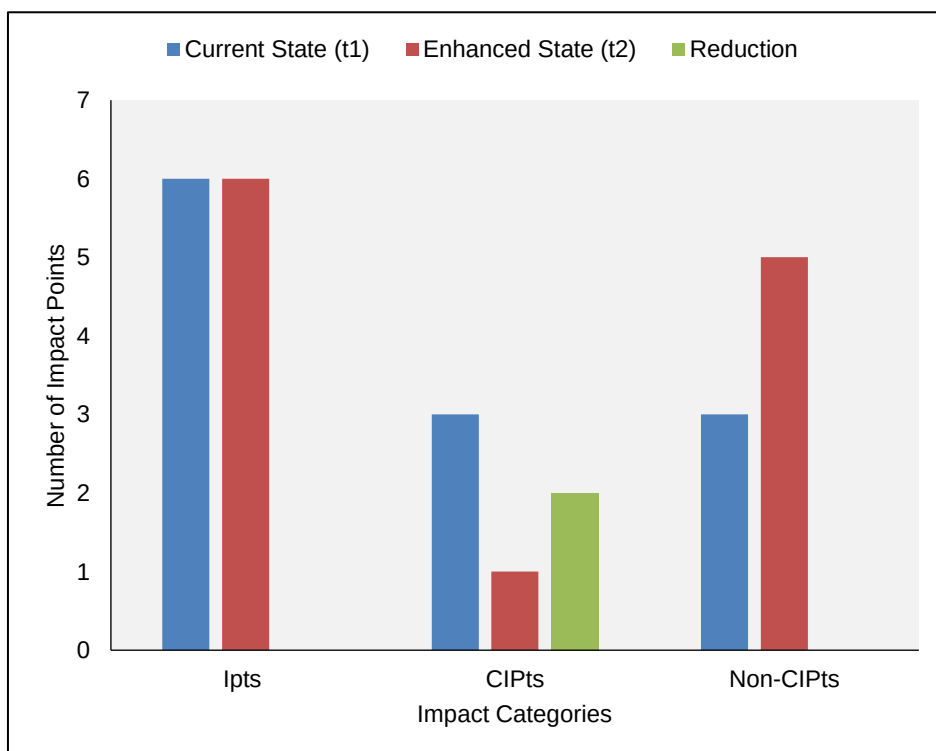


Figure 8-5: Workforce Aggregate-Level Vulnerability Reductions

8.3.5 Analysis and Summary

The results from evaluating security risk reduction suggests that reduction can be achieved from both technology and people (workforce) perspectives, and at different levels. Following the open-nearly closed-closed model, it can be observed that significant security reductions were achieved at both component-level and aggregate-levels for the technology entities. After system security enhancement that was guided by the prioritisation of criticality impact, some initially open attack entity doors were closed in the PLC and extended I/O module of the testbed. In the Control Workstation, 4 attack entry doors including the most impacting were closed. This left fewer than initial less-impacting attack entry doors open.

From the people perspective, the 'nearly closed' attribute applied since each of the workforce was seen to improve in security capability. However, the vulnerability capacity of each workforce did not close-up completely. This indicates a 'nearly close' door characteristic since there were still partial opening for possible exploitations. Viewing risk reductions through the '*open-nearly closed-closed*' viewpoint presents some advantages. If an attacker's resource investment and target is solely pointing towards specific vulnerabilities, closing-up such target vulnerabilities hardens if not make impossible the process of an attack. McQueen et al, (2006) considers the approach to be seemingly optimistic in nature since it adopts a linear relationship between vulnerability occurrences that overlooks other crucial factors such as the exploit complexity of vulnerabilities, and the attacker type. In this work, we believe that these factors have been considerably addressed by the use of dynamic temporal and environmental metrics attributes, rather than the usual base score metric used by McQueen et al, (2006).

In summary, of the five questions expected to be addressed by the S2R-CIPA process plan, Table 8-3 is used to describe where these questions were addressed by the various

components of S2R-CIPA. How the questions are addressed are also described to provide a clear ICSE security risk reduction process plan.

Table 8-3: S2R-CIPA Mapping to Objective Questions

Questions	Process Plan Component	Approach for Questions Resolutions
(1) What security vulnerabilities exist in the assets of an ICSE?	Step1: Perform Asset (Technology and People) vulnerability Analysis	The use of vulnerability databases for scanning networks supports the process of identifying security vulnerabilities in technology assets Workforce Security Capability evaluation can also be used to derived vulnerabilities in humans within the ICSE
(2) Which technology components retain the vulnerability if exploited can cause the highest impact on the ICSE?	Step 2: Identify Security Impact Points	Establishing security baselines for the criticalities in both technology and people entities can support the identification of the impacting vulnerabilities. The highest impacting vulnerabilities and components can then be derived while comparing each impacting vulnerability against the baseline.
(3) Which workforce member is most susceptible and more likely to fall victim to human-targeted attacks?	Step 3: Establish Critical Impact Point limits	
(4) What security controls can be employed to resolve the most critical and impacting vulnerabilities in both technology and people components of the ICSE.	Step 4: Implement Controls	Following standard security guidelines and best practices for system/component hardening and defence-in-depth targeted the highest impacting vulnerabilities can support improved security.
(5) What significant vulnerability and risk reductions can be achieved from applying identified security controls?	Step 5: Evaluate Reductions	Obtaining the Vulnerability and Impact changes between the current and enhanced state evaluations of Impact and Critical Impact Points supports the determination of risk reductions

9 DISCUSSIONS AND CONCLUSIONS

9.1 Appraising ICSE Cyber Security Landscape

One of the findings from the literature review on security control applications in the ICSE involves a false sense of security often presumed by the operational technology (OT) workforce. The results suggest that industrial workforce often think they cannot be victims of cyber-attacks since they do not directly operate on the internet/cyber domain. This group are also often unaware of the various ways cyber-attacks can be initiated against them or the infrastructure they operate.

Another significant finding from the literature is the misplacement or lack of understanding of the attack direction changes within the ICSE following incident records. This may have been the reason most available security solutions were perceived to be non-holistic in covering all aspects and dimensions of security with the ICSE. A trend analysis of attack patterns to security control methods showed some variations. While defensive security direction inclined towards consolidating technology-oriented patterns and solutions to enhance security, attack direction inclined more towards exploiting people (human-factor) patterns and incapability to sabotage security. Security solutions in this direction would be considered timely and valuable. Understanding and responding to this disparity and need can make the difference between an effective security solution and a less effective one.

The demonstration of cyber-attack on ICSE network using the testbed approach indicates that the range of cyber security threats and vulnerabilities span both IT and OT infrastructures, and can easily be compromised. It further demonstrated the need for adequate ICS-specific security awareness and control improvement through varied aspects relating to criticality and impact analysis that can support effective prioritisation of control efforts and implementations to achieve a possible optimum security outcome.

9.1.1 Security Metrics Framework Development

Following the analysis of research findings, a novel Operational Security Metrics Generation framework for ICSE was proposed. The framework provides a unified and purposeful guide for generating security metric quantities in relations to specific security requirements.

that can be applied when measuring certain security perspectives within the ICSE. The framework offers a conceptual and step-wise outline for selecting appropriate security metrics and their associated specification profiles to support effective and more relevant security evaluations. Building on the limitation of similar existing methods, the framework offers improvements in the aspect of adaptability and repeatability.

The framework had three main phases: target definitions, objective definition, and metrics synthesis. Target definition involves the outline of security dimensions (capability or vulnerability), ICSE segment of interest, and constituent. Objective definition involves identifying desirable security requirements, together with a contextual description. This phase enables an understanding of the security characteristics of the system to be measured and contributes to providing a knowledge-base for the varied security objectives. Metrics-synthesis involves the process of outlining the control capacity directions that can be adopted (proactive, reactive, or both), indication of how certain security metric values can be derived (measurable or computable) and the metric specification profile that provide a description of the metric characteristics.

An instance of the application of the framework was demonstrated using the people (human) entity dimension. This served as a first-level (initial) validation of the framework from a practical formative decomposition approach applied on a case study scenario. The case study was used to demonstrate how the proposed framework can be applied to a real scenario in the industrial environment to generate security metric quantities. Thus, the human security capability scenario emphasised an example of the framework's generalisability, and aptitude to handle and direct the development of security metrics. To further consolidate on the validity of the proposed framework, a second-level validation was conducted using expert elicitation through an online questionnaire (survey) technique. This approach was used to gain expert opinions on the framework's structure, its suitability to meet the requirements of supporting security metrics development, and validity of its output. The results of the two validation approaches of the proposed framework showed that the framework was supportive of the target objective for its development. Also, the results from the validation were used to drive improvements on the framework. These guided the identification of effectiveness and limitations of the framework.

9.1.2 Technical Vulnerability Impact Analysis

Based on the analysis of research gaps, and in relations to existing works, a novel probabilistic Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model is presented. MAVCA provides a means for obtaining improved insight into vulnerability impacts and how they can cascade through an ICSE network domain. This can be achieved by considering multiple dynamic attributes of technology-based vulnerabilities, and their host environments (components and systems). The improved insights are then used to proffer solutions in the form of improved vulnerability resolution approaches built on an improved estimation of security impacts associated to vulnerabilities with an ICSE network.

MAVCA provides value to security analysts and system owners by proffering basis for prioritising security controls and responses based on estimated magnitudes of severity impacts. This can be achieved through a step-by-step approach for enumerating vulnerability exploit and impact potentials.

CVSS temporal attributes of vulnerabilities and their respective probabilities of exploitation constitute valuable input variables in the evaluation of vulnerability exploit potentials. CVSS environmental attributes of vulnerabilities and the functional dependency attributes of vulnerability host components also constituted valuable input variables in the evaluation of vulnerability impact potentials. Exploit and impact potentials are combined to achieve criticality indices associated to vulnerabilities within the ICSE network. The criticality index attribute indicates the potential cascading functional impacts that may occur when an associated vulnerability is successfully exploited.

A probabilistic approach was used to evaluate the criticality index since it was impractical to accurately determine the impact of attacks. Accuracy in this regard may only be possible if several other factors within and outside the network environment are considered. The criticality index represents a measure of likelihood for an estimated impact scale considering factors from the user/defender point of view while assuming the worst-case scenario from the attacker's perspective. Understanding the cascading negative impact magnitudes associated to all vulnerabilities, especially those classified as 'critical' from traditional CVSS ratings, can support the process of identifying the most critical vulnerability, host component, and system. It can also provide basis for prioritising

security control and response measures to achieve an optimum security outcome each time security control/response becomes necessary and is engaged.

The MAVCA evaluation model was validated on a testbed environment, to demonstrate the model's usability and workability within an industrial network use case. Applications underscore the identification of technical vulnerabilities on the network, characterisation of vulnerability impact magnitudes, identification of the weakest link, and setting priority for security controls and responses. The accuracy and validity of results depended on the credibility of the testbed as representative of a real ICS network. This credibility is satisfied using minimum acceptable design requirements from standards. The results of the validation also revealed areas of improvements as well as the limitation of the model. These indicated prospective areas where further research can be engaged.

9.1.3 Human (Workforce) Cyber Security Capability and Vulnerability Evaluation

Following the analysis of research findings, a novel quantitative human-factor cyber security capability and vulnerability evaluation model was proposed. In the ICSE, learning the capability states of the human constituents (workforce) to appropriately recognise and respond to cyber intrusion events within the ICS environment enables insights that can support effective security improvement efforts.

The proposed capability evaluation approach was modelled based on two human-factor security attributes: security knowledge and security skills. The model was aimed at providing an approach to quantitatively evaluate and determine the security-complaint weak-links amongst a group of human industrial workforce. The model also helps to identify the security capability and vulnerability domain areas where a majority of the workforce express weaknesses. This can help to direct strengthened actions on a first-line defence against human-targeted security threats and breaches in the ICSE.

The proposed model offered a five-step evaluation process: definition, data collection, formulation, representation, and attribution. At the definition stage, guided security standards and best practices are defined, as well as; security baseline requirements for security knowledge, skills, and personalised capabilities. At the data collection stage, a test-style questionnaire tool is used to gather information from industrial workforce about their security knowledge and skills in relations to defined baseline requirements. At the

formulation stage, the results/data from the definition and data collection stages are fed as inputs into the model evaluation functions to derive knowledge, skills, and personalised security capabilities and vulnerabilities measures. This represents a gauge of the security levels of the workforce. At the representation stage, charts and tabular structures are used to visualise and represent the capabilities and vulnerabilities derived from the prior stage. The identification of the weakest link capability and the adoption of appropriate remediation measures are accomplished at the attribution stage. Depending on the objectives, appropriate reviews and repetition of the process may be engaged to optimise security capacity levels while reducing vulnerability levels in the industrial workforce.

The proposed human-factor (workforce) security evaluation model was validated using an assumed real-life case environment involving actual industrial environment workers from different industrial sectors. A test-based online questionnaire-style approach was used to gather data from the workforce respondents about their cyber security knowledge and skills. The UK 10 Steps to Cyber Security guide was used as a guiding standard, because it offered a general security requirement that can support the improvement of cyber security within organisations, a knowledge of which was necessary for organisation personnel. The result of the workforce evaluation showed the model's usefulness to achieve workforce security capability evaluation. The result was presented as part of a paper in a conference, where expert views were received. Although the model was generally judged as usable, the comments from security experts revealed the extent of effectiveness and limitation of the model. Some of the limitations were addressed through further work and improvements on the proposed model.

9.1.4 Security Risk Reduction through Vulnerability Analysis and Critical Impact Point Process

Based on the analysis of research gaps from literature, and in relations to existing works, a Security Risk Reduction through Critical Impact Point Assessment (S2R-CIPA) model was proposed. The case for this type of approach was made following evolving security trends where threats now target and exploit security vulnerabilities in both technical and human entities within the ICSE. The need for security assessment to include both technical and human-factors has become more relevant. S2R-CIPA provides a holistic approach for reducing security risks in the ICSE by ensuring that both technical and human-factor vulnerability and security impact points are considered in security analysis

procedure. This can support the early or proactive employment of appropriate security controls and countermeasures to forestall future occurrences or reduce negative impacts.

The proposed S2R-CIPA model assumes that security risk level is proportionate to security vulnerabilities and their impacts on overall system functionality. These impacts are often aggravated by the interactions between technologies and human operators that constitute the ICSE. On the other hand, security risks also relate to the criticality levels of the vulnerabilities that exist in both technologies and human entities. Thus, the S2R-CIPA process plan provides a flow guide for evaluating the attractiveness and criticality impact of ICSE assets (technologies and humans). These assets function and interact to enable industrial operations in the ICSE.

The dataset used for describing the nature of security vulnerabilities and risk reductions were derived from a testbed and theoretical scenarios that were structured to include both technology and people entities. Computational approaches were used to derive the potential impact criticalities associated to vulnerabilities in the two-entity groups, and the outcomes were used to derive linear-oriented security risk reductions. The process of vulnerability identification, criticality evaluation, and risk reduction were built upon widely recommended approaches and guidelines in vulnerability analysis, security impact analysis, dependency analysis, and risk assessment. These drive risk reductions in the ICSE assets; technology and process that retained highly impacting vulnerabilities, and whose exploitation can potentially cause negative consequences that are critical to the functions of other components and the ICSE at large. These are used to infer reduction rates in security risks attributed to the vulnerabilities in identified assets following the two-stage process flow and comparative analysis.

Numerical results obtained suggest that security risks are associated to attributes of asset entities that function in an ICSE. The relationship between security risks and functional entity attributes is quite coherent to normal security predisposition, and emphasises the types of control strategy, action, and implementations required to effectively reduce security risks to as much as possible. For example, the process plan demonstrates the dynamic nature of technology security vulnerabilities in response to difference or changes in the host evaluation environment. This, combined with the variations in functional dependencies of each technology component hosting a vulnerability, further influences the security impact criticalities that can ensue. The impact criticalities may only change

positively if consistent efforts are engaged and maintained to harden security in components through reconfigurations, installation of security updates and patches, or disabling unused services, etc., once new vulnerabilities are discovered. Further positive changes in impact criticalities can be enabled by multiple evaluation and control implementations. A reduction in component-level or aggregate-level criticality impacts can be considered as reductions in security risks associated to the respective vulnerabilities. Similarly, the process plan also demonstrates the dynamic nature of workforce security vulnerabilities, and how this translates to security risks. Vulnerabilities in the workforce suggest limitations in security knowledge and skills for effective response to security scenarios. These can be reduced following systematic identification of potential weak links whose vulnerability levels exceed the tolerable baseline and identifying the prominent weak areas/themes. Security vulnerability blocking activities can then be engaged targeting the less most vulnerable workforce, and the weak security areas.

In general, S2R-CIPA model suggests the need to strengthen the weakest-links in both technology and people entities of a system. This constitutes an improvement to the usual approach of focusing solely on technology component securities. The model also emphasizes the importance of maintaining a view of security vulnerabilities from both technology and people perspectives, as a means towards gaining a wider and better understanding of overall security susceptibilities within an ICSE. Considering either perspectives singly and separately does not provide sufficient disposition about environment security postures and risks in an organisation. The process plan also re-echoes the significance of selective security remediation of vulnerabilities and risk reduction, which are based on prioritised associated security impact criticalities. This offers a means for achieving resource-effective appropriation of security controls and improvements.

9.2 Key Research Contributions

This section presents key contributions of this research in line with defined research objectives.

From a combination of conference interactions and reviews of literature, a critical analysis and description of the landscape of security issues and risk enablers in ICSE was achieved. Knowledge gaps related to; (i) the misalignment or lag in current security

approaches to include human-factor evaluations, (ii) their insufficiency to address the dynamic and growing attack patterns in ICSE, (iii) security awareness and capability enhancements of the workforce, (iv) security metrics generation, and (v) estimation of vulnerability impacts with dependency attributes inclusive, all form parts of current reflective fissures highlighted, and which require research attention.

A prior and clear understanding of these issues and their implications to improved security in ICSE can assist both the academia and industry in characterising the relevant security dimensions, types, and scope to engage in certain application contexts. For the academia, it provides a wide overview of potential security research and development areas that can be explored to improve security. For the industry, it will help the engagement of appropriate and encompassing security analysis, threat and vulnerability identification, and the development or adoption of new and suitable mitigation and control efforts to improve security and productivity.

Exploring cyber security vulnerabilities and their exploitation potentials in ICSE was achieved using a small-scale shop-floor ICS testbed network comprising actual industrial components. Both insider and outsider threats and attack scenarios comprising vulnerability assessment, denial-of-service (DoS), privilege escalation and System Hijack were experimented. The outcome shows that ICSE networks can be reached and exploited by motivated and determined malicious actors. Thus, the need for security improvement solutions in line with the issues outlined above. Achieving these support, the fulfilment of research objective 1.

9.2.1 A list of good characteristics for security metric frameworks

The fulfilment of research objective 2 contributes to knowledge by providing information related to the characteristics of good security metrics development methodologies following the prior lack of such precise information in literatures with respect to ICSE cyber security. The proposed characteristics include: scope-definitive, objective-oriented, reliable, simple, adaptable, and repeatable (SORSAR). The outlined characteristics can be used as criteria and guiding basis for identifying, selecting or adopting trustworthy metrics generation methods. They can also assist with the development of new methodologies where needed. The metrics characteristics also provide insights to

possible criteria that can be used to evaluate the reliability and up-to-date nature of existing security metrics development tools and methods.

With these characteristics, future research paths in the areas of security metrics methodology validations are opened, as well as future security metric development advances.

9.2.2 A framework to guide a holistic generation of security metrics

The fulfilment of research objective 2 also contributes to knowledge by introducing a novel ICSE-centric framework for Operational Security Metrics Generation (OSMG). The framework demonstrates adherence to the proposed security metrics methodology characteristics. It offers new insights on metrics development requirements to security metrics developers and industrial owners, following the lack of such clarity in existing methodologies to suite the nature of ICSE security.

The new framework proffers knowledge using analytical means to describe the factors, dimensions, and scopes to consider while engaging the process of generating security metrics for the ICSE. The framework incorporates several essential framework components and features such as security environment dimensions, security objectives, and control capability variations, which collectively offer a more detailed and clearer guidance for the development of security metrics in ICSE. It will assist security metrics producers and consumers within industrial organisations to derive robust and suitable metric quantities for measuring security capabilities or vulnerabilities.

9.2.3 A novel approach for evaluating and prioritising technical security criticality impacts

The fulfilment of research objective 3 contributes to knowledge by providing a new probabilistic Multi-Attribute Vulnerability Criticality Analysis (MAVCA) approach that combines dynamic attributes of vulnerabilities with attack graph probabilities and functional dependency attributes. This combination, not found in any prior works reviewed, can be used to better evaluate security criticality indices of technical vulnerabilities in ICS networks.

The proposed MAVCA model provides a sound theoretical concept to the development and application of security metrics, and their combination with dependency and probability

metrics. The combination can help to realise more realistic security viewpoints like severities and cascading impacts in response to recurrent environmental changes. The proposed approach can assist organisations to effectively analyse the criticality impacts of security vulnerabilities, and resolve the uncertainties often introduced by the multiplicity of the same vulnerabilities in different assets, and the same base severity ratings for different vulnerabilities. The model also supports easy prioritisation of security controls to obtain the best possible security control improvement per remediation time.

9.2.4 A novel approach to evaluate and prioritise human cyber security capabilities.

The fulfilment of research objective 4 contributes to knowledge by proposing a novel approach to characterise and quantify human-factor security capabilities based on security knowledge and security skills. It also supports the identification of potential security weakest links amongst an evaluated industrial workforce (human agents). It involves concept description and capability evaluations with reference to defined security standards, guidelines, and baseline requirements. The methodology then prescribed control interventions that are based on discovered weak links and weak security areas. For the industrial organisations, the approach proffers a means of measuring the effectiveness of continuous cyber security awareness, tailored and resource-effective security control and remediation efforts, and speeds-up cyber security risk-related problem-solving with the best possible results.

9.2.5 A novel approach for security risk reduction

The fulfilment of research objective 5 contributes to knowledge by introducing a security risk reduction process flow based on vulnerability and impact analysis. The proposed risk reduction process presents a novel Security Risk Reduction through Critical Impact Point Assessment (S2R-CIPA) process model, which abstracts from traditional Hazard Analysis Critical Control Point Process (HACCP) concepts and principles. The proposed S2R-CIPA model supports risk reduction based on time-dependent evaluations stages, incorporating both technical and human security evaluations. The level of generalisation provides detailed information to support the process of performing security vulnerability discovery, analysis, impact criticality analysis, weak link identification, and prioritised control implementations across the entities that function in an ICSE.

9.3 Research Limitations

This research focuses on investigating the development of security solution approaches (techniques, frameworks, and models) that can be adopted towards improving cyber security in the ICSE using manufacturing as a case study. However, there were some limitations to the study. From a generalised perspective, the research explored security concepts that can be typically applied to already active and operational modern (IP/Ethernet-enabled) ICSE. It essentially exemplified a 'security-in-operation' - (SiO) concept rather than a 'security-by-design' (SbD) concept. In this research, SiO is used to describe the concept of introducing, adding, or improving security capabilities to an existing and already operational system, which were otherwise not included in the design process and stages of the system. This differs from 'security-by-design' concepts where security capacities are included in the initial design structure and process of a system. It involves critical reviews of cyber security issues in the ICSE, the evaluation of existing operational ICSE with view to identifying security vulnerabilities in the domain, which relate to the entities that constitute the ICS domain (ICSE). Thus, the outcomes of this research may not be aptly suitable while considering security solutions at the initial design and development stages of ICSEs. Outcomes focus on understanding the damage implications of existing vulnerabilities and determining what can be done to optimally improve security from both technology and human-factor vulnerability perspectives within an ICSE that has been operational prior to the emergence of security issues or have been upgraded via integration with IT infrastructures to improve performance and productivity. Other specific research limitations are discussed accordingly.

- i. **Framework for Operational Security Metrics Generation:*** - The Operational Security Metrics Generation framework did not directly consider the requirements that related to safety within the industrial environment. Hence, the framework might not be directly (literally) suitable to cater for metric developments for enhancing operational safety in ICSE. Although safety is considered relevant and mutually related to security, the concepts and phenomena that characterise safety within the ICSE is not within the scope of this research. There is also the potential for not gaining accurate information from the survey part of the work, and upon which more accurate inferences could be drawn on the status (awareness and diagnostic abilities) of

industrial/manufacturing personnel with respect to cyber security. This may limit the accuracy of findings.

- ii. *Technical Vulnerability Impact Analysis:*** - From the technology and risk security evaluation perspectives, the effectiveness of the research outcomes depends on the ability to distinguish sufficiently and correctly between normal system functionalities and(or) human responses, and the outcome of a malfunctions introduced by inherited perturbations from connected and trusted assets. The effectiveness of outcomes also relies solely on known or identified technology-based vulnerabilities, their exploit potentials, and the dynamic nature of impacts due to control and environmental changes. These, combined with the lack of generic ICS-oriented vulnerability scanning and assessment databases/tools introduce a likelihood of missing-out certain ICSE technology vulnerabilities that may not be contained in the IT-oriented vulnerability databases used. The reliance on known and documented technical vulnerabilities and their associated base scores also presents another limitation. This makes the impact analysis model and process directly unusable for assessing the impacts of unknown or undocumented vulnerabilities, or vulnerabilities that are not contained or updated in the vulnerability scanning and analysis tool at the time of use. Usability of the model then depends on the subjective quantification of undocumented vulnerabilities. Therefore, accuracy and strength of outcomes are dependent on an up-to-the-minute status of the vulnerability scanning/analysis database in use, and often limited by expert subjectivity in the case of undocumented vulnerabilities. Furthermore, any limitation(s) associated with an adopted vulnerability scoring protocol/scheme, such as CVSS 2.0 or CVSS 3.0 also typically affect the proposed approaches. For example, the subjectivity in the determination of temporal and environmental sub-group metrics in the CVSS scoring system allows for a potential variability of scores for the same vulnerability. The values would be dependent on the knowledge, expertise, and interpretation of the security accessors, which may vary. These could enable inconsistencies from multiple sources, especially due to uncertainties about software configurations.
- iii. *Human-factor cyber security evaluation:*** - From the human-factor security perspective, there are only a few researches on human-factor security that focus on characterising and attributing security capacity or vulnerability levels to the ICSE

workforce. Current research in security performance evaluation of human constituents within organisations typically focused on comparative analysis of security perceptions. The aspects of capability attributions using quantitative evaluation methods are under study and development phases. This implied that the research had to adopt engagement with experts from both information security and operational security fields to guide the development and validation process of the research. Also, only knowledge and skills factors are the only human-factor security attributes considered. Other human-factor security attributes such as security culture, attitude and behaviour, perception, policy, and guidelines, which can potentially contribute to overall workforce security capability are not directly considered due to time and research scope constraints. Typically, these human-factor security attributes are mostly characterised by research that are qualitative in nature and include high-level subjectivity. This typically makes direct quantitative evaluations using a uniform measuring scale pretty difficult. Effective research in this regard often requires independent and specialised researches that explore the varied factors and how they affect security states in human elements.

iv. Security Risk Reduction: - The S2R-CIPA process plan bears some limitations. It relies solely on known/discovered vulnerabilities, which also depend on recorded inputs in conventional vulnerability databases. These databases are not always up-to-date since updates for new vulnerabilities are included periodically. It implies that evaluations will most often be as current as the vulnerability database used. There is the likelihood of missing certain ICSE technology vulnerabilities that are not contained in the IT-oriented vulnerability databases used. Combining outputs from multiple vulnerability databases may yield more vulnerability occurrences than using just a single database. This may also provide support solution to the first limitation. The proposed S2R-CIPA process plan provides a uniform and integrated evaluation guide for security vulnerabilities, their impacts, and relevant controls. It supports security risk reduction based on time-dependent evaluations stages. The level of generalisation is considered sufficient to provide reasonable and detailed information to support the process of performing security vulnerability discovery, analysis, impact criticality analysis, weak link identification, and prioritised control implementations across the entities that function in an ICSE. We believe that the proposed process plan provides a useful guide for adopting effective security risk assessment and reduction strategies.

The research explored metric-driven approaches for security enhancements in ICESs. Precisely, it investigated the development and utilisation of security metrics from technology and people (human) perspectives to evaluate ICSE security capabilities and vulnerabilities, prior to employing security controls and countermeasures. The aspects of process security metrics, capacity, and vulnerability assessments were not considered due to time scope and time constraints. Thus, in the actual industrial environment, other system, or environment-specific process-oriented factors and metrics related to culture, supply chain interactions, etc., which can affect overall system security are not accounted for in the metrication concepts presented in this research.

An experimental testbed is used in this research as alternative to directly apply the research on actual ICSE network. There was a lack of real ICSE to apply the research objectives. Because of the direct severe consequences of cyber-attacks and intrusions on ICSEs, and the potential cascading damaging impacts that such consequences may bring to case study organisations, most industrial organisations are sceptical towards supporting independent researches that can expose or divulge their cyber security shortcomings and weaknesses. Moreover, organisations are often opposed to divulging cyber intrusion incidents that they have fallen to victims to, for fear of losing corporate reputation, staking clients' confidence, losing competitive advantage, and exposing their lack of requisite knowledge and in-house policies for spotting and resolving cyber-attacks. In using the testbed approach, there were potentials for errors, imprecision, and limitation of results and outcomes due to the use of free software tools with minimal features, prototype field equipment, and the absence of a complete and realistic industrial operational process. Essentially, the testbed experimental results are heavily affected by the testing environment, which often do not account for all the factors and constraints feasible in the real industrial environment network. Also, testing environments are most often highly random and uncontrollable. For example, a slightest change such as temperature and(or) pressure increase around a testbed asset or communication nodes can affect the communication quality, and thus affect their impacts, which may not be necessarily due to attack exertions. The precision and validity of potential research outcomes such as the Metrics frameworks and Security Evaluations models would be limited to the weaknesses of the modelling approaches adopted. Thus, testbed results might not clearly represent the exact or true nature of the system in real

environment/world. However, testbeds still offer a more realistic representation of the actual industrial network environment than simulation systems.

9.4 Conclusions

This research addresses crucial issues in the industrial control system environment regarding practical solutions for improving cyber security capabilities. The following points provide summaries of the main conclusions of this research study:

- i. Cyber security is a growing issue of concern in modern industrial and manufacturing developments driving the fourth industrial revolution (industry 4.0) and Industrial Internet-of-Things (IIoT). The trends significantly impact on operational performance, productivity, and business continuity in the modern ICSEs by enabling potentials for interferences and sabotages to normal industrial and business processes.
- ii. Increased connectivity of the ICS infrastructure with Information Technology infrastructures (open standards, protocols, and devices) potentially increases cyber security vulnerabilities, threats, attacks, impacts, and risk in the modern ICSE. Cyber security issues in the ICSE can be categorised into three key dimensions, which include; technology, people, and process fissures. Human actions and(or) inactions influenced by security knowledge and security skills can contribute to the vulnerability potentials, and successes of cyber intrusions in the ICSE.
- iii. The cyber-attack demonstration corroborates literature dispositions that cyber-attacks can be executed directly and(or) indirectly against an ICSE network infrastructure. Typical attacks on ICSE network can cause significant damages or interruptions that can affect industrial reliability: performance and productivity, and operational safety. Cyber-attacks on ICSE network can be executed using open source tools and technologies, and with little cyber intrusion knowledge, skills, and experience.
- iv. Relevant and practicable security metrics can be obtained when ICSE owners and(or) security metrics developers are able to clearly define and describe three key metric attributes: system scope, security objective of interest, and control capability dimension. A security metric development methodology that may be considered robust, strongly mapped to intended security capability objectives, and responsive to

security changes when it conveys the following characteristics: scope-definitive, objective-oriented, reliable, simple, adaptable, and repeatable (SORSAR). This means that such frameworks are easily usable, consistent in process applications, can be verified and tailored to suite various environmental security objectives and changes.

The proposed Operational Security metrics framework satisfies these criteria and offers insights (for security analysts and decision-makers) towards learning the broad developmental dimensions for effectively obtaining security metrics. Effective security metrics depend on effective metrics development approaches.

- v. In an ICSE security impact analysis, considering and combining vulnerability temporal (*exploit code maturity, remediation level, and report confidence*) and environmental (*confidentiality, integrity, and availability requirements*) attributes, probability of attack (*vulnerability frequency*) attributes, and functional dependency (*number of dependent devices*) attributes of vulnerability host components can help provide an easy approach and basis for resolving typical security control uncertainties caused by the presence of similar vulnerabilities in multiple components, and similar severity rating for multiple vulnerabilities. The proposed Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model demonstrates how these can be achieved by supporting the identification of the most vulnerable technology component, and the prioritisation of countermeasure and security controls based on obtained criticality indices of vulnerabilities.
- vi. The level of security knowledge and security skills are important and relevant direct human-factors attributes that can contribute to a workforce cyber security capability state. If an organisation is only as strong as its weakest human link, the least capable human user in an ICSE potentially represents the security strength of the organisation. As the capability level of the industrial workforce increases, the overall security state of the organisation also improves, and vice versa. Evaluating and understanding workforce cyber security knowledge and skills can help to estimate and attribute individual workforce cyber security capabilities. It can also help to identify the least capable human entity (workforce weakest link), identify the specific areas of security

where most workforce members show weaknesses, thus, guide the process of adopting prioritised security control strategy(ies).

Thus, people (human) cyber security knowledge and skills also contribute capacities in the improvement of cyber security in the ICSE. This capacity can be improved through security awareness and training, identifying the specific human with security weaknesses, and the specific knowledge or skills training needs. The proposed human-factor (workforce) security evaluation model shows how workforce security relates to organisational security, and how improvements can be attained via assessments techniques. Findings suggest that a lack of cyber security knowledge is as bad as a lack of cyber security skill, and it is a matter of an organisation and(or) system being only as strong as its weakest link. Potentially, the weaker links there are in the organisation, the lower the security capacity. Applying a systematic and strategic analysis of workforce security capacities can spur ICS organisations towards good and well-informed cyber hygiene. It can help maintain effective responses to possible cyber security factors through removing or reducing weak links in the system.

- vii. ICSE security risks are associated to vulnerability attributes of the entities that function and interact to keep the ICSE operational. In ICSEs, cyber security risks can be reduced, and security capability improved by reducing the security vulnerabilities found in both technology and people (human, workforce) constituents of the environment. The relationship between security risks and both technical and human-factor attributes is quite coherent to evolving security predispositions, and can help highlight the types of control strategy, action, and implementation approach required to effectively reduce security risks to as low as possible. A reduction in component-level or aggregate-level criticality impacts can be considered as reductions in security risks associated to the respective vulnerabilities. Considering both technology and human-factor vulnerabilities and associated impact criticalities, more encompassing contexts about security can be improved by identifying and strengthening the weak links in both technology and people entities of a system. This approach can enable a selective and more precise security remediation of vulnerabilities, and drive risk reduction based on prioritised impact criticalities. The technique offers a means for achieving time and resource-effective appropriation of security controls and

improvements. This can translate to economic rewards when considered from cost of security maintenance and management.

In general, improving cyber security in the industrial control system environment requires solution approaches that consider and combine technical and human-factor security capabilities and vulnerabilities evaluations. Such evaluations enable the identification of security weak links, the criticality of impacts associated to their weaknesses, and provide bases for strategic and effective prioritisation of security controls. This research underscores the significance of security capability and vulnerability evaluations (assessments) in relations to the entities that constitute and interact in the ICSE. Evaluations offer a means to learn the security state of an ICSE entity with reference to a standard or desired baseline and providing bases for more productive decision-making. Security capability and vulnerability evaluation can be considered as the first line of defence in the processes of attaining security assurance.

In relation to the manufacturing control system environment, cyber security vulnerabilities may exist in technology and human entities that constitute the operational environment. These make cyber-attacks to be feasible anywhere in the production system setup and lifecycle. A holistic security metrics development approach, and a guided enhancement of security capabilities in both technology and human constituents through evaluation; can contribute to a significant improvement of cyber security state in the ICSE.

9.5 Future Work

This PhD research has also identified some open areas of research that can be beneficially furthered in the areas of improving cyber security in the industrial control system environments.

The categorisation of security issues in the ICSE needs to follow a multilateral approach that considers the different threats, vulnerability, attack patterns, target entities, and potential impact dimensions that can emerge in an analysis process. Thus, the development of a comprehensive taxonomy or categorisation scheme for security issues within the ICSE remains an area that is open for further research. A comprehensive taxonomy of security issues may assist in the investigation and analysis of relevant and effective security improvement models and approaches.

Further research can be engaged to explore the application of the proposed security metrics development framework to handle the generation of process-oriented security metrics. This will provide the potential for deeper insights to the strengths or limitations of the existing framework and hewn a solution path for improvement. Investigations can be conducted to ascertain the effectiveness of the different security metrics dimensions that can be derived using the proposed framework. For example: comparing the effectiveness of achieving improved security using proactive control capability metrics as against reactive control capability metrics. Also comparing the effectiveness of results between computable and measurable security metric quantities. Another area of further research involves investigating the application and efficiency of the proposed framework in an actual industrial environment and scenarios. These can help consolidate validity and reliability of the framework to support the generation of effective security metrics in the ICSE. It will also provide a means of discovering any metric parameters and dimensions that may not have been considered in the development process, and which indicate limitations in the current framework structure. This understanding can support further improvements of the framework accordingly.

Existing parameters used in the dependency modelling part of the MAVCA model are quantitative in nature. There are prospects for achieving better dependency modelling in the context of ICSE considering qualitative parameters that extend beyond the boundaries of an organisation, historic threat and vulnerability data. The MAVCA model can be expanded to include qualitative parameters especially related to the dependency modelling part of the model in relations to other dependency models. The MAVCA model can be expanded into an automated process and software tool with the capabilities of evaluating and refreshing security criticality attributes (dependency modelling, probability of attack, security exploitability and impact potentials) by pulling together updated dynamic security-related information in a consistent manner. Further investigations can be conducted to determine the effectiveness and scalability of the MAVCA approach for estimating the security cascading impacts associated to discovered vulnerabilities. Trade-offs between the accuracy and timeliness of evaluation can be analysed. The potential to use the methodology or a modified version to evaluate undocumented (non-scored) vulnerabilities can also be explored.

ICSs are federated systems, thus, there is a need to investigate models for assessing and enforcing trustworthiness of system components managed in different structural security schedules. The issues of trust in such distributed system setups need to be investigated. The development of trust models to support dependency segregation for different functional components of a system is an open area for future work. The trust model must be such that different component of an ICS should be able to achieve self-availability and reliability, and without a central point of vulnerability impact.

In the human-factor security evaluation perspective, developing an automated evaluation tool that can be used to replicate and quicken the processes of the proposed approach presents an area for further work. Another open research involves investigating the relationship between ICSE cyber security improvement and other indirect human-factor attributes such as culture, attitude and behaviour, perception, policies and management, values, and concerns. It will be important to learn of the impacts of these indirect human-factor attributes to the attainment of improved cyber security in the ICSE. Additionally, investigations can be furthered on how these indirect human-factors attributes can be combined with the evaluated direct human-factor attributes (knowledge and skills) adopted in this study, to achieve a wider viewpoint of human-factor security capabilities for effective security in the ICSE.

The security risk reduction approach can be further explored in the context of financial implications. The modelling of cost relationships amongst the various security risk factors and attributes can be explored to help achieve specific cost attributes in relations to the vulnerabilities and impacts evaluated. This can help provide the business and investment case for improving cyber security in the industrial control system environment (ICSE).

Other open research areas include exploring the security-by-design approach for establishing and improving security in the ICSE. This would involve considering security as part of initial design processes and structures. The development and application of adaptive security architecture for ICSs needs to be investigated. This includes considering the security implication of data placement structures, system control and monitoring. Further researches need to consider and critically analyse how cyber-attacks affect control algorithms, and the consequent impact on the physical world. Current security solutions are quite supportive; however, they are insufficient towards actualising the popularly prescribed defense-in-depth for ICSE. A clear and in depth understanding of the

interrelationships and interactions inside the ICSE, and with the physical world can support improved security capacities such as: (i) better understanding of attack consequences from the perspective of an attacker who has successfully compromised a control network, (ii) develop novel attack/intrusion detection algorithms that combine both technology and human-factor attributes, and (iii) develop novel algorithms and architectures that enforce cyber-resilience, so that control commands and instructions can be easily and timely changed or updated in the event of an attack on the ICSE network or system.

REFERENCES

- Abbadi, Z. (2006) *Security Metrics What Can We Measure ? What is a “ Metric ”*, Presentation. OWASP. Available at: https://www.owasp.org/images/b/b2/Security_Metics-What_can_we_measure-_Zed_Abbadi.pdf. (Accessed: 15 September 2016).
- Abraham, S. and Nair, S. (2014a) ‘Cyber security analytics: A stochastic model for security quantification using absorbing markov chains’, *Journal of Communications*, 9(12), pp. 899–907. doi: 10.12720/jcm.9.12.899-907.
- Abraham, S. and Nair, S. (2014b) ‘Predictive Cyber Security Analytics Framework: A Non-Homogenous Markov Model for Security Quantification’, in *NeTCoM, CSIT, GRAPH-HOC, SPTM. CS & IT-CSCP*, pp. 195–209. Available at: <http://airccj.org/CSCP/vol4/csit43116.pdf>.
- Abraham, S. and Nair, S. (2015a) ‘A Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models’, in *2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE Xplore, pp. 774–781. doi: 10.1109/Trustcom.2015.446.
- Abraham, S. and Nair, S. (2015b) ‘Exploitability analysis using predictive cybersecurity framework’, in *Proceedings - 2015 IEEE 2nd International Conference on Cybernetics, CYBCONF 2015*. IEEE Xplore, pp. 317–323. doi: 10.1109/CYBConf.2015.7175953.
- Adams, M. and Makramalla, M. (2015) ‘Cybersecurity Skills Training : An Attacker-Centric Gamified Approach’, *Technology Innovation Management Review*, (January), pp. 5–14. Available at: https://timreview.ca/sites/default/files/article_PDF/AdamsMakramalla_TIMReview_January2015.pdf.
- Adhikari, U., Morris, T. H. and Pan, S. (2014) ‘A Causal Event Graph for Cyber-Power System Events Using Synchrophasor’, in *PES General Meeting | Conference & Exposition, 2014 IEEE*. IEEE Xplore, pp. 1–5.
- Ahmed, I., Roussev, V., Johnson, W., Senthivel, S. and Sudhakaran, S. (2016) ‘A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy’, in *Proceedings of the 2nd Annual Industrial Control System Security Workshop on - ICSS ’16*. Los Angeles, CA: ACM, pp. 1–9. doi: 10.1145/3018981.3018984.
- Aissa, A. Ben, Rabai, L. B. A., Abercrombie, R. K., Mili, A. and Sheldon, F. T. (2014) ‘Quantifying availability in SCADA environments using the cyber security metric MFC’, in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR ’14*. New York, New York, USA: ACM Press, pp. 81–84. doi: 10.1145/2602087.2602103.
- Al-Shehri, S. M., Loskot, P., Numanoglu, T. and Mert, M. (2017) *Common Metrics for Analyzing, Developing and Managing Telecommunication Networks*. Available at: <http://arxiv.org/abs/1707.03290>.
- Alcaraz, C. and Zeadally, S. (2015) ‘Critical infrastructure protection: Requirements and challenges for the 21st century’, *International Journal of Critical Infrastructure Protection*. Elsevier, 8, pp. 53–66. doi: 10.1016/j.ijcip.2014.12.002.
- Allodi, L., Woohyun Shim and Massacci, F. (2013) ‘Quantitative Assessment of Risk Reduction with Cybercrime Black Market Monitoring’, in *2013 IEEE Security and Privacy Workshops*. San Francisco, CA, USA: IEEE Computer Society, pp. 165–172. doi: 10.1109/SPW.2013.16.

