



CYBER MAINTAINABLE SAFETY-CRITICAL  
COMPLEX-SYSTEMS

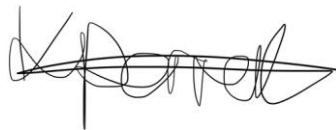
KIRSTY PERRETT

DOCTOR OF PHILOSOPHY

2023

## Candidate declaration

*This is to certify that, except where specific reference is made, the work described in this thesis is the result of my own research. Neither this thesis, nor any part of it, has been presented or is currently submitted, in candidature for any other award at this or any other University.*



**Signed**

**Kirsty Perrett**

**Candidate**

**Date**

**Tuesday 24<sup>th</sup> October 2023**

# ACKNOWLEDGEMENTS

Composing this thesis has proven to be an extremely challenging and prolonged endeavour, fraught with numerous obstacles along the way. Nevertheless, the experience and lessons learned from this journey has been undoubtedly the most rewarding and I am forever grateful for the unwavering support and encouragement that I received along the way. Becoming a parent midway through my PhD journey was not without its difficulties, but Freddie served as a source of inspiration and motivation for me to persevere. I hope that one day he will be able to reflect on my achievements with pride and use them to fuel his own aspirations.

On a personal level, it has meant the world to me to be the first in my family to achieve this academic qualification. It was not something I really thought feasible. However, this journey would not have been possible if it were not for the support and the belief I received from colleagues, fellow students namely Andrea, other academics, friends and family and I would like to acknowledge the following key individuals:

- First and foremost, I wanted to extend my heartfelt gratitude to Dr Ian D Wilson, my PhD Supervisor, for the incredible support and guidance he have provided throughout my PhD journey. Our long chats and regular conversations felt more like life coaching on times and I cherished our discussions immensely. His consistency and understanding, coupled with his persistence in chasing me for updates and meetings in the early days, always kept me on track, even when I felt overwhelmed. Every week, our insightful discussions and his timely advice helped me navigate through the challenges. I will undoubtedly miss his guidance and the humour he brought to our interactions and I thank him for not just being a supervisor but also a mentor and a source of inspiration. I would not have got this far without him.
- Thales Ebbw Vale; Dene Yandle, Adam Jefferis, Leanne Connor and Chris Hilbourne.
- Thales as my sponsor, in particular Dr Alex Tarter and Dr Craig Read.
- My Parents and Sister for supporting and believing in me throughout.
- Finally, I would like to express my gratitude to my partner Kieran, for generously dedicating his time to support me throughout the completion of my PhD.

The authors acknowledge the support of the Knowledge Economy Skills Scholarships (KESS) and Thales Ltd. KESS is a pan-Wales higher level skills initiative led by Bangor University on behalf of the HE sectors in Wales. It is part funded by the Welsh Government's European Social Fund (ESF) convergence programme for West Wales and the Valleys.

*"Only when the design fails does it draw attention to itself; when it succeeds, it's invisible."*

**John D. Berry**

*"Without commitment, you'll never start but without consistency you'll never finish."*

**Denzel Washington**

# ABSTRACT

The industrial manufacturing sector is a rapidly growing and highly technical industry undergoing significant change. These changes are being driven by the growing emphasis on sustainability, the need to streamline production processes, cost-cutting pressures and the demand for safer working environments. This is further exacerbated by the growing threat of cyber-attacks on control systems. Whilst the convergence of Operational and Informational Technology becomes essential, the traditional security approach has proven inadequate in addressing the unique challenges faced by such industries. As a result, Cyber Resilience is rapidly gaining momentum.

The idea of resilience and its successful attribution in other disciplines has ignited research in the cyber domain. However, the confusion around the application of Cyber Resilience, along with its various definitions and scope of meanings, has triggered debate in literature. Emerging as a topic of government discussion over a decade ago, resilience metrics have since been a key objective for the research community. Although developments are being made towards Cyber Resilience, the metrics and approaches available are not yet suitable for specific cases such as in a critical manufacturing system (e.g., metrics that are essential for evaluating production impact during a cyber-attack). Consequently, this thesis offers an approach that enables an objective, quantitative measurement of a critical manufacturing systems Cyber Resilience.

The research presented in this thesis provides two case study evaluations, performed at real-world manufacturing plants, a comprehensive description of an experimental method and physical test bed that were specifically designed to acquire resilience-related data from a manufacturing system. The testbed composition closely mirrors those systems identified during the case studies. A remote cyber-attack is described and Cyber Resilience metrics have been proposed and modelled to assess the impact of a successful cyber-attack, before and after resilience enhancements were applied. The findings uncover specific attributes and parameters that stood out from the experimental data, revealing which attributes serve as a practical and meaningful quantitative indicator of a system's Cyber Resilience. The improvements made to the testbed significantly increased the system's ability to endure and recover from a successful cyber-attack. Interestingly, the experiments demonstrated that, when designed in accordance with secure control practices, the inherent resilience mechanisms that exist in a safety-critical system exhibited the highest single success rate in maintaining nominal performance relative to other enhancement measures. Where

enhancement measures are combined, the system was able to absorb and withstand the disruption.

The outcomes of this research suggest that a combination of security, system and safety engineering practice is critical to enhancing Cyber Resilience. The findings exemplify how Cyber Resilience can help address the emerging complexities with respect to safety-critical complex-systems. Results show that development of a universal metric that applies to all manufacturing systems is unrealistic.

# CONTENTS

<b>ACKNOWLEDGEMENTS</b> .....	<b>I</b>
<b>ABSTRACT</b> .....	<b>III</b>
<b>CONTENTS</b> .....	<b>V</b>
<b>LIST OF TABLES</b> .....	<b>X</b>
<b>LIST OF FIGURES</b> .....	<b>XII</b>
<b>LIST OF ABBREVIATIONS AND ACRONYMS</b> .....	<b>XVI</b>
<b>KEY WORDS</b> .....	<b>XVI</b>
<b>CHAPTER 1 INTRODUCTION</b> .....	<b>1</b>
1.1    HYPOTHESES .....	5
1.2    MOTIVATION.....	5
1.3    AIM .....	6
1.4    RESEARCH QUESTIONS .....	6
1.5    OBJECTIVES .....	7
1.6    RESEARCH METHODS.....	8
1.7    CONTRIBUTION .....	11
1.8    RELATED PUBLICATIONS .....	11
1.9    THESIS ROADMAP .....	13
1.10   CHAPTER SUMMARY .....	15
<b>CHAPTER 2 BACKGROUND</b> .....	<b>16</b>
2.1    INTRODUCTION .....	16
2.2    SAFETY-CRITICAL INDUSTRIAL CONTROL SYSTEMS.....	17
2.2.1 <i>Background</i> .....	18
2.2.2 <i>Challenges Securing OT Environments</i> .....	21
2.2.3 <i>Safety-Critical Systems</i> .....	23

2.3	COMPLEX SYSTEMS.....	28
2.3.1	<i>Application of Complex Systems</i> .....	31
2.4	RESILIENCE.....	32
2.4.1	<i>History of Resilience</i> .....	32
2.4.2	<i>Ecological vs. Engineering Resilience</i> .....	33
2.4.3	<i>Resilience Definitions and Concepts</i> .....	34
2.5	CYBER SECURITY AND CYBER RESILIENCE .....	39
2.5.1	<i>Cyber-Attacks on OT Environments</i> .....	43
2.5.2	<i>Towards OT Cyber Resilience</i> .....	48
2.6	CHAPTER SUMMARY .....	52
<b>CHAPTER 3 LITERATURE REVIEW.....</b>		<b>53</b>
3.1	INTRODUCTION .....	53
3.2	SELECTION OF RELEVANT LITERATURE.....	53
3.3	CHARACTERISTICS OF CYBER RESILIENCE.....	54
3.3.1	<i>Cyber Resilience Attributes</i> .....	55
3.3.2	<i>Cyber Resilience Parameters</i> .....	69
3.4	MEASUREMENT APPROACHES .....	77
3.4.1	<i>Quantitative Objective Approaches</i> .....	77
3.4.2	<i>Qualitative Subjective Approaches</i> .....	83
3.4.3	<i>Standards and Frameworks of Relevance</i> .....	88
3.5	CONNECTING THE ABOVE .....	98
3.6	PROBLEM STATEMENT AND CHAPTER SUMMARY.....	99
<b>CHAPTER 4 EXPERIMENT DESIGN .....</b>		<b>101</b>
4.1	INTRODUCTION .....	101
4.2	RESEARCH OVERVIEW .....	101
4.2.1	<i>Phase 1: Case Studies</i> .....	102



4.2.2	<i>Phase 2: Testbed Design</i> .....	110
4.2.3	<i>Phase 3: Definition of metrics and specification of tests</i> .....	114
4.2.4	<i>Phase 4: Functions of Resilience</i> .....	114
4.3	CHAPTER SUMMARY .....	116
<b>CHAPTER 5 ANALYSIS OF CASE STUDIES .....</b>		<b>117</b>
5.1	INTRODUCTION .....	117
5.2	PHASE 1- CASE STUDY A .....	117
5.2.1	<i>Data Analysis</i> .....	117
5.2.2	<i>Baseline Results</i> .....	124
5.2.3	<i>Case Study A - Conclusion</i> .....	134
5.3	PHASE 1 - CASE STUDY B.....	135
5.3.1	<i>Data Analysis</i> .....	135
5.3.2	<i>Baseline Results</i> .....	139
5.3.3	<i>Case Study B – Conclusion</i> .....	168
5.4	COMPARATIVE ANALYSIS OF CASE STUDY RESULTS .....	169
5.5	CHAPTER SUMMARY .....	172
<b>CHAPTER 6 SIMULATION &amp; MODELLING .....</b>		<b>173</b>
6.1	INTRODUCTION .....	173
6.2	PHASE 2 - TESTBED DESIGN .....	174
6.2.1	<i>Testbed Description and Scenario Use Case</i> .....	174
6.2.2	<i>Physical and Logical Components</i> .....	179
6.2.3	<i>Cyber-Attack Design</i> .....	186
6.3	PHASE 3 – DEFINITION OF METRICS AND SPECIFICATION OF TESTS .....	190
6.3.1	<i>Selection of Resilience Enhancements</i> .....	190
6.3.2	<i>Definition of Metrics</i> .....	193
6.3.3	<i>Specification of Tests</i> .....	198

6.4	PHASE 4 - FUNCTIONS OF RESILIENCE - SIMULATION RESULTS .....	204
6.4.1	<i>Introduction to Results</i> .....	205
6.5	CHAPTER SUMMARY .....	215
<b>CHAPTER 7 DISCUSSION .....</b>		<b>216</b>
7.1	INTRODUCTION .....	216
7.2	CASE STUDY DISCUSSION .....	217
7.3	SIMULATION DISCUSSION .....	218
7.3.1	<i>Discussion - Test 1</i> .....	220
7.3.2	<i>Discussion - Test 2</i> .....	221
7.3.3	<i>Discussion - Test 3</i> .....	221
7.3.4	<i>Discussion - Test 4</i> .....	222
7.3.5	<i>Discussion - Test 5</i> .....	223
7.3.6	<i>Discussion - Test 6</i> .....	224
7.4	ANSWERING THE RESEARCH QUESTIONS .....	226
7.4.1	<i>In response to Question 1</i> .....	226
7.4.2	<i>In response to Question 2</i> .....	228
7.4.3	<i>In response to Question 3</i> .....	230
7.5	LIMITATIONS .....	235
7.6	CHAPTER SUMMARY .....	235
<b>CHAPTER 8 CONCLUSION AND FUTURE WORK .....</b>		<b>237</b>
8.1	INTRODUCTION .....	237
8.2	SUMMARY OF FINDINGS .....	237
8.3	RESEARCH OBJECTIVES .....	240
8.4	FUTURE WORK .....	241
8.5	CONTRIBUTION TO KNOWLEDGE .....	242
<b>REFERENCES .....</b>		<b>243</b>

<b>APPENDIX 1 CASE STUDY FRAMEWORK .....</b>	<b>259</b>
<b>APPENDIX 2 TESTBED PLC CONFIGURATION .....</b>	<b>276</b>
<b>APPENDIX 3 EQUATIONS .....</b>	<b>280</b>
<b>APPENDIX 4 RESEARCH OUTPUT .....</b>	<b>281</b>

## List of Tables

TABLE 2-1 CHARACTERISTICS OF COMPLEX SYSTEMS .....	29
TABLE 2-2 SYSTEMS CLASSIFIED BY DEGREE OF COMPLEXITY: ADOPTED FROM (MAGEE & DE WECK, 2004) .....	30
TABLE 2-3 DIFFERENCES BETWEEN ENGINEERING AND ECOLOGICAL RESILIENCE (BAGHERI & RIDLEY, 2017).....	34
TABLE 2-4 RESILIENCE CONCEPTS .....	39
TABLE 2-5 OT THREAT TAXONOMY EXAMPLE.....	41
TABLE 3-1 COMMON METRIC CRITERIA RELATING TO CYBER RESILIENCE. ....	72
TABLE 3-2 METRICS WITH FOCUS ON THE MANUFACTURING SECTORS .....	73
TABLE 3-3 METRICS WITH FOCUS ON CYBER SECURITY.....	75
TABLE 3-4 CYBER RESILIENCE MEASUREMENT APPROACHES.....	79
TABLE 3-5 P3R3 CYBER RESILIENCE MECHANISMS - ADOPTED FROM (THERON, 2013) .....	86
TABLE 3-6 COMMONLY ADOPTED OT CS FRAMEWORKS .....	88
TABLE 3-7 THE CYBER RESILIENCE MATRIX – ADOPTED FROM (LINKOV, ET AL., 2013) .....	91
TABLE 3-8 IEC 62443 MATURITY LEVEL DEFINITIONS .....	94
TABLE 3-9 TOP 20 SECURE PLC PRACTICES – ADOPTED FROM (PLC SECURITY, 2021) .....	96
TABLE 4-1 SELECTION OF CASE STUDY SUBJECTS .....	104
TABLE 5-1 DATA TYPES COLLECTED.....	119
TABLE 5-2 ASSET TYPE TO PHYSICAL LOCATION MAPPING.....	120
TABLE 5-3 PHYSICAL TOPOLOGY - MAPPING ASSETS TO GEOGRAPHICAL LOCATION.....	123
TABLE 5-4 VULNERABILITY ASSESSMENT .....	129
TABLE 5-5 RECOMMENDATIONS .....	131
TABLE 5-6 CYBER RESILIENCE EVALUATION .....	132
TABLE 5-7: IEC 62443 MATURITY LEVEL DEFINITIONS .....	137
TABLE 5-8: MATURITY LEVEL DESCRIPTION FOR INSUFFICIENT DATA .....	137
TABLE 5-9: THALES OT ASSESSMENT SCORING SYSTEM .....	138
TABLE 5-10: INDICATIVE MAPPING OF THALES OT ASSESSMENT TO IEC 62443-2-1 (2019) MATURITY LEVEL..	139

TABLE 5-11 SUMMARY OF FINDINGS BY TOPIC.....	140
TABLE 5-12 ORG 1 MATURITY LEVEL - SECURITY RELATED ORGANISATION AND POLICIES.....	143
TABLE 5-13 ORG 2 MATURITY LEVEL – SECURITY ASSESSMENTS AND REVIEWS .....	145
TABLE 5-14 ORG 3 MATURITY LEVEL – SECURITY OF PHYSICAL ACCESS .....	146
TABLE 5-15 CM1.A MATURITY LEVEL – DOCUMENTATION .....	147
TABLE 5-16 CM1.B MATURITY LEVEL – CONFIGURATION AND CHANGE MANAGEMENT .....	148
TABLE 5-17 NET 1 MATURITY LEVEL – SYSTEM SEGMENTATION .....	149
TABLE 5-18 NET 2 MATURITY LEVEL – SECURE WIRELESS NETWORKS .....	151
TABLE 5-19 NET 3 MATURITY LEVEL – SECURE REMOTE ACCESS.....	151
TABLE 5-20 COMP 1 MATURITY LEVEL – DEVICES AND MEDIA.....	153
TABLE 5-21 COMP 2 MATURITY LEVEL – MALWARE PROTECTION .....	154
TABLE 5-22 COMP 3 MATURITY LEVEL – PATCH MANAGEMENT .....	155
TABLE 5-23 DATA1.A MATURITY LEVEL – DATA MANAGEMENT .....	156
TABLE 5-24 USER 1 MATURITY LEVEL – IDENTIFICATION AND AUTHENTICATION .....	158
TABLE 5-25 USER 2 MATURITY LEVEL – AUTHORISATION AND ACCESS CONTROL.....	160
TABLE 5-26 EVENT 1.A MATURITY LEVEL – DETECTION AND LOGGING.....	161
TABLE 5-27 EVENT 1.B MATURITY LEVEL – INCIDENT AND VULNERABILITY HANDLING .....	162
TABLE 5-28 AVAIL 1 MATURITY LEVEL (SYSTEM AVAILABILITY AND INTENDED FUNCTIONALITY) .....	163
TABLE 5-29 AVAIL 2 MATURITY LEVEL (BACKUP/RESTORE/ARCHIVE).....	164
TABLE 5-30 IEC 62443-2-1 ASSESSMENT SCORING.....	168
TABLE 5-31 CASE STUDY RESULTS COMPARISON MAPPINGS.....	171
TABLE 6-1 PHYSICAL COMPONENTS IN THE TESTBED .....	179
TABLE 6-2 ENHANCEMENTS MADE TO THE TESTBED - ADOPTED FROM (PLC SECURITY, 2021). .....	192
TABLE 6-3 CR DOMAINS MAPPED TO RELEVANT ATTRIBUTES IN THIS RESEARCH. ....	194
TABLE 6-4 ENHANCEMENT TECHNIQUES MAPPED TO STANDARDS/Frameworks.....	195
TABLE 6-5 MAPPINGS BETWEEN THIS STUDY AND THE CR MATRIX SET OUT IN (LINKOV, ET AL., 2013) .....	196

TABLE 6-6 SPECIFICATION OF MODELLING METRICS AND TESTS.....	197
---	-----

## LIST OF FIGURES

FIGURE 1-1 RESEARCH APPROACH .....	10
FIGURE 1-2 THESIS OUTLINE.....	14
FIGURE 2-1 PLC (INTERNATIONAL SOCIETY OF AUTOMATION (ISA), 2020).....	19
FIGURE 2-2 PLC LADDER LOGIC CONFIGURATION EXAMPLE .....	20
FIGURE 2-3: AN EXAMPLE PURDUE MODEL ADOPTED FROM (GENERAL ELECTRICS, 2017) .....	21
FIGURE 2-4 THE FOUR INDUSTRIAL REVOLUTIONS – ADOPTED FROM (MELOENY, 2022) .....	23
FIGURE 2-5 INDUSTRY SPECIFIC SAFETY STANDARDS. IMAGE ADOPTED FROM (TUVSUD, 2022) .....	25
FIGURE 2-6 THE SCOPE OF IEC 62601 ADOPTED FROM (TUVSUD, 2022).....	26
FIGURE 2-7 STATE OF OT/ICS CYBER SECURITY SURVEY – ADOPTED FROM (ASSANTE & LEE, 2015) .....	40
FIGURE 2-8 CYBER INTRUSION STAGE 1 & 2 - ICS ATTACK – ADOPTED FROM (ASSANTE & LEE, 2015) .....	42
FIGURE 2-9 MITRE ATT&CK FOR ICS MATRIX (MITRE, 2017) .....	44
FIGURE 2-10 STUXNET ATTACK - ICS KILL CHAIN; ADOPTED FROM (ASSANTE & LEE, 2015) .....	45
FIGURE 3-1 NUMBER OF SEARCHES RELATED TO THE TERM CYBER RESILIENCE. (GOOGLE NGRAM VIEWER, 2022)	54
FIGURE 3-2 NUMBER OF SEARCHES RELATED TO THE TERM CYBER RESILIENCY. (GOOGLE NGRAM VIEWER, 2022)	54
FIGURE 3-3 HIGH-LEVEL DIMENSIONS OF CYBER RESILIENCE .....	56
FIGURE 3-4 DEPENDABILITY, RELIABILITY AND AVAILABILITY (AN EXAMPLE) .....	58
FIGURE 3-5 ENHANCING OR COUNTERACTING CYBER RESILIENCE .....	67
FIGURE 3-6 ATTRIBUTE EXAMPLES .....	68
FIGURE 3-7 CYBER RESILIENCE MEASUREMENT THEMES IN LITERATURE. ....	77
FIGURE 3-8 CYBER SECURITY AND RESILIENCE RELATIONSHIPS. (ADOPTED FROM CARIAS, ET AL., 2018) .....	82
FIGURE 3-9 IEC 62443-2-1 ASSESSMENT SUMMARY .....	95
FIGURE 3-10 HOLISTIC OVERVIEW OF CYBER RESILIENCE LANDSCAPE .....	100

FIGURE 4-1 DIAGRAMMATIC STRUCTURE OF THE RESEARCH DESIGN .....	102
FIGURE 4-2 CASE STUDY QUESTIONNAIRE (EXAMPLE) .....	106
FIGURE 4-3 CASE STUDY STEPS .....	107
FIGURE 4-4 A DIAGRAMMATIC STRUCTURE OF THE CASE STUDY METHODOLOGY .....	108
FIGURE 4-5 CASE STUDY DATA ENTITY DIAGRAM.....	109
FIGURE 4-6 THE HUMAN CONTROLLER MODEL ADOPTED FROM (LEVESON, 2020) .....	111
FIGURE 4-7 DIAGRAMMATIC STRUCTURE OF THE SIMULATION METHODOLOGY .....	113
FIGURE 4-8 QUANTITATIVE DATA COLLECTION PROCESS - RESEARCH APPROACH.....	114
FIGURE 4-9 HIGH-LEVEL QUANTITATIVE MEASUREMENT APPROACH - TESTBED .....	115
FIGURE 4-10 FUNCTIONS OF RESILIENCE APPROACH .....	115
FIGURE 5-1 OT ASSETS TO PURDUE LEVEL.....	120
FIGURE 5-2 LOGICAL TOPOLOGY WITH NOTABLE TRAFFIC CONCERNS HIGHLIGHTED IN RED.....	122
FIGURE 5-3 SUMMARY OF REQUIRED VS ACTUAL MATURITY LEVEL INDICATIONS PER AREA.....	128
FIGURE 5-4 CREDENTIALS ON STICKY NOTE .....	159
FIGURE 5-5 MAPPING CASE STUDY FRAMEWORK RESULTS.....	170
FIGURE 6-1 PRODUCTION PROCESSING STEPS.....	175
FIGURE 6-2 OT NETWORK ARCHITECTURE TOPOLOGY .....	176
FIGURE 6-3 PLC THRESHOLD CONFIGURATION .....	177
FIGURE 6-4 PLC THRESHOLD CONFIGURATION .....	178
FIGURE 6-5 EUROTHERM FUNCTION BLOCK SET-POINT .....	178
FIGURE 6-6 PHYSICAL TESTBED (FULL).....	180
FIGURE 6-7 PHYSICAL TESTBED (ZOOMED) .....	180
FIGURE 6-8 SCHEMATIC DIAGRAM 01 DRAWN BY DENE YANDEL (2023) .....	181
FIGURE 6-9 SCHEMATIC DIAGRAM 02 DRAWN BY DENE YANDEL (2023) .....	181
FIGURE 6-10 SCHEMATIC DIAGRAM 03 DRAWN BY DENE YANDEL (2023) .....	182
FIGURE 6-11 REPRESENTATIVE PHYSICAL SYSTEM – HMI .....	182

FIGURE 6-12 THE EWON SERVER INTERFACE .....	183
FIGURE 6-13 THE EWON VPN REMOTE INTERFACE .....	183
FIGURE 6-14 TOPOLOGY OF THE REPRESENTATIVE ENVIRONMENT CREATED ON THE CYBER RANGE.....	184
FIGURE 6-15 DIAGRAMMATIC STRUCTURE OF THE REMOTE ATTACK.....	186
FIGURE 6-16 CYBER-ATTACK SEQUENCE .....	188
FIGURE 6-17 ZONING EXAMPLE, ADOPTED FROM (GENERAL ELECTRICS, 2017).....	191
FIGURE 6-18 EXPERIMENT CYBER RESILIENCE ATTRIBUTES .....	193
FIGURE 6-19 DIAGRAMMATIC STRUCTURE OF TESTS PERFORMED .....	198
FIGURE 6-20 HMI TEMPERATURE READING .....	199
FIGURE 6-21 PLC CONFIGURATION LOGIC .....	199
FIGURE 6-22 PLC LOGIC.....	201
FIGURE 6-23 SECURE LIMITS CONFIGURATION SET IN THE PLC.....	202
FIGURE 6-24 SECURE LIMITS CONFIGURED IN THE PLC. ....	202
FIGURE 6-25 PHYSICAL SYSTEM CR MEASUREMENT .....	204
FIGURE 6-26 NOMINAL SYSTEM PERFORMANCE MEASURED TEMPERATURE TEST.....	206
FIGURE 6-27 HMI INTERFACE .....	206
FIGURE 6-28 QUALITY OF INFANT MILK FORMULA DURING NORMAL OPERATING CONDITIONS .....	207
FIGURE 6-29 SYSTEM PERFORMANCE SHOWING THE MEASURED TEMPERATURE FOLLOWING A CYBER-ATTACK...	208
FIGURE 6-30 QUALITY OF INFANT MILK FORMULA BEFORE AND AFTER A CYBER DISRUPTION.....	208
FIGURE 6-31 SYSTEM PERFORMANCE FOLLOWING A CYBER DISRUPTION - WITHOUT CR ENHANCEMENTS.....	210
FIGURE 6-32 PRODUCT QUALITY % FOLLOWING A CYBER DISRUPTION (WITHOUT CR ENHANCEMENTS) .....	210
FIGURE 6-33 SYSTEM PERFORMANCE DURING A CYBER DISRUPTION - WITH CR ENHANCEMENTS .....	211
FIGURE 6-34 TEST 4 - QUALITY % OF PRODUCT FOLLOWING A CYBER DISRUPTION - WITH CR ENHANCEMENTS ..	212
FIGURE 6-35 TEST 5 – TIME BETWEEN START OF ADVERSARY ACTIVITIES AND THEIR DISCOVERY - WITHOUT CR ENHANCEMENTS .....	213
FIGURE 6-36 SIEM ALERT FOLLOWING ENHANCEMENTS.....	214
FIGURE 6-37 SIEM ATTACK LOGS .....	214



FIGURE 6-38 TEST 6 – TIME BETWEEN START OF ADVERSARY ACTIVITIES AND THEIR DISCOVERY - WITH CR ENHANCEMENTS. ....	215
FIGURE 7-1 RESEARCH APPROACH TO OBTAINING CR METRICS.....	217
FIGURE 7-2 COMPARISON OF SYSTEM PERFORMANCE DURING TESTS 1, 3 AND 4 .....	219
FIGURE 7-3 QUALITY % OF IMF FOLLOWING A CYBER-ATTACK - WITH AND WITHOUT CR ENHANCEMENTS.....	220
FIGURE 7-4 EXPERIMENT CYBER RESILIENCE ATTRIBUTES.....	228
FIGURE 7-5 OLDSMAR WATER ATTACK - HYPOTHETICAL USE CASE.....	231
FIGURE 7-6 THE CYBER RESILIENCE ATTRIBUTES SELECTED FOR THEORETICAL USE CASE. ....	233
FIGURE 7-7 ATTACK STEPS INTO THE PLANT. ....	234

## LIST OF ABBREVIATIONS AND ACRONYMS

<b>Term</b>	<b>Definition</b>
CNI	Critical National Infrastructure
CPS	Cyber-Physical Systems
CR	Cyber Resilience
CS	Cyber Security
FuSE	Future of Systems Engineering
HMI	Human Machine Interface
ICS	Industrial Control System
IIOT	Industrial Internet of Things
IOT	Internet of Things
ISA	International Standards Authority
ISO	International Standards Organisation
IT	Information Technology
NIST	National Institute Standards and Technology
OT	Operational Technology
PLC	Programmable Logic Controller
CPPS	Cyber Physical Production Systems
CMS	Cyber Manufacturing Systems

### Key Words

Safety-Critical Systems, Cyber-Physical Systems, Cyber Resilience, System Resilience, Engineering Resilience, Complex-Systems, Operational Technology, Industrial Control Systems, Control Theory, Automation and Control Systems, Cyber Resiliency Metrics, Emergence, Systems Engineering, Systems-of-Systems, Complexity.

# Chapter 1

## Introduction

The term 'resilience', we see it everywhere of late. Some refer to it as a 'buzz' word, others with high hopes it can save our planet. It is in the media, medicine and psychology, it is used in parliament, sport, engineering and now in the world of cyber. But what is it? And why suddenly has it gained such attraction?

Resilience has its roots in many disciplines but the term itself, its many definitions and scope of means all take quite different perspectives depending on the discipline in which its applied or the person who you ask (Smith, 2023). The idea of resilience and its successful attribution in other disciplines has ignited research into Cyber Resilience (CR). Which is rapidly gathering momentum in the manufacturing sector due to the advancements in technology and the initiative for better efficiency through data-backed manufacturing processes (Jacobs, et al., 2018). Further expanded by the race towards industrial digital transformation and the growing threat of cyber-attacks on manufacturing and production systems.

Industry has lived through three eras of technological transformation in the last two hundred years. A fourth industrial transformation is underway that has demonstrated the convergence of the cyber and physical worlds, which includes Information Technology (IT) and Operational Technology (OT), the early development of smart technology and the interconnection of safety-critical complex-systems (Carías, et al., 2021). IT and OT represent two distinct technology domains within an organisation. IT deals with the computing systems, networks and data management that support administrative and business functions, such as email, office software, networks and databases. In contrast, OT is focused on managing and controlling physical processes and equipment in critical

industries, like manufacturing, energy and infrastructure, using specialised technologies like SCADA systems and industrial control systems.

The IT and OT convergence refers to the integration and overlap of these two traditionally separate domains. It's driven by the desire to improve operational efficiency and decision-making by sharing data between IT and OT systems. This convergence allows organisations to harness the power of data analytics, IoT (Internet of Things) and automation to enhance productivity and reduce costs. However, it also introduces new security challenges, as the priorities and threats in IT and OT can differ significantly, requiring a holistic approach to manage the combined environment effectively (Kagermann, et al., 2013).

With this continued drive for efficiency to increase competitiveness through automation and manufacturing processes, many control systems established in the industrial age have been thrown into today's data-driven digital world. Whilst the evolution provides benefits for businesses and society, industrial systems, historically, have not been planned or executed with digital security as a priority and although these systems are programmed to fail safely, the concern is how they might function when being operated by a malicious actor (National Institute of Standards and Technology, 2021).

This convergence means that we now live in a complex interconnected ecosystem consisting of technology, data, people, processes and infrastructure (Carías, et al., 2021). The challenges this represents within industry often creates division between personnel, depending on their disciplines, in that they have different profiles, urgencies, priorities and systems to maintain and manage. Exacerbated by the global shortfall in IT/OT/cyber security trained professionals remains a significant issue facing industry and governments. It is also a significant factor in Cyber Resilience.

In addition there is confusion around principles in the two- environments, for example, the CIA triad is a fundamental concept in information security, representing three core principles: Confidentiality, Integrity and Availability. Confidentiality ensures that data remains private and is only accessible to authorised individuals. Integrity ensures that data remains accurate and unaltered by unauthorised users or processes. Availability ensures that data and systems are consistently accessible when needed. In the realm of Operational Technology (OT), which involves managing industrial control systems, the concept extends to include safety as a crucial factor. Safety emphasises the protection of physical assets and human lives, particularly in critical infrastructure sectors like energy, transportation and manufacturing. Hence, the security priorities in OT encompass both the preservation of data integrity and the safeguarding of physical safety, making it slightly different from the traditional CIA triad, reflecting the unique challenges and

priorities of the OT environment. Furthermore, the excessive reliance on digital technology and the complexity in which these systems interconnect, means that the number of high-profile cyber-attacks on critical infrastructure will only grow (Schlaepfer, et al., 2015).

Cyber Resilience's primary objective is to ensure that a system can endure, recuperate or adjust in the event of a cyber-attack. Its focus lies not in assessing the system's ability to resist or prevent an attack but rather on its capacity to withstand, recover or adapt. The responsibility for resistance and prevention falls under the domain of Cyber Security and risk management. The adoption of a metrics-based approach to Cyber Resilience has gained significant popularity as it enables a quantifiable evaluation of a system's ability to withstand, recover or adapt during a cyber-attack (Caralli, et al., 2016). Nevertheless, the discipline is still relatively new and in need of further advancement in terms of the techniques, tools and methods that are necessary to obtain an objective measurement (Kott & Linkov, 2021). In the absence of a universally accepted definition and a clear methodology for measuring Cyber Resilience, it becomes challenging to determine whether resilience has improved or not. Determining whether the addition of a security control to a critical-safety and complex-system either enhances or diminishes its CR is also challenging (Jacobs, et al., 2018). The only means of ascertaining this would involve measuring the system's performance with and without a specific set of controls (Linkov & Kott, 2018); (Kott & Linkov, 2021). Though, without a clear approach in the steps needed to measure resilience, then how can one know whether it's improved or not? Can a system, organisation or even an entire species really become more resilient and how is this measured? This topic has caused much debate in literature (discussed in Chapter 3). Yet, despite this, the quest to become 'Cyber `Resilient' and the search for metrics to objectively measure it, is ever more present.

In pursuit of enhancing resilience in complex cyber-physical systems, might the obvious place to search lie with nature? Our every breath, our food, our water – humankind's very existence – comes from nature. Our very survival depends on the laws of nature all working together and in balance. In fact, humans are a fitting example of an interconnected complex and resilient system that is comparable with a computer system, for example: we have an intelligent neural communication network with vital information flowing through our bloodstream; information passed on via DNA from those before us and containing code to ensure life of the next and of the next; we have vital organs, some of which have redundancy and or a backup resource such as our kidneys and lungs. Conversely, other critical safety organs, such as our heart or brain, are standalone but these are vital organs and as such, are protected from external factors with defence in depth armours such as the multiple layers of skin, bone and tissue. Our white blood cells are our anti-virus or malware

protections ensuring the blood is safely transported without compromise and will attack any foreign body or intruder virus that breaks through our perimeter barriers. All of this relies on sensors and inputs from the other vital organs. These must work together and in harmony to provide a set of advantages by enabling each system to deliver its intended outcome time after time. This complex interconnection between components, systems and environments enables not only the sharing of valuable information but also the ability to adapt in a changing environment overtime.

This analogy or way of thinking is not particularly different from OT and IT environments and systems becoming interconnected and more complex. An example of the interconnections and general patterns observed in many complex systems and those observed in human cells is also given in (Ma'ayan, 2017) and (Mthunzi, et al., 2019). However, although this Ecological Resilience approach to reaching Cyber Resilience looks promising, the engineered systems of today are not yet capable or ready for such evolution and unfortunately the only likely approach currently, in the authors view, is the Engineering Resilience approach. This will change as systems become more intelligent and adaptable. However, in the Industrial domain, many historical systems are just not capable of adopting such an approach without the use of Artificial Intelligence (AI). Nevertheless, regardless of which approach is followed, the engineering world wants to mimic this and are taking steps to progress that (Sikula, et al., 2015). However, to truly realise this goal, we first need to measure it.

This thesis aims to increase understanding of the bigger picture in the context of complex safety critical systems. It identifies uses and perceptions of the term across multi-disciplinary sectors and highlights similarities of metric approaches identified and contributes by identifying and addressing the gap in literature. It looks at the practical steps needed to ensure resilience in systems by understanding what Cyber Resilience means and how it derives objectives, aims and requirements that translate to system design and implementation. In addition, this thesis explores the challenges of incorporating resilience into holistic system design that includes social, technical, educational and economic considerations as well as the variation in engineering such as software, hardware and data engineering disciplines. It examines the benefits of shifting current thinking towards combining security and safety considerations within systems, particularly having security and safety as functional requirements (INCOSE Resilient Systems Working Group, 2020), promotes this shift in thinking and is likely to improve overall system integrity.

## 1.1 Hypotheses

- i. It is possible to create and validate a cyber-maintainable safety-critical complex system architecture (with focus on the manufacturing and production sectors) through the construction of an advanced prototype system to obtain quantitative objective metrics.
- ii. Cyber Resilience is independent from Cyber Security, although it builds upon a foundation of Cyber Security. While the absence of security can jeopardise the resilience of a manufacturing system, even with security measures in place, the system's functionality can still be compromised due to inadequately planned deployment.

## 1.2 Motivation

There is an inherent conflict between the accreditation needs of safety-critical manufacturing systems that drive static configurations and the needs of cyber-secure systems to be maintainable to co-evolve with intentional and hostile threats in the manufacturing and production industries. This dichotomy will take on increasing importance as autonomous cyber-physical systems assume safety-related roles in the industrial digital eco-system. The growth in safety-critical complex systems is stimulating research into the measurement of Cyber Resilience for Industrial Control Systems (ICS). This area is a complex and evolving field of research, specifically in the field of Industrial Manufacturing. Furthermore, the misleading impression and fallacy of Cyber Resilience is inhibiting its adoption uptake in industry (Dupont, 2019).

Consequently, there are several gaps in research related to measuring Cyber Resilience for an industrial manufacturing system which include:

- Lack of consensus on what Cyber Resilience means in the context of Industrial Control Systems: There is no commonly accepted definition of Cyber Resilience. Different organisations and stakeholders have their own understanding of what it means to be Cyber Resilient.
- Insufficient metrics and methodologies: There are a lack of standardised and validated quantitative metrics and methodologies to measure the Cyber Resilience of a manufacturing system. The metrics that do exist are often focused on specific measures and do not capture the broader organisational and human factors that also impact Cyber Resilience.

- Limited understanding of the impact of cyber incidents on a systems resilience: There is a lack of empirical data and case studies on the impact of cyber incidents to the resilience of ICS. This makes it difficult to develop effective strategies and metrics to enhance CR.
- Limited research on Cyber Resilience in manufacturing industries: There is a lack of research in specific industries, such as manufacturing. This is problematic because different industries have different operational and organisational contexts that affect Cyber Resilience.

### 1.3 Aim

To address the gaps in research, there have been several efforts to develop new methodologies, frameworks and metrics to measure Cyber Resilience in Industrial Control Systems. However, overall, there is still much work to be done to improve our understanding and to develop effective methodologies and metrics to measure and improve this area. The aim of this study is to investigate if Cyber Resilience can reduce the impact of a successful remote cyber-attack to a critical manufacturing system using a combination of subjective qualitative analysis and empirical quantitative metrics to measure a given system accordingly.

### 1.4 Research Questions

To attain this aim, the following three research questions need to be addressed:

1. What are the current methods employed to analyse the level of Cyber Resilience in manufacturing systems?
2. What Cyber Resilience attributes and parameters are appropriate?
3. How is it possible to provide a level of assurance that a critical manufacturing system is Cyber Resilient using this research approach?



## 1.5 Objectives

The research objectives are derived from the aim and defined as follows:

1. To establish the various definitions of 'Resilience', clearly identifying how definitions vary between domains and contexts.
  - a. To establish a definition of Cyber Resilience in the context of this research for an industrial manufacturing system.
2. To conduct a literature study on the topic of Cyber Resilience in safety-critical complex-systems with concentration to the manufacturing industry to establish the current state of the art.
  - a. To discuss current approaches in literature toward the measurement of Cyber Resilience and to define which of the approaches are most relevant and meaningful.
3. To define the characteristics and parameters of cyber resilience.
4. To conduct primary research by way of case studies to collect original datasets from various sources across the industrial manufacturing sectors.
  - a. To analyse case study results, with focus on the most critical systems, zones and communications.
  - b. To establish qualitative baseline maturity levels and provide a series of recommendations through various frameworks and best practice guidance on how each study can enhance their Cyber Resilience maturity.
  - c. To clearly identify any limitations with the selected frameworks.
5. To design and build a representative physical test bed emulating a critical manufacturing system informed from case study observations.
  - a. To develop a cyber-attack to target the representative system, informed by case study evaluations.
  - b. To define a series of metrics to quantitatively measure Cyber Resilience on a representative manufacturing system in the event of a cyber-attack.
  - c. To implement and test simulation and modelling techniques to determine if the metrics and approaches defined enable a manufacturing system to achieve sustainability in a degraded situation.
  - d. To analyse, record and discuss the results.

## 1.6 Research Methods

This study aims to examine the attributes and parameters of Cyber Resilience with a specific emphasis on the measurement of Cyber Resilience for a critical manufacturing system when impacted by a cyber-attack. In this context, the objective of this research is to develop an approach that caters to the essential needs of specific manufacturing systems including their interdependencies and the processes involved in the manufacturing of services or products within an industrial organisation. By conducting a comprehensive impact evaluation of a critical manufacturing system to measure the effectiveness of various resilience enhancements implemented in accordance with the Secure PLC Practices (PLC Security, 2021), STPA Framework (Leveson, 2020), IEC – 62443 Framework (International Electrotechnical Commission (IEC), 2021) and the NIST Cyber Resilience Framework (National Institute of Standards and Technology, 2021).

The research employs a case study approach and an experimental physical testbed, informed from the case studies, to gain a comprehensive understanding of the factors that contribute towards obtaining an objective measurement of Cyber Resilience. The case study method was used as it qualitatively provides an organisational context that allows for a detailed examination of the security challenges faced by organisations in securing their industrial systems. Meanwhile, the physical testbed permits the collection of quantitative data of the systems performance under different scenarios, which can help develop more accurate and reliable metrics for Cyber Resilience.

Two industrial manufacturing plants were selected as case study settings, which operate across both Operational Technology and Informational Technology domains. The primary data collection methods used for the case studies were the use of an industrial network probe to gather data logs and visual site inspections to assess the critical system design, supplemented by established frameworks on best practice guidance to enable baseline maturity scoring. Other secondary data sources used for triangulation included documents, interviews, questionnaires, Cyber Security processes and procedures.