Aloul, F. a. (2012) 'The Need for Effective Information Security Awareness', *Journal of Advances in Information Technology*, 3(3), pp. 176–183. doi: 10.4304/jait.3.3.176-183.

Amin, S. and Sastry, S. (2015) '1 Introduction 2 Analysis of the Secure Control Problem', *Control*, pp. 1–14.

Amtoft, T. and Banerjee, A. (2007) 'A logic for information flow analysis with an application to forward slicing of simple imperative programs', *Science of Computer Programming*, 64(1), pp. 3–28. doi: 10.1016/j.scico.2006.03.002.

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I. and Timorin, A. A. (2016a) *Industrial Control Systems Vulnerabilities Statistics*. Available at: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf.

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I. and Timorin, A. A. (2016b) *Industrial Control Systems Vulnerabilities Statistics*.

Ani, U. P. D., He, H. (Mary) and Tiwari, A. (2017) 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *Journal of Cyber Security Technology*. Taylor & Francis, 1(1), pp. 32–74. doi: 10.1080/23742917.2016.1252211.

Ani, U. P. D., He, H. M. and Tiwari, A. (2016) 'Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure', in Nicholson, D. (ed.) *Advances in Human Factors in Cyber Security: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA*. Florida: Springer International Publishing, pp. 169–182. doi: 10.1007/978-3-319-41956-5.

Ani, U. P. D., He, H. and Tiwari, A. (2016) 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *Journal of Cyber Security Technology*. Taylor & Francis, pp. 1–43. doi: 10.1080/23742917.2016.1252211.

Antrobus, R., Frey, S., Green, B. and Rashid, A. (2016) 'SimaticScan: Towards A Specialised Vulnerability Scanner for Industrial Control Systems', in *4th International Symposium for ICS & SCADA Cyber Security Research 2016*. BCS Learning & Development Ltd, pp. 11–18. doi: <http://dx.doi.org/10.14236/ewic/ICS2016.2>.

Anwar, R. W. and Ali, S. (2012) 'Trust Based Secure Cyber Physical Systems', in Fitzgerald, J., Mak, T., Romanovsky, A., and Eds, Y. (eds) *Proceedings of the Workshop on Trustworthy Cyber-Physical Systems run on September 3, 2012 in conjunction with CONCUR 2012*. Newcastle, pp. 1–10. Available at: <http://www.cs.ncl.ac.uk/publications/trs/papers/1347.pdf>.

Asgharpour, F., Liu, D. and Camp, L. J. (2007) 'Mental models of security risks', in Dhamija, R. (ed.) *Lecture Notes in Computer Science*. Berlin; Heidelberg: Springer, pp. 367–377. doi: 10.1007/978-3-540-77366-5_34.

Ashford, W. (2016) 'Lack of cyber security awareness putting UK organisations at risk', *ComputerWeekl.com Online Article*, March. Available at: <http://www.computerweekly.com/news/4500278074/Lack-of-cyber-security-awareness-putting-UK-organisations-at-risk>.

Austin, M. (2017) 'Sophisticated "Triton" malware shuts down industrial plant in hacker attack'. Designtecnica Corporation, p. Digital Trends Website (Computing). Available at: <https://www.digitaltrends.com/computing/triton-industrial-plant-hacker-attack/> (Accessed: 20

December 2017).

Azuwa, M. ., Ahmad, R., Sahib, S. and Shamsuddin, S. (2012) 'Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard', *International Journal of Cyber-Security and Digital Forensics*, 1(4), pp. 280–288. Available at: <http://sdiwc.net/digital-library/technical-security-metrics-model-in-compliance-with-isoiec-27001-standard>.

Azuwa, M. P., Ahmad, R., Sahib, S. and Shamsuddin, S. (2012) 'A propose technical security metrics model for SCADA systems', *International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, pp. 70–75. doi: 10.1109/CyberSec.2012.6246089.

Baiardi, F., Telmon, C. and Sgandurra, D. (2009) 'Hierarchical, model-based risk management of critical infrastructures', *Reliability Engineering and System Safety*. Elsevier, 94(9), pp. 1403–1415. doi: 10.1016/j.ress.2009.02.001.

Barabanov, R., Kowalski, S. and Yngstrom, L. (2011) *Information security metrics: Research directions*, *European Security Conference*. Available at: <http://www.diva-portal.org/smash/get/diva2:469569/FULLTEXT01.pdf>.

Bartman, T. and Carson, K. (2017) 'Securing communications for SCADA and critical industrial systems', in *69th Annual Conference for Protective Relay Engineers, CPRE 2016*. College Station, TX, USA: IEEE Xplore. doi: 10.1109/CPRE.2016.7914914.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, M. A. (2016) 'Productive Security: A scalable methodology for analysing employee security behaviours', in *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*. Denver: www.usenix.org, pp. 1–18. Available at: <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement>.

Beautement, A., Sasse, M. and Wonham, M. (2009) 'The compliance budget: Managing security behaviour in organisations', in *Proceedings of the 2008 Workshop on New Security Paradigms*. Lake Tahoe, California, USA: ACM New York, NY, USA, pp. 47–58. doi: 10.1145/1595676.1595684.

Beecham, S., Hall, T., Britton, C., Cottee, M. and Rainer, A. (2005) 'Using an expert panel to validate a requirements process improvement model', *Journal of Systems and Software*, 76, pp. 251–275. doi: 10.1016/j.jss.2004.06.004.

Beechey, J. (2010) *Application Whitelisting: Panacea or Propaganda?* Available at: <http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599>.

Beitel, G. A., Gertman, D. I. and Plum, M. M. (2004) 'Balanced scorecard method for predicting the probability of a terrorist attack', in *Risk Analysis IV. Fourth International Conference of Computational Simulation in Risk Analysis*. WIT Press, pp. 581–592. Available at: <https://www.witpress.com/Secure/elibrary/papers/RISK04/RISK04053FU.pdf>.

Bellettini, C. and Rushi, J. (2008) 'Combating memory corruption attacks on scada devices', in Papa, M. and Sheno, S. (eds) *IFIP International Federation for Information Processing*. Springer, IFIP Publications, pp. 141–156. doi: 10.1007/978-0-387-88523-0_11.

Bellovin, S. M. (2006) 'On the brittleness of software and the infeasibility of security metrics', *IEEE Security and Privacy*, 4(4), p. 96. doi: 10.1109/MSP.2006.101.

- Ben-Asher, N. and Gonzalez, C. (2015) 'Effects of cyber security knowledge on attack detection', *Computers in Human Behavior*. Elsevier Ltd, 48(June), pp. 51–61. doi: 10.1016/j.chb.2015.01.039.
- Beres, Y., Mont, M. C., Griffin, J. and Shiu, S. (2009) 'Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes', in *Third International Symposium on Empirical Software Engineering and Measurement*. IEEE, pp. 564–573.
- Bistarelli, S., Fioravanti, F. and Peretti, P. (2006) 'Defense trees for economic evaluation of security investments', in *Proceedings - First International Conference on Availability, Reliability and Security, ARES 2006*. Vienna, Austria: IEEE Xplore, pp. 416–423. doi: 10.1109/ARES.2006.46.
- Bistarelli, S., Fioravanti, F., Peretti, P. and Santini, F. (2012) 'Evaluation of complex security scenarios using defense trees and economic indexes', *Journal of Experimental & Theoretical Artificial Intelligence*, 24(2), pp. 161–192. doi: 10.1080/13623079.2011.587206.
- Bobbio, A., Egidio, L., Terruggia, R., Ciancamerla, E. and Minichino, M. (2013) 'Weighted attack trees for the cybersecurity analysis of SCADA systems', in *3rd International Defense and Homeland Security Simulation Workshop, DHSS 2013, Held at the International Multidisciplinary Modeling and Simulation Multiconference, I3M 2013*. Caltek s.r.l., pp. 33–40. Available at: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84898874295&partnerID=tZOtx3y1>.
- Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B. (2007) 'Towards understanding IT security professionals and their tools', in *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, PA, pp. 100–111. doi: <http://doi.acm.org/10.1145/1280680.1280693>.
- Boyes, H. a. (2013) 'Trustworthy cyber-physical systems - a review', *8th IET International System Safety Conference incorporating the Cyber Security Conference 2013*, pp. 1–8. doi: 10.1049/cp.2013.1707.
- Brenner, J. F. (2013) 'Eyes wide shut: The growing threat of cyber attacks on industrial control systems', *Bulletin of the Atomic Scientists*, 69, p. 15. doi: 10.1177/0096340213501372.
- Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness', *MIS Quarterly*, September, pp. 523–548. Available at: http://130.18.86.27/faculty/warkentin/BIS9613papers/MISQ_SpecialIssue/BulgurcuCavusogluBenbasat2010_MISQ34_RationalityAwareness.pdf.
- Burmester, M. (2013) 'A trusted computing architecture for critical infrastructure protection', *Iisa 2013*, pp. 1–6. doi: 10.1109/IISA.2013.6623706.
- Burmester, M., Magkos, E. and Chrissikopoulos, V. (2012) 'Modeling security in cyber-physical systems', *International Journal of Critical Infrastructure Protection*, 5, pp. 118–126. doi: 10.1016/j.ijcip.2012.08.002.
- Byres, E., Leversage, D. and Kube, N. (2007) 'Security incidents and trends in SCADA and process industries', *The Industrial Ethernet Book*, 39(May), pp. 12--20. Available at: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Security+incidents+and+trends+in+SCADA+and+process+industries#0>.
- C'ardenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y. and Sastry, S. (2011) 'Attacks

Against Process Control Systems: Risk Assessment, Detection, and Response', in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11)*. ACM, pp. 355–366. Available at: http://delivery.acm.org/10.1145/1970000/1966959/p355-cardenas.pdf?ip=138.250.109.141&id=1966959&acc=ACTIVE SERVICE&key=BF07A2EE685417C5.C9C3422D7A5E53A6.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=676313516&CFTOKEN=17328626&__acm__=1476093021_c56e08f3601.

CACI International Inc. (2010) 'Cyber Threats to National Security.', in Pino, M. (CACI I. I. (ed.) *Symposium on Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain*. Virginia: CACI International Inc, pp. 1–31. Available at: http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf.

Caltagirone, S., Pendergast, A. and Betz, C. (2013) 'The Diamond Model of Intrusion Analysis', *Threat Connect*, 298(0704), pp. 1–61. Available at: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586960%5Chttps://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf>.

Campbell, G. K. (2009) *Measures and Metrics in Corporate Security*. Security Executive Council. Available at: https://www.securityexecutivecouncil.com/content/measures_metrics_mini_200801.pdf.

Candell Jr., R., Zimmerman, T. A. and Stouffer, K. A. (2015) 'An Industrial Control System Cybersecurity Performance Testbed'. U.S. Department of Commerce. doi: 10.6028/NIST.IR.8089.

Candell, R., Stouffer, K. and Anand, D. (2014) 'A Cybersecurity Testbed for Industrial Control Systems', *Proceedings of the 2014 Process Control and Safety Symposium*.

Candell, R., Zimmerman, T. and Stouffer, K. (2015) 'An industrial control system cybersecurity performance testbed (NISTIR 8089)'. National Institute of Standards and Technology.

Chalkias, K., Baldimtsi, F. and Stephanides, G. (2008) 'Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols', *Communications in Computer and Information Science*, 23, pp. 227–238. Available at: http://download.springer.com/static/pdf/740/chp%253A10.1007%252F978-3-540-88653-2_17.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F978-3-540-88653-2_17&token2=exp=1445943007~acl=%2Fstatic%2Fpdf%2F740%2Fchp%25253A10.1007%252F978-3-54.

Chandrakumar, T., Parthasarathy, S., Maragathameena, R. and Pandian, S. A. R. (2013) 'Security Metrics for a Business Information System', *International Journal of Computer Applications*, pp. 33–38. Available at: <http://www.ijcaonline.net/proceedings/ic2it/number1/14389-1308>.

Chandrika, N. (2011) 'Cyber Security in the UK', *POSTnote*, (389), pp. 1–4. Available at: <http://www.parliament.uk/business/publications/research/briefing-papers/POST-PN-389>.

Chapman, S. (2018) 'Manufacturing accounted for 46% of all UK cyber-attacks in 2017', *Global Manufacturing*, May.

Chaula, J., Yngström, L. and Kowalski, S. (2004) 'Security metrics and evaluation of information systems security', in *Conference on Information Security for South Africa*, pp. 1–12. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.8565&rep=rep1&type=pdf>.

Chejara, P., Garg, U. and Singh, G. (2013) 'Vulnerability Analysis in Attack Graphs Using Conditional Probability', *International Journal of Soft Computing and Engineering (IJSCE)* 13, 3(2), pp. 18–21. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.677.3265&rep=rep1&type=pdf>.

Chen, L. (2010) 'The Model and Method of Trustworthiness Level Evaluation for Software Product', (Icnc), pp. 709–715.

Chen, P.-C., Liu, P., Yen, J. and Mullen, T. (2012) 'Experience-based cyber situation recognition using relaxable logic patterns', in *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. New Orleans, LA: IEEE Xplore, pp. 243–250. doi: 10.1109/CogSIMA.2012.6188392.

Chen, Q. and Abdelwahed, S. (2014) 'A Model-based Approach to Self-Protection in SCADA Systems', in *9th International Workshop on Feedback Computing (Feedback Computing 14)*. IEEE Xplore, pp. 1–7. Available at: <https://www.usenix.org/conference/feedbackcomputing14/workshop-program/presentation/chen>.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016) 'A review of cyber security risk assessment methods for SCADA systems', *Computers & Security*. The Authors, 56, pp. 1–27. doi: 10.1016/j.cose.2015.09.009.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. and Robinson, W. (2008) *Performance Measurement Guide for Information Security, NIST Special Publication 800-55 Revision 1*. Gaithersburg, Maryland: National Institute of Standards and Technology (NIST). Available at: <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>.

Chi, M. T. H. (2006) 'Two approaches to the study of experts' characteristics', *The Cambridge handbook of expertise and expert performance*, pp. 21–30. doi: 10.1017/CBO9780511816796.002.

Choo, K.-K. R. (2011a) 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, 30(8), pp. 719–731. doi: 10.1016/j.cose.2011.08.004.

Choo, K.-K. R. (2011b) 'The cyber threat landscape: Challenges and future research directions', *Computers and Security*, 30, pp. 719–731. doi: 10.1016/j.cose.2011.08.004.

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., Curtis, P. and Dolan, T. (2014) *Cybersecurity Capability Maturity Model (C2M2)*, *Department of Homeland Security*. Available at: <https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program>.

CIS (2010) *The CIS Security Metrics v1.1.0*. The Center for Internet Security. Available at: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf.

CLOUDMARK (2016) *Survey Reveals Spear Phishing as a Top Security Concern to Enterprises, Website Blog Inforgraph*. Available at: <https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/> (Accessed: 25 April 2017).

Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A. and Linkov, I. (2016) 'Security Metrics in Industrial Control Systems', in Colbert, E. J. M. and Kott, A. (eds) *Cyber-security of SCADA and Other Industrial Control Systems, Advances in Information Security*. Switzerland: Springer International Publishing, pp. 167–185. doi: 10.1007/978-3-319-32125-7.

Conte de Leon, D., Alves-Foss, J., Krings, A. and Oman, P. (2002) 'Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack', in *ACM Workshop on Scientific Aspects of Cyber Terrorism*. ACM, pp. 1–10. Available at: <http://www2.cs.uidaho.edu/~krings/publications/SACT-2002-D.pdf>.

Cook, A., Janicke, H., Smith, R. and Maglaras, L. (2017) 'The industrial control system cyber defence triage process', *Computers and Security*. Elsevier Ltd, 70, pp. 467–481. doi: 10.1016/j.cose.2017.07.009.

CPNI (2009) *RESILIENCE IN CONVERGED NETWORKS Resilience in Converged Networks*: London. Available at: http://www.cpni.gov.uk/Documents/Publications/2009/2009023-GPG_Resilience-guide.pdf.

CPNI (2014) 'Cyber-attacks: Effects on UK Companies', *Oxford Economics CPNI Publication*, (July). Available at: <http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb>.

Creswell, J. W. (2014) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th Editio, *Research design Qualitative quantitative and mixed methods approaches*. 4th Editio. Edited by V. Knight, J. Young, K. Koscielak, B. Bauhaus, and M. Markanich. California - London - New Delhi - Singapore: Sage Publications, Inc. doi: 10.1007/s13398-014-0173-7.2.

Cruz, T., Proença, J., Simões, P., Aubigny, M., Ouedraogo, M., Yasakhetu, L. and Graziano, A. (2014) 'Improving cyber-security awareness on Industrial Control Systems: the CockpitCI approach', in Liropoulos, A. and Tsihrintzis, G. (eds) *13th European Conference on Cyber Warfare and Security Th University U i it of f Piraeus Pi*. Greece: ACPI, UK, pp. 59–69. doi: 10.13140/2.1.2939.7287.

CSC (2014) *CSC GLOBAL CIO SURVEY: 2014–2015, CIOs EMERGE AS DISRUPTIVE INNOVATORS, An Annual Barometer Of Global Cios' Plans, Priorities, Threats, And Opportunities*. Available at: http://assets1.csc.com/cio_survey_2014_2015/downloads/CIO_Survey_Disruptive_innovation.pdf.

Cybenko, G. and Cybenko, G. (2014) *TIM Lecture Series Cybersecurity Metrics and Simulation, Technology Innovation Management Review*. Talent First Network.

D'Amico, A. and Whitley, K. (2008) *VizSEC 2007: The real work of computer network defense analysts, Proceedings of the Workshop on Visualization for Computer Security*. Edited by J. R. Goodall, G. Conti, and K.-L. Ma. Springer Berlin Heidelberg. doi: 10.1007/978-3-540-78243-8.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B. and Roth, E. (2005) 'Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts', in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. DoD, pp. 229–233. doi: 10.1177/154193120504900304.

Dacier, M., Deswarte, Y. and Kaâniche, M. (1996) 'Quantitative assessment of operational security: Models and tools', *Information Systems Security*, (October), pp. 1–22. doi: 10.1007/978-1-5041-2919-0_15.

Defence Signals Directorate (2012) *Network segmentation and segregation*. Available at: http://www.asd.gov.au/publications/csocprotect/Network_Segmentation_Segregation.pdf.

DeSmit, Z., Elhabashy, A. E., Wells, L. J. and Camelio, J. A. (2016) 'Cyber-physical Vulnerability

Assessment in Manufacturing Systems', *Procedia Manufacturing*, 5, pp. 1060–1074. doi: 10.1016/j.promfg.2016.08.075.

Dickman, F. (2009) *Hacking The Industrial SCADA Network*, *Pipeline & Gas Journal*. [online]. Available at: <http://pipelineandgasjournal.com/hacking-industrial-scada-network> (Accessed: 1 April 2015).

Dodig-Crnkovic, G. (2002) : 'Scientific Methods in in', in *Computer Science. Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden*. Sweden: Malardalen University Website. Available at: http://www.es.mdh.se/pdf_publications/375.pdf.

Dong, P., Han, Y., Guo, X. and Xie, F. (2015) 'A Systematic Review of Studies on Cyber Physical System Security', 9(1), pp. 155–164.

Dorfler, F., Pasqualetti, F. and Bullo, F. (2011) 'Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach', in *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE Xplore, pp. 1486–1491. doi: 10.1109/Allerton.2011.6120343.

Drias, Z., Serhrouchni, A. and Vogel, O. (2015) 'Analysis of Cyber Security for Industrial Control Systems', in *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. Shanghai, China: IEEE, pp. 1–8. doi: 10.1109/SSIC.2015.7245330.

Dudenhofer, D. D., Permann, M. R., Woolsey, S., Timpany, R., Miller, C., McDermott, A. and Manic, M. (2007) 'Interdependency modeling and emergency response', in *Summer Computer Simulation Conference*. San Diego, CA: ACM, pp. 1230–1237. doi: 10.1145/1357910.1358101.

Dumont, D. (2010) 'Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems', *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. Boston Waltham, MA, USA: IEEE, pp. 473–475. doi: 10.1109/THS.2010.5654964.

Edmonds, J., Papa, M. and Shenoi, S. (2007) 'Security analysis of multilayer SCADA protocols: A Modbus TCP case study', in Goetz, E. and Shenoi, S. (eds) *IFIP International Federation for Information Processing*. Springer, IFIP Publications, pp. 205–221. doi: 10.1007/978-0-387-75462-8_15.

Emerson Network Power (2013) 'Integrating People , Process and Technology to Transform Data Center Operations and Performance'. Columbus: Emerson Network Power, p. 12. Available at: http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white_papers/people_process_technology_sl-25674.pdf.

ENISA (2011) *Protecting Industrial Control Systems Recommendations for Europe and Member States*. Greece. Available at: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states>.

Evans, M., Maglaras, L., He, Y. and Janicke, H. (2016) 'Human Behaviour as an aspect of Cyber Security Assurance', *arXiv preprint arXiv:1601.03921*, pp. 1–22. Available at: <http://arxiv.org/abs/1601.03921>.

Fan, X., Fan, K., Wang, Y. and Zhou, R. (2015) 'Overview of cyber-security of industrial control system', in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings*. IEEE Xplore, pp. 1–7. doi: 10.1109/SSIC.2015.7245324.

Fernandez, E. B., Wu, J., Larrondo-Petrie, M. M. and Shao, Y. (2009) 'On building secure SCADA systems using security patterns', *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW '09*, p. 17. doi: 10.1145/1558607.1558627.

FIRST (2015) 'Common Vulnerability Scoring System v3.0: Specification Document', *Forum of Incident Response and Security Teams (FIRST)*, pp. 1–21. Available at: <https://www.first.org/cvss/specification-document> (Accessed: 14 September 2015).

FIRST (no date) CVSS v2 Complete Documentation. Available at: <https://www.first.org/cvss/v2/guide> (Accessed: 13 February 2017).

Fovino, I. N., Carcano, A., Masera, M. and Trom-Betta, A. (2009) *Design and implementation of a secure Modbus protocol*, *IFIP Advances in Information and Communication Technology*. Edited by C. Palmer and S. Sheno. Springer, IFIP Publications. doi: 10.1007/978-3-642-04798-5_6.

Fovino, I. N., Masera, M., Guglielmi, M., Carcano, A. and Trombetta, A. (2010) 'Distributed intrusion detection system for SCADA protocols', in Moore, T. and Sheno, S. (eds) *IFIP Advances in Information and Communication Technology*. Springer, IFIP Publications, pp. 95–110. doi: 10.1007/978-3-642-16806-2_7.

Francia, G. a, Thornton, D. and Dawson, J. (2012) 'Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems', in *Security BP*. Semantic Scholar. Available at: <https://www.semanticscholar.org/paper/Security-Best-Practices-and-Risk-Assessment-of-SCA-Francia/3143940955a76a49646ba2954e0735a0ec18d7ca>.

Franklin, J., Wergin, C. and Booth, H. (2014) *CVSS Implementation Guidance (NISTIR 7946)*, National Institute of Standards and Technology, NISTIR-7946. doi: <http://dx.doi.org/10.6028/NIST.IR.7946>.

Frechtling, J. (2002) *An Overview of Quantitative and Qualitative Data Collection Methods, The 2002 User-Friendly Handbook for Project Evaluation*. Available at: <http://www.nsf.gov/pubs/2002/nsf02057/nsf02057.pdf>.

Frei, S. (2009) *Security Econometrics - The Dynamics of (In)Security*. ETH ZURICH. Available at: file:///C:/Users/s234671/Downloads/eth_dissertation_stefan_frei_2009.pdf.

Freitas, R. (2009) 'Scientific Research Methods and Computer Science', in *MAPI Seminars Workshop 2009*, pp. 1–6. Available at: <http://map.edu.pt/i/2008/map-i-research-methods-workshop-2009/RicardoFreitasFinal.pdf>.

Fruehwirth, C., Biffi, S., Tabatabai, M. and Weippl, E. (2010) 'Addressing misalignment between information security metrics and business-driven security objectives', in *6th International Workshop on Security Measurements and Metrics*. AC, p. 7. doi: 10.1145/1853919.1853927.

Frühwirth, C. and Männistö, T. (2009) 'Improving CVSS-based vulnerability prioritization and response with context information', in *2009 3rd International Symposium on Empirical Software Engineering and Measurement, ESEM 2009*. Florida, USA: IEEE, pp. 535–544. doi: 10.1109/ESEM.2009.5314230.

Gamage, T. T., Roth, T. P. and McMillin, B. M. (2011) 'Confidentiality Preserving Security Properties for Cyber-Physical Systems', *2011 IEEE 35th Annual Computer Software and Applications Conference*, (October 2010), pp. 28–37. doi: 10.1109/COMPSAC.2011.13.

Gary A, R. (2000) *SNMP Community Strings*. Available at: <https://www.giac.org/paper/gcih/44/default-snmp-community-strings-set-public-private/100366>.

Gervais, A. (2012) *Security Analysis of Industrial Control Systems*. KTH Stockholm and Aalto University. Available at: http://nordsecmob.aalto.fi/en/publications/theses_2012/gervais-arthur_thesis.pdf.

Gibbs, S. (2017) 'Triton: hackers take out safety systems in "watershed" attack on energy plant | Technology | The Guardian', *The Guardian News (Online)*, 15 December, p. Technology News page. Available at: <https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant> (Accessed: 20 December 2017).

Gilbert, N. (2008) *Researching social life*. 3rd Editio. London: Sage Publications Ltd, London 2008.

Gold, S. (2009) 'The SCADA challenge: securing critical infrastructure', *Network Security*, 2009(8), pp. 18–20. doi: 10.1016/S1353-4858(09)70078-9.

Goldenberg, N. and Wool, A. (2013) 'Accurate modeling of Modbus / TCP for intrusion detection in SCADA systems', 6, pp. 63–75. Available at: <https://www.eng.tau.ac.il/~yash/goldenberg-wool-ifip-2013-01-04.pdf>.

Gollmann, D. (2011) *Computer Security*. Third Edit. West Sussex: John Wiley & Sons, Ltd.

Gollmann, D. (2012) 'Veracity, Plausibility, and Reputation', in Askoxylakis, I., Pöhls, H. C., and Posegga, J. (eds) *Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems, Volume 7322 of the series Lecture Notes in Computer Science*. Egham, UK: Springer Berlin Heidelberg, pp. 20–28. doi: 10.1007/978-3-642-30955-7_3.

Gonzalez, C., Ben-Asher, N., Oltramari, A. and Lebiere, C. (2014) 'Cognition and Technology', *Cyber Defense and Situational Awareness*. Edited by A. Kott, C. Wang, and R. F. Erbacher. Springer Publishers: Advances in Information Security 62, pp. 93–117. doi: 10.1007/978-3-319-11391-3.

Goodall, J. R., Lutters, W. G. and Komlodi, A. (2004) 'I Know My Network: Collaboration and Expertise in Intrusion Detection', in *ACM conference on Computer supported cooperative work*. Illinois, USA: ACM, pp. 342–345. doi: <http://doi.acm.org/10.1145/1031607.1031663>.

Goodall, J. R., Lutters, W. G. and Komlodi, A. (2009) 'Developing expertise for network intrusion detection', *Information Technology & People*, 22(2), pp. 92–108. doi: 10.1108/09593840910962186.

Hadjsaid, N., Tranchita, C., Rozel, B., Viziteu, M. G. and Caire, R. (2009) 'Modeling cyber and physical interdependencies - Application in ICT and power grids', in *2009 IEEE/PES Power Systems Conference and Exposition, PSCE 2009*. IEEE, pp. 1–6. doi: 10.1109/PSCE.2009.4840183.

Hadžiosmanović, D., Bolzoni, D. and Hartel, P. H. (2012) 'A log mining approach for process monitoring in SCADA', *International Journal of Information Security*, 11, pp. 231–251. doi: 10.1007/s10207-012-0163-8.

Hadžiosmanović, D., Simionato, L., Bolzoni, D., Zambon, E. and Etalle, S. (2012) 'N-gram against the machine: On the feasibility of the N-gram network analysis for binary protocols', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes*

in *Bioinformatics*), 7462 LNCS, pp. 354–373. doi: 10.1007/978-3-642-33338-5_18.

Haehner, J., Rudolph, S., Tomforde, S., Fisch, D., Sick, B., Kopal, N. and Wacker, A. (2013) 'A Concept for Securing Cyber-Physical Systems with Organic Computing Techniques', in *Architecture of Computing Systems (ARCS), Proceedings of 2013 26th International Conference on*. Prague, Czech Republic: IEEE Xplore, p. 1. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6468887>.

Hahn, A., Ashok, A., Sridhar, S. and Govindarasu, M. (2013) 'Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid', *IEEE Transactions on Smart Grid*, 4(2), pp. 847–855. doi: 10.1109/TSG.2012.2226919.

Haimes, Y., Santos, J., Crowther, K., Henry, M., Lian, C. and Yan, Z. (2007) 'Risk analysis in interdependent infrastructures', in Palmer, C. and Shenoi, S. (eds) *IFIP International Federation for Information Processing*. Springer Berlin Heidelberg, pp. 297–310. doi: 10.1007/978-0-387-75462-8_21.

Han, J., Shah, A., Luk, M. and Perrig, A. (2007) *Don't Sweat Your Privacy: Using Humidity to Detect Human Presence*. Available at: http://www.netsec.ethz.ch/publications/papers/han_jain_luk_perrig_privacy.pdf.

Harp, D. and Gregory-Brown, B. (2016) *SANS 2016 State of ICS Security Survey*. Available at: <https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067>.

Hawrylak, P. J., Haney, M., Papa, M. and Hale, J. (2012) 'Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid', in *Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012*. IEEE Xplore, pp. 161–164. doi: 10.1109/ISRCS.2012.6309311.

Henning, R., Abrams, M., Kahn, J., Peoples, D., Vaughn, R., Connolly, J., McHugh, J. and Tippet, J. (2002) 'Information System Security Attribute Quantification or Ordering (Commonly but improperly known as iSecurity Metrics)', in *Workshop on Information Security System Scoring and Ranking*. Silver Spring: Applied Computer Security Associates (ACSA) The MITRE Corporation, pp. 1–70. Available at: <https://www.acsac.org/measurement/proceedings/wissr1-proceedings.pdf>.

Henrie, M. (2013) 'Cyber Security Risk Management in the SCADA Critical Infrastructure Environment', *Engineering Management Journal*, 25(2). Available at: <http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=10429247&AN=93744073&h=mOv0mttB4RJ1LlevmE4RyFehcmPetUWAeFR2I5T5u2DLkO8yuObTaJHLFI2ikas90KNrXGymFLUXwbvK6i+RQQ==&crl=c>.

Henry, M. H. and Haimes, Y. Y. (2009) 'A comprehensive network security risk model for process control networks', *Risk Analysis*, 29(2), pp. 223–248. doi: 10.1111/j.1539-6924.2008.01151.x.

Hershberger, P. (2014) *Security Skills Assessment and Training: The "Make or Break" Critical Security Control*, *SANS Institute InfoSec Reading Room*. Available at: <https://uk.sans.org/reading-room/whitepapers/leadership/security-skills-assessment-training-critical-security-control-break-o-35637>.

Hieb, J., Graham, J. and Guan, J. (2009) 'An ontology for identifying cyber intrusion induced faults in process control systems', in Palmer, C. and Shenoi, S. (eds) *IFIP Advances in Information and Communication Technology*. Springer, IFIP Publications, pp. 125–138. doi: 10.1007/978-3-642-04798-5_9.

HM Government (2015) *2015 Information Security Breaches Report*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.

Holm, H., Ekstedt, M. and Andersson, D. (2012) 'Empirical analysis of system-level vulnerability metrics through actual attacks', *IEEE Transactions on Dependable and Secure Computing*, 9(6), pp. 825–837. doi: 10.1109/TDSC.2012.66.

Holm, H., Karresand, M., Vidstrom, A. and Westring, E. (2015) 'A Survey of Industrial Control System Testbeds', in Buchegger, S. and Dam, M. (eds) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. NordSec 20. Springer International Publishing Switzerland, pp. 11–26. doi: 10.1007/978-3-319-26502-5.

Holm, H., Karresand, M., Vidström, A. and Westring, E. (2015) 'A Survey of Industrial Control System Testbeds', in In: Buchegger S., Dam M. (eds) *Secure IT Systems. Lecture Notes in Computer Science*. Switzerland: Springer, Cham, pp. 11–26. doi: 10.1007/978-3-319-26502-5.

Homeland Security (2009) *Primer Control Systems Cyber Security Framework and Technical Metrics, Primer*. doi: 10.1017/CBO9781107415324.004.

Homer, J., Zhang, S., Ou, X., Schmidt, D., Du, Y., Rajagopalan, S. R. and Singhal, A. (2013) 'Aggregating Vulnerability Metrics in Enterprise Networks using Attack Graphs', *Journal of Computer Security*, 21(4), pp. 561–597. doi: 10.3233/JCS-130475.

Honeywell (2011) *Cyber Security in Manufacturing & Production, Honeywell Int'l Inc., Whitepaper on Advanced solutions*. Available at: https://www.honeywellprocess.com/library/marketing/whitepapers/HoneywellIndustrialCyberSecurity_CyberSecurityinManufacturingandProduction_WP686.pdf.

Hurst, W., Shone, N., Shi, Q. and Bazli, B. (2016) 'Micro-CI: A Critical Systems Testbed for Cyber-Security Research', in *EMERGING 2016: The Eighth International Conference on Emerging Networks and Systems Intelligence*. Venice, Italy: researchonline.ljmu.ac.uk website, pp. 17–22. Available at: <http://researchonline.ljmu.ac.uk/4681/>.

IBM (2013) 'SPSS Statistics for Windows'. IBM. Available at: http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/9/897/ENUS213-309/index.html&lang=en&request_locale=en.

IBM Security (2015) *Security attacks on industrial control systems*. Available at: <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03046USEN&attachment=SEL03046USEN.PDF>.

Ibrahim, O. Al and Nair, S. (2011) 'Cyber-physical security using system-level PUFs', *IWCMC 2011 - 7th International Wireless Communications and Mobile Computing Conference*, pp. 1672–1676. doi: 10.1109/IWCMC.2011.5982786.

ICSJWG (2013) *Protecting Critical Infrastructures from Emerging Cyber Threats Cyber Security by Design*, [Online] at: <https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>. S2013. Available at: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/S2013/Al-Issa_ProtectingCriticalInfrastructuresfromEmergingCyberThreats_s5.pdf.

Igure, V. M., Laughter, S. A. and Williams, R. D. (2006) 'Security issues in SCADA networks',

Computers & Security, 25(7), pp. 498–506. doi: 10.1016/j.cose.2006.03.001.

Ingoldsby, T. R. (2013) *Attack Tree-based Threat Risk Analysis*. Edited by Third. Amenaza Technologies Limited. Available at: www.amenaza.com.

IRM (2015) *Amateyrs attack technology. Professional hackers target people*, Website Article. Available at: <https://www.irmplc.com/issues/human-behaviour/> (Accessed: 15 June 2015).

ISA99 (no date) *ISA-62443 [multiple parts], Security for Industrial Automation and Control Systems*. Research Triangle Park, North Carolina. Available at: http://isa99.isa.org/ISA99Wiki/WP_List.aspx.

Ishiguro, M., Tanaka, H., Matsuura, K. and Murase, I. (2006) 'The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market', in *The Workshop on the Economics of Securing the Information Infrastructure*. CITESEERX, pp. 1–15. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.212.4556&rep=rep1&type=pdf>.

ISO/IEC (2018) *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and Vocabulary*.

ISO/IEC, I. O. for S. E. C. (2013) *ISO/IEC 27001: 2013, Information Technology Standard*. Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en> (Accessed: 2 March 2015).

Jaganathan, V., Cherurveetil, P. and Sivashanmugam, P. M. (2015) 'Using a prediction model to manage cyber security threats', *Scientific World Journal*, 2015, pp. 1–5. doi: 10.1155/2015/703713.

Jajodia, S. and Noel, S. (2010) *Advanced Cyber Attack Modeling , Analysis , and Visualization, Advance Cyber Attack Modelling, Analysis, and visualization*. Rome, New York. Available at: <file:///C:/Users/s234671/Downloads/ADA516716.pdf>.

Jansen, W. (2009) *Directions in Security Metrics Research, NISTIR 7564, National Institute of Standards and Technology*. National Institute of Standards and Technology (NIST). Available at: http://books.google.com/books?hl=en&lr=&id=fXgyeLTsinQC&oi=fnd&pg=PA1&dq=Directions+in+security+metrics+research&ots=Nv2e-BdNnM&sig=_jglZu9krpcof8rj9sxPZQoVDfY%5Cncsrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf?%5Cnhttp://scholar.goo.

Jiang, W., Guo, W. and Sang, N. (2010) 'Periodic Real-Time Message Scheduling for Confidentiality-Aware Cyber-Physical System in Wireless Networks', *2010 Fifth International Conference on Frontier of Computer Science and Technology*, pp. 355–360. doi: 10.1109/FCST.2010.117.

Johansen, G., Allen, L., Heriyanto, T. and Ali, S. (2016) 'Penetration Testing Methodology', in Jain, N., Nair, R., Pandey, K., and Rao, S. (eds) *Kali Linux 2 – Assuring Security by Penetration Testing*. 3rd edn. Birmingham: PACKT Publishing, p. 568. doi: 10.1016/S1353-4858(14)70077-7.

Johansson, E., Sommestad, T. and Ekstedt, M. (2009) 'Issues of cyber security in SCADA-systems-On the importance of awareness', *The 20th International Conference on Electricity Distribution CIRED*, (0969), pp. 1–4. doi: 10.1049/cp.2009.1099.

Jonsson, E. and Pirzadeh, L. (2011) 'A framework for security metrics based on operational system attributes', in *3rd International Workshop on Security Measurements and Metrics, Metrisec*

2011, pp. 58–65. doi: 10.1109/Metrisec.2011.19.

Kao, J. and Marculescu, R. (2007) 'Minimizing eavesdropping risk by transmission power control in multihop wireless networks', *IEEE Transactions on Computers*, 56(8), pp. 1009–1023. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4264318.

Karnouskos, S. (2011) 'Stuxnet worm impact on industrial cyber-physical system security', in Yu, X. and Dillon, T. (eds) *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*. Melbourne: IEEE, pp. 4490–4494. doi: 10.1109/IECON.2011.6120048.

Kaspersky-Labs (2015) *Kaspersky-Labs: Empowering Industrial Cyber Security*. Available at: <http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Empowering-Industrial-Cyber-Security.pdf>.

Kavak, H., Padilla, J. J., Vernon-Bido, D., Gore, R. J. and Diallo, S. Y. (2016) 'A Characterization of Cybersecurity Simulation Scenarios', in *19th Communications and Networking Simulation Symposium (CNS'16)*. CA, USA: Society for Modelling & Simulation International (SCS) & ACM, pp. 1–8.

Keramati, M., Akbari, A. and Keramati, M. (2013) 'CVSS-based security metrics for quantitative analysis of attack graphs', in *Proceedings of the 3rd International Conference on Computer and Knowledge Engineering, ICCKE 2013*. Mashhad, Iran: IEEE Xplore, pp. 178–183. doi: 10.1109/ICCKE.2013.6682816.

Keramati, M. and Keramati, M. (2014) 'Novel security metrics for ranking vulnerabilities in computer networks', in *7th International Symposium on Telecommunications, 2014 IST*. IEEE, pp. 883–888. doi: 10.1109/ISTEL.2014.7000828.

Kheir, N., Cuppens-Boulahia, N., Cuppens, F. and Debar, H. (2010) 'A service dependency model for cost-sensitive intrusion response', in Gritzalis, D., Preneel, B., and Theoharidou, M. (eds) *Computer Security – ESORICS 2010 (LNCS 6345)*. Lecture No. Athens: Springer Berlin Heidelberg, pp. 626–642. doi: 10.1007/978-3-642-15497-3_38.

Kightley, E. P., Reyes-García, V., Demps, K., Magtanong, R. V., Ramenzoni, V. C., Thampy, G., Gueze, M. and Stepp, J. (2013) 'An empirical comparison of knowledge and skill in the context of traditional ecological knowledge', *Journal of Ethnobiology and Ethnomedicine*, 9(1), p. 71. doi: 10.1186/1746-4269-9-71.

King-Turner, M. (2014) *Three Keys to IT System Success: People, Process, Technology (National B2B Centre), The National B2B Centre, UK*. Available at: http://www.nb2bc.co.uk/managing_it_projects/articles/?id=181 (Accessed: 12 August 2015).

Kisner, R. a., Manges, W. W., MacIntyre, L. P., Nutaro, J. J., Munro, J. K., Ewing, P. D., Howlader, M., Kuruganti, P. T., Wallace, R. M. and Olama, M. M. (2010) *Cybersecurity through Real-Time Distributed Control Systems, Energy*. Oak Ridge Tennessee: U.S Department of Energy. Available at: http://www.ornl.gov/sci/electricdelivery/pdfs/ORNL_Cybersecurity_Through_Real-Time_Distributed_Control_Systems.pdf.

Kitchenham, B. A., Pickard, L., Linkman, S. and Jones, P. (2005) 'A framework for evaluating a software bidding model', *Information and Software Technology*, 47(11), pp. 747–760. doi: 10.1016/j.infsof.2004.05.005.

Klahr, R., Amili, S., Shah, J. N., Button, M. and Wang, V. (2016) *Cyber Security Breaches Survey 2016, Cyber Security Breaches Survey 2016*. London. doi: 10.13140/RG.2.1.4332.6324.

- Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. and Jones, K. (2015) 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection*. Elsevier, 9, pp. 52–80. doi: 10.1016/j.ijcip.2015.02.002.
- Konidaris, G., Kaelbling, L. and Lozano-Perez, T. (2014) 'Constructing Symbolic Representations for High-Level Planning', in *Conference on Artificial Intelligence*. Association for the Advancement of Artificial Intelligence, pp. 1932–1940. Available at: http://people.csail.mit.edu/gdk/pubs/orig_sym_aaai.pdf.
- Korkmaz, E., Dolgikh, A., Davis, M. and Skormin, V. (2016) 'Industrial Control Systems Security Testbed', in *11th Annual Symposium on Information Assurance (Asia '16)*. Albany, NY: www.albany.edu website, pp. 13–18. Available at: http://www.albany.edu/iasymposium/proceedings/2016/04_Korkmaz_etal_ASIA2016.pdf.
- Kotenko, I. and Chechulin, A. (2013) 'A Cyber Attack Modeling and Impact Assessment Framework', in *5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, pp. 1–24. Available at: <http://ccdcoe.org/429.html>.
- Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D. (2013) 'Cascading Effects of Common-Cause Failures in Critical Infrastructures', in Butts, J. and Shenoi, S. (eds) *Critical Infrastructure Protection VII*. Series Vol. Berlin Heidelberg: Springer Berlin Heidelberg, pp. 171–182. doi: 10.1007/978-3-642-45330-4_12.
- Krotofil, M. and Gollmann, D. (2013) 'Industrial control systems security: What is happening?', *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, pp. 664–669. doi: 10.1109/INDIN.2013.6622963.
- Kuhl, M. E., Kistner, J., Costantini, K. and Sudit, M. (2007) 'Cyber Attack Modelling And Simulation For Network Security Analysis', in Henderson, S. G., Biller, B., Hsieh, M.-H., Shortle, J., Tew, J. D., and Barton, R. R. (eds) *Proceedings of the 2007 Winter Simulation Conference*. IEEE Xplore, pp. 1180–1188.
- Kundur, D., Feng, X., Liu, S., Zourtos, T. and Butler-Purry, K. L. (2010) 'Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid', in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Gaithersburg, Maryland: IEEE, pp. 244–249. doi: 10.1109/SMARTGRID.2010.5622049.
- Kwon, C., Liu, W. and Hwang, I. (2013) 'Security analysis for Cyber-Physical Systems against stealthy deception attacks', in *2013 American Control Conference*. Washington DC: IEEE Xplore, pp. 3344–3349. doi: 10.1109/ACC.2013.6580348.
- Kwon, J. and Johnson, M. E. (2015) *PROACTIVE VS. REACTIVE SECURITY INVESTMENTS IN THE HEALTHCARE SECTOR*, *Reseach*. doi: 10.1017/CBO9781107415324.004.
- Lai, Y.-P. and Hsia, P.-L. (2007) 'Using the vulnerability information of computer systems to improve the network security', *Computer Communications*, 30(9), pp. 2032–2047. doi: 10.1016/j.comcom.2007.03.007.
- Larkin, R. D., Lopez Jr., J., Butts, J. W. and Grimaila, M. R. (2014) 'Evaluation of Security Solutions in the SCADA Environment', *Data Base for Advances in Information Systems*, 45(1), pp. 38–53. doi: 10.1145/2591056.2591060.
- Lee, R. M., Assante, M. J. and Conway, T. (2014) *German Steel Mill Cyber Attack*. Available at: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

- Lei, C., Ma, D. H., Zhang, H. Q. and Wang, L. M. (2016) 'Moving target network defense effectiveness evaluation based on change-point detection', *Mathematical Problems in Engineering*, 2016, pp. 1–11. doi: 10.1155/2016/6391502.
- LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H. and Muehrcke, C. (2011) 'Model-based security metrics using ADversary Vlew Security Evaluation (ADVISE)', in *8th International Conference on Quantitative Evaluation of Systems, QEST 2011*. IEEE, pp. 191–200. doi: 10.1109/QEST.2011.34.
- Leyden, J. (2012) *Hack on Saudi Aramco hit 30,000 workstations, oil firm admits.*, [online] at: [Theregister.co.uk](http://www.theregister.co.uk). Available at: http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/ (Accessed: 30 March 2015).
- Leyden, J. (2018) 'Now Meltdown patches are making industrial control systems lurch', *The Register*, January.
- Li, H., Xi, R. and Zhao, L. (2015) 'Study on the distribution of CVSS environmental score', in *ICEIEC 2015 - Proceedings of 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*. Beijing, China: IEEE, pp. 122–125. doi: 10.1109/ICEIEC.2015.7284502.
- Li, Y., Shi, L., Cheng, P., Chen, J. and Quevedo, D. E. (2013) 'Jamming attack on Cyber-Physical Systems: A game-theoretic approach', in *2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*. Nanjing, China: IEEE Xplore, pp. 252–257. doi: 10.1109/CYBER.2013.6705454.
- Lin, F. Y. S., Wang, Y. S. and Huang, M. Y. (2013) 'Effective proactive and reactive defense strategies against malicious attacks in a virtualized honeynet', *Journal of Applied Mathematics*, 2013, pp. 1–11. doi: 10.1155/2013/518213.
- Linkov, I., Eisenberg, D. ., Plourde, K., Seager, T. ., Allen, J. and Kott, A. (2013) 'Resilience metrics for cyber systems', *Environment Systems and Decisions*, 33(4), pp. 471–476. doi: 10.1007/s10669-013-9485-y.
- Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. and Seager, T. (2013) 'Measurable Resilience for Actionable Policy', *Environmental Science and Technology*, (ii), pp. 10108–10110. Available at: <http://pubs.acs.org/doi/ipdf/10.1021/es403443n>.
- Lu, T., Guo, X., Li, Y., Peng, Y., Zhang, X., Xie, F. and Gao, Y. (2014) 'Cyber-Physical Security for Industrial Control Systems Based on Wireless Sensor Networks', *Downloads.Hindawi.Com*, 2014. doi: 10.1155/2014/438350.
- Lu, T., Xu, B., Guo, X., Zhao, L. and Xie, F. (2013) 'A New Multilevel Framework for Cyber-Physical System Security', in *First International Workshop on the Swarm at the Edge of the Cloud (SEC'13 @ ESWeek)*. Montreal: The TerraSwarm Research Center, pp. 2–3. Available at: http://www.terraswarm.org/pubs/136/lu_newmultiframe_edge.pdf.
- Lu, T., Zhao, J., Zhao, L., Li, Y. and Zhang, X. (2015) 'Towards a Framework for Assuring Cyber Physical System Security', 9(3), pp. 25–40.
- Luders, S. (2006) 'CERN Tests reveal Security flaws with Industrial Networked Devices', *Industrial Ethernet Book*, (35), p. 12-.
- Macaulay, T. and Singer, B. L. (2012) 'ICS Vulnerabilities', in *Cybersecurity for Industrial Control*

Systems: SCADA, DCS, PLC, HMI, and SIS. Boca Raton, FL: CRC PRESS : Taylor & Francis Group, pp. 81–124. Available at: <https://www.crcpress.com/Cybersecurity-for-Industrial-Control-Systems-SCADA-DCS-PLC-HMI-and/Macaulay-Singer/9781439801963>.

MacDermott, Á., Shi, Q., Merabti, M. and Kifayat, K. (2012) 'Intrusion Detection for Critical Infrastructure Protection', *Cms.Livjm.Ac.Uk*. Available at: <http://www.cms.livjm.ac.uk/pgnet2012/Proceedings/Papers/1569604987.pdf>.

Madden, J., McMillin, B. and Sinha, A. (2010) 'Environmental obfuscation of a Cyber Physical System - Vehicle example', in *Proceedings of the 34th IEEE Annual International Computer Software and Applications Conference*. IEEE, pp. 176–181. doi: 10.1109/COMPSACW.2010.39.

Maize, K. (2014) *Just Hop on the Bus, Gus: 13 Ways to Hack a Power Plant*, [online] at <http://www.powermag.com/>. Available at: <http://www.powermag.com/just-hop-on-the-bus-gus-13-ways-to-hack-a-power-plant/?printmode=1> (Accessed: 6 April 2015).

Majdalawieh, M., Parisi-Presicce, F. and Wijesekera, D. (2006) 'DNPsec: Distributed Network Protocol Version 3 (DNP3) Security Framework', in Elleithy, K., Sobh, T., Mahmood, A., Iskander, M., and Karim, M. (eds) *Advances in Computer, Information, and Systems Sciences, and Engineering*. Springer Netherlands, pp. 227–234. doi: 10.1007/1-4020-5261-8_36.

Mander, T., Nabhani, F., Wang, L. and Cheung, R. (2007) 'Integrated Network Security Protocol Layer for Open-Access Power Distribution Systems', in *IEEE Power Engineering Society General Meeting, 2007*. IEEE, pp. 1–8. doi: 10.1109/PES.2007.386070.

Mandiant (2013) *APT1: Exposing One of China's Cyber Espionage Units*. Available at: <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

Manikandan, S. (2011) 'Measures of central tendency: The mean', *Journal of Pharmacology and Pharmacotherapeutics*, 2(2), p. 140. doi: 10.4103/0976-500X.81920.

Markovic-Petrovic, J. D. and Stojanovic, M. D. (2014) 'An improved risk assessment method for SCADA information security', *Elektronika ir Elektrotechnika*, 20(7), pp. 69–72. doi: 10.5755/j01.eee.20.7.8027.

Mathur, A. P. and Tippenhauer, N. O. (2016) 'SWaT: A water treatment testbed for research and training on ICS security', in *2016 International Workshop on Cyber-physical Systems for Smart Water Networks, CySWater 2016*. Vienna, Austria: IEEE, pp. 31–36. doi: 10.1109/CySWater.2016.7469060.

McMillen, D. (2016) *Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent*, *Securityintelligence.com Website*. Available at: <https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/> (Accessed: 7 August 2017).

McMillin, B. (2009) 'Complexities of information security in cyber-physical power systems', in *2009 IEEE/PES Power Systems Conference and Exposition, PSCE 2009*. IEEE. doi: 10.1109/PSCE.2009.4840093.

McQueen, M. A., Boyer, W. F., Flynn, M. A. and Beitel, G. A. (2006) 'Quantitative cyber risk reduction estimation methodology for a small SCADA control system', in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Kauia, HI, USA, USA: IEEE, p. 226. doi: 10.1109/HICSS.2006.405.

McQueen, M., Boyer, W., McBride, S., Farrar, M. and Tudor, Z. (2008) *Measurable Control System*

Security Through Ideal Driven Technical Metrics SCADA Security Scientific Symposium, Security. INL/CON-07-13581. Available at: <http://www.inl.gov/technicalpublications/Documents/3881671.pdf>.

Mell, P., Scarfone, K. and Romanosky, S. (2007) 'A Complete Guide to the Common Vulnerability Scoring System Version 2.0', *FIRSTForum of Incident Response and Security Teams*, pp. 1–23. Available at: <https://www.first.org/cvss/cvss-v2-guide.pdf>.

Méndez, A. C., Fernández-Navarro, F., Gutiérrez, P. A., Baena-García, M. and Hervás-Martínez, C. (2011) 'Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011', *Advances in Intelligent and Soft Computing*, 87(March), pp. 263–270. doi: 10.1007/978-3-642-19644-7.

Metke, A. R. and Ekl, R. L. (2010) 'Security technology for smart grid networks', *IEEE Transactions on Smart Grid*, 1(1), pp. 99–107. doi: 10.1109/TSG.2010.2046347.

Miller, B. and Rowe, D. (2012) 'A survey SCADA of and critical infrastructure incidents', *Proceedings of the 1st Annual conference on Research in information technology - RIIT '12*, p. 51. doi: 10.1145/2380790.2380805.

Mirashe, S. P. and Kalyankar, N. V (2010) 'Cloud Computing', *Communications of the ACM*. Edited by N. Antonopoulos and L. Gillam. ACM (Informatik im Fokus), 51(7), p. 9. doi: 10.1145/358438.349303.

Mitchell, R. and Chen, I.-R. (2013) 'Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems', *IEEE Transactions on Reliability*, 62(1), pp. 199–210. doi: 10.1109/TR.2013.2240891.

Mitchell, R. and Chen, I. R. (2011) 'A hierarchical performance model for intrusion detection in cyber-physical systems', in *2011 IEEE Wireless Communications and Networking Conference, WCNC 2011*. IEEE Xplore, pp. 2095–2100. doi: 10.1109/WCNC.2011.5779477.

Mix, S. (2003) *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide*.

Mo, B. Y., Kim, T. H., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B. (2011) 'Cyber – Physical Security of a Smart Grid Infrastructure', *Proceedings of the IEEE*, 100(1), pp. 1–15. doi: 10.1109/JPROC.2011.2161428.

Morgan, L. (2014) *List of cyber attacks and data breaches in 2014*, [Online] at <http://www.itgovernance.co.uk>. Available at: <http://www.itgovernance.co.uk/blog/list-of-the-hacks-and-breaches-in-2014/> (Accessed: 3 April 2015).

Muessig, P. R., Laack, D. R. and Wroblewski, J. J. (2001) *An Integrated Approach To Evaluating Simulation Credibility, Unclassified Research Update Report*. California. Available at: <http://www.dtic.mil/dtic/tr/fulltext/u2/a405051.pdf>.

Musliner, D. J., Friedman, S. E., Marble, T., Rye, J. M., Boldt, M. W. and Pelican, M. (2014) 'Self-Adaptation metrics for active cybersecurity', in *Proceedings - IEEE 7th International Conference on Self-Adaptation and Self-Organizing Systems Workshops, SASOW 2013*. Washington, DC.: IEEE Computer Society, pp. 53–58. doi: 10.1109/SASOW.2013.31.

Navarro, L. (2007) 'Train employees - your best defense - for security awareness', *SC Magazine Online*. Available at: <http://www.scmagazine.com/train-employees-your-best-defense-for-security-awareness/article/34589/>.

Neg, R., Kumar, A., Shukla, S. K. and Dayal, A. (2016) 'A SCADA test bed For Cyber Security Education & Research'. Cyber Security Centre, Indian Institute of Technology, Kanpur, pp. 1–16. Available at: https://security.cse.iitk.ac.in/sites/default/files/title_page_2.pdf.

Nguyen, D. N. (2012) *Security Metrics in SCADA System*. University of South Australia School. Available at: <https://wiki.cis.unisa.edu.au/wiki/images/0/0a/Ngudy041-minorthesis.pdf>.

Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012a) 'SCADA security in the light of cyber-warfare', *Computers and Security*, 31, pp. 418–436. doi: 10.1016/j.cose.2012.02.009.

Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012b) 'SCADA security in the light of Cyber-Warfare', *Computers & Security*, 31(4), pp. 418–436. doi: 10.1016/j.cose.2012.02.009.

NIST (2004) *Standards for security categorization of federal information and information systems, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*. Gaithersburg, Maryland. doi: 10.6028/NIST.FIPS.199.

NIST (2012) *Guide for Conducting Risk Assessments, NIST Special Publication*. Gaithersburg, Maryland. doi: 10.6028/NIST.SP.800-30r1.

NIST (2013a) 'Glossary of Key Information Security Terms', *NISTIR 7298*. National Institute of Standards and Technology (NIST), p. 222. doi: 10.6028/NIST.IR.7298r2.

NIST (2013b) *Security and Privacy Controls for Federal Information Systems and Organizations, SP-800-53A Rev 4*. National Institute of Standards and Technology (NIST). doi: 10.6028/NIST.SP.800-53Ar4.

NIST, N. I. of S. and T. (2014) *Framework for Improving Critical Infrastructure Cybersecurity*. Available at: <http://www.nist.gov/cyberframework/>.

Northcutt, S. (2014) *Breaches Happen : Be Prepared*. Available at: <https://www.sans.org/reading-room/whitepapers/riskmanagement/breaches-happen-prepared-35527>.

Nourian, A. and Madnick, S. (2014) 'A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet', *Systems Journal*, (September), pp. 1–12. Available at: <http://ic3.mit.edu/ResearchSamples/2014-13.pdf>.

NSA (2010) *A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)*. National Security Agency, U.S.A. Available at: https://scadahacker.com/library/Documents/Assessment_Guidance/NSA - Framework for Assessing and Improving Security Posture of ICS.pdf.

O'Neill, P. (2013) 'Protecting Critical Infrastructure by Identifying Pathways of Exposure to Risk', *Technology Innovation Management Rev*, (August), pp. 34–40. Available at: <http://timreview.ca/article/714>.

Ou, X., Govindavajhala, S. and Appel, A. W. (2005) 'MuIVAL: a logic-based network security analyzer', in *Proceedings of the 14th conference on USENIX Security Symposium - Volume 14*. Baltimore: ACM, pp. 8–8. Available at: https://www.usenix.org/legacy/events/sec05/tech/full_papers/ou/ou.pdf?CFID=800680043&CFTOKEN=80073812.

Ozturk, M. and Aubin, P. (2011) *SCADA Security: Challenges and Solutions*. Ontario-Canada. Available at: <http://www2.schneider-electric.com/documents/support/cybersecurity/WP->

SCADA Security-schneider-electric.pdf.

PA Consulting Group (2015) *Security for Industrial Control Systems: Framework Overview - A Good Practice Guide*. London: The Crown. doi: Retrieved June 30, 2015, from http://www.21stcenturyskills.org/index.php?option=com_content&task=view&id=254&Itemid=120.

Pan, S., Morris, T. H., Adhikari, U. and Madani, V. (2013) 'Causal event graphs cyber-physical system intrusion detection system', in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. ACM, pp. 1–4. doi: 10.1145/2459976.2460022.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers and Security*. Elsevier Ltd, 42, pp. 165–176. doi: 10.1016/j.cose.2013.12.003.

Parvin, S., Hussain, F. K., Hussain, O. K., Thein, T. and Park, J. S. (2013) 'Multi-cyber framework for availability enhancement of cyber physical systems', *Computing*, 95(10–11), pp. 927–948. doi: 10.1007/s00607-012-0227-7.

Pasqualetti, F., Dorfler, F. and Bullo, F. (2011) 'Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design', in *Proceedings of the IEEE Conference on Decision and Control*. IEEE, pp. 2195–2201. doi: 10.1109/CDC.2011.6160641.

Pasqualetti, F., Dorfler, F. and Bullo, F. (2015) 'Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems', *IEEE Control Systems*, 35(1), pp. 110–127. doi: 10.1109/MCS.2014.2364725.

Pasqualetti, F., Dörfler, F. and Bullo, F. (2013) 'Attack Detection and Identification in Cyber-Physical Systems', *IEEE Transactions on Automatic Control*, 58(11), pp. 2715–2729.

Paul (2014) *Cyberattack Inflicts Massive Damage on German Steel Factory*, [online] at: <https://securityledger.com>. Available at: <https://securityledger.com/2014/12/cyberattack-inflicts-massive-damage-on-german-steel-factory/> (Accessed: 30 March 2015).

Paul, C. L. and Whitley, K. (2013) 'A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness', in Marinos, L. and Askoxylakis, I. (eds) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer, Berlin, Heidelberg, pp. 145–154. doi: 10.1007/978-3-642-39345-7-16.

Payne, S. C. (2006) *A Guide to Security Metrics*, SANS Security Essentials G EC Practical Assignment Version 1.2e. SANS Institute. Available at: <https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55>.

Perumal, T. (2014) 'Research Methodology', *Course Material*. Open University Malaysia, pp. 87–104. Available at: http://www.tankonyvtar.hu/en/tartalom/tamop412A/2011-0021_22_research_methodology/course_guide.html.

Pescatore, J. (2017) *Back to Basics: Focus on the First Six Critical Security Controls*. Available at: <https://www.sans.org/reading-room/whitepapers/analyst/basics-focus-first-cis-critical-security-controls-37537>.

Peuhkurinen, K. (2008) 'Plans for a Balanced Scorecard Approach to Information Security Metrics', in *MetriCon* 3.0. San Jose, CA. Available at:

<http://www.securitymetrics.org/attachments/Metricon-3-Peuhkurinen.pdf>.

Pham, N., Abdelzaher, T. and Nath, S. (2010) 'On Bounding Data Stream Privacy in Distributed Cyber-physical Systems', *2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 221–228. doi: 10.1109/SUTC.2010.74.

PWC (2013) 'Embedding cyber security into the energy ecosystem: An integrated approach to assessing cyber threats and protecting your assets', *White Paper*, (February), pp. 1–16. Available at: <https://www.pwc.com/gx/en/oil-gas-energy/publications/assets/pwc-embedding-cyber-security-into-the-energy-ecosystem-pdf.pdf>.

Radack, S. (2011) 'Protecting Industrial Control Systems - Key Components of Our Nations Critical Infrastructures', *ITL Bulletin*, August, pp. 1–7. Available at: <http://csrc.nist.gov/publications/nistbul/August-200-ITL-Bulletin.pdf>.

Ralston, P. A. S., Graham, J. H. and Hieb, J. L. (2007) 'Cyber security risk assessment for SCADA and DCS networks.', *ISA transactions*, 46(4), pp. 583–94. doi: 10.1016/j.isatra.2007.04.003.

Rapid7 (2017) *Top Rated Vulnerability Management Software | Rapid7*, *Rapid7 website*. Available at: <https://www.rapid7.com/products/nexpose/> (Accessed: 11 October 2017).

Rautmare, S. (2011) 'SCADA System Security: Challenges and Recommendations', in Negi, A., Narayana, M. G. P. L., Rao, N. V., Narayana, M. L., Vemuri, P., Rao, K. D., Sarma, D. S., Kumar, A., and Devarapalli, H. (eds) *2011 Annual IEEE India Conference (INDICON)*. Hyderabad, India: IEE, pp. 1–4. doi: 10.1109/INDCON.2011.6139567.

Reichert, P., Borsuk, M., Hostmann, M., Schweizer, S., Sp??rri, C., Tockner, K. and Truffer, B. (2007) 'Concepts of Decision Support for River Rehabilitation', *Environmental Modelling and Software*, 22(2), pp. 188–201. doi: 10.1016/j.envsoft.2005.07.017.

Reyes-García, V., McDade, T., Vadez, V., Huanca, T., Leonard, W. R., Tanner, S. and Godoy, R. (2008) 'Non-market returns to traditional human capital: Nutritional status and traditional knowledge in a native amazonian society', *Journal of Development Studies*, 44(2), pp. 217–232. doi: 10.1080/00220380701789901.

Ridley, G., Young, J. and Carroll, P. (2004) 'COBIT and its utilization: a framework from the literature', in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. HI, USA: IEEE, pp. 1–8. doi: 10.1109/HICSS.2004.1265566.

Robson, C. and McCartan, K. (2015) *Real World Research*. 4th Editio. UK: John Wiley and Sons.

Roland-Berger (2015) *Think Act: Cyber-Security, Managing threat Scenarios in manufacturing companies*. Munich. Available at: https://www.rolandberger.com/media/pdf/Roland_Berger_TAB_Cyber_Security_20150305.pdf.

Rozel, B., Viziteu, M., Caire, R., Hadjsaid, N. and Rognon, J. P. (2008) 'Towards a common model for studying critical infrastructure interdependencies', in *IEEE Power and Energy Society 2008 General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*. IEEE, pp. 1–6. doi: 10.1109/PES.2008.4596465.

Rrushi, J. and Campbell, R. (2009) 'Detecting cyber attacks on nuclear power plants', *Critical Infrastructure Protection II*, 290, pp. 41–54. Available at: http://link.springer.com/chapter/10.1007/978-0-387-88523-0_4.

- Rrushi, J. L. (2011) 'An exploration of defensive deception in industrial communication networks', *International Journal of Critical Infrastructure Protection*, 4, pp. 66–75. doi: 10.1016/j.ijcip.2011.06.002.
- Rrushi, J. L. (2012) 'SCADA protocol vulnerabilities', in *Critical Infrastructure Protection*. Heidelberg: Springer-Verlag Berlin, pp. 150–176.
- Rungger, M. and Tabuada, P. (2013) 'A Notion of Robustness for Cyber-Physical Systems', pp. 1–27. Available at: <http://arxiv.org/abs/1310.5199>.
- Rungger, M. and Tabuada, P. (2014) 'Abstracting and refining robustness for cyber-physical systems', *Proceedings of the 17th international conference on Hybrid systems: computation and control - HSCC '14*, pp. 223–232. doi: 10.1145/2562059.2562133.
- Ryan, S. and O'Connor, R. V. (2009) 'Development of a team measure for tacit knowledge in software development teams', *Journal of Systems and Software*. Elsevier Inc., 82(2), pp. 229–240. doi: 10.1016/j.jss.2008.05.037.
- Ryle, G. (2009) *The Concept of Mind*. 60th Anniv, *Re-published Edition*. 60th Anniv. London and New York: Routledge Taylor & Francis. doi: 10.7208/chicago/9780226922652.001.0001.
- Sadeghi, A.-R., Wachsmann, C. and Waidner, M. (2015) 'Security and Privacy Challenges in Industrial Internet of Things', in *52nd Annual Design Automation Conference on - DAC '15*. San Francisco, CA, USA: ACM, pp. 1–6. doi: 10.1145/2744769.2747942.
- Saltzman, R. and Sharabani, A. (2009) *Active man in the middle attacks : A Security Advisory, IBM Rational Application Security Group White Paper*. Available at: <http://www.security-science.com/pdf/active-man-in-the-middle.pdf%5Cnpapers2://publication/uuid/86ED7095-6BDA-4141-94A0-467236EE1BB8>.
- Sargent, R. G. (2010) 'VERIFICATION AND VALIDATION OF SIMULATION MODELS', in *Proceedings of the 2010 Winter Simulation Conference*. IEEE, pp. 166–183. doi: 10.1109/WSC.2010.5679148.
- Savola, R. and Abie, H. (2009) 'Development of Measurable Security for a Distributed Messaging System', *International Journal on Advances in Security*, 2(4), pp. 358–380. doi: 10.1109/SECURWARE.2009.26.
- Savola, R. M. (2007) 'Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry', in *International Conference on Software Engineering Advances (ICSEA 2007)*. IEEE Computer Society, pp. 60–60. doi: 10.1109/ICSEA.2007.79.
- Savola, R. M. (2009) 'A security metrics development method for software intensive systems', *Communications in Computer and Information Science*, 36, pp. 11–16. doi: 10.1007/978-3-642-02633-1_2.
- Savola, R. M. and Abie, H. (2009) 'Development of security metrics for a distributed messaging system', in *2009 International Conference on Application of Information and Communication Technologies, AICT 2009*. IEEE, pp. 1–6. doi: 10.1109/ICAICT.2009.5372566.
- Savola, R. M. and Abie, H. (2013) 'Metrics-Driven Security Objective Decomposition for an E-Health Application with Adaptive Security Management', in *International Workshop on Adaptive Security Article No. 6*. New York: ACM New York, pp. 1–8. doi: 10.1145/2523501.2523507.

- Schechter, S. E. (2004) *Computer Security: A Quantitative Approach*. Harvard University, Cambridge. Available at: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/thesis-6.pdf>.
- Schnaubelt, C. M., Larson, E. B. and Boyer, M. E. (2014) 'Vulnerability Assessment Method Pocket Guide', *Small Wars Journal*, pp. 2–3. Available at: http://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf.
- Schneider, F. B. (2003) 'Enforceable security policies', *Foundations of Intrusion Tolerant Systems, 2003 [Organically Assured and Survivable Information Systems]*, 3(1), pp. 30–50. doi: 10.1109/FITS.2003.1264930.
- Seeber, S., Sehgal, A., Stelte, B., Rodosek, G. D. and Schonwalder, J. (2013) 'Towards a trust computing architecture for RPL in Cyber Physical Systems', in *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*. Zurich: IEEE Xplore, pp. 134–137. doi: 10.1109/CNSM.2013.6727823.
- Sgouras, K. I., Birda, A. D. and Labridis, D. P. (2014) 'Cyber attack impact on critical Smart Grid infrastructures', in *2014 IEEE PES Innovative Smart Grid Technologies Conference, ISGT 2014*. IEEE, pp. 1–5. doi: 10.1109/ISGT.2014.6816504.
- Shandilya, V., Simmons, C. B. and Shiva, S. (2014) 'Use of attack graphs in security systems', *Journal of Computer Networks and Communications*, 2014. doi: 10.1155/2014/818957.
- Shaw, W. T. (2006) 'INTRODUCTION TO SCADA SYSTEMS SECTION 1: The Technological Evolution of SCADA Systems', in *Cyber*. Oklahoma: PennWell Corporation, pp. 1–22. Available at: Google ebooks.
- Sheng, S., Chan, W. L., Li, K. K., Xianzhong, D. and Xiangjun, Z. (2007) 'Context information-based cyber security defense of protection system', *IEEE Transactions on Power Delivery*, 22(3), pp. 1477–1481. doi: 10.1109/TPWRD.2006.886775.
- Sheyner, O., Haines, J., Jha, S., Lippmann, R. and Wing, J. M. (2002) 'Automated generation and analysis of attack graphs', in *Proceedings - IEEE Symposium on Security and Privacy*. Berkeley, CA, USA: IEEE Computer Society, pp. 273–284. doi: 10.1109/SECPRI.2002.1004377.
- Shin, J., Son, H. and Heo, G. (2017) 'Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET', *Nuclear Engineering and Technology*. Elsevier B.V., 49(3), pp. 517–524. doi: 10.1016/j.net.2016.11.004.
- Shu, X., Tian, K., Ciambrone, A. and Yao, D. (2017) *Breaking the Target: An Analysis of Target Data Breach and Lessons Learned*. Available at: <https://arxiv.org/pdf/1701.04940.pdf>.
- Shyamasundar, R. K. (2013) 'Security and Protection of SCADA: A Bigdata Algorithmic Approach', in *Proceedings of the 6th International Conference on Security of Information and Networks*. New York, New York, USA: ACM, pp. 20–27. doi: 10.1145/2523514.2523595.
- Singhal, A. and Ou, X. (2011) *Security risk analysis of enterprise networks using probabilistic attack graphs*. Gaithersburg, Maryland. doi: 10.6028/nist.ir.7788.
- Siponen, M., Adam Mahmood, M. and Pahlila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information and Management*. Elsevier B.V., 51(2), pp. 217–224. doi: 10.1016/j.im.2013.08.006.

Snowdon, P. (2004) 'The Presidential Address: Knowing How and Knowing That: A Distinction Reconsidered', *Proceedings of the Aristotelian Society*, 104, pp. 1–29. Available at: https://www.jstor.org/stable/4545403?seq=1#page_scan_tab_contents.

Song, J.-G., Lee, J.-W., Lee, C.-K., Kwon, K.-C. and Lee, D.-Y. (2012) 'A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants', *Nuclear Engineering and Technology*, 44(8), pp. 919–928. doi: <http://dx.doi.org/10.5516/NET.04.2011.065>.

Soupionis, Y. and Benoist, T. (2015) 'Cyber-Physical Testbed - The Impact of Cyber Attacks and the Human Factor', in *The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)*. London, UK: IEEE, pp. 326–331. doi: 10.1109/ICITST.2015.7412114.

Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S. and Adhikari, U. (2013) 'Modeling cyber-physical vulnerability of the smart grid with incomplete information', *IEEE Transactions on Smart Grid*, 4(1), pp. 235–244. doi: 10.1109/TSG.2012.2232318.

Stallings, W. (2010) *Cryptography and network security: principles and practice*. 5th Editio. Upper Saddle River, NY: Pearson Education, Inc., publishing as Prentice Hall. I. Available at: [http://faculty.mu.edu.sa/public/uploads/1360993259.0858Cryptography and Network Security Principles and Practice, 5th Edition.pdf](http://faculty.mu.edu.sa/public/uploads/1360993259.0858Cryptography%20and%20Network%20Security%20Principles%20and%20Practice,5th%20Edition.pdf).

Stamp, J., McIntyre, A. and Ricardson, B. (2009) 'Reliability impacts from cyber attack on electric power systems', *2009 IEEE/PES Power Systems Conference and Exposition, PSCE 2009*, pp. 1–8. doi: 10.1109/PSCE.2009.4840054.

Stelte, B. and Rodosek, G. D. (2013) 'Assuring trustworthiness of sensor data for cyber-physical systems', *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*, pp. 395–402.

Stewart, M. G. (2010) 'Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure', *International Journal of Critical Infrastructure Protection*. Elsevier B.V., 3(1), pp. 29–40. doi: 10.1016/j.ijcip.2009.09.001.

Stoddard, M., Carlson, R., Haimes, Y., Bodeau, D., Lian, C., Santos, J., Glantz, C. and Shaw, J. (2005) *Process Control System Security Metrics – State of Practice*. Institute for Information Infrastructure Protection (I3P). Available at: https://www.researchgate.net/publication/228337301_Process_Control_System_Security_Metrics_State_of_Practice.

Stouffer, K., Falco, J. and Scarfone, K. (2011) 'Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology', *NIST Special Publication*, pp. 1–157. Available at: [http://industryconsulting.org/pdfFiles/NIST Draft-SP800-82.pdf](http://industryconsulting.org/pdfFiles/NIST_Draft-SP800-82.pdf).

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. (2015) *Guide to Industrial Control Systems (ICS) Security - NIST.SP.800-82r2*. Available at: <http://dx.doi.org/10.6028/NIST.SP.800-82r2>.

Symantec (2017) 'Triton: New Malware Threatens Industrial Safety Systems | Symantec Blogs'. Symantec. Available at: <https://www.symantec.com/blogs/threat-intelligence/triton-malware-ics> (Accessed: 20 December 2017).

Symantec Corporation (2015) *Internet Security Threat Report*. Mountain View, CA. Available at:

https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Tabuada, P., Caliskan, S. Y., Rungger, M. and Majumdar, R. (2014) 'Towards Robustness for Cyber-Physical Systems', *IEEE Transactions on Automatic Control*, 59(12), pp. 3151–3163. doi: 10.1109/TAC.2014.2351632.

Tang, H. and McMillin, B. M. (2008) 'Security property violation in CPS through timing', in *International Conference on Distributed Computing Systems*. Beijing, China: IEEE, pp. 519–524. doi: 10.1109/ICDCS.Workshops.2008.79.

Tang, L.-A., Yu, X., Kim, S., Han, J., Hung, C.-C. and Peng, W.-C. (2010) 'Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems', *2010 IEEE International Conference on Data Mining*, pp. 1079–1084. doi: 10.1109/ICDM.2010.63.

Tekeoglu, A. and Tosun, A. Ş. (2017) 'A Testbed for Security and Privacy Analysis of IoT Devices', *Proceedings - 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2016*, pp. 343–348. doi: 10.1109/MASS.2016.051.

Telang, R. and Wattal, S. (2007) 'An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price', *IEEE Transactions on Software Engineering*, 33(8), pp. 544–557. doi: 10.1109/TSE.2007.70712.

Ten, C. W., Manimaran, G. and Liu, C. C. (2010) 'Cybersecurity for critical infrastructures: Attack and defense modeling', *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*. IEEE, 40(4), pp. 853–865. doi: 10.1109/TSMCA.2010.2048028.

Tenable, I. (2017) *Nessus Professional | Tenable™, Tenable Nessus Website*. Available at: <http://www.tenable.com/products/nessus-vulnerability-scanner/nessus-professional> (Accessed: 11 October 2017).

The Open Group (2012) 'Dependency Modeling (O-DM): Constructing a Data Model to Manage Risk and Build Trust between Inter-Dependent Enterprises'. Reading, Berkshire, UK: The Open Group, pp. 1–50. Available at: <https://publications.opengroup.org/downloadable/download/link/id/MC45MTQ2MTgwMCAxNTE1NjgxOTMwNjgyMTI3NDc1NDU3Ng,/>.

The Open University (2016) *Models and modelling*. Walton Hall, Milton Keynes, UK. Available at: <http://openlearn.open.ac.uk/mod/oucontent/view.php?id=397581&section=3.1>.

Theoharidou, M., Kotzanikolaou, P. and Gritzalis, D. (2010) 'A multi-layer Criticality Assessment methodology based on interdependencies', *Computers and Security*, 29(6), pp. 643–658. doi: 10.1016/j.cose.2010.02.003.

Tobias, S. (2014) *2014: The Year in Cyberattacks*, *Newsweek*. Available at: <http://www.newsweek.com/2014-year-cyber-attacks-295876> (Accessed: 23 November 2016).

Tran, T. T., Shin, O. S. and Lee, J. H. (2013) 'Detection of replay attacks in smart grid systems', in *2013 International Conference on Computing, Management and Telecommunications, ComManTel 2013*. Ho Chi Minh City, Vietnam: IEEE Xplore, pp. 298–302. doi: 10.1109/ComManTel.2013.6482409.

Tupakula, U. and Varadharajan, V. (2014) 'Techniques for detecting attacks on critical infrastructure', in *Computing, Networking and IEEE*, pp. 48–52. doi:

10.1109/ICCNC.2014.6785303.

Tupper, M. and Zincir-Heywood, A. N. (2008) 'VEA-bility security metric: A network security analysis tool', in *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*. Barcelona, Spain: IEEE Computer Society, pp. 950–957. doi: 10.1109/ARES.2008.138.

U.S. Department of Energy (2009) 'National SCADA Testbed - Fact Sheet'. Department of Energy, USA, pp. 1–2. Available at: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf.

UK-Cabinet-Office (2012) *10 Steps to Cyber Security, Cyber Security Strategy*. Available at: <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary> (Accessed: 26 March 2015).

US-FDA (2017) *Hazard Analysis Critical Control Point (HACCP)*, U.S. Food & Drugs Administration Website. Available at: <https://www.fda.gov/Food/GuidanceRegulation/HACCP/> (Accessed: 20 October 2017).

Venkatasubramanian, K. K. (2009) *Security Solutions for Cyber-Physical Systems*, Arizona State University Tempe, AZ, USA. Arizona State University Tempe.

Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K. and Chow, K. P. (2010) 'Security Issues and Challenges for Cyber Physical System', in Zhu, P., Wang, L., Xia, F., Chen, H., McLoughlin, I., Tsao, S.-L., Sato, M., Chai, S.-K., and King, I. (eds) *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*. Hangzhou, China: IEEE, pp. 733–738. doi: 10.1109/GreenCom-CPSCoM.2010.36.

Wang, L., Islam, T., Long, T., Singhal, A. and Jajodia, S. (2008a) 'An Attack Graph-Based Probabilistic Security Metric', in Atluri, V. (ed.) *Data and Applications Security XXII: 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security London, UK, July 13-16, 2008 Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 283–296. doi: 10.1007/978-3-540-70567-3_22.

Wang, L., Islam, T., Long, T., Singhal, A. and Jajodia, S. (2008b) 'An Attack Graph-Based Probabilistic Security Metric', in Atluri, V. (ed.) *Data and Applications Security XXII: 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security London, UK, July 13-16, 2008 Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 283–296. doi: 10.1007/978-3-540-70567-3_22.

Wang, P. A. (2013) 'Assessment of Cybersecurity Knowledge and Behavior : An Anti-phishing Scenario', in *ICIMP 2013: The Eighth International Conference on Internet Monitoring and Protection*. Rome, Italy: IARIA, pp. 1–7. Available at: https://www.thinkmind.org/index.php?view=article&articleid=icimp_2013_1_10_30003.

Wang, P. and Liu, J. C. (2014) 'Threat Analysis of Cyber Attacks with Attack Tree+', *Journal of Information Hiding and Multimedia Signal Processing*, 5(4), pp. 778–788. Available at: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84923381869&partnerID=tZOTx3y1>.

Wang, S., Xia, C., Gao, J. and Jia, Q. (2016) 'Vulnerability Evaluation Based on CVSS and Environmental Information Statistics', in *Proceedings of 2015 4th International Conference on Computer Science and Network Technology, ICCSNT 2015*. Harbin, China: IEEE Xplore, pp. 1249–1252. doi: 10.1109/ICCSNT.2015.7490958.