To simulate a typical manufacturing system, a testbed using industrial hardware and network communications was designed. The scenario is based on the production of Infant Milk Formula (IMF), which consists of a safety-critical and complex Industrial Control System that utilises both IT and OT domains. The testbed emulates the application of a temperature control system with remote access functionality. The components of the test bed include a PLC Eurotherm 2000, an HMI Station, a Type K Thermocouple temperature sensor and a remote access router known as a EWON. All other components in the test bed are virtualised within a cyber-range. A cyber-attack

was specifically designed to target the weaknesses identified from the case studies undertaken. Finally, the study describes the approach to assessing the Cyber Resilience metric parameters and the tests conducted that relate to the research hypotheses. It is worth noting that the function control block metrics specified in this research can be easily substituted with other control automation functions, such as replacing temperature with pressure, demonstrating the versatility of the model so it can be extended to other industrial use cases.

To select appropriate practices to assess the safety, security and resilience of the model proposed, various frameworks and approaches were combined. First to assess the safety elements of the given system, Leveson's STPA framework and Secure PLC coding practices approach was employed (Leveson, 2020); (PLC Security, 2021). Second, to assess the security elements of the testbed, IEC-62443 and NIST Cyber Security Frameworks was employed (International Society of Automation (ISA), 2020); (National Institute of Standards and Technology, 2018) and finally to assess the resilience elements of the testbed the NIST Cyber Resilience Framework and Linkov, et al Resilience Matrix was employed (National Institute of Standards and Technology, 2021); (Linkov, et al., 2013).

The key resilience enhancements made to the testbed focused on a subset of techniques including secure remote access, segmented networks, monitoring of logs for detection and recovery and inherent safety for reactive responses through secure PLC coding, which encompasses techniques for hardening and measuring resilience (PLC Security, 2021). These enhancements were selected because of the key problem areas identified in the case studies but also due to their broad applicability across various manufacturing systems which enable them to be measured in a general manner.

Modelling the impacts of the system both before and after enhancements are implemented ensures results can be compared. To contextualise the work within this thesis in relation to these enhancements, the methodology put forth (Figure 1-1) aims to assess the impact by modelling the performance of a manufacturing system at various stages of a cyber-attack. For instance, the model outlines the resilience attributes and measures that yield optimal performance for a given system or scenario.

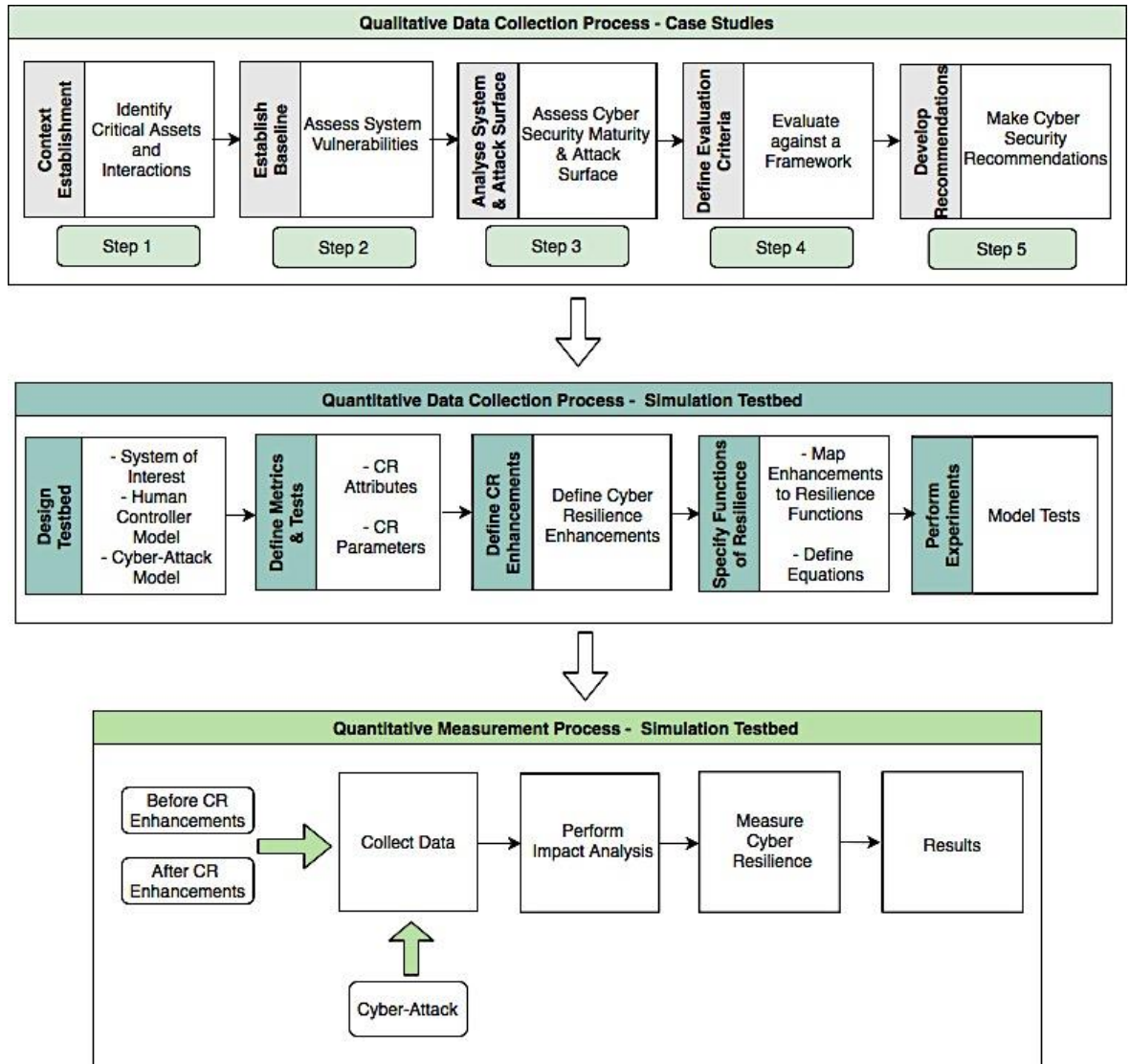


Figure 1-1 Research Approach

It is important to note that the focus of this research concentrates on the measurement of a system’s Cyber Resilience and therefore excludes the overall organisations resilience (although aspects of this were considered in the case studies) and it also excludes disruption events unrelated to cyber-attacks.

The next section discusses the contributions of this research.

## 1.7 Contribution

The field of Cyber Resilience measurement on industrial manufacturing systems is crucial for ensuring the security and safety of critical infrastructure. This PhD thesis makes valuable contributions to this field.

- It provides a detailed evaluation on the characteristics and parameters of Cyber Resilience (presented in Section 3.3).
- It uses case studies to validate qualitative approaches, which themselves are a contribution to knowledge given the sparsity of examples in literature (described in Chapter 5).
- It documents the creation of a physical testbed to perform analysis and obtain quantitative metrics, which others can emulate (presented in Section 6.2).
- It documents the development of an original cyber-attack with a labelled dataset, collected from the industrial manufacturing testbed, which provides an invaluable resource for researchers working in this field (explained in Section 6.2.3).
- It provides a comprehensive evaluation of the factors that contribute to Cyber Resilience in industrial control systems (described in Section 6.3.1).
- It includes a Cyber Resilience milk formula production use case (expressed in Section 6.4).
- It proposes and documents an approach to obtaining a quantitative, objective, Cyber Resilience metric for a critical manufacturing system (described in Section 6.4.1).

Overall, this PhD thesis represents a significant contribution to the field of Cyber Resilience measurement of Industrial Control Systems. It provides an approach to obtain both qualitative and quantitative metrics, demonstrated through several case studies, a physical test bed and provision of an original cyber-attack with labelled dataset, which makes it a valuable resource for researchers and practitioners alike.

## 1.8 Related Publications

The research presented in this thesis has led to the following publications:

### **Papers published in International Journals:**

- Perrett, K., Wilson, I.D. A Cyber Resilience analysis case study of an industrial operational technology environment. *Environmental Systems & Decisions*. Springer. 2023.

### **Papers awaiting submission:**

- Perrett, K., Wilson, I.D. Towards enhancing Cyber Resilience in manufacturing environments. Environmental Systems & Decisions. 2023.

## 1.9 Thesis Roadmap

This section outlines the thesis structure and remaining chapters (see the schematic index shown in Figure 1-2).

**Chapter 2** discusses the background and scope of the problem along with insight into the methodology used to conduct the literature review, which is further discussed in the next chapter.

**Chapter 3** outlines the critical literature review including a range of primary and secondary literature sources. The chapter explains the literature reviewed and the search methods used to undertake the review including the key words and methods used in searching online databases and demonstrating the evaluation of each source for relevance.

**Chapter 4** sets out the research design, research strategies and the data collection methods. The use of multiple research methods is explored with consideration given to the implications each approach would have on the research findings and conclusions. Exploring the issues related to data access and potential ethical issues in relation to each stage of the process. It discusses the range of qualitative and quantitative sampling techniques used in this research; looks at issues of sample size and the choice of techniques selected to assess the representativeness of experts or systems through both case studies and an experimental testbed.

**Chapter 5** presents two case studies, with associated discussion and case study observations comparing the collective data results and finally offering a concluding summary.

**Chapter 6** presents an overview of the simulation and modelling of the physical OT equipment used in this experiment including each component both virtual and physical that aim to replicate the environment of the case study findings (discussed in Chapter 5). It includes the specification of the metrics and tests, the description of resilience enhancements, specification of the mathematical equations and definition of experiments. Finally, it provides a discussion of the results of the experiments undertaken that measure the system's resilience before and after implemented recommendations were applied.

**Chapter 7** discusses the findings of the case study and simulation results, setting out where contributions were made and the hypothesis findings, the limitations of the findings and future work is established.

**Chapter 8** sets out a concluding summary and assessment of the research accomplished in this thesis. It draws on the research aim and objectives that were established in the introductory chapter of this thesis alongside the results shown in individual chapters to justify the conclusions.

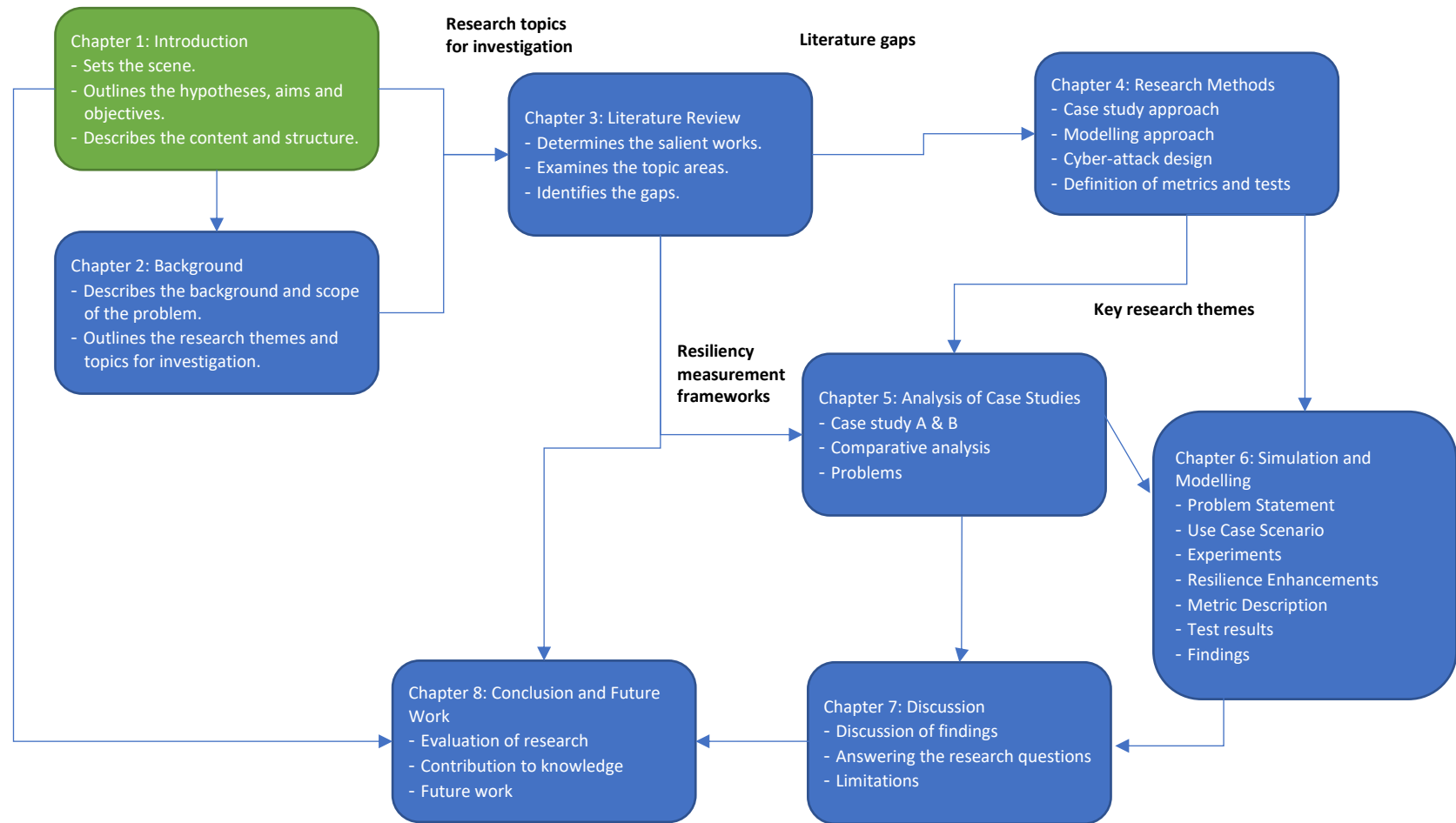


Figure 1-2 Thesis outline



## 1.10 Chapter Summary

This chapter introduced the reader to the subject of Cyber Resilience in Safety-Critical, Complex-Systems by first providing background and context around the topic and context of the different subject areas looked at in this thesis. It discussed the motivation for the project, the aim, questions, objectives and thesis roadmap.

The remaining chapters presents the reader with a background review, followed by a literature review, methodology and project design including primary and secondary research, case studies involving two industrial plants, a description of the simulation environment, tests conducted and a discussion. Finally, future work is considered and a conclusion is offered.

# Chapter 2

## Background

### 2.1 Introduction

The use of automated intelligent systems that control and or manage the physical real world, Operational Technology (OT), collectively working together with Information Technology (IT) enterprise networks are seen as critical enablers to better efficiency (Cherdantsevaa, et al., 2016). These foundations enable operational data to be analysed and provided to a centralised control platform. This convergence between IT/OT systems evolved over the past decade and is still in transit. Further expanding into the realms of complex, interconnected systems. Bridging cross-sector domains, infrastructure technology, physical safety equipment, data, people, processes and society. Whilst this evolution brings many advantages to industry and society in terms of efficiency, the traditional safety-critical cultures of past have been thrown into a world where engineering best practices are now contradicted by lack of basic cyber hygiene controls that we see in today's systems. A Cyber Security incident to such system is inevitable and the impact of a catastrophic safety event arising due to lack of knowledge of the other interconnected systems sharing the same space is, in the authors view, a disaster waiting to happen. New Cyber Resilient approaches have been proposed (discussed in the next chapter) to address the threats that are targeting OT systems with the concerns first acknowledged in 2006 in the EU project IRRIS (IRRIIS, 2006). Organisations must be armed with the information necessary to assess whether the realisation of Cyber Resilience can be effective, necessitating a demand for quantitative metrics, as can be seen in a recent EU funded project, Cyber4Dev (Patriarca, et al., 2022) and the EU Digital Europe Programme to boost Cyber Resilience for critical infrastructure (European Commission, 2022).

To align the context of Cyber Resilience to the purposes of this thesis, the following definition is provided:

“Cyber Resilience is a combination of characteristics that together ensure the secure and safe operation of a critical system(s); including its capacity to anticipate, adapt, maintain or recover from adverse cyber events.”

(Kirsty Perrett, 2023).

The work presented in this thesis focuses on the measurement of Cyber Resilience for a safety critical, complex industrial system as defined by Thales Group. As such, three separate technological themes are considered. First, Safety-Critical Industrial Control Systems, Second, Complex-Systems and Third, Cyber Security and Cyber Resilience. As technological advancements are rapidly underway, it is important to comprehend the historical context and development of each theme, as well as the reasons behind their interconnection and coevolution. The following sections provide a summary introducing each of the three topics before moving onto the literature review.

## 2.2 Safety-Critical Industrial Control Systems

Operational Technology (OT) is the umbrella term used to describe a category of industrial systems that manage, interact with or control the physical environment, defined as:

“The hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices and systems, processes and events in the organisation” (International Society of Automation (ISA), 2020).

More commonly referred to as Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS) or Cyber-Physical Systems (CPS). An Industrial Control System is defined as:

“A general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).” (National Institute of Standards and Technology, 2014)

IACS and CPS terms refers to the integration of physical and computational systems with the aim of achieving specific objectives. IACS is defined as:

“...the collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process.”  
(International Society of Automation (ISA), 2020)

The term ‘control systems’ is employed in this context to avoid the narrow or overly broad application of the CPS label, ensuring it encompasses all systems that involve or utilise both software and hardware to manage physical processes including acknowledging humans as integral components of these systems (Leveson, 2020). Critical National Infrastructures (CNI), which enable us to go about our daily lives, are primarily enabled by these systems and include Manufacturing, Water, Oil and Gas, Transport, Emergency Services and Energy (Biringer, et al., 2013).

### 2.2.1 Background

Here, Operational Technology is classified as a system outside of the IT enterprise. They include a combination of physical, human, network or machine interfaces used to provide control, safety, manufacturing operations or functionality to continuous, batch, discrete and other processes (Cherdantsevaa, et al., 2016). OT environments are often unique to accommodate the complex requirements within each specific industry and include a range of different systems including:

- Basic Process Control Systems
- Process Alarm Management Systems
- Supervisory Control and Data Acquisition (SCADA)
- Distributed control systems (DCS)
- Manufacturing Execution Systems (MES)
- Plant Information Management Systems (PIMS)
- Energy Management System (EMS)
- Monitoring and Diagnostic Systems
- Building Management Systems (BMS)
- Safety Instrumented Systems (SIS)

Each system is comprised from some, or all, of the following components:

- Human and Machine Interface (HMI)
- Programmable Logic Controller (PLC)
- Remote Terminal Unit (RTU)
- Intelligent Electronic Device (IED)
- Sensors

- Actuators
- Graphical Interface
- Advanced Control
- Variable Control
- Online Optimiser
- Equipment Monitor
- Process Historian

These are different from typical IT systems for many reasons (Cherdantsevaa, et al., 2016) since they support complex interconnectivity between physical and logical infrastructure, which often communicates through propriety protocols that rely on computational equipment to convert electronic or analogue signals to digital (Easley & Kleinberg, 2010). For example, a PLC is a set of electrical relays in addition to many other features to enable smart controlling. It is ruggedised to function for 30+ years in industrial environments. A PLC is not a standalone device but rather incorporated as part of a system of other peripheral devices (see Figure 2-1) such as a Human Machine Interface (HMI), which provide engineers and operators with an interface to interact with the control system.

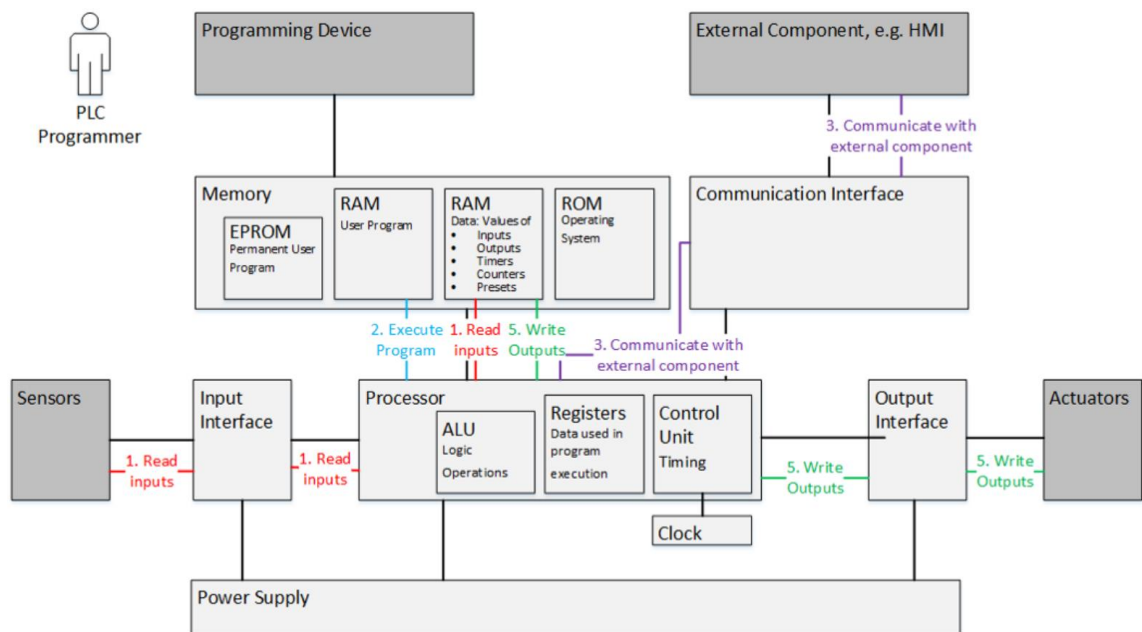


Figure 2-1 PLC (International Society of Automation (ISA), 2020)

A PLC typically uses a technique of programming known as Ladder Logic, which is software structured on electrical signals and based on an old style of relay schematics (International Society of Automation (ISA), 2020). It follows the structure of 'if something is true, then do something else'.

Ladder logic has no parallel functionality - it goes in a sequential order of rungs to execute one thing at a time; hence its name (shown in Figure 2-2).

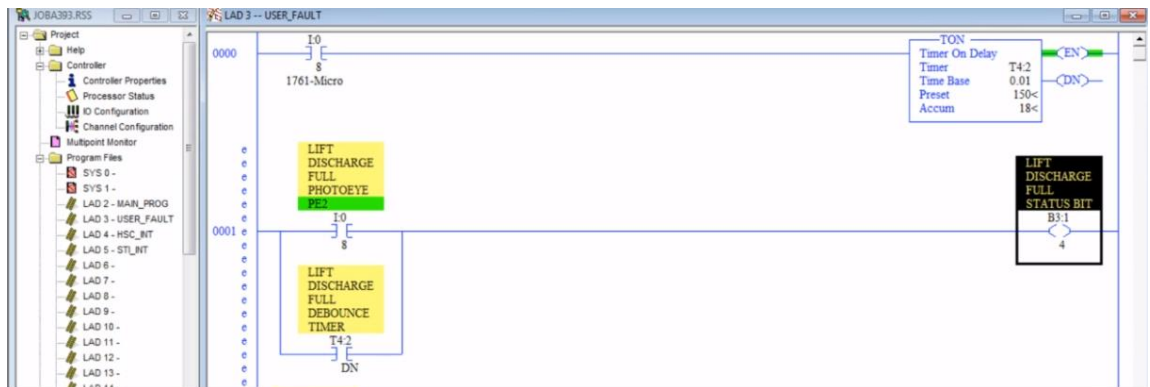


Figure 2-2 PLC Ladder Logic configuration example

There are several frameworks and guidance in literature that discuss the approaches to which these systems should ideally be designed when interconnecting with the IT domains for example, in ISA-95, which is the international standard for the integration of enterprise and control systems (known as IEC/ISO 62264) (Williams, 1992). ISA-95 consists of models and terminology. One example is the Purdue Model which incorporates layers of technology and business practice used by industrial corporations. An example of a Purdue Model is represented in Figure 2-3. The Manufacturing systems all reside in Levels 0-3 of the model, Level 3.5 represents the interconnectivity between the OT and IT layers, referred to as the Demilitarised Zone (DMZ), which separates the IT and OT assets. Level 4 is the corporate IT and finally Level 5 represents unknown assets such as external connectivity to the internet.

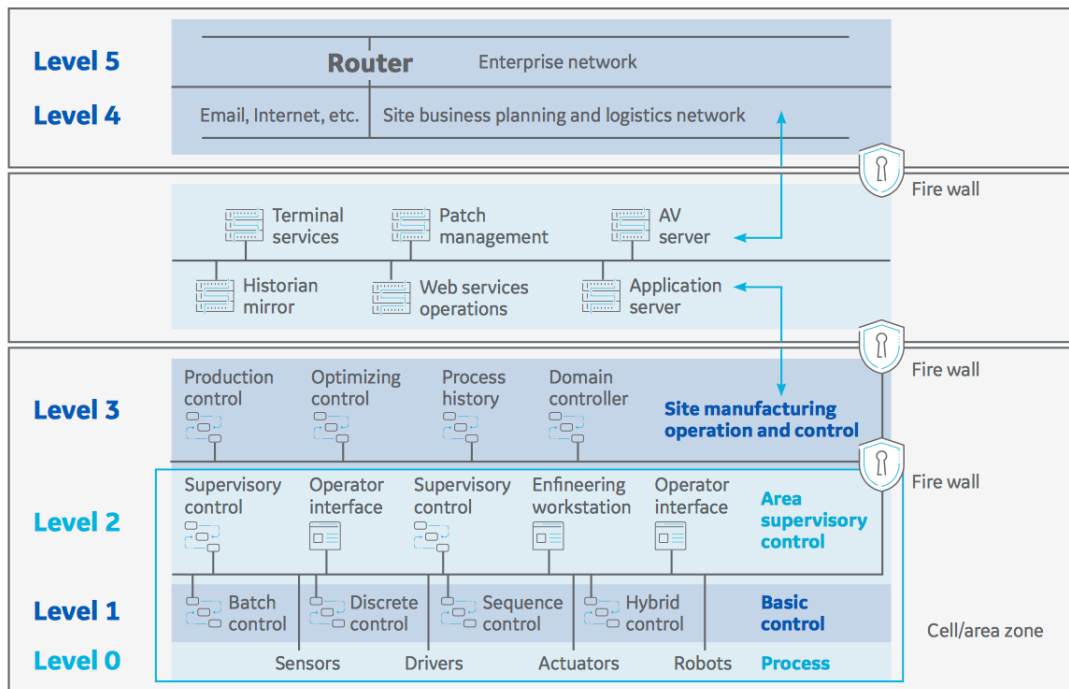


Figure 2-3: An example Purdue model adopted from (General Electrics, 2017)

### 2.2.2 Challenges Securing OT Environments

Industrial environments are increasingly targeted by cyber attackers as their integration into the IT environment grows. As touched on in the previous sections, OT systems were built to function for many years with little error due to a safety culture guaranteeing that systems degrade gracefully, fail in a safe manner and have little to no downtime (General Electrics, 2017). However, the challenge is that these systems were not designed with security as a priority consequently meaning that the conventional risk assessment approach that we see in IT systems has proven to be unmanageable in OT environments (Linkov, et al., 2013), (Groenendal & Helsloot, 2021) and there is a growing threat to the security of safety-critical systems (Johnson, 2016).

Unlike in IT environments, where a successful hack can result in loss of data or reputational damage the stakes are higher in OT since the environment, public safety and physical real-world systems are affected (Leandros & Maglaras, 2018). Organisations responsible for critical infrastructure need to have a consistent and evolving approach to identifying, assessing and managing safety and cyber-security risk. This approach is necessary regardless of an organisation's size, threat exposure or cyber-security sophistication today (National Institute of Standards and Technology, 2018).

Efforts to improve safety systems, including accident analysis, risk assessment, safety culture promotion and human-centred design, are discussed in literature (Hollnagel, et al., 2014); (Leveson,

2009); (Leveson, 2017); (Rasmussen, 1997). However, the different approaches offer opposing views (Leveson, 2020). The safety of something can only be rigorously evaluated by considering the specific context in which it operates (Ford, et al., 2012). Furthermore, the similarities between safety & security standards have led to IT security policies that cannot easily execute in a safety-critical system. Whilst regulators and engineers understand the fundamental safety requirements of such systems (Maglaras, et al., 2018), i.e., Safety Integrity Levels (SIL) and best practice, security requirements simply do not translate well, which increases the risk of an unexpected event or compromise.

It is important to note that Industrial Control Systems (ICS) may already possess certain forms of resilience mechanisms that were initially incorporated into their design for safety reasons unrelated to security (Ford, et al., 2012). For instance, consider the case of a fuse within an electronic circuit, which is intended to interrupt power supply to a system when the temperature exceeds a certain limit. This is an example of inherent resilience which refers to the built-in mechanisms or features in the design of a system that allow it to withstand and recover from cyber-attacks or other forms of disruptions without relying solely on external defences. In the case of the electronic circuit example, the fuse acts as an inherent resilience mechanism by cutting off power to prevent damage to the system and reduce the risk of harm to humans. Inherent resilience is important because it reduces the reliance on reactive measures, such as incident response plans and backup systems, which may not always be effective or reliable. It also enables ICS systems to continue functioning during and after an attack or disruption, minimising the impact on critical infrastructure and essential services. However, inherent resilience can also cause negative effects to the system if the attackers' incentive is to cause the system to halt or in the case of the fuse, shut off for a safety measure.

Manufacturers are increasingly turning to Cyber Resilience strategies as they seek to strengthen their complex systems. A review of the literature relevant to Cyber Resilience in OT environments and analysis into the current gaps in research is discussed further in Chapter 3.

The next sections explore safety-critical systems.



## 2.2.3 Safety-Critical Systems

This section will explore the history and application of safety systems, the current challenges and the relationship between security, safety and resilience.

### 2.2.3.1 History of Health and Safety

Over the past two centuries, industry has undergone three significant technological transformations and a fourth transition is currently underway. A timeline showing the Industrial movements can be seen in Figure 2-4. The United Kingdom was the first nation to industrialise in the late 1700s, marking the beginning of the first Industrial Revolution. This period witnessed the shift from rural agricultural practices to the use of steam power and mechanical machinery. The introduction of electricity, mass production and improved communication characterised the second shift in the mid-1800s. Steam-powered locomotives revolutionised production and travel during this time. By 1831, according to Census (Census-Records, 1831), close to 3 million UK people worked and or lived within a manufacturing industry town. The Factory Act of 1844, which mandated the enclosure of dangerous machinery, served as a foundation for the protection of workers' safety and public health. It led to investigations into industrial pollution and its impact on public health (Banerjee Ruths, 2009). The discoveries made by John Snow, a London physician, regarding the spread of disease through contaminated water, further influenced government regulations on industrial pollution.

## THE FOUR INDUSTRIAL REVOLUTIONS

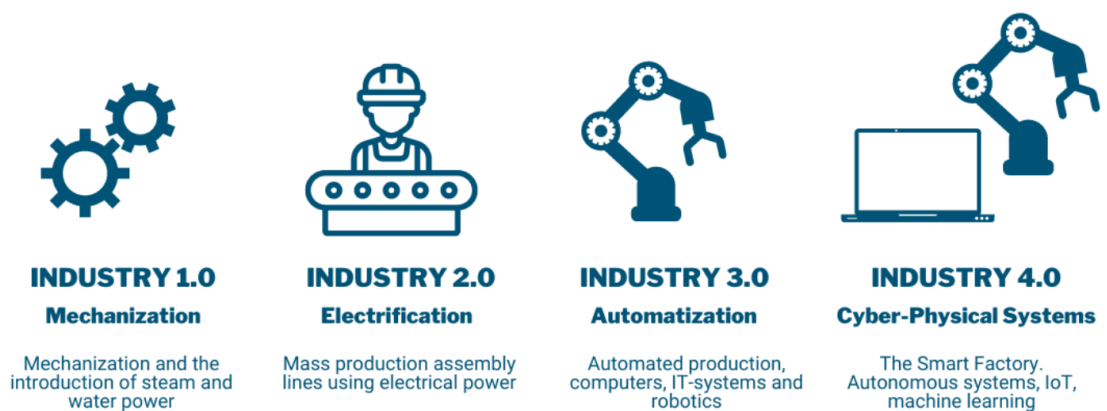


Figure 2-4 The four industrial revolutions – adopted from (Meloeny, 2022)

The third Industrial Revolution occurred in the early 1900s, marked by advancements in computers, automation, robots and the internet. Throughout these technological advancements, there have been continuous improvements in safety laws and standards (Eves, 2014). However, although legislation aims to mitigate undesirable events by reducing the number of potential negative outcomes, it is important to recognise that complete security, safety or resilience cannot be guaranteed. There will always be residual risk or an acceptable level of risk that remains (Donnelly, et al., 2022). Differentiating between risk and uncertainty, risk assessments consider all outcomes and assign probabilities, whereas uncertainty acknowledges that it is impossible to know all potential outcomes in advance (Scoblic, 2020). This concept is also reflected in reliability assessments of calculation models for Safety Instrumented Systems (SIS), which address three key areas of logical assessment: Model Uncertainty, Data Uncertainty and Completeness Uncertainty (Janbu, 2009).

It is particularly difficult to articulate what counts as safe enough for a secure complex-system and who decides. A resilient safety system is best described as:

“Resilience requires a constant sense of unease that prevents complacency. It requires knowledge of; what has happened, what happens and what will happen, as well as what to do. It must be aware of the impact of actions as well as the failure to take action. A resilient system must be proactive, flexible, adaptive and prepared.” (Hollnagel, et al., 2006)

According to (Hollnagel, 2015), safety management can be categorised into two groups known as Safety-I and Safety-II, which are now referred to as Functional Safety and Physical Safety [Donnelly, 2022]. The Functional Resonance Analysis Method (FRAM) was developed to model complex socio-technical systems based on functional resonance, capturing performance variability and its propagation (Hollnagel, 2015). While FRAM is primarily a system modelling method, it can also be used for accident investigation and risk assessment within the framework of Safety-II. However, (Leveson, 2020) disagrees with Hollnagel's characterisation of Safety-I and argues that the concept of Safety-I and Safety-II is flawed, not aligning with current safety engineering practices nor the historical development of the field. Leveson proposes a systems approach called "Safety-III" as a way forward for the future.

(Volos, et al., 2017) conducted a study on the effects of different cyber-attack scenarios on the safety and security of OT processes. They found that OT environments can be more securely integrated with IT systems using distributed cryptographic techniques. However, adding complexity to system security becomes challenging when the primary objective of safety systems is availability.

### 2.2.3.2 Functional and Physical Safety

Functional Safety refers to the term used to describe safety in different industries, systems or products (Donnelly, et al., 2022). While industry-specific standards exist, IEC 61508 serves as the overarching standard applicable to all industries. Industry-specific standards have been developed based on IEC 61508 as a baseline, tailoring them to their respective sectors. This approach of adapting similar but different standards could be a solution when considering the approach to Cyber Resilience frameworks.



Figure 2-5 Industry Specific Safety Standards. Image adopted from (TUVSUD, 2022)

EN 954-1, published in 1996, served as the functional safety standard for control systems in the field of machine building and end-user applications for about fifteen years. However, with the rapid advancement of technology, this standard became inadequate to address the evolving systems and components. In 2007, EN 954-1 was replaced by two new standards: EN ISO 13849-1 and IEC 62061, specifically developed to accommodate these technological changes (see Figure 2-5).

EN ISO 13849-1 focuses on the safety of various system technologies, including mechanical, hydraulic and pneumatic products. It is applicable when safety functions are performed by safety-

related parts of the control system (SRP/CS). Compliance with the Essential Health and Safety Requirements (EHSRs) of the Machinery Directive 2006/42/EC can be demonstrated through adherence to EN ISO 13849-1.

IEC 62061, on the other hand, is a generic functional safety standard that considers the entire lifecycle of electrical, electronic or programmable electronic (E/E/PE) systems and products as shown in Figure 2-6. It is a machinery-specific implementation of IEC/EN 61508. Compliance with the EHSRs of the Machinery Directive 2006/42/EC can be established by following the guidelines outlined in IEC 62061.

<b>IEC 62601</b>				
Machinery sector hardware			Machinery sector software and application software	
In scope	Not in scope	In scope	In scope	Not in scope
Design of low complexity subsystems	Design of complex subsystems	Integration of subsystem into a safety related control system	Using hardware predesigned according to IEC 61508 or other functional safety standards	Design of complex subsystems

*Figure 2-6 the scope of IEC 62601 adopted from (TUVSUD, 2022)*

These updated standards provide improved methodologies and approaches to address the safety requirements of modern systems and equipment in different industries, ensuring compliance with relevant directives and regulations however security guidance is still lacking in these approaches.

Another important component related to functional safety is the use of software tools. When developing software for safety systems, the use of appropriate tools becomes crucial (Donnelly, et al., 2022). However, these software tools need to meet specific criteria and comply with predefined requirements in functional safety development projects. The qualification of software tools is a topic of concern for industry stakeholders. In certification projects, the selection of the right tool can be a risk and uncertainty, as such, can lead to lengthy discussions and costly delays during project lifecycles. Tool certification is particularly relevant in safety-related environments such as automotive, automation, railway, medical or nuclear sectors.

Lastly, Safety Integrity Levels (SILs) play a significant role in functional safety standards. SILs are well-defined in these standards; however, the integrity of SIL levels can vary between industry-specific standards (TUVSUD, 2022). For example, EN 17206 focuses primarily on manufacturing equipment and may not translate well to other industries, leading to differences in risk assessments.

Moving onto the topic of Physical Safety, which is another important aspect, as it encompasses various considerations related to ensuring the physical safety of individuals, systems and the environment (Leveson, 2020). Learning from engineering failures of the past is essential, as they can provide insights into potential failures in present-day systems (Donnelly, et al., 2022). The classification of past failures may not seem applicable to current systems; however, these lessons still serve as a validation mechanism to verify requirements that inform the system engineering process, including safety, resilience, redundancy and fault-finding efforts. Examining past engineering disasters can offer valuable lessons to address future risks and improve Cyber Security and Resilience practices.

The next section takes a brief look at some examples of past engineering disasters that may provide insight into the system engineering design process to address future risk.

#### 2.2.3.3 Safety-Critical Engineering Disasters of past

NASA's \$125-million Mars Climate Orbiter was unfortunately lost due to a crucial oversight by spacecraft engineers who neglected to convert essential data from English to metric measurements prior to the launch (Hotz, 1999). Lockheed Martin, the main contractor for the Mars orbiter, used English metrics for the satellite's thrusters. JPL used SI units for the model of the thrusters. The units of measurements were not explicitly set out in the requirements development design. This was a fundamental error. However, mistakes can and do happen, which is why there is a need for verification and validation of the requirements. Fundamental errors should be highlighted during these checks, which may then highlight the mismatch between the model and satellite system.

Another example is the northeast electric power blackout in August 2003 and more recent failures including cyber-attacks to critical systems such as the Ukrainian grid blackout and more recent colonial pipeline attacked in the US (Reeder & Hall, 2021).

The next section will provide an overview of complex systems.

## 2.3 Complex Systems

Complexity is described as the state of intellectual challenges that surpass our capacity to handle (Leveson, 2020). Complex systems can be found in a wide range of fields, including physics, biology, economics and social systems and has been defined as:

“A system with numerous components and interconnections, interactions or interdependence that are difficult to describe, understand, predict, manage, design and/or change.” (Magee & De Weck, 2004)

In the computer science domain, complex systems are often referred to as "systems of systems" and can encompass physical, digital and hybrid realms. These systems, which may involve intercontinental communication and regulation (Theron, 2013), are diverse in terms of industry sector, supply chain or engineering discipline. Each system within this complex network, including its human components, has its own unique perspective on best practices and standards, contributing to the overall complexity through the number of links within the system.

A complex system is characterised by the presence of numerous interacting components that exhibit emergence (Gates & Bremicker, 2017). Complex systems share some common characteristics (provided in Table 2-1). The study of complex systems is challenging but they are powerful tools for understanding and modelling a wide range of natural and artificial phenomena. The notion of ‘emergence’ refers to phenomena that occur at a system-level that are not present at the component-based level in the system. Since a system is expected to comprise a certain level of emergent behaviours, while at the same time avoiding other evolving properties, a richer insight into emergent properties is essential (Axelsson, 2022). It has also been identified as one of the key aspects of systems-of-systems. However, the concept has been the topic of much debate in both philosophy, systems science and complexity science for a long time. Yet, there is no precise characterisation on which there is general agreement.

Table 2-1 Characteristics of complex systems

Characteristic	Description
Non-linearity	The behaviour of a system is not directly proportional to the inputs making it difficult to predict its behaviour.
Emergence	Complex systems exhibit properties that cannot be explained by the properties of the individual components but instead arise from the interactions between them (Axelsson, 2022).
Feedback loops	Complex systems often have feedback loops where the output of the system affects its own behaviour.
Adaptability	Complex systems can adapt and change over time often in response to external influences (Hollnagel, et al., 2006).
Hierarchical structure	Complex systems often have a hierarchical structure with various levels of organisation and interactions between them.
Interdependence	Complex systems are often made up of many interdependent parts where the failure of one component can affect the entire system.
Self-organisation	Complex systems often self-organise meaning that the system's structure and behaviour emerges spontaneously from the interactions of the components (Heeks & Ospina, 2018).
Robustness and fragility	Complex systems can be both robust and fragile meaning they can withstand small disturbances but can fail catastrophically under certain conditions (Heeks & Ospina, 2018); (Kott & Abdelzaher, 2014).

The degree of a systems complexity depends on its number of components, their interconnections and the extent of information needed to describe the given system (Kott & Abdelzaher, 2014); (Magee & De Weck, 2004).

Table 2-2 explains the degree of complexity, adopted from (Magee & De Weck, 2004).

Table 2-2 Systems classified by degree of complexity: adopted from (Magee & de Weck, 2004)

Level of Complexity	Technical System	Characteristics	Examples
I (simplest)	Part, Component	Elementary system produced without assembly operations	Bolt, bearing sleeve, spring, washer
II	Group, mechanism, Sub-assembly	Simple system that can fulfil some higher functions.	Gear box, hydraulic drive, spindle head, brake unit, shaft coupling.
III	Machine, Apparatus, Device	System that consists of sub-assemblies and parts that perform a closed function.	Lathe, motor vehicle, electric motor.
IV	Plant, Equipment, Complex machine unit	A complicated system that fulfils several functions and that consists of machines, groups and parts that constitute a functional and spatial unity.	Hardening plant, machining transfer line, factory equipment.

A snapshot of a complex system at a given time only serves to capture the systems variables' state at that time (Janbu, 2009). These variables or types can evolve, such as in computer programming. The difference between variables and types is clear. Variables can be of distinct types. Variables are first declared but then assigned different values that fit their type during execution and as such, can change while the program is running. The variables containing the values live within the program for a brief period when the program runs (Ma'ayan, 2017). Similarly, cells have DNA that serve as a template to produce instances of RNA and protein molecules. Such analogies can help with considering the distinction between an instance and a type or a template of a complex system or a variable within a complex system.

The next section discusses the application of complex systems.



### 2.3.1 Application of Complex Systems

Complex systems theory has found application in various computer science-related fields. In relation to Cyber Resilience, numerous papers in literature discuss the application of complex systems theory. One area of study is network systems, such as the internet, social networks and transportation networks. The theory has been used to analyse the topology, dynamics and resilience of these networks (Easley & Kleinberg, 2010). Observing that the internet's structure follows a power-law distribution, a hallmark of complex systems. Artificial intelligence and machine learning have also been explored using complex systems theory, whereby researchers have investigated the behaviour of artificial neural networks and other machine learning algorithms, revealing non-linear dynamics reminiscent of complex systems. For example, (Xu, et al., 2023) present a physics-informed machine learning approach to building and maintaining Cyber Resilient systems for reliability and systems safety applications. Furthermore, it has been applied to distributed systems (Coulouris, et al., 2021), providing insights into the dynamics, scalability, fault-tolerance and emergence of collective behaviour in these systems.

This insight and understanding led to the development of new methods for modelling, analysis and control. However, accurately measuring the level of Cyber Resilience in industrial systems is a complex task. It requires in-depth knowledge of the interconnected activities within and surrounding a system, encompassing the design, implementation and maintenance of technological infrastructure, systems engineering, formal procedures and organisational culture (Kott & Abdelzaher, 2014). According to (Gates & Bremicker, 2017) there will be an increasing requirement for collective governance and norms to ensure Cyber Resilience in the future.

The next section provides a general overview of Resilience then leads on to Cyber Security and Cyber Resilience.

The review of Cyber Resilience begins with a discussion of its background and definitions. CR is a dynamic process that references both cyber risk and system performance (Dupont, 2019); (Gates & Bremicker, 2017) while covering a variety of different factors, such as technical architecture, processes and systems, human factors and business objectives (Theron, 2013). CR is also discussed in relation to other Cyber Security measures, such as prevention and detection, as well as the ability of a system to recover after an attack (Mitre Corp., 2012). Thus, Cyber Resilience is not the only definition that is important for this thesis. The thesis tackles measurement of CR and to do so, the definition and understanding of its relationship and history to other terms is also important. Poor definitions will have unhelpful nuance and ambiguity in later discussion. To continue, it is important

to decide upon definitions that are appropriate for this thesis, aligning with its context. Where possible, definitions have been taken from accepted standards. Where not possible, due to variation in literature and lack of consensus on definition (Smith, 2023), this thesis sets a definition that is in the context of the research and is described in the next sections.

## 2.4 Resilience

This section will provide the history and concepts of resilience in general, including its multiple definitions and application in other domains.

### 2.4.1 History of Resilience

Resilience has its roots in many disciplines. From Materials Engineering to Psychology (Seligman & Csikszentmihalyi, 2000), Ecology (Yi & Jackson, 2021), Urban Planning (Tasan-Kok, et al., 2013) and Engineering (Ross, et al., 2018) to name a few. All of which share a common set of principles that overlap domains including preparation, mitigation and adaptation.

Use of the term dates to as early as the 15th century (Goss, 2009) in the book by Johannes Amos Comenius (1592–1670). Also given in the Oxford English Dictionary stating that the word may have been based on its late Latin origins (Oxford English Dictionary, 2013):

“...sight is the resiliencie [Latin: resiliencia] of the light from the object to the eye.”

Here we see the metaphorical sense of the word ‘bounciness’ which stems from the word ‘resilire’, the Latin word for “bounce” and nowadays referred to as ‘reflection’ (Manyena, 2006). In 1960, an elastic protein was named ‘resilin’ (Wordsworth, 2014). These ‘natural elasticity’ characteristics began the resilience paradigm with its concept first applied to physics in the material sciences domain and later adopted in the medical and veterinary sciences, nowadays referred to as System or Engineered Resilience whereby resilience was used to define the elasticity of biological tissues. In this context, resilience refers to a limited set of measurable parameters specified by the material's predictability to maintain a state of equilibrium (Smith, 2023). The term's popularity broadened in the 1970s to the fields of Ecology and Psychology and nowadays the disciplines are collectively referred to as ‘Ecological Resilience’.

The founder of Ecological resilience, C.S Holling (a Canadian ecologist) (Holling, 1973), introduced this new concept of resilience in 1973, applicable to a system when confronted by unexpected changes, in that it could not maintain a constant state of equilibrium unlike in Engineered resilience.

Holling argued instead that the study of resilience should focus on the perseverance of systems and their capability to absorb change and disruption. He explained the System Resilience concept as a:

“Shift of perspective does not require a precise capacity to predict the future, but only a qualitative capacity to devise systems that can absorb and accommodate future events in whatever unexpected form they may take.”  
(Holling, 1973)

In a later article (Holling, 1996), Holling elaborated on his thinking, stipulating the distinctive features between *Ecological Resilience* and *Engineered Resilience*. Consequently, these two overarching fields of resilience study remain consistent even today. Although there is limited research on whether Engineering or Ecological resilience dominates in the context of Cyber Resilience, nonetheless, each approach leads to different strategic decisions and there are therefore inevitably “subtle differences that need to be explored to avoid excessive simplification, loss of meaning and misinterpretation (Holling, 1996).

The next section explores the two overarching directions of resilience study.

#### 2.4.2 Ecological vs. Engineering Resilience

This section discusses two directions of resilience: system/engineering resilience and ecological resilience. Both approaches are used to handle unstable situations. The two approaches are based on the idea of equilibrium, which refers to a balanced state (see Table 3-1). The original application of Engineering Resilience is typically associated with a single steady state, while the more recent application of Ecological Resilience can have multiple states (Holling, 1996).

With respect to Cyber Resilience, Engineering Resilience focuses on fast recovery to the original state after cyber incidents, while Ecological Resilience emphasises adapting to change with less emphasis on fast recovery. Understanding an organisation's approach during a cyber-crisis is crucial for developing appropriate Cyber Resilience metrics. The study by (Bagheri & Ridley, 2017) aims to identify the preferred type of resilience thinking in the domain of Organisational Cyber Resilience, the authors explore these two resilience approaches (see Table 3-1) and concludes that Organisational Resilience typically falls in the category of Engineering Resilience.

Table 2-3 presents the differences between each approach (adopted from (Bagheri & Ridley, 2017).

*Table 2-3 Differences between engineering and ecological resilience (Bagheri & Ridley, 2017)*

Engineering Resilience	Ecological Resilience
------------------------	-----------------------

Single steady state	Multiple states
Returns to a previous state	Appears in different states
Focus on level of disturbance	Focus on absorbing the change
Physical aspects of a system	Dynamic features if a system
Functionality based on original shape	Functionality based on multiple shapes
Fast recovery time	Less attention paid to fast recovery
Optimises operational procedures	Focus on adaptation and adjustment

In the Engineering Resilience domains, resilience is focused on efficiency, constancy and predictability. Whereas Ecological Resilience focuses on unpredictability, change and persistence (Holling, 1996). Etymologically resilience is connected to 'going back'. Nowadays, the characteristics of 'not going back' is equated with determination or persistence, which is the opposite of steadiness. However, it is important to remember that this perspective is grounded in Ecology. The practical implication of this line of reasoning is that efficiency and resilience are not always aligned (Holling, 1996). This contribution is essential for decision-makers today to understand that achieving resilience requires an understanding of each domain and a balance of sometimes often conflicting priorities (Dupont, 2019).

Despite the contrasting views in literature, Sikula et al. (2015), propose that the optimal resilience approach is to combine both perspectives. By integrating Engineering and Ecological resilience, an organisation can assess the overall resilience of a complex system, considering both the speed of recovery and the ability to adapt to change (Sikula, et al., 2015).

The next sections will discuss the various resilience definitions and scope of meanings.

### 2.4.3 Resilience Definitions and Concepts

The previous section identified the two primary fields of Resilience Study defined in 1973 namely, Ecological Resilience and Engineered Resilience. Jump forward some decades and already the "loss of meaning, misinterpretation and excessive simplification" surrounding the Resilience approaches, that Holling cautioned against (Holling, 1996), has unfolded. The next sections will demonstrate the multiple definitions of resilience, both in general terms and applied to disciplines.

#### 2.4.3.1 Resilience Definitions in General

The misunderstanding of the meaning of resilience and its generalised definitions creates confusion and frustration in literature (Smith, 2023); (Linkov, et al., 2013); (Bagheri & Ridley, 2017); (Davidson, et al., 2016). For example, according to the Oxford English Dictionary (Oxford English Dictionary, 2013), resilience is “the act of rebounding or springing back”. This definition refers to the Engineered Resilience and materials which return to their original shape after distortion. Resilience is also defined by the Oxford dictionary as “the capacity to recover quickly from difficulties”.

Similar findings are given in the Cambridge Dictionary (Cambridge Dictionary, 2023), whereby three definitions of the term are given and vary depending on the domain in which the definition applies as follows: “the ability to be happy, successful, etc. again after something difficult or bad has happened”, this definition refers to Psychology grounded in the Ecological Resilience approach and the remainder of definitions refer to the Engineering Resilience approach as follows: “the ability of a substance to return to its usual shape after being bent, stretched, or pressed” and “the quality of being able to return quickly to a previous good condition after problems”. The general perception or most accepted definition nowadays typically depicts the following:

“Resilience is the ability to maintain capability in the face of a disruption.” (Brtis & McEvilley, 2019)

Further context around the specific definitions of Resilience, is provided in the next sections.

#### 2.4.3.2 System or Engineering Resilience

System Resilience typically incorporates the Economic, Physics, Engineered and Cyber Resilience domains as part of its remit. System Resilience practices refer to ‘resilience’ as a characteristic of a system’s performance (Hollnagel, 2015). System resilience is the result of a combination of influencing factors both internal and/or external to the system under consideration and typically impacted by the day-to-day decision-makers or the ecosystem influences (Hollnagel, et al., 2006). Each factor can impact the overall resilience either positively or negatively and at times counteract the other factors (Linkov & Kott, 2018), (Jackson & Ferris, 2016). Hollnagel, in his pioneering research discovered that ‘resilience’ refers to something that is rather than what something has. To realise the true meaning of resilience with respect to a system, one should first understand the term ‘ability’ and the scope of means in which resilience definitions are based. He stated that resilience is an outcome of functions and systems and not a feature or quality. In other words, ‘Resilience’ refers to what the system does rather than the qualities of a system itself (Hollnagel,

2015). This means that a system can function in a resilient manner when it performs its intended outcome in both expected and unexpected adverse conditions. Then, a system's function is also a system's purpose. Westrum's paper on regular, irregular and unexampled threats discusses being prepared for something that has not yet happened but has the potential to happen (Westrum, 2006); if the system changes, even slightly, during its lifecycle then it is necessary to anticipate changes (Hollnagel, 2015). For engineered systems, System Resilience is:

“...the ability of an engineered system (or System of Systems) to provide required capability when facing adversity.” (INCOSE Resilient Systems Working Group, 2020).

The definition of Cyber Resilience, for the purposes of this thesis, aligns with the preceding description and is:

**“Cyber Resilience is a combination of characteristics that together ensure the secure and safe operation of a critical system(s); including its capacity to anticipate, adapt, maintain or recover from adverse cyber events.” (Kirsty Perrett, 2023).**

This working definition aligns with the scope of this thesis. A Cyber Resilient system (or System of Systems) should incorporate a series of characteristics that include proactive measures to protect against cyber threats, robust strategies to adapt even in the face of cyber-attacks or disruptions and the capacity to maintain or recover production and safety functions. Cyber resilience in manufacturing should therefore integrate cyber security practices with safety engineering and operational processes, emphasising the preservation of physical safety, data integrity and the proper functioning of machinery and systems, ultimately bolstering the industry's ability to navigate the evolving threat landscape while maintaining its core operational objectives.

More recent definitions of Engineered Resilience appear in literature. For example, a system is resilient:

“...to the degree to which it rapidly and effectively protects its critical capabilities from harm caused by adverse events and conditions.” (Firesmith, 2022)

The authors highlight certain ambiguities with the earlier definitions, testifying that system resilience is not an isolated attribute but instead directly interconnected with other quality attributes including, for example: Robustness, Safety, Capacity and Cyber-Security. Emphasising that the scope in which System Resilience is concerned is to ensure continuity of operations following an adverse event and not prior too. Therefore, the 'prevention' term, to detect and respond, that is frequently associated with the term system resilience, is consequently outside of

its scope. However, it is important to note that whilst this is true, the 'prevention' aspect, is indirectly connected with resilience since it forms part of the other attributes that are directly associated such as Safety and Security for example.

#### 2.4.3.3 Infrastructure and Safety Resilience

Infrastructure and Safety Resilience also forms part of the Engineering Resilience domain. The US Department of Homeland Security defines Infrastructure Resilience as:

"Ability of systems, infrastructures, government, business and citizenry to adapt to changing conditions and withstand and rapidly recover from disruption."  
(Department of Homeland Security, 2018)

The late Jens Rasmussen is an influential figure in the Safety Resilience and engineering community. Rasmussen introduced the dynamic safety model in 1997 (Rasmussen, 1997) advocating a cross-disciplinary systems-based approach to thinking about infrastructure resilience and accident causation. This area of research listed in 2005 as one of the most difficult research topics to address in national security (Fisher & Norman, 2010). Building on Rasmussen's work, Nancy Leveson writes about this issue in detail; Leveson developed a framework STAMP (Leveson, 2011) and later built on this to form the STPA framework, which addresses the weaknesses in a safety critical system. Later analysis into the metrics of infrastructure resilience directed towards natural disasters were conducted by (Biringer, et al., 2013). Cyber-specific resilience metrics is an emerging field. However, academia has built many concepts from Leveson's work and further frameworks such as STPA-sec (Friedburg, et al., 2017) and Safety III (Leveson, 2020) has surfaced as a direct result.

#### 2.4.3.4 Cyber Resilience

Much like in the other resilience domains, the definition of Cyber Resilience also differs across domain. CR refers to the ability of the system to prepare, absorb, recover and adapt to adverse effects; especially those associated with cyber-attacks. (Linkov & Kott, 2018). NIST defines it as:

"The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." (National Institute of Standards and Technology, 2021)

There are copious potential definitions for the term Cyber Resilience. These vary depending on context (Smith, 2023). For example, the European Central Bank defines Cyber Resilience as:

“Cyber Resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack.” (European Central Bank, 2021)

A slightly different perspective by the UK Government is given:

“...the ability for organisations to prepare for, respond to and recover from cyber-attacks and security breaches.” (GOV.UK, 2020)

Much like the term ‘resilience’, the term ‘Cyber Resilience’ and its expression can be seen everywhere of late. Despite no universal consensus on the definition (Smith, 2023), we still see a common holistic theme of which they all share common terms such as the ability to prepare for and adapt to changing conditions and to rapidly withstand and recover from cyber disruptions (Goldbeck, et al., 2019). Cyber Resilience is often confused with other similar but different concepts such as redundancy, risk and security and not treated collectively as one (Jacobs, et al., 2018). It is therefore essential to distinguish the attributes, concepts and related terms that are directly associated to CR, as such, the concepts and related qualities are consequently examined in the following sections.

#### 2.4.3.5 Resilience Concepts

As discussed in Chapter 2, countless concepts of resilience can be identified in literature spanning many disciplines, albeit in an inconsistent manner. There is wild variation in perceptions, which is the case across domains but is also the case even within the cyber domain. The characteristics that influence resilience in a safety-critical complex system, as described in (National Institute of Standards and Technology, 2018), include three classical concepts, namely: avoiding, withstanding and recovering from adversity (Brtis & McEvilley, 2019). Table 3-2 presents various concepts that influence resilience.



Table 2-4 Resilience concepts

<b>Q1. Against what is resilient?</b>	Citations with Emphasis on 'Change'	Emphasis on 'Disturbance' or 'Adverse Effects'	Emphasis on 'Major Disruption'	Emphasis on 'Shock'
	(Holling, 1973); (Hollnagel, 2015)	(Walker, et al., 2004) ; (Linkov & Kott, 2018)	(Haimes, 2009)	(Bruneau, et al., 2003); (Manyena, 2006)
<b>Q2. How is it resilient?</b>	Emphasis on 'Adapt'	Emphasis on 'Withstand'	Emphasis on 'Prepare', 'Plan' & 'Respond'	Emphasis on 'Absorb'
	(Manyena, 2006); (National Institute of Standards and Technology, 2021) (Linkov & Kott, 2018); (Jackson & Ferris, 2016)	(Haimes, 2009); (National Institute of Standards and Technology, 2018) ; (Brtis & McEvilley, 2019)	(Hollnagel, et al., 2011); (National Institute of Standards and Technology, 2021)	(Holling, 1973); (National Institute of Standards and Technology, 2018); (National Institute of Standards and Technology, 2021); (Kott & Linkov, 2019)
<b>Q3. What is the outcome of resilience?</b>	Emphasis on 'Survive'	Emphasis on 'Maintain'	Emphasis on 'Recover'	Emphasis on 'Emerge'
	(Manyena, 2006)	(Walker, et al., 2004); (Chang, et al., 2015)	(National Institute of Standards and Technology, 2021); (Linkov & Kott, 2018); (Brtis & McEvilley, 2019)	(Jackson & Ferris, 2016)

The next section discusses Cyber Security and Cyber Resilience in further detail.

## 2.5 Cyber Security and Cyber Resilience

It is critical to the normal running of manufacturing operations that OT systems inevitably need to interconnect with IT systems to increase productivity, profitability and efficiency and lower costs and downtime. However, OT systems are exposed to many threats and potential attacks of different nature. Whilst some industries have a good understanding of their assets and configuration associated with their OT environment and can appreciate the need for OT and IT security, many other industries have limited knowledge of their associated OT estate and its criticality to their operations, leaving room for cyber threats.

Cyber threats can be internal, external, accidental or intentional (see Figure 2-7). Dragos found that OT utility networks are significantly more vulnerable to an attack than the IT utility networks (Dragos, 2022); breaches also have a more destructive impact on operations.

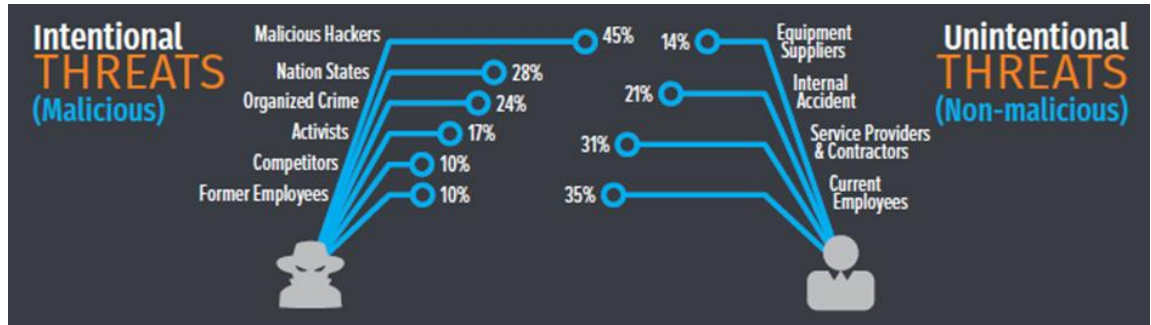


Figure 2-7 State of OT/ICS Cyber Security Survey – adopted from (Assante & Lee, 2015)

Although there are numerous ways to attack an OT System environment, (Assante & Lee, 2015) suggests the most common methods fall into three categories: loss, denial and manipulation. Another way to look at the threat actors is a method in which the UK Governments DCMS review followed in 2020. NCSC (2020), led a security strand and created a set of attack trees for Telecoms networks in the UK and produced four classes of attack categories namely: espionage, disruption, pre-positioning and national dependence. Using these four classes of attack they generated a set of attack vectors to determine the method an attacker might use. They found 140 different attack vectors and scored them according to highest priority first. The NCSC’s threat model was performing using threat trees. With the thinking that to know what to defend, you first need to understand how the networks can be attacked. For example, the goal would sit at the root of the tree and the routes to the leaves of that tree is a path to attain that goal.

A cyber threat assessment can be performed to determine the overall risk of each OT asset (National Institute of Standards and Technology, 2021). An example of the attack methods typically used by threat actors in OT environments is demonstrated in Table 2-3.

Target	Possible Attack Vectors	Possible Attack Methods	Possible Consequences
Access control system	Identification cards	Exploitation of unpatched application (building management system)	Unauthorised physical access
	Closed-circuit television (CCTV)	RFID spoofing	Lack of (video) detection capabilities
	Building management network	Network access through unprotected access points	Unauthorised access to additional ICS assets (pivoting)

*Table 2-5 OT Threat Taxonomy example*

An OT cyber-attack requires an attacker to have a deep technical understanding of the underlying engineering processes and assets being automated (Assante & Lee, 2015). This includes the architecture design and safety mechanisms of each OT system at hand; such knowledge would enable them to bypass the critical safety mechanisms in place. This complexity makes it significantly difficult for attackers to gain entry without alerting defenders. This type of attack is often referred to as a Cyber-Physical attack (Assante & Lee, 2015), which is unlike the typical attacks we read about in the news. To accomplish such an attack, a two-stage attack is required (see Figure 2-8) as follows:

**The ICS Cyber Kill Chain: Stage 1** is the first stage of an ICS cyber-attack and is primarily the intelligence gathering stage as shown in Figure 2-8. Like Lockheed Martin’s Cyber Kill Chain, the purpose of stage 1, is to gain knowledge about the OT assets at hand; to understand each of the mechanisms needed to bypass perimeter security and gain access to the ICS.

**The ICS Cyber Kill Chain: Stage 2** the complexity of launching an attack is determined by the security of the system, the process being monitored and controlled, the safety design and controls and the intended impact. For example, a simple denial of service that disrupts the ICS is significantly easier to achieve than manipulating the process in a designed way or being able to attack the system and have the option of re-attacking.

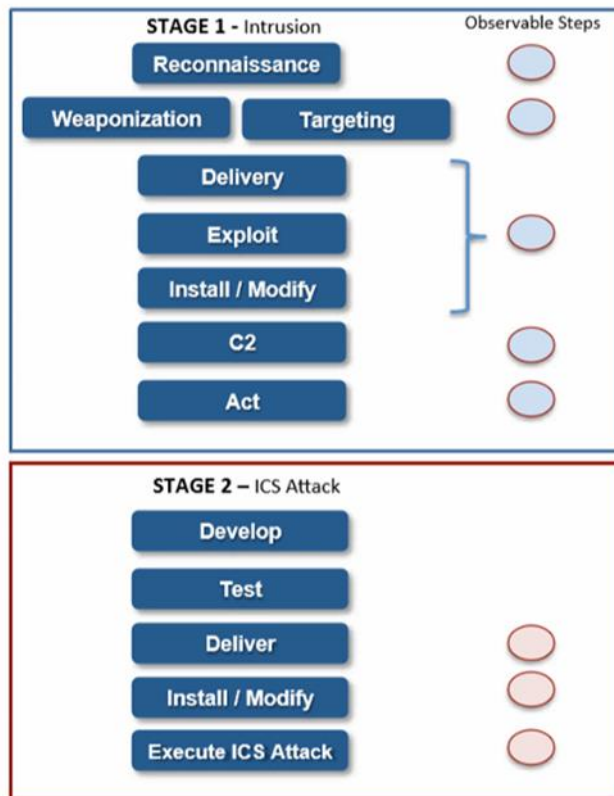


Figure 2-8 Cyber Intrusion Stage 1 & 2 - ICS Attack – adopted from (Assante & Lee, 2015)

A properly architected ICS system should have multiple interconnected layers of defence coupled with detection sensors that an attacker must bypass during Stage 1 before they even begin to attempt to gain access to the ICS/OT system components. However, unfortunately, by directly connecting an ICS system to the same network segment as a typical IT infrastructure, this often means directly connecting OT systems to the Internet. This significantly undermines the layered security implementation. These defensible architectures must be designed into the roll out of such systems and the choices around how OT and IT systems are integrated should have security in mind as well as safety (Assante & Lee, 2015).

The next section will explore some of the historical cyber-attacks on OT environments.

### 2.5.1 Cyber-Attacks on OT Environments

Cyber-attacks on OT systems are a real problem. (Kaspersky, 2018) reported a 600% increase in attacks on ICS between 2012 and 2014. Year in review statistics identified that industrial manufacturing was targeted close to twice as often as all the other industrial sectors combined in 2021 (Dragos, 2022). With increased connectivity and interconnected safety systems, this problem will only grow.

The rise in cyber-attacks is also well documented in academic literature (Reeder & Hall, 2021), (Johnson, 2016), (Kaspersky, 2018), (Leandros & Maglaras, 2018). Cyber-attacks can take many forms and may stem from a variety of sources, including criminal and nation-state actors. Dragos found that manufacturing firms are particularly vulnerable to cyber threats and that their attention to their Cyber Security strategies is therefore particularly important (Dragos, 2022). Whilst it is true that industrial cyber-attacks are on the rise, not all attacks are achieved through malicious malware infections (Assante & Lee, 2015). Defenders should not assume the threat will always arrive by a form of malware. Existing capabilities such as the common Microsoft Windows tools, provides enough functionality for an adversary to perform an invasion, without the need for actual malware.

Examination of past cyber-attacks on critical infrastructures (Stoddart, et al., 2016), may help to inform the attack paths and methods used by attackers and identify past lessons learned in history. It is useful to look at some of the most recent disruptive incidents that have targeted the industrial sector in which organisations learn to coexist with destructive hazards, the inevitability and disruptiveness of cyber-attacks (Tedim & Leone, 2017).

The cyber-attack on the Oldsmar Water System Florida in February 2021. During a press conference (Levenson, 2021), the City of Oldsmar announced there was an “unlawful intrusion into the City’s water treatment system and that an adversary attempted to poison the water supply”. Figure 2-9 demonstrates the possible steps taken by the adversary to gain access to the plant based on the MITRE ATT&CK for ICS Matrix (MITRE, 2017). Despite the heightened media attention, subsequent FBI reports (Walser, 2023) indicate that the attack never actually occurred and that it was an error on the part of the operator at the time. Nonetheless, the media coverage for such attacks demonstrated the potential vulnerabilities of water systems throughout the world. Highlighting that technological solutions alone should not be the only choice when it comes to securing Critical Infrastructure, as demonstrated in this case, since the human component could be the primary cause of incidents reducing the resilient performance of a critical system (Giacomello & Pescaroli, 2019).

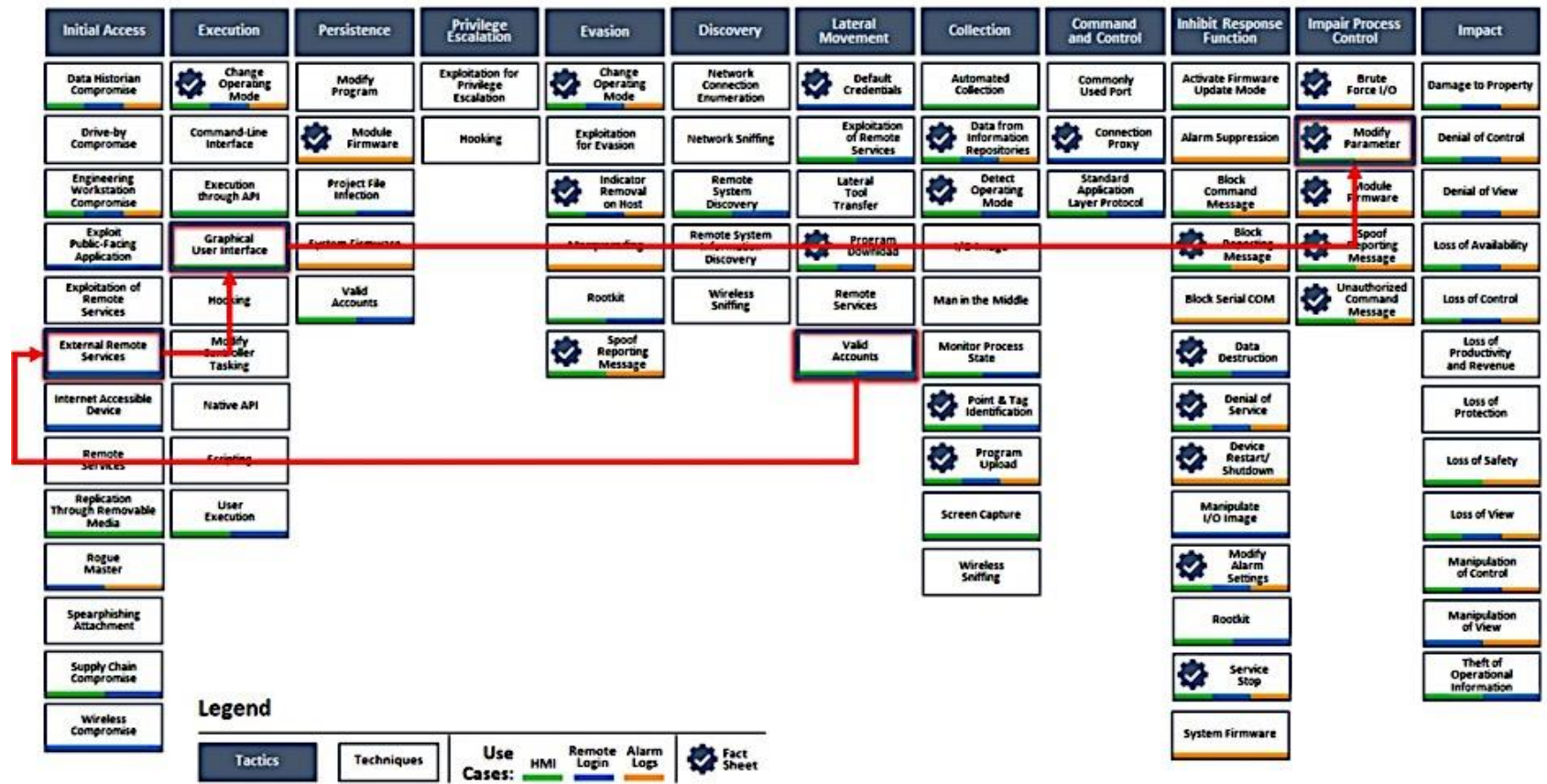


Figure 2-9 MITRE ATT&CK for ICS Matrix (MITRE, 2017)

The Colonial Pipeline Ransomware Attack in May 2021, one of the largest gas fuel pipelines in the U.S. announced a ransomware attack on its IT systems. To contain and limit damage of the attack, pipeline operations were halted, resulting in gas shortages and panic-buying by its consumers (Reeder & Hall, 2021).

Also in May 2021, one of the largest beef suppliers in the world - JBS Foods, with meatpacking facilities in the U.S., UK, Australia, Canada, Mexico and Brazil, announced it detected ransomware targeting the food and beverage infrastructure within their Sao Paulo branch. It shut down many of its operations and paid out \$11 million in Bitcoin ransom (Dragos, 2022).

Following a failed attack on a petroleum processing plant at Saudi Aramco, the global concern surrounding CS risks to critical OT infrastructure was significant. Although the ‘Shamoon’ attack did not cause any physical damage to the production facility, it did awaken the world to the capabilities of other countries in the cyber warfare game (Bronk & Tikk, 2013).

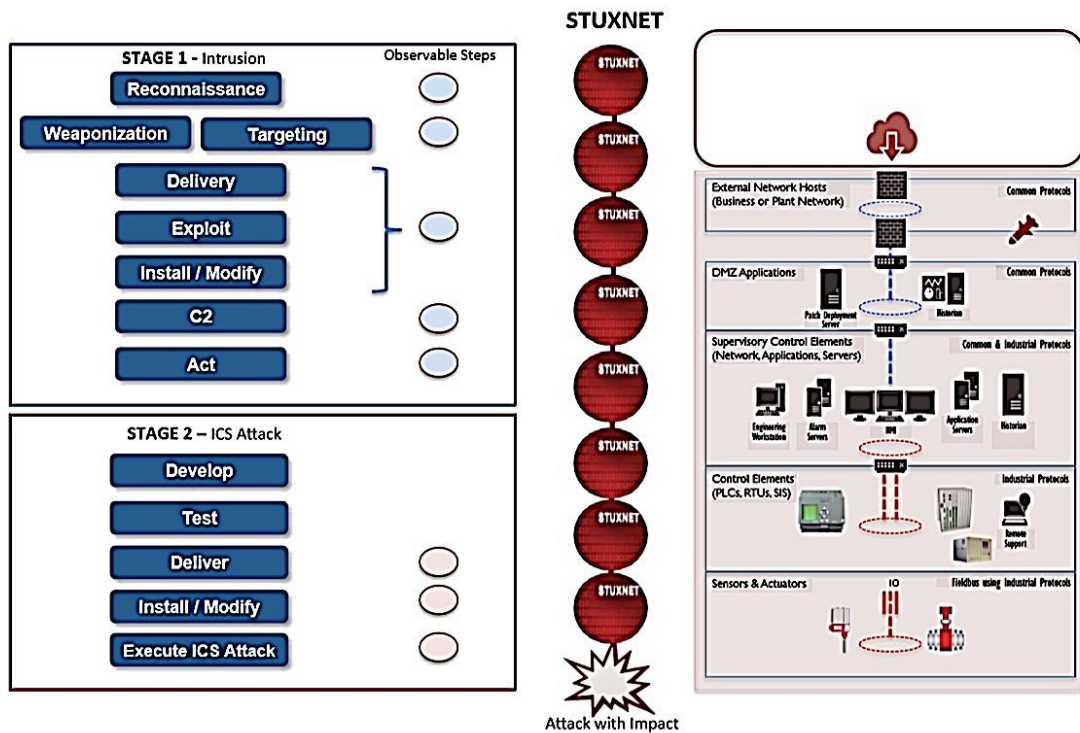


Figure 2-10 STUXNET Attack - ICS kill chain; adopted from (Assante & Lee, 2015)

Stuxnet was a highly targeted attack that was able to physically destroy centrifuges at the Natanz facility in Iran. The Iranian uranium enrichment was of significant concern across the globe. The malware was delivered by USB and installed itself on various versions of Windows. It repeated the process until it could establish communication with its C2. Once on the targets, a WinCC SIMATIC server connected to specific Siemens controllers and performed the Execute ICS Attack phase. The

Intelligence gathering is believed to have gone on over many years. The impact of the attack was the modification of the processing systems forcing the centrifuges into physically destroying themselves. The malware evolved, searching for older versions of itself and updating with the latest attack modules. Figure 2-10 shows the SANS ICS Kill chain diagram to demonstrate how the attack was constructed (Assante & Lee, 2015), (Dragos, 2022).

Another espionage campaign that took place over the course of 3 years was the 'Havex' remote access Trojan (Assante & Lee, 2015). It could gather sensitive data from thousands of OT industrial sites around the globe. The Trojan had multiple methods of delivery to ensure its success including: spear phishing emails containing infected attachments, a compromise of the OT Vendor websites used to infect engineering workstations after visiting (known as a Watering Hole Attack) and malicious code injected into the OT vendor's software installer, intended to infect the host system when users attempted to run it. By manipulating engineers into unintentionally transporting infected software files from an Internet facing computer into the production OT network, the attackers could bypass the usual perimeter defence mechanisms described in stage 1 of the ICS kill chain (Assante & Lee, 2015).

State sponsored actors have access to more resources and expertise than their criminal counterparts and can therefore be challenging to defend against. They can also introduce additional legal uncertainty for the private sector targets, as illustrated in a 2018 lawsuit initiated by the Mondelez Food Conglomerate against its insurer Zurich (Evans, 2018), which initially refused the \$100 million dollar claim on the grounds that the NotPetya ransomware attack, to which it had fallen victim, had been caused by a government-sponsored actor and could therefore be considered an act of war. After a long-standing lawsuit, the claim was settled in April 2023. Further developments relating to this case surfaced in May 2023 (Regmedia, 2023), whereby Mondelez employee data was compromised in a law firm cyber-attack. This is another case of a third-party service provider being compromised leading to data exposure.

While interconnecting OT systems with IT systems is necessary for enhancing productivity and efficiency, the traditional 'air gap' approach that provided protection against external attacks for many years, is no longer sufficient, as highlighted by (Johnson, 2016); (Dragos, 2022) and (General Electrics, 2017). Many sites believed to be air-gapped were found to be connected to the internet, emphasising the need for stronger security measures (Johnson, 2016). When conducting case studies on Industrial OT sites, General Electric found that every site thought to be air gapped was not air gapped at all and in most cases, connected to the Internet (General Electrics, 2017). As also demonstrated by (Dragos, 2022) whereby 90% of their customer engagements last year for



manufacturing industries alone, had limited visibility into their OT networks and poor network configurations. Eighty percent of which exposed their production lines to external internet. This finding is also identified in the case studies conducted for this research, as discussed in Chapter 5. The case study observations unfortunately show how many manufacturers are still ill prepared in dealing with cyber-attacks to their production. Dragos believe with a high degree of certainty that OT will continue to be a target and attempts to disrupt industrial environments through 2023 will increase (Dragos, 2022).

As well as the growing cyber threats to CNI, we have little understanding on the intentions of a particular business when addressing CR. As a business develops and begins to acquire or build additional facilities, it is often left with a disparate set of configurations and limited asset visibility that are complex and fragile. Furthermore, adding to the problem domain is the lack of understanding due to the similarities between safety & security standards. This means that IT security policies, which cannot easily be implemented in safety-critical systems, are governing the operations of the factory plant. Whilst regulators and engineers understand the fundamental safety requirements of such systems, security requirements do not easily follow on (Leandros & Maglaras, 2018). This presents significant blockers to efficiency and increases the risk of compromise.

As a result, the initial step in a cyber-physical security analysis is conducting an asset discovery process to clearly identify the System under Consideration (SuC) and its interconnections according to NIST (National Institute of Standards and Technology, 2021). This exercise helps understand the current systems architecture, identify access points, define the security perimeter and pinpoint sensitive assets and functionalities. It aids in proposing a more resilient architecture.

Traditional segmentation mechanisms like VLANs and routing are impractical and complex in OT environments, posing risks of misconfiguration and downtime. They lack effective security policies and enforcement, leaving OT systems vulnerable to malware, unauthorised commands and device vulnerabilities (General Electrics, 2017); (International Electrotechnical Commission (IEC), 2021). Although IT firewalls are often suggested for securing and segmenting network traffic, they are designed to inspect IT protocols, not OT protocols. They offer limited security capabilities in detecting harmful payloads or unauthorised commands in an OT network. Merely identifying the presence of an OT protocol does not provide actionable security information (Assante & Lee, 2015).

The potential for catastrophic disasters is evermore present, not only from cyber-attacks but natural phenomena inflicting substantial disruption. Globally, the risk landscape has intensified as have the frequency and severity with which shocks are occurring and rippling into the economic, social, geopolitical, technological and health domains (Vescuso, 2022).

## 2.5.2 Towards OT Cyber Resilience

The term 'resilience' is a new concept in the system engineering (SE) domain. Findings on the idea of resilience in systems first appeared almost 50 years ago (Holling, 1973) and only in the last 15 years has it become a topic of government discussion with respect to safety systems engineering (SSE) and Cyber Resilience domains, during which, CR metrics have been the goal for the OT research community. Measuring the Cyber Resilience of an Industrial Control System is challenging since it encompasses multiple domains including organisational, social and technical. For example, organisational resilience is comprised of a range of factors such as the organisational structure, policies, decision-making processes, managerial influence, employee knowledge and cultural issues (Goodman & Haisley, 2007). Moreover, one of the major requirements of a Cyber Resilience analysis is to supply a basis for relative comparison so that decision makers can make well-informed actions based on in-depth knowledge of both the system and business environment (Leversage & Byres, 2008). The strategies adopted by an organisation guide the high-level decision-making procedures to attain Cyber Resilience (Elebute, 2018). Organisations may find it difficult to translate Cyber Resilience frameworks and models into roadmaps since there is no easy-to-follow process on how an industry can adopt and measure CR.

In comparison, system resilience is a property of functions and systems and not features, unlike we measure most organisational events against (Hollnagel, et al., 2006). As described in (Ford, et al., 2012), resilience metrics are specific to a particular disruption since different disruptions elicit varying system responses. The failure and subsequent restoration of a specific system component could lead to diverse output patterns. This fundamental concept of events in resilience has been recognised not only in the security sector but also in organisational (Westrum, 2006) and systems resilience (Sugden, 2001) domains.

“A system is resilient if –and only if– there is justifiable and enduring confidence that it will function as expected, when expected.” (Davies, 2021)

In all cases, the notion pertains to the challenge or interruption that affects the standard system operation. The primary objective of Cyber Resilience is to ensure the core functionality of a critical system (as a collective) in comparison to Cyber Security, which seeks to protect all components individually (Creese, 2019); (Bagheri, et al., 2023). Therefore, when gauging resilience, we are, in essence, measuring each individual disruption and its varying magnitudes and establishing an order that may be unique to a specific set of circumstances (Ford, et al., 2012).

Risk management, Cyber Security (CS) and Cyber Resilience (CR), although intertwined, are quite different. Risk management quantifies the probability and impact of cyber risks and Cyber Security defends against those risks whereas Cyber Resilience is essential when cyber risk is ineffective, such as “when hazardous conditions are a complete surprise when the risk analytic paradigm has been proven in-effective.” (Linkov, et al., 2013). While Cyber Security risk management is concerned with the minimisation of threats (Bagheri & Ridley, 2017), Cyber Resilience seeks to maintain functioning regardless of the “presence or absence of hazards.” (Dupont, 2019).

The traditional concept of Cyber Security focuses primarily on protecting systems from cyber-attacks known as *fail-safe*. Cyber Resilience focuses on the business mission as a whole and the events that follow in the aftermath of a cyber-attack known as *safe-to-fail* (Björk, et al., 2015). In other words, CR takes over when risk management has been unsuccessful at guarding an organisation from disruption and involves a constant cycle of undertakings to implement the necessary measures needed to deal with the next unpredictable event (Dupont, 2019).