- Wang, W. and Lu, Z. (2013) 'Cyber security in the Smart Grid: Survey and challenges', *Computer Networks*. Elsevier B.V., 57(5), pp. 1344–1371. doi: 10.1016/j.comnet.2012.12.017.
- Wells, L. J., Camelio, J. A., Williams, C. B. and White, J. (2014) 'Cyber-physical security challenges in manufacturing systems', *Manufacturing Letters*, 2(2), pp. 74–77. doi: 10.1016/j.mfglet.2014.01.005.
- Woo, P. S. and Kim, B. H. (2015) 'A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems', *Journal of Energy Engineering*, 24(1), pp. 123–131. doi: 10.5855/ENERGY.2015.24.1.123.
- Work, D., Bayen, A. and Jacobson, Q. (2008) 'Automotive Cyber Physical Systems in the Context of Human Mobility', in *National Workshop on High-Confidence Automotive Cyber-Physical Systems*. Troy, MI, pp. 3–5. Available at: <http://bayen.eecs.berkeley.edu/sites/default/files/conferences/cps1.pdf>.
- Wu, L. and Kaiser, G. (2012) 'An Autonomic Reliability Improvement System for Cyber-Physical Systems', *2012 IEEE 14th International Symposium on High-Assurance Systems Engineering*, pp. 56–61. doi: 10.1109/HASE.2012.33.
- Wu, L. and Kaiser, G. (2013) 'FARE: A framework for benchmarking reliability of cyber-physical systems', *9th Annual Conference on Long Island Systems, Applications and Technology, LISAT 2013*. doi: 10.1109/LISAT.2013.6578226.
- Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y. and Sztipanovits, J. (2013) 'Taxonomy for Description of Cross-domain Attacks on CPS', in *Proceedings of the {2Nd} {ACM} International Conference on High Confidence Networked Systems*. ACM, pp. 135–142. doi: 10.1145/2461446.2461465.
- Yan, J., Govindarasu, M., Liu, C.-C. and Vaidya, U. (2013) 'A PMU-based risk assessment framework for power control systems', in *Power and Energy Society General Meeting (PES), 2013 IEEE*. Vancouver, BC, Canada: IEEE, pp. 1–5. doi: 10.1109/PESMG.2013.6672731.
- Yang, G., Wang, Y., Li, J., Liu, J., Ru, Y., Yuan, K., Wu, Y. and Liu, K. (2016) 'An Assessment Method of Vulnerabilities in Electric CPS Cyber Space', in. Changsha, China: IEEE, pp. 397–402. doi: 10.1109/FSKD.2016.7603206.
- Yi, S., Peng, Y., Xiong, Q., Wang, T., Dai, Z., Gao, H., Xu, J., Wang, J. and Xu, L. (2013) 'Overview on attack graph generation and visualization technology', in *Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID*. Shanghai, China: IEEE. doi: 10.1109/ICASID.2013.6825274.
- Younis, A., Malaiya, Y. K. and Ray, I. (2016) 'Assessing vulnerability exploitability risk using software properties', *Software Quality Journal*. Springer US, 24(1), pp. 159–202. doi: 10.1007/s11219-015-9274-6.
- Yuan, Y., Zhu, Q., Sun, F., Wang, Q. and Basar, T. (2013) 'Resilient control of cyber-physical systems against Denial-of-Service attacks', in *2013 6th International Symposium on Resilient Control Systems (ISRCs)*. IEEE Xplore, pp. 54–59. doi: 10.1109/ISRCs.2013.6623750.
- Yusta, J. M., Correa, G. J. and Lacal-Arántegui, R. (2011) 'Methodologies and applications for critical infrastructure protection: State-of-the-art', *Energy Policy*, 39(10), pp. 6100–6119. doi: 10.1016/j.enpol.2011.07.010.

Zhang, H., Cheng, P., Shi, L. and Chen, J. (2013) 'Optimal DoS Attack Policy Against Remote State Estimation', in *52nd IEEE Conference on Decision and Control*. Florence, Italy: IEEE Xplore, pp. 5444–5449. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6760746>.

Zhang, L., Zhou, Y., Chen, Y., Zhang, M. and Zhang, J. (2013) 'Stability of Software Trustworthiness Measurements Models', *2013 IEEE Seventh International Conference on Software Security and Reliability Companion*, pp. 219–224. doi: 10.1109/SERE-C.2013.23.

Zhu, B. (2010) 'SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy', in *WSCS 2010*. WSCS Conference, pp. 1–16. Available at: <http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/zhu.pdf>.

Zhu, B., Joseph, A. and Sastry, S. (2011) 'A taxonomy of cyber attacks on SCADA systems', in Xia, F., Chen, Z., Pan, G., Yang, L. T., and Ma, J. (eds) *Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCoM 2011*. Dalian, China: IEEE, pp. 380–388. doi: 10.1109/iThings/CPSCoM.2011.34.

Zhu, Q., Rieger, C. and Başar, T. (2011) 'A hierarchical security architecture for cyber-physical systems', in *Proceedings - ISRCS 2011: 4th International Symposium on Resilient Control Systems*. IEEE, pp. 15–20. doi: 10.1109/ISRCS.2011.6016081.

APPENDICES

Appendix A: Tables

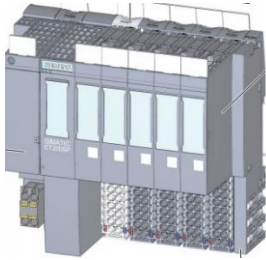
Table A-1: Reviewed Cybersecurity Principles Relative to ICS

SECURITY REQUIREMENT/PRINCIPLES	OVERVIEW (I/MCS, CPS, SCADA)	AUTHORS	SPECIFIC APPROACH/CONCEPT
AVAILABILITY	Emphasizes the steadfast, uninterrupted access and use of information services.	(Work, Bayen and Jacobson, 2008)	High-availability-driven
		(Parvin <i>et al.</i> , 2013)	Multi-cyber security framework based on Markov Model
INTEGRITY	Guarantees that a system performs in the manner it is intended without alteration or manipulation of information or functionality	(Wang <i>et al.</i> , 2010) (Larkin <i>et al.</i> , 2014)	Concept representation
		(Madden, McMillin and Sinha, 2010)	Automotive Engine Management System (EMS) model approach
		(Venkatasubramanian, 2009)	Cpysec solution - Physiological Signal based Key Agreement (PSKA).
		(Ibrahim and Nair, 2011)	Physical Unclonable Functions (PUFs) technology solution
CONFIDENTIALITY	The graceful preservation of products/production (design, process, quality control, supply chain, personnel) data and information from access by unauthorised or external entities	(Wang <i>et al.</i> , 2010) (Wang and Lu, 2013) (Larkin <i>et al.</i> , 2014)	Concept description
		(Han <i>et al.</i> , 2007)	Concept description and exploration using humidity detection
		(Pham, Abdelzaher and Nath, 2010)	Privacy Measure perturbation Algorithm based on mutual information approach
		(Gamage, Roth and McMillin, 2011)	A self-obfuscating, non-deducibility model composed of simple CPS building blocks.
		(Schneider, 2003)	Policy enforcement and adherence approach

SECURITY REQUIREMENT/PRINCIPLES	OVERVIEW (I/MCS, CPS, SCADA)	AUTHORS	SPECIFIC APPROACH/CONCEPT
		(Amtoft and Banerjee, 2007)	Information flow analysis approach using a Hoare-like logic.
		(Jiang, Guo and Sang, 2010)	Risk-based security profit model using a Security-Slack based Heuristic Algorithm (SSHA) for periodic messages.
ACCOUNTABILITY	Ability to ensure unique trace of a user/entity's action to the user/entity	(Gollmann, 2011)	Concept description
NON-REPUDIATION	Ability to ensure that an entity is unable to challenge the authorship of process or instruction commands	(Gollmann, 2011)	Concept description
AUTHENTICITY	Ensures the substantiation of all ICS-related processes like sensing, communications and actuation, and their respective initiators, emphasizing unpretentious data, transactions and communications within any computing system or process	(Wang <i>et al.</i> , 2010) (Stallings, 2010)	Concept description
VERACITY	Process measurements and control instructions are truthfully captured from control algorithm executions without fear of any misguidance from external sources.	(Gollmann, 2012) in (Krotofil and Gollmann, 2013)	Concept description
TIMELINESS	Any demanded, reported, and distributed information should not be obsolete but correspond to real-time	(Zhu, Joseph and Sastry, 2011)	Concept description
GRACEFUL DEGRADATION	Ability to localize attack impacts, suppressing contaminated data flow within contaminated region to avoid without further escalating into a full-scale incident.	(Zhu, Joseph and Sastry, 2011)	Concept description
RELIABILITY	Ability to perform intended function(s) for a given period under a given set of conditions	(Stamp, McIntyre and Ricardson, 2009)	Concept description
		(Wu and Kaiser, 2013)	Failure Analysis and Reliability Estimation (FARE) Benchmarking approach
		(Wu and Kaiser, 2012)	Autonomic Reliability Improvement System (ARIS); data-centric runtime monitoring system for improving the reliability using online evaluation approach

SECURITY REQUIREMENT/PRINCIPLES	OVERVIEW (I/MCS, CPS, SCADA)	AUTHORS	SPECIFIC APPROACH/CONCEPT
		(Mitchell and Chen, 2013)	Probability model based on stochastic Petri nets for behavioural description of the attacker-invaded CPS, and an intrusion detection and response system (IDRS).
ROBUSTNESS	The degree to which a system or component can function correctly in the presence of invalid inputs or stressful environment conditions	(Rungger and Tabuada, 2013) (Rungger and Tabuada, 2014) (Tabuada <i>et al.</i> , 2014)	An abstraction and refinement process (input-output dynamical stability) model
TRUSTWORTHINESS	The extent to which a system can be relied upon to perform exclusively and correctly the system task(s) under defined operational and environmental conditions over a defined period, or at a given instant in time	(Boyes, 2013)	Concept description
		(Chen, 2010)	Trustworthiness Evaluation Approach (Software-oriented)
		(L. Zhang <i>et al.</i> , 2013)	Stability rule with which measurement model using Monte Carlo method (Software-oriented)
		(Anwar and Ali, 2012)	A two tier (blanket) trust-oriented approach
		(Stelte and Rodosek, 2013)	Device redundancy approach for trustworthiness in WSN
		(Tang <i>et al.</i> , 2010)	Alarms alerting approach for trustworthy inferences

**Table A-2: Network Components of Industrial Control System Conveyor
Testbed Setup**

S/N	Name of component	Description	Picture
1.	Industrial robot	Fischertechnik 96785 Punching machine with conveyor belt: This is an object/item punching robot with a conveyor belt, two light barriers and a machining station.	 <p>Conveyor/Punching machine industrial robot - Fischertechnik (2013)</p>
2.	PLC	Siemens Simatic S7-1200: This is a basic controller designed for automation tasks within a small project scope. Wiring workload (or program) developed on a TIA portal (Siemens automation software) can be saved directly on this device, thus enabling it to control connected robots independently off a server.	 <p>Simatic S7-1200 - Siemens (no date)</p>
3.	External I/O module	Siemens Simatic ET 200SP distributed I/O system: This is a scalable and flexible system that enables the connection of process signals through an interface module (with a profinet port); processes I/O signals through a CPU module; can accommodate up to 64 I/O modules, plugged into passive base units (in any combination: white, black, light blue or dark blue) and a server module. The experimentation system holds two I/O modules, 1 input and 1 output, plugged into white and black base units respectively.	 <p>Simatic ET 200SP - Siemens (2012)</p>
4.	Ethernet industrial switch	Moxa EDS-408A Ethernet switch: This is an 8-port Ethernet switch designed specifically for industrial applications.	 <p>Moxa EDS-408A Ethernet switch</p>

S/N	Name of component	Description	Picture
5.	Firewall	<p>Moxa EDR-810-2GSFP:</p> <p>This is an industrial secure router with Firewall designed for Ethernet security applications that provides an electronic security perimeter protection for cyber assets.</p>	 <p>Moxa EDR-810-2GSFP Firewall</p>
6.	HMI	<p>Siemens KPT700 basic panel HMI:</p> <p>This is a 7" screen display device designed for simple HMI applications.</p>	 <p>Siemens KPT700 basic panel HMI</p>
7.	Power pack	<p>TDK-Lambda DPP240-24-1 power supply</p>	 <p>TDK-Lambda DPP240-24-1 power supply</p>

Table A-3: CVSS 2.0 Standard Metrics Scoring Values [77]

Metric	Metric Value	Numeric Value
Exploitability (Ex)	Unproven	0.85
	Proof-of-concept	0.90
	Functional	0.95
	High	1.00
	Not defined	1.00
Remediation Level (RL)	official-fix	0.87
	temporary-fix	0.90
	Workaround	0.95
	Unavailable	1.00
	Not defined	1.00
Report Confidence (RC)	Unconfirmed	0.90
	Uncorroborated	0.95
	Confirmed	1.00
	Not Defined	1.00
Collateral Damage Potential (CDP)	None	0
	Low	0.1
	Low-medium	0.3
	Medium-high	0.4
	High	0.5
	Not defined	0
Target Distribution (TD)	None	0
	Low	0.25
	Medium	0.75
	High	1.00
	Not defined	1.00
Confidentiality Requirement (CR)	Low	0.5
	Medium	1.0
	High	1.51
	Not defined	1.0
Integrity Requirement (IR)	Low	0.5
	Medium	1.0
	High	1.51
	Not defined	1.0
Availability Requirement (AR)	Low	0.5
	Medium	1.0
	High	1.51
	Not defined	1.0

Table A-4: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (1)

Vulnerability Number	Description	Vulnerability Label	IP Address	Devices Affected	Base Score	Base Score Severity Factor
<u>CVE-1999-0517</u>	41028 - SNMP Agent Default Community Name (public)	V1	192.168.1.2	PLC	7.5	High
<u>CVE-1999-0517</u>	41028 - SNMP Agent Default Community Name (public)	V2	192.168.1.4	I/O Module	7.5	High
CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148	97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)	V3	192.168.1.11	Control Workstation	10.0	Critical
<u>CVE-2005-1794</u>	18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	V4	192.168.1.11	Control Workstation	5.1	Medium
No Vulnerability Number	35291 - SSL Certificate Signed Using Weak Hashing Algorithm	V5	192.168.1.11	Control Workstation	4.0	Medium
No Vulnerability Number	42873 - SSL Medium Strength Cipher Suites Supported	V6	192.168.1.11	Control Workstation	5.0	Medium
No Vulnerability Number	45411 - SSL Certificate with Wrong Hostname	V7	192.168.1.11	Control Workstation	5.0	Medium
No Vulnerability Number	51192 - SSL Certificate Cannot Be Trusted	V8	192.168.1.11	Control Workstation	6.4	Medium
No Vulnerability Number	57582 - SSL Self-Signed Certificate	V9	192.168.1.11	Control Workstation	6.4	Medium
No Vulnerability Number	57690 - Terminal Services Encryption Level is Medium or Low	V10	192.168.1.11	Control Workstation	4.3	Medium
No Vulnerability Number	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	V11	192.168.1.11	Control Workstation	4.3	Medium
No Vulnerability Number	94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	V12	192.168.1.11	Control Workstation	5.0	Medium
No Vulnerability Number	30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	V13	192.168.1.11	Control Workstation	2.6	Low
No Vulnerability Number	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	V14	192.168.1.11	Control Workstation	2.6	Low
<u>CVE-1999-0511</u>	50686 - IP Forwarding Enabled	V15	192.168.1.15	Ethernet Switch	5.8	Medium
No Vulnerability Number	42263 - Unencrypted Telnet Server	V16	192.168.1.15	Ethernet Switch	5.8	Medium
<u>CVE-1999-0517</u>	41028 - SNMP Agent Default Community Name (public)	V17	192.168.1.15	Ethernet Switch	7.5	High
OSVDB:125796	76474 - SNMP 'GETBULK' Reflection DDoS	V18	192.168.1.15	Ethernet Switch	5.0	Medium
No Vulnerability Number	23817 - Modbus/TCP Coil Access	V19	192.168.1.15	Ethernet Switch	5.0	Medium
No Vulnerability Number	83301 - Modbus/TCP Device Identification	V20	192.168.1.15	Ethernet Switch	5.0	Medium
No Vulnerability Number	Operating System Design Flaws enabling administrative access	UV1	192.168.1.11	Control Workstation	-	-

Table A-5: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (1)

Vulnerability	Description	Label	Devices Affected	Base Score	Exploitability (Ex)	Exploitability Value	Remediation Level (RL)	RL Value	Report Confidence (RC)	RC Value	Temporal Score	Corrected Temporal Score
CVE-1999-0254	Default or guessable SNMP community names: public	k1	Ethernet Switch	10.0	functional	0.95	workaround	0.95	confirmed	1.00	9.025	9.1
		k2	PLC	10.0	functional	0.95	workaround	0.95	confirmed	1.00	9.025	9.1
		k3	I/O Module	10.0	functional	0.95	workaround	0.95	confirmed	1.00	9.025	9.1
CWE-319	SNMP credentials transmitted in clear text	k4	Ethernet Switch	8.0	high	1.00	workaround	0.95	confirmed	1.00	7.6	7.6
		k5	PLC	8.0	high	1.00	workaround	0.95	confirmed	1.00	7.6	7.6
		k6	I/O Module	8.0	high	1.00	workaround	0.95	confirmed	1.00	7.6	7.6
	Reset Password Backdoor Vulnerability in Windows 7	k7	Control Workstation	7.9	proof-of-concept	0.9	workaround	0.95	uncorroborated	0.95	6.416775	6.5
CVE-2015-6465	RESOURCE EXHAUSTION: authenticated users to cause a denial of service (reboot) - Port 80	k8	Ethernet Switch	6.8	high	1.00	official-fix	0.87	confirmed	1.00	5.916	6
CVE-1999-0524	ICMP timestamp response	k9	Control Workstation	0.0	functional	0.95	workaround	0.95	confirmed	1.00	0	0
		k10	Ethernet Switch	0.0	functional	0.95	workaround	0.95	uncorroborated	0.95	0	0
		k11	HMI	0.0	functional	0.95	workaround	0.95	uncorroborated	0.95	0	0

Table A-6: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (2)

Vul. Label	Access Vector	Access Vector Value	Access Complex	Access Complex Value	Auth.	Auth. Value	Conf Impact	Conf Impact Value	Integ Impact	Integ Impact Value	Avail Impact	Avail Impact Value	Colat Damage Potential	Colat Damage Potential Value	Target Distribution
k1	network access	1.00	low	0.71	none	0.704	complete	0.660	complete	0.660	complete	0.660	medium-high	0.4	high
k2	network access	1.00	low	0.71	none	0.704	complete	0.660	complete	0.660	complete	0.660	medium-high	0.4	medium
k3	network access	1.00	low	0.71	none	0.704	complete	0.660	complete	0.660	complete	0.660	medium-high	0.4	low
k4	network access	1.00	med	0.61	none	0.704	complete	0.660	complete	0.660	complete	0.660	medium-high	0.4	high
k5	network access	1.00	med	0.61	none	0.704	complete	0.660	complete	0.660	complete	0.660	medium-high	0.4	medium
k6	network access	1.00	med	0.61	none	0.704	complete	0.660	complete	0.660	complete	0.660	medium-high	0.4	low
k7	local access	0.395	low	0.71	none	0.704	complete	0.660	complete	0.660	complete	0.660	high	0.5	high
k8	network access	1.00	low	0.71	single	0.56	partial	0.275	complete	0.660	complete	0.660	high	0.5	high
k9	local access	0.395	low	0.71	none	0.704	UKN	unknown	UKN	unknown	UKN	unknown	none	0.0	none
k10	local access	0.395	low	0.71	none	0.704	UKN	unknown	UKN	unknown	UKN	unknown	none	0.0	none
k11	local access	0.395	low	0.71	none	0.704	UKN	unknown	UKN	unknown	UKN	unknown	none	0.0	none

Table A-7: Testbed Network Vulnerability and Impact Analysis Data (Nexpose Scan) – (3)

ConfReq	ConfReq Value	IntegReq	IntegReq Value	AvailReq	AvailReq Value	Adjust Impact Computed	Adjust Impact Corrected	Adjusted Temporal Value	Adjusted Temporal Value Corrected	Environm Score	Environm Score Corrected
medium	1.00	high	1.51	high	1.51	9.9999607	9.999960696	9.02496453	9.1	9.46	9.5
medium	1.00	high	1.51	high	1.51	9.9999607	9.999960696	9.02496453	9.1	7.095	7.1
medium	1.00	high	1.51	high	1.51	9.9999607	9.999960696	9.02496453	9.1	2.365	2.4
high	1.51	high	1.51	high	1.51	9.99999961	9.999999607	9.49999963	9.5	9.7	9.7
high	1.51	high	1.51	medium	1.00	9.9999607	9.999960696	9.49996266	9.5	7.275	7.3
high	1.51	high	1.51	medium	1.00	9.9999607	9.999960696	9.49996266	9.5	2.425	2.5
high	1.51	high	1.51	medium	1.00	9.9999607	9.999960696	8.12246808	8.2	9.1	9.1
medium	1.00	high	1.51	high	1.51	9.99991619	9.99991619	8.69992709	8.7	9.35	9.4
medium	1.00	not defined	1.0	not defined	1.0	Null	Null	Null	Null	Null	Null
medium	1.00	not defined	1.0	not defined	1.0	Null	Null	Null	Null	Null	Null
medium	1.00	not defined	1.0	not defined	1.0	Null	Null	Null	Null	Null	Null

Functional Dependency Index	Number of Attack Path Occurrence	Total No. of Attack Paths	Probability of Attack	Vulnerability Attack Potential	TSr	Esr	FD Ratio	Vulnerability Exploit Potential (β)	Vulnerable Impact Potential (γ)	Criticality Index Pot
7	12	15	0.8	7.28	0.91	0.95	1	0.728	0.95	0.831624915
4	8	15	0.533333333	4.853333333	0.91	0.71	0.571429	0.485333333	0.405714286	0.443741667
2	4	15	0.266666667	2.426666667	0.91	0.24	0.285714	0.242666667	0.068571429	0.128996124
7	12	15	0.8	6.08	0.76	0.97	1	0.608	0.97	0.767958332
4	8	15	0.533333333	4.053333333	0.76	0.73	0.571429	0.405333333	0.417142857	0.411195701
2	4	15	0.266666667	2.026666667	0.76	0.25	0.285714	0.202666667	0.071428571	0.120317042
6	10	15	0.666666667	4.333333333	0.65	0.91	0.857143	0.433333333	0.78	0.581377674
7	12	15	0.8	4.8	0.6	0.94	1	0.48	0.94	0.671714225
6	10	15	0.666666667	0	0	Null	0.857143	0	Null	Null
7	12	15	0.8	0	0	Null	1	0	Null	Null
1	1	15	0.066666667	0	0	Null	0.142857	0	Null	Null

Table A-8: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (1)

Vulnerability Number	Description	Vulnerability Label	IP Address	Devices Affected	Base Score	Base Score Severity Factor
CVE-1999-0517	41028 - SNMP Agent Default Community Name (public)	V1	192.168.1.2	PLC	7.5	High
CVE-1999-0517	41028 - SNMP Agent Default Community Name (public)	V2	192.168.1.4	I/O Module	7.5	High
CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148	97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)	V3	192.168.1.11	Control Workstation	10.0	Critical
CVE-2005-1794	18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	V4	192.168.1.11	Control Workstation	5.1	Medium
No Vulnerability Number	35291 - SSL Certificate Signed Using Weak Hashing Algorithm	V5	192.168.1.11	Control Workstation	4.0	Medium
No Vulnerability Number	42873 - SSL Medium Strength Cipher Suites Supported	V6	192.168.1.11	Control Workstation	5.0	Medium
No Vulnerability Number	45411 - SSL Certificate with Wrong Hostname	V7	192.168.1.11	Control Workstation	5.0	Medium
No Vulnerability Number	51192 - SSL Certificate Cannot Be Trusted	V8	192.168.1.11	Control Workstation	6.4	Medium
No Vulnerability Number	57582 - SSL Self-Signed Certificate	V9	192.168.1.11	Control Workstation	6.4	Medium
No Vulnerability Number	57690 - Terminal Services Encryption Level is Medium or Low	V10	192.168.1.11	Control Workstation	4.3	Medium
No Vulnerability Number	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	V11	192.168.1.11	Control Workstation	4.3	Medium
No Vulnerability Number	94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	V12	192.168.1.11	Control Workstation	5.0	Medium
No Vulnerability Number	30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	V13	192.168.1.11	Control Workstation	2.6	Low
No Vulnerability Number	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	V14	192.168.1.11	Control Workstation	2.6	Low
CVE-1999-0511	50686 - IP Forwarding Enabled	V15	192.168.1.15	Ethernet Switch	5.8	Medium
No Vulnerability Number	42263 - Unencrypted Telnet Server	V16	192.168.1.15	Ethernet Switch	5.8	Medium
CVE-1999-0517	41028 - SNMP Agent Default Community Name (public)	V17	192.168.1.15	Ethernet Switch	7.5	High
OSVDB:125796	76474 - SNMP 'GETBULK' Reflection DDoS	V18	192.168.1.15	Ethernet Switch	5.0	Medium
No Vulnerability Number	23817 - Modbus/TCP Coil Access	V19	192.168.1.15	Ethernet Switch	5.0	Medium
No Vulnerability Number	83301 - Modbus/TCP Device Identification	V20	192.168.1.15	Ethernet Switch	5.0	Medium

Table A-9: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (2)

Vulnerability Label	Exploitability	Exploit Value	Remediation Level	RL Value	Report Confidence	RC Value	Temporal Score	Corrected Temporal Score
V1	functional	0.95	not defined	1.00	not defined	1.00	7.125	7.1
V2	functional	0.95	not defined	1.00	not defined	1.00	7.125	7.1
V3	proof-of-concept	0.9	official-fix	0.87	confirmed	1.00	7.83	7.8
V4	functional	0.95	workaround	0.95	not defined	1.00	4.60275	4.6
V5	not defined	1.00	official-fix	0.87	confirmed	1.00	3.48	3.5
V6	functional	0.95	temporal-fix	0.90	uncorroborated	0.95	4.06125	4.1
V7	proof-of-concept	0.9	temporal-fix	0.90	unconfirmed	0.90	3.645	3.6
V8	functional	0.95	workaround	0.95	confirmed	1.00	5.776	5.8
V9	proof-of-concept	0.9	temporal-fix	0.90	uncorroborated	0.95	4.9248	4.9
V10	High	1.00	workaround	0.95	confirmed	1.00	4.085	4.1
V11	High	1.00	workaround	0.95	confirmed	1.00	4.085	4.1
V12	functional	0.95	not defined	1.00	not defined	1.00	4.75	4.8
V13	functional	0.95	temporal-fix	0.90	uncorroborated	0.95	2.11185	2.1
V14	functional	0.95	temporal-fix	0.90	not defined	1.00	2.223	2.2
V15	functional	0.95	workaround	0.95	not defined	1.00	5.2345	5.2
V16	High	1.00	workaround	0.95	not defined	1.00	5.51	5.5
V17	functional	0.95	not defined	1.00	not defined	1.00	7.125	7.1
V18	functional	0.95	unavailable	1.00	not defined	1.00	4.75	4.8
V19	functional	0.95	unavailable	1.00	uncorroborated	0.95	4.5125	4.5
V20	functional	0.95	unavailable	1.00	unconfirmed	0.90	4.275	4.3

Table A-10: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (3)

Access Vector	Access Vector Value	Access Complex	Access Complex Value	Authentic.	Authentic Value	conflmpact	Conflmpact Value	IntegImpact	IntegImpact Value	AvailImpact	AvailImpact Value
network access	1.00	low	0.71	none	0.704	partial	0.275	partial	0.275	partial	0.275
network access	1.00	low	0.71	none	0.704	partial	0.275	partial	0.275	partial	0.275
network access	1.00	low	0.71	none	0.704	complete	0.660	complete	0.660	complete	0.660
network access	1.00	high	0.35	none	0.704	partial	0.275	partial	0.275	partial	0.275
network access	1.00	high	0.35	none	0.704	partial	0.275	partial	0.275	none	0.00
network access	1.00	low	0.71	none	0.704	partial	0.275	none	0.00	none	0.00
network access	1.00	low	0.71	none	0.704	none	0.00	partial	0.275	none	0.00
network access	1.00	low	0.71	none	0.704	partial	0.275	partial	0.275	none	0.00
network access	1.00	low	0.71	none	0.704	partial	0.275	partial	0.275	none	0.00
network access	1.00	med	0.61	none	0.704	partial	0.275	none	0.00	none	0.00
network access	1.00	med	0.61	none	0.704	partial	0.275	none	0.00	none	0.00
network access	1.00	low	0.71	none	0.704	partial	0.275	none	0.00	none	0.00
network access	1.00	high	0.35	none	0.704	partial	0.275	none	0.00	none	0.00
network access	1.00	high	0.35	none	0.704	partial	0.275	none	0.00	none	0.00
adj. network access	0.646	low	0.71	none	0.704	partial	0.275	partial	0.275	partial	0.275
network access	1.00	med	0.61	none	0.704	partial	0.275	partial	0.275	none	0.00
network access	1.00	low	0.71	none	0.704	partial	0.275	partial	0.275	partial	0.275
network access	1.00	low	0.71	none	0.704	none	0.00	none	0.00	partial	0.275
network access	1.00	low	0.71	none	0.704	partial	0.275	none	0.00	none	0.00
network access	1.00	low	0.71	none	0.704	partial	0.275	none	0.00	none	0.00

Table A-11: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (4)

ColatDamage Potential	ColatDamage Potential Value	Target Distribution	Target Distribution Value	ConfReq	ConfReq Value	IntegReq	IntegReq Value	AvailReq	AvailReq Value
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51
medium-high	0.4	medium	0.75	medium	1.00	high	1.51	high	1.51
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	medium	1.00
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51
high	0.5	high	1.0	high	1.51	high	1.51	high	1.51

Table A-12: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (5)

Adjust Impact Computed	Adjust Impact Corrected	Adjusted Temporal Value	Adjusted Temporal Value Corrected	Environm Score	Environm Score Corrected		Functional Dependency Index	Number of Attack Path Occurrence	Total No. of Attack Paths	Probability of Attack	Vulnerability Attack Potential
8.00054934	8.000549341	7.60052187	7.7	8.85	8.9		4	8	15	0.533333333	3.8
7.52098892	7.520988922	7.14493948	7.2	6.24	6.3		2	4	15	0.266666667	1.9
9.9999607	9.999960696	7.82996922	7.9	8.95	9		6	10	15	0.666666667	5.22
7.52098892	7.520988922	6.7876925	6.8	8.4	8.4		6	10	15	0.666666667	3.0685
6.58067438	6.580674375	5.72518671	5.8	7.9	7.9		6	10	15	0.666666667	2.32
4.1525	4.1525	3.37286813	3.4	6.7	6.7		6	10	15	0.666666667	2.7075
4.1525	4.1525	3.0271725	3.1	6.55	6.6		6	10	15	0.666666667	2.43
6.58067438	6.580674375	5.93905862	6	8	8		6	10	15	0.666666667	3.850666667
6.58067438	6.580674375	5.06382893	5.1	7.55	7.6		6	10	15	0.666666667	3.2832
4.1525	4.1525	3.944875	4	7	7		6	10	15	0.666666667	2.723333333
4.1525	4.1525	3.944875	4	7	7		6	10	15	0.666666667	2.723333333
4.1525	4.1525	3.944875	4	7	7		6	10	15	0.666666667	3.166666667
4.1525	4.1525	3.37286813	3.4	6.7	6.7		6	10	15	0.666666667	1.4079
4.1525	4.1525	3.5503875	3.6	6.8	6.8		6	10	15	0.666666667	1.482
8.00054934	8.000549341	7.22049578	7.3	8.65	8.7		7	12	15	0.8	4.1876
6.58067438	6.580674375	6.25164066	6.3	8.15	8.2		7	12	15	0.8	4.408
8.00054934	8.000549341	7.60052187	7.7	8.85	8.9		7	12	15	0.8	5.7
4.1525	4.1525	3.944875	4	7	7		7	12	15	0.8	3.8
4.1525	4.1525	3.74763125	3.8	6.9	6.9		7	12	15	0.8	3.61
4.1525	4.1525	3.5503875	3.6	6.8	6.8		7	12	15	0.8	3.42

Table A-13: Testbed Vulnerability and Impact Analysis (NESSUS Scan) – (6)

Vulnerability Label	Devices Affected	Base Score	Temporal Score	Environmental Score Corrected	RTS	RTS	Functional Dependency Index	RYv	Probability of Attack	Vulnerability Exploit Potential	Vulnerability Impact Potential	Criticality Index	Prioritisation Index
V1	PLC	7.5	7.1	8.9	0.7125	0.89	4	0.571428571	0.533333333	0.38	0.508571429	0.193257143	11
V2	I/O Module	7.5	7.1	6.3	0.7125	0.63	2	0.285714286	0.266666667	0.19	0.18	0.0342	20
V3	Control Workstation	10.0	7.8	9	0.783	0.9	6	0.857142857	0.666666667	0.522	0.771428571	0.402685714	2
V4	Control Workstation	5.1	4.6	8.4	0.460275	0.84	6	0.857142857	0.666666667	0.30685	0.72	0.220932	9
V5	Control Workstation	4.0	3.5	7.9	0.348	0.79	6	0.857142857	0.666666667	0.232	0.677142857	0.157097143	15
V6	Control Workstation	5.0	4.1	6.7	0.406125	0.67	6	0.857142857	0.666666667	0.27075	0.574285714	0.155487857	16
V7	Control Workstation	5.0	3.6	6.6	0.3645	0.66	6	0.857142857	0.666666667	0.243	0.565714286	0.137468571	17
V8	Control Workstation	6.4	5.8	8	0.5776	0.8	6	0.857142857	0.666666667	0.385066667	0.685714286	0.264045714	6
V9	Control Workstation	6.4	4.9	7.6	0.49248	0.76	6	0.857142857	0.666666667	0.32832	0.651428571	0.213877029	10
V10	Control Workstation	4.3	4.1	7	0.4085	0.7	6	0.857142857	0.666666667	0.272333333	0.6	0.1634	13
V11	Control Workstation	4.3	4.1	7	0.4085	0.7	6	0.857142857	0.666666667	0.272333333	0.6	0.1634	13
V12	Control Workstation	5.0	4.8	7	0.475	0.7	6	0.857142857	0.666666667	0.316666667	0.6	0.19	12
V13	Control Workstation	2.6	2.1	6.7	0.211185	0.67	6	0.857142857	0.666666667	0.14079	0.574285714	0.080853686	19
V14	Control Workstation	2.6	2.2	6.8	0.2223	0.68	6	0.857142857	0.666666667	0.1482	0.582857143	0.086379429	18
V15	Ethernet Switch	5.8	5.2	8.7	0.52345	0.87	7	1	0.8	0.41876	0.87	0.3643212	3
V16	Ethernet Switch	5.8	5.5	8.2	0.551	0.82	7	1	0.8	0.4408	0.82	0.361456	4
V17	Ethernet Switch	7.5	7.1	8.9	0.7125	0.89	7	1	0.8	0.57	0.89	0.5073	1
V18	Ethernet Switch	5.0	4.8	7	0.475	0.7	7	1	0.8	0.38	0.7	0.266	5
V19	Ethernet Switch	5.0	4.5	6.9	0.45125	0.69	7	1	0.8	0.361	0.69	0.24909	7
V20	Ethernet Switch	5.0	4.3	6.8	0.4275	0.68	7	1	0.8	0.342	0.68	0.23256	8

Table B-14: Testbed Vulnerability - Risk Reduction (Technology and People Assets)

Technology Assets	Number of Vulnerabilities		
	Current State (t1)	Enhanced State (t2)	Reduction
PLC	1	0	1
I/O Module	1	0	1
HMI	0	0	0
Control Workstation	12	8	4
Ethernet Switch	6	4	2
Total	20	12	8
Technology Assets	Security Vulnerability Scores		
	Current State (t1)	Enhanced State (t2)	Reduction
PLC	0.193	0.000	0.193
I/O Module	0.034	0.000	0.034
HMI	0.000	0.000	0.000
Control Workstation	2.236	1.285	0.950
Ethernet Switch	1.981	1.207	0.773
Total	4.444	2.493	1.951
People Assets	Security Vulnerability Scores		
	Current State (t1)	Enhanced State (t2)	Reduction
WF01	0.595	0.252	0.344
WF02	0.655	0.315	0.340
WF03	0.668	0.351	0.316
WF04	0.290	0.175	0.115
WF05	0.378	0.195	0.183
WF06	0.476	0.141	0.335

Table A-15: Complete (37-Member) Workforce Capability Evaluation Results

WF ID	Kc	Sc	PSC	Priority Ranking
WF014	34	31	32.47	High
WF036	31	35	32.94	High
WF035	58	50	53.85	Moderate
WF023	64	48	55.43	Moderate
WF018	58	58	58.00	Moderate
WF037	60	60	60.00	Moderate
WF034	65	57	60.87	Moderate
WF019	66	57	61.34	Moderate
WF016	57	67	61.80	Moderate
WF032	71	54	61.92	Moderate
WF004	68	63	65.45	Moderate
WF028	70	62	65.88	Moderate
WF013	64	69	66.45	Moderate
WF002	59	75	66.52	Moderate
WF031	70	64	66.93	Low
WF012	67	67	67.00	Low
WF008	72	63	67.35	Low
WF026	72	64	67.88	Low
WF006	64	75	69.28	Low
WF003	72	67	69.46	Low
WF033	73	69	70.97	Low
WF029	72	70	70.99	Low
WF015	69	74	71.46	Low
WF007	80	66	72.66	Low
WF025	83	65	73.45	Low
WF009	79	69	73.83	Low
WF021	72	81	76.37	Low
WF001	76	77	76.50	Low
WF020	83	72	77.30	Low
WF024	81	75	77.94	Low
WF010	74	83	78.37	Low
WF017	84	76	79.90	Low
WF022	80	82	80.99	Low
WF030	63	109	82.87	Low
WF005	87	79	82.90	Low
WF027	81	88	84.43	Low
WF011	90	80	84.85	Low

Table A-16: Common Industrial Control Systems Protocols

Protocols	Organisation/Standard	Main features
MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)	Encapsulates fieldbus packets over TCP; attempting to become an IETF standard
DNP3	(IEC) Technical Committee 57, Working Group 03 standard	It is also based on the 3-layer OSI model
PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)	3-layer OSI model; has extensions for safety features; ProfiNet version provides Ethernet compatibility
Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Object-oriented, protocol; provides interoperability over Ethernet and fieldbus networks
DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Belongs to the CIP (Control and Information Protocol) family; CAN protocol defines layers 1 & 2; the rest are defined by DeviceNet and CIP
ControlNet	ControlNet International (www.controlnet.org)	Belongs to the same CIP (Control and Information Protocol) family; new physical layer with higher speed, strict determinism, and repeatability with greater range
Foundation Fieldbus	The Fieldbus Foundation/open standard protocol (www.fieldbus.org)	Incorporates many safety features that make it a good candidate for mission-critical applications

Table A-17: IT and ICS Specific Security Standards, and Guidelines

Specific Application Area & Scope	Publication
Information Security - Cross-Industry (Generic)	ISO/IEC 27000 Series
	NIST 800 Series
	FIPS 199
	FIPS 200
	DoD Instruction 8510.01: DIACAP
	DoD Instruction 8500.1 and 2: Information Assurance Implementation
Industrial Control System Security - Cross-Industry (Generic)	IEC 62443 (ISA-99)
	CPNI Good Practice Guide
	NIST SP 800-82
	NIST Framework to Reduce Cyber Risks to the Critical Infrastructure (forthcoming)
	U.S. DHS Securing Your SCADA and Industrial Control Systems
	U.S. DHS Catalog of Control Systems Security: Recommendations for Standards Developers
	U.S. DHS Cyber Security Assessments of Industrial Control Systems
	NAMUR NA 115 IT-Security for Industrial Automation Systems: Constraints for Measures in Process Industries
	SEMA Guide to Increased Security in Process Control Systems for Critical Societal Functions
	New Zealand NCSC Voluntary Cyber Security Standards for Industrial Control Systems v.1.0
	U.S. TSA Pipeline Security Guidelines
Industrial Control System Security – Industry-specific (Oil and Gas)	API Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries
	API Security Guidance for the Petroleum Industry
	API 1164 Pipeline SCADA Security
	AGA Report No. 12
	Norwegian Oil and Gas Association Guideline No. 104
	Norwegian Oil and Gas Association Guideline No. 110
	Norwegian Oil and Gas Association Guideline No. 123
	IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security
Industrial Control System Security – Industry-specific (Energy)	OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace
	NERC CIP 001-011
	U.S. DoE 21 Steps to Improve Cyber Security for SCADA Systems
	U.S. DoE Electricity Subsector Cybersecurity Risk Management Process
	U.S. DoE Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities
	U.S. Nuclear Regulatory Commission Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities
	VGB Guideline R 175
	U.S. DHS Chemical Facility Anti-Terrorism Standards
Industrial Control System Security – Industry-specific (Chemical)	ACC Guidance for Addressing Cyber Security in the Chemical Industry

Table A-18: Technology Vulnerability Analysis and Resolution Results

Vulnerability Label	Devices Affected	Description	Severity	Criticality Index	Resolution State
V1	PLC	41028 - SNMP Agent Default Community Name (public)	High	0.19	Resolved
V2	I/O Module	41028 - SNMP Agent Default Community Name (public)	High	0.03	Resolved
V3	Control Workstation	97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialled check)	Critical	0.40	Resolved
V4	Control Workstation	18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium	0.22	Resolved
V5	Control Workstation	35291 - SSL Certificate Signed Using Weak Hashing Algorithm	Medium	0.16	Not Resolved
V6	Control Workstation	42873 - SSL Medium Strength Cipher Suites Supported	Medium	0.16	Not Resolved
V7	Control Workstation	45411 - SSL Certificate with Wrong Hostname	Medium	0.14	Not Resolved
V8	Control Workstation	51192 - SSL Certificate Cannot Be Trusted	Medium	0.26	Not Resolved
V9	Control Workstation	57582 - SSL Self-Signed Certificate	Medium	0.21	Not Resolved
V10	Control Workstation	57690 - Terminal Services Encryption Level is Medium or Low	Medium	0.16	Resolved
V11	Control Workstation	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Medium	0.16	Resolved
V12	Control Workstation	94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	Medium	0.19	Not Resolved
V13	Control Workstation	30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	Low	0.08	Not Resolved
V14	Control Workstation	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Low	0.09	Not Resolved
V15	Ethernet Switch	50686 - IP Forwarding Enabled	Medium	0.36	Not Resolved
V16	Ethernet Switch	42263 - Unencrypted Telnet Server	Medium	0.36	Not Resolved
V17	Ethernet Switch	41028 - SNMP Agent Default Community Name (public)	High	0.51	Resolved
V18	Ethernet Switch	76474 - SNMP 'GETBULK' Reflection DDoS	Medium	0.27	Resolved
V19	Ethernet Switch	23817 - Modbus/TCP Coil Access	Medium	0.25	Not Resolved
V20	Ethernet Switch	83301 - Modbus/TCP Device Identification	Medium	0.23	Not Resolved

Table A-19: Current State Vulnerability Impact Point Analysis Results

Current State (t ₁) Evaluation Results								
Label	Host Component	IPts	CIPTs	Weakest Link	Label	IPts	CIPT	Weakest Link
V1	PLC	0.193	0.193		WF01	0.595	0.595	
V2	I/O Module	0.034			WF02	0.651	0.651	
V3	Control Workstation	0.403	0.403		WF03	0.668	0.668	0.668
V4	Control Workstation	0.221	0.221		WF04	0.290	-	
V5	Control Workstation	0.157	0.157		WF05	0.378	-	
V6	Control Workstation	0.155	0.155		WF06	0.476	-	
V7	Control Workstation	0.137	0.137					
V8	Control Workstation	0.264	0.264					
V9	Control Workstation	0.214	0.214					
V10	Control Workstation	0.163	0.163					
V11	Control Workstation	0.163	0.163					
V12	Control Workstation	0.190	0.190					
V13	Control Workstation	0.081						
V14	Control Workstation	0.086						
V15	Ethernet Switch	0.364	0.364					
V16	Ethernet Switch	0.361	0.361					
V17	Ethernet Switch	0.507	0.507	0.507				
V18	Ethernet Switch	0.266	0.266					
V19	Ethernet Switch	0.249	0.249					
V20	Ethernet Switch	0.233	0.233					

Table A-20: Enhanced State Vulnerability Impact Point Analysis Results

Enhanced State (t ₂) Evaluation Results											
Label	Host Component	IPts	CIPTs	Weakest Link	Label	IPts	CIPT	Weakest Link			
V5	Control Workstation	0.157	0.157		WF01	0.251	-				
V6	Control Workstation	0.156	0.156		WF02	0.316	-				
V7	Control Workstation	0.138	0.138		WF03	0.351	-	0.351			
V8	Control Workstation	0.264	0.264		WF04	0.175	-				
V9	Control Workstation	0.214	0.214		WF05	0.195	-				
V12	Control Workstation	0.190	0.190		WF06	0.141	-				
V13	Control Workstation	0.081									
V14	Control Workstation	0.087									
V15	Ethernet Switch	0.364	0.364						0.364		
V16	Ethernet Switch	0.362	0.362								
V19	Ethernet Switch	0.249	0.249								
V20	Ethernet Switch	0.233	0.233								

Table A-21: ICS Cyber Incidents in History

Year	Location	Category	Details (Impacts)
2014	Germany	Real	A blast furnace at a German steel mill suffered massive damage following a cyber-attack on the plant's network
2014	Ukraine, US, and Others	Real	Sandworm, a sophisticated malware that targeted and compromised the human-machine interface (HMI) of numerous popular ICS vendors. Attackers used the internet connected HMIs to exploit vulnerabilities in the ICS software.
2014	South Korea	Real	South Korean nuclear plant in Wolsong had its computers compromised, and lost nearly 10,000 employee details to hackers
2014	USA	Real	Sony Pictures Entertainment was hacked
2014	Norway	Real	More than 50 oil companies were hacked via phishing attacks for access to sensitive information.
2013	South Korea and Japan	Real	Icefog APT group sustained grip on corporate and government networks stealing sensitive information.
2012	Saudi Arabia	Real	Saudi Aramco oil company had over 30,000 of its computers invaded by attackers. Information on the systems were wiped clean, and system rendered unusable
2012	Qatar	Real	RasGas company computers were attacked with a virus and rendered dysfunctional for a while
2012	Global	Real	Elderwood Attacks, spear phishing emails, zero-day exploits, and watering hole were used to target defence, technology, supply-chain, and human rights organizations in the so-called "Operation Aurora" attacks
2012	Middle East	Real	Flame was being used for targeted cyberespionage in Middle Eastern countries
2011	Not Specified	Real	Attack combinations tagged 'Night Dragon' targeted corporate networks belonging to some companies operating SCADA systems.
2011	Global	Real	Duqu virus was found, a complex attack tool specifically for critical infrastructure
2011	USA	Real	Hackers attacked the control systems of water supply facilities in Illinois
2011	Japan	Real	Hackers invaded the control and management system of Shinkansen in Japan
2010	Iran, Global	Real	Stuxnet virus was found in Iran's Nuclear Power plant that damaged equipment and delayed productions.
2009	USA	Real	Russia & Chinese spies purportedly penetrated the US power grid, leaving behind potentially disruptive software programs
2008	Poland	Real	Teenager attacked the suburban railway system in Lodz, Poland
2007	Canada	Real	Attacker invaded one of Canada's Water SCADA control system and destroyed the control computer system.