Moreover, Cyber Resilience metrics and Cyber Security metrics serve different purposes in assessing the performance of a system during a cyber-attack. Cyber Security metrics focus on the effectiveness of preventative and detective controls, while Cyber Resilience metrics focus on the ability of the system to continue operating in the face of a cyber-attack. A system can have strong Cyber Security metrics, indicating effective controls but still be vulnerable to disruption in the event of a successful attack. Therefore, both sets of metrics are necessary for a comprehensive Cyber Resilience assessment of a system since they measure distinct aspects of the system's performance during a cyber-attack.

As a nation, we fully trust that the essential services (we often take for granted) will be available at the flick of a switch (literally) and in truth, these services give us no reason to doubt otherwise. They are exceptionally dependable and result in little disruption. However, the conventional risk assessment approach to Cyber Security has proven to be ineffective in OT environments (Linkov, et al., 2013); (Groenendal & Helsloot, 2021) and there is a rising threat to the security of traditional OT systems (Johnson, 2016). An example is the high-profile attack on the Colonial Pipeline in May 2021 where hackers successfully shut down the largest petroleum pipeline in the United States (Reeder & Hall, 2021). This explains why “organisations can have Cyber Security without being resilient, but not the other way around” (Bryson, 2018).

The view and computation of risk is not only determined by the amount of information available or from which sources but is also influenced by poor decisions and cognitive biases of the day-to-day decision makers. Choices and decisions made day to day in an organisation, may have long

term consequences that may or may not be considered at the time for reasons such as cost, time shortage or lack of resource.

“This marks the beginning of a transition from research questions to engineering management tools.” (Hollnagel, et al., 2006)

Several accident theories on organisational or human error have been proposed over the years (Hollnagel, et al., 2006). Other attempts dating back to 1936 look at the bigger picture events such as (Merton, 1936) paper on why unanticipated consequences often stem from social actions. Also noted in (Meyer & Kunreuther, 2017), where the authors identified six biases that hinder the adoption of resilience practices. These biases are as follows: Myopia bias: The tendency to prioritise immediate savings rather than considering future harms that will require mitigation, Amnesia bias: The inclination to quickly forget the lessons learned from past disasters, Optimism bias: Minimising the potential impact of adverse events on ourselves, even if we recognize their effects on others, Inertia bias: A passive response when faced with high levels of uncertainty, Simplification bias: Selectively considering only convenient factors when confronted with complex risks and Herding bias: Aligning with the actions of others instead of relying on a more specific analysis of the situation. According to (Meyer & Kunreuther, 2017), these biases act as barriers, impeding individuals from embracing resilience practices effectively.

Furthermore, looking at the holistic picture, an interesting blog by (World Economic Forum, 2022), puts into perspective the criticality and importance of Cyber Resilience for our future survival, stating that in the past twenty years, New York City alone has faced a series of unprecedented events, commonly referred to as ‘black swan’ or ‘one in 100 years’ occurrences. These include the September 11 terrorist attacks, the 2008 financial crisis, Hurricane Sandy in 2012 and most recently, the COVID-19 pandemic in early 2020. The ability to anticipate and prepare for such future events is one of the significant challenges confronting business leaders today. Similarly, the United Kingdom has also experienced a series of noteworthy events over the past two decades that have had a profound impact on various aspects of society. While not necessarily identical to the specific events mentioned in the previous statement, the UK has faced its own unique challenges. Some notable events include the London bombings in 2005, the 2008 financial crisis that had global ramifications, the Brexit referendum in 2016 and subsequent negotiations and the ongoing COVID-19 pandemic. These events have shaped and influenced the country's economic, social and political landscape, requiring adaptive responses and resilience in the face of unforeseen circumstances.

Despite these challenges, researchers from different areas such as computer science, engineering, operations research and industrial organisations have been attempting to develop objective

metrics (Ligo, et al., 2021) that can measure the Cyber Resilience of a manufacturing system (Linkov, et al., 2013) (Linkov, et al., 2014) (Linkov & Kott, 2018), (Kott & Linkov, 2019), (Kott & Linkov, 2021). The most recent work however, highlights that there is insufficient research on cyber resiliency measurements and only recently have researchers begun to investigate quantitative measures (Kott & Linkov, 2021). We, therefore, typically see qualitative approaches (Groenendal & Helsloot, 2021). This supports early findings by (Haque, et al., 2018), who states that: “although many of the frameworks provide some subjective guidance of resilience study, they all lack clear explanation on the quantitative resilience metrics formulation.”

To begin to address the limitations identified in the previous sections, the proceeding sections provide a high-level overview of the different topic areas within the domain of CR, these include the Technical, Organisational and Human elements which demonstrate the importance of considering multiple dimensions of Cyber Resilience when developing metrics and measurement frameworks.

#### 2.5.2.1 Technical Cyber Resilience

Technical resilience refers to the measures that organisations take to protect their systems, networks and data from cyber threats. This includes using firewalls, antivirus software, intrusion detection systems and other security technologies (Cybenko, 2019); (Coulouris, et al., 2021); (Chittister & Haines, 2011); (Brtis & McEvilley, 2019); (Biringer, et al., 2013).

#### 2.5.2.2 Organisational Cyber Resilience

Organisational resilience refers to the ability of an organisation to maintain its operations and functions in the face of cyber threats (Ahmad, et al., 2015). This includes having effective incident response plans, disaster recovery plans and business continuity plans in place (Dupont, 2019); (Bagheri, et al., 2023); (Syrmakeisis, et al., 2022).

#### 2.5.2.3 Human Resilience

Human or Social Resilience refers to the human elements of Cyber Resilience (Bruneau, et al., 2003); (Dunigan O'Keeffe, 2021).

By taking a comprehensive approach, organisations can better understand their Cyber Resilience posture and develop strategies to mitigate cyber risks.

## 2.6 Chapter Summary

The previous sections have provided a summary of the examined topic areas in this thesis. In summary, the concept and interpretation of Cyber Resilience (CR) have not yet achieved a universally recognised consensus. There is a need for guidance and clarity on the methods, frameworks, metrics and approaches used for assessing resilience (Linkov & Kott, 2018). Cyber Resilience can be easily confused with other cyber-related terms, standards and best practices and different approaches are found in academic literature and industry guidance. Some approaches resemble cyber-security hygiene practices, which may not directly translate into the operational technology (OT) realm. It is important to note that while security is relevant, it is not the sole determinant of Cyber Resilience. Various factors, such as the definition of CR, its context and understanding, existing standards, regulations and risk considerations may influence how resilience is conceptualised across different industries (National Institute of Standards and Technology, 2021); (International Society of Automation (ISA), 2020). Although the importance of Cyber Resilience is acknowledged, there are limited practical approaches and comprehensive guidance available to help organisations enhance their Cyber Resilience (Ford, et al., 2012); (Kott & Linkov, 2021). The lack of practical methods in the literature hinders successful collaboration among organisations in creating and implementing CR (Ferdinand, 2015). It is crucial to address this gap and develop practical approaches to improve Cyber Resilience.

The next chapter will provide the reader with a literature review on the topic of Cyber Resilience, with a particular focus to the Manufacturing and Production Industries.

# Chapter 3

## Literature Review

### 3.1 Introduction

This literature review takes a journey through A) an examination of different characteristics and parameters of Cyber Resilience B) the various theories and concepts relating to the CR problem C) an examination of the applicable measurement frameworks D) an examination of emerging and existing CR assessment frameworks E) a summary connecting each of the above concepts F) the seminal works around the topics G) the gaps in the current literature and statement of the problem. The literature review identifies the seminal works associated with the topic of CR, its measurement within the OT domain, with a particular focus on the Manufacturing and Production Industry.

### 3.2 Selection of relevant literature

An overview of the papers, methodologies and standards covering fundamental concepts of Cyber Security and Cyber Resilience in ICSs are critically reviewed in the proceeding sections. This study performs a systematic review of the current literature, selected through a search of academic journals and databases including (Elsevier – Scopus, IEEE Xplore and Springer) with respect to the following concepts: Cyber Resilience, Cyber Security, Industrial Control Systems and Complex Systems. The review uses descriptive analysis and thematic categorisation to provide insight into cross domain disciplines and varying topic scope pertaining to the terms mentioned above. The analysis identifies gaps, similarities and synergies in the current literature. From the papers reviewed, each were scored according to their relevance for this research. Adopting a concept-centric approach by using the top reviews then grouping them accordingly.

According to Ngram Viewer (Google Books, 2022) between 2014 – 2019 the number of searches related to the term CR and Cyber Resiliency has increased exponentially (see Figure 3-1 and Figure 3-2).

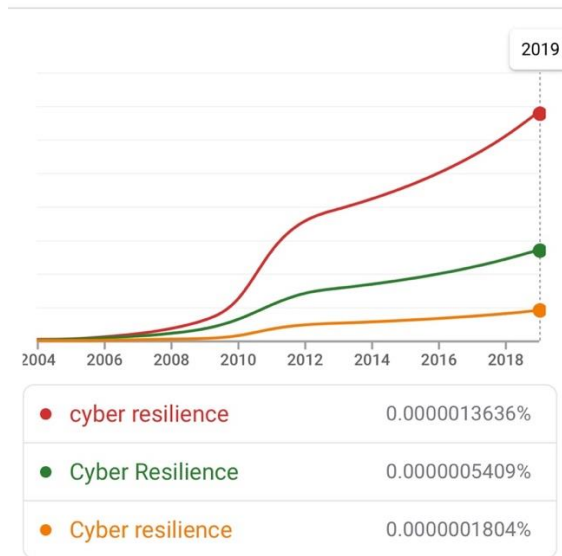


Figure 3-1 Number of searches related to the term Cyber Resilience. (Google Ngram viewer, 2022)

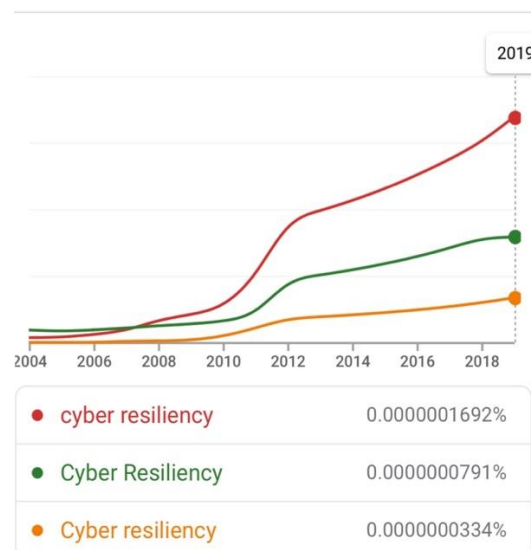


Figure 3-2 Number of searches related to the term Cyber Resiliency. (Google Ngram viewer, 2022)

Following on from the background discussions in the previous Chapter, the next sections will explore the characteristics and attributes associated with Cyber Resilience and that either contribute towards enhancing the CR of a critical-system or by counteracting the other attributes (Linkov & Kott, 2018).

### 3.3 Characteristics of Cyber Resilience

Cyber Resilient attributes and parameters refer to different aspects of Cyber Resilience. Cyber resilient attributes refer to the characteristics or features of a system that contribute to its ability to withstand and recover from cyber-attacks, disruptions and failures. Examples of Cyber Resilient



attributes include redundancy, flexibility, efficiency, diversity and complexity (Berger, et al., 2021). On the other hand, Cyber Resilient parameters, refer to the specific metrics or measurements that organisations use to assess the resilience of their systems. These parameters are used to quantify the effectiveness of the CR attributes and to evaluate the overall resilience of a system in a systematic and quantitative manner.

The difference between cyber resilient attributes and parameters can be compared to the difference between the traits and the measurements of a person. For example, a person's height and weight are measurements that quantify the person's traits, such as their overall health and fitness. In the same way, CR parameters are the quantitative measurements that quantify the effectiveness of the CR attributes of a system. Therefore, while CR attributes describe the characteristics that contribute to the resilience of a system, CR parameters describe the specific measurements used to evaluate the effectiveness of these attributes. By using a combination of both CR attributes and parameters, organisations can develop a comprehensive understanding of the resilience of their systems and take informed actions to improve it.

The next sections will describe the attributes and parameters of CR in further detail.

### 3.3.1 Cyber Resilience Attributes

The following sections will describe the high-level attributes of Cyber Resilience. Figure 3-3 provides a high-level overview of the primary CR attributes.

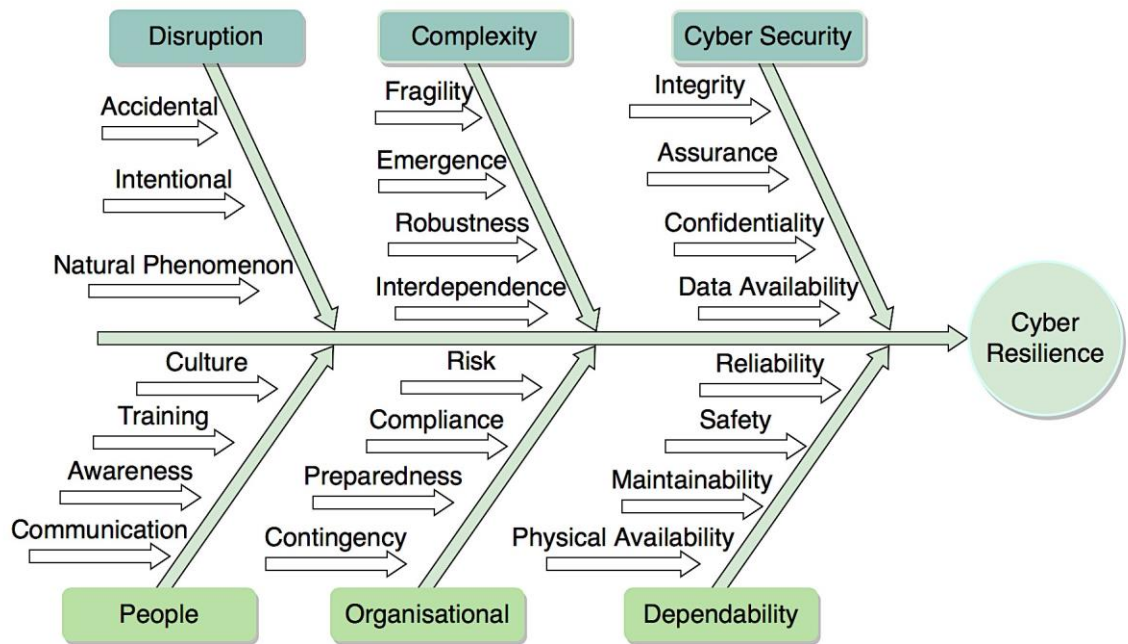


Figure 3-3 High-level dimensions of Cyber Resilience

### 3.3.1.1 Robustness

Defined by the Oxford dictionary as “The ability to withstand or overcome adverse conditions or rigorous testing”. Robustness refers to the ability of a system or a process to maintain its functionality and performance even in the presence of uncertainties, disturbances or variations in its operating conditions (Haque, et al., 2018). A robust system is designed to withstand and adapt to changes and perturbations without compromising its overall effectiveness.

The term has been used in various fields, including engineering, computer science and statistics. While the terms ‘robustness’ and ‘Cyber Resilience’ share similarities and often used interchangeably, there are subtle differences in their focus and scope.

Robustness primarily emphasises the ability of a system or organisation to withstand and resist cyber threats, disruptions or failures. It emphasises the strength and durability of the system's defences, its capacity to resist attacks and its ability to maintain functionality under adverse conditions. Robustness is typically associated with preventive measures and building a strong security foundation. On the other hand, Cyber Resilience encompasses a much broader perspective.

### 3.3.1.2 Dependability

Dependability refers to the ability to deliver a justifiably trusted service (Avizienis, et al., 2004). It incorporates the following sub-attributes: Reliability, Availability, Safety, Integrity and Maintainability. The concept of dependency also refers to that of 'trust' and the extent to which the manufacturing industry's operations are dependent on technology, systems or people. For example, a manufacturing industry might be highly dependent on a particular software program or communication network. High levels of dependency (see Figure 3-4) can increase the risk of a cyber-attack and reduce the manufacturing industry's ability to operate in the event of a disruption (Avizienis, et al., 2004).-

#### *Reliability*

Reliability refers to the consistency of a system's performance and a measure of its ability to deliver the required services over time (Barbacci, 1995) or the continuity of correct service (Avizienis, et al., 2004). Although like resilience, reliability does not consider the stresses or disturbance factors that can impact a systems normal operating. Reliability refers to the difference between reliability and resilience is discussed in (Clark-Ginsberg, 2016).

#### *Availability*

Availability refers to the readiness of correct service (Avizienis, et al., 2004) or the amount of time a system is operational and accessible to users.

#### *Safety*

Safety refers to absence of devastating significances on the people and the environment (Avizienis, et al., 2004). Safety systems refer to the systems and processes that are in place to ensure the safety of workers and prevent accidents or other incidents. Safety systems are an important component of Cyber Resilience, as cyber-attacks can potentially impact safety systems and lead to physical harm or damage to equipment (Xu, et al., 2023).

Safety and reliability are often confused however, they are distinct system properties. In the past, reliability served as a reasonable proxy for safety, since improving component reliability led to enhanced safety. This is no longer the case, nowadays, reliability and safety can be separate and often conflicting attributes of a system (Leveson, 2020) when it comes to resilience.

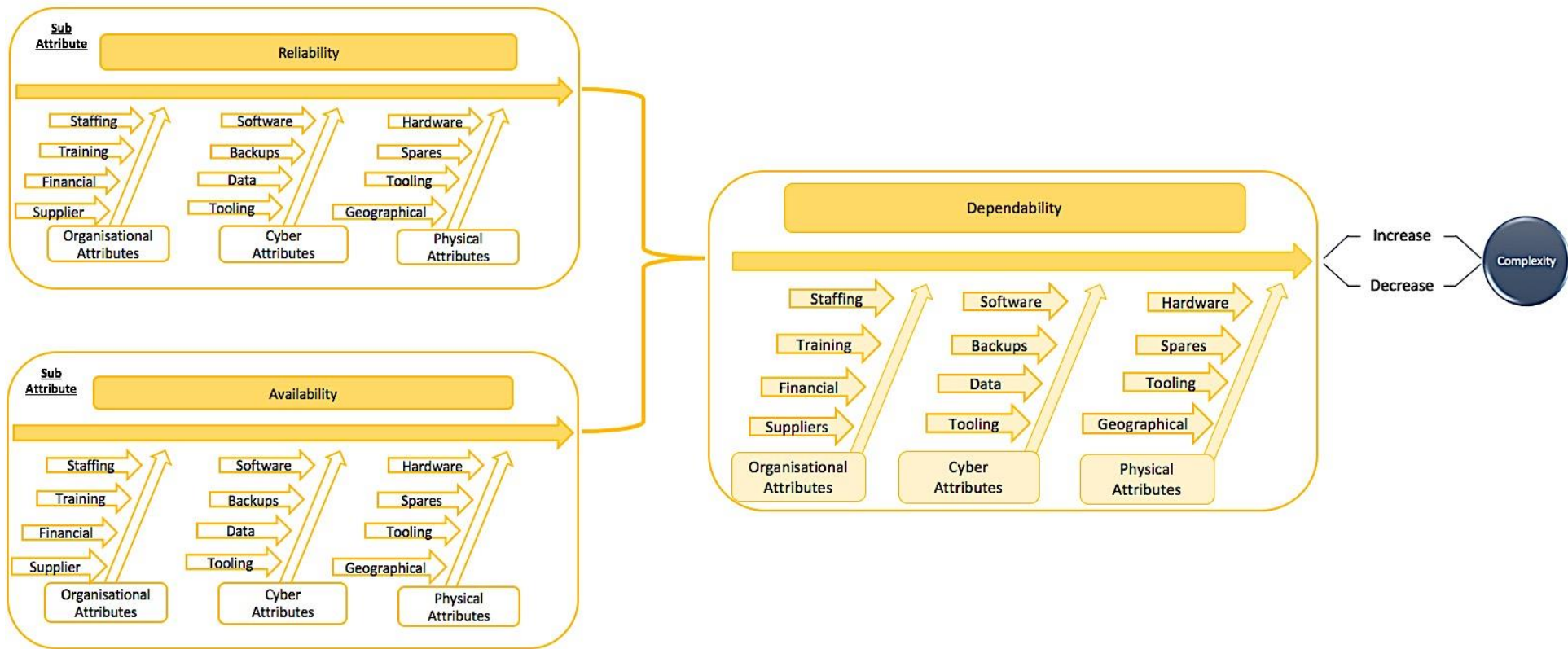


Figure 3-4 Dependability, reliability and availability (an example)

Accidents can occur even when system components operate with 100% reliability. These accidents often result from unsafe interactions among the components, stemming from system design errors or complexities that surpass our ability to anticipate and manage all potential unsafe interactions. Likewise, the broader environment surrounding the system, known as the context, plays a crucial role in determining safety. This principle applies not only to system components but also to entire systems. For instance, as discussed by (Leveson, 2020), consider firing a gun in the middle of a vast, uninhabited desert, away from anyone or anything. In this setting, the gun and the action can be considered both reliable and safe. However, performing the same action in a crowded public place, changes the safety assessment, even though the gun's reliability and the action itself remain unchanged.

### *Maintainability*

Maintainability refers to the ability of a system to undertake modification and repairs (Avizienis, et al., 2004).

### 3.3.1.3 Security

In the context of this study, Security refers to the protection of data, systems and networks from unauthorised access and cyber-attacks. Whilst security covers both the physical and cyber domains, this research will focus on its Cyber Security elements that covers the management of information and how it is protected from unauthorised access or theft. It incorporates the following sub-attributes: Confidentiality, Integrity and Availability. Cyber Security refers to the technologies, processes and policies that are in place to protect the manufacturing industry's systems and data from cyber threats. It is a critical attribute of Cyber Resilience, as it is essential for preventing, detecting and responding to cyber-attacks (Watkins & Hurley, 2015).

Though Cyber Resilience encompasses Cyber Security, CR is more comprehensive and includes the ability to withstand, respond and recover from an attack.

### *Confidentiality*

Confidentiality refers to “the obligations of individuals and institutions to use information that has been disclosed to them and is under their control appropriately.” (Cambridge Dictionary, 2023).

### *Integrity*

Integrity refers to deficiency of improper system modifications (Avizienis, et al., 2004).

#### 3.3.1.4 Stability

Defined by the Cambridge Dictionary as: “A situation in which something such as an economy, company, or system can continue in a regular and successful way without unexpected changes” (Cambridge Dictionary, 2023). Stability refers to a system's ability to maintain its performance over time, regardless of changes in environment or inputs.

#### 3.3.1.5 Complexity

Complexity is an important attribute of Cyber Resilient systems. Complex systems are characterised by many components, multiple levels of interconnections and non-linear relationships between components (Kott & Abdelzaher, 2014). Complexity Science has multiple sub-components of study, as described in Chapter 2. While complexity can pose challenges for organisations seeking to maintain the resilience of their systems, it can also contribute to the resilience of the system in the following ways:

- **Increased Robustness:** Complex systems can be more robust than simple systems, as they have a greater number of components that can continue to operate even if some components fail.
- **Improved Fault Tolerance:** Complex systems can be designed with redundant components, which can help to ensure that the system can continue to operate even if some components fail.
- **Improved Adaptability:** Complex systems can be designed to respond to changing conditions, making them more adaptable to changing environments.
- **Improved Self-Healing:** Complex systems can be designed with self-healing capabilities, which can help to minimise the impact of failures and reduce the time required to recover from incidents and disruptions.

However, it is important to note that complexity can also have negative effects on the resilience of a system, as it can increase the risk of unintended consequences and make it more difficult to understand and manage the system (Axelsson, 2022). Additionally, complex systems can be more vulnerable to cyber-attacks, as they have more entry points and interconnections that can be targeted by attackers. Therefore, when designing and implementing Cyber Resilient systems, it is important to balance the need for complexity with the need for simplicity, considering the specific challenges posed by each. Organisations need to understand the trade-offs between complexity

and simplicity and make informed decisions about how to achieve the optimal balance between these two concepts (Linkov, et al., 2013); (Linkov & Kott, 2018); (Dupont, 2019).

The next section discusses another attribute of Cyber Resilience known as Network Science.

#### 3.3.1.6 Network Science

Network science is a novel field of study that provides a set of mathematical and computational tools for analysing and understanding complex networks. It can be used to study the resilience of complex systems, such as computer networks, power grids or manufacturing systems. Network science can help identify critical nodes, components or links within a system, as well as understand the dependencies and interconnections between different parts of the system. By applying network science, organisations can gain a deeper understanding of the resilience of their systems and can identify areas that are most vulnerable to disruption or attack. Additionally, network science can be used to model and simulate different scenarios, allowing organisations to assess the potential impact of different incidents and to develop and test resilience strategies.

#### 3.3.1.7 Topology

Topology refers to the arrangement or structure of components and interconnections within a system. Moore and Cho, explores the role of topology & methods to analyse the influence of topology on Cyber Resilience (Moore & Cho, 2019). Topology plays an important role in determining the vulnerability of a system to incidents and disruptions. For example, the topology of a network can impact the speed and efficiency of data transmission, as well as the ability of the network to withstand failures of individual components. Similarly, the topology of a power grid for example, can impact the ability of the grid to provide reliable power to consumers and the topology of a manufacturing system can impact the efficiency and speed of manufacturing. By understanding the topology of their networks, organisations can develop and implement resilience strategies that consider the specific challenges posed by the topology. Topology is an attribute that can be used to assess and improve Cyber Resilience in a manufacturing industry. Topology refers to the physical and logical arrangement of the network infrastructure, including the location of devices, the connections between them and the protocols used to transmit data. A well-designed network topology can improve Cyber Resilience in several ways. For example:

- **Segmentation:** A segmented network topology can help to isolate critical systems and data from potential cyber threats. By dividing the network into smaller segments, a

manufacturing industry can reduce the impact of a cyber-attack by containing it to a smaller portion of the network.

- **Redundancy:** A redundant network topology can help to ensure that critical systems and data remain available in the event of a cyber-attack. By providing multiple paths for data transmission, a redundant network can help to mitigate the impact of a cyber-attack on network availability.
- **Access control:** A well-designed topology can help to enforce access control policies and prevent unauthorised access to critical systems and data. By restricting access to certain parts of the network, a manufacturing industry can reduce the risk of a cyber-attack.
- **Monitoring:** A well-designed network topology can also make it easier to monitor network activity and detect potential cyber threats. By placing monitoring tools at key points in the network, a manufacturing industry can quickly detect anomalous activity and take appropriate action.

By designing a well-structured network topology, a manufacturing industry can improve its ability to prevent, detect and respond to cyber threats. The next sub-sections explore some examples of topology in further detail.

### *Purdue-Model*

The Purdue Model, also known as the Purdue Enterprise Reference Architecture Model for Cyber-security (PERA-CS), is a framework for understanding and assessing the cyber-security posture of an organisation (Williams, 1992). It provides a common language and framework for discussing and assessing different aspects of cyber-security, including risk management, threat management and incident response. The model is organised around four and sometimes five levels of cyber-security (Simonovich, 2020), each of which corresponds to a specific set of capabilities and practices (discussed later in this Chapter). The primary four levels are:

- **Technical Level:** focuses on the protection of information and information systems using technical controls such as firewalls, intrusion detection systems and encryption.
- **Management Level:** focuses on the management of information security risks, including the development and implementation of policies, procedures and standards.
- **Organisational Level:** focuses on the integration of cyber-security into the overall structure and culture of the organisation, including the alignment of cyber-security with business objectives and the allocation of resources.



- **Strategic Level:** focuses on the alignment of cyber-security with the broader goals and objectives of the organisation, including the development of a strategic vision for cyber-security.

While the Purdue Model is primarily used to assess the cyber-security posture of an organisation, the concept of levels of cyber-security can also be applied to the assessment of the resilience of a system. By understanding the different levels of resilience, organisations can develop and implement resilience strategies that consider the specific challenges posed by different types of incidents and disruptions.

### *Zone & Conduit*

The concept of zones and conduits is used to assess the resilience of a networked system. In this approach, a network is divided into different zones, each of which represents a separate and distinct component of the network (International Electrotechnical Commission (IEC), 2021). The zones are interconnected through conduits, which represent the communication pathways between the zones. The use of zones and conduits can help organisations understand the resilience of their networks by enabling them to identify and isolate critical components, assess the impact of failures and develop and implement strategies to manage incidents. For example, by creating separate zones for critical components such as servers, databases and applications, organisations can ensure that disruptions in one zone do not affect the operation of other zones. Additionally, by creating separate conduits for distinct types of traffic, organisations can better protect and prioritise critical traffic. By using the zones and conduits approach, organisations can better understand the structure and dependencies of their networks and can develop and implement more effective resilience strategies (General Electrics, 2017). Additionally, the use of zones and conduits can help organisations better understand the interconnections between various parts of the network and can help identify areas that are most vulnerable to incidents and disruptions.

### **3.3.1.8 Continuity**

Business continuity is the ability of an organisation to continue operating despite a disruptive event. CR is a component of business continuity, specifically relating to the continuity of operations in the face of a cyber-attack. Continuity also encompasses 'Disaster Recovery' which is a subset of CR and is concerned with the processes and procedures used to restore systems and data after a disaster or cyber-attack.

### 3.3.1.9 Resources

Resources refer to the assets, capabilities and capacity of a system required to support its operation and enable it to recover from incidents and disruptions. Resources include physical assets, infrastructure and facilities, as well as human assets such as personnel, skills and expertise. Factors that fall under the resources umbrella include:

- **Hardware and software:** These include the physical and virtual infrastructure that supports the manufacturing industry's operations. Hardware and software must be updated regularly to ensure that they remain secure and functional.
- **Data backups:** Data backups are a critical component of Cyber Resilience, as they ensure that important data can be recovered in the event of a cyber-attack or other disruption.
- **Staffing and training:** The human resources required to maintain and operate the manufacturing industry's systems are also an important factor in Cyber Resilience. Staff must be trained and aware of cyber threats and best practices for preventing and responding to them (Carias, et al., 2018).
- **Financial resources:** Adequate financial resources are required to invest in Cyber Resilience technologies and services, as well as to maintain and update existing systems (Dupont, 2019).

The availability and allocation of resources are critical factors in determining the resilience of a system. For example, having sufficient resources such as backup power supplies and redundant communication links can help a system recover from an incident more quickly and effectively. Similarly, having trained personnel and access to specialised skills and expertise can help a system respond more effectively to incidents. By understanding the resources required to support the operation of a system and enable it to recover from incidents and disruptions, organisations can develop and implement resilience strategies that consider the specific challenges posed by the availability and allocation of resources. Additionally, by having a clear understanding of the resources required to support their systems, organisations can ensure that they have the capacity to respond effectively to incidents and disruptions and can make informed decisions about investments in resources to improve resilience.

#### *Diversity*

Diversity is a sub-component of 'resources' in respect to Cyber Resilience and refers to the variety and heterogeneity of a system's components, which can help reduce the risk of failure and increase the ability of the system to recover from incidents and disruptions (Davies, 2021); (Li, et al., 2020).

Diversity refers to the use of multiple technologies, systems or processes to achieve the same or similar outcomes. For example, a manufacturing industry might use multiple types of sensors to monitor the same process or it might use different communication protocols to transmit data. Diversity can help to reduce the impact of a cyber-attack by ensuring that the manufacturing industry's operations are not entirely reliant on a single technology or system. In the context of resilience, diversity can take various forms that include:

- Technical diversity: refers to the use of different technologies, platforms and systems within a networked environment.
- Supplier diversity: refers to the use of multiple suppliers and vendors to support the operation of a system.
- Geographical diversity: refers to the distribution of system components across separate locations.
- Organisational diversity: refers to the use of different organisational units, departments and teams to support the operation of a system.

By having a diverse range of components, systems can become more resilient to failures and incidents, as the risk of widespread disruption is reduced. For example, by using multiple suppliers and vendors, organisations can ensure that they are not reliant on a single source of support, reducing the risk of disruption. Similarly, by distributing system components across different locations, organisations can ensure that failures in one location do not affect the entire system. By understanding the importance of diversity in supporting resilience, organisations can develop and implement resilience strategies that consider the need for diversity and can invest in building and maintaining diverse systems. Additionally, by having a clear understanding of the role of diversity in supporting resilience, organisations can make informed decisions about investments in diversity to improve resilience.

### *Redundancy*

Redundancy refers to the use of multiple, separate components or systems to provide backup and ensure the continued functioning of critical systems in the event of a failure or attack. Redundancy can be implemented through hardware, software, network or data redundancy, which help improve the reliability and availability of systems. Redundancy is often considered a sub-component of resources when it comes to measuring Cyber Resilience. Redundancy refers to the availability of backup systems or resources that can be used in the event of a cyber-attack or other disruption. In the context of a manufacturing industry, this might include redundant servers, power supplies or communication lines. Redundancy is an important component of Cyber Resilience

because it can help to ensure that critical systems and data remain available even in the face of a cyber-attack or other disruption. However, redundancy is just one aspect of resources that can impact Cyber Resilience. Redundancy is an important sub-component of resources when it comes to measuring Cyber Resilience.

### *Memory*

Memory is a subcomponent of 'Resource'. Memory refers to the storage capacity of a system or component that is used to retain information or data. It plays an important role in maintaining the integrity of data and ensuring that it can be recovered in the event of an incident. For example, having adequate memory for backups and snapshots can help ensure that data can be recovered to a known state in a timely manner. Additionally, having sufficient memory for logs and audit trails can help organisations detect and respond to incidents more effectively.

#### **3.3.1.10 Flexibility**

Flexibility refers to the ability of a system to adapt and respond to changing conditions, whether internal or external. Flexibility enables organisations to quickly and efficiently respond to evolving threats, changing business requirements and unexpected disruptions. By having flexible systems and processes, organisations can better maintain their operations, even in the face of adversity. Flexibility, on the other hand, refers to the ability of a manufacturing industry to adapt to changing circumstances and respond to cyber threats in a flexible manner. For example, a manufacturing industry might need to change its operations in response to a cyber-attack, or it might need to adopt new technologies or processes to improve its Cyber Resilience. Flexibility is important as it can help to ensure that a manufacturing industry remains adaptable and responsive in the face of cyber threats.

#### **3.3.1.11 Efficiency**

Efficiency refers to the ability of systems to perform their intended functions with a minimum of waste, in terms of resources such as time, energy and money. Efficient systems are optimised for performance and use resources effectively, which helps ensure that they can function effectively in times of stress or disruption. By having efficient systems, organisations can reduce the costs associated with maintaining their operations, as well as increase their ability to respond to unexpected events.

Efficiency with respect to a manufacturing industry for example, could mean efficient operations that involve minimising downtime, maintaining high levels of productivity and ensuring that critical systems and data remain available. Efficiency is an important component of Cyber Resilience, as it can help to minimise the impact of cyber threats on the manufacturing industry's operations however, Bain & Company conducted a study revealing that organisations solely focused on efficiency may experience higher profits but also exhibit heightened vulnerability in their daily operations. Conversely, the research found that organisations with higher levels of resilience demonstrate a survival rate almost double that of those with lower resilience (Dunigan O'Keeffe, 2021). These findings emphasise the importance of prioritising resilience alongside efficiency to ensure the sustained functioning and success of an organisation in the face of challenges and disruptions.

Efficiency and flexibility can be viewed as separate components of Cyber Resilience, although they are often interrelated. While efficiency and flexibility are separate components of Cyber Resilience, they are often interrelated. For example, a manufacturing industry that is efficient in its operations may be better able to adapt to changing circumstances and respond to cyber threats in a flexible manner. Similarly, a manufacturing industry that is flexible in its operations may be able to respond more quickly to cyber threats and maintain higher levels of efficiency even in the face of disruption.

In summary, Diversity and Redundancy are subcomponents of 'Resources' and should be used with caution when considering CR strategies. While diversity, redundancy and complexity can both contribute to the resilience of a system, they can also have competing effects. For example, a complex system may be more resilient if it has a high level of diversity, as this can reduce the risk of widespread failure. However, the same system may also be less resilient if it is too complex, as this can increase the risk of unintended consequences and reduce the ability of the system to recover from incidents and disruptions (shown in Figure 3-5).

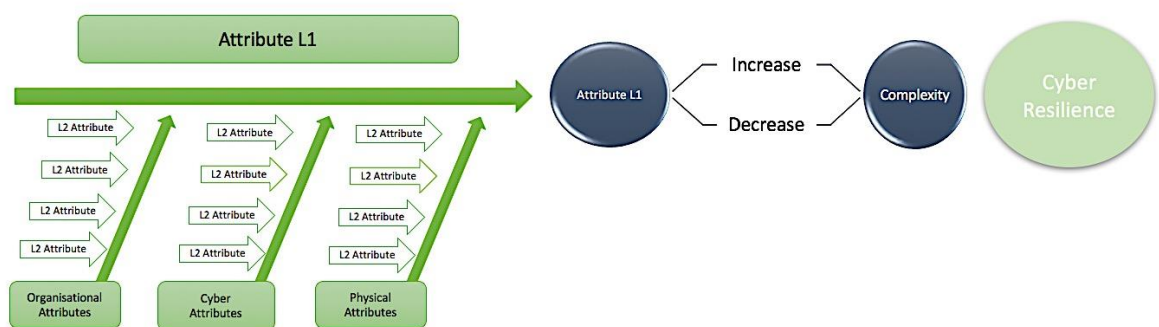


Figure 3-5 Enhancing or Counteracting Cyber Resilience

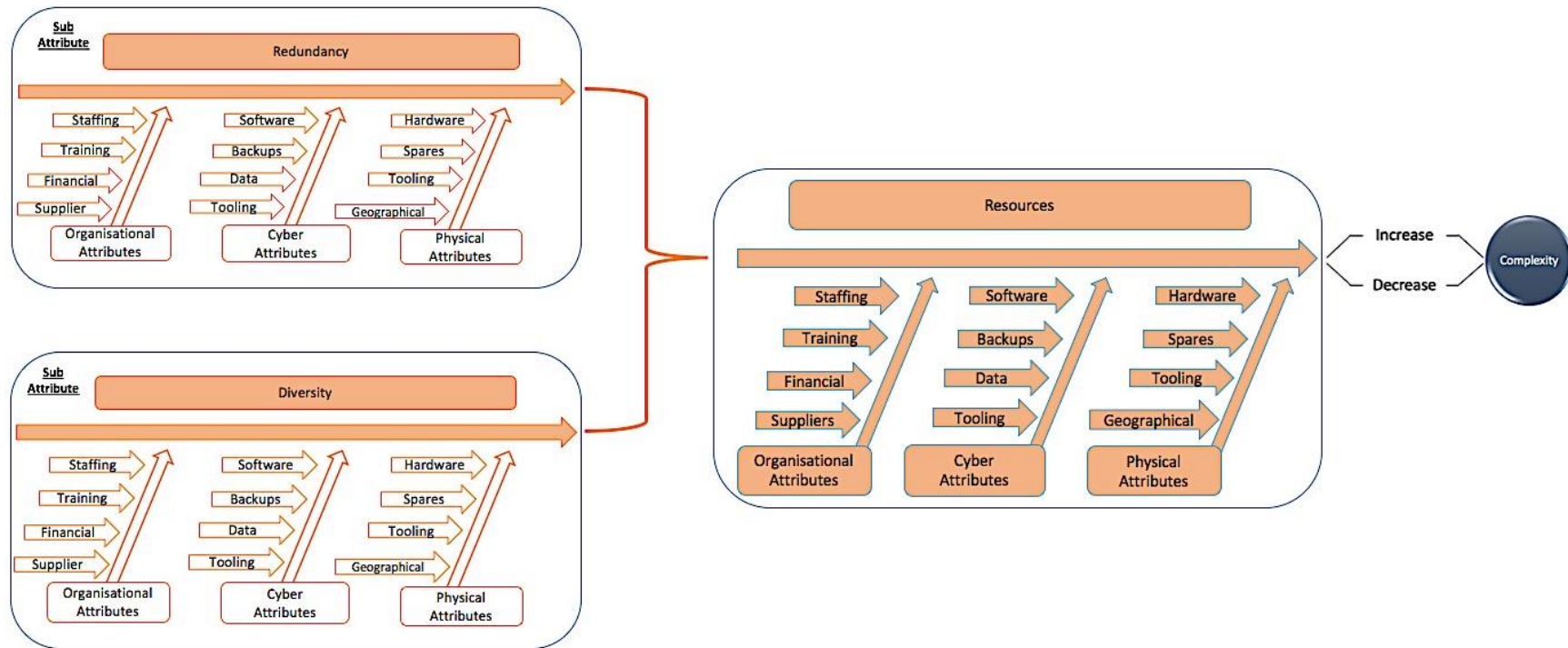


Figure 3-6 Attribute Examples

When designing and implementing Cyber Resilient systems, it is important to balance the need for diversity and complexity, considering the specific challenges posed by each (see Figure 3-6).

Additionally, organisations need to understand the trade-offs between diversity, redundancy, reliability, safety and complexity and make informed decisions about how to achieve the optimal balance between these concepts.

---

### 3.3.2 Cyber Resilience Parameters

This section will explore the parameters of Cyber Resilience.

#### 3.3.2.1 Critical-Function

Critical-Function is a parameter used to assess the resilience of a system. It refers to the essential activities or processes that must continue to operate for an organisation to fulfil its mission or maintain its operations. Critical functions are identified as priorities during incident response and recovery planning. They form the basis for prioritising resources and activities. The identification of critical functions helps organisations understand what is most important to protect and maintain. It helps guide the development of resilience strategies to ensure the continued functioning of these critical functions in the event of an incident.

#### 3.3.2.2 Threshold

Threshold is another parameter used to assess the resilience of a system. It refers to the level of performance or capacity below which a system is compromised or non-functional. Thresholds are used to define the acceptable level of degradation or disruption that a system can withstand without becoming inoperable. Thresholds can be based on metrics such as response time, data loss, or availability and they help organisations determine the point at which a system or component has failed or is no longer able to perform its intended function. The establishment of thresholds helps organisations understand the impact of incidents and determine when to trigger incident response and recovery activities.