2007	USA	Experimental	Idaho National Laboratory researchers on experimental display, blew-up a diesel-electric generator by taking over its control remotely and changing commands and settings in a bid to prove that cyber-attacks were possible on physical equipment.
2006	USA	Real	Hackers invaded the systems of the sewage treatment plant in Harrisburg, Pennsylvania
2006	USA	Real	Browns Ferry nuclear power plant got its PLC crashed by 'data storm' spikes in traffic, resulting in failure of automation in some equipment, forcing a manual shutdown of reactors
2005	USA	Real	Zotob worm was found in the automobile corporate network and control network.
2004	USA	Experimental	ISA Expo 2004 attendees witnessed the compromise of a running PLC program. Attacker was able to alter speed and direction of blinking light, and ultimately shut down the PLC system.
2003	USA	Real	Teenager invaded the computer system of Houston Ferry
2003	USA	Real	SQL-Slammer worm was found in the control network of Davis-Besse nuclear power plant. It disabled the safety monitoring system for 5 hrs before it was fixed.
2001	USA	Real	Hacker invaded the control system of electricity transmission system in California (Cal-ISO attack)
2000	Russia	Real	Hacker had controlled Gazprom, the largest natural gas pipeline network in the world.
2000	Australia	Real	A former contractor compromised Maroochy Shire sewage plant, releasing copious quantities of sewage into the environment
1997	USA	Real	A Teenager hacked into the Worcester-Massachusetts area NYNEX (now Bell Atlantic) telephone system using his personal computer and modem. This led to the shutdown of the telephone service to 600 customers in the local community; with a resulting disruption that affected all local police, fire 911 services, and inbound airport operations at Worcester airport
1994	USA	Real	Hacker invaded the Salt River Project in Arizona
1992	USA	Real	Chevron former employee closed the emergency alarm system located in 22 states
1982	Russia	Real	A Trojan (virus hidden inside legal software) infected Siberian gas pipeline SCADA system, blowing up the trans-siberian gas pipeline causing enormous damages.

Source: Compiled from (Dickman, 2009; Miller and Rowe, 2012; Nicholson et al., 2012a; Shyamasundar, 2013; Larkin et al., 2014; Morgan, 2014; Symantec Corporation, 2015)

Table A-22: Analysed Incident Classification based on Security Principles Targeted

Year	Attack Description	Category	Violated Primary Security Principles		
			Availability	Integrity	Confidentiality
2014	German Steel Mill Attack	Real	✓*		
2014	Sandworm Attack	Real		✓	✓
2014	South Korea, Wolsong Nuclear Plant Attack	Real			✓
2014	Sony Pictures Attack	Real	✓*		
2014	Norway Oil Company Phishing Attacks	Real		✓	
2013	Icefog APT group Sensitive Information Stealing Attack			✓	✓
2012	Saudi Aramco Oil Company Attack	Real	✓*		
2012	Qatar-based RasGas virus Attack	Real	✓*		
2012	Elderwood "Operation Aurora" Attacks				✓
2012	Flame Virus Middle East Attack	Real		✓	✓
2011	Night Dragon Attack	Real		✓	✓
2011	Duqu Global Virus Attack	Real		✓	✓
2011	Water Supply ICS Attack, Illinois	Real	✓	✓	
2011	Shinkansen ICS Attack	Real		✓	✓
2010	Iranian Nuclear, Global Stuxnet Attack	Real	✓	✓	
2009	USA Power Grid invasion attack	Real		✓	✓
2008	Suburban Railway System attack in Lodz, Poland	Real	✓	✓	✓
2007	Canadian Water SCADA system attack	Real	✓*		
2007	Idaho National Laboratory test attack, USA	Experimental	✓*		
2006	Harrisburg Sewage treatment plant attack, Pennsylvania	Real	✓	✓	
2006	Browns Ferry nuclear power plant attack	Real	✓*		
2005	Zotob worm attack, USA	Real			✓

Year	Attack Description	Category	Violated Primary Security Principles		
			Availability	Integrity	Confidentiality
2004	ISA Expo 2004 test attack, USA	Experimental	✓	✓	
2003	Houston Ferry system attack, USA	Real		✓	✓
2003	SQL-Slammer worm attack, USA	Real	✓*		
2001	Electricity transmission Control system attack, California Cal-ISO, USA	Real		✓	✓
2000	Russian Gazprom attack	Real	✓	✓	✓
2000	Maroochy Shire sewage plant attack, Australia	Real		✓	
1997	Worcester-Massachusetts area NYNEX (now Bell Atlantic) telephone hack	Real	✓	✓	✓
1994	Salt River Project attack, USA	Real	✓	✓	
1992	Chevron emergency alarm system closure	Real	✓	✓	
1982	Trans-Siberian gas pipeline attack Russia	Real	✓*		

* Availability only priority target incident

Table A-23: Cyber Security Methodologies relative to ICS Critical Infrastructure

Security Approach and Overview	Concept Description
<p>ARCHITECTURAL DESIGN:</p> <p>Security through the outline of potentially secure integration of technologies (hardware and software) for industrial and (or) service devices and equipment into a structural setup to enable protection from attacks.</p>	<ol style="list-style-type: none"> 1. Employing the security machineries of a Trusted Platform Module (TPM) to protect the communication in an RPL (Routing protocol) for LLNs (Low-power Lossy Networks) - (Seeber <i>et al.</i>, 2013) 2. The use of defence-in-depth and hierarchical network structure strategies for attaining multiple security mechanisms on an ICS/CPS infrastructure - (Dong <i>et al.</i>, 2015) 3. Involves innovative solution approach that explores Organic Computing (OC) principles for designing and implementing a potentially secure system/network architecture to meet the emerging cyber threats targeting both IT and OT infrastructure of ICS/CPS - (Haehner <i>et al.</i>, 2013) 4. The CockpitCI Approach which presented a technology-oriented cyber threat awareness improvement approach as a measure towards effective cybersecurity in ICS environments - (Cruz <i>et al.</i>, 2014) 5. A Hierarchical cross-layered design, game-theoretical approach with cross-layered security scheme for securing CPS/ICS - (Zhu, Rieger and Başar, 2011) 6. Security Enhancement Using Testbed (protocol security), or structured design approach with enhanced security features like Encryption and authentication, etc for ICS/CPS systems - (Ozturk and Aubin, 2011), (Belletini and Rrushi, 2008), (Majdalawieh <i>et al.</i>, 2006), (Rrushi, 2012), (Fovino <i>et al.</i>, 2009), (Edmonds <i>et al.</i>, 2007). 7. A Trusted Computing (TC) architecture that combines TC engines with real-time access control infrastructure for system protection. Functional by supporting application platforms for secure distributed applications and enforces the integrity of execution targets, thus preventing the running of untrusted software and guards against insider threats - (Burmester, 2013) 8. The application of effective key management technology solutions like Public Key Infrastructure (PKI) for securing the smart systems from cyber-breaches - (Metke and Ekl, 2010).
<p>STRATEGY IMPLEMENTATION STYLE:</p> <p>Security through scope and landscape investigations, and the structuring of policies, procedures, and technologies to meet security threats, vulnerabilities, and potential attack patterns</p>	<ol style="list-style-type: none"> 9. A method that utilizes security patterns (a packaged solution to a recurrent problem) to analyse, build, and evaluate a secure SCADA system. Security patterns are then used as tools to design a secure SCADA system that manages the identified attacks - (Fernandez <i>et al.</i>, 2009). 10. Threat analysis and risk assessment covering four different perspectives, which include; assets, threats, vulnerabilities, and damages. And strong accent on defense-in-depth - (Dong <i>et al.</i>, 2015), (Lu <i>et al.</i>, 2013). 11. Critical Security Controls Framework that proffers cybersecurity through the combination of the outcomes of improved malware reporting, and gateway monitoring with internal and external security intelligence resources - (Northcutt, 2014). 12. Context-aware security approach consisting of three (3) broad level security aspects; sensing security, cyber-security, and control security - (Wang <i>et al.</i>, 2010). 13. A Big Data algorithmic (data-intensive) approach for defending and safeguarding SCADA system from malware attacks - (Shyamasundar, 2013). 14. A modelling technique based on weighted Attack and Defense Trees (ADT) structures on ICS/Scada architectures representing attacks through Multi-Terminal Binary Decision Diagrams (MTBDD) that allow for the identification of most

Security Approach and Overview	Concept Description
	<p>probable attack scenarios, in term of probability cost and impact, and proffer mitigation countermeasures for located breaches - (Bobbio <i>et al.</i>, 2013).</p> <p>15. The application of system-theoretic approaches to the real-time security of smart grids, which encompasses two main parts: contingency analysis (CA) and system monitoring - (Mo <i>et al.</i>, 2011).</p> <p>16. Security framework based on adherence to the security objectives of ICS/CPS - (Lu <i>et al.</i>, 2015).</p>
<p>ATTACK MODELLING:</p> <p>Security through the replication of cyberattacks on real or emulator environments and studying the direct effects and impacts, and making the most of the observations to bring about defensive solutions</p>	<p>17. A self-contained unified modelling control-theoretic approach to securing ICS systems which employs geometric control, deterministic static detection concepts for various cyberattack modes – (Pasqualetti, Dorfler and Bullo, 2011), (Pasqualetti, Dorfler and Bullo, 2015).</p> <p>18. A framework for modelling the security of a cyber–physical systems in which the adversarial behaviour is controlled by a threat model that captures – in a unified manner – the cyber aspects (with discrete values) and the physical aspects (with continuous values) of the cyber–physical system - (Burmester, Magkos and Chrissikopoulos, 2012).</p> <p>19. The modelling and analysis of Vulnerability of information and communication (cyber) network using concepts of discovery, access, feasibility, communication speed and detection of threat - (Srivastava <i>et al.</i>, 2013).</p> <p>20. Using simulation modelling approach for representing computer networks and intrusion detection systems (IDS) to efficiently mimic cyber-attack scenarios and detection potentials – (Kuhl <i>et al.</i>, 2007).</p> <p>21. Using Hybrid Attack Graph (HAG) for modelling both the physical and cyber components of the attack. The HAG provides insight into potential attack vectors, and potential points of security improvements - (Hawrylak <i>et al.</i>, 2012).</p>
<p>ATTACK DETECTION:</p> <p>Security through the uncovering of, attacks, faults, and malfunction because of attacks, and proffering isolation and recovery controls.</p>	<p>22. A System Theoretical Accident Model and Process (STAMP) approach to safety and security, which views systems as dynamic entities with safety and security control issues. STAMP methodology is based on three supports: (i) safety control structure, (ii) safety constraint, and (iii) process model – (Nourian and Madnick, 2014)</p> <p>23. A Model-based Approach to Self-Protection that employs autonomic computing technology to monitor system performance, and proactive estimation of imminent attacks for a given system model of a physical infrastructure – (Chen and Abdelwahed, 2014)</p> <p>24. Intrusion/Anomaly Detection Systems and Approach for attack identification and remediation in ICS/CPS environments – (Krotofil and Gollmann, 2013), (Pasqualetti, Dörfler and Bullo, 2013), (Zhu, 2010), (Hadžiosmanović, Bolzoni and Hartel, 2012), (Goldenberg and Wool, 2013), (Fovino <i>et al.</i>, 2010), (Hieb, Graham and Guan, 2009), (Rrushi, 2011), (Hadžiosmanović <i>et al.</i>, 2012), (Rrushi and Campbell, 2009), (Tupakula and Varadharajan, 2014), (Méndez <i>et al.</i>, 2011).</p> <p>25. Recommends the adoption of the NIST Guide to ICS Security, with specific highlights security-oriented network architectures via network segregation practices, as well as disengaging redundant connections, and maintaining a closed-loop (air-gap) as much as possible – (Stouffer, Falco and Scarfone, 2011)</p> <p>26. Enabling security through configuration management setup with application whitelisting system to lessen attacks that bypass firewalls and trick users into executing malware - (Beechey, 2010).</p> <p>27. A generic hierarchical model for performance analysis of intrusion detection techniques as applied to a cyber-physical system ICS/CPS consisting of mobile nodes with navigation, manipulation, sensing, and actuating capability. Intrusion detection techniques developed for malicious discovery of ICS/CPS directed attacks include; positional discontinuity and</p>

Security Approach and Overview	Concept Description
	<p>enviro-consistency, with propositions of potentially optimal design settings under which the reliability of the ICS/CPS may be maximized – (Mitchell and Chen, 2011).</p> <p>28. Security through a coupled design framework that adopts the cyber configuration policy of Intrusion Detection Systems (IDSs) and the robust control of dynamical system. Uses design algorithms based on value iteration methods and linear matrix inequalities for computing the optimal cyber security policy and control laws – (Yuan <i>et al.</i>, 2013).</p> <p>29. Using a unified modelling framework and an advanced detection procedure requiring only local network knowledge for implementation. The modelling framework captures details about system properties like network components malfunction and measurements corruption, and uses same to guide the detection of cyberattacks – (Dorfler, Pasqualetti and Bullo, 2011).</p> <p>30. Modelling the causal relationship between devices in a cyber-physical system using a Bayesian Networks and a resultant expansion called ‘causal event graphs’, used to model deterministic signatures which can be used by an intrusion detection system to classify events – (Pan <i>et al.</i>, 2013), (Adhikari, Morris and Pan, 2014).</p>
<p>ATTACK CATEGORISATION:</p> <p>Security through the categorisation of cyberattacks based on the mode adopted for exploiting ICS systems, and engaging specific control to meet specific attack mode.</p>	<p>31. Concepts that project categorisation using taxonomy of cross-domain attack patterns – (Yampolskiy <i>et al.</i>, 2013), (Pasqualetti, Dorfler and Bullo, 2011).</p> <p>32. Development of defensive solutions to guard against the excessive flooding of device controllers and systems with invalid traffic data – (H. Zhang <i>et al.</i>, 2013), (Yuan <i>et al.</i>, 2013).</p> <p>33. Jamming attack – using game theoretical framework to study the interactive decision-making process of attacks, and effectively congestion communication channels, to slow or bar communication – (Li <i>et al.</i>, 2013).</p> <p>34. Solution through the study of the performance of Stealthy Deception Attacks from a systems perspective - (Kwon, Liu and Hwang, 2013).</p> <p>35. Solution potential against Man in the middle attack – the interception of correct messages, and sending of false messages to a devices or operator – (Saltzman and Sharabani, 2009).</p> <p>36. Security against the access and interpretation of encrypted or secure information using compromised-key attacks - (Chalkias, Baldimtsi and Stephanides, 2008)</p> <p>37. Study and proposition of new detection scheme against replay attacks based on prior control system solutions – (Tran, Shin and Lee, 2013).</p> <p>38. Security solution against Eavesdropping – the listening in on information communicated by cyber-physical systems - (Kao and Marculescu, 2007)</p>

Table A-24: Comparative Review of ICS Security Risk Management (Assessment and Reduction) Methods

Risk Method	Author(s)	Concepts and Attributes	Scope & Limitation	Application
Industrial Control System Cyber Defence Triage Process (ICS-CDTP)	Cook <i>et al</i> (2017)	Combines: Diamond Model of Intrusion Analysis (Caltagirone, Pendergast and Betz, 2013), Mandiant Attack Lifecycle Model (Mandiant, 2013), and the CARVER Matrix (Schnaubelt, Larson and Boyer, 2014). Framework process include: Attack behaviour modelling, investigation of deployed architectures, antagonistic target determination, attack option analysis, security testing and remediation, security, monitoring, and incident response planning.	Framework consider both technical and non-technical aspects of security. However, non-technical aspects only include attack capabilities, and does not consider human-factor defence capabilities	Generic ICS System
Quantitative Cyber Security Risk Assessment Methodology for SCADA	Woo and Kim (2015)	Quantifying vulnerabilities from historic data, threats, and asset value in terms of outage costs using the optimal power flow and power flow tracing concept. Optimal power flow estimation is derived by the minimum cost of power generation for all generators subject to generators and line capacities restriction	Considers only technology aspects, does not consider Human aspect of SCADA vulnerabilities	Power Generation
Improved Risk Assessment Method for SCADA Information Security	Markovic-Petrovic and Stojanovic (2014)	uses weighting factors to determine optimum level of security investment, define varied levels of acceptable risks, and achieve better estimation of loss expectancy, i.e. Return on Security Investment - ROSI	Considers only technology aspects, does not consider non-technical (human) weighting factors in the evaluation of ROSI.	Hydro-Power System

Risk Method	Author(s)	Concepts and Attributes	Scope & Limitation	Application
The Phasor Measurement Unit (PMU)-based risk assessment framework for SCADA	Yan <i>et al</i> (2013)	Risk assessment steps included: identification of system configurations, identification of security vulnerabilities, quantification of vulnerabilities using the Duality Element Relative Fuzzy Evaluation Method (DERFEM), determination of intrusion scenario using attack graph techniques, and attack probability evaluation.	Considers only technical risk assessment, does not consider non-technical risk assessment.	Power Grid
Quantitative Threat-Risk Index Model (QTRIM)	Beitel <i>et al</i> (2004)	Predicting security risks in relations to terrorist attacks against a national infrastructure. Risk is evaluated on a balanced scorecard framework, and from terrorist-specific constrictions, goals, system value, logistics, and opportunities.	Considers only technical risk assessment, does not consider non-technical risk assessment.	Critical Infrastructure
Application of CORAS-based risk assessment methodology to SCADA	Francia <i>et al</i> (2012)	Specific steps in this application approach include: identification of assets and relative importance levels, outline of threats and vulnerabilities, and threat modelling.	Considers both technical and non-technical aspects of security. However, non-technical aspects do not include the quantitative evaluation of end-user security vulnerability levels	Prototype Industrial Control System
Cyber security risk assessment methodology for instrumentation and control system processes	Song <i>et al</i> (2012)	Cyber security risk assessment at component and system design, and equipment supply stages plant development. Steps include: system identification and cyber security modelling, analysis of assets and impacts to overall system, threat analysis, vulnerability analysis, security control design, and penetration testing	Does not consider non-technical security risk assessment attributes	Nuclear Power Plant
Security risk assessment methodology for instrumentation and control system processes	Shin <i>et al</i> (2017)	Adopts Bayesian network and event tree models to evaluate cyber security risk for nuclear instrumentation and control systems. Method is guided by domain-specific standards, e.g. U.S. NRC Regulatory Guide 5.71.	Considers only technical risk assessment, does not consider non-technical security risk assessment attributes	Nuclear Power Plant

Risk Method	Author(s)	Concepts and Attributes	Scope & Limitation	Application
Real-time Monitoring, Anomaly detections, Impact analysis, and Mitigation strategies (RAIM) SCADA security framework	Ten <i>et al</i> (2010)	Real-time monitoring and anomaly detection modules are aimed to achieve continuous monitoring of system logs, and the aggregation of anomaly data. Impact analysis module comprise of: cybernet capture of system configurations, power flow simulations, calculation of vulnerability index, and security improvement.	Considers only technical risk assessment. Does not consider non-technical security vulnerability and risk assessment/improvement factors.	Electric Power Control
ADversary View Security Evaluation (ADVISE) metrics-driven model	LeMay <i>et al</i> (2011).	combines system information, adversary information, and desired security metrics to produce quantitative metrics data. Model comprise a three-step process: (i) characterising adversaries and systems, (ii) attack graph development for potential attack descriptions, (iii) graph execution.	Considers both technical and non-technical aspects of security. However, model process does not consider human-factor defense capabilities attributes	Generic SCADA Networks
Quantitative Security Risk Reduction Estimation Methodology	McQueen <i>et al</i> (2006)	determining quantitative measurement of reduction risks in modified control system. Uses probabilistic attributes and evaluation, and time-dependent evaluations.	Considers only technical risk assessment. Does not consider non-technical security risk assessment attributes	SCADA Testbed
Two-indices methodology for quantitative assessment of the vulnerability of critical information systems	Baiardi <i>et al</i> (2009)	Based on a set of hierarchical-labelled hypergraphs reflecting the security dependencies between infrastructure components	Considers only technical risk assessment. Does not consider non-technical security risk assessment attributes	Water Distribution Graph Representation
Network Security Risk Model (NSRM)	Henry and Haines (2009)	Model is based on directed graph representation of an attack, and is aimed at assisting the selection of risk management controls through the computation of risk measures for baseline and enhanced system states	Considers only technical risk assessment. Does not consider non-technical security risk assessment attributes	Crude oil pipeline pump station

Table A-25: A Sample Collection Security Metrics from selected literature

(A). Technology-Oriented Security Metrics (Tc)

Note: Cap = Capability, Vul = Vulnerability, Proact = Proactive, React = Reactive, c = computable, m = Measurable, cnt-b = count-based, prop-b = proportion-based

No.	Metric Quantities	Source	Characterisation
Tc1	Rogue Change Days	(McQueen <i>et al.</i> , 2008; Homeland Security, 2009)	(Vul), Proact & React, c, t-b
Tc2	Security Evaluation Deficiency Count		(Vul), Proact, c, cnt-b
Tc3	Data Transmission Exposures		(Vul), Proact & React, c, cnt-b
Tc4	Reachability Count		(Vul), Proact & React, c, cnt-b
Tc5	Attack Path Depth		(Vul), Proact, c, cnt-b
Tc6	Known Vulnerability Days		(Vul), Proact & React, c, cnt-b
Tc7	Password Crack Time		(Cap), Proact, m, t-b
Tc8	Worst Case Loss		(Vul), Proact, c, cnt-b
Tc9	Detection Mechanism Deficiency Count		(Cap), Proact & React, c, cnt-b
Tc10	Restoration time		(Cap & Vul), React, m, t-b
Tc11	Root Privilege count		(Cap & Vul), Proact & React, c, cnt-b
Tc12	Vulnerability Counts	(Abbadi, 2006)	(Vul), Proact & React, c, cnt-b
Tc13	Number of Virus infections		(Vul), React, c, cnt-b
Tc14	Number of SPAM blocked		(Vul), React, c, cnt-b
Tc15	Number of port probes		(Cap & Vul), React, c, cnt-b
Tc16	Number of incidents		(Cap & Vul), Proact & React, c, cnt-b
Tc17	Number of successful Logons compromise		(Vul), Proact & React, c, cnt-b
Tc18	Number of unsuccessful Logons compromise		(Cap), Proact & React, c, cnt-b
Tc19	Probability of attack	(Wang <i>et al.</i> , 2008b; Chejara, Garg and Singh, 2013)	(Cap & Vul), Proact, c, prob-b
Tc20	Cumulative probability of attack		(Cap & Vul), Proact, c, prob-b
Tc21	Expected Path Length	(Abraham and Nair, 2014a, 2015a)	(Cap), Proact, c, cnt-b
Tc22	Probability Path		(Cap & Vul), Proact, c, prob-b

Tc23	Node Rank		(Cap & Vul), Proact & React, c, cnt-b
Tc24	Number of Path	(Keramati and Keramati, 2014)	(Cap & Vul), Proact, c, cnt-b
Tc25	Shortest Path		(Cap & Vul), Proact, c, cnt-b
Tc26	Vulnerability Impact		(Vul), Proact, c, cnt-b
Tc27	Weighted number of attack paths		(Cap & Vul), Proact, c, cnt-b
Tc28	Probability of Vulnerability Exploitation		(Vul), Proact, c, prob-b
Tc29	Probability of Attack Path		(Cap & Vul), Proact, c, prob-b
Tc30	Number of Shortest Path		(Cap & Vul), Proact, c, prop-b
Tc31	Vulnerability danger degree		(Vul), Proact, c, prop-b
Tc32	Vulnerability Emergency Degree		(Vul), Proact, c, prop-b
Tc33	Exploitability	(Tupper and Zincir-Heywood, 2008)	(Cap & Vul), Proact, c, cnt-b
Tc34	Attackability		(Cap & Vul), Proact, c, cnt-b
Tc35	Vulnerability Base Score	(FIRST, no date; Keramati, Akbari and Keramati, 2013)	(Cap & Vul), Proact & React, c, cnt-b
Tc36	Exploitability		(Cap & Vul), Proact & React, c, cnt-b
Tc37	Attack vector		(Cap & Vul), Proact & React, m, cnt-b
Tc38	Attack Complexity		(Cap & Vul), Proact & React, m, cnt-b
Tc39	Privilege Required		(Cap & Vul), Proact & React, m, cnt-b
Tc40	User Interaction		(Cap & Vul), Proact & React, m, cnt-b
Tc41	Vulnerability Impact		(Cap & Vul), Proact & React, c, cnt-b
Tc42	Confidentiality impact		(Cap & Vul), Proact & React, m, cnt-b
Tc43	Integrity Impact		(Cap & Vul), Proact & React, m, cnt-b
Tc44	Availability Impact		(Cap & Vul), Proact & React, m, cnt-b
Tc45	Vulnerability Temporal Score		(Cap & Vul), Proact & React, c, cnt-b
Tc46	Exploit code maturity		(Cap & Vul), Proact & React, m, cnt-b
Tc47	Remediation level		(Cap & Vul), Proact & React, m, cnt-b
Tc48	Report Confidence		(Cap & Vul), Proact & React, m, cnt-b
Tc49	Vulnerability Environmental Score		(Cap & Vul), Proact & React, c, cnt-b
Tc50	Modified Base metrics		(Cap & Vul), Proact & React, c, cnt-b
Tc51	Confidentiality Requirements		(Cap & Vul), Proact & React, m, cnt-b
Tc52	Integrity requirements		(Cap & Vul), Proact & React, m, cnt-b
Tc53	Availability Requirements		(Cap & Vul), Proact & React, m, cnt-b

(B). Process-Oriented Security Metrics (Pr)

No.	Metric Quantities	Source	Characterisation
Pr1	Number of Policy Violations	(Abbadi, 2006)	(Vul), React, c, cnt-b
Pr2	Percent of Systems with formal risk assessments		(Cap), Proact, c, prop-b
Pr3	Percent of Systems with tested security controls		(Cap), Proact, c, prop-b
Pr4	Percent of weak passwords		(Vul), Proact, c, prop-b
Pr5	Number of Identified risks and severity		(Cap & Vul), Proact, c, cnt-b
Pr6	Number of systems with contingency plans		(Cap), React, c, cnt-b
Pr7	Percent of Users with no background checks		(Vul), Proact, c, prop-b
Pr8	Percent of users without security training	(Jonsson and Pirzadeh, 2011)	(Vul), Proact, c, prop-b
Pr9	Mean time to failure (MTTF)		(Cap & Vul), React, c, t-b
Pr10	Mean time to intrusion (MTTI)	(Jonsson and Pirzadeh, 2011; Al-Shehri <i>et al.</i> , 2017)	(Cap & Vul), React, c, t-b
Pr11	Mean time to catastrophic failure (MTTCF)		(Cap & Vul), React, c, t-b
Pr12	Mean time between failure (MTBF)		(Cap), React, c, t-b
Pr13	Mean time to recover (MTTR)	(Dacier, Deswarte and Kaâniche, 1996)	(Cap), React, c, t-b
Pr14	Mean effort to security failure (METF)		(Cap & Vul), React, c, t-b

(C). People-Oriented Security Metrics (Ppl)

No.	Metric Quantities	Source	Characterisation
Ppl1	Number of Personnel Needing Security Training	(Campbell, 2009)	(Cap & Vul), Proact & React, c, cnt-b
Ppl2	Number of successful human-facilitated attacks		(Vul), React, c, cnt-b
Ppl3	Number of thwarted human-facilitated attacks		(Cap), React, c, cnt-b
Ppl4	Number of incidents caused by terminated personnel		(Cap & Vul), Proact & React, c, cnt-b
Ppl5	Number of Technology Abuse Incidents		(Cap & Vul), Proact & React, c, cnt-b
Ppl6	Personnel Security Knowledge Rating	(Ani, H. M. He and Tiwari, 2016)	(Cap), Proact & React, m, cnt-b
Ppl7	Personnel Security Skill Rating		(Cap), Proact & React, m, cnt-b
Ppl8	Harmonised Personnel Security Rating		(Cap), Proact & React, m, cnt-b
Ppl9	Mean Human-factor Security Knowledge rating		(Cap), Proact, c, cnt-b
Ppl10	Mean Human-factor Security Skill Rating		(Cap), Proact, c, cnt-b
Ppl11	Mean Human-factor organisation security rating		(Cap), Proact, c, cnt-b

Appendix B: Figures

Figure B-1: Demonstrator System Testbed Setup (Screenshots)

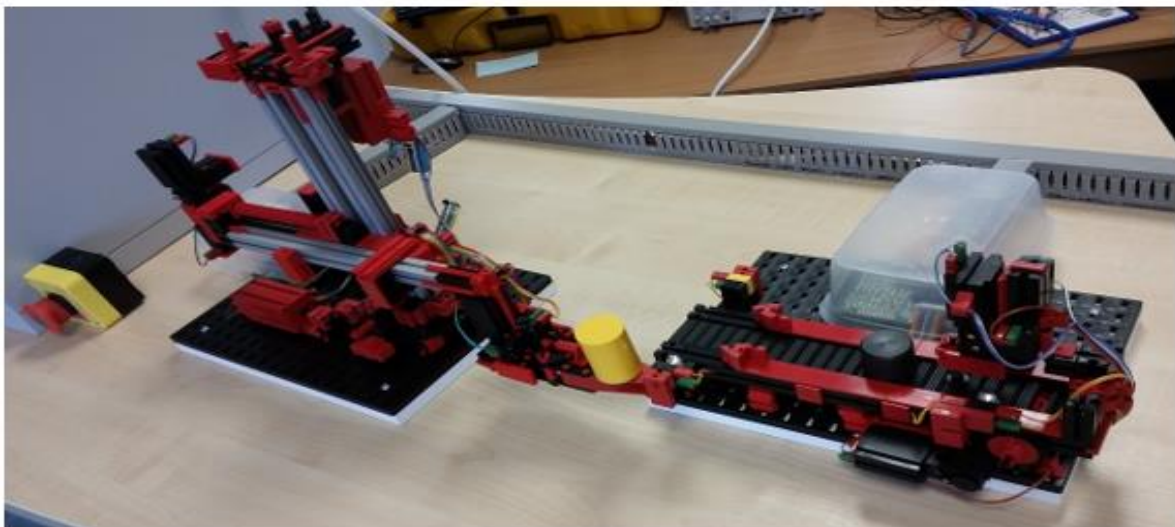


Figure B-2:Wiring Schematics for ICS-CS Conveyor Testbed Setup

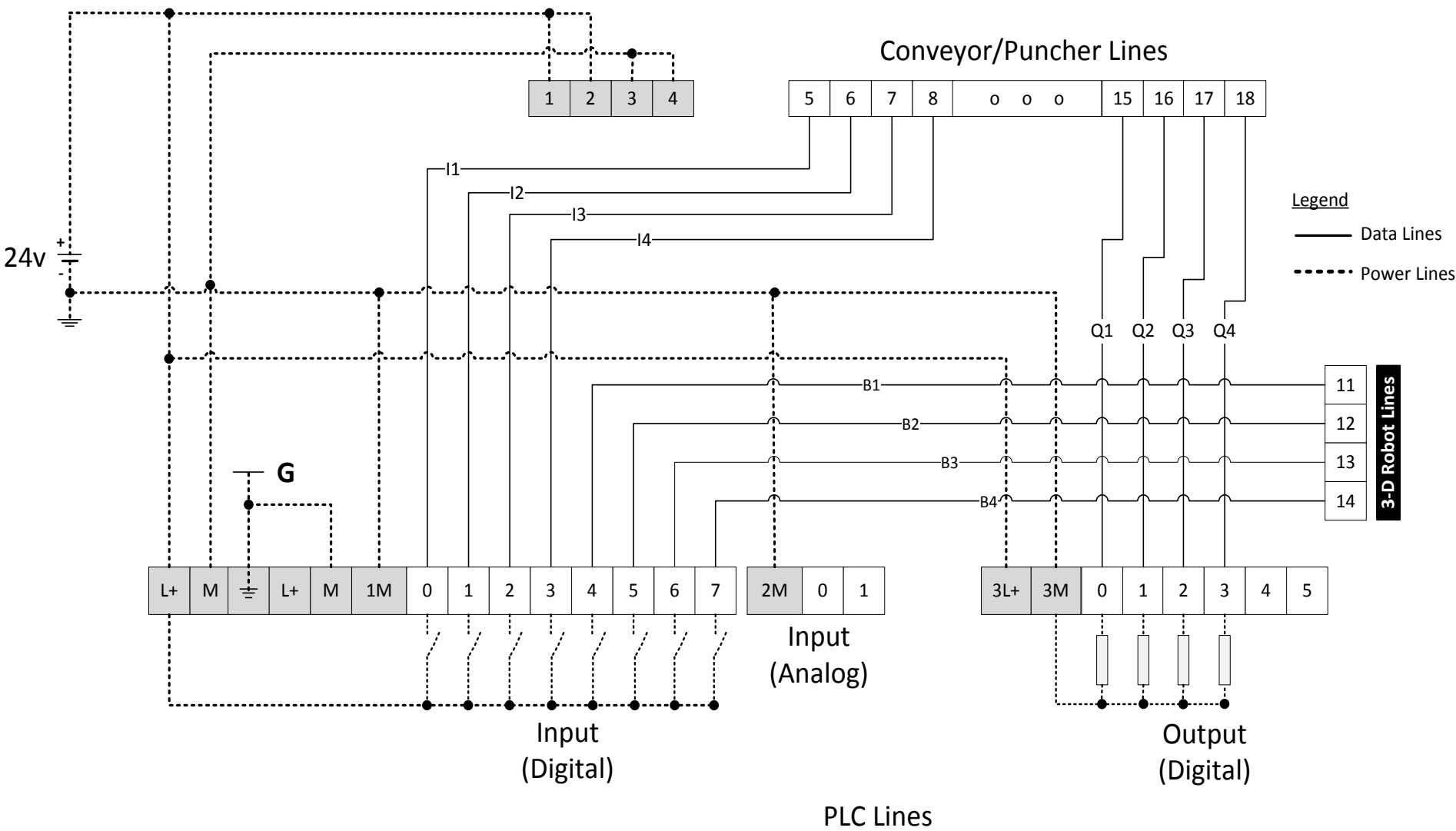


Figure B-3: Totally Integrated Portal ICS-CS Testbed Topology and Network Configurations

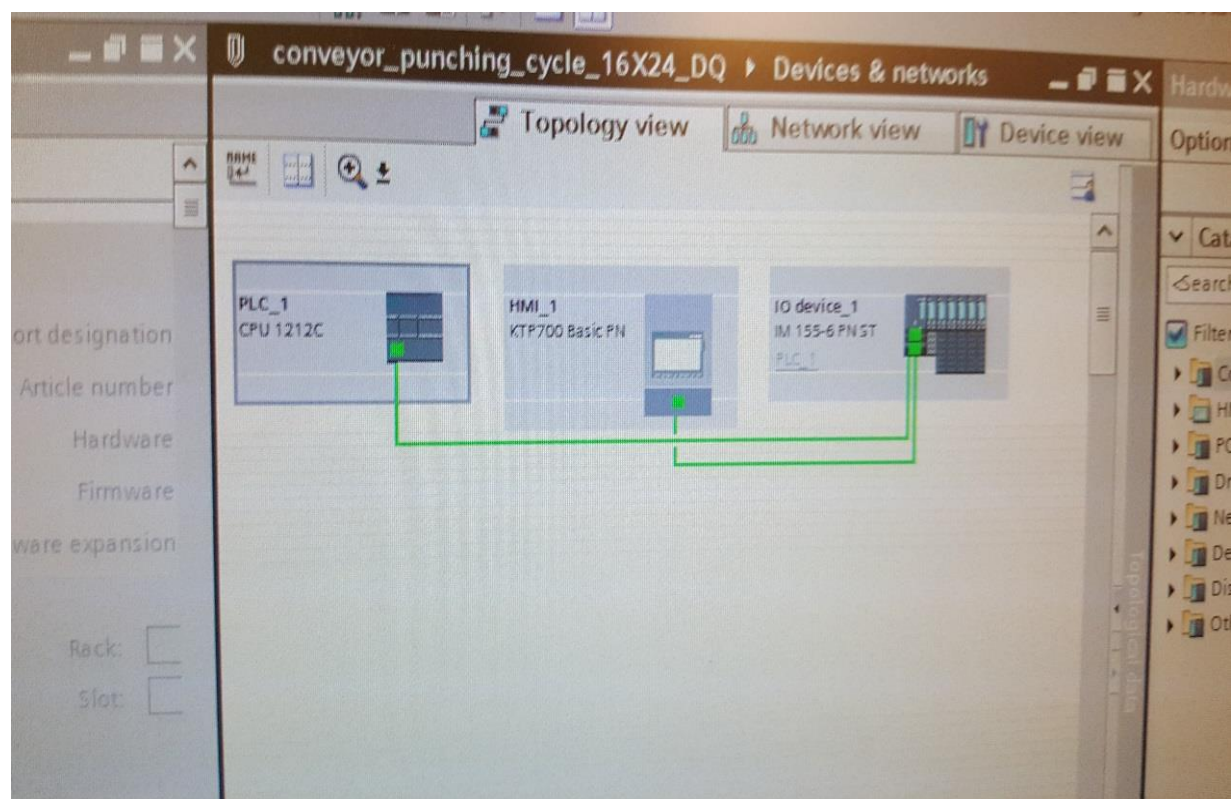
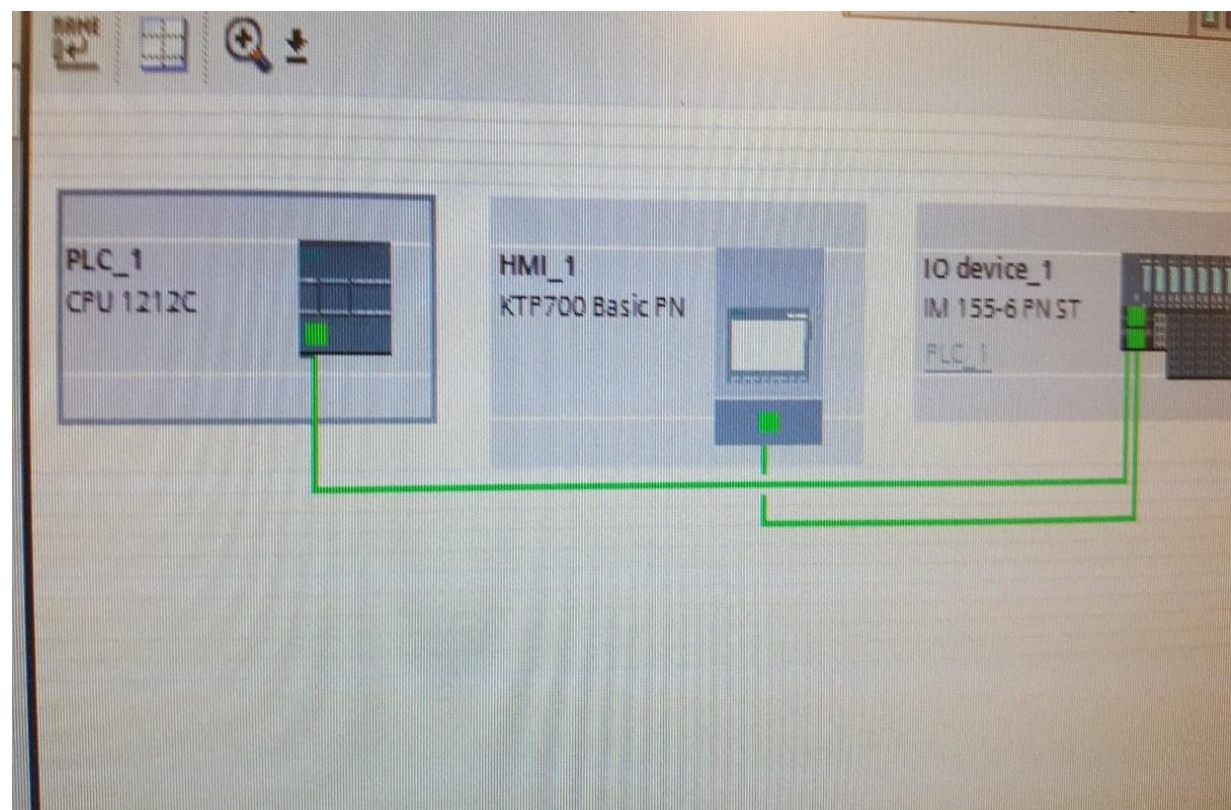