#### 3.3.2.3 Time

Time is a critical parameter used to assess the resilience of a system. It refers to the amount of time it takes for a system or component to recover from an incident or to perform a specific task, such

as data backup or system restoration. In the context of resilience, time is often expressed in terms of recovery time objectives (RTOs) and recovery point objectives (RPOs). RTOs represent the maximum amount of time that can elapse before a critical function must be restored, while RPOs represent the maximum amount of data that can be lost or the maximum amount of time that can pass before data is backed up. By understanding and managing the time required for different activities, organisations can develop and implement resilience strategies that meet their specific needs and requirements.

#### 3.3.2.4 Complexity

Complexity is an attribute (as discussed in Section 3.5) but also a parameter used to assess the resilience of a system. It refers to the number of components, interconnections and interactions within a system, as well as the level of difficulty in understanding and managing those components. Complex systems are often more difficult to understand and control, which can make them more vulnerable to incidents and disruptions. Additionally, complex systems are often more difficult to recover from incidents, as there are more components that need to be restored or reconfigured. Complexity can be a critical factor in determining the time required to recover from an incident, as well as the likelihood of secondary failures or cascading effects. In his pioneering work, (Perrow, 1984) explains that catastrophic failures of any systems emerge from high complexity of links which lead to interactions that the systems designer cannot anticipate or guard against. “The links are so numerous heterogeneous and often implicit, incomprehensible to the initial design.” By understanding the complexity of their systems, organisations can develop and implement resilience strategies that consider the specific challenges posed by complexity.

#### 3.3.2.5 Relevant Parameters

This section provides a set of CR metrics that are relevant to the topic scope within this study. This section focuses specifically on the metric criteria and section 3.6 considers the approaches reported in literature.

Metrics, where referenced, have been proposed in literature whilst others have been set out by the author, taking inspiration from the various case studies and real-world manufacturing plants. It is important to note that there is no one-size-fits-all set of metrics for measuring Cyber Resilience in a manufacturing industry, as the specific metrics that are appropriate will depend on the organisations operations, infrastructure, security and safety strategies.



Many of the metrics from other disciplines can be repurposed in the domain of CR however the use of a single metric in a specific dimension is not enough to conclusively offer an empirical objective CR measure of a system instead a variety of metrics to form a rounded value that can provide enough insight and information to decision-makers. That is not to say that one specific measurement is bad for CR however should be specified as such. For example, 'the CR metric of a given systems temperature fluctuations when faced with a cyber-attack'.

There are multiple metrics proposed in literature towards the measurement of Cyber Resilience, for example the MITRE corporation (Bodeau, 2011) proposed a thorough list of metrics. Each metric has an identifier, a descriptor and an objective description (refer to the original paper for detailed information). Table 3-3 lists the most common metric criteria used to measure Cyber Resilience in industrial control systems. The specific metrics measured may vary depending on the research goals and the specific testbed or system being evaluated.

The next section discusses the general Cyber Resilience metrics.

### General Cyber Resilience Metrics

Some of the common metric criteria relating to Cyber Resilience in ICS systems include:

*Table 3-1 Common metric criteria relating to Cyber Resilience.*

Metric	Description
Response Time	These metric measures how quickly a system can respond to a cyber-attack. A faster response time can indicate better Cyber Resilience.
Downtime	This metric measures the amount of time a system is unavailable due to a cyber-attack, which can impact productivity and product quality. A shorter downtime can indicate better Cyber Resilience.
Discovery	This metric measures the average length of time between the start of adversary activities and their discovery (MT-35) (Bodeau, 2011).
Recovery Time	This metric measure how quickly a system can recover from a cyber-attack and return to normal operations. A shorter recovery time can indicate better Cyber Resilience. The metric measures the length of time between initial disruption and restoration. (MT-20) (Bodeau, 2011).
Effectiveness of Countermeasures	This metric measure how well the system's countermeasures can withstand a cyber-attack e.g., firewalls and Secure PLC design (PLC Security, 2021). A higher effectiveness score can indicate better Cyber Resilience.
System Performance	This metric measures the systems nominal performance compared to the degraded performance measure.
Protection Time	The time a system can withstand an incident without performance degradation (Zhu, et al., 2016).
% of System Availability Performance	% of pre-disruption availability/performance after disruption. (MT-21) (Bodeau, 2011)
% of Systems with implemented Cyber Resilience techniques	% of individually managed systems in which one or more resiliency techniques have been implemented. (MT-89) (Bodeau, 2011).
% of critical components with anti-tamper, shielding or power line filtering applied.	% of mission-critical components that apply anti-tamper, shielding and power line filtering. (MT-115) (Bodeau, 2011).

Level of limitations applied for remote access-control.	Level of access limitation for external maintenance personnel. (MT-121) (Bodeau, 2011).
Threshold limits	The time a system can remain within the threshold (lower and upper-level limits).

It is important to note that each of these metrics can be further broken down into sub-metrics or customised according to the specific needs of an organisation and, therefore, is not a complete list of metrics. The next section will explore the manufacturing specific metrics.

### *Manufacturing Specific Metrics*

There are many control blocks or functions that could be measured in a manufacturing context, depending on the specifics of the industry and the equipment and processes in use. For example, temperature may be an important metric to consider when measuring Cyber Resilience in a manufacturing industry, particularly if the industry uses vessels or furnaces that operate at high temperatures. Malicious cyber-attacks can target industrial control systems (ICS) that control the temperature of such equipment, resulting in unsafe operating conditions or product quality issues. Additionally, System performance and product quality can also be impacted, therefore, it may be useful to include additional metrics related to these aspects when measuring Cyber Resilience.

The following metrics (see Table 3-4) could be used to assess the impact of cyber-attacks on various control blocks within a manufacturing industry:

Table 3-2 Metrics with focus on the manufacturing sectors

<b>Metric</b>	<b>Description</b>
Production loss	This metric measures the amount of production that is lost due to a cyber-attack. This could include products that are damaged, destroyed, or not produced due to the attack.
Defect rate / scrap rate	This metric measures the percentage of defective/wasted products produced/discarded after a cyber-attack. Cyber-attacks can disrupt the manufacturing process, resulting in errors, defects, quality issues, equipment damage or production disruptions.
Mean time between failures (MTBF)	This metric measures the average amount of time between system failures. Cyber-attacks can cause system failures, leading to decreased MTBF
Mean time to repair (MTTR)	This metric measures the average time it takes to repair a system after a cyber-attack. Longer MTTR can impact production and product quality.

Temperature variance	This metric measures the difference between the set temperature and the actual temperature of the system after a cyber-attack. Higher variance can lead to unsafe operating conditions or product quality issues.
Heat stress	This metric measures the amount of heat stress that equipment and products are exposed to because of temperature control system failure.
Product quality	This metric measures the impact of control fluctuations on product quality. Such as Temperature. Inconsistent temperatures can result in product defects, contamination, deformities, discoloration or brittleness.
Inverter speed	Inverters are devices that convert DC power to AC power and are commonly used in industrial equipment such as pumps and fans. The speed of the inverter can be measured to ensure that the equipment is operating correctly and efficiently. A cyber-attack on an inverter could result in a loss of control over the equipment, leading to production issues or safety hazards.
Culinary ingredient ratios	In industries that manufacture products such as food, beverages or pharmaceuticals, the precise ratios of ingredients must be maintained to ensure consistent product quality. Cyber-attacks on control systems that regulate ingredient ratios could result in product quality issues or safety hazards.
Pressure and flow rate	In industries that use pipelines or other fluid-based systems, pressure and flow rate must be carefully controlled to ensure safe and efficient operation. Cyber-attacks on control systems that regulate pressure and flow rate could result in production issues or safety hazards.
Machine cycle time	In industries that use automated equipment, machine cycle time is a key metric that measures the time it takes to complete a specific process. Cyber-attacks on control systems that regulate machine cycle time could result in production delays or quality issues.
Energy consumption	In industries that consume significant amounts of energy, such as those that use large machinery or operate 24/7, energy consumption can be a key metric for monitoring operational efficiency. Cyber-attacks on control systems that regulate energy consumption could result in increased costs or production issues.

### Cyber Security Metrics

There are many Cyber Security metrics that can be used alongside other resilience metrics towards the measurement of CR within a manufacturing environment. Table 3-5 provides some common metrics:

*Table 3-3 Metrics with focus on Cyber Security*

<b>Metric</b>	<b>Description</b>
Mean time to detect (MTTD) cyber incidents:	This metric measures the time it takes to detect a security incident, from the moment the breach occurred to the point where it is identified.
Mean time to respond (MTTR) to cyber incidents:	This metric measures the time it takes for the company to respond to a cyber-incident after it has been detected.
The number of successful cyber-attacks:	This metric can be used to measure how often the company has experienced successful cyber-attacks over a given period.
The number of unsuccessful cyber-attacks:	These metric measures how many cyber-attacks the company has successfully prevented, stopped or mitigated over a given period.
Risk assessment score:	This metric can be used to quantify the potential risk of a security breach, based on the likelihood and impact of various cyber threats.
Compliance with regulations and industry standards:	This metric measures the extent to which the company adheres to relevant industry standards and regulatory requirements for cyber-security.
Employee training and awareness:	This metric can assess the effectiveness of employee training programs to help employees understand cyber risks and how to prevent them.
Investment in cyber-security:	This metric measures the amount of money the company invests in cyber-security, which can provide an indication of how seriously the company takes Cyber Resilience.
Incident response time:	This metric measures the time it takes for a manufacturing industry to detect and respond to a cyber-attack. Faster incident response times can help to minimise the impact of the attack.
Recovery time objective (RTO):	This metric measures the amount of time it takes for a manufacturing industry to recover its operations after a cyber-attack. A shorter RTO can help to minimise the impact of the attack on productivity and profitability.

Mean time between Cyber Security incidents (MTBCSI):	This metric measures the average amount of time between Cyber Security incidents. A longer MTBCSI indicates that a manufacturing industry is more resilient to cyber-attacks.
Cyber Security training completion rate:	This metric measures the percentage of employees who have completed Cyber Security training. Higher completion rates can help to improve overall Cyber Resilience by ensuring that employees are aware of cyber threats and best practices for protecting against them (Carias, et al., 2018).
Access controls compliance rate:	This metric measures the percentage of users who comply with access control policies. Effective access controls can help to prevent unauthorised access to critical systems and data.
Vulnerability patching time:	This metric measures the amount of time it takes for a manufacturing industry to patch known vulnerabilities in its systems and software. Faster patching times can help to reduce the risk of cyber-attacks. By measuring these and other metrics, a manufacturing industry can gain a comprehensive understanding of its Cyber Resilience and take appropriate steps to improve its Cyber Security posture.

In summary, a comprehensive approach to Cyber Resilience requires organisations to consider many of the attributes and relevant parameters discussed in Section 3.5 and develop tactics that address the attributes of most relevance. These attributes and parameters are all important components of Cyber Resilience in a manufacturing industry. While each are distinct, they are often interrelated and can work together to improve the manufacturing industry's ability to prevent, detect, respond and recover from cyber disruptions.

The next section discusses the approaches proposed in literature towards the measurement of Cyber Resilience.

### 3.4 Measurement Approaches

This section aims to provide an overview of the literature on Cyber Resilience measurement approaches to identify potential research gaps and areas for future research. The topic has become increasingly pertinent among researchers, particularly as more businesses have adopted digital and online technologies (Rehmani, et al., 2018). Consequently, the body of literature on CR measurement is expansive and covers a range of perspectives, including theoretical, technical and organisational approaches (Tiwari et al., 2020). Overall, the main high-level themes can be divided into qualitative and quantitative approaches, with a small number that make use of both qualitative and quantitative approaches. Each approach is described further in the proceeding sections.

#### 3.4.1 Quantitative Objective Approaches

Quantitative approaches to Cyber Resilience include metric-based approaches which provides an objective metric based on empirical or experimental observations. This involves using specific metrics to measure CR. Metrics could include a systems performance during a cyber-attack and its ability to withstand nominal operating performance or the time to detect and respond to an incident for example. Further details on metric approaches proposed in literature are discussed in the next sections.

Quantitative themes can further be broken into the following categories (see Figure 3-7):

- Metric-Based
- Model-Based
- Hybrid-Based

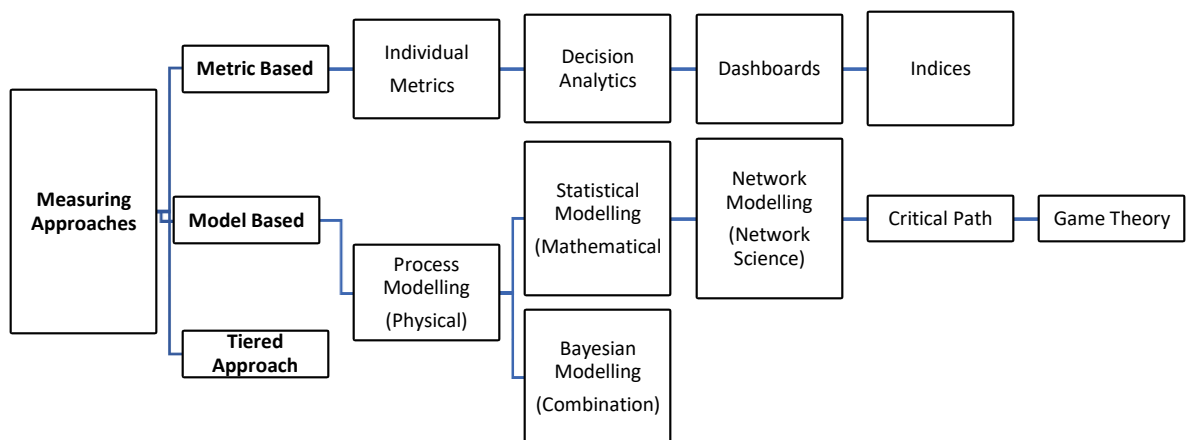


Figure 3-7 Cyber Resilience measurement themes in literature.

Literature relating to the quantitative measurement of Cyber Resilience across other critical or industrial domains include (Albasrawi, et al., 2014) who compares the smart grids functionality relative to disastrous functionality levels to identify recovery approaches. (Clark & Zonouz, 2017) use a game theory approach to develop metrics that enhance better cyber protection policies for power systems. (Choudhury, et al., 2015) makes use of a graph theory approach to look at the Network Science attribute such as (latency, frequency of access requests and QOS metrics).

In the Military context, (Hassell, et al., 2012) considers the Cyber Security characteristics and uses it to measure a systems resilience to a cyber-attack such as (% of successful attacks, mean number of disruptions due to attack, duration of attack and defensive efficiency).

In the ICS domain, (Wei & Ji, 2010) measure resilience using a consequence driven approach for example (performance degradation or loss and the protection/recovery time). (Ramuhalli, et al., 2013) focuses on continuity of operations, system recovery and financial implications.

Reviews covering the current analytical methods for interdependent infrastructure systems are presented in (Goldbeck, et al., 2019). The authors' model and measure resilience by combining Minimum Cost Flow (MCF) models and stochastic simulations to show asset failure and repair using Bayesian Networks. The authors consider three different models that look at the network flows for each asset and their operation under the uncertainty of risk and cascading failures.

The paper by (Espinoza-Zelaya & Bai Moon, 2022) presents a framework to identify and classify the resilience mechanisms in a cyber-manufacturing system. Their paper is focused on a system of interest, a disturbance source and the authors set out the function of resilience enhancing mechanisms. They categorise resilience enhancing mechanisms as:

“...reduce the probability of successful cyber-attacks, reduce the time to detect a cyber-attack, reduce the adverse effects of a successful cyber-attack and to reduce the time to recover from cyber-attacks” (Espinoza-Zelaya & Bai Moon, 2022).

In (Watkins & Hurley, 2015), the authors collected N datasets from NO experts – e.g., N=10. Individual expert responses were aggregated by using the geometric mean of the Physical, Organisational and Technical domains. Whereby each criterion each has four sub-criteria, Access Control, Segmentation, Diversity and Risk. The sub criterion takes values from three alternative scores: High, Medium and Low. This research used a Multi Criteria Decision-Making framework (MCDM), validated through surveying subject matter experts and analysed through BWM. However, the results are based primarily on subjective metrics and do not offer an empirical



objective metric. Similar findings are given in (Saaty, 2008), (Saaty, 2009), (Tusher, et al., 2022) and (Wilamowski, et al., 2017).

Subsequently, a study proposed a method of grading a system’s CR (Singh, et al., 2021). The paper only considers the system technology rather than the whole organisation, which is the underlying focus for a CR analysis. The metric criteria are not yet consistent or repeatable. The authors recognise this and aim to improve this in their future work.

This overlap between multiple domains has also been identified in (Bodeau, et al., 2015) whereby the authors consider the challenges of each problem domain and states:

“As Cyber Resilience techniques mature and are more widely adopted, the disciplines of Cyber Resilience, Cyber Security and conventional security will merge”. (Bodeau, et al., 2015)

Since many of the traditional CS analysis approaches and metrics can be repurposed in a CR analysis then, in principle, an industry should be able to reach some sort of baseline metric through use of multiple frameworks and existing maturity models (Bodeau, et al., 2015). These themes also cover the following approaches as listed in Table 3-4.

*Table 3-4 Cyber Resilience measurement approaches*

IT Domains			OT Domains		
Scope	Impact Factors	Data Sources	Scope	Risk Factors	Performance Measures
Network Architecture & Design	Network Performance	Internal System Logs & Monitoring	System-Level Approach	Supply Chain	System Efficiency
Security & Forensics	Data Security & Threats	External Sensors & Probes	Technological Design	Production Risks	Security Protocols
Performance & Availability	Regulatory Requirements	Regulatory & Guidelines	Operational Procedures	Human-Computer Interaction	User Engagement
-	Proactive & Reactive Responses	-	-	-	-

(Linkov, et al., 2013) explored resilience metrics in detail and the alternative approaches taken to define and scope Cyber Resilience metrics. Linkov found that model-based approaches focus on theoretical or physical concepts usually through mathematical or maturity-based scoring models. These are typically used as a way of translating resilience values into language that can be interpreted in the real world. Usually, comparison to cost or risk (Linkov & Kott, 2018). In a later paper, the authors also found that modelling approaches require a detailed and former knowledge of the system and its environment stating that: "A resiliency analysis should not be designed or introduced without appropriate understanding of the decision choices made in the analysis that is capable of revealing potentially negative impacts and systemic efforts" (Kott & Linkov, 2019). Comparative-analytical studies should be conducted with and without the proposed measure before recommendations are given. Models can represent a logical method to simulating real behaviours of industrial systems over time, enabling users' better insight into the complexity of a system. (Carias, et al., 2018).

"Metrics are typically a property that can be measured to determine and quantify how the system functions." (Collier, et al., 2016)

Several approaches such as probabilistic modelling which include cross-disciplinary analysis and complex Systems (Ayyub, 2014); (Fox-Lent, et al., 2018). Non-Probabilistic methods including possibility theory and baseline assessments (Dubois & Prade, 2012). Other approaches in literature include subjective and adaptive management approaches, modelling and simulation approaches which include network flow theory, graph theory, input-output modelling, game theory, agent-based modelling and system dynamics.

System Dynamics is a modelling and simulation methodology established in the theory of nonlinear dynamics and feedback control which deals with the internal feedback loops and time delays that influence a system. Such as collating the system interactions through use of causal relationships (Min, et al., 2007). A System Dynamics methodology considers the analysis of complex changing systems involving interdependencies and is used in several disciplines of research including engineering. It is an effective tool used to model indecisive properties as such can often appear chaotic, unpredictable or counterintuitive and yet not random (Carias, et al., 2018). This approach enables the modelling of unintentional consequences which help to minimise their impact. This is important, since experience teaches that countless strategies that initially appear effective, often have devastating inadvertent long-term consequences. Based on these specific characteristics of System Dynamic modelling techniques, it appears a plausible modelling approach toward the analysis of CR in safety-critical complex systems. However, while simulation models like System

Dynamics offer valuable insights and help in understanding the complexities of enhancing CR in the manufacturing OT industry, they should be regarded as a starting point. Real-world validation and accounting for environmental factors are crucial to ensure the model's reliability and practicality in guiding actual decision-making and policy implementation.

“On the one hand, Cyber Resilience development involves complex and multiple relations between variables. The process of building Cyber Resilience needs to consider variables that evolve quickly, like new types of cyberattacks or software upgrades, with others that need longer times to change, such as organisational culture or individual attitudes towards security. On the other hand, building Cyber Resilience involves soft variables that cannot be directly measured, such as manager’s commitment or employee’s awareness.” (Carias, et al., 2018)

The need for diverse networking, otherwise referred to as significant difference, is discussed in (Davies, 2021). Davies explains how diversity leads to increased resilience in complex systems. Two diversity approaches include the managed approach which considers software diversity at the level of networks. Building on the work of (Davies, 2021), (Li, et al., 2020) have developed an approach at the network level. In contrast to much of the earlier work, they model networks in which nodes may be running multiple, vulnerable products and in which there may be constraints with certain products not having the ability to run on certain operating systems. The main objective of their work is to study the similarities between products which may cause malware to propagate more rapidly through a network – the output from their work is an optimal allocation of products to nodes that slows malware propagation as far as possible. The technique proposed in their work is for the first time making a diversification strategy to increase a system’s resilience.

In the paper by (Carias, et al., 2018) the authors presented a simulation model for SMEs to reflect the short and long-term effects of enhancing CR. Their model makes explicit the key factors to enhancing resilience by representing the relationships to reduction of security breaches. They do this using a preliminary System Dynamics (SD) model. Their model shows how technology, processes and people exist together and why CR cannot be achieved through technological solutions alone and that social factors should also be considered in the design and implementation of effective policies, with the aim to seek commitment between technology and training. The author explains that although the concepts of CS and CR are different, they are still related stating that:

“...having cyber security technology should theoretically improve Cyber Resilience. However, to improve Cyber Resilience, training should be of key importance, because personnel training level, knowledge and contributions in

the contingency planning are key in the processes involved in CR planning.”  
 (Carias, et al., 2018)

Their model (shown in Figure 3-8) looks promising. However, since it was not applied in a case study or tested outside of their simulation environment, the authors acknowledge that the results were based on theoretical notions and the results have not been validated with real scenarios. The model also lacks the environmental aspects that can affect a system in terms of CR.

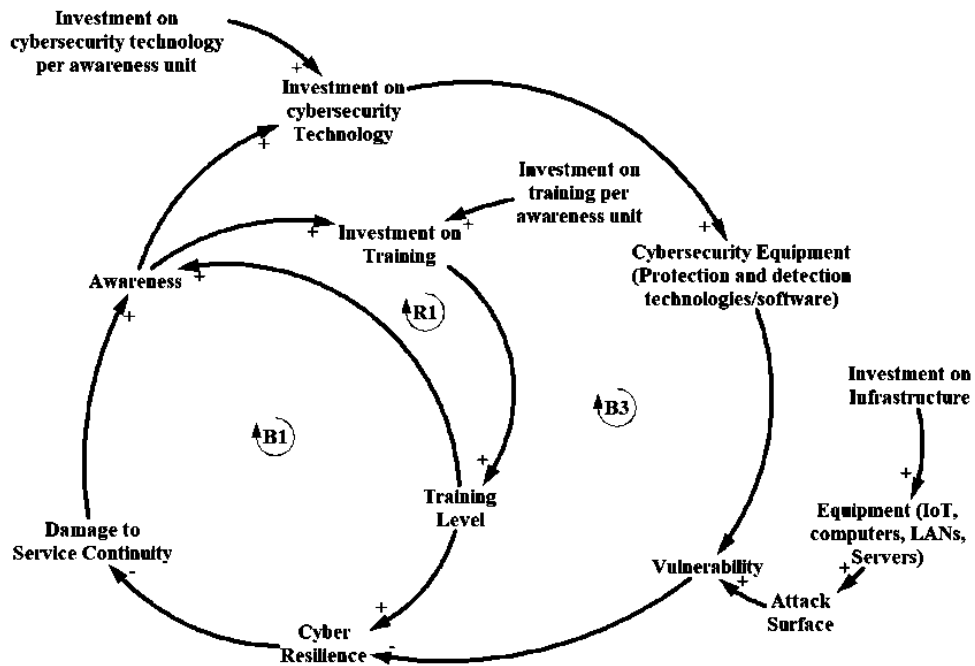


Figure 3-8 Cyber Security and resilience relationships. (Adopted from Carias, et al., 2018)

In summary, the benefits of simulation models, particularly System Dynamics, is their ability to excel at capturing the interdependencies and feedback loops within complex systems, thus, explicitly connecting the concepts and contributing to understanding CR dynamics. This is essential for assessing the multifaceted nature of CR in safety-critical industrial systems. They can also help uncover unintended consequences of cyber resilience strategies, which is critical as strategies that seem effective initially might lead to unforeseen issues in the long term. Furthermore, the use of such models can reveal the importance of considering both technological and social factors in CR, highlighting the need for a holistic approach involving technology and training. However, there are also limitations to using simulation models in this context. For example, one of the major limitations of the study by (Carias, et al., 2018), is that the results are based on theoretical notions and the model has not been validated through real-world scenarios. This means the accuracy and real-world applicability of the model are uncertain. The absence of real-world case studies limits the

practicality of the model. CR strategies that may look promising in simulation might not work as expected in real manufacturing environments and finally the model lacks consideration of environmental aspects, which can significantly affect a system's resilience. Neglecting these factors may lead to an incomplete understanding of CR in the manufacturing OT industry.

The next section discusses the qualitative subjective approaches to cyber resilience.

### 3.4.2 Qualitative Subjective Approaches

Qualitative approaches to Cyber Resilience include framework-based assessments which are typically performed by subject matter experts and based on subjective measures such as an expert opinion rather than an objective metric (Keys & Shapiro, 2019) (Haque, et al., 2018) (Jacobs, et al., 2018). Qualitative approaches include structured frameworks, such as the NIST Cyber-security or NIST Cyber Resilience Frameworks (National Institute of Standards and Technology, 2021), the ISO/IEC 27001, ISA/IEC 62443 standards (ISA, 2020), (International Electrotechnical Commission (IEC), 2021), (Tusher, et al., 2022) which provide a set of guidelines and best practices for managing cyber-security risks.

Other approaches, which supply ideas for CR metrics using qualitative or semi-quantitative values such as (Low, Medium and High) and with focus to Organisation Resilience include: the CERT Resilience Management Model (Caralli, et al., 2016); MITRE's 'Cyber Resiliency Metrics, Measures of Effectiveness and Scoring' framework (Bodeau, 2011) updated in May 2015 (Bodeau, et al., 2015), (DiMase, et al., 2015) and 'The Cyber Resilience Matrix' in (Linkov, et al., 2013) which evaluates the capacity of organisations in dealing with cyber incidents before and after a crisis. Further information relating to the latter approach is provided in Section 3.6.3.2.

Other qualitative means are maturity-based approaches: which involves assessing the maturity of an organisation's cyber-security program based on a set of predefined stages (Office of Cybersecurity, Energy Security, and Emergency Response, 2012); (Watkins & Hurley, 2015). The stages may range from an immature state with ad-hoc processes to a mature state with well-defined and integrated cyber-security processes and risk-based approaches: which involves assessing the level of risk associated with industrial environments (IRRIIS, 2006), (National Institute of Standards and Technology, 2018). Capability maturity models form the basis for CS metrics in literature. Capability maturity models (widely used in the CS domain) typically depict existing practices within an organisation as a basis for comparison. However, although there are attempts in literature to provide a method for measuring the maturity of an organisations Cyber Resilience,

few offer a method to achieve a baseline maturity measure of an organisation's resilience during the context establishment stage and of the few that do, only qualitative metrics are offered.

Cyber Resilience frameworks proposed in literature range from government institutions, Industry specific advice (INCOSE Resilient Systems Working Group, 2020), academia and private organisations from the World Economic Forum (World Economic Forum, 2022) to the Energy firms (General Electrics, 2017).

A systematic review of Cyber Resilience Assessments and Frameworks by (Estay, et al., 2020), who perform a systematic literature review to identify CR frameworks and use descriptive analysis and thematic categorisation to classify each framework. Their work presents a map of the current CRF research landscape relevant research gaps, similarities and synergies between them. Another review is given in (Carías, et al., 2021), the authors conducted a literature review of the most popular frameworks and standards in CR. 41 documents identified as being relevant to CR analysis and only 4 documents had a self-assessment tool. Of the forty-one papers, five contained maturity models and only one contained any guidelines on how to prioritise the CR analysis. The authors produced a CR assessment tool to aid Small and Medium Enterprises (SMEs) in their CR operationalisation. Three case studies formed the basis for his study with reported success. However, the study related to SMEs with a limited level of CR and focused primarily within the IT domain. The need for this type of tool within OT environments would be of benefit.

The paper by (Chittister & Haines, 2011) is the earliest research paper concerning the proposal of a CR framework. The authors suggest that a business case for the development of CR requirements should be endorsed and signed for prior to an assessment starting. The authors stress that once resilience requirements are established, they only serve as a single point in time decision and should be reviewed with changing environments throughout the systems life cycle (Brtis & McEvelley, 2019).

The paper by (Rahman, et al., 2021), analysed the resilience property of an ICS system in the events of cyber-attacks using a subjective approach and qualitative data. Their proposed framework is based on subjective opinion from subject matter experts.

#### 3.4.2.1 Frameworks with focus to the Operational Technology domain

A plethora of standards, frameworks and directives on the topics of Risk, Cyber Security and Cyber Resilience have appeared over the last decade (Keys & Shapiro, 2019). The following introduces these frameworks whereby a particular emphasis is given towards ICS.

The U.S. Department of Commerce published a framework (National Institute of Standards and Technology, 2014) to promote the protection of critical infrastructure and to support operators to manage CS related risks (National Institute of Standards and Technology, 2013), (COBIT 5), (ISA 62443) and ISO/IEC 2700. NIST subsequently released a framework for developing CR systems (National Institute of Standards and Technology, 2021) updated in August 2021 to align to the MITRE ATT&CK Framework (MITRE, 2017).

The MITRE ATT&CK framework, originally developed for threat intelligence in the IT domain, has been extended to cover the ICS domain and can be used to identify vulnerabilities and improve Cyber Resilience in ICS (MITRE, 2017).

ISA-95 is the international standard for the integration of enterprise and control systems. ISA-95 consists of models and terminology (Williams, 1992). As discussed in Chapter 2, one example widely used across OT environments is the Purdue Model which incorporates layers of technology and business practice used by industrial corporations and incorporates them as levels for the standard (Simonovich, 2020).

The US energy sector developed a 'Cyber-security Capability Maturity Model' (C2M2) in 2012 to assist organisations running critical infrastructure. The model comprises ten domains, objectives and practices aligned to maturity indicator levels (Office of Cybersecurity, Energy Security, and Emergency Response, 2012). An updated version (released in July 2021) aligned with the main changes to NIST CS framework (National Institute of Standards and Technology, 2018).

The Cyber-security Framework (CSF) developed by the National Institute of Standards and Technology (NIST) provides a set of guidelines and best practices for improving cyber-security and resilience across critical infrastructure sectors, including manufacturing. The framework aligns with the MITRE framework (Mitre Corp., 2012) and sets out five functions: Identify, Protect, Detect, Respond, Recover). The Resilience Analysis Grid (RAG) is a methodology developed by (Hollnagel, 2015) to evaluate the resilience of complex systems, including ICS.

Table 3-5 P3R3 Cyber Resilience Mechanisms - adopted from (Theron, 2013)

P3R3 Mechanisms	GENERIC P3R3 CYBER RESILIENCE CAPABILITIES
<b>P1- Prevision (identifying threats)</b>	P1.1- Threat intelligence (public or private sources & means, ...)
	P1.2- Threat analysis (identification, capacities, targets, vectors, risks)
	P1.3- Threat evaluation & prioritisation and Resilience policy & strategy
<b>P2- Prevention (of identified threats)</b>	P2.1- Public-Private cooperation & legislative support
	P2.2- Reduction of threats at source or deterrence
<b>P3- Protection (of systems against residual threats)</b>	P3.1- Incident / attack avoidance and absorption dispositions engineering
	P3.2- Incident / attack coping dispositions engineering
	P3.3- Awareness raising, education, testing & training (preparation)
	P3.4- Management of systems' configuration, lifecycle and procurement
<b>R1- Recognition (of an incident)</b>	R1.1- Monitoring & analysis of events and detection of incidents
	R1.2- Confirmation of incidents
	R1.3- Alarm on incident
<b>R2- Response (to incidents in order to defend missions &amp; systems)</b>	R2.1- Mobilisation process (response activation decision and activation)
	R2.2- Response
	R2.3- Evidence management & exploitation, forensics & inquiries
<b>R3- Rebound (to new course of life / operation &amp; status)</b>	R3.1- Repair and reconstruction (Healing)
	R3.2- Lesson learning and sharing
	R3.3- Adaption & improvement (Renewal)
	R3.4- Investigations, legal suits, insurance claims, retaliation

The Industrial Control Systems Cyber Resilience Guide developed by (International Electrotechnical Commission (IEC), 2021) provides a framework for assessing and improving the Cyber Security of ICS. A Cyber Resilience Capabilities framework (P3R3) is given in (Theron, 2013) which sets out six resilience mechanisms (



Table 3-5) similar to those set out in (Mitre Corp., 2012), (National Institute of Standards and Technology, 2021). When mapping OT assessments to CS industry standards, the most adopted OT CS frameworks are identified in Table 3-6.

Table 3-6 commonly adopted OT CS frameworks

Framework	Description
IEC 62443	All Requirements / controls 62443-2-1.- Risk Assessment Requirements Cyber Risk Assessment process from 62443-3-2 – Risk Assessment and System Design
NIST CSF	Controls across all domains (Prevent   Protect   Detect   Respond   Recover) (NIST also provides mapping against IEC 62443)

The next section discusses the Standards and Frameworks of relevance to this study.

### 3.4.3 Standards and Frameworks of Relevance

This section details all applicable standards and descriptions of specific organisations used in this research. It sets out the frameworks related to the safety, security and resilience elements of this research.

#### 3.4.3.1 Relevant Frameworks on Secure Safety Systems

Due to the rapid advancement of technology, the management of system safety has become more complicated since accidents can have complex causes that cannot be identified through traditional safety assessment techniques (Young & Leveson, 2013). One approach that has emerged is Systems Theory Process Analysis (STPA) (Leveson, 2009), which is used in conjunction with other hazard analysis tools to improve safety in complex systems. The model is based on systems theory rather than reliability theory. Leveson’s latest approach (Leveson, 2020), in summary, points out the current challenges with industrial safety systems. First, that engineers who initially designed the system did so without fully understanding the necessary connections such as the physical interactions among components that we see today. Second, that architecture development does not fully consider the detailed requirements or system properties. This separation of requirements and architecture leads to inefficiencies and problems with safety and security. Issues surface late in development or during operation resulting in inflated costs and limited opportunities for significant changes. Leveson’s proposed solution is to shift the focus to early development stages, reducing resource-intensive aspects of system engineering and improving safety, security and other system properties. Whilst this is true, this approach only addresses the initial stages of system

design and does not consider the challenges with existing industrial systems that have been in operation for many years. Going forward, this approach will be crucial however currently, manufacturers will continue to use equipment and systems that are already in deployment until their graceful degradation or failure. Furthermore, the effectiveness of STPA framework remains a subject of debate in literature and there are ongoing efforts to address this issue (Dakwat & Villani, 2018), (Baumgart, et al., 2018).

Traditionally, engineers have either ignored human factors in system hazard analysis or treated them in a superficial manner, such as if they behave randomly. Another paper by (Leveson, 2017) describes how Rasmussen's concept (Rasmussen, 1997) can be used in three different areas of systems engineering practice. Firstly, the concept of abstraction hierarchy can be applied to engineering specifications, especially requirements specification. Secondly, Rasmussen's ideas can be utilised in safety modelling and analysis to create a more effective accident causation model that can better handle human-operated, software-intensive, sociotechnical systems. By using a formal, mathematical foundation based on systems theory, the author opens new possibilities for modelling and analysing safety systems. Thirdly, the application of Rasmussen's model of human error to a robust hazard analysis technique can help incorporate human behaviour into engineering hazard analysis.

The use of automation is increasingly common in various industries due to the benefits it offers in terms of cost reduction and enabling new approaches and solutions. When machines are automated and integrated into a system-of-systems, it is crucial to conduct a comprehensive analysis of potential critical scenarios to ensure that appropriate design solutions are developed to ensure safety. Hazard analysis methods such as PHA, FTA or FMEA are often used to identify and manage potential risks for machine operators or bystanders, especially in the development of safety-critical machinery (Baumgart, et al., 2018). However, safety certification for individual machines is not sufficient to guarantee safety in the context of a system-of-systems, as their integration and interactions may lead to new hazards. It is therefore essential to understand the application scenarios of the system-of-systems and apply a structured method to identify all potential hazards. In this paper, the authors provide an overview of proposed hazard analysis methods for system-of-systems, describe a case study from the construction equipment domain and apply the System-Theoretic Process Analysis (STPA) to a case study. The author's experiences during their case study and analysis of the results highlight certain inadequacies of STPA in the context of system-of-systems and emphasise the need for the development of improved techniques for safety analysis of system-of-systems.

### 3.4.3.2 Relevant Frameworks on Cyber Resilience

The National Institute of Standards and Technology (NIST) developed a framework to assist organisations with techniques and approaches to improving CR. (National Institute of Standards and Technology, 2021). Though, there is a sparsity of case studies that speak to the adoption or measurement of these novel approaches within a complex industrial control environment. The NIST approach to performing a CR assessment is set out in five steps:

**Step 1:** Context establishment. Identify key stakeholders, OT assets, system categorisation, NetFlow discovery and other capabilities from functional areas such as CS, cyber defence and contingency planning.

**Step 2:** Establish a baseline, identify gaps and critical business resources using the data collected and identify critical resources. Gaps can also be identified from historical reviews such as penetration test reports, after action or risk management reports and vulnerability assessments with respect threat/attack events.

**Step 3:** Analyse the system and attack surfaces. Graphically map logical and physical systems. In this step, the system is analysed from two perspectives (architectural improvements can then be identified), specifically:

- Identify the critical business resources through a graphical analysis of network assets communicating.
- Identify high value targets of APT (Advanced Persistent Threat) actors and develop attack scenarios.

**Step 4:** Define evaluation criteria and threat/vulnerability assessment. Cyber resiliency can be evaluated in multiple ways and should be distinguished before the assessment can begin. See (National Institute of Standards and Technology, 2021) for further evaluation criteria. A typical evaluation criterion could be a cyber-risk assessment especially if the organisation already makes use of a Risk Management Framework such as (National Institute of Standards and Technology, 2018).

**Step 5:** Develop recommendations (plan of action). Make recommendations following the NIST framework guidelines.

Another well-known standard in the resilience context is the Cyber Resilience Matrix by Linkov, Eisenberg & Plourde who developed the matrix to evaluate the system capacity of organisations in dealing with cyber incidents, both before and after a crisis (Linkov, et al., 2013). Their Matrix is given in Table 3-9:

Table 3-7 The Cyber Resilience matrix – adopted from (Linkov, et al., 2013)

Plan and prepare for	Absorb	Recover from	Adapt to
<p><b>Physical</b></p> <p>(1) Implement controls/sensors for critical assets</p> <p>(2) Implement controls/sensors for critical services</p> <p>(3) Assessment of network structure and interconnection to system components and to the environment</p> <p>(4) Redundancy of critical physical infrastructure</p> <p>(5) Redundancy of data physically or logically separated from the network</p>	<p>(1) Signal the compromise of assets or services</p> <p>(2) Use redundant assets to continue service</p> <p>(3) Dedicate cyber resources to defend against attack</p>	<p>(1) Investigate and repair malfunctioning controls or sensors</p> <p>(2) Assess service/asset damage</p> <p>(3) Assess distance to functional recovery</p> <p>(4) Safely dispose of irreparable assets</p>	<p>(1) Review asset and service configuration in response to recent event</p> <p>(2) Phase out obsolete assets and introduce new assets</p>
<p><b>Information</b></p> <p>(1) Categorise assets and services based on sensitivity or resilience requirements</p> <p>(2) Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers</p> <p>(3) Prepare plans for storage and containment of classified or sensitive information</p> <p>(4) Identify external system dependencies</p>	<p>(1) Observe sensors for critical services and assets</p> <p>(2) Effectively and efficiently transmit relevant data to responsible stakeholders/ decision makers</p>	<p>(1) Log events and sensors during event</p> <p>(2) Review and compare systems before and after the event</p>	<p>1) Document incident's impact and cause</p> <p>(2) Document time between problem and discovery/discovery and recovery</p> <p>(3) Anticipate future system states post-recovery</p> <p>(4) Document point of entry (attack)</p>

<p>(i.e., Internet providers, electricity, water)</p> <p>(5) Identify internal system dependencies</p>			
<p><b>Cognitive</b></p> <p>(1) Anticipate and plan for system states and events</p> <p>(2) Understand performance trade-offs of organisational goals</p> <p>(3) Scenario-based cyber war gaming</p>	<p>(1) Use a decision-making protocol or aid to determine when event can be considered “contained”</p> <p>(2) The ability to evaluate performance impact to determine if mission can continue</p> <p>(3) Focus effort on identified critical assets and services</p> <p>(4) Utilise applicable plans for system state when available</p>	<p>(1) Review critical points of physical and information failure to make informed decisions</p> <p>(2) Establish decision making protocols or aids to select recovery options</p>	<p>(1) Review management response and decision-making processes</p> <p>(2) Determine motive of event (attack)</p>
<p><b>Social</b></p> <p>(1) Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish point of contact)</p> <p>(2) Educate/train employees about resilience and organisation’s resilience plan</p> <p>(3) Delegate all assets and services to specific employees</p> <p>(4) Prepare/establish resilience communications</p> <p>(5) Establish a cyber-aware culture</p>	<p>(1) Locate and contact identified experts and resilience responsible personnel</p>	<p>(1) Follow resilience communications plan</p> <p>(2) Determine liability for the organisation</p>	<p>(1) Evaluate employee’s response to event to determine preparedness and communications effectiveness</p> <p>(2) Assign employees to critical areas that were previously overlooked</p> <p>(3) Stay informed about latest threats and state of the art protection methods/share with organisation</p>

In a separate study conducted by (Bagheri, et al., 2023), it was discovered that several critical organisational and behavioural elements that contribute to Cyber Resilience, such as cultural issues and the organisational structure, were excluded from their Matrix however the author acknowledged that the matrix did highlight some organisational aspects and formed the basis of his study towards Organisational Cyber Resilience.