Figure B-4: Totally Integrated Portal ICS-CS Testbed Device and Network Configurations

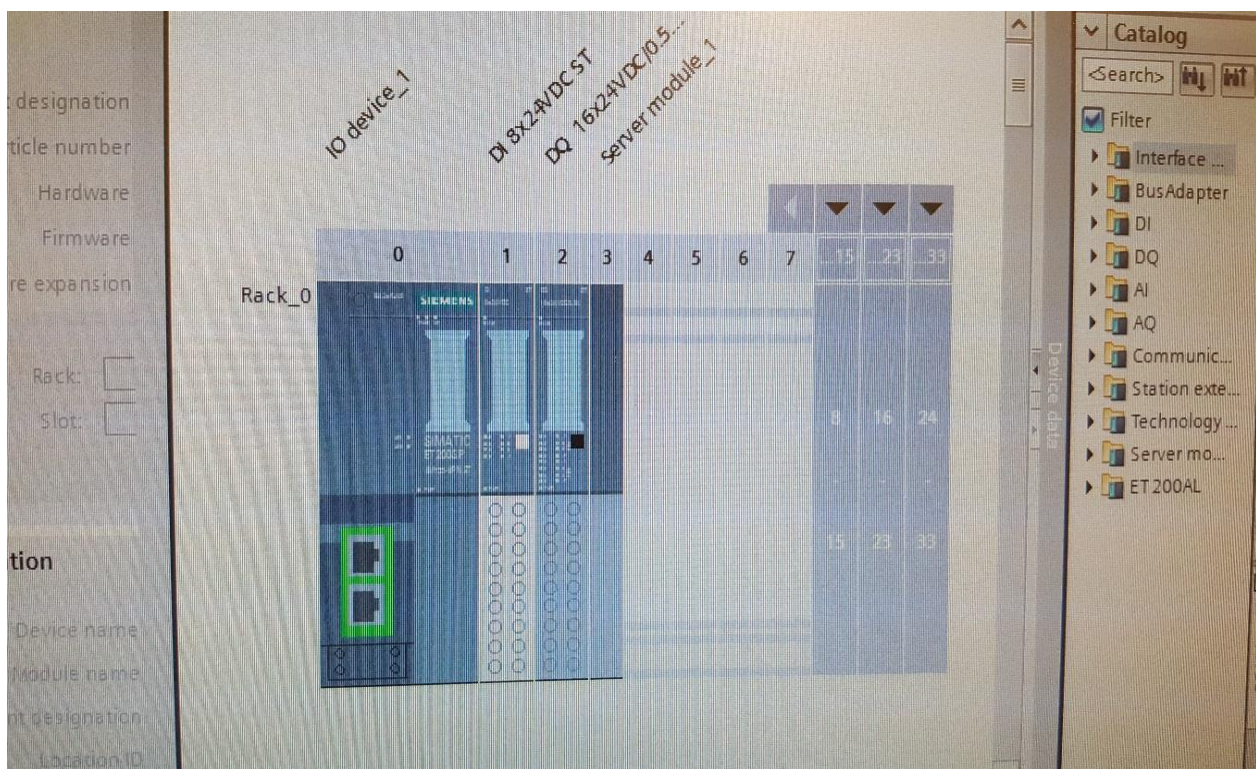
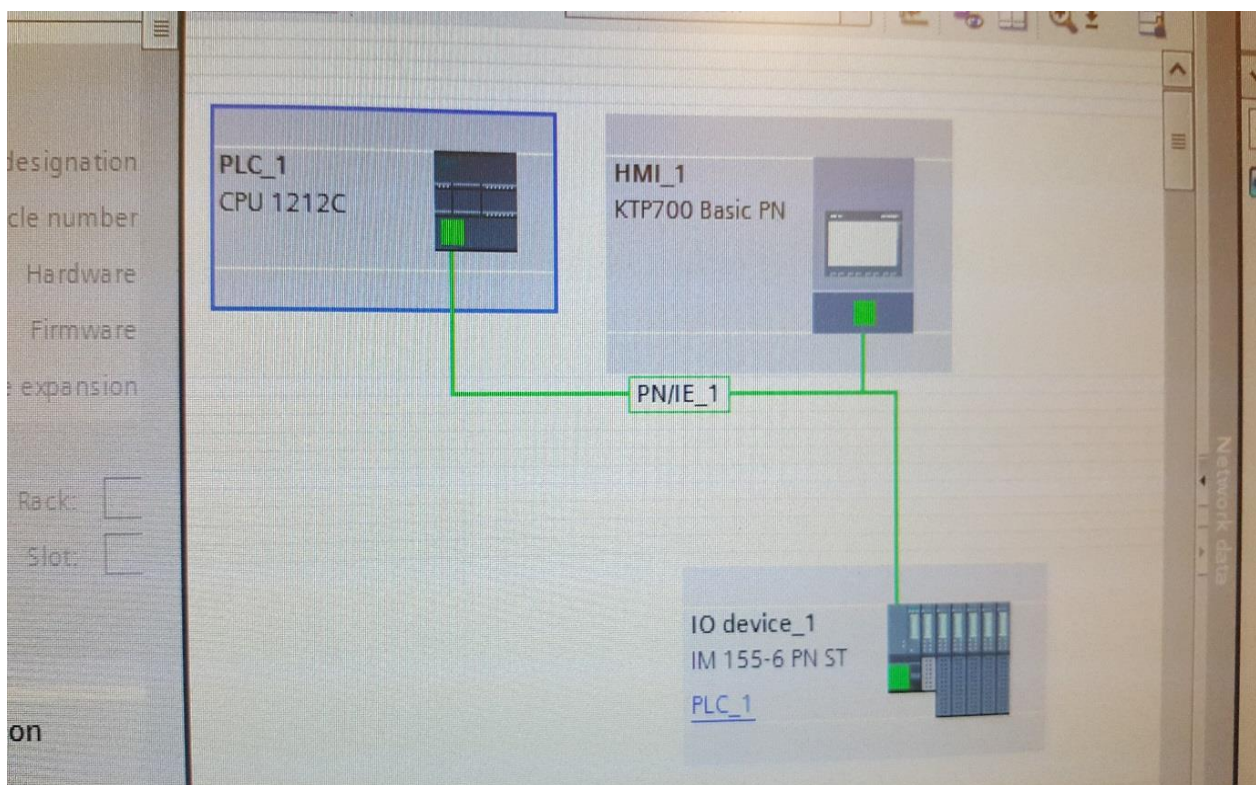


Figure B-5: Ladder Logic Programme for Conveyor Testbed Process Control (1)

Totally Integrated Automation Portal		
--------------------------------------	--	--

conveyor_punching_cycle_16X24_DQ_Screen_Added / PLC_1 [CPU 1212C DC/DC/DC] / Program blocks

Main [OB1]

Main Properties							
General							
Name	Main	Number	1	Type	OB	Language	LAD
Numbering	automatic						
Information							
Title	"Main Program Sweep (Cycle)"	Author		Comment		Family	
Version	0.1	User-defined ID					

Main			
Name	Data type	Default value	Comment
▼ Input			
Initial_Call	Bool		Initial call of this OB
Remanence	Bool		=True, if remanent data are available
▼ Temp			
Temp_1	Bool		
Constant			

Network 1:

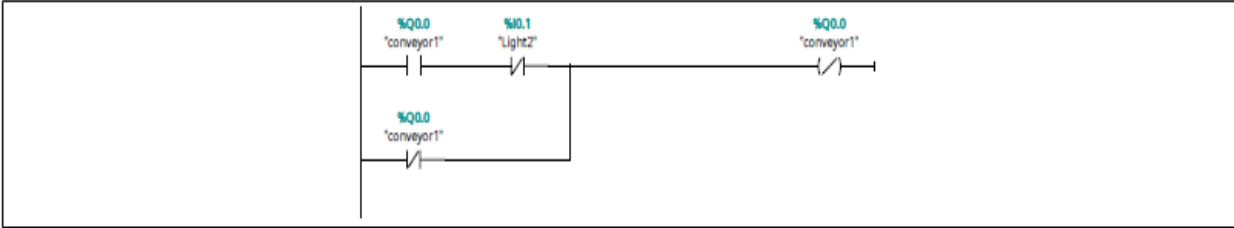
```

graph LR
    I00["%I0.0  
'Light1'"] --- I01["%I0.1  
'Light2'"]
    I01 --- Q00["%Q0.0  
'conveyor1'"]
    Q00 --- Q00_coil["%Q0.0  
'conveyor1'"]
    
```

Symbol	Address	Type	Comment
'conveyor1'	%Q0.0	Bool	
'Light1'	%I0.0	Bool	
'Light2'	%I0.1	Bool	

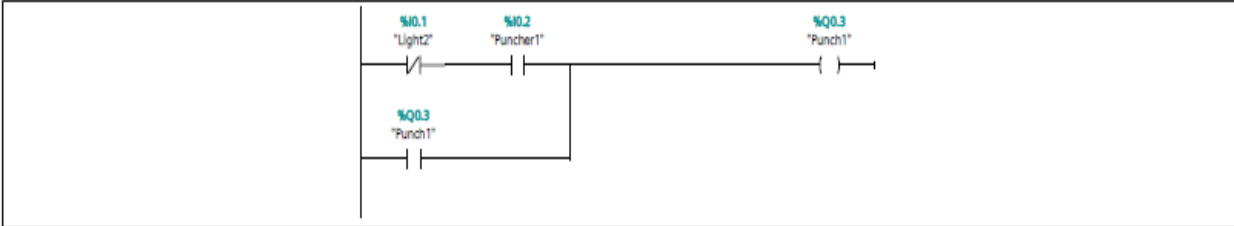
Figure B-6: Ladder Logic Programme for Conveyor Testbed Process Control
(2)

Network 2:



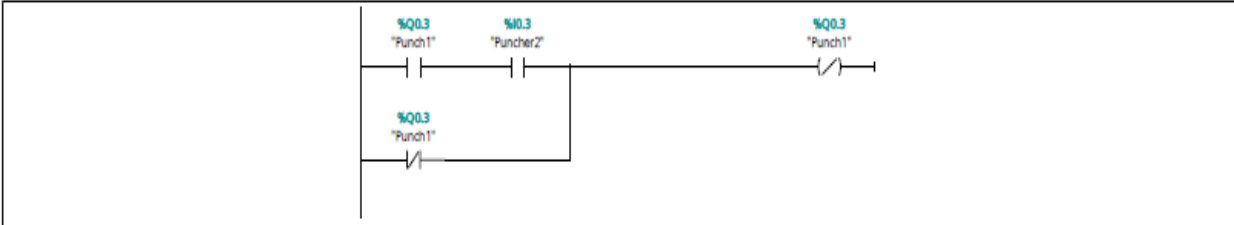
Symbol	Address	Type	Comment
'conveyor1'	%Q0.0	Bool	
'Light2'	%I0.1	Bool	

Network 3:



Symbol	Address	Type	Comment
'Light2'	%I0.1	Bool	
'Punch1'	%Q0.3	Bool	
'Puncher1'	%I0.2	Bool	

Network 4:



Symbol	Address	Type	Comment
'Punch1'	%Q0.3	Bool	

**Figure B-7: Ladder Logic Programme for Conveyor Testbed Process Control
(3)**

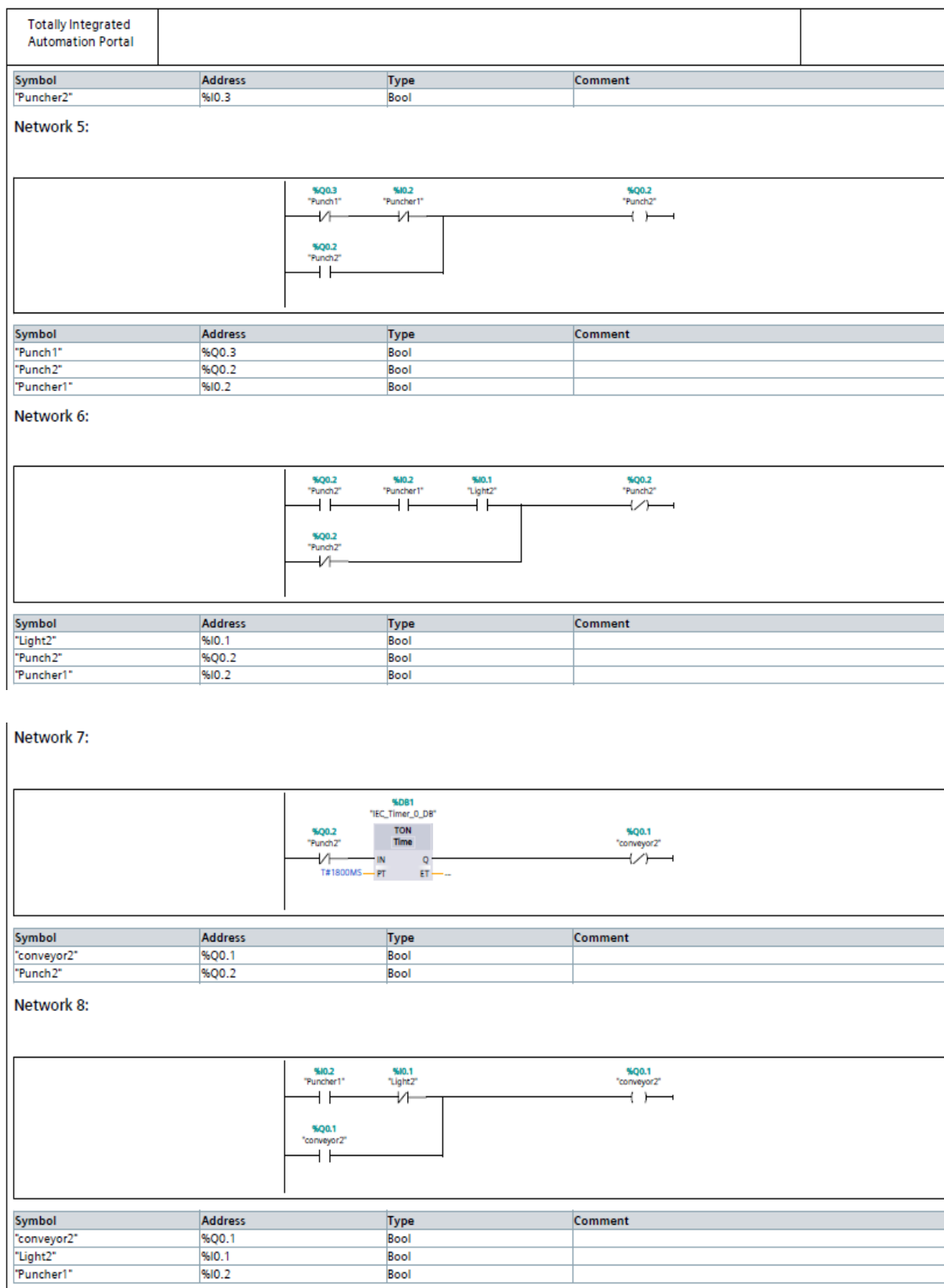


Figure B-8: ICS-CS Testbed Network Live Host Scan Results (Nmap)

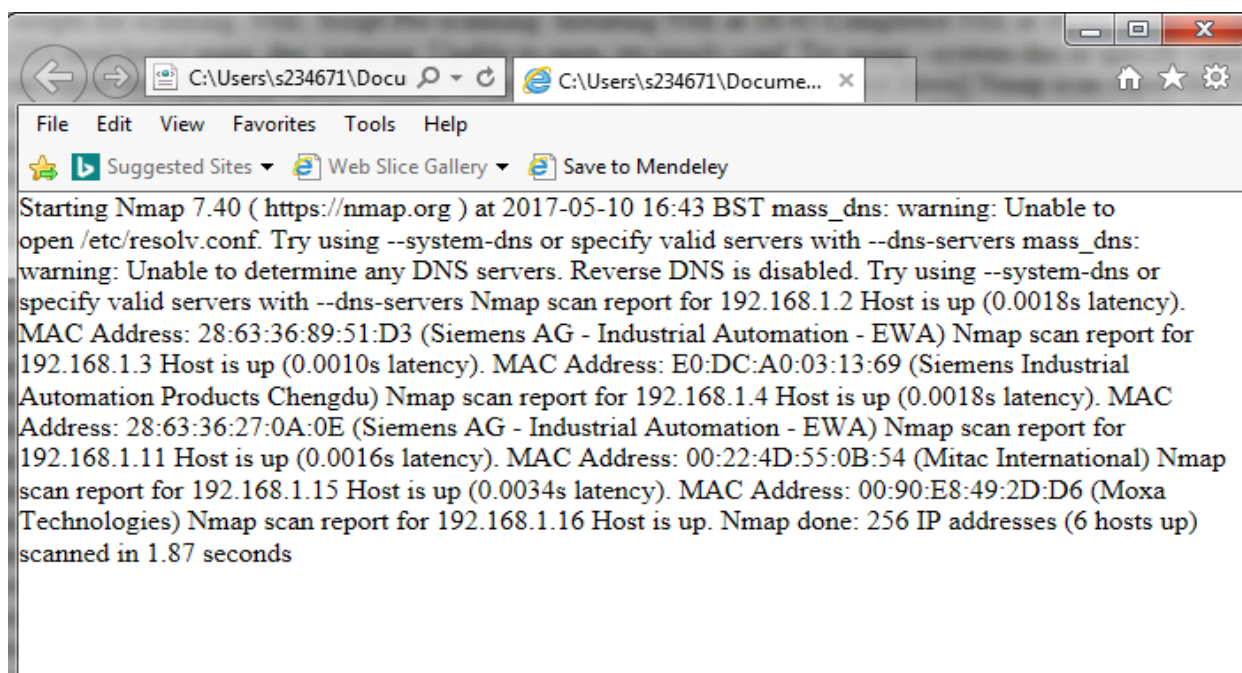


Figure B-9: ICS-CS Testbed Network Port Scan Results (Nmap)

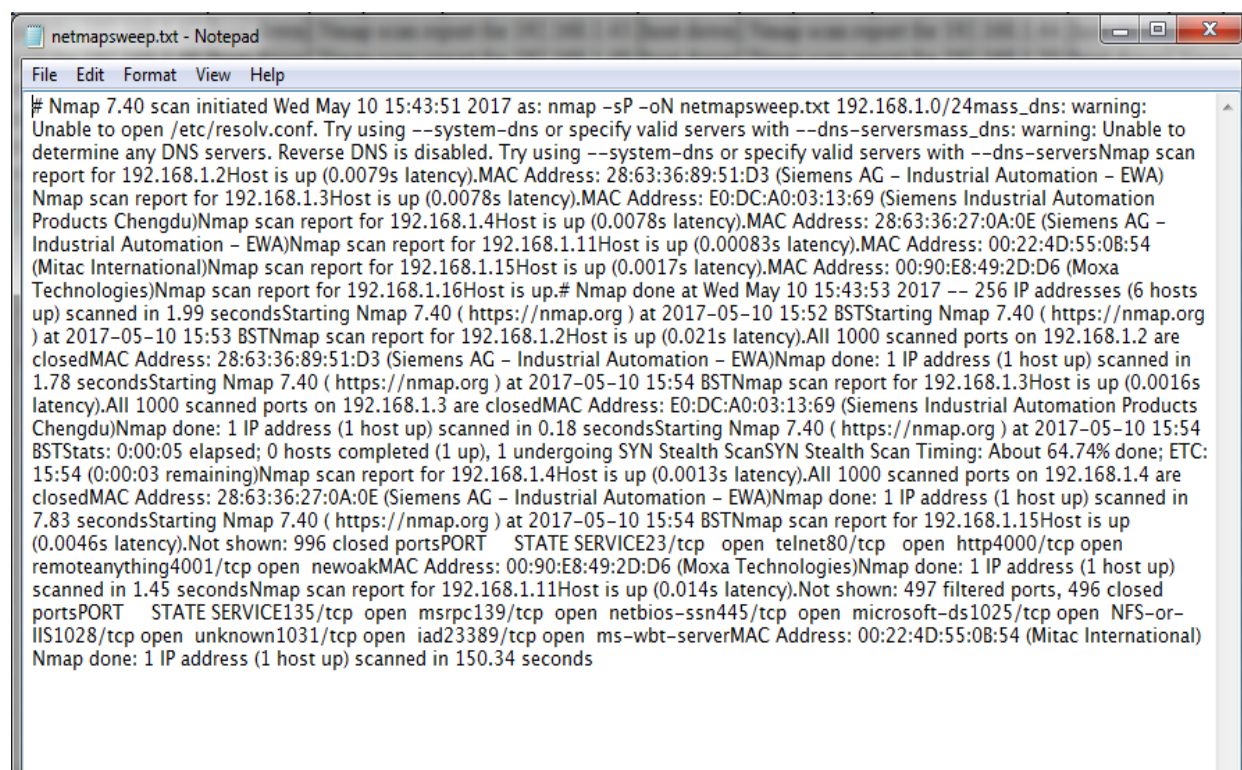


Figure B-10: ICS-CS Testbed Network Host Reachability Scan Results (Fping)

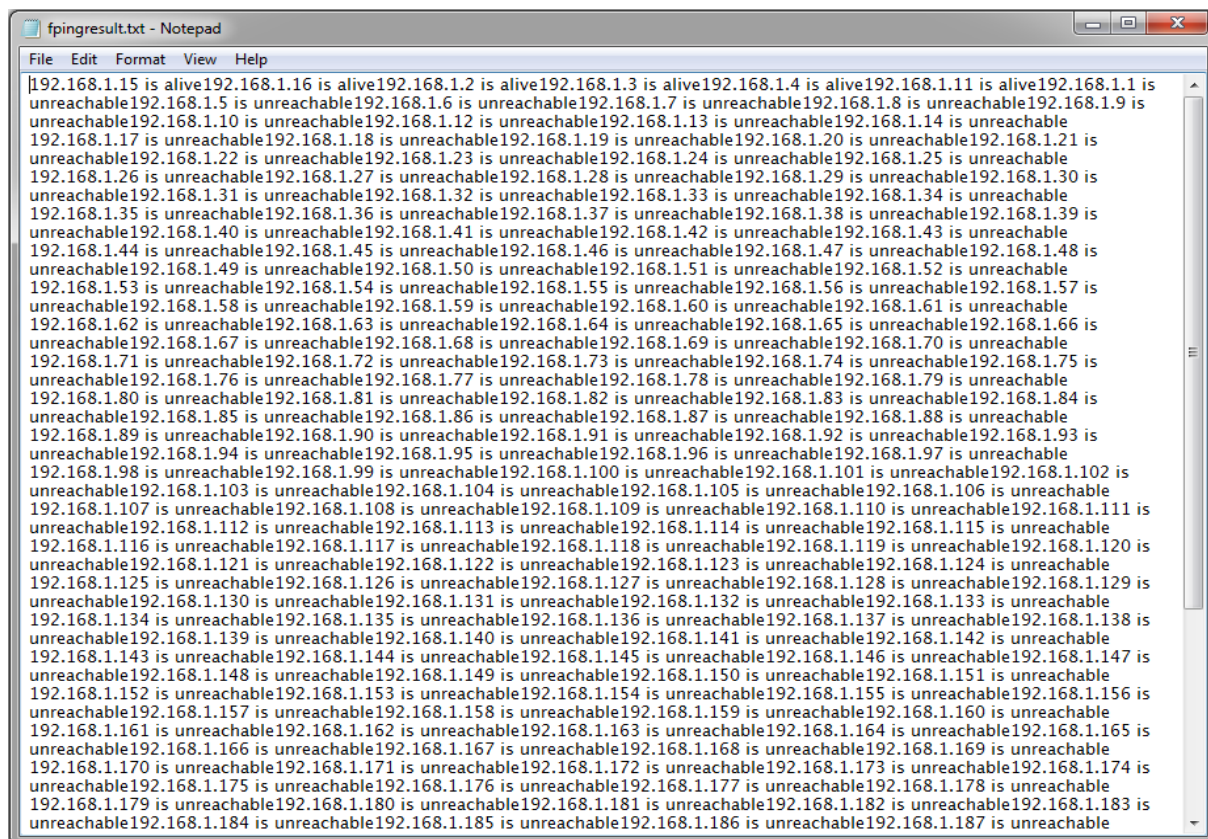


Figure B-11: ICS-CS Host Vulnerability Scan Summary (NESSUS)

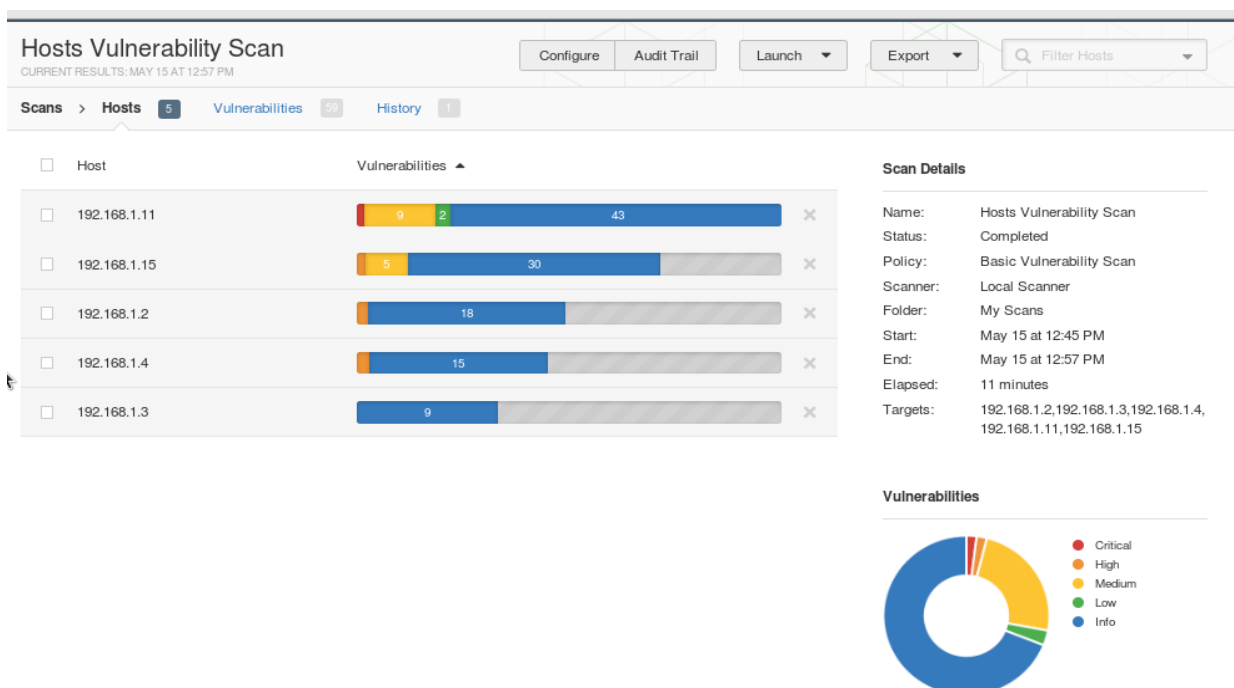
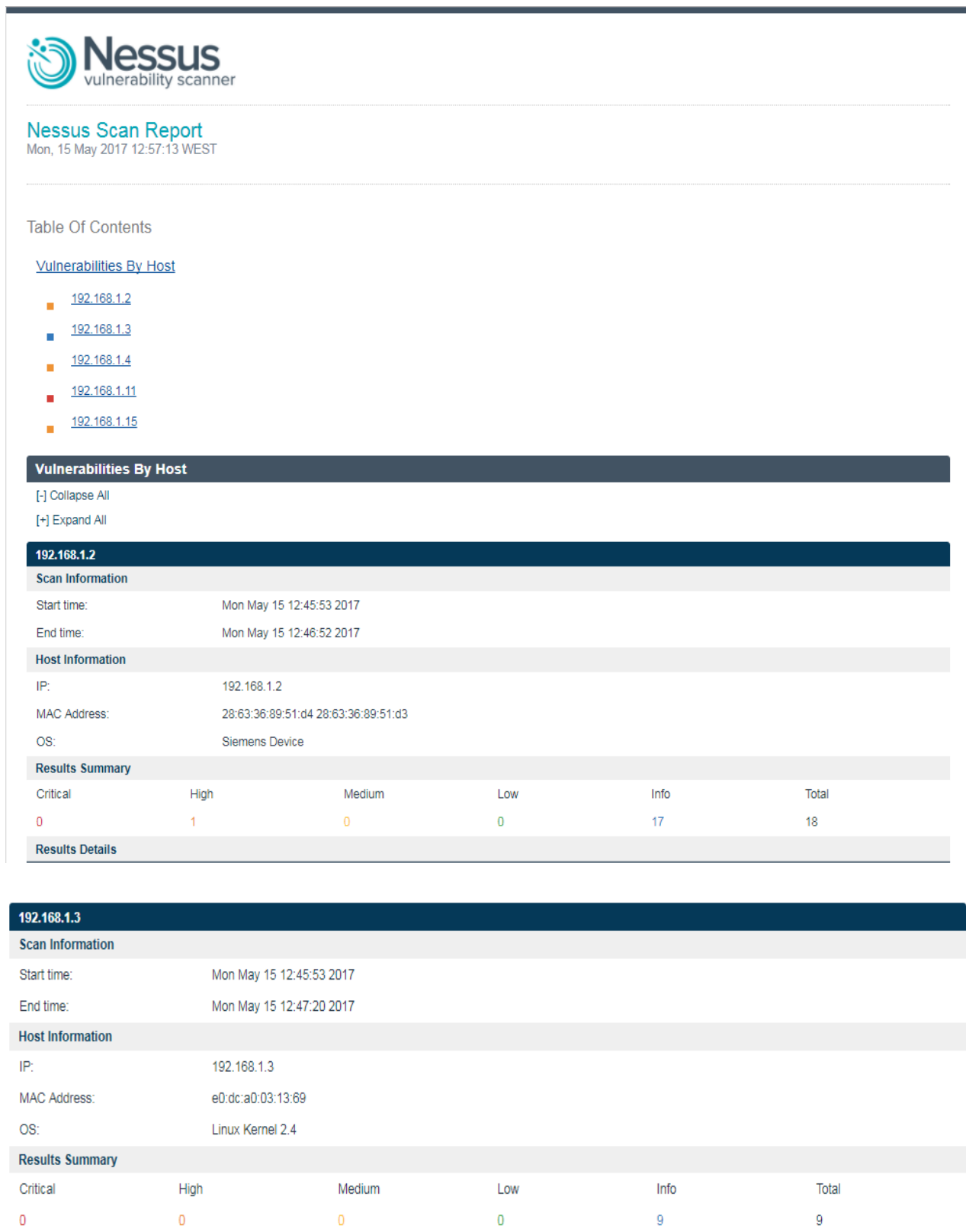


Figure B-12 : ICS-CS Testbed Network Vulnerability Scan (NESSUS)



192.168.1.4**Scan Information**

Start time: Mon May 15 12:45:53 2017
End time: Mon May 15 12:48:20 2017

Host Information

IP: 192.168.1.4
MAC Address: 28:63:36:27:0a:10 28:63:36:27:0a:0e 28:63:36:27:0a:0f
OS: Siemens Device

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	0	0	14	15

192.168.1.11**Scan Information**

Start time: Mon May 15 12:51:27 2017
End time: Mon May 15 12:57:13 2017

Host Information

Netbios Name: SSW748571C
IP: 192.168.1.11
MAC Address: 00:22:4d:55:0b:54
OS: Microsoft Windows 7 Enterprise

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	9	2	43	55

192.168.1.15**Scan Information**

Start time: Mon May 15 12:45:54 2017
End time: Mon May 15 12:47:47 2017

Host Information

DNS Name: gateway
IP: 192.168.1.15
MAC Address: 00:00:00:00:00:00 00:90:e8:49:2d:d6
OS: 3Com Baseline Switch, FreeBSD 4.4

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	5	0	27	33

Figure B-13: ICS-CS Testbed Network Control Workstation Privilege Escalation Attack Scenario – Windows Login Attempt



Figure B-14: ICS-CS Testbed Network Control Workstation Privilege Escalation Attack Scenario – TIA Portal Access

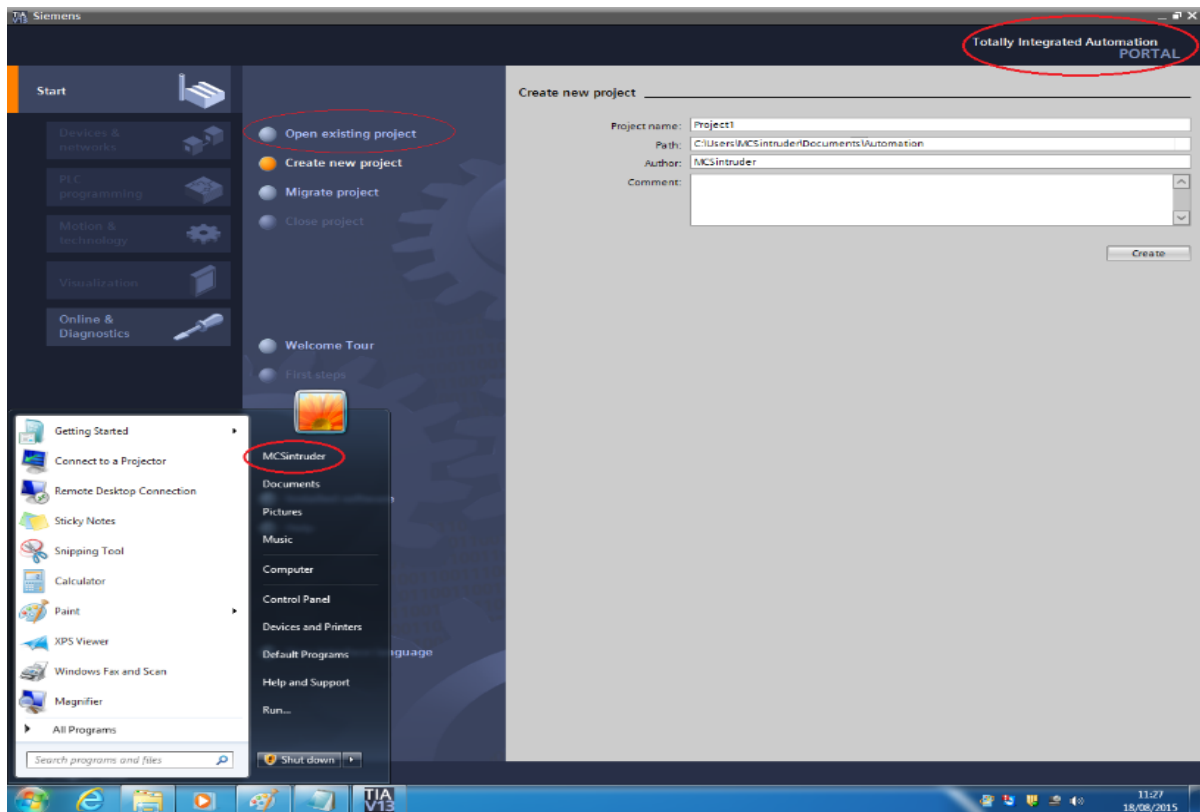


Figure B-15: PLC Denial-of-Service Attack Scenario: Hping3 Flood Instance

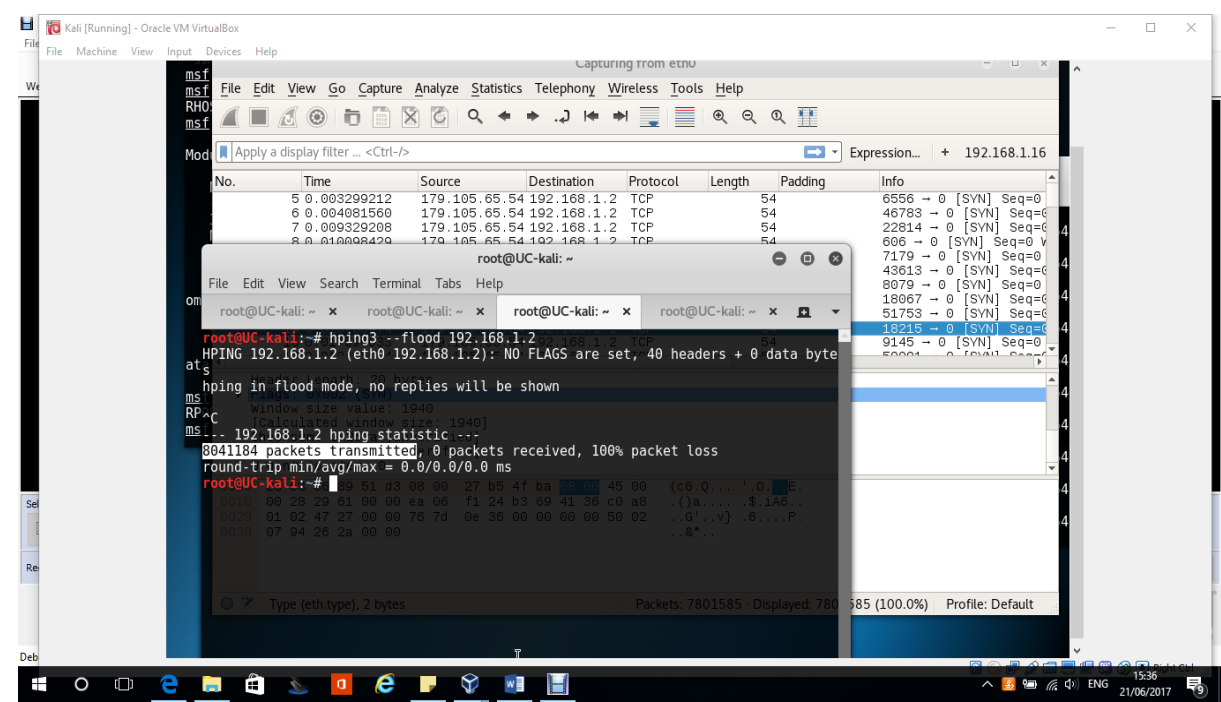


Figure B-16: PLC Denial-of-Service Attack Scenario: Packet Flood Analysis – 1 (Wireshark)

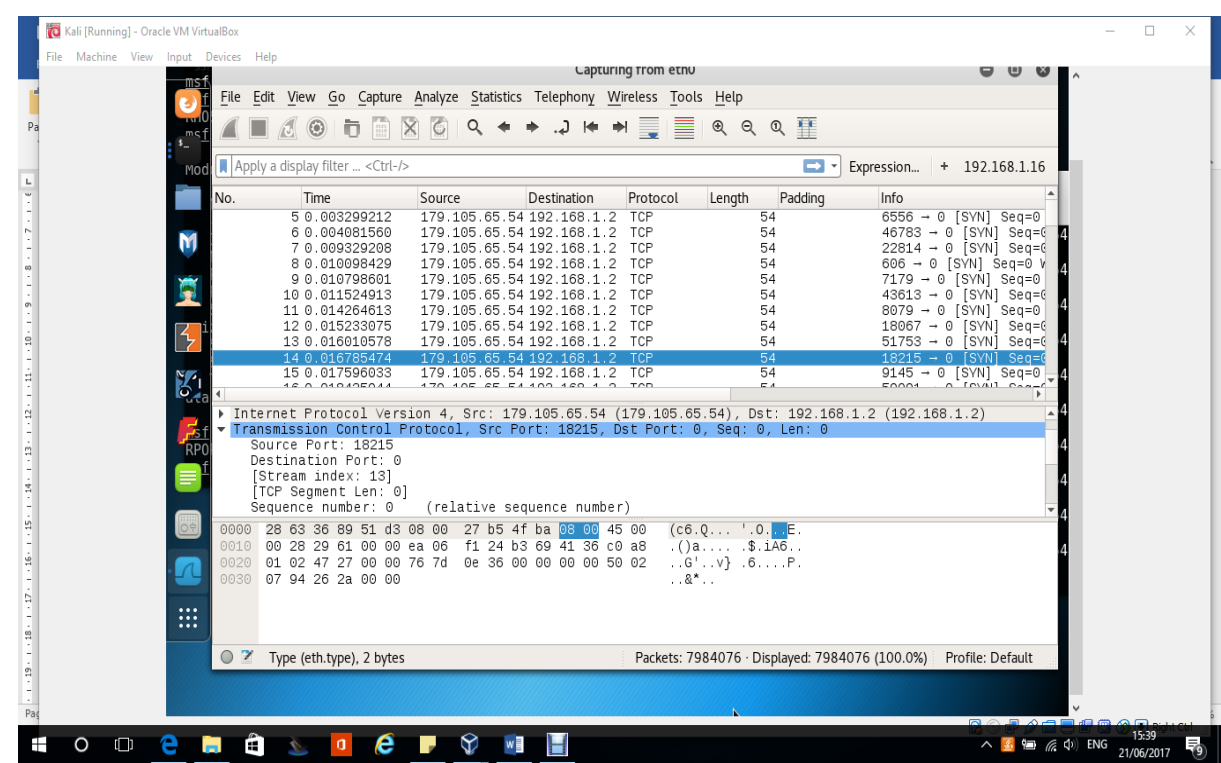


Figure B-17: PLC Denial-of-Service Attack Scenario: Packet Flood Analysis – 2 (Wireshark)