In summary, despite the existence of various methods suggested for enhancing the resilience of manufacturing systems, a comprehensive resilience framework has yet to be established. Currently, most of these approaches are either in the initial phases of development (such as planning or proof-of-concept) or fail to address all the crucial attributes of resilience. Furthermore, certain approaches concentrate solely on specific areas like system design and lack general applicability.

The next section discusses the relevant security frameworks with focus to the Operational Technology context.

#### 3.4.3.3 Relevant Frameworks on OT Security

IEC 62443 (International Electrotechnical Commission (IEC), 2021) is a series of standards based on best practice guidance for Industrial Automation and controls systems (IACS) and OT environments. It was initially developed to secure (IACS) throughout their lifecycle and expanded also into other domains such as power and energy distribution and transport. The series currently includes nine standards, technical reports and technical specifications. The Cyber Security maturity model described in ISA/IEC 62443 is the international standard for Industrial Automation Process Systems and helps to provide context on how an organisation views CS risk and how those risks are managed. The IEC 62443-2-1 'maturity level' (ML) is used to provide an indication of how the site performs when assessed strictly against the standard. The ML levels are defined as: Initial, Managed, Defined and Improving. Discussed further in Chapter 5. The level requirements are given in Table 3-10.

Table 3-8 IEC 62443 Maturity Level definitions

Requirements	Description
ORG 1	Security Related Organisation and Policies
ORG 2	Security Assessments and Reviews
ORG 3	Security of Physical Access
CM 1	Inventory Management of Hardware / Software Components & Network Communications
CM 1. a	Documentation
CM 1. b	Configuration and Change Management
NET 1	System Segmentation
NET 2	Secure Wireless Networks
NET 3	Secure Remote Access
COMP 1	Devices and Media
COMP 2	Malware Protection
COMP 3	Patch Management
DATA 1	Protection of Data
DATA 1. a	Data Management
DATA 1. b	Cryptographic Technologies
USER 1	Identification and Authentication
USER 2	Authorisation and Access Control
EVENT 1	Event and Incident Management
EVENT 1. a	Detection and Logging
EVENT 1. b	Incident and Vulnerability Handling
AVAIL 1	System Availability and Intended Functionality
AVAIL 2	Backup / Restore / Archive

There are several sub-categories of individual security practices within the IEC 62443-2-1 standard which set the requirements for the standard and indicate what a 'good' OT CS site would look like. Each sub-category is shown in more detail in the Figure 3-9.





Figure 3-9 IEC 62443-2-1 Assessment Summary

The above description is only a short summary of the framework, due to the length of the guidance, please refer to Appendix 1 for an in-depth overview of the framework requirements defined in IEC 62443-2-1 and adopted for this research during the case study phase, discussed in Chapter 5.

Another framework that specifically focus their guidance on securing the actual control systems used in industrial environments is the ‘Top 20 Secure PLC Practices’ released in 2021 (PLC Security, 2021). This framework was developed by PLC Security in collaboration with industry partners to provide a set of best practices for securing Programmable Logic Controllers (PLCs). As examined in Chapter 2, PLCs are commonly used in Industrial Control Systems to automate the operation of machinery and equipment and are critical to the functioning of many industries. It is therefore important to ensure that they are secure and protected from cyber threats. The guidance provides a framework for securing PLCs by outlining a set of best practices that organisations can follow. Table 3-9 provides a summary of these practices.

Table 3-9 Top 20 Secure PLC Practices – adopted from (PLC Security, 2021)

Technique Number	Security Technique	Description
1	Modularise the PLC code.	Split PLC code into modules, using different function blocks (sub-routines). Test modules independently.
2	Track operating modes.	Keep the PLC in RUN mode. If PLCs are not in RUN mode, there should be an alarm to the operators.
3	Leave operational logic in the PLC.	Wherever feasible Leave as much operational logic e.g., totalising or integrating, as possible directly in the PLC. The HMI does not get enough updates to do this well.
4	Use PLC flags as integrity checks.	Put counters on PLC error flags to capture any math problems.
5	Use cryptographic and/or checksum integrity checks for PLC code.	Use cryptographic hashes or checksums if cryptographic hashes are unavailable, to check PLC code integrity and raise an alarm when they change.
6	Validate timers and counters.	If timers and counters values are written to the PLC program, then the PLC should validate them for reasonableness and verify backward counts below zero.
7	Validate and alert for paired inputs/outputs.	If you have paired signals, ensure that both signals are not asserted together. Alarm the operator when input / output states occur that are physically not feasible. Consider making paired signals independent or adding delay timers when toggling outputs could be damaging to actuators.
8	Validate HMI input variables at the PLC level, not only at HMI.	HMI access to PLC variables can (and should) be restricted to a valid operational value range at the HMI but further cross-checks in the PLC should be added to prevent or alert on, values outside of the acceptable ranges which are programmed into the HMI.
9	Validate indirections.	Validate indirections by poisoning array ends to catch fence-post errors.
10	Assign designated register blocks by function (read/write/validate).	Assign designated register blocks for specific functions to validate data, avoid buffer overflows and block unauthorised external writes to protect controller data.
11	Instrument for plausibility checks.	Instrument the process in a way that allows for plausibility checks by cross-checking different measurements.

12	Validate inputs based on physical plausibility.	Ensure operators can only input what is practical or physically feasible in the process. Set a timer for an operation to the duration it should physically take. Consider alerting when there are deviations. Also alert when there is unexpected inactivity.
13	Disable unneeded / unused communication ports and protocols.	PLC controllers and network interface modules support multiple communication protocols that are enabled by default. Disable ports and protocols that are not required for the application.
14	Restrict third -party data interfaces.	Restrict the type of connections and available data for third party interfaces. The connections and/or data interfaces should be well defined and restricted to only allow read/write capabilities for the required data transfer.
15	Define a safe process state in case of a PLC restart.	Define safe states for the process in case of PLC restarts (e.g., energise contacts, de-energise, keep previous state).
16	Summarise PLC cycle times and trend them on the HMI.	Summarise PLC cycle time every 2-3 seconds and report to HMI for visualisation on a graph.
17	Log PLC uptime and trend it on the HMI.	Log PLC uptime to know when it has been restarted. Trend and log uptime on the HMI for diagnostics.
18	Log PLC hard stops and trend them on the HMI.	Store PLC hard stop events from faults or shutdowns for retrieval by HMI alarm systems to consult before PLC restarts. Time sync for more accurate data.
19	Monitor PLC memory usage and trend it on the HMI.	Measure and provide a baseline for memory usage for every controller deployed in the production environment and trend it on the HMI.
20	Trap false negatives and false positives for critical alert.	Identify critical alerts and program a trap for those alerts. Set the trap to monitor the trigger conditions and the alert state for any deviation.

The next section connects the findings discussed above.

### 3.5 Connecting the Above

The Industrial sector is facing a rapid rise in Cyber Resilience due to the increasing threat of cyber-attacks on Operational Technology. Numerous Cyber Resiliency frameworks are available to aid organisations in enhancing CR, but there is a dearth of real-life case studies that demonstrate the adoption and effectiveness of these approaches within an OT environment.

The lack of a clear and meaningful understanding of Cyber Resilience and its practical interpretation poses a challenge in selecting the appropriate technique or method for empirically applying it to a manufacturing system and determining objective metrics (Cybenko, 2019), (Linkov & Kott, 2018). Existing proposed metrics for quantifying Cyber Resilience often neglect the combination of Security and Safety and a definitive link between these metrics and operationally meaningful evaluations remains elusive (Cybenko, 2019).

Though various frameworks, tools and methods for assessing and improving CR exist, many are designed for the IT sector and are not suitable for the manufacturing industry. Additionally, conflicting definitions and perceptions of CR further hinder the comprehensive assessment and enhancement of CR within the industrial domain (Haque, et al., 2018), (Smith, 2023).

The absence of internationally recognised descriptions for ‘good’ and ‘bad’ resilience metrics leads to the utilisation of maturity or screening assessments to establish a baseline resilience level but these methods provide relative rather than absolute results (Linkov & Kott, 2018). The selection of appropriate tools for determining the baseline resilience becomes complex, as their domain-specific approaches lead to high variability in outcomes, making cross-comparison challenging. Despite the increasing publication of CR approaches and frameworks, most are tailored to specific industries, lacking general applicability. Traditional Risk Assessment methods do not fully account for the complexities of interconnected OT and IT systems, OT operational priorities and safety constraints in many industries. Researchers from diverse fields have attempted to develop objective metrics for measuring CR in manufacturing systems but standardisation and consensus on definitions and meanings of CR metrics are still lacking, hampering consistent and effective evaluation in different contexts (Fisher & Norman, 2010).

Moreover, confusion between Cyber Resilience and Cyber Security persists, with both having distinct roles and purposes. Cyber Security focuses on reducing high-impact risks through security mechanisms, while Cyber Resilience addresses significant-impact, low-likelihood events, adapting and evolving in changing environments. There are clear differences between OT and IT Cyber

Resilience. OT emphasises protecting physical assets and production processes, while IT Cyber Resilience deals with safeguarding computer systems, networks and electronic data.

Considering these challenges and gaps in understanding, research and standardisation, further investigation and development of metrics and methodologies are necessary to enable effective assessment and enhancement of Cyber Resilience in the Industrial sector.

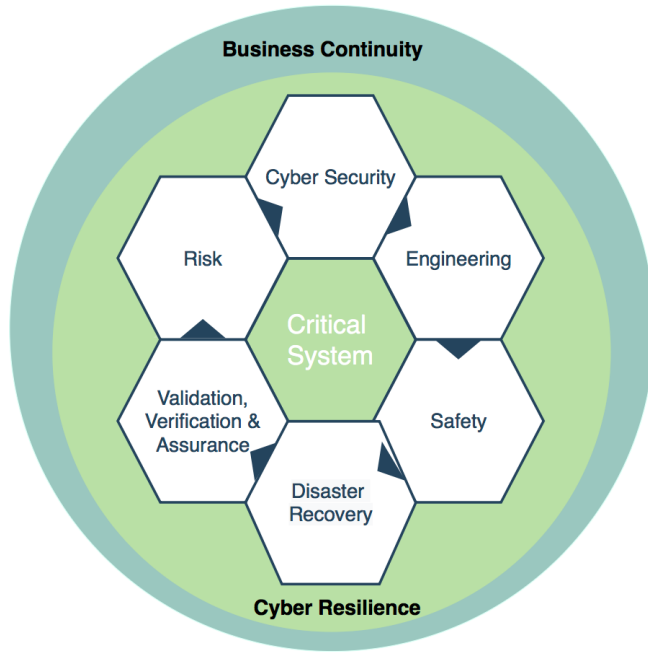
The next section summarises the gaps in literature in a problem statement.

### 3.6 Problem Statement and Chapter Summary

Quantitatively measuring Cyber Resilience in Industrial Control Systems (ICS) is a complex and evolving field of research. There are several current gaps in research including:

- Lack of consensus on what Cyber Resilience means in the context of ICS: There is no commonly accepted definition of Cyber Resilience. Different organisations and stakeholders have their own understanding of what it means to be cyber-resilient.
- Insufficient metrics and methodologies to measure Cyber Resilience: There is a lack of standardised and validated metrics and methodologies to quantitatively measure the Cyber Resilience of ICS. The metrics that do exist are often focused on technical measures alone and do not capture the broader organisational or human factors that also impact Cyber Resilience.
- Limited understanding of the impact of cyber incidents on ICS resilience: There is a lack of empirical data and case studies on the impact of cyber incidents to the resilience of ICS. This makes it difficult to develop effective strategies and metrics to improve Cyber Resilience.
- Limited research on Cyber Resilience in manufacturing industries: There is a lack of empirical research on Cyber Resilience in specific industries, such as manufacturing. This is problematic because different industries have different operational and organisational contexts that affect Cyber Resilience.

To address these gaps in research, there have been several efforts to develop new methodologies and frameworks to measure Cyber Resilience in ICS (as described in the previous section). However, overall, there is still much work to be done to improve our understanding in the manufacturing sectors and to develop effective methodologies and metrics to measure and improve a critical manufacturing system. Figure 3-10 represents the holistic role of Cyber Resilience for an organisation:



*Figure 3-10 Holistic overview of Cyber Resilience landscape*

The next chapter discusses the research approach undertaken for this Thesis.

# Chapter 4

## Experiment Design

### 4.1 Introduction

This chapter details the specific procedures and techniques that were used to gather and analyse data to address the research questions. It sets out both qualitative and quantitative methods of data collection (case studies, frameworks, standards and approaches), data analysis/results, simulation environment / experimental setup, description of metrics and tests and finally a summary is offered.

### 4.2 Research Overview

This research approach aims to cover aspects across three of the CR domains namely: 'Physical, Cyber and Organisational, in addition to the five lifecycle stages of resilient systems namely: 'Prevent', 'Withstand', 'Adapt', 'Detect and Respond' and 'Recover' as set out in the NIST CRF discussed in Chapter 3 – Section 3.5.3.1 (National Institute of Standards and Technology, 2021). These stages are also mapped to the 'Plan and Prepare, Absorb, Recover and Adapt' stages as set out in 'The Cyber Resilience Matrix' by (Linkov, et al., 2013) as also discussed in Chapter 3 – Section 3.5.3.4.

It is important to note the limitations of this study in that the focus of this research concentrates on the measurement of a system's Cyber Resilience and therefore excludes the overall organisations resilience (although aspects of this were considered in the case studies) and it also excludes disruption events unrelated to cyber-attacks.

This experiment design is split into four separate phases, which are discussed further below. A schematic index of this high-level methodology is provided in Figure 4-1 for clarity.

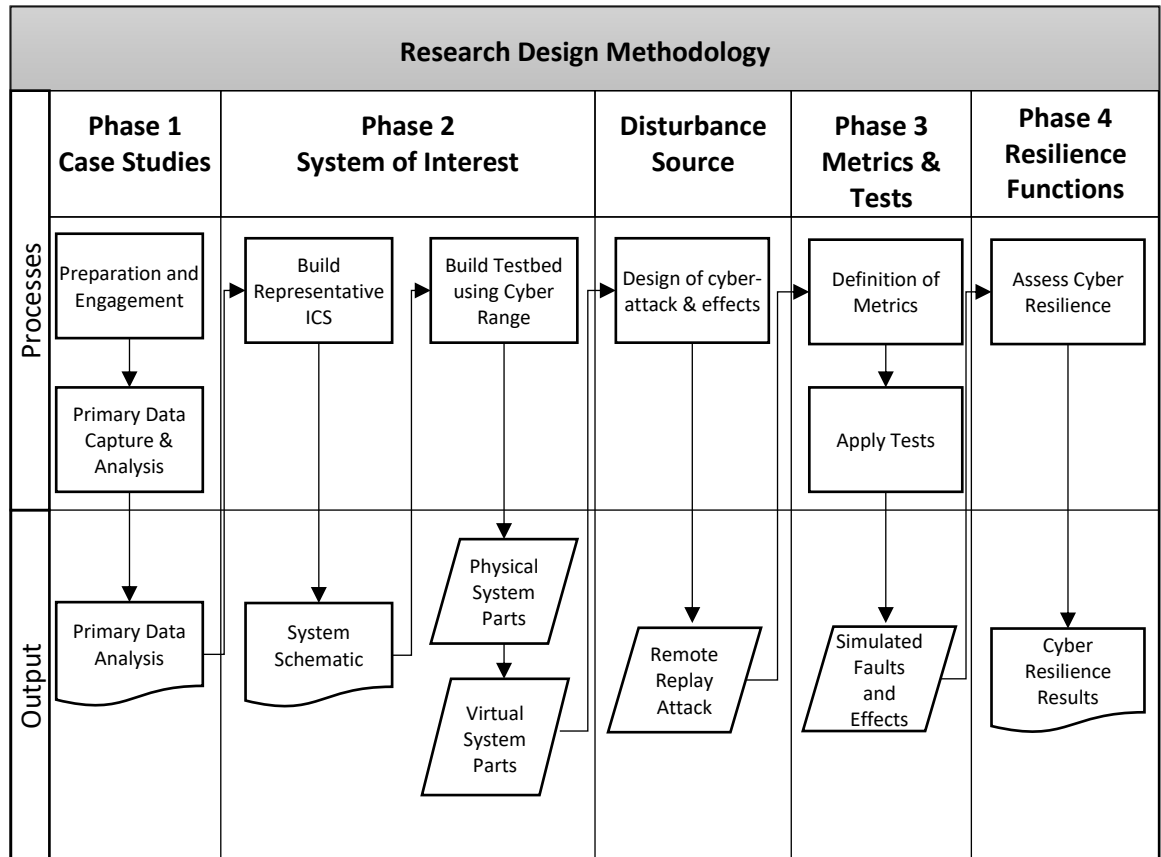


Figure 4-1 Diagrammatic structure of the research design

#### 4.2.1 Phase 1: Case Studies

The **first phase** of the study was to conduct several real-life case studies to obtain primary data concerning the state of OT security in the field. Two case studies at separate anonymous industrial factories were undertaken in collaboration with sponsoring company Thales. The main objective for each case study was to gain an understanding of real-life Cyber Security practices in OT environments baselined against industry best practice maturity frameworks namely (National Institute of Standards and Technology, 2021), (National Institute of Standards and Technology, 2018) and (International Electrotechnical Commission (IEC), 2021). A comparative analysis of the data collected in both studies was performed to identify the top three problem areas determined by the most re-occurring themes captured across all case studies. The case study analysis and results (discussed further in Chapter 5), informed phase 2 of this study namely the design of the testbed model and cyber-attack.



Phase 1 aimed to respond to the following research objectives, as indicated in Chapter 1:

- **Objective 6:** To conduct primary research by way of case studies to collect original datasets from various sources across the industrial manufacturing sectors.
- **Objective 6 (a):** To analyse case study results, with focus on the most critical systems, zones and communications. Establish qualitative baseline maturity levels and provide a series of recommendations through various frameworks and best practice guidance on how each study can enhance their CR maturity.
- **Objective 6 (b):** To clearly identify any limitations with the selected frameworks.

This phase entailed a visit to two separate industrial factories running OT equipment to capture a baseline dataset for each study that was used to inform phases 2 - 4. The data obtained from the two case studies was analysed to critically evaluate each business's Cyber Security practices against a given set of criteria /standard / framework to obtain a baseline maturity score.

Each study was then measured against ISA 62443 (International Electrotechnical Commission (IEC), 2021) standard to obtain a comparative baseline maturity of each study. The first part of each case study applied a best practice cyber security framework (National Institute of Standards and Technology, 2018) and (ISA-62443) to model and provide context on how an organisation viewed CS risk and how those risks were managed. This data was analysed to provide a gap analysis and offer key recommendations to enhance Cyber Resilience in the form of expert opinion and best practice guidance (National Institute of Standards and Technology, 2021).

The success criteria for each case study assessment follows.

- Identify the impact of CS and OT security risks that could result in public or environmental safety issues and/or monetary loss and assess the likelihood of them happening at the site.
- Determine how the site compares to ISA-62443-2-1 (International Electrotechnical Commission (IEC), 2021).
- Collaboration deploying probe and collecting data, in conjunction with the various processes deployed to support these activities.
- Provide a series of pragmatic, actionable next steps which can be easily digested and implemented by on-site personnel to secure vulnerable assets and address immediate security concerns.

#### 4.2.1.1 Selection of subjects

The description of subjects for each case study is shown in Table 4-1.

Table 4-1 Selection of case study subjects

Case Study	Requirement	Activity
<b>Manufacturer of Electronic Components</b>	<p>A detailed inventory of their OT assets and their interconnectivity.</p> <p>An understanding of their current vulnerabilities and threats.</p> <p>Options and recommendations for next steps to achieve comprehensive OT CS</p>	<p>OT Asset Discovery and data flow analysis</p> <p>Mapping Logical and Physical Networks</p> <p>Gap Analysis</p> <p>Vulnerability Assessment</p> <p>OT Security Maturity Check</p>
<b>Ingredient Manufacturer</b>	<p>Gain an understanding of the current cyber-security maturity.</p> <p>Understand how to segregate IT/OT and understand the third-party supplier connectivity.</p> <p>Unlock funding from their Engineering team to find a global cyber-security improvement programme</p>	<p>OT Asset Discovery and data flow analysis</p> <p>Mapping third party connections</p> <p>Gap Analysis</p> <p>Vulnerability Assessment</p> <p>OT Security Maturity Check</p>

#### 4.2.1.2 Scope

The scope of the case study engagements was as follows: OT Local Area Network (OT Network), Process Environment, Filling and Packaging Environment, Integration between OT Network and the IT Local Area Network and OT processes or systems reliant on the IT Local Area Network.

The Technical information and tasks required from each plant prior to the site visit included: documents relating to the plants network architecture, request certain information in the form of questionnaires, Network Diagrams and plant floor plans, a Review session with customer (remote or in person), the configuration of an RSPAN port on a Switch to enable adequate Port Mirroring for the probe and Agree on logistics, a Risk Assessment form completed and signed and finally requirements for any safety clothing or apparatus.

The following outline the limitations of the analysis.

- Findings in the IT Local Area Network (Office Network) that were not related to the OT environment or to the primary operations of the study site were excluded from the results.

#### 4.2.1.3 Data Access Negotiations and Ethics

Obtaining datasets or intercepted traffic to use in test labs for further analysis is most challenging. The freely available datasets, in most cases, are guarded and not always applicable. Data protection and GDPR laws prevent the use of any confidential data, such as what is required from an Industrial network. Cyber related projects require a continuous update to its data feed in respect threat data to understand traffic to optimise machine learning patterns (Li, et al., 2020).

There are several solutions to obtaining relevant datasets. One of which is to visit an actual industrial factory and install a passive monitoring tap with permission to use their data for research purposes. An industrial site visit enables a true observation of data collected and can provide actionable data logs for further testing. A visit will provide net flow observations bringing together a test bed to simulate the data in a virtual capacity. However, this data must still be obfuscated, given its confidential nature. This is often difficult to translate into an academic paper without showing the original data. Additionally, there are also other key challenges to consider.

- There are a limited number of competent professionals with background in both IT, OT and safety-critical systems.
- There is a lack of awareness in the criticality of CS in the OT domain.
- The employee mind set and the belief that ICS has no relation to IT.
- The cost may be prohibitive.
- There may be a lack of training.
- There is a lack of mutual understanding of what CR means.
- Stakeholders may have a false sense of security surrounding safety systems.
- People are often unwilling to accept change.

#### 4.2.1.4 Questionnaires

Any data that was not collected during the assessment was collected via the form of questions. An example of such questions and the topics discussed at each plant is given in Figure 4-2.

**Organisation Name :**

**Site Name :**

**Your name :**

**Role:**

**email:**

Section	Sub-section	21 Total Questions	21 Questions Remaining	
Organisational security measures	Security awareness training	1	1	Start
	Supplier management	1	1	Start
	Physical access Control	1	1	Start
Configuration management	Asset inventory	1	1	Start
	System documentation	1	1	Start
	Change control	1	1	Start
Network and communications	Network security	1	1	Start
	Wireless communication	1	1	Start
	Remote access	1	1	Start
Component Security	Device security	1	1	Start
	Removable media	1	1	Start
	Malware protection	1	1	Start
	Patching and Updates	1	1	Start
User Access Control	User logins	1	1	Start
	User permissions	1	1	Start
	Password protection	1	1	Start
	Authorising Access	1	1	Start

*Figure 4-2 Case study questionnaire (example)*

The next section discusses the case study methodology.

#### 4.2.1.5 Case Study Methodology

A high-level overview of the case study process is given in Figure 4-3.

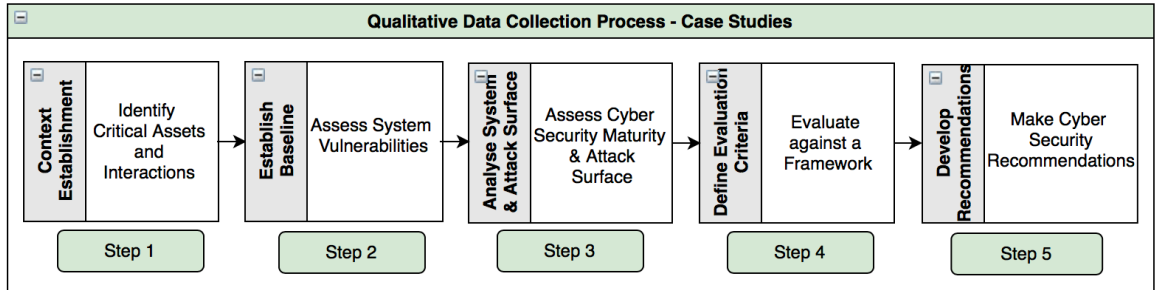


Figure 4-3 Case study steps

The steps taken were:

- i. Identify the critical assets and components: To apply CR to an ICS, you must first identify the critical assets and components that need protection. This could include sensors, actuators, controllers, networks, computers and other components used in the control system.
- ii. Assess system vulnerabilities: Once the critical assets and components have been identified, the next step is to assess the current vulnerabilities of the system. This includes analysing system inputs and outputs and looking for signs of exploitation, intrusion or malware infection. Additionally, system performance can be monitored for any changes or anomalies that could indicate a security issue or inadequate CR.
- iii. Recommend security enhancements: After the system vulnerabilities have been identified, the next step is to recommend security enhancements to minimise the risk of exploitation. This includes hardening systems, patching flaws, implementing defence in depth strategies, controlling access to the system and ensuring privileged users have secure access rights.

A more granular diagrammatic structure of the case study methodology is provided in Figure 4-4 for clarity.

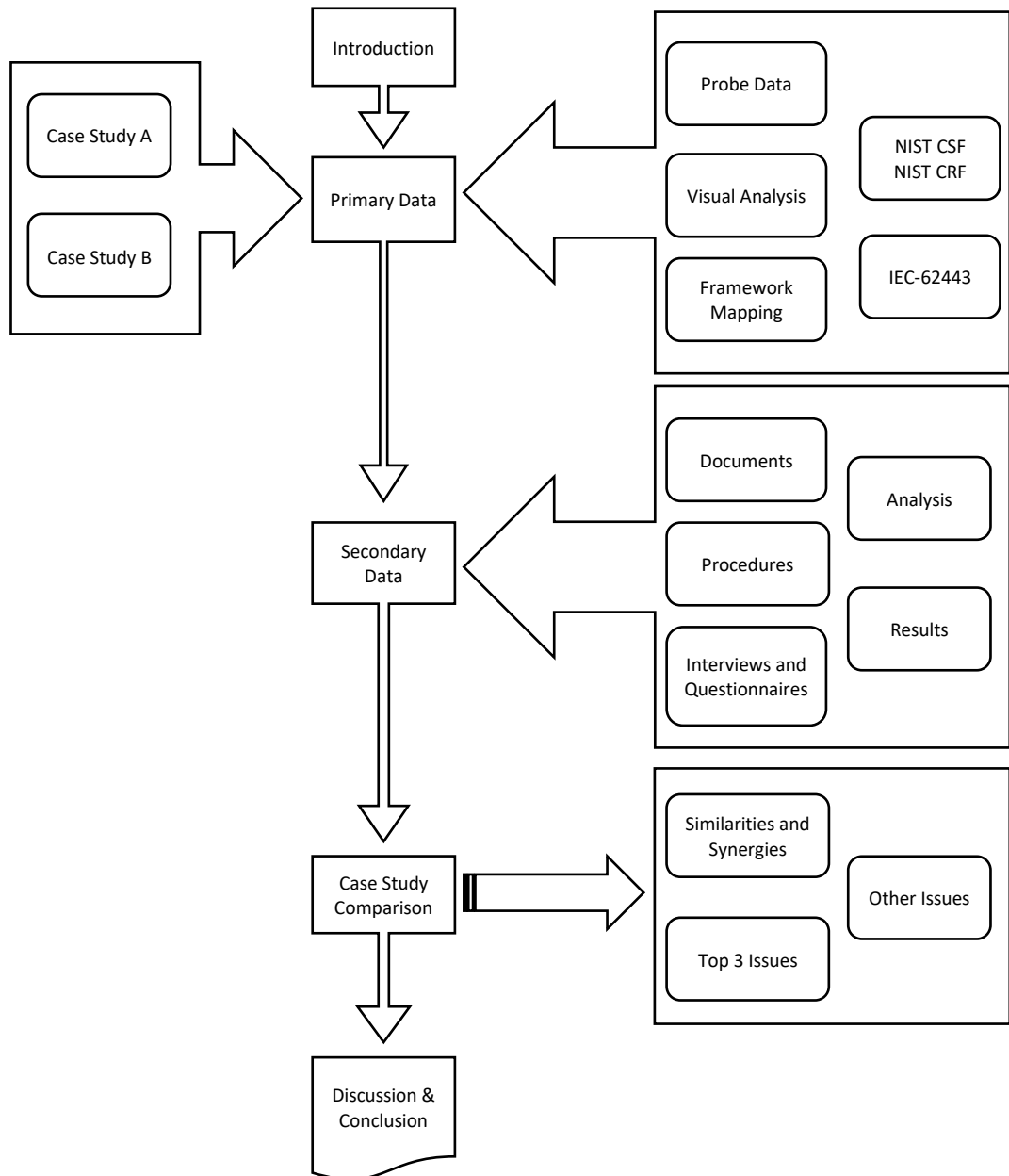


Figure 4-4 A diagrammatic structure of the case study methodology

An entity map is provided in Figure 4-5 below to identify the data variables required during case study assessment to map OT assets and vulnerabilities accordingly.

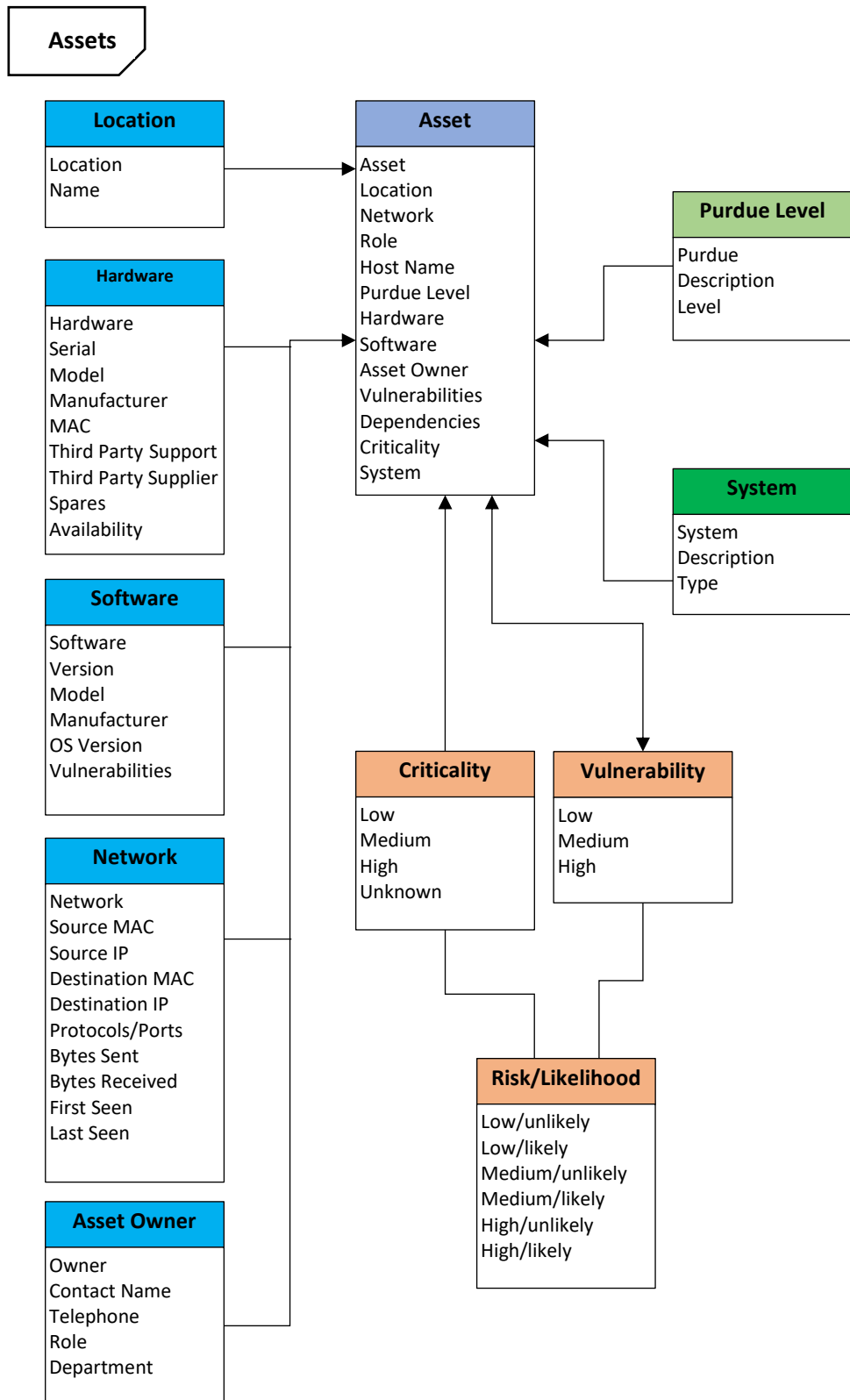


Figure 4-5 Case study data entity diagram

The framework selected to evaluate each case study varied slightly and is therefore discussed in greater detail in each of the case study sections in Chapter 5.

#### 4.2.2 Phase 2: Testbed Design

The **second phase** was the design of an accurate testbed model based on a representative manufacturing system, this included the approach, the physical and virtual components of the test bed, the logical process control configuration and the systems interlinked dependencies and data flows. The physical test bed and simulation set up description and finally the description and design of the disturbance source scenario namely a remote cyber-attack. This phase of the study aimed to respond to the following research objectives, as indicated in Chapter 1:

- **Objective 5:** To design and build a representative physical test bed emulating a critical manufacturing system informed from case study observations.
- **Objective 5 (a):** To Develop a cyber-attack to target the representative system, informed by case study evaluations.

##### 4.2.2.1 Testbed Approach

The resilience assessment of an industrial manufacturing system involves incorporating various models and components. This includes, the cyber elements, the physical elements and the human or organisational elements. Understanding the holistic view of these components and their interactions is crucial for generating scenarios and designing safeguards in a resilience assessment (Leveson, 2020). The data elicited from the case studies covered much of the cyber and organisational elements, touching on some human aspects also. The testbed focuses on the physical and human elements, although the cyber elements are also touched on.

As set out in Chapter 3, to appropriately design a testbed that incorporates the system components necessary, Leveson's safety engineering approach was considered (Leveson, 2020) (see Figure 4-6). This approach was used to inform the design specification of the testbed.



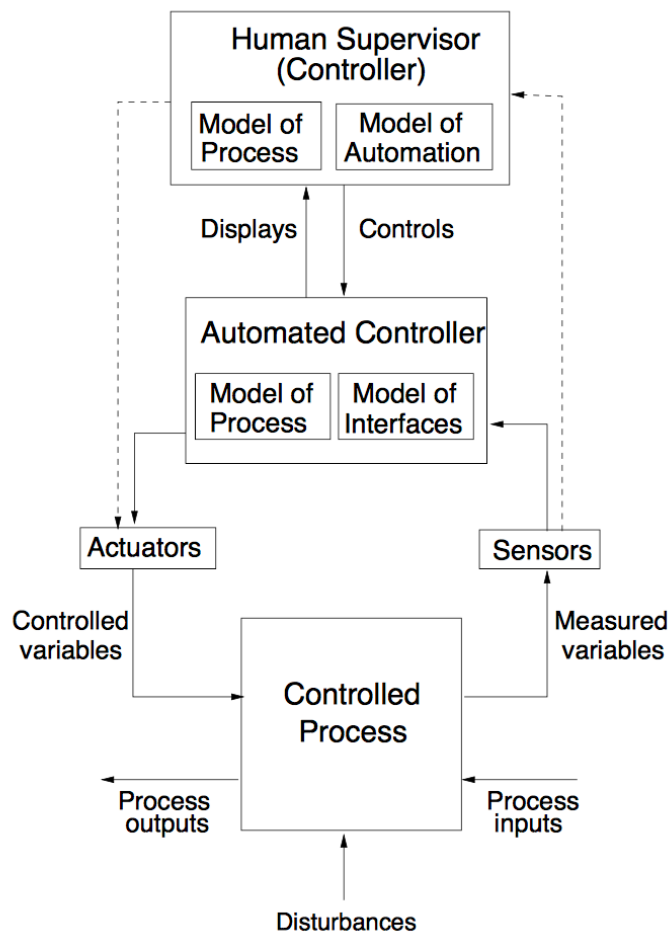


Figure 4-6 The human controller model adopted from (Leveson, 2020)

A model frequently used in the field of Safety Engineering is the Human Controller Model (Leveson, 2020), which considers the human controller state and the sensors employed that gather relevant information about the system and its process. This information is then used by the automated control algorithm (in this experiment we refer to this as the PLC) to determine its behaviour. Additionally, other environmental inputs may also need to be considered, such as room temperature information for example, as this input may directly affect the automated controller without passing through the human controller.

In complex systems, multiple controllers may share control responsibilities, leading to potential conflicting commands and inconsistencies between models. The transmission of information between the automation and its supervisors is essential as any flaws in this transmission can impact the scenarios and resilience assessment. Furthermore, there may be direct changes made to the controller changing its initial design without the knowledge of the other human controllers, posing safety and security concerns.

Generating control actions involves integrating information from various models, external factors and or commands from other controllers. Clear delineation of control responsibilities is vital to avoid confusion and hazards. Identifying unsafe control actions and the associated context helps in limiting the number of causal scenarios and guides the design of the testbed architecture. Additionally, a human controller may interact directly with the controlled process in certain systems, bypassing the automation.

Analysing the controlled process involves considering various factors that can contribute to a changed or undesired state. The state of the controlled process, such as the temperature of a vessel or speed of the inverter is a key aspect. Changes in the state of the controlled process are influenced by its components or variables. Failures or degradation of the hardware components can lead to undesired states, including failures of control devices or other hardware. External disturbances, such as weather or environmental factors such as electricity faults, can also affect the process and create undesired affects.

Maintenance activities or the lack thereof can also influence the process. Automated controllers provide control actions to actuators, which in turn affect the state of the controlled process. Problems in the control path, such as actuator failure, communication or transmission issues, can lead to undesired states. Additionally, the feedback path, involving sensors that provide information about the process state to the automated controller, can also have impact due to transmission problems or sensor failure. The automated control algorithm is responsible for generating control actions and maintaining accurate information about the process state and any external factors.

With these considerations made, an overview of the testbed design and setup is provided in the next section and discussed in detail in Chapter 6.

#### 4.2.2.2 Testbed Setup

Phase two also defines the experimental setup created to mirror the architecture of a representative system (identified during Phase 1 of the case studies) of which includes three further sub-sections: Testbed Description (System of Interest), Physical and Logical components, including the cyber range integration and finally the cyber-attack design. A diagrammatic structure of this phase is given in Figure 4-7.

### Simulation Methodology

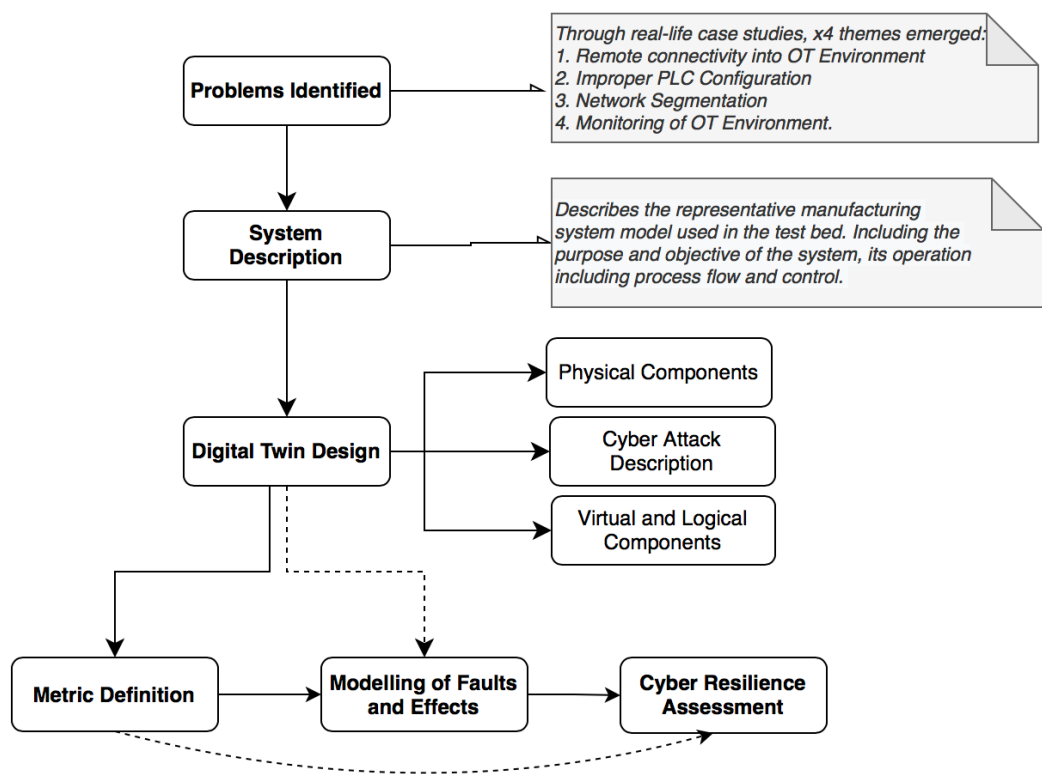


Figure 4-7 Diagrammatic structure of the simulation methodology

Each of the above phases are described further in Chapter 6. The next section discusses the specification of the metric parameters and test conducted in this testbed.

### 4.2.3 Phase 3: Definition of metrics and specification of tests

The **third phase** was the definition of selected metrics and description of the tests performed to measure performance of nominal operating scenario and disrupted operating scenario before and after CR enhancements were made, through the modelling of a cyber-attack and its causal relationship to faults and effects on the representative system (illustrated in Figure 4-8).