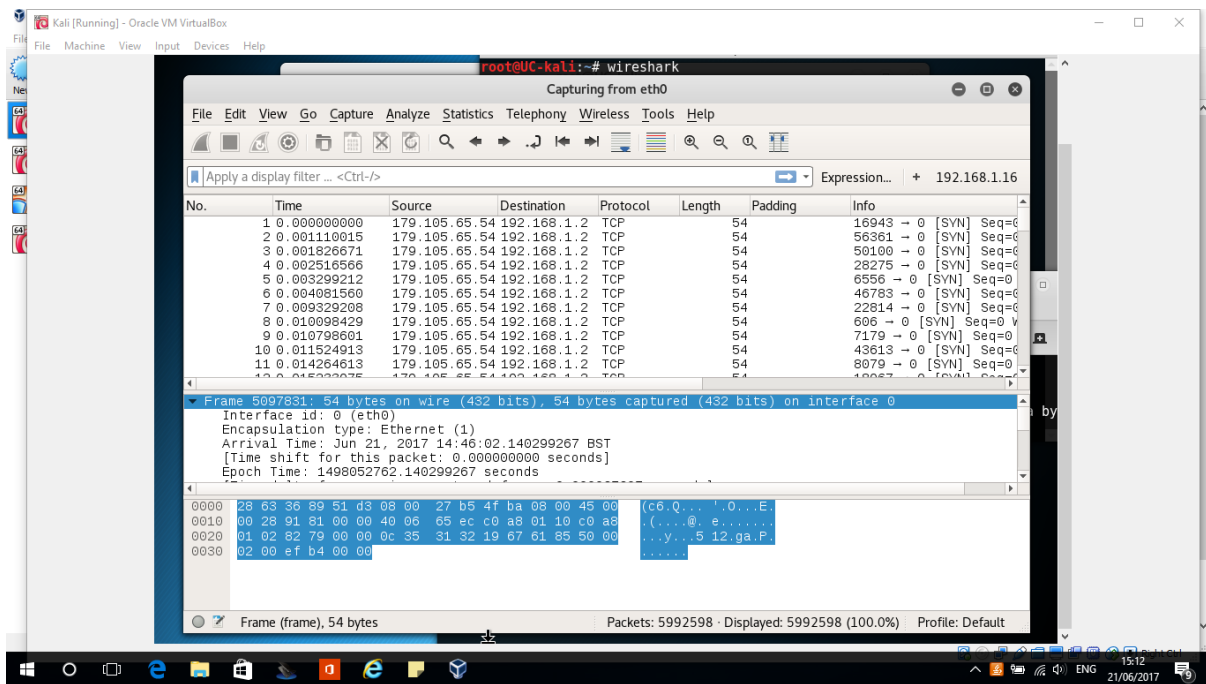


Figure B-18: PLC Denial-of-Service Attack Scenario: SMOD Utility Attack (1)

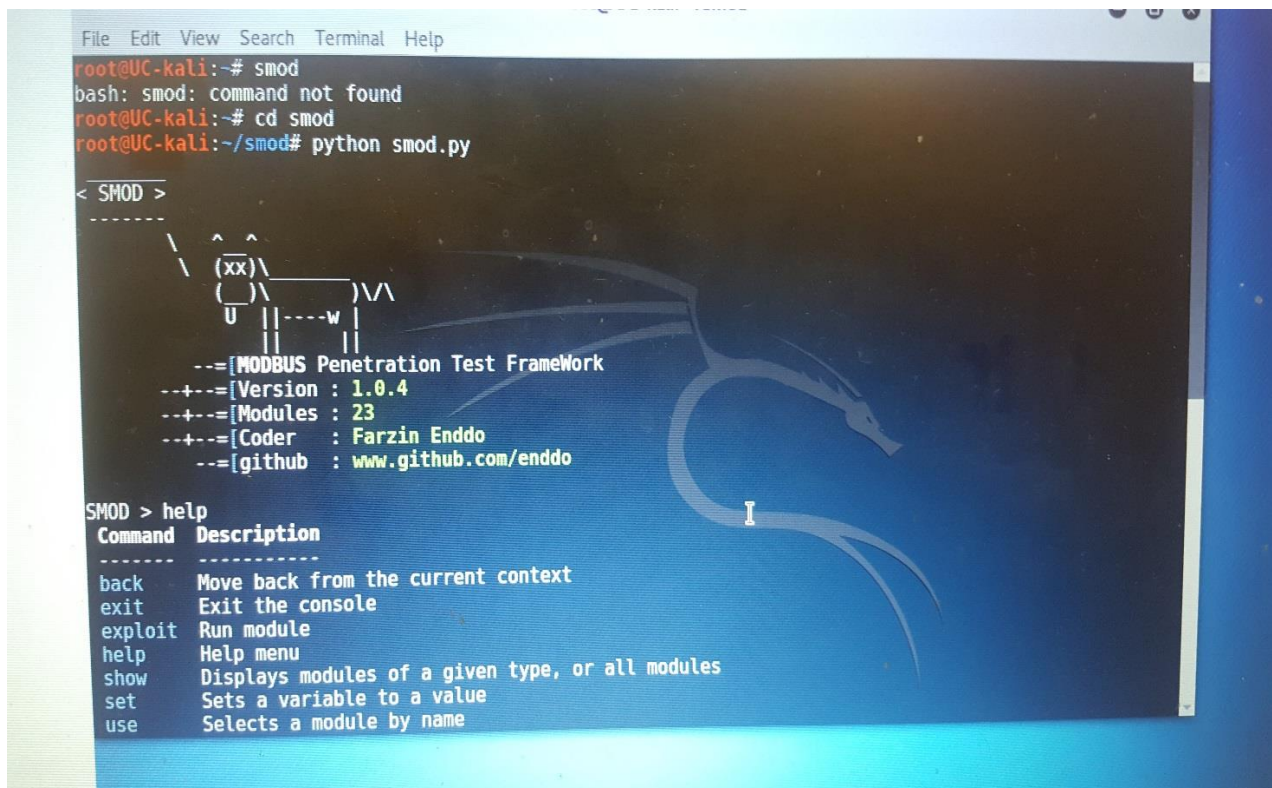


Figure B-19: PLC Denial-of-Service Attack Scenario: SMOD Utility Attack (2)

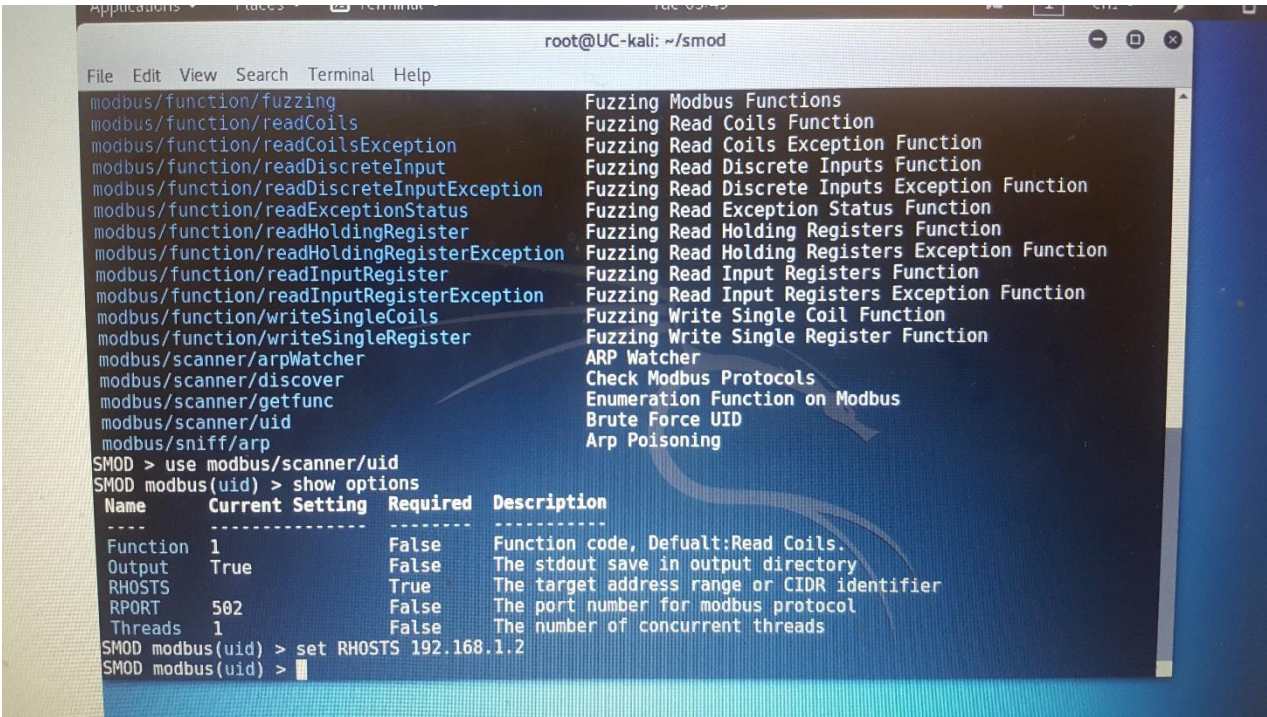


Figure B-20 : PLC Denial-of-Service Attack Scenario: SMOD Attack Impact (1)

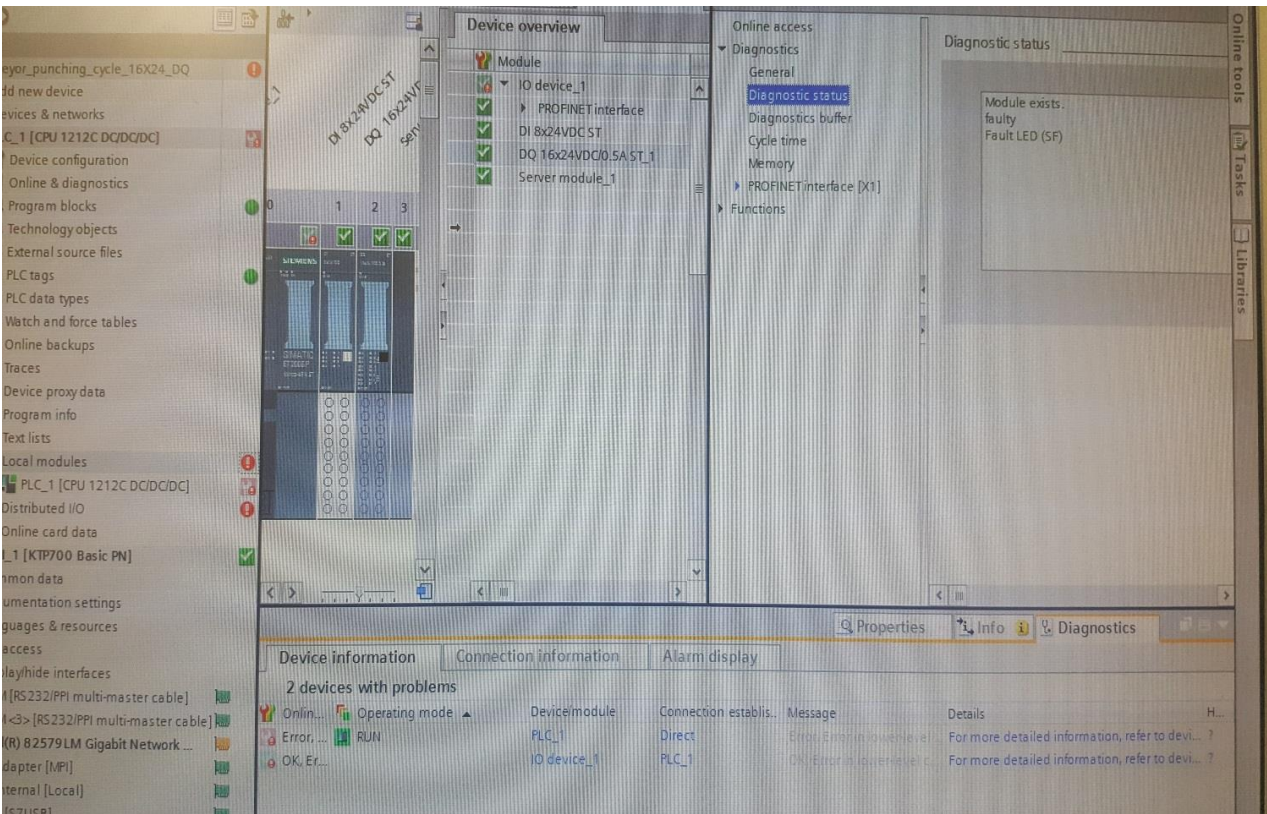


Figure B-21 : PLC Denial-of-Service Attack Scenario: SMOD Attack Impact
(2)

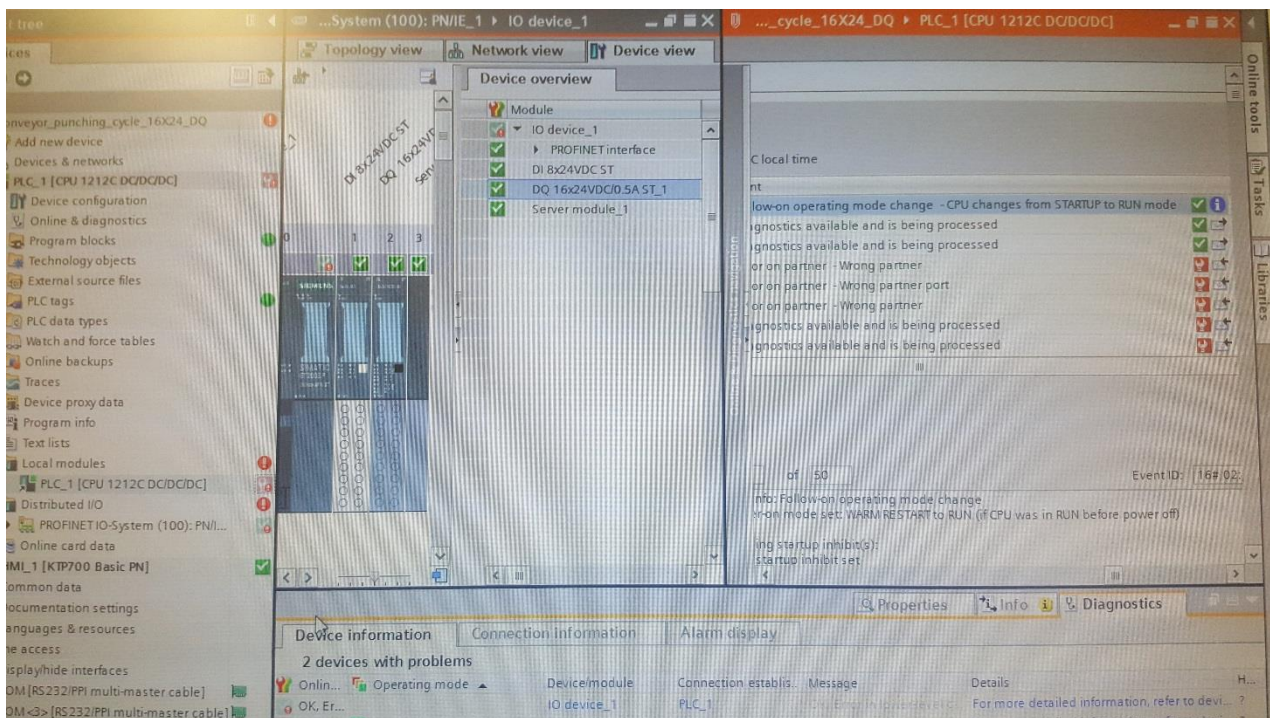


Figure B-22 : PLC Denial-of-Service Attack Scenario: SMOD Attack Impact
(3)

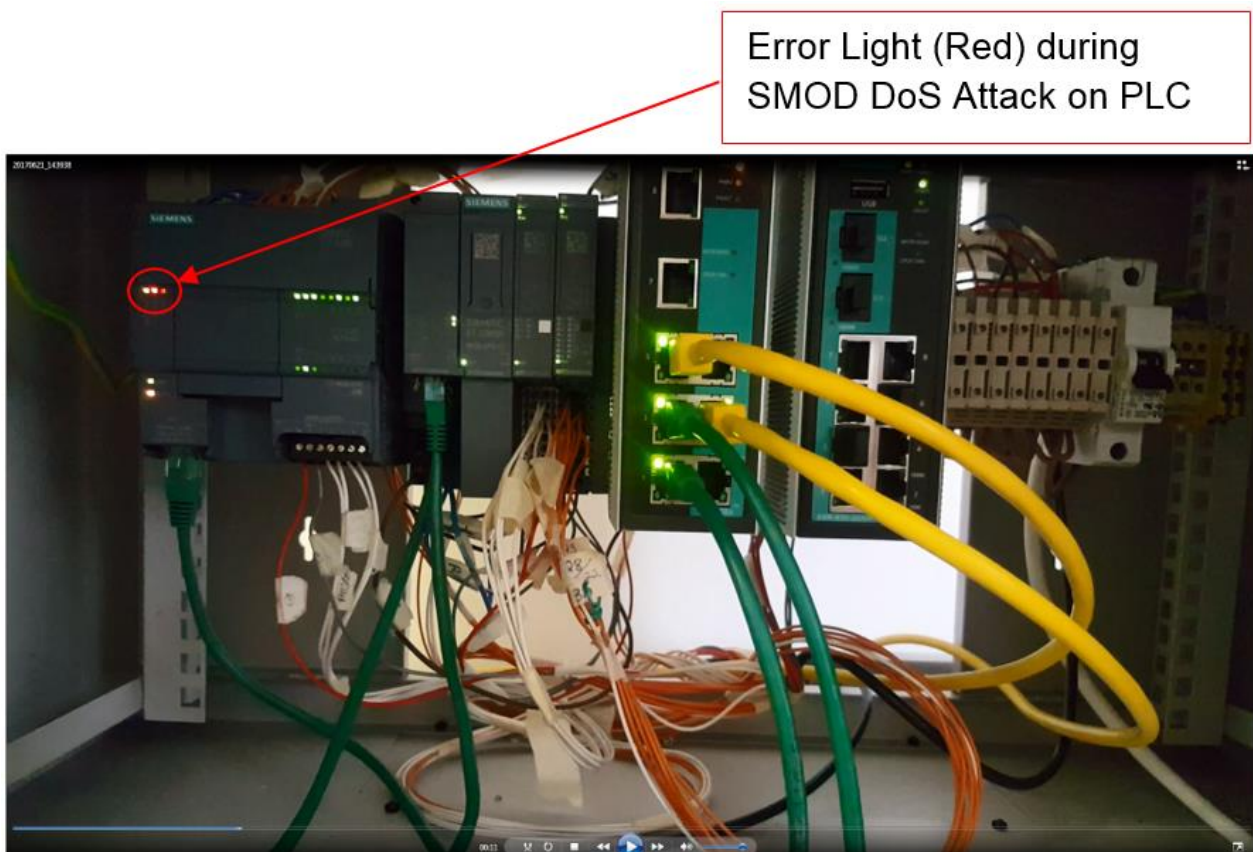


Figure B-23: Nexpose Vulnerability Scanner Start-up from Metasploit Framework in Kali Linux

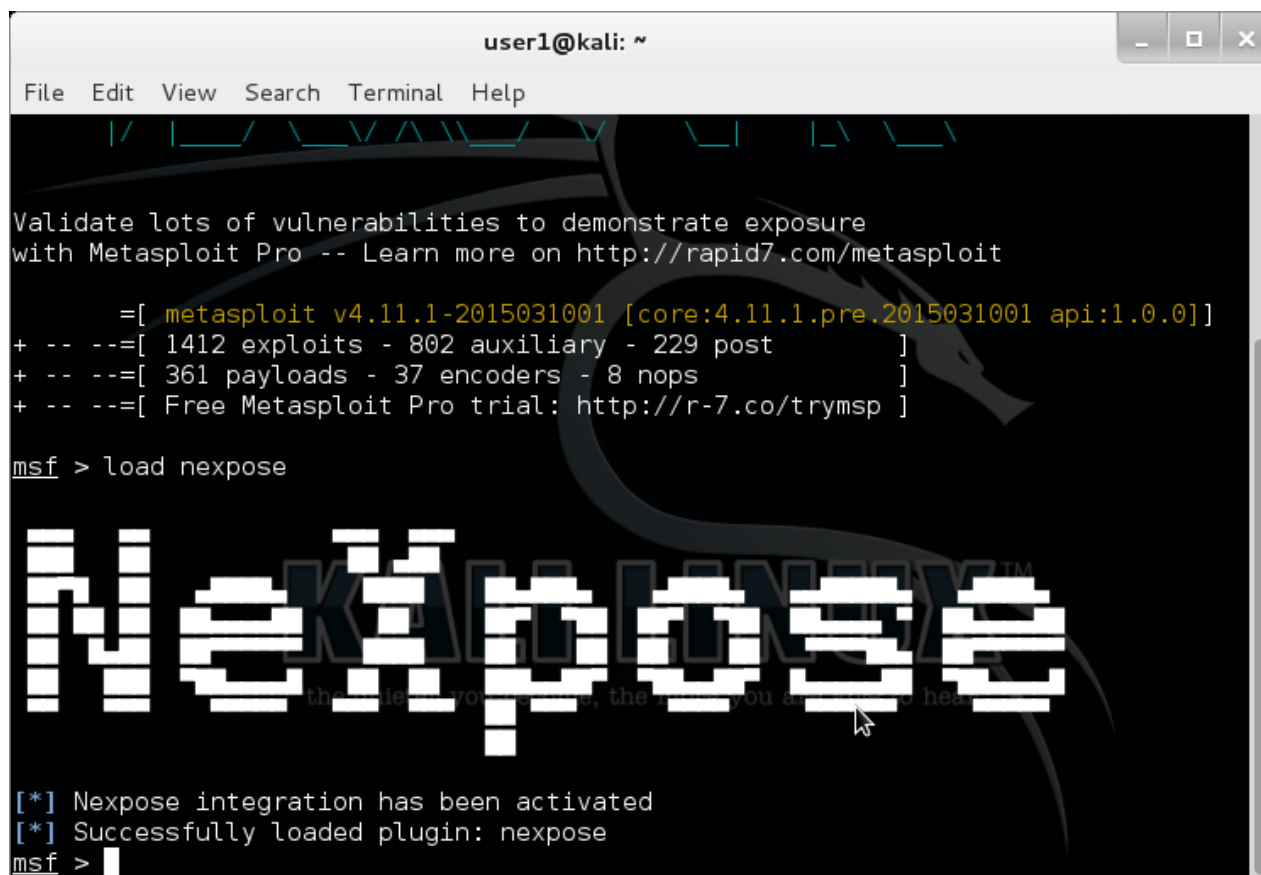


Figure B-24: Nexpose Vulnerability Scanner – Host IP Scanning Parameter Setup

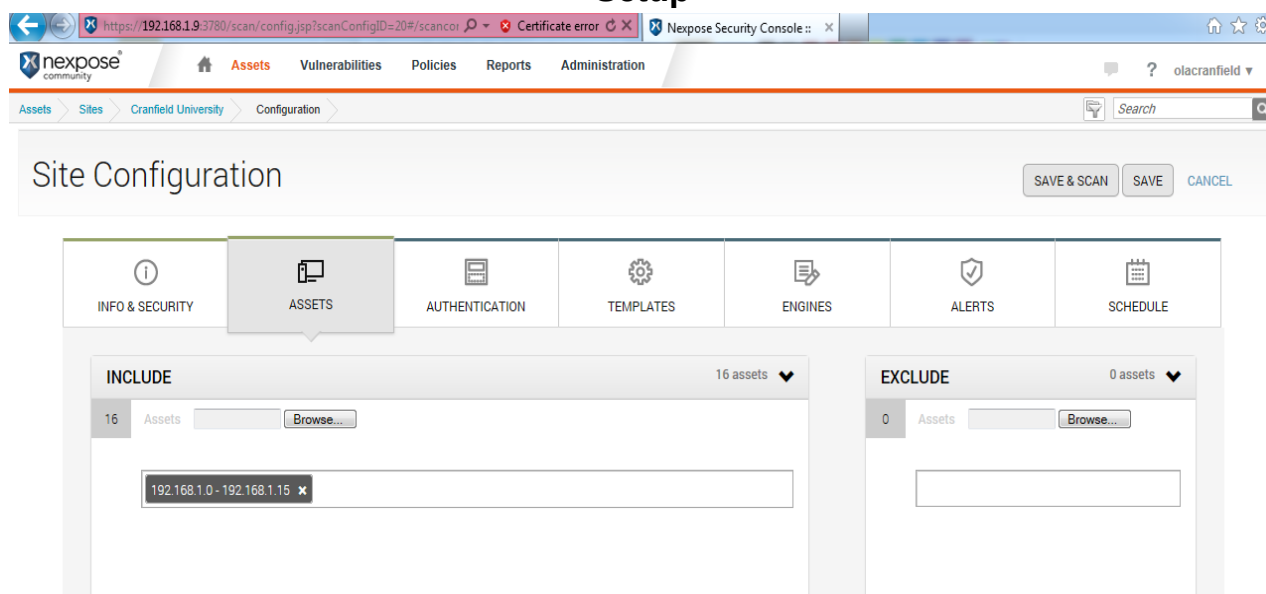


Figure B-25: Nexpose Vulnerability Scanner – Vulnerability Scan Results

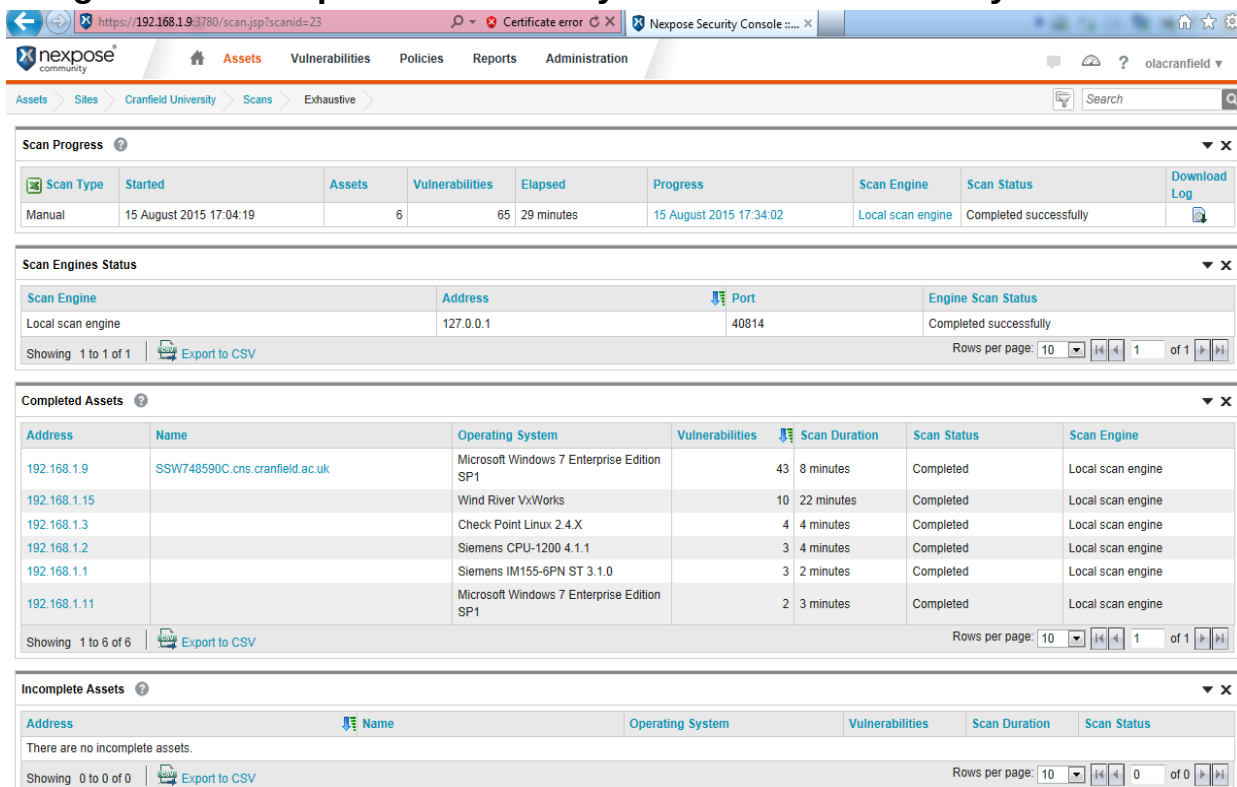


Figure B-26: Nexpose Vulnerability Scanner –Vulnerability Description Results

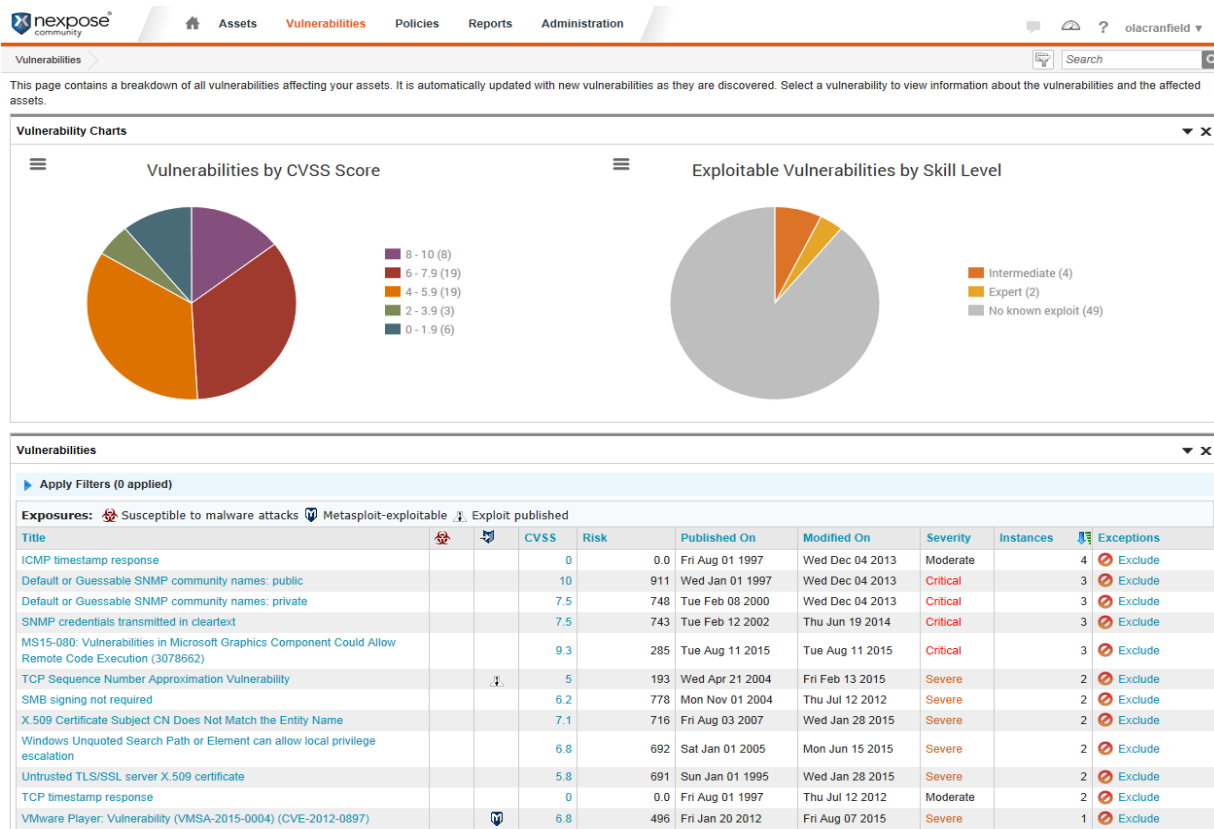


Figure B-27: Complete (37-Member) Workforce Capability Chart

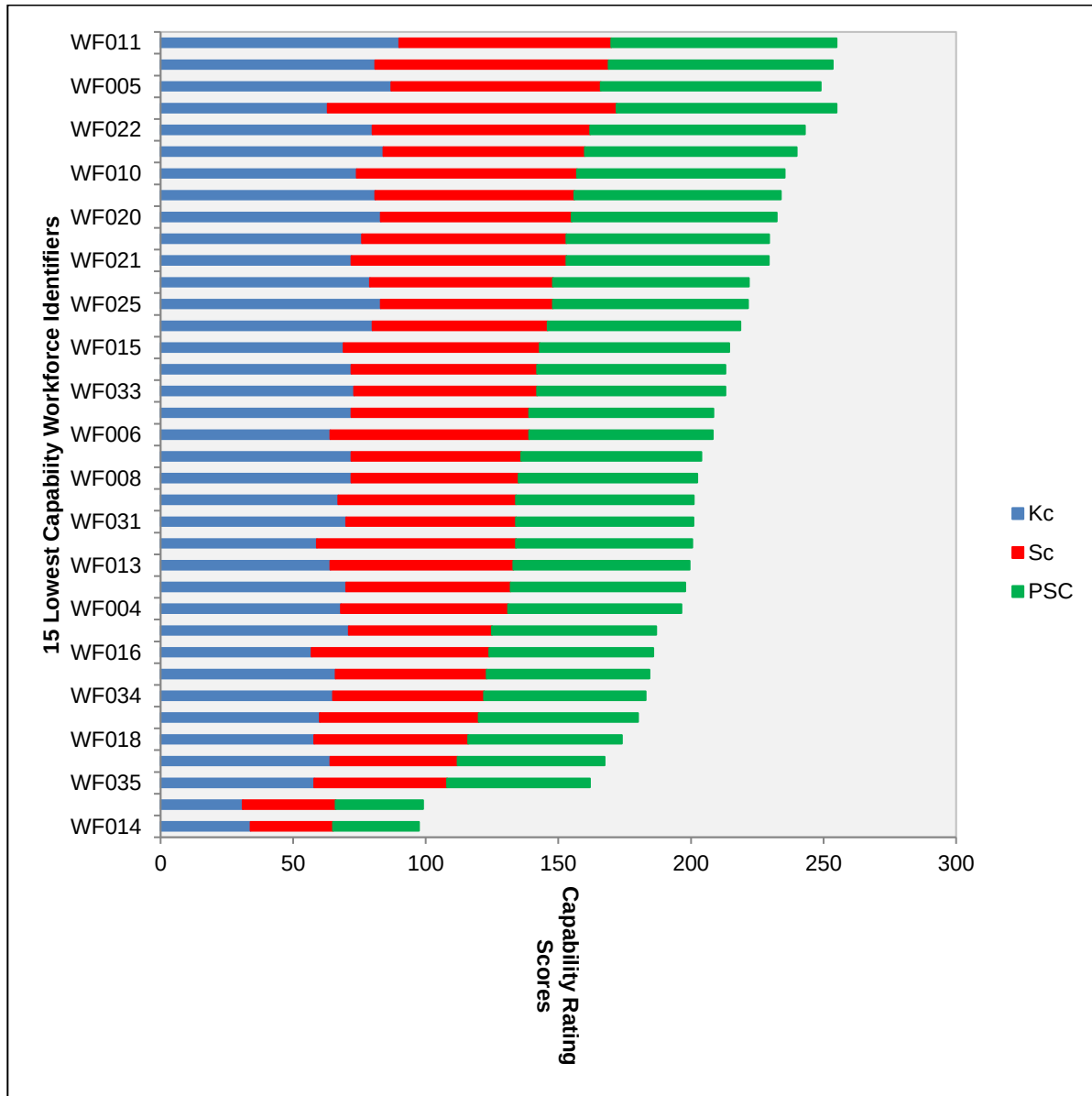


Figure B-28: Complete Chart Representation of Cumulative Capability Ratings (CCR)

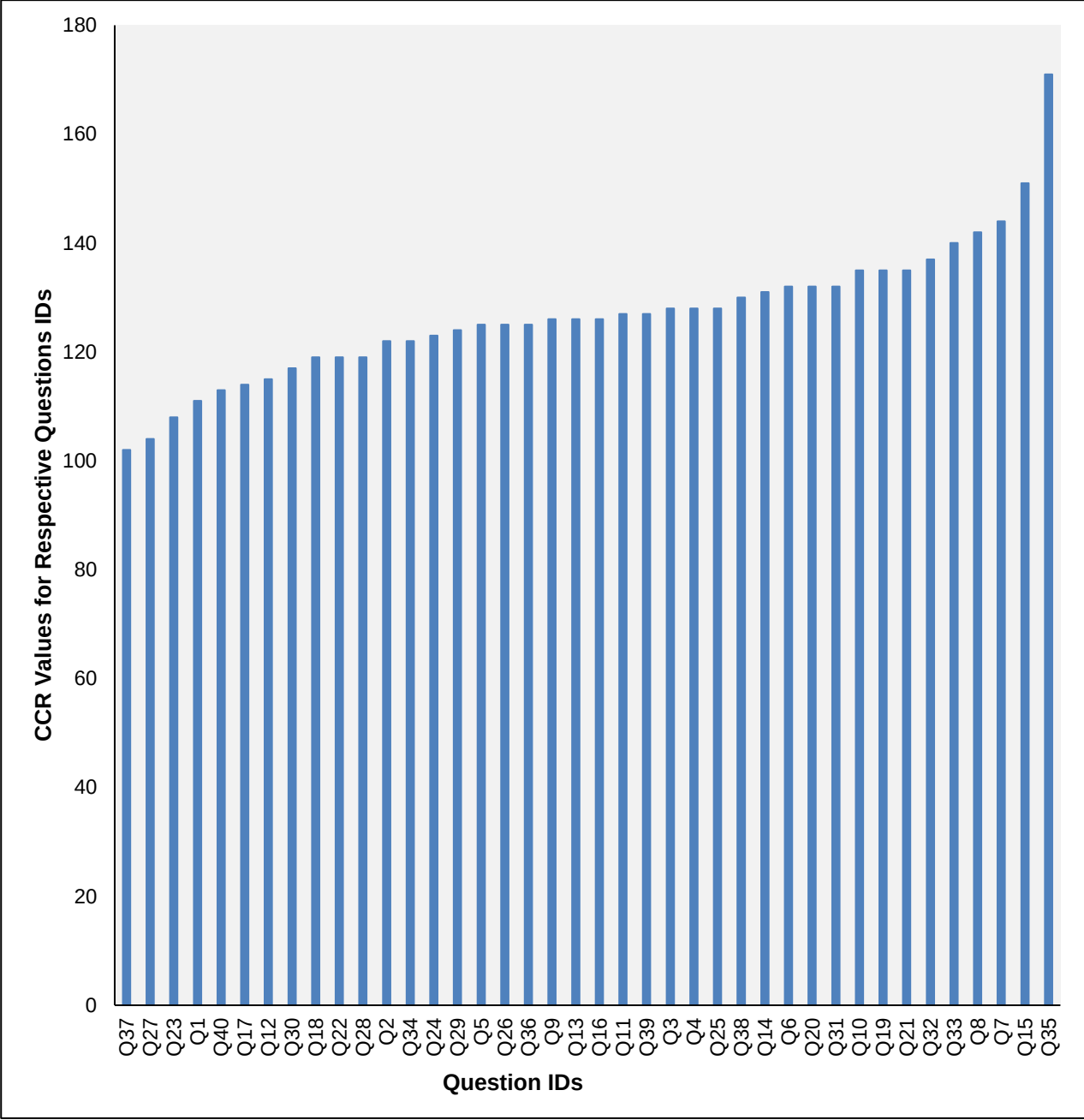


Figure B-29: Testbed Control Network Components integration

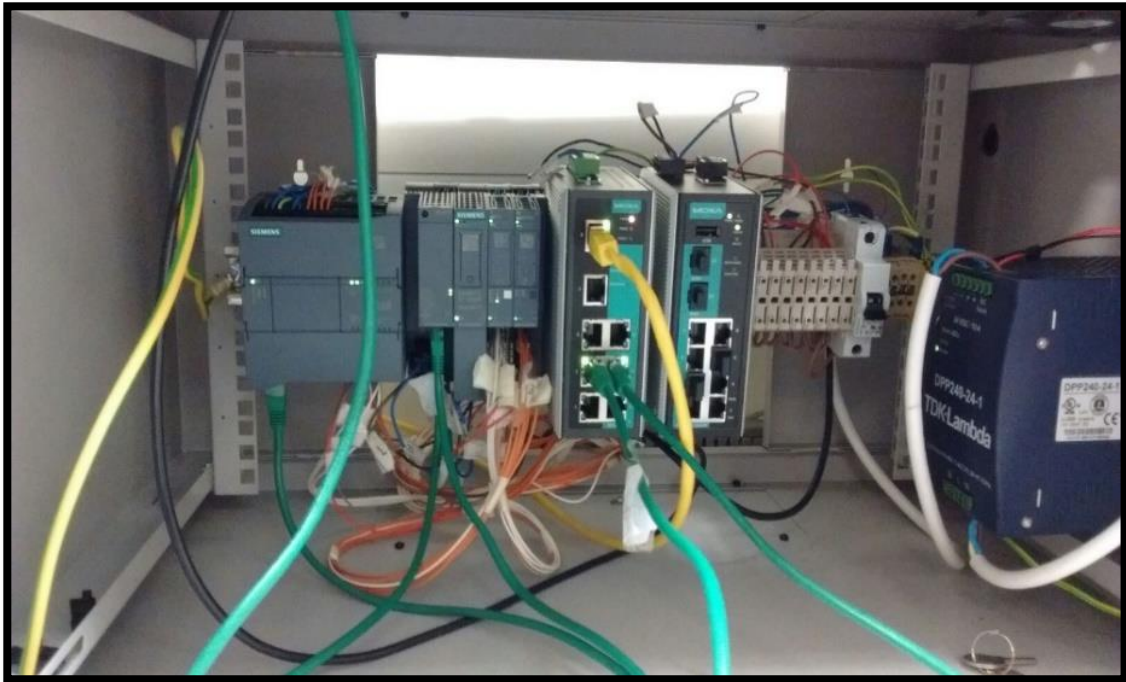


Figure B-30: Complete ICS-CS Testbed Implementation

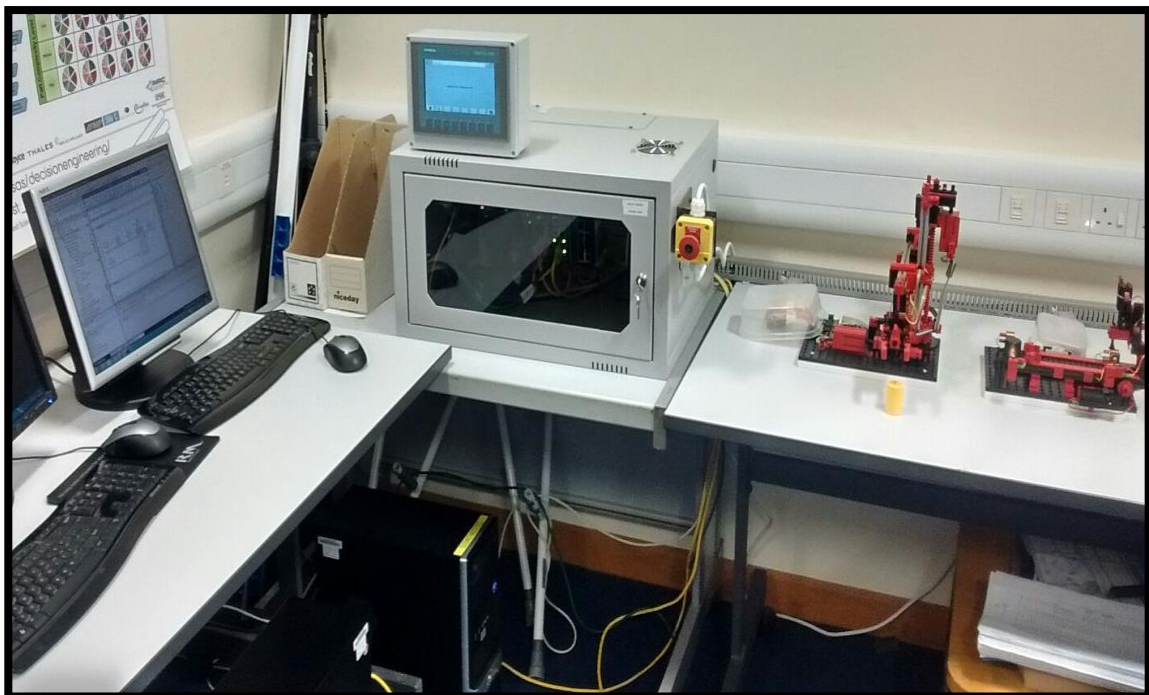


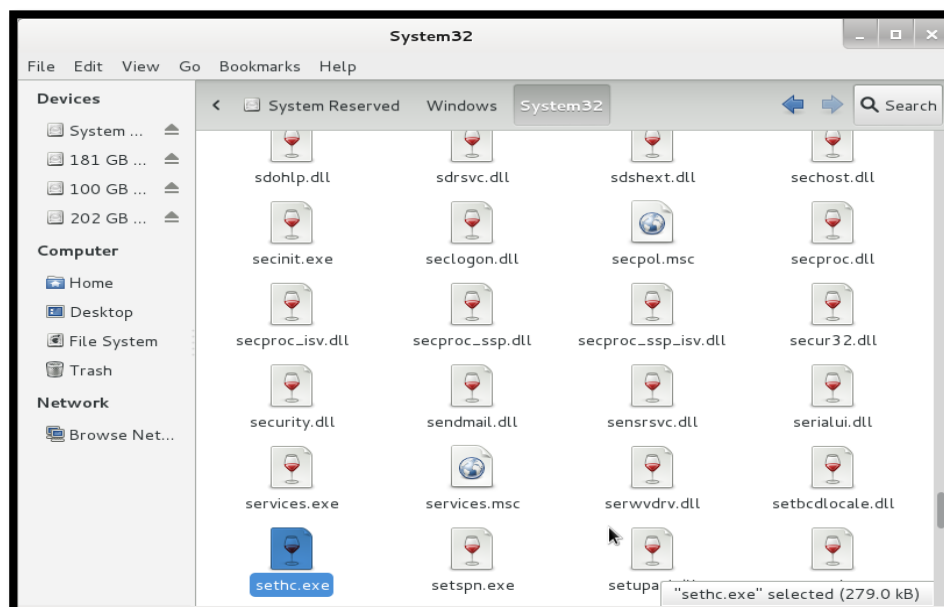
Figure B-31: Privilege Escalation Attack Procedures and Screenshots