This phase of the study aimed to respond to the following research objectives, as indicated in Chapter 1:

- **Objective 5 (b):** To define a series of metrics to quantitatively measure Cyber Resilience on a representative manufacturing system in the event of a cyber-attack.
- **Objective 5 (c):** To implement and test simulation and modelling techniques to determine if the metrics and approaches defined enable a manufacturing system to achieve sustainability in a degraded situation.

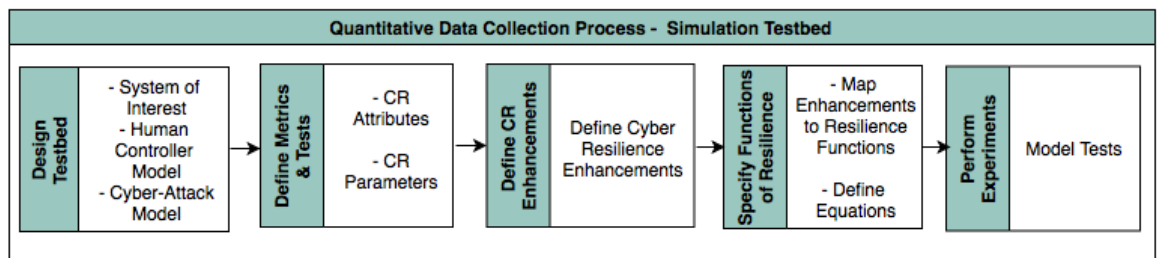


Figure 4-8 Quantitative data collection process - research approach

### 4.2.4 Phase 4: Functions of Resilience

The **fourth phase** was the CR results, whereby resilience metrics are given based on the time taken for the system to withstand, respond and restore functionality. The approach for measuring the functions of resilience is given in Figure 4-9 and Figure 4-10.

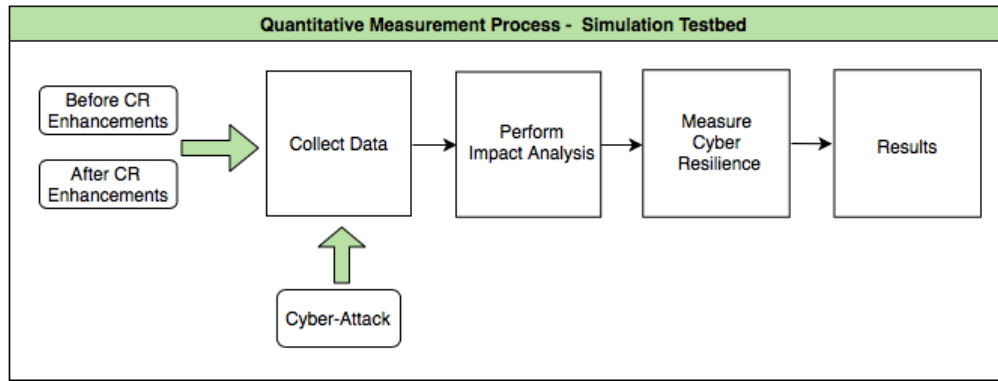


Figure 4-9 High-level quantitative measurement approach - testbed

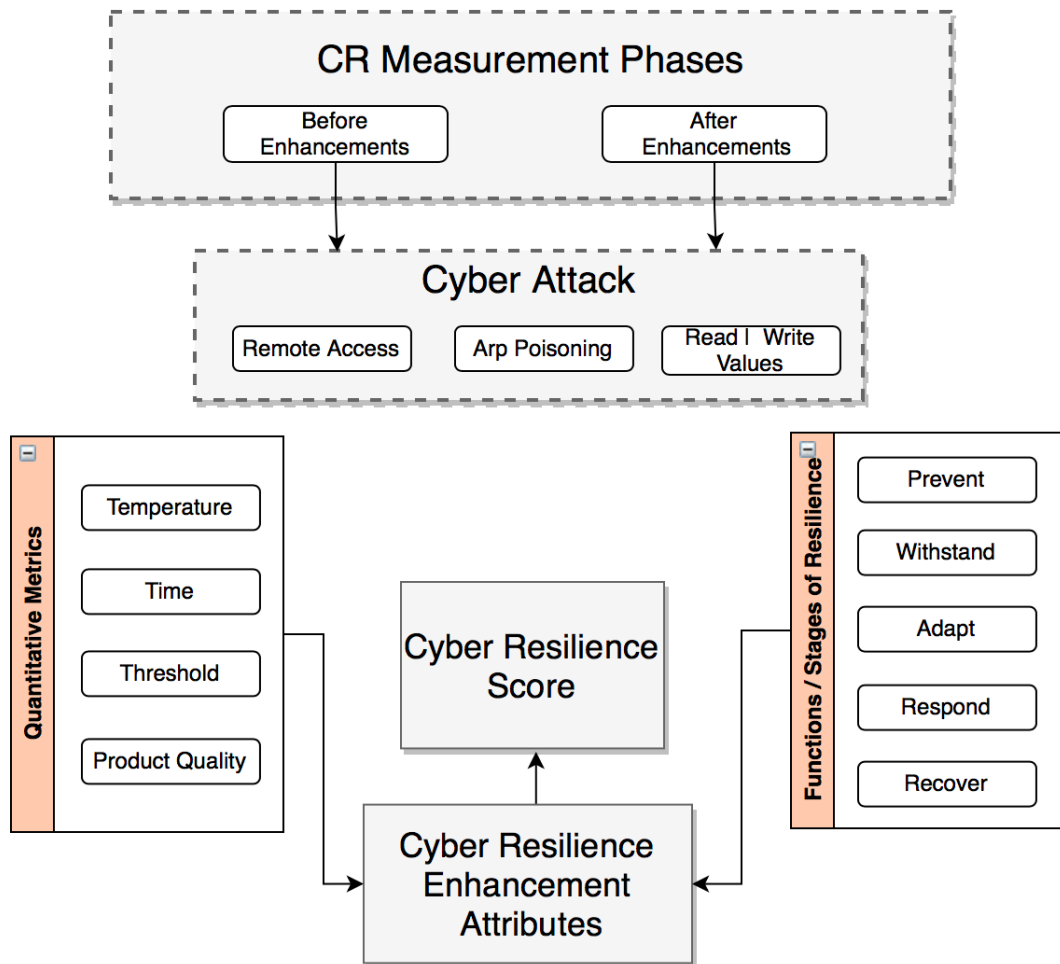


Figure 4-10 Functions of resilience approach

This phase of the study aimed to respond to the following research objectives, as indicated in Chapter 1:

- **Objective 5 (d):** To analyse, record and discuss the results.

### 4.3 Chapter Summary

This chapter detailed the specific methods used to gather and analyse data to address the research objectives. It set out the methods of data collection including the case studies, frameworks, standards and approaches, the representative system and its simulation environment.

The next chapter discusses the analysis and results of the case studies conducted, of which informs the simulation and testbed set out in Chapter 6.

# Chapter 5

## Analysis of Case Studies

### 5.1 Introduction

This section is organised as follows. Section 5.2 presents case study A and Section 5.3 presents case study B, with associated approach, results and discussion. Section 5.4 discusses all case study observations comparing the collective data results and finally offering a concluding summary in Section 5.5.

### 5.2 Phase 1- Case Study A

This section presents a case study analysis of a manufacturing plant assessment drawing on key themes from the NIST literature. The study presented in this case assesses the contribution of the NIST Cyber Security and Cyber Resilience framework (National Institute of Standards and Technology, 2021) and offers findings derived from a case study of an industrial plant consultation undertaken with the Thales Group. The case study draws on key themes that appeared from the literature to analyse Cyber Security gaps, to what degree constructs can be adopted to improve CR and to determine if an evaluation of the results could provide a measure of an organisation's resilience. The presented case study and conclusions drawn afford a baseline for future research into Cyber Resilient improvements.

#### 5.2.1 Data Analysis

The following section outlines the Cyber Security analysis performed for this case study. The analysis is based on the (National Institute of Standards and Technology, 2021) framework (discussed in Chapter 3 – Section 3.6.3.2) and tailored to the organisation through use of other frameworks and standards, such as the Purdue Model and NIST CNI guidance (also discussed in Chapter 3) to evaluate the outcome. The study focuses on the business mission, its OT

infrastructure, it's current cyber risk posture and sets out the recommendations provided to the customer.

The following sections provide a high-level analysis of an industrial factory belonging to a globally established company with presence in multiple countries. The business (anonymised to protect their identity) manufactures products used in the Aerospace and Defence industries as well as many other industrial marketplaces.

The following sections describes the approach, data analysis and results of case study A.

#### 5.2.1.1 Step 1 – Context establishment

This step is twofold.

- I. First, the assessor enters the planning stage, considers the scope of the study and identifies the stakeholders.
- II. Second, the assessor moves on to the data collection stage where personnel are interviewed, OT Network architectures/floor plans are reviewed, the connection of passive monitoring equipment is established and other metrics found during a physical walkthrough such as configuration assessment of factory end points is documented (summarised in Table 5-1).



Table 5-1 Data types collected.

Architectural Analysis	
System Field Parameters - Metadata:	<ul style="list-style-type: none"> <li>-Asset Reference (e.g., 001)</li> <li>-Asset Type</li> <li>-Criticality</li> <li>-Location Reference</li> <li>-Location Name</li> <li>-IP Address</li> <li>-MAC Address</li> <li>-Role</li> <li>-Manufacturer</li> <li>-Model</li> <li>-Host Name</li> <li>-Firmware V</li> <li>-OS Version</li> <li>-Client Protocols</li> <li>-Server Protocols</li> <li>-Purdue Level</li> <li>-Serial Number</li> <li>-Description</li> <li>-VLAN</li> <li>-Network Location (If known)</li> <li>-Protocol/Service, i.e., Modbus Eth/Ip</li> <li>-Date/Time</li> </ul>
Risk Value Parameters (Critical to business operations): Vulnerability Assessment Parameters:	<ul style="list-style-type: none"> <li>-High</li> <li>-Medium</li> <li>-Low</li> </ul>
Log data variables criteria:	<ul style="list-style-type: none"> <li>- Timestamp</li> <li>- Asset ID</li> <li>- Title / Event</li> <li>- Impact level</li> <li>- Sensor / Trigger</li> <li>- User (optional)</li> <li>- Unique Identifier</li> </ul>

### 5.2.1.2 Step 2 - Data Examination and Gap Analysis

Analysing the data collected in Step 1 established a baseline and identified the gaps in cyber resiliency that may directly cause harm to the organisation. An analysis of data sources contributed to understanding how the customer’s OT communicated with their IT and external networks including third party suppliers and maintenance contractors. An OT vulnerability assessment for each of the assets was completed to determine how likely they could be targeted by Advanced Persistent Threat, followed by a risk assessment (National Institute of Standards and Technology, 2018) of critical assets to determine their Purdue level and value to the business. Figure 5-1 shows the total number of OT and IT assets.

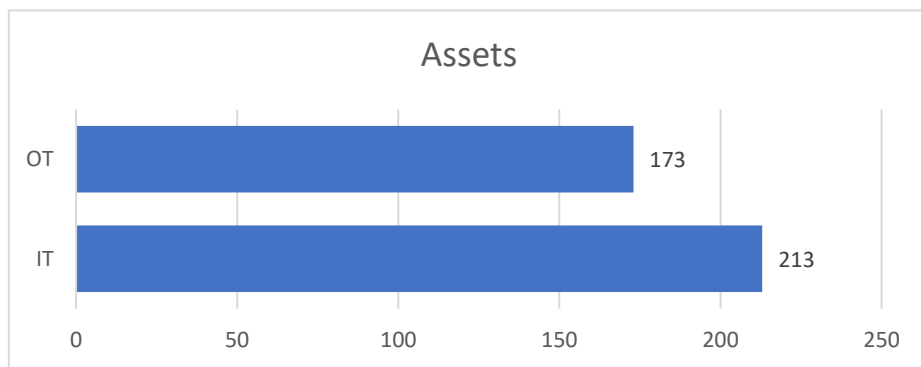


Figure 5-1 OT Assets to Purdue Level

Each OT asset is mapped to its Purdue level (shown in bold) by system type (see Table 5-2).

Table 5-2 Asset Type to Physical Location Mapping

Purdue Level	Room Location																				Total			
Asset Location Asset Role	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	Total	
<b>LEVEL 0</b>						2			1			1	4		1	1	3		1		4	3	<b>21</b>	
Scale						2			1			1	2			1	2					3	12	
Sensor													2		1		1		1		1	3	9	
<b>LEVEL 1</b>				2	5			3		1	1				1		1			1	1	2	4	<b>22</b>
PLC				2	5			3		1	1				1		1			1	1	2	4	22
<b>LEVEL 2</b>	1	1			2	2	1		2			2	4	1			1	1		2	4	2	<b>26</b>	
HMI	1	1			2	2	1		2			2	4	1			1	1		2	4	2	26	
<b>LEVEL 3</b>		1	10																				<b>11</b>	
Application Server			1																				1	
EWS			2																				2	
Historian			2																				2	
Printer		1																					1	
Terminal server			5																				5	
<b>LEVEL 3.5</b>			2		1																		1	<b>4</b>
IP Camera																							1	1
Switch			2		1																			3
<b>LEVEL 4</b>			1																					<b>1</b>
Gateway			1																					1

### 5.2.1.3 Step 3 - Mapping Logical and Physical Networks

A logical and physical topology arrangement of assets provided a graphical representation of critical assets and data flows (shown in Figure 5-2). The logical topology representation classifies the network and illustrates the subnets and traffic flows. Each asset is identified (where possible) with their criticality to business, host names, IP addresses and their roles with any notable traffic communications highlighted in red (see below). Note the topology drawing is for visual understanding only and is purposely obfuscated to protect the identity of the organisation.

Using the data triaged in stages 1 and 2, the Logical Network Infrastructure is mapped to a physical location for each asset (see Table 5-3). The physical topologies mapped each asset to the geographical location using the business's floorplans (not included to protect the identity of the customer).

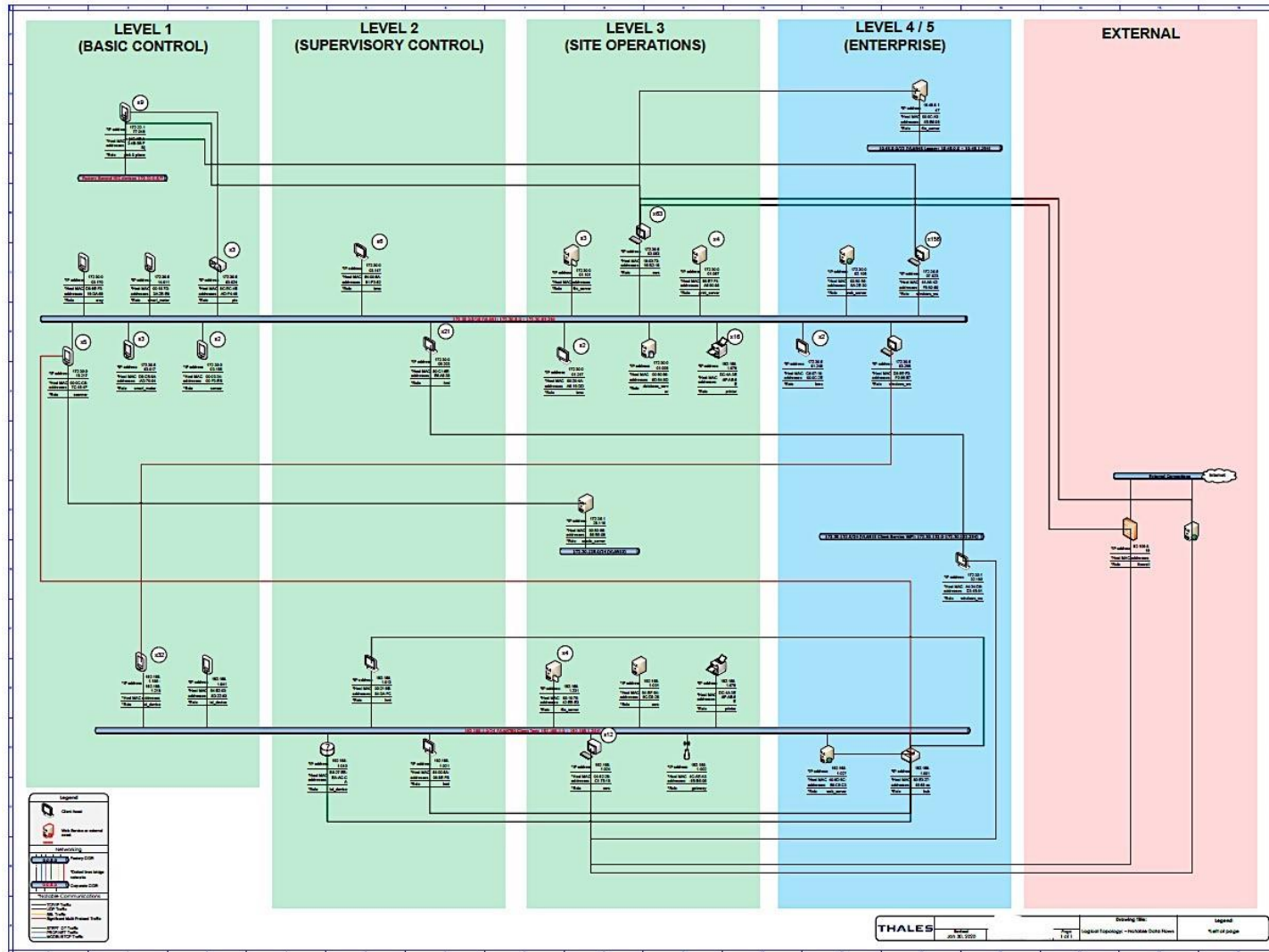


Figure 5-2 Logical Topology with notable traffic concerns highlighted in red.

Table 5-3 Physical Topology - Mapping assets to geographical location

Location	Asset Ref	Description
A	243	Engineer Workstation
B	001	Gateway
	002	Switch
	003	PLC
	100	Application server
	104	Terminal server
	105	Historian
	106	HMI
	107	Sensor
	199	EWS
	200	Firewall

#### 5.2.1.4 Step 4 - Define Evaluation Criteria

Other elements of the Operational business processes were audited to complete the evaluation. The results presented each of the findings as prioritised risks. The associated mitigating recommendations and a set of objectives needed to drive a cyber resiliency approach were assessed incorporating the data identified from the gap analysis and discovered during the site walk-round which summarised:

- Operational issues (e.g., failed Modbus connections, device restarts).
- Security Threats (e.g., port scans, login attempts).
- Networking problems (e.g., unstable connections, unanswered requests).
- Connection attempts to public IP addresses.
- Contextual analysis of information.
- Deep dives into any areas of concern.
- Samples of single assets of high risk.

#### 5.2.1.5 Step 5: Develop Recommendations

Please refer to Section 5.3.2.2 of the case study data analysis and results for the findings.

## 5.2.2 Baseline Results

This section is an objective view of what security controls are in place at the factory using the (National Institute of Standards and Technology, 2018) baseline set of activities framework. This framework provided a baseline control set to perform a gap analysis. Due to the lack of any comprehensive CS risk assessment analysis, this section does not make any determinations as to if such controls are necessary, just if they appear to exist and how they are used.

### 5.2.2.1 Cyber Risk Analysis – Baseline Control Set

#### **Asset Management**

A functioning system exists based on an excel inventory. Many of these required human interactions to ensure data integrity is coordinated and is potentially prone to data inconsistencies. The list of recorded assets does not include asset priority ratings based on criticality, business value, or supply chain availability (given the number of legacy systems). No overarching strategy for managing and or maintaining the configuration of assets was apparent. There did not appear to be a list of external dependencies or critical business assets – this could mean that they either have none or that a determination has not been conducted. There did not appear to be a formalised process for ensuring a consistent supply of engineering spares, conversely the onsite teams appeared both knowledgeable and capable of ensuring critical assets could be replaced and maintained. The process was expert driven rather than documented and process driven. There was no clear RACI structure in place for CR; primarily due to the fact it was not a significant concern for the factory.

#### ***Business Environment***

The staff and organisation were clear about their role in the successful operation of their business. The mission for the factory and staff appeared to be well articulated and of the people talked to, they agreed on similar missions and objectives (e.g., on time delivery in a safe and reliable manner). Dependencies and critical functions of systems were identified by the customer and managed from a physical and supply chain perspective, but not clearly from an information or digital perspective. Resilience was not a key priority or addressed maturely from a digital or cyber perspective. Physical resiliency within the factory was possible through component/system & production line reuse. Although there is awareness about the importance of an OT cyber resiliency approach, a consistent approach had not been adopted. There is no standalone separate network environment for OT infrastructure.

### *Governance*

It was acknowledged that no governance or risk management process for OT CS had been put in place. Cyber was treated in a similar fashion to other large corporate risks and managed through the same management process. The roles & responsibilities for CS seemed to align with those for the IT operation of the factory (e.g., cyber was not treated any differently to other engineering aspects). It was clear who staff would communicate with should an issue arise with the factory (cyber or otherwise). There was acknowledgement that specific CS legislative or regulatory requirements are not tracked at the factory level, instead it was assumed that the corporate IT on / off-site were likely to provide that info to the factory.

### *Risk Assessment*

There is a process in place to identify, track or respond to asset vulnerabilities for those assets managed by the corporate AV. This does not cover unknown or unregistered devices onsite that client IT are unaware of. There is no formal method of receiving cyber threat intelligence – the factory relies on corporate IT to inform them of any issue. But there was no method of tracking response to that issue. And it was acknowledged that IT does not provide threat or vulnerability intelligence for OT assets. No business-aligned OT cyber continuity plan has been defined. There was no formal method of reviewing threats and their potential business impacts (cyber or otherwise). Therefore, new risks are not consistently identified, scored, or addressed. Cyber risks are only identified or prioritised when informed by corporate IT.

### *Risk Management Strategy*

There is no formal CS risk management process or strategy, beyond the corporate risk management approach. The organisational risk tolerance is determined on an ad-hoc basis. The approach to risk seems to be divorced from the wider business.

### *PROTECT*

#### **Identity Management and Access Control**

Identity is not comprehensively managed within the factory infrastructure. Most of the access is through shared role-based access, limited audit capability to identify critical actions carried out by an individual. Access to critical resources is limited to IT staff. There is external remote access into the facility. Enterprise remote access is limited to IP addresses through Firewall rules. There is limited network segregation through a DMZ. The firewall is managed remotely by another site through an external software defined firewall on the external to internal interface and controlled through a software/VM firewall on the internal to external interface. A zone & conduit approach

to network integrity is not in effect. Identities are handled through corporate access to assets and first-hand knowledge of those people. Access to engineering laptops is controlled through informal process. There did not appear to be any central authentication OT management solution or multi-factor solution – especially when it came to OT assets. Everyone has access to the factory assets and any information critical assets reside on the IT enterprise network.

### **Awareness and Training**

There is no regular or formal training on CS from an OT or factory perspective, just regarding the corporate IT Roles & responsibilities are inherited from existing work structures rather than explicit RACI charts. There is some engineering reliability on external third parties. Senior executives understand their roles and make themselves available to the team. There are no dedicated CS personnel for OT.

### **Data Security**

There did not appear to be any whole disk encryption products in use. Therefore, within the factory there was limited to no data-at-rest protection. There did not appear to be any data-in-transit protection in use – except where the default protocols/configurations use it. There was limited to no ability or approach to detecting or controlling for information leakage, disposition, or removal of information from the factory domain. There was no formal method for checking the integrity of vendor supplied software/firmware.

### **Information Protection Process and Procedures**

The concept of least functionality is not routinely or consistently deployed. There did however appear to be a consistent or deliberate use of baseline configurations from the IT side. There is a formal approach to configuration change management. This is routinely handled through IT coordination between individuals and logged via their IT Helpdesk. There is no comprehensive or tested method for backups. There appeared to be confusion between the IT teams about which critical assets were being backed up. There did not appear to be a well-known and followed process for data destruction when not required. Protection technologies and processes are not regularly checked or validated. Response plans and recovery plans do not include cyber or cyber incidents directly.

### **Maintenance**

Maintenance is performed by engineering experts as required. There is a ticketing system in place to log and track issues. Remote access for maintenance is permitted as discussed.



### **Protective Technology**

Audit logs are not reviewed according to business needs or risks. Removable media is not currently restricted but plans for this are underway. Technology resilience is in place for some critical assets (e.g., core switches, virtualised servers) – but the conditions and resiliency requirements driving them were not clearly articulated.

#### *DETECT*

### **Anomalies and Events**

Security event logs are not collected on the OT equipment. There was an absence of an event monitoring and reporting systems. Therefore, a baseline knowledge of expected data flows & volumes was not known. There is no vulnerability management process or solution for OT. There was an expert led approach to reviewing events and their impacts.

### **Security Continuous Monitoring**

There is an absence of automated vulnerability assessment (VA). There did not appear to be a regular or routine review of critical security functions such as credential reuse/compromise. There was no detection or audit of security credentials to detect unauthorised creation or use. There was some use of anti-malware solutions in place to help detect the deployment of malicious code. There was no regular audit for the use of unauthorised connections, devices, or software.

### **Detection Processes**

Security IT related management procedures for firewalls, security appliances, network segmentation and intrusion detection are managed by the IT Network to authorise access and control information flows from and to networks. However, no security is in place on the OT LAN Network. The OT infrastructure is manually maintained, system by system. Detection processes do not appear to be regularly tested, evaluated or continuously improved.

#### *RESPOND*

### **Response Planning**

No network security policy in place for the OT Network No procedure or guidelines. There have not been any significant cyber issues – therefore response plans have not been tested in anger.

### **Communications**

No adequate follow-up actions or playbooks are defined for indications of inappropriate or unusual activities. Staff rely on IT and engineers to report anomalies in an ad-hoc manner. Information sharing between stakeholders (internal & external) is done in an ad-hoc manner.

**Analysis**

Ad hoc risk analysis and use of measures by individuals. No incidents have occurred requiring forensic or impact analysis.

**Mitigation**

No incidents have occurred requiring containment or mitigation. New vulnerabilities are not mitigated but may be documented as accepted risks.

**Improvements**

Response plans have not been required to be enacted for OT, therefore no lessons learned to be included.

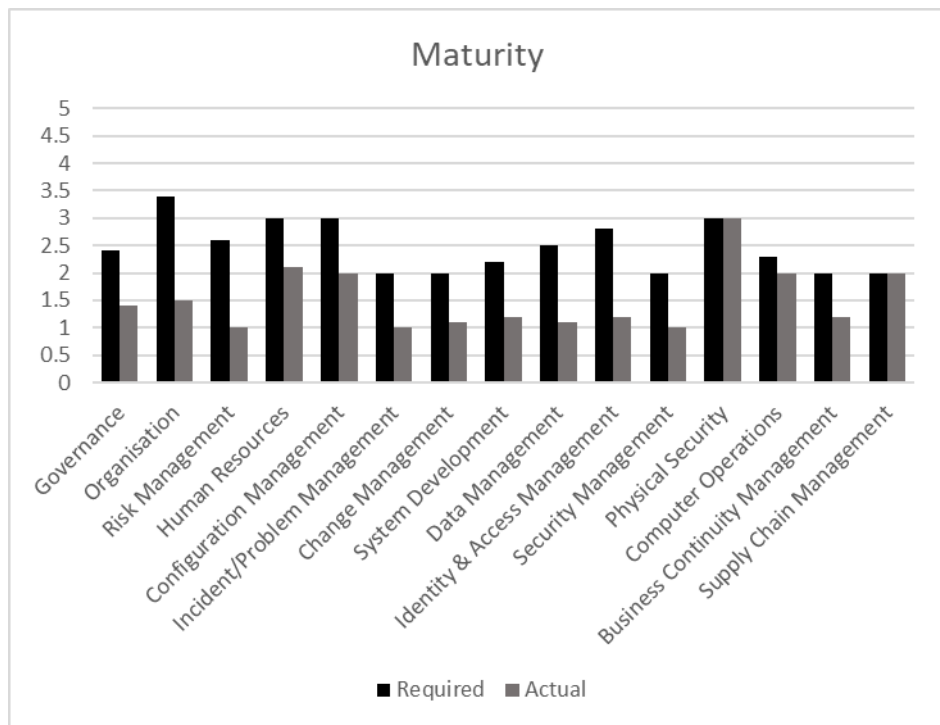


Figure 5-3 Summary of Required vs Actual Maturity Level Indications per Area

Figure 5-3 provides a summary comparison of maturity levels by area. The next section outlines examples of vulnerabilities and practices discovered during the analysis that represent weaknesses in the organisations approach to CR.

*Threat/Impact Analysis*

The described vulnerabilities (shown in Table 5-4) were assessed based on whether there is a reasonable prospect of exploitation. They represent avenues for compromise or use as part of a wider campaign. Each impact rating is scored based on an assessment of an attacker’s ability to turn that finding into a severe, major or minor impact to factory operations. Each rating is based on expert opinion and, although impartial, it should be validated by a wider risk and impact assessment that includes on-site factory personnel.

*Table 5-4 Vulnerability Assessment*

Area	Control	CR Weakness	Impact to Business	Impact Rating
Architectural Analysis	Flat layer two network architecture	No network segmentation or defences within the OT factory network.	If one asset is compromised – every asset can be compromised. It would be quite easy to access an OT system in the event of an untargeted or enterprise compromise. Should any part of the interlinked assets fail (such as loss of power) it could impact other parts of the OT network. The introduction of malware into the factory would not be inhibited from spreading throughout the network to other HMIs/x86 devices and even to the IT enterprise assets.	Severe
Programmatic Analysis	Inconsistent use of software versions, or hardware.  AV Malware control	There are multiple OS versions, types and software builds in use throughout the factory including Windows XP.  There is good use of end- point protection controls in place such as AV however not been deployed to all assets.	Untargeted attacks such as crypto malware leverage well-known software vulnerabilities. The wide range of OS versions and legacy software make the factory pre-disposed to having significant compromise, should any be introduced accidentally.  Coupled with the wide variety of legacy OS’s & applications, the ability for malware (even widely known & signature friendly instances) to spread is high once compromise occurs. Endpoints without AV are extremely vulnerable to well- known attacks.	Major

	Windows XP used as HMIs.	Windows XP machines were frequently found to be operating as an HMI to the OT machines.	Blue Keep is a recent but well publicised vulnerability in Microsoft's RDP service (CVE-2019-0708). Patches are available for legacy OSs including XP. It is advised that the systems are patched, as XP machines are critical within the factory and exploits are in the wild.	Major
Operational Analysis	Good use of change control.	There does appear to be a patching / configuration change management approach in place. However, OT assets were running versions of firmware that contain known vulnerabilities.	The wide range of insecure OS systems such as XP makes it quite easy for unsophisticated attackers to use off-the-shelf attack kits to compromise the factory. Regular exploits for much of these systems exist in toolkits such as Metasploit.	Major
	No backup plans	There seemed to be some confusion between what the factory thought was being backed up and what was backed up.  Backups of configuration changes were accomplished through file-sharing over FTP.	Traffic identified to/from a server IP address appear to allow a wide range of services traversing the network to across all VLANs including test to communicate between any device in the factory network.  Whilst this allows file- sharing to occur, it would also allow any compromise of those assets to spread into the OT factory.  This is a typical example of how an exploit such as Eternal Blue (e.g., WannaCry) could spread from the enterprise IT network to the factory network.	Severe
	Reliability on experienced staff	The factory is increasingly reliant on IT staff. Critical information is stored on the enterprise ERP system.	If you cut off or impact enterprise connectivity, then the factory is quickly constrained by what it can do.  Just as with the NotPetya attacks it is clear how a severe impact to enterprise systems would have knock on consequences to the factory operations.	Major

### 5.2.2.2 Recommendations

This section provides observations & recommendations (summarised in Table 5-5) based on what was seen. Note: that no in-depth threat or risk assessment was performed, therefore recommendations are given from an informed point of view, rather than an outcome from a formal risk management process. Overall, it is fair to say that the organisation did have some basic protections in place. However, they had no systemic ability to detect, respond or recover from a cyber-attack and no resiliency to an insider attack or accidental compromise.

Table 5-5 Recommendations

Area	Recommendation	Priority
Strategy	The business should have a defined CS strategy for factory OT infrastructures separate to the IT strategy.	High
Governance	The business should ensure that a clear RACI structure is in place for governing CR and cyber incident response.	High
Risk Management	The business should establish and use a common approach for performing risk identification, assessment and management. This does not have to be in-depth, but it should be consistent to allow for improvement.	High
Security Audit	The business should develop a sufficient security audit plan to measure compliance against the effectiveness of its security controls.  The business should then start to perform regular security audits of its controls and approaches.	Medium
Identity & Access Management	The business should have a user-auditable method for accessing critical systems, consider segregation of duties to reduce the likelihood of single individuals compromising critical processes. Consider restricting the broad access into the factory network, to only those necessary services. Regularly review and validate the rules and authorisations into the factory domain through the Firewall.	High
Change Management	The business should formalise an OT change management process to ensure the current configurations and assets builds are known. This includes OT endpoints such as engineering terminals and HMIs.	Medium
Security Architecture	The business should take a zone & conduit approach to network architecture within the factory. Deploying industrial	High

	<p>firewalls strategically would reduce the ability for a single asset compromise to impact wider sections of the factory.</p> <p>The business should institute a segregation between the factory and enterprise networks. Boundary segregation devices should monitor and restrict services not just IPs through application firewalls.</p> <p>The business should review its network architecture from an OT/IT resiliency perspective and determine if it is sufficient for the business expectations in the event of a cyber-incident and ensure that there are no single points of failure.</p>	
External Supplier Management	The business should ensure remote visitors are strictly monitored for the entire session or restricted entirely from accessing factory machines until more robust security controls are implemented to reduce the potential impact from accidental/intentional infection or data infiltration.	Medium
Threat Intelligence	The business should require factories to include cyber in its high-level threat assessment. Provide an appropriate feed of threat intelligence relevant to the factories and their assets and establish a routine method of reviewing and evaluating that threat intelligence as it pertains to their operations.	Low
Incident Management	Capabilities to react and recover from CS incidents should be routinely tested and exercised. Accidental or insider compromises are assessed to be the most likely cause of cyber incidents. Swift recovery will minimise impacts to operations.	Medium
Business Continuity	The business should require factories to include significant cyber incidents in its business continuity plans, including recovery from APT or other destructive cyber consequence.	Medium
Human Resources	The business should review the limited succession planning and staff backup for key/critical individuals and/or departments.	Medium

### 5.2.2.3 Cyber Resiliency Evaluation

Several techniques, set out in (National Institute of Standards and Technology, 2021), that enhance Cyber Resiliency were selected as recommendations for this case study and outlined in

Table 5-6.

*Table 5-6 Cyber Resilience Evaluation*

Techniques	Approaches	Examples
<p><b>PRIVILEGE RESTRICTION</b></p> <p>Definition: Restrict privileges based on attributes of users and system elements as well as on environmental factors.</p> <p>Discussion: Apply existing capabilities more stringently to deliver a trusted and complete response.</p>	<p><b>TRUST-BASED PRIVILEGE MANAGEMENT</b></p> <p>Definition: Define, assign and maintain privileges based on established trust criteria consistent with the principles of least privilege.</p> <p>Informal description: Trust no more than necessary.</p> <p>Discussion: Separate roles and responsibilities and use dual authorisation.</p>	<p>Implement least privilege.</p> <p>Employ location-based account restrictions.</p> <p>Employ time-based restrictions on automated processes.</p> <p>Require dual authorisation for critical actions.</p>
<p><b>REALIGNMENT</b></p> <p>Definition: Structure systems to meet business missions and reduce current anticipated risks.</p> <p>Discussion: Look for restructuring opportunities related to new assets and any upgrades to current assets.</p>	<p><b>PURPOSING</b></p> <p>Definition: Ensure that cyber resources are used consistently with business function purposes and approved uses, thereby avoiding unnecessary sharing and complexity.</p> <p>Informal description: Ensure that resources are used consistently with mission or business function purposes and approved uses.</p>	<p>Ensure that no resource is designated as trusted unless a business reason justifies it.</p> <p>Ensure that privileged accounts are not used for non-privileged functions.</p> <p>Use allow-listing to prevent the installation of unapproved applications.</p> <p>Use allow-listing to restrict communications to a specified set of addresses.</p>
<p><b>REDUNDANCY</b></p> <p>Definition: Provide multiple protected instances of critical resources.</p> <p>Discussion: Redundancy is integral to system resilience, however, manage carefully to avoid vulnerabilities and increasing the attack surface</p>	<p><b>PROTECTED BACKUP AND RESTORE</b></p> <p>Definition: Back up information and software in a way that protects its confidentiality, integrity and authenticity. Enable safe and secure restoration in case of disruption or corruption.</p> <p>Informal description: Back up resources securely and defend the restore process from adversary exploitation.</p>	<p>Maintain and protect system-level backup information (e.g., operating system, application software, system configuration data).</p> <p>Increase monitoring and analysis during restore operations.</p>

<p><b>SEGMENTATION</b></p> <p>Definition: Define and separate system elements based on criticality and trustworthiness.</p> <p>Discussion: Reduce the adversary's scope for lateral movement or command and control (C2).</p>	<p><b>PREDEFINED SEGMENTATION</b></p> <p>Definition: Define enclaves, segments, micro-segments, or other restricted types of resource sets based on criticality and trustworthiness so that they can be protected separately and if necessary, isolated.</p> <p>Informal description: Separate OT and IT Networks at the very least.</p>	<p>Use virtualisation to maintain separate processing domains based on user privileges.</p> <p>Use cryptographic separation for maintenance.</p> <p>Partition applications from system functionality.</p> <p>Isolate security functions from non- security functions.</p> <p>Use physical separation (air gap) to isolate security tools and capabilities.</p> <p>Isolate components based on organisational mission.</p>
---	--	---

The next section provides the reader with the conclusions drawn for Case Study A.

### 5.2.3 Case Study A - Conclusion

This case study analysis applied key themes from the NIST literature to show CR gaps, highlight to what degree the adoption of its constructs might improve CR and determined if an evaluation of the results could supply a measure of an organisation's CR. Conclusions drawn demonstrate that although the framework did assist with some of the analysis process, the framework's ease of adoption assumes an organisation has a conventional cyber-security foundation; NIST should make this clear within their guidance. Furthermore, the accompanying evaluation process was not sufficient to quantitatively measure the overall CR maturity for this case study. For this reason, the assessor utilised elements of different frameworks and maturity models alongside NIST to evaluate the organisation. Furthermore, it is agreed that there is insufficient research on cyber resiliency measurements (Kott & Linkov, 2021).

The next section will discuss the findings from Case Study B.



## 5.3 Phase 1 - Case Study B

This section presents a case study analysis of a manufacturing plant assessment drawing on key themes from the IEC 62443-2-1 framework. The author, alongside sponsoring company, Thales Group engaged with personnel from Customer B site to perform a Cyber Security risk assessment of their OT environment. Thales used specialist tools to collect and analyse data from the OT systems during normal operation and made high-level observations on how the site addresses specific security topics. These observations were assessed against the CS maturity model described in ISA/IEC 62443, the international standard for Industrial Automation Process Systems, to provide context on how an organisation views CS risk and how those risks are managed. The maturity model is described in detail in section 5.1.2.2 of this report. The presented case study and conclusions drawn afford a baseline for future research into Cyber Resilient improvements.

The Customer B's main objective is to ensure that effective security controls are in place to ensure security and resilience of site operations. Thales use an assessment model based on ISA/IEC 62443-2-1, subsequently referred to as 'the standard' throughout this case study. This has been tailored to suit the scope of the assessment for Customer B.

### 5.3.1 Data Analysis

The approach for obtaining the data in this case study followed the approach discussed in Chapter 4, Section 4.2.1.5. The IEC 62443-2-1 framework (summarised in Chapter 3 and detailed further in Appendix 1) was used for this case study. This framework aims to provide an organisation a means to obtain an objective high-level overview of how their Cyber Security practices compare with best practice guidance. Additionally, it provides Initial recommendations on the steps needed for an organisation to improve.

The main objectives for this study were as follows:

- i. Assess the status of OT security at Customer B site including assessing the OT network, compare best practices and highlight areas of improvement.
- ii. Identify areas of concern that may present a risk of cyber indecent and affect business continuity, based on currently known and emerging threats.
- iii. Provide a series of pragmatic and actionable next steps that can be easily digested and implemented by on-site personnel to secure vulnerable assets and address immediate security concerns.

The scope of the engagement encompassed the:

- OT Local Area Network (OT Network) across multiple VLANs
- OT air gapped, or other, networks
- Integration between assets in the OT network and those in non-OT networks
- OT processes or systems reliant on non-OT resources

### **Limitations**

The Customer B site process environment contained equipment that was not integrated into the network by design. These networks are packages used on the factory floor which were used to fulfil a specific purpose – for example, a collection of devices that make up a machine controlled via a PLC that is not networked. Thales worked with the Engineering and IT teams at Customer B to maximise the data that could be collected to produce a useful high-quality output. However, the data collected does not represent a complete detailed inventory of all OT equipment on site as a large proportion of OT equipment was not integrated into the network and therefore not discoverable by the network probe deployed by Thales whilst on site.

The network structure at the Customer B site consisted of multiple VLANs both at distribution layers and access layers including complex-interconnected links present between different layers of the Purdue model including safety systems, which were outside of the scope of this security assessment. Due to the time limitations on site, only two areas were visually inspected, which presented a challenge from a reporting perspective, as not all production areas could be analysed visually. Non-OT systems (i.e., IT LAN (Office Network) and WAN (Customer B IT networks) observed that did not demonstrate an interconnection to the OT environment or to the primary operations of the Customer B site are not included in this report.

In the report, Thales provide indicative scoring of the security practices observed during the assessment. This scoring is based entirely on analysis of data collected from the Customer B site and the supplementary questionnaires and evidence provided by Customer B staff. Thales's assessment of OT security practices is scored following two systems: the IEC 62443-2-1 Maturity Level (ML) which is used to provide an indication of how the site performs when assessed strictly against the standard (see Table 5-7 and 5-8) and the Thales Scoring Level (see Table 5-9 and 5-10).