System Access and modifications:

- Booting into the Kali Live USB (See [Error! Reference source not found.](#))
- Locating a file 'sethc.exe' from 'System32' sub-folder in the Windows folder resident in the 'Windows' partition. The file 'sethc.exe' is an executable file/process related to Windows NT High Contrast Invocation. The file is included in Microsoft Windows Operating System. With default Windows settings, this file is called-up and executed when the shift key on the keyboard is pressed 5 times in succession to invoke the Sticky Keys configuration window (See [Error! Reference source not found.](#)).
- The file 'sethc.exe' file is renamed to 'sethc.bak'. This is to keep a backup copy of the file for future system recovery. In real attack scenario that involves a malicious insider attacker, such threat agents may well delete the file completely.
- From the same 'System32' sub-folder, the file 'cmd.exe' is located and duplicated. 'CMD.exe' file/process is the Microsoft Windows file responsible for loading user profiles on logon.
- The duplicate 'CMD(copy).exe' is renamed to 'sethc.exe'. This procedure causes the Windows platform to launch a 'sethc.exe' file name with 'cmd.exe' executable instructions, which prompts and accessibility option to the computer.
- Kali Live OS environment is restarted to enable booting into Windows platform.



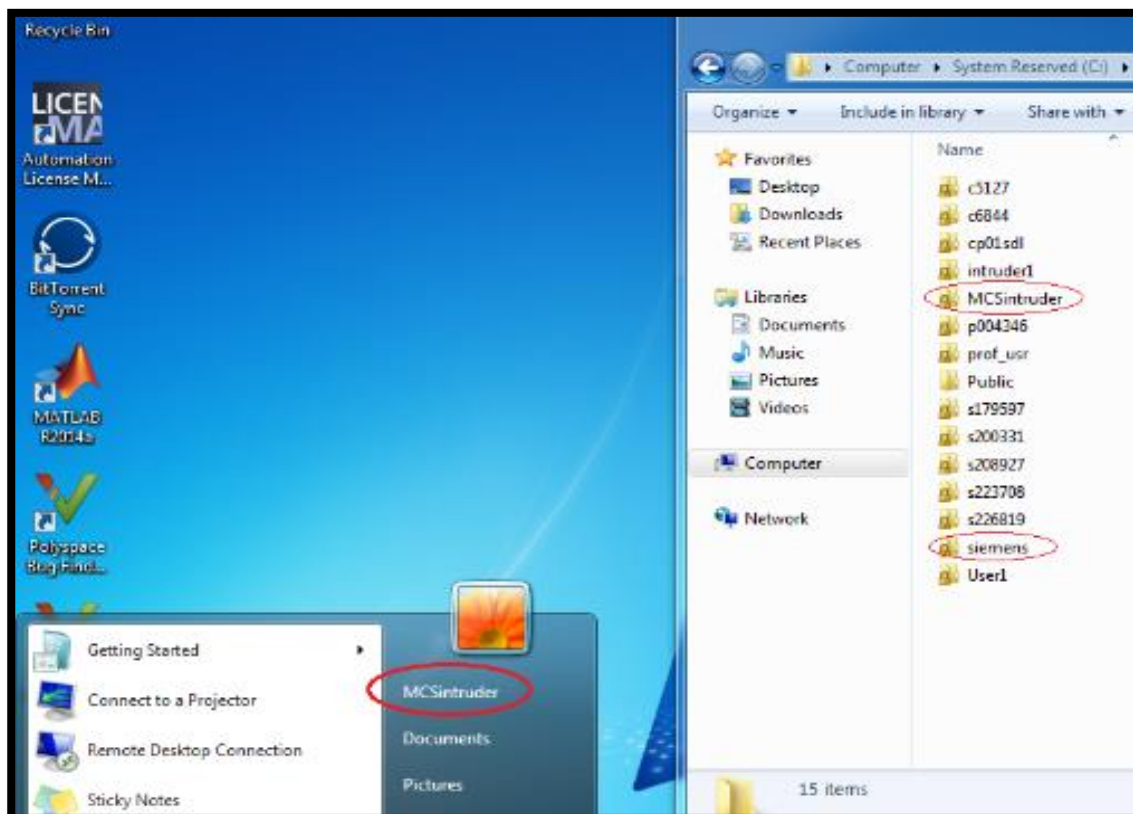
A. Privilege escalation - Kali Linux Live



B. Privilege escalation - Kali Linux sethc.exe

New User Creation and Escalation of Privilege:

- i. On windows platform, the 'Shift' key on the keyboard is pressed 5 times successively to call-up the command prompt.
- ii. At the command prompt, a new user and password is created using the desired details. The command "*net user /add MCSintruder Password1*" creates a new user named "MCSintruder" with a password "Password1"
- iii. A second command is used to add the newly created user to the 'Administrators' group of exploited system. The command used was "*net localgroup administrators MCSintruder /add*"
- iv. Normal system login was now attempted using the new credentials - username: *MCSintruder*, password: *Password1*. Access to the system was successful with capabilities to manipulate files and programs - (See **Error! Reference source not found.**). Appendices B-13 and B-14 present other exploit access login screens of the attack.



C. System Access with file and program modification capabilities

Appendix C: Questionnaires and Ethics Approvals

Figure C-1: Framework Validation Questionnaire (Tool)

Introduction:

As part of research being undertaken in SATM, PhD student, we are appealing for assistance in completing and/or sharing this research survey with individuals (industrial and academic research experts) working or previously worked in security metrics and assessment, especially in the industrial environment. Our research is looking at enhancing cyber security assurance in the ICS domain, part of which includes the adoption of an effective all-encompassing metrics development framework that can guide the generation of appropriate security metric taxonomies for the evaluation of security posture in an ICS environment. The survey target experts with understanding/experience in metrics generation, evaluations, and applications in cyber security, information security, network security metrics (development frameworks, and quantities). It is focused on determining desirable properties of potential security metrics development frameworks, the validity of a proposed framework and metric taxonomy; in response to the dynamic nature of cybersecurity threats and vulnerabilities in the ICS environment.

If you know of anyone working in these areas who might be able to spare some time to complete the survey, please send them a link to the survey:
https://cranfielduniversity.eu.qualtrics.com/jfe/form/SV_cCq8Ot86uWykZk9

If you know of anyone working in these areas who might be able to spare some time to complete the survey, please send them a link to the survey:
https://cranfielduniversity.eu.qualtrics.com/jfe/form/SV_cCq8Ot86uWykZk9

This research has been approved by Cranfield University ethics committee, and will not record sensitive personal or commercial data.

If you have any queries, please contact Uchenna P Daniel Ani – u.p.ani@cranfield.ac.uk , or h.he@cranfield.ac.uk

Consent:

If you are unsure whether your role is applicable, feel free to contact the researcher Informed Consent This survey will take few minutes to accomplish. You are free to withdraw your consent and to ask for the destruction of all or part of the data that you have contributed at any time up to 14 days after you have submitted your response. After this time it will not be possible to distinguish your response from the aggregated results. Withdrawing your consent will not be viewed negatively. Unless you otherwise give permission, all data is collected anonymously. The data you supply will be used only for the research purposes of this study and while the results may be published in (for example) scientific journals or conference proceedings, it will not be possible to identify any individual from the published results. The individual survey results will only be seen by the researcher and a select number of supervising staff at Cranfield University. You may save your progress, close your browser, and continue completing the survey later. Partially completed surveys however will not be counted in the final results.

I welcome any further questions or comments at: u.p.ani@cranfield.ac.uk

Do you understand and wish to continue with this survey?

- ☐ Yes (1)
- ☐ No (0)

Condition: No Is Selected. Skip To: End of Survey.

D1 How long (in years) have you worked in the operational security aspect of the industry?

☐ 1 (1) -----

D2 Which of these security capability (knowledge and skill) classifications best describes you?

☐ Security Knowledge (1)

☐ Security Skill (2)

☐ Both Security Knowledge and Skill (3)

D3 Using a rating range of 1 – 5; 1 being least, and 5 being highest, how do you rate your knowledge, skills, experience, or expertise in security metrics development, security metrics-driven assessment, and general information/cyber-security?

☐ 1 (1)

☐ 2 (2)

☐ 3 (3)

☐ 4 (4)

☐ 5 (5)

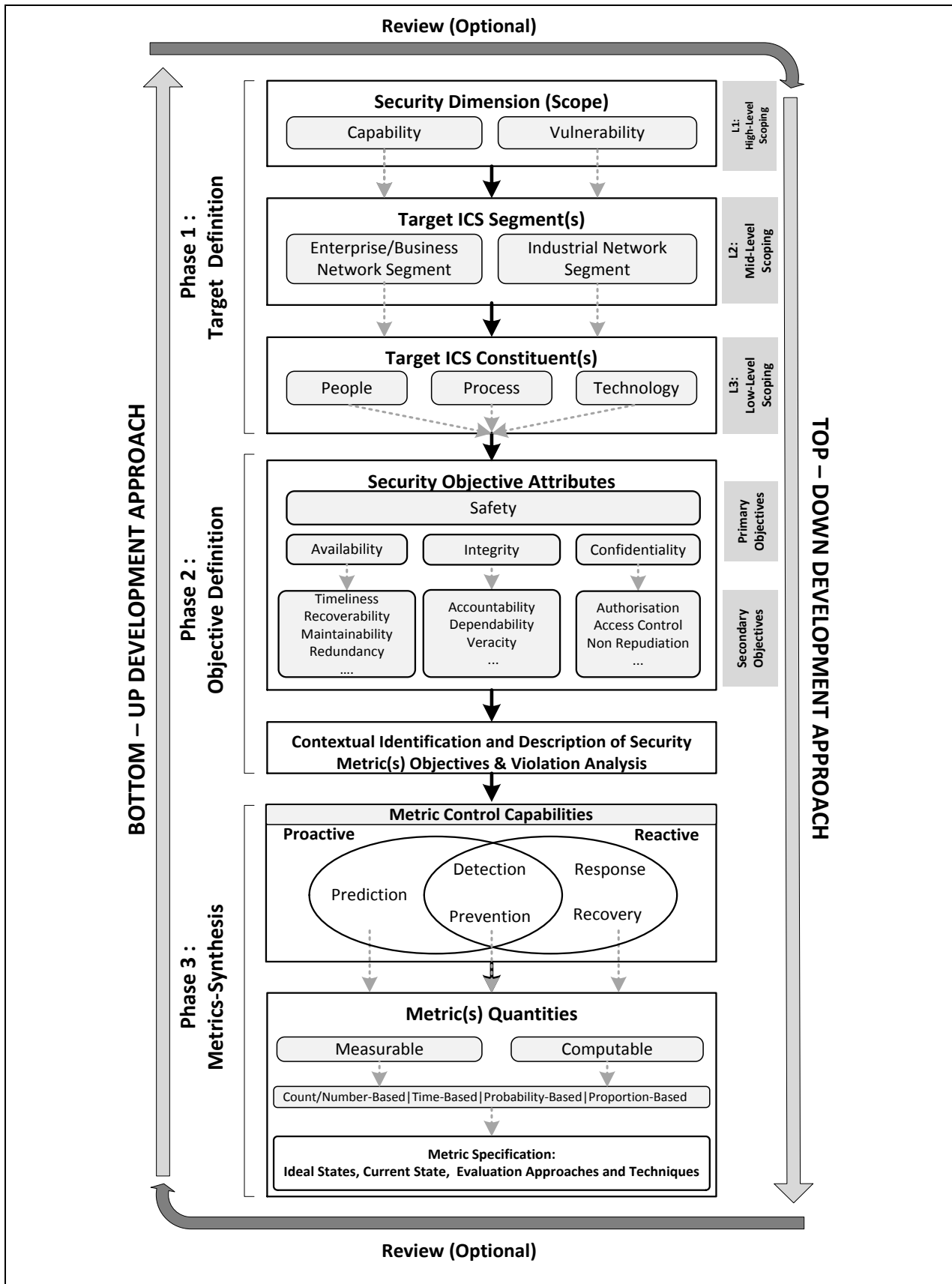
The Operational Security Metrics Generation (OSMG) Framework for Industrial Environments

Operational security metrics are measures or attributes that tell or used to determine the state or degree of security relative to specific operational reference points or objectives and informs of what is required for improvement. Operational Security metrics are very crucial towards guiding the direction in the measurement of security states and susceptibilities. However, practical security metrics lies in effective development approaches. The characteristics of an effective framework for security metrics development should include: feasibility, repeatability, adaptability, goal-definitive, scope-definitive (FRAGS). A framework for Operational Security Metrics Generation (OSMG) for industry control environments is presented, unifying existing approaches, inheriting their characteristics, and adding the characteristics of adaptability.

The figure below presents the OSMG Framework that incorporates valuable requirements and features in an inclusive, concise, step-wise method. The framework focuses on guiding security metrics development in the industrial control system environment following three broad phases as described below:

- i. Target System definition (scope definitions for security dimension, system, and constituent segment).
- ii. Target (Security) Objective definition (primary, secondary, and tertiary security objective definitions).

Metrics-synthesis (control dimensions, metric quantities, and profile definitions). The framework will help create effective and efficient security metrics taxonomies that can be used to enhance security assurance within industrial operational environments



Q1 Section B: Framework Evaluation

A good security metrics development framework should possess/retain the following characteristics:

1. Scope-definitive: Guide the clear outline of targeted system scope.
2. Objective-definitive: Guide the clear delineation of targeted security objectives.
3. Simple: Easy and straightforward to employ or use.
4. Adaptive: Enable the adoption of reviews in response to dynamic changes in scope and objectives.
5. Iterative: Enable repetitions of processes or procedures where necessary.
6. Reliable: Trusted to yield a consistent desirable outcome (metrics)

	Very High (1)	High (2)	Moderate (3)	Low (4)	Very Low (5)
Scope-definitive (1)	☐	☐	☐	☐	☐
Objective-definitive (2)	☐	☐	☐	☐	☐
Simple (3)	☐	☐	☐	☐	☐
Adaptive (4)	☐	☐	☐	☐	☐
Iterative (5)	☐	☐	☐	☐	☐
Reliable (6)	☐	☐	☐	☐	☐

Q2 The proposed OSMG framework for ICS Environment is considered complete in providing adequate means for process and objective scoping.

- ☐ Strongly Agree (5)
- ☐ Agree (4)
- ☐ Disagree (3)
- ☐ Strongly Disagree (2)
- ☐ No Opinion / Don't Know (1)

Q3 How consistent is the level of details given in the proposed OSMG framework?

- ☐ Strongly Consistent (5)
- ☐ Consistent (4)
- ☐ Inconsistent (3)
- ☐ Strongly Inconsistent (2)
- ☐ No Opinion / Don't Know (1)

Q4 How easy do you think it is to understand the path from initial 'security dimension' to final process of 'metrics specification' in the proposed OSMG framework?

- ☐ Strongly Easy (5)
- ☐ Easy (4)
- ☐ Uneasy (3)
- ☐ Strongly Uneasy (2)
- ☐ No Opinion / Don't Know (1)

Q5 How much previous knowledge of security metrics development do you think you need to be able to interpret this framework?

- ☐ Very Much (5)
- ☐ Much (4)
- ☐ Little (3)
- ☐ Very Little (2)
- ☐ No Opinion / Don't Know (1)

Q6 How easy would it be to adapt (add/remove/mend) security target(s), objective(s), and(or) metrics from the proposed OSMG framework?

- ☐ Strongly Easy (5)
- ☐ Easy (4)
- ☐ Uneasy (3)
- ☐ Strongly Uneasy (2)
- ☐ No Opinion / Don't Know (1)

Q7 The level of detail provided by this OSMG Framework can yield metrics that will enable a fair assessment of the security strengths and weaknesses of an ICS domain

- ☐ Strongly Agree (5)
- ☐ Agree (4)
- ☐ Disagree (3)
- ☐ Strongly Disagree (2)
- ☐ No Opinion / Don't Know (1)

Q8 How appropriate is it to include/consider people, process, and technology security attributes/dimensions to gain an overall, system/organisation-wide perspective of security postures and vulnerabilities?

- ☐ Strongly Appropriate (5)
- ☐ Appropriate (4)
- ☐ Inappropriate (3)
- ☐ Strongly Inappropriate (2)
- ☐ No Opinion / Don't Know (1)

Q9 Each Phase and attribute-decomposition in the OSMG framework relates to a relevant security requirement, standard or best practice guide.

- ☐ Strongly Agree (5)
- ☐ Agree (4)
- ☐ Disagree (3)
- ☐ Strongly Disagree (2)
- ☐ No Opinion / Don't Know (1)

Q10 Each Phase and sub-phase of the OSMG framework is easy to understand (i.e., clearly defined and unambiguous).

- ☐ Strongly Agree (5)
- ☐ Agree (4)
- ☐ Disagree (3)
- ☐ Strongly Disagree (2)
- ☐ No Opinion / Don't Know (1)

Q11 How realistic is it for industrial organisations to use this OSMG framework to view their security requirements, generate and use security metrics to understand organisational security capabilities (postures or vulnerabilities)?

- ☐ Strongly Realistic (5)
- ☐ Realistic (4)
- ☐ unrealistic (3)
- ☐ Strongly Unrealistic (2)
- ☐ No Opinion / Don't Know (1)

Q12 How easy would it be to adapt (add/remove/amend) this proposed OSMG framework to meet individual and varied industrial operational environments?

- ☐ Strongly Easy (5)
- ☐ Easy (4)
- ☐ Uneasy (3)
- ☐ Strongly Uneasy (2)
- ☐ No Opinion / Don't Know (1)

Q13 How useful would this framework be to the industrial community in the pursuit of operational security assurance?

- ☐ Strongly Useful (5)
- ☐ Useful (4)
- ☐ Not Useful (3)
- ☐ Strongly Not Useful (2)
- ☐ No Opinion / Don't Know (1)

Q14 How useful would this framework be to the academic and research community to guide further developments towards effective operational security assurance?

- ☐ Strongly Useful (5)
- ☐ Useful (4)
- ☐ Not Useful (3)
- ☐ Strongly Not Useful (2)
- ☐ No Opinion / Don't Know (1)

Q15 to what extent do you think the proposed OSMG framework is applicable for yielding desirable security metrics relative to industrial operations scenarios?

- ☐ Strongly Applicability (5)
- ☐ Applicable (4)
- ☐ Not Applicable (3)
- ☐ Strongly Not Applicable (2)
- ☐ No Opinion / Don't Know (1)

Figure C-2: Ethics Approval for Framework Validation Questionnaire (Tool)

12/1/2017

CURES Submission: Approved - Ani, Uchenna p.

CURES Submission: Approved

donotreply@infonetica.net

Thu 11/05/2017 14:01

To: Ani, Uchenna p. <u.p.ani@cranfield.ac.uk>;

Cc: He, Hongmei <h.he@cranfield.ac.uk>;

Dear Uchenna p.

Reference: CURES/2682/2017

Title: A Framework for Operational Security Metrics Development for Industrial Control Environments

Thank you for your application to the Cranfield University Research Ethics System (CURES).

Your proposed research activity has been confirmed as Level 2b risk in terms of research ethics. You may now proceed with the research activities you have sought approval for.

Please remember that CURES occasionally conducts audits of projects. We may therefore contact you during or following execution of your fieldwork. Guidance on good practice is available on the [research ethics intranet pages](#).

If you have any queries, please contact cures-support@cranfield.ac.uk

We wish you every success with your project.

Regards

CURES Team

May we remind you of the importance of addressing health and safety issues in your research. Templates and further guidance are available [here](#).

Figure C-3: Ethics Approval for Workforce Cyber Security Capability Test-based Questionnaire

12/1/2017

CURES Submission: Approved - Ani, Uchenna p.

CURES Submission: Approved

donotreply@infonetica.net

Thu 14/07/2016 11:08

To: Ani, Uchenna p. <u.p.ani@cranfield.ac.uk>;

Cc: He, Hongmei <h.he@cranfield.ac.uk>;

Dear Uchenna p.

Reference: CURES/1811/2016

Title: Industrial Control System Cyber Security Assurance through Workforce capability evaluation approach and Validation

Your proposed research activity has been reviewed by CURES and you can now proceed with the research activities you have sought approval for.

Please remember that CURES occasionally conducts audits of projects. We may therefore contact you during or following execution of your fieldwork. Guidance on good practice is available on the [research ethics intranet pages](#).

If you have any queries, please contact cures-support@cranfield.ac.uk

We wish you every success with your project.

Regards

CURES Team

May we remind you of the importance of addressing health and safety issues in your research. Templates and further guidance are available [here](#).

Figure C-4: Cyber Security Capability Questionnaire

With focus on standard security models, best practices, ISO, NIST, PCI-DSS, UK-Cyber Security Essentials, NIST Special Publication 800-82 "Guide to ICS Security", and the Framework for Improving Critical Infrastructure Cyber Security.

Assessment of organizations cyber security susceptibility, via its employee's conformance to the NIST's Infrastructural Cyber security framework core activities (identification, protection, detection, response and recovery). Current cyber security trends show that a major challenge to effective cyber protection is not with the technologies or their applications, but rather with the human (employee) workforce. Traditionally, the academia and industry have focused more on mitigating cyber insecurities associated with technical capabilities and solutions, not much has been considered towards improving the fragile cyber security posture of the organizational workforce, and lowering their susceptibility to prevailing cyber-attack techniques. A critical initiative and measure towards achieving this is the building of capacities through awareness and diagnostic abilities, which usually should be guided by organizational policies and standards for safe process operations, handling sensitive data/equipment, internet-use best practices, breach/compromise identification, response, reporting, and effective recovery amongst others. This will potential help guard individuals and the organization from compromise.

However, parallel to the significance of assessing and tracking the fortes of technological system defences, it is similarly essential to gauge the latent efficiency of awareness and diagnostic abilities of the organizational workforce. This we prefer to suitably term as their *Susceptibility* to cyber-attacks, which invariably offers a general view of the organization's cyber-attacks susceptibility. Assessing organization's cyber-attack susceptibility posture from the perspectives of workforce awareness and diagnostic capacities. The outcomes of such assessment could help identify and prioritize the workforce and susceptibility scope for improvement within the context of unremitting and repeatable process, which will further give light on the progress towards a targeted attack susceptibility state. Additionally, the knowledge inferred from such susceptibility assessment could spur improvements in the right directions and reduce the overheads in resources needed to boost the cyber security capacities of the industrial workforce

A. Cyber Security Knowledge (Awareness) Questions

1. How well secure do you feel about your industrial equipment, networks, operations and(or) critical infrastructure against cyber vulnerabilities, threats and attacks?

A. Very well secure	[2]
B. Fairly well secure	[3]
C. Not very well secure	[4]
D. Not at all secure	[5]
E. Don't Know	[1]

2. The frequency of monitoring and tuning of the capacity or usage statistics of your Industrial Control Systems and IT critical infrastructure?

A. Regularly	[5]
B. Irregularly	[2]
C. As I deem necessary	[3]
D. As prescribed by Company/Organization	[4]
E. Not Necessary (since basic functionalities are stable)	[1]

3. Clear understanding of your duties and responsibilities in the protection of industrial computing assets and critical infrastructures as contained in the following: (i) CPNI Good Practice Guide, (ii) ISO/IEC 27002, (iii) IEC 62443 (ISA-99), (iv) NIST SP 800-82, and (v) COBIT 5

A. Totally agree	[5]
B. Tend to agree	[4]
C. Tend to disagree	[3]
D. Totally disagree	[2]
E. Don't Know	[1]

4. Clearly understand and able to recognise better and easily all potential forms of social engineering attacks (Physical Access, ID/Email Spoofing, Phishing, Spear Phishing, etc.)?

1. Totally agree	[5]
2. Tend to agree	[4]
3. Tend to disagree	[3]
4. Totally disagree	[2]
5. Don't Know	[1]

6. Cyber-security goes beyond just ensuring that physical equipment and computing devices are not directly compromised, it extends to ensuring I am not compromised either.

A. Totally agree	[5]
B. Tend to agree	[4]
C. Tend to disagree	[3]
D. Totally disagree	[2]
E. Don't Know	[1]

7. On the knowledge and availability of adequate recorded and evolving cyber threats, attack intelligence, potential consequences and safeguard solutions provided by employer

A. Yes there is, and I know and understand clearly	[5]
B. Yes there is, I know and understand only a part	[4]
C. Yes there is, I do not know and understand clearly	[3]
D. No Not sure there is	[1]
E. No there is none	[2]

8. Our operations and services make our industrial network/critical infrastructure is a potential target for cyber-attacks
- A. Totally agree [5]
 - B. Tend to agree [4]
 - C. Tend to disagree [3]
 - D. Totally disagree [2]
 - E. Don't Know [1]
9. Being knowledgeable in the current Cyber Security Essentials and my role expectations in keeping to the guidelines
- A. Totally agree [5]
 - B. Tend to agree [4]
 - C. Tend to disagree [3]
 - D. Totally disagree [2]
 - E. Don't Know [1]
10. Availability and awareness of security policies on what, and how you can and cannot link-up or communicate with entities outside the industrial network
- A. Yes, there are policies limiting external communications via emails and other mediums, how to and not to communicate, whom to and not to communicate to while at work, I agree to ALL [5]
 - B. Yes there are policies on external communication, and I do not understand and agree to SOME [4]
 - C. Yes there are policies on external communication, and I do not agree ANY [3]
 - D. No, there are no policies and I do not think it is necessary in this case, as I should be able to communicate freely to everyone [2]
 - E. No idea [1]
11. Do you agree to using personal (private) owned computing devices (phones, PDAs, laptops, etc) to store, transfer and (or) process industrial/company information?
- A. Totally agree [2]
 - B. Tend to agree [3]
 - C. Tend to disagree [4]
 - D. Totally disagree [5]
 - E. Don't Know [1]
12. For easy access and recollection, it is better to use same user access/authentication credentials (ID and password) for both personal and work (company) accounts
- A. Totally agree [2]
 - B. Tend to agree [3]
 - C. Tend to disagree [4]
 - D. Totally disagree [5]
 - E. Don't Know [1]
13. How well informed on strong password generation or selection techniques and ideas that can be used to strengthen your password, and make it difficult to guess or crack?
- A. Very well informed [5]
 - B. Fairly well informed [4]
 - C. Not very well informed [3]
 - D. Not at all informed [2]
 - E. Don't Know [1]
14. How well informed do you feel about the risk of cyber-attacks and cybercrime on your ICS infrastructure and working environment?
- A. Very well informed [5]
 - B. Fairly well informed [4]
 - C. Not very well informed [3]
 - D. Not at all informed [2]
 - E. Don't Know [1]
15. Please to what extent do you agree or disagree with the following statement?
You believe the risk of your industrial process/operational environment becoming a victim of a cyber-attack has increased in the past year, and you are conscious of the this while undertaking your routine duties in the workplace.
- F. Totally agree [5]
 - G. Tend to agree [4]
 - H. Tend to disagree [3]
 - I. Totally disagree [2]
 - J. Don't Know [1]
16. Please to what extent do you agree or disagree with the following statement?
You are able to recognise and respond appropriately to all forms of cyber-attacks that target you, or your industrial process operations, or infrastructure
- A. Totally agree [2]
 - B. Tend to agree [3]
 - C. Tend to disagree [4]
 - D. Totally disagree [5]
 - E. Don't Know [1]

17. Equipment Vendors, Supplier, Customers, Specialist Contractors, Internet Service Providers, Social Networks, etc, RARELY contribute to increasing security threats and vulnerabilities for cyber-attacks to your immediate working (industrial/operational) domain.
- A. Totally agree [2]
 - B. Tend to agree [3]
 - C. Tend to disagree [4]
 - D. Totally disagree [5]
 - E. Don't Know [1]
18. Please to what extent do you agree or disagree with the following statement?
- In the event of being a target or victim of a cyber-attack, you know where and whom to report to for support
- A. Totally agree [5]
 - B. Tend to agree [4]
 - C. Tend to disagree [3]
 - D. Totally disagree [2]
 - E. Don't Know [1]
19. Which statement best describes your knowledge of potential solutions available for addressing cyber security threats to ICS/SCADA infrastructure and(or) enterprise network
- A. I know what solutions are available for ALL ICS/SCADA security threats [2]
 - B. I know what solutions are available for MOST ICS/SCADA security threats [3]
 - C. I know what solutions are available for SOME ICS/SCADA security threats [5]
 - D. I know what solutions are available for FEW ICS/SCADA security threats [4]
 - E. I DO NOT know what solutions are available for ICS/SCADA security threats [1]
20. Who do you think is, or could be attacking your ICS/SCADA infrastructure and networks
- A. Outsider Hackers [3]
 - B. Insider Hackers [4]
 - C. Both insiders and Outsiders [5]
 - D. No One [2]
 - E. Don't Know/Not Sure [1]

B. Cyber Security Skills Questionnaire

Note: Higher capability for appropriate response implies lesser security risk potential

1. How do you manage your passwords/credentials to prevent loss, or not being locked-out of your industrial/production system?
- A. On mobile devices [4]
 - B. In Physical or Electronic Diary [3]
 - C. On Sticky Notes on Desk [1]
 - D. Memorised (Off-heart) [5]
 - E. Shared-password with colleagues [2]
2. How often does the company update its industrial antivirus and antimalware applications?
- A. Weekly [2]
 - B. As prescribed by security policy [4]
 - C. Monthly [3]
 - D. I don't Know [1]
 - E. As soon as Available [5]
3. How do you access and exchange files and documentations on your Industrial Network USB drives and other external medias
- A. Using External Storage media [1]
 - B. Using Remote Access Configurations/Networks [5]
 - C. Through Email attachments [4]
 - D. As intuition directs (alternates between A and B) [3]
 - E. Using Wireless Mediums (e.g. Bluetooth, Near Field, Infrared, HotKnot, etc) [2]
4. Knowing the channel and mode of reporting in the event of being a victim of a (suspected) cyber-attack/intrusion/infection.
- A. Totally agree [5]
 - B. Tend to agree [4]
 - C. Tend to disagree [3]
 - D. Totally disagree [2]
 - E. Don't Know [1]
5. Ever noticed/discovered any form of hack/attack/intrusion or compromise in your work system or industrial control network/equipment?
- A. Yes, One or more of these have been attack/compromised before [5]
 - B. No, None of these have been attack/compromised before [4]
 - C. I do not know if any of these have been attack/compromised before [2]
 - D. Never had to consider such potentials [1]
 - E. My work domain is completely isolated and unreachable for hackers [3]
6. Knowing what to look-out for, and how to tell if your industrial domain (work station, network or other critical infrastructure) is attacked or infected
- A. Totally agree [5]

- B. Tend to agree [4]
- C. Tend to disagree [3]
- D. Totally disagree [2]
- E. Don't Know [1]

7. How do you respond to the either of the following; the mouse on your workstation screen begins to move around on its own and click things, or the controls on your monitoring station (HMI) get activated on their own.
- A. Call your co-workers over so they can see and witness [3]
 - B. Inform your supervisor / line manager immediately, and call for technical support [5]
 - C. Run system and antivirus updates/patches immediately to fix the problem [2]
 - D. Disconnect the mouse, control station network from others, and power off the abnormal system immediately [4]
 - E. Don't worry, take time to observe the behaviour and only inform your supervisor/line manager if problem persists or is beyond your control [1]
8. In your opinion, which of these offers a stronger and more secure password type to adopt?
- A. %\$E-@*#! [1]
 - B. 1234pwd [2]
 - C. Qwert#xk [4]
 - D. UdG7@zm[5]
 - E. Password8[3]
9. Because you are keen on enhancing your cyber security knowledge and skills, you subscribed to a number of free online ICS/SCADA Security Magazines. To activate your free subscription, you are required to register with your work email. One magazine asks for your year of birth, a second asks for your month of birth, a third asks for your mother's maiden name. How do you respond to all these?
- A. Supply all the correct information as the organisation needs to know you better to provide you with the best and most useful information [1]
 - B. Give out your personal email rather than your work email [2]
 - C. Do not trade-off your private information for any information you are not certain about, not to unknown persons or organisation [5]
 - D. It does not matter what information you supply, so long as you gain access to the Information/Cyber Security Magazines you subscribed. [3]
 - E. Supply false details [4]
10. Two different offices in your workplace are working to straighten out an error in your Single Sign-On Account (Login) configurations and Bank payments details. Office 1 asks you to email your correct account details. You send the requested details via email to office 1, which is subsequently forwarded via email to office 2. Office 2 confirms to have straightened the error out. What do you think could be wrong here?
- A. Nothing could be wrong, as the error has been straightened out [3]
 - B. It is wrong sending your bank details, but OK sending your login details [4]
 - C. It is wrong sending your sensitive information via unsecure channels like emails [5]
 - D. I am not sure if anything is wrong here. [1]
 - E. It is wrong not sending emailing the required information to the bank [2]
11. Your line manager / supervisor is very busy and asks you to log into the Industrial Control System Server / Data Historian using his/her user credentials (User-ID, Password, Pin, etc) to retrieve some control system data for reporting. What should you do?
- A. Obey your boss, and do as instructed following official procedures [4]
 - B. Ignore the instruction, and hope that he/she forgets [3]
 - C. Decline the request, and remind your boss that it is against user compliance policy [5]
 - D. Do as instructed, but keep it a secret [2]
 - E. Do nothing [1]
12. You are an industrial staff whose duties involves interaction with external or third party vendors, suppliers, engineers, contractors, etc. How do you respond when contacted (email, instant messaging, phone, etc) with the following information;
- Dear,*
- Three days from now, we will be deleting all inactive business/email accounts in order to create space for more users. You are required to reply back with the following information in order to continue using your business/email account. If we do not receive this information from you by the end of the third day, your business/email account will be deleted. (1) Full Name on Account (2) Account/Email Login ID (3) Password. Please contact the webmail team for any inquiries. Thank you for your timely response.*
- A. Reply immediately with the required information to meet the short notice [1]
 - B. Ignore the information and do not report to anyone [4]
 - C. Do not provide the information required to anyone, and report or confirm with technical support for actions [5]
 - D. Do your private investigation and only send the requested information when satisfied [3]
 - E. Reply with the requested information, and copy your line manager and(or) technical support [2]

13. As an industrial workforce (operator, technician, engineer, supervisor, etc) you notice that a configured process now completes at a time 2 to 3 minutes earlier than the known or pre-configured duration. What do you do?
- Perform your own private investigation about the change, and only divulge after you are done [3]
 - Do not worry as any anomaly would soon be discovered [2]
 - Discuss the time change with other operators and take their opinion [4]
 - It is a sign of efficiency and improvement, so do not do anything [1]
 - Report the change to appropriate line manager and verify the authenticity of the change [5]
14. It is festivity time; you receive an electronic greeting card (e-card) to your work email from a friend. The mail requires you to click on the attachment to view the electronic card. What should you do?
- Use other means possible to verify the origin and authenticity of the email before opening the attachment [3]
 - Open the email and attachment to verify it truly came from your friend, if not delete it. [2]
 - It is OK and normal to receive e-cards from friends and family during festive seasons [1]
 - Forward the email to your private/personal email and open it there [4]
 - Do not click or open the attachment, delete it immediately [5]
15. Which of the following character set do you, or are you likely to use for your strong account password as a system user?
- Combined Upper Case, Lower Case, Numbers, and Symbol (special characters) [5]
 - Combination of any 3 [4]
 - Combination of any 2 [3]
 - Any one set of characters will do [2]
 - Not keen on password character set and strength. [1]
16. Outside the scheduled/planned maintenance period, you receive an email or pop-up notification on your workstation to urgently initiate a 'critical' security update or patch that you are not sure has been tested but addresses certain security flaws on your ICS node.
- Do not install the update/patch, and leave the security flaw [4]
 - Quickly install the update/patch to enhance the security of your ICS node. [2]
 - Test the acceptability of the patch yourself, and install when satisfied [3]
 - Seek and verify the approval and accountability for the update/patch from technical support [5]
 - Neither install or verify patch since your system is not breached and is working normal [1]
17. How often do you change/review your account password assuming organisational security policy is in place for that?
- Whenever I deem necessary [1]
 - Bi-annually [4]
 - When my password is compromised [2]
 - Monthly [5]
 - Annually [3]
18. How often do you use your personal device or email for office works?
- Most times [2]
 - Not at all [5]
 - When necessary [4]
 - Always [1]
 - When asked to do so [3]
19. You possess the requisite operational cyber security certification(s) that affirm your security capability to secure your operational endpoint (HMI, Control station, MTU, RTU, etc) from cyber-attacks while undertaking your job duties and responsibilities?
- Totally agree [5]
 - Tend to agree [4]
 - Tend to disagree [3]
 - Totally disagree [2]
 - Don't Know [1]
20. It is the sole responsibility of the information security department to protect company assets by engineering protection and proper use of information assets, deploying security technologies for securing industrial processes, and developing proper security practices for daily activities
- Totally agree [2]
 - Tend to agree [3]
 - Tend to disagree [4]
 - Totally disagree [5]
 - Don't Know [1]