Table 5-7: IEC 62443 Maturity Level definitions

Maturity Level (ML)	Description
1 – Initial	Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time may not be able to be shown.
2 – Managed	Documentation exists that describes how to manage the delivery and performance of the capability. This documentation may be in the form of written procedures or written training programs for performing the capability. The discipline reflected by ML 2 helps to ensure that practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3 – Defined	At this level, operational effectiveness of ML 2 can be demonstrated. The performance of a Level 3 practice can be shown to be repeatable over time within the OT.
4 – Improving	Using suitable process metrics, the effectiveness or performance improvements of the process or both, can be demonstrated. This results in a security program that improves the process through technological, procedural and management changes.

In some cases, where referenced, there may have been insufficient data available to enable a reasonable assessment of the maturity level. In these cases, the ML is not scored.

Table 5-8: Maturity level description for Insufficient data

Maturity Level (ML)	Description
NS – Not Scored	Insufficient data supplied by site or obtained through network monitoring to support informed assessment of the maturity level.

As an international standard for managing an OT security program, the scoring ‘maturity model’ defined in IEC 62443-2-1 standard is primarily focussed on an organisation’s policies and procedures. An organisation with good technical practices but requiring better governance may therefore score poorly.

To provide a more granular picture of how the Customer B site is aligned with industry recommended practices, each area in the report has also been scored using the Thales OT scoring system. As a result, scoring is given for assessment in two areas:

- I. Governance (Gov) – Assessing cyber organisational governance i.e., policies, procedures, standards and guidance that formalise the OT CS program and its execution.
- II. Operational (Ops) – The implementation of controls, principally technical in nature, which provide a practical operational security capability and their assessed efficacy.

Table 5-9: Thales OT assessment scoring system

ML	Description
1-Minimal	Gov: The organisation does not appear to have defined governance, or its governance is loosely defined and not formalised or documented. Good practice guidelines for industry are not evident.
	Ops: Appropriate controls to address risk are not evident. Some controls are in place, but application appears inconsistent or ad-hoc, they are not well defined and documented.
2-Partial	Gov: The organisation has defined some governance that describes the security strategy and its delivery. Governance is documented and there is some evidence of alignment with industry good practice although it may not form part of a more widely coordinated company strategy.
	Ops: Some risk controls are defined, documented and applied in practice to provide a foundation of security showing some alignment with good industry practice. However, groups of different controls are not coordinated as part of a broader design for security.
3-Developing	Gov: Governance is well defined, formally documented in detail and follows good industry practice. Governance shows some input from different business stakeholders and considers key factors that enable delivery. There is some evidence that defined governance and practical implementation are coordinated.
	Ops: Risk controls are well defined, documented in detail and applied consistently. Some coordination of different groups of complementing controls is evident. Practical implementation shows at least some alignment with defined governance.

4-Extensive	Gov: Governance is continually managed and monitored for performance ensuring it remains effective and relevant. It is fully coordinated with all relevant stakeholders in the organisation to ensure that its requirements can be and are applied consistently in practice.
	Ops: Technical controls are fully implemented, continually managed and fully coordinated. Performance is monitored ensuring controls remain effective, relevant and maintained. Operational practice is fully aligned with defined governance.

The following table provides an indication of how the Thales OT scoring methodology is mapped across to an IEC 62443-2-1 (2019) maturity level as shown in Table 5-10.

*Table 5-10: Indicative mapping of Thales OT assessment to IEC 62443-2-1 (2019) Maturity Level*

62443> Thales		Governance			
		1	2	3	4
Operational	1	Initial	Managed	Managed	N/A
	2	Initial	Managed	Managed	Managed
	3	Initial	Defined	Defined	Improving
	4	N/A	Defined	Defined	Improving

The next section will discuss the findings from Case Study B.

### 5.3.2 Baseline Results

This section highlights notable findings of the assessment. This is a combination of relevant alerts highlighted by the passive network monitoring and further analysis of the collected data by Thales.

#### 5.3.2.1 Summary of Findings

The analysis of the observed site security practices and assessment highlights are first summarised in Table 5-11 and explored in further detail in section 5.3.2.1.

Table 5-11 summarises the findings of the security assessment by order of the IEC's Security Program Elements (SPE) as defined in IEC 62443-2-1. It provides an indication of the potential impact on the security posture of the OT production systems. This is informed by the understanding

of the current threat environment and real-world incidents, particularly those in the manufacturing industries most relevant to Customer B. The following table provides only a summary of the results. The entire assessment findings for Customer B will follow the summary.

Table 5-11 Summary of findings by topic

Summary of Findings	Potential Impact
SPE 1 - Organisational security measures	
<p>There were considerations taken for organisational security measures for OT at the Customer B site, however, there were no specific OT security policies and procedures in place.</p> <p>Although the OT engineers had a good understanding around the importance of CS, no OT cyber specific training had been provided.</p>	<p>Well-defined and documented governance, policies and procedures underpin the implementation and operation of a robust OT security program.</p> <p>However, unless personnel at the site operational level have the training and experience to understand the guidance and the required scope of application, it is unlikely to be applied consistently and will be insufficiently coordinated to manage risk effectively in practice.</p>
SPE 2 - Configuration management	
<p>Asset registers for equipment on site existed and updated.</p> <p>Drawings for OT equipment were available and situated on the engineering shared drive.</p> <p>Good change control was also present for OT equipment.</p>	<p>Any OT asset that does not have an accurate inventory management is likely to fail. Creating an accurate inventory is a vital first step to define the nature and behaviour of system components. This will lead to OT security controls that are required to protect the operational equipment at an appropriate level.</p> <p>Change management procedures ensure this documentation is kept up-to-date and that controls remain effective. An OT CS program is unlikely to be effective when overly reliant on verbal communication and embedded knowledge.</p>
SPE 3 - Network and communications security	
<p>A small proportion of the OT production processes operated in an</p>	<p>isolated networks are common in legacy OT processes, but isolation alone does not protect against most cyber</p>

<p>air-gapped environment. Details of the nature of expected / authorised communications on these networks were not documented since they had little or no integration into IT level management, monitoring and security processes that help to protect and/or detect cyber incidents.</p>	<p>incidents. A common threat is malware ransomware via USB media (i.e., for backups) and engineering maintenance laptops.</p> <p>The lack of protection and detection controls in these networks means a cyber incident is unlikely to be identified proactively to minimise disruption. Resulting disruption has a high likelihood of spreading extensively throughout the system with and significantly affect normal production operation.</p>
<p>SPE 4 - Component security</p>	
<p>Thales did not find noteworthy evidence for hardening of equipment, however, did find coverage of malware protection and the use of ESET was in play for the OT systems visually inspected.</p> <p>Mitigations considered for systems that were unpatched were not considered, however, of the systems visually inspected, they primarily appeared isolated from the rest of the IT network and therefore have an element of protection from IT assets and vice versa.</p>	<p>The core principle of effective OT CS is defence in depth where multiple discrete controls are applied to protect against threats.</p> <p>Network security can be ineffective when the communicating components are not sufficiently secured.</p> <p>Legacy assets where good practice cannot be applied presents a significant risk as known vulnerabilities are more likely to exist. Outdated computers are particularly susceptible to compromise that can then spread throughout the OT environment, even where other assets are patched and up to date.</p>
<p>SPE 5 - Protection of data</p>	
<p>There was no data classification scheme in place at site there was not a full understanding of what critical and sensitive data existed and therefore what controls would be required.</p>	<p>Where OT data is not identified, catalogued and appropriately protected it undermines operational resilience. Examples of OT data included the configuration of assets controlling routine operation of production systems and extends to data such as backups, which need to be protected to enable rapid recovery after a failure or a CS incident.</p>

SPE 6 - User access control	
<p>User access control was performed at IT site level however, there were no OT specific policies or procedures detailing steps taken. Access to devices running process control software in production areas appeared to be controlled by generic accounts. Much of the equipment visually inspected consisted of stand-alone devices each managing their own usernames and passwords.</p>	<p>User access control is difficult to manage effectively at scale without centralised management systems. Where stand-alone assets are managed individually it tends to be a resource intensive manual process. This may discourage periodic review and auditing which is necessary to maintain security and increases the risk of unauthorised access.</p>
SPE 7 - Event and incident management	
<p>There were evident policies, processes, or controls in place for event and incident management, fit for purpose, for IT.</p> <p>The site had a business continuity plan and this also detailed specific OT procedures for handling a CS incident.</p>	<p>Restoration of production and recovery to normal operating conditions is unlikely to be reliable and timely when incident management processes are not defined and unified across all areas of the production process. CS incidents are complex and require specific considerations for detection and response. The impact of a cyber incident and consequential financial losses are likely to increase when this is not considered. If a cyber incident were to occur the time taken to restore normal operations would be increased without proper event and incident planning.</p>
SPE 8 - System integrity and availability	
<p>Critical elements of the system are designed to be resilient to failure and replacement stock stored at site for the areas visually inspected. Backups</p>	<p>Reliable backups are an essential part of the business continuity and disaster recovery strategy ensuring that production capability can be restored quickly after a failure or cyber incident. This is particularly important</p>



for OT were in place however, these were stored on engineer laptops.	where the system design does not employ a resilient architecture with built-in redundancies.
--	--

The next sections expand on the findings summarised above.

### 5.3.2.2 Detailed Findings

This section will explore the data results in further detail, aligning to IEC 62443-2-1.

#### *SPE 1 – Organisational Security Measures*

The requirements of SPE 1 ensure that an organisation is prepared to address OT security adequately. It focuses on organisational policies and procedures for applying security practices and ensuring that its personnel are security aware and trained for their security responsibilities.

#### *ORG 1 – Security Related Organisation and Policies*

*Table 5-12 ORG 1 Maturity Level - Security related organisation and policies*

<b>Assessed Criteria</b>	OT security is coordinated with IT and other relevant business stakeholders.			✓
	Background checks are performed for personnel accessing key systems.			✓
	OT Security roles and responsibilities are formally defined and assigned.			✗
	General security awareness training is provided to all OT personnel.			✗
	Specific security training is provided for key roles and responsibilities.			✗
	Security threats and risks in the supply chain are tracked and managed.			✗
<b>IEC 62443-2-1 Requirements</b>	<b>ORG 1.1 – ORG 1.6</b>	<b>Gov</b>	<b>2</b>	<b>ML-2</b>
		<b>Ops</b>	<b>2</b>	<b>Managed</b>

#### *ORG 1 Findings:*

- Although Customer B had resources applied to IT security, this was not the case for OT security across the site.
- There was a lack of governance relating to OT security.
- Thales found that little policies, procedures or training that relate directly to OT security were present.
- At site level, there was expert knowledge of the OT and networking of equipment but this was not formalised and was reliant on individuals that did not perform an OT specific role rather than formal documentation.

- The site team based in Customer B confirmed that the local HR policy was to perform background checks.
- OT was not formally defined in job roles and responsibilities and it is apparent that knowledge of the site systems is help in addition to normal roles and responsibilities.
- Security awareness training was underway at a corporate IT level but there were no specific OT related training modules or programs assigned to OT specific staff.
- There was no risk framework for Cyber Security relating to OT at the Customer B site and this extended to the supply chain. This is of utmost importance considering the reliance on third parties that existed in the essential operation of OT equipment at site.
- Security system management was performed in-house and appears to be performed well as per networking standards.
- Network management was conducted exceptionally well at Customer B. This role is filled by two engineers on site and covers all cloud and site networks.

*ORG 1 Recommendations:*

- It is presumed that Customer B has an ISMS aligned with their corporate IT systems. According to ISA/IEC 62443, an asset owner should align their ISMS with an OT SP and co-ordinate in the same manner. The creation of an OT SP would structure the OT security activities required in a formal method that would allow for executive buy in and a common understanding among all stakeholders for future direction of the SP.
- Thales recognise the significant competence of site staff on operation of the facility and were impressed by knowledge of the network and OT equipment. Consideration should be taken to introducing OT roles and responsibilities and its follow-on impact to resourcing.
- Thales recommend the Customer B site extend their training topics to cover OT for general awareness and add specific modules relating to OT security to those staff that have responsibilities for OT. These modules extensively address various aspects of OT security and encompass a wide range of topics such as common threats and vulnerabilities, incident detection and response.
- Consideration should be taken for networking resource requirements. Two roles covering all networking across Customer B is difficult from a resource standpoint and from a single point of failure.

ORG 2 – Security Assessments and Reviews

Table 5-13 ORG 2 maturity level – security assessments and reviews

<b>Assessed Criteria</b>	OT Security risks are identified, assessed and controlled.			✘
	Processes are in place to discover and investigate OT security anomalies.			✘
	Security is managed through the lifecycle of systems and components.			✘
	Security factors are regularly reviewed and updated where required.			✔
<b>IEC 62443-2-1 Requirements</b>	ORG 2.1 – 2.4	<b>Gov</b>	<b>1</b>	<b>ML-1</b> Initial
		<b>Ops</b>	<b>2</b>	

ORG 2 Findings:

- There was no risk governance in place for OT systems. A risk framework was not chosen so the downstream tasks of risk identification, analysis and treatment could not be completed in a uniform manner.
- Security anomalies were present in the Customer B OT network and instances of this has been included in the accompanying documentation. These were also discussed with the security and network team upon discovery during the on-site assessment. The professionally managed network is typically segregated between IT and OT devices where possible. However, several IT and OT combined segments existed without proper segregation and increased the attack surface for OT equipment. Therefore, an anomaly detected on the IT network has the potential to impact downstream OT equipment such as Windows 7 HMI which was found to be vulnerable to Eternal Blue (Eternal Blue exploits a vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol).
- OT equipment newly installed on site is mostly performed by third parties and then managed internally. It is unclear what FAT (Factory Acceptance Test) and SAT (Site Acceptance Test) procedures have been performed.

ORG 2 Recommendations:

- To successfully integrate risk into OT security, the first step is to choose an OT specific risk framework. Multiple frameworks exist and each have their own benefits and features that can match the way an organisation works. Once a risk framework has been chosen it should be implemented and communicated such that each member of staff involved with the risk process understand their roles and responsibilities. Then risk identification can take place which leads to risk assessment, treatment and management.

- Consideration should be taken to implementing an automated alert on Darktrace to assess endpoints against TCP/IP ports to ensure that they are closed by default and only opened for a specific purpose.
- Any new OT equipment installed at site should be evaluated against security standard practices. As part of the procurement process, an agreed timeline for accepting the equipment both at the factory where it is created (FAT) and when the equipment arrives on site (SAT) so that the delivered product meets the initial requirements. As part of this process, security requirements should be assessed and documented so that any future changes to the equipment can be compared against the initial installation.
- Once an OT Security Program has been implemented it should be regularly reviewed to ensure its original requirements are being fulfilled and is still fit for purpose. An OT security steering committee could be setup to involve key stakeholders which ensures input from across the business is included in the program.

*ORG 3 – Security of Physical Access*

*Table 5-14 ORG 3 maturity level – security of physical access*

<b>Assessed Criteria</b>	Physical access to facilities, equipment and cabling is controlled.			✔
<b>IEC 62443-2-1 Requirements</b>	ORG 3.1	Gov	4	ML-4
		Ops	4	Improving

*ORG 3 Findings:*

Customer B site had strong external physical security controls and extensive internal security controls. The external perimeter was guarded by a complete fence and CCTV, along with security guards both internal and external. The staff and visitor entrance were protected with physical and logical security operated by reception and security when reception is closed.

Access to the building was controlled through card access automated doors or operated by reception if a visitor attends site. Visitor access control was operated by reception and includes a site induction for new contractors. All visitors must be assisted with a site representative. Access to the factory floor was fob accessed.

Visitors attending the factory floor must be escorted. All visitors attending site must complete a safety induction.

Access to OT equipment whilst on the factory floor was controlled through panel keys which are kept by engineering staff only. Access to OT cabinets was conducted via key access by the engineering staff at site. Key Management was controlled by engineering management.

Access to IT server room was managed via a key card system and the process to grant a new key card for a member of staff is controlled by HR.

*ORG 3 Recommendations:*

- None

**SPE 2 – Configuration Management**

In the standard, the requirements of SPE 2 ensure that the OT architecture is documented and an inventory of hardware and software components is maintained with all changes to components adequately controlled.

**CM 1 – Inventory Management**

CM 1 consists of two parts namely 'CM1.a' and 'CM1.b', described further in the next sections.

**CM1.a – Documentation**

*Table 5-15 CM1.a maturity level – documentation*

<b>Assessed Criteria</b>	An inventory of OT assets is recorded and maintained.			✓
	Drawings and documentation for OT systems are maintained.			✓
<b>IEC 62443-2-1 Requirements</b>	CM 1.1 – 1.2	Gov	3	ML-3
		Ops	3	Defined

*CM1.a Findings:*

- During the visual inspection of the production areas, it was clear that there were proportions of assets that were not connected to any network. Although the probe is capable of reading information about software running on OT equipment it cannot detect software running on non-networked equipment.
- Drawings and documentation for OT equipment existed. Drawings also existed for panels made by third parties that will include documentation and layout drawings for equipment installed in the panel.

CM1.a Recommendations:

- Thales recommends using the asset register provided as part of the deliverables as a starting point for inventory management. Using this document with the fields and columns provided to capture non-networked equipment will bolster the understanding of the OT network and what security requirements are needed. As a minimum, the following details should be capture for all OT assets; organisational responsibilities, manufacturer, model, version number, serial number, revision/patch level and history. Having an asset register will also help Customer B move forward regarding any new equipment to be installed on site as a format will exist that can be used as a requirement for third parties to use for implementation.
- Drawings and documentation for OT equipment should be properly controlled by Customer B and any changes made via a management of change process would update these documents and provide a full revision history. The primary purpose of doing this is to provide a basis for conducting security assessments, including the identification of trust boundaries as described in the IEC 62443 standard. These documents should include line drawings, functional drawings, rack and room layouts and security perimeter drawings.

CM1.b – Configuration and Change Management

Table 5-16 CM1.b maturity level – configuration and change management

<b>Assessed Criteria</b>	Records of OT device and system configuration settings are maintained.			✘
	An effective change control process is enforced for all OT changes.			✔
<b>IEC 62443-2-1 Requirements</b>	<b>CM 1.3 – 1.4</b>	<b>Gov</b>	<b>3</b>	<b>ML-2 Managed</b>
		<b>Ops</b>	<b>2</b>	

CM1.b Findings:

- Records of OT device and system configuration changes were maintained and documented via the change management processes. A change request process for any changes made to production equipment and an IT change management process both existed independently.

CM1.b Recommendations:

- Recording OT configurations is imperative for verification of their function. Without this it is impossible to verify if the currently installed configuration matches what has been approved and could lead to unapproved changes being pushed to OT assets.

- The change control process can be used to support a key Cyber Security principle of separation of duty so that those who are implementing the change are different from those who are approving and authorising.

*SPE 3 – Network and Communications Security*

In the standard, the requirements of SPE 3 ensure that the OT is protected from attacks conducted through the network and through communications capabilities. These attacks can originate externally to the OT, across security zone boundaries within the OT and from unauthorised devices connected to OT networks.

*NET 1 – System Segmentation*

*Table 5-17 NET 1 maturity level – system segmentation*

<b>Assessed Criteria</b>	There is effective control of traffic between OT and non-OT networks.	✔		
	Networks for OT are understood, documented, assessed for security risk.	✘		
	Networked safety systems are protected from interference.	✔		
	External dependencies and the consequence of unavailability are known.	✔		
	There is a defined procedure for safely isolate OT from external networks.	✘		
	Internal OT networks are segmented and traffic flows are controlled.	✘		
	All devices connected to OT networks are identified.	✔		
	OT network services are protected from unauthorized access.	✔		
	End-user and general business functions and traffic are separate to OT.	✔		
	OT devices are synchronised to a shared source of accurate time.	✔		
<b>IEC 62443-2-1 Requirements</b>	NET 1.1 – 1.10	<b>Gov</b>	<b>2</b>	<b>ML-2 Managed</b>
		<b>Ops</b>	<b>2</b>	

*NET 1 Findings:*

- Thales found that network segmentation was deployed in the following scenarios:
- Machinery, although logically segmented on centrally managed switches, Thales discovered that some IT systems were present on OT VLANS.
- A small proportion of the OT production processes operated in an air-gapped environment. Details of the nature of expected / authorised communications on these networks were not documented since they had little or no integration into IT level management, monitoring and security processes that help to protect and/or detect cyber incidents.

- The network at Customer B was sufficiently managed, with plentiful subnets and good documentation. Data from the Thales probe however, found that there were some connections between OT, IT and third parties. Thales also highlight the use of legacy networks including the use of a shared drive.
- Staff at site were aware of the xxx subnet and relayed information about the ongoing and longer-term plan to move assets from a legacy subnet to a newly structured network consisting of several OT VLANs. Initial inspection of the probe data found that this plan was underway however had not been fully enacted as some equipment was still residing on the legacy VLAN however this may take some time to resolve given the nature of the task at hand.
- There was an extensive understanding around how the OT networks currently work at site. This was made evident upon discussions with IT networking staff and security staff.
- Third party remote access equipment was installed on several factory lines typically included vendor specific equipment could be enabled upon request. OT safety systems were present on site however were not part of this assessment. Discussed further in NET 3.
- Some OT assets could operate with autonomy separate to the rest of the network due to network segregation. A failure in external systems is unlikely to cause a follow-on event failure to OT production equipment on site. However, it was noted a failure in connectivity for the Building Management System (BMS) may be critical.
- It was noted during visual inspection that one of the HMI systems had an Internet connection.

*NET 1 Recommendations:*

- Traffic between the OT network and external networks should be identified, managed, authorised and documented. Third party risk is rarely well understood but can cause serious Cyber Security related incidents. As it stands the site in Customer B does manage third party remote access well, however, only two of the production areas were inspected visually (due to limited time).
- Once segmentation to the network has been completely implemented IEC 62443 suggests grouping OT networks into zones and conduits, where a zone is a logical grouping of OT assets that deliver a function and a conduit is a connection between two or more zones.
- OT systems should not be connected to the Internet unless for a specific purpose and the method should be scrutinised such that the connection is as secure as possible. This should



be removed unless required. A review of further critical systems would have been beneficial should Thales have had more time at site.

NET 2 – Secure Wireless Networks

Table 5-18 NET 2 maturity level – secure wireless networks

<b>Assessed Criteria</b>	Wireless devices in OT systems are documented and managed.			
	Different wireless networks are segmented and traffic flow is controlled.			
	Wireless networks are designed to avoid leaking sensitive information.			
<b>IEC 62443-2-1 Requirements</b>	NET 2.1 – 2.3	<b>Gov</b>	<b>0</b>	<b>N/S</b>
		<b>Ops</b>	<b>0</b>	

NET 2 Findings:

Whilst on site Thales found multiple Wi-Fi SSIDs controlled by Customer B. Good security practices were observed joining the guest Wi-Fi as access was provided by a member of Customer B staff. However, an in-depth wireless investigation was not conducted as part of this assessment and therefore not scored.

Discussions with engineering personnel indicated that there had been instances whereby OT equipment had been temporarily connected to the wireless network.

NET 2 Recommendations:

- Thales recommends that Customer B engage in a wireless assessment that will provide deeper insights into their wireless activity.

NET 3 – Secure Remote Access

Table 5-19 NET 3 maturity level – secure remote access

<b>Assessed Criteria</b>	Only dedicated and approved secure remote access solutions are used.			✘
	Remote access follows commonly accepted good security practice.			✔
	External access is individually authorised, documented and logged.			✔
	Scope and duration of access are limited to the minimum required.			✘
	Remote access connections can be easily monitored and controlled.			✘
<b>IEC 62443-2-1 Requirements</b>	NET 3.1 – 3.3	<b>Gov</b>	<b>2</b>	<b>ML-2</b>
		<b>Ops</b>	<b>1</b>	<b>Managed</b>

#### *NET 3 Findings:*

- Multiple methods of connecting to the Customer B network remotely were noted. This included third party boxes with VPN capabilities that connect directly into the OT network. Team Viewer and EWON VPN were both used for remote access into the production systems.
- A review of the physical OT equipment found an HMI system in the production area on IP address was communicating with an external IP address 94.xx.xx.xx on port 5938 (the default TeamViewer port). This IP address and port both match a TeamViewer endpoint.
- It was clear remote access had been documented across site which applied to authorisation, documentation, logging and monitoring of remote access. However, the duration and termination of each access request was not documented. As evidenced upon inspection, whereby an active remote connection session could be identified via team viewer on an HMI in the production area.

#### *NET 3 Recommendations:*

- The first step to controlling methods of remote access is to document existing methods and risk assess each to determine if these methods fall within Customer B's risk tolerance and to determine what, if any, control measures are to be applied. Several secure remote access tools exist and Thales recommends using one of these technologies as a central access into the Customer B site that can meet the criteria highlighted above.
- Once all third-party remote access methods of entry have been discovered and documented, a risk assessment should be performed to properly discover the level of risk involved with each connection. From this risk assessment controls can be implemented to bring the risk to a level acceptable for Customer B.
- Each critical system should be identified and reviewed.

#### *SPE 4 – Component Security*

In the standard, the requirements of SPE 4 ensures that the OT and its components are appropriately protected from attacks. These attacks can originate through component interfaces, both external and internal. Examples of external interfaces include network interfaces, USB interfaces and configuration ports. Examples of internal interfaces include inter-process communications interfaces and application programming interfaces (APIs).

COMP 1 – Devices and Media

Table 5-20 COMP 1 maturity level – devices and media

<b>Assessed Criteria</b>	All OT devices have a specific non-default secure hardened configuration.			✘
	Only the minimum required device functionality is enabled.			✘
	If removable media is required, only dedicated authorized media is used.			✘
<b>IEC 62443-2-1 Requirements</b>	COMP 1.1 – COMP 1.2	<b>Gov</b>	<b>1</b>	<b>ML-1</b>
		<b>Ops</b>	<b>1</b>	

COMP 1 Findings:

- Thales found that OT systems were not sufficiently hardened as per best practice. There was no hardening standard or governance covering OT assets specifically, only the IT hardening policies existed, which were often applied to the OT assets where USB access was blocked on some engineering machines. However, this was not applied to all assets and was demonstrated through the HMIs with internet access (as discussed above) and some HMI equipment with USB port enabled.

COMP 1 Recommendations:

- All critical systems should be reviewed for software inventory and any unnecessary software should be removed. Each critical system should have access control reviews and ensure that by default administrator control is not granted. Once a hardened configuration has been implemented access control will ensure that any changes made are performed by authorised personnel. The CIS (Centre for Internet Security) has security templates that can be applied to critical systems that provide a hardened operating system.
- All USB devices used in the OT system should be dedicated for that use and that use alone. Ideally each USB device should be encrypted, or password protected such that possession of the device is not enough to transfer data to and from the device. OT assets should not have undocumented connections to the Internet. On the rare occasion this is required, a risk assessment should be performed to ensure that the connection is required and all risks have been accounted for. Controls and restrictions will be applied to the asset such that the risk is at an acceptable level for the organisation to allow the function of the connection.

COMP 2 – Malware Protection

Table 5-21 COMP 2 maturity level – malware protection

<b>Assessed Criteria</b>	Devices and removable media are tested for malware before connection.			✘
	OT assets are protected against malicious software and firmware.			✘
	Anti-malware product status and updates are monitored and managed.			✔
<b>IEC 62443-2-1 Requirements</b>	COMP 2.1 – COMP 2.3	Gov	2	ML-2
		Ops	1	Managed

COMP 2 Findings:

- Discussions with OT Engineers highlighted the fact that USB devices were used to download information to OT Assets and while these devices were controlled by IT and enabled via their UID there seemed to be no process to check the device for malware before the connection to the OT environment is made.
- Customer B had a solution deployed for anti-malware that applied to OT equipment running any operating system above windows CE in the production areas.
- An HMI was an embedded version of Windows 7, SPv1 which was known to be vulnerable to Eternal Blue Worm. This was flagged to the site team upon discovery and should be investigated.
- An IP address was found communicating with several block-listed IP addresses. However, an investigation revealed that it to be the checkpoint secondary perimeter Firewall and it is performing its duty effectively.

COMP 2 Recommendations:

- In addition to using a dedicated USB device as recommended in the previous section, the USB drive should be scanned for malware before being used in the OT equipment. An install of a “sheep dip” machine in each manufacturing facility would allow for Engineers to assess the removable media’s content for malicious code.
- All critical systems and any OT system that requires anti-malware should be inventoried and checked to ensure that the anti-malware software is installed and updated.

COMP 3 – Patch Management

Table 5-22 COMP 3 maturity level – patch management

<b>Assessed Criteria</b>	There is a defined process for managing OT security updates.			✘	
	The applicability of updates to OT devices is documented and maintained.			✘	
	Updates are validated for authenticity and compatibility before installation.			✘	
	Updates are examined for side effects that may reduce security.			✘	
	Compensating controls are considered where updates are not applied.			✘	
<b>IEC 62443-2-1 Requirements</b>	COMP 3.1 – COMP 3.5		Gov	1	ML-1
			Ops	1	Initial

COMP 3 Findings:

- Patch management was not considered for lower Purdue layer assets (i.e., PLC’s) and has no coverage or process in place to update assets. Several vulnerabilities on the OT equipment with Common Vulnerability Scoring System (CVSS) scores of ten, which is the highest risk.
- Some OT software and patching are controlled via a central server running Windows operating systems. In these cases (e.g., some HMI or engineering workstations) updates have recently been installed but it is unclear on coverage of the production areas not visually inspected.

COMP 3 Recommendations:

- In the report are details of vulnerabilities that potentially exist in OT equipment connected to the network currently. Such as the HMI in the production area vulnerable to eternal blue exploit. Thales recommend patching with MS17-010, to mitigate adversaries that leverage low hanging fruit. This is indicative of assets that have not been patched as resolutions for these vulnerabilities have been found and published. After a full asset inventory is completed for all networked and non-networked equipment, a list of equipment will show operating system version and patch level. This can then be compared with known vulnerabilities for each and if a patch exists.
- Before applying patches to OT equipment, it should be checked for integrity and authenticity. This allows assurance that the patch has not been changed in transit and is from the correct software author. This can be achieved by using digital signatures or by using tamperproof seals where the media is distributed physically.

- In some cases, applying patches can have unintended consequences such as modifying some of the configuration of the OT asset. For this reason, patch management should be integrated into change control processes so that each time a process can be performed that has a backup capability as a backup of the software should be taken before applying a patch.
- Not all security patches can be applied. If this is the case, then the justification for this should be captured and evaluated on a periodic basis to ensure the justification is still valid.

**SPE 5 – Protection of Data**

In the standard, the requirements of SPE 5 relate to protecting data to ensure that it is not subject to unauthorised access or modification, i.e., maintaining confidentiality and integrity.

*DATA1.a – Data Management*

*Table 5-23 DATA1.a maturity level – data management*

<b>Assessed Criteria</b>	Sensitive and operationally critical OT data is identified and catalogued.			✓	
	Controls are applied to protect data commensurate to its classification.			✗	
	Data relating to safety systems is protected from unauthorised changes.			✓	
	Data retention is defined and managed to meet operational requirement			✗	
	Company data is purged when devices or media are decommissioned.			✗	
<b>IEC 62443-2-1 Requirements</b>	DATA 1.1 – DATA 1.6		Gov	2	ML-2
			Ops	1	Managed

*DATA1.a Findings:*

- Data classification (e.g., confidential, internal, public) and data categorisation (data at rest or data in transit) does exist at policy level for the site however no evidence of this being applied operationally was present.
- Although out of scope for this assessment the safety systems in the CPR were identified as being completely segregated from other systems.
- No policy for data purging or destruction was found in place at site for OT equipment but IT had a secure disposal process that had the potential to cover OT assets also.

*DATA1.a Recommendations:*

- The first step to data management is to identify what data is in use on the OT network. The information provided in this report is a strong starting place from which to build. Several types of on-site network communication are outlined and security vulnerabilities are

highlighted. Example categories for information that should be identified and classified are as follows, user authentication information, testing data, configuration data, backup data and auditing and security logs.

- Each OT system should be evaluated for failure status, whether it is fail-safe or fail-secure in the event of a security breach. Ideally systems should default to fail secure where the system moves to a state that limits any further risk or damage to people or the environment.
- A data retention scheme has been implemented at site level and consideration given to implementing a group wide scheme. This includes retaining logs and events for a period after archival from the system to assist with recovery or forensics – consider work to ensure all critical assets are covered in the logging platform to allow for greater visibility of potential incidents.
- It would make sense for OT equipment to be included in the IT asset disposal process if the third party that carries out this process is able to support.

#### *DATA1.b – Cryptographic Technologies*

##### *DATA1.b Findings:*

- The application of cryptographic processes captured at the Customer B site typically followed best practice however there were some discrepancies as summarised below.
- Thales found use of an insecure SSL protocol version (SSLv3) and TLS protocol version (TLSv1.0). The remote service accepts connections that are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
- An SSL certificate had expired in at least one instance as the expiry date had passed.
- Thales found evidence of use of an insecure SNMPv1 protocol. SNMPv1 is a legacy client-server protocol used over port 161. It is an insecure means of text-based communication since all the information it sends and receives is sent in plain text with no encryption.
- Many instances of block-listed SMB (Server Message Block) shares detected were found using the network probe. In Windows systems, hidden default network shares can be used for lateral movement using administrator credentials. An example of this share was '\$'.

##### *DATA1.b Recommendations:*

- Using insecure and deprecated protocols can make connections vulnerable to exploits. SSL 3.0 and TLS 1.0 is no longer acceptable for secure communications. Disable SSL v 2.0 and 3.0 and use TLS 1.2 protocol instead which is much more secure.

- SSL certificates should be in date whether used internally or externally. Either purchase or generate new SSL certificates to replace existing certificates and create a process to renew these certificates when expiration is close.
- SNMPv1 should be disabled and replaced with another protocol that is not vulnerable to the same exploitation. As an example, the SNMPv3 protocol is more secure and could be used in its place.
- SMB share configuration should be evaluated across the network.

**SPE 6 – User Access Control**

In the standard, the requirements of SPE 6 ensure that users (human users, software processes and devices) are assigned accounts that are used to control access to OT systems and their resources and commands. Access control involves identification and authentication of users, assignment and enforcement of access rights for those users and control of user sessions.

*USER 1 – Identification and Authentication*

*Table 5-24 USER 1 maturity level – identification and authentication*

<b>Assessed Criteria</b>	There is a defined process for issuing access credentials.	✓
	Access is continually managed and is revoked when no longer required.	✗
	Authentication security mechanisms do not impede legitimate access.	✓
	Minimum access rights are assigned based on defined role requirements.	✗
	Human users are individually authenticated and do not share accounts.	✗
	Software and services are specifically authenticated and managed.	✗
	Password policies are defined and password security is managed.	✗
	Multifactor authentication is enforced for externally accessible systems.	✓
	Excessive login failure and other suspicious account activity is monitored.	✗
	Active authenticated sessions are protected against unauthorised access.	✗
Unattended systems are protected against unauthorised access.	✗	
<b>IEC 62443-2-1 Requirements</b>	<b>USER 1.1 – USER 1.18</b>	Gov 2 ML-2 Ops 1 Managed

*USER 1 Findings:*

- There is a defined process for issuing access credentials however, operationally the use of shared passwords was present in the production area and thus the policy is not being followed religiously.



- No access review policy existed for periodic reviews of credentials and is not performed on a periodic basis to ensure gradual accumulation of access rights beyond what an individual need to do their job does not occur.
- User management was controlled via an on-boarding and off-boarding process controlled by IT/Line Manager. OT user management was in place for operator and engineer accounts, but this was not widespread across OT systems with OT systems still using default credentials supplied by the vendor.
- IT have a password policy. However, this does not apply to OT assets. Password sharing was evident and these were not changed when a staff member leaves the organisation. Credentials were noted as being stuck onto devices in manufacturing zones with sticky notes (see Figure 5-4).



*Figure 5-4 Credentials on sticky note*

- There was currently no software inventory at site and this would be required before understanding accounts related to software running on OT equipment and its respective permission level.
- Login failures were not logged in OT equipment.

*USER 1 Recommendations:*

- Login failures are not logged in OT equipment but can provide valuable information in the event of breach/malicious actor being present.
- Shared passwords should be evaluated and any actions required undertaken without delay.
- Roles, such as operator, process engineer, maintenance engineer and administrator, represent groups/sets of access rights that can be assigned to human users. The use of identifiers, authenticators and roles, simplifies the management of user access controls and reduces the potential for errors and omissions in the associated processes.
- Thales recommended that all devices that support interactive user login, such as workstations and that are granted access to the OT environment should be evaluated to determine if they face the risk of access by unauthorised personnel. Those that do, should be protected by a multifactor authentication scheme. Where the use of multifactor

authentication is not feasible, compensating countermeasures, such as physical access, in combination with single-factor authentication can be used when the risk of access by unauthorised personnel must be reduced.

- Shared accounts and privileges should be reviewed on an annual basis. This prevents privilege creep and ensures users have access to only those systems authorised. Credentials should be removed from fronts of OT Equipment.

*USER 2 – Authorisation and Access Control*

*Table 5-25 USER 2 maturity level – authorisation and access control*

<b>Assessed Criteria</b>	All system functions require individually authorised accounts for access.			✘
	High privilege access is limited to defined legitimately required functions.			✘
	High privileges are elevated as required and not used for routine access.			✘
	Multiple approval process is enforced to authorise high-risk activity.			✘
<b>IEC 62443-2-1 Requirements</b>	USER 2.1 – USER 2.4	Gov	1	ML-1 Initial
		Ops	1	

*USER 2 Findings:*

- Typically, OT systems required an authorised account for access. In some cases, shared accounts were used to perform specific functions as discussed in User 1.

*USER 2 Recommendations:*

- A user review should be undertaken to determine users currently on the OT network and respective access level.
- Any action that could have an impact to health and safety should be verified by more than one user if possible.

**SPE 7 – Event and Incident Management**

In the standard, the requirements of SPE 7 support detection, logging and analysis of security-related events and compromises. Such activities are used to identify security-related issues and ensure that users cannot unreasonably deny that they were responsible for certain actions.

*EVENT 1.a – Detection and Logging*

*Table 5-26 EVENT 1.a maturity level – detection and logging*

<b>Assessed Criteria</b>	Relevant events are recorded to enable effective security management.			✘
	Security events are reported and investigated in a timely manner.			✘
	Events from various sources are logged and correlated.			✔
	Relevant events and activity are logged to protected locations for auditing.			✘
	Logs contain sufficient detail to enable effective investigation of events.			✘
	Logs are protected from unauthorised access.			✔
	Event logs can be analysed to identify security incident characteristics.			✘
<b>IEC 62443-2-1 Requirements</b>	EVENT 1.1 – EVENT 1.7	Gov	1	ML-1
		Ops	1	Initial

*EVENT 1.a Findings:*

- The Historian system had event and log management mostly used for troubleshooting the OT environment – data is understood to be held for 3 months however, these logs had little relevance pertaining to Cyber Security.
- The lack of protection and detection controls for these assets means a cyber incident is unlikely to be identified proactively to minimise disruption. Resulting disruption has a high likelihood of spreading extensively throughout the system with and significantly affect normal production operation.
- Site staff indicated that OT VLANs were covered by their monitoring platform. However, upon further inspections, the X machine assets were not identified in the monitoring solution. Furthermore, deployment of Thales’ network probe identified assets covering 20 OT networks. Therefore, Thales concludes that the deployment of network monitoring was not fully operational nor effective. This would prevent the site from proactively mitigating network-based Cyber Security incidents.

*EVENT 1.a Recommendations:*

- Identification of critical systems should be completed and this will determine which systems require intricate logging and event management. A key system is likely to be the data logging platform as this has a far-reaching access in the OT environment a logging server could be setup to receive logs from this system along with investigation into how much of the OT environment can be seen from monitoring and how adept that solution is at catching suspicious behaviour. As the monitoring platform is an AI learning solution there is every chance that suspicious activity already in place could be learnt by the system as “normal” and therefore not flagged appropriately. From here a baseline can be built and any suspicious behaviour flagged. Once suspicious behaviour is flagged this should be assigned to a member of staff within an appropriate timescale.
- Ensure the following events are captured and analysed; login attempts, access to controlled commands and data, OS events, IACS events, backup and restore events, configuration changes and potential reconnaissance activity and audit log events. These logs should be kept for an adequate time depending on the system and should be secure so that tampering cannot take place. Logs should contain information that can support non-repudiation and time correlated analysis of events.

*EVENT 1.b – Incident and Vulnerability Handling*

*Table 5-27 EVENT 1.b maturity level – incident and vulnerability handling*

<b>Assessed Criteria</b>	There is a defined process for responding to security incidents.			✔	
	Security deficiencies are identified, assessed and addressed.			✘	
<b>IEC 62443-2-1 Requirements</b>	EVENT 1.8 – EVENT 1.9		Gov	2	ML-2
			Ops	1	Managed

*EVENT 1.b Findings:*

- A Business Continuity Plan (BCP) is in place at site but unclear if reference is made to any OT security related events.
- As OT risks are not documented fully, it is assumed vulnerabilities are not captured or assessed on a frequent basis to ensure any critical security events are addressed.

*EVENT 1.b Recommendations:*

- OT security events should be considered as part of the BCP and should have its own Disaster Recovery (DR) policies. As an example, if there were to be a group IT security incident affecting corporate machines it would make good sense to try to isolate the OT network given the current network structure that would allow the security incident to potentially travel into the OT network.
- Once documentation of all OT assets has been completed with software and firmware versions recorded these should be checked against known vulnerabilities to ensure any security related patches are applied in a timely manner. Potential vulnerabilities affecting OT equipment installed at site presently have been included as part of this report.

**SPE 8 – System Integrity and Availability**

In the standard, the requirements of this SPE ensure that the integrity and availability of the OT are protected and that the appropriate capabilities are present to recover the system to a previous state when necessary.

*AVAIL 1 – System Availability and Intended Functionality*

Table 5-28 summarises the system availability and intended functionality maturity level.

*Table 5-28 AVAIL 1 maturity level (system availability and intended functionality)*

<b>Assessed Criteria</b>	There are defined business continuity and disaster recovery plans.			✓
	Resources required to maintain availability are monitored and maintained			✗
	Systems are protected against failure from overload or lack of resources.			✗
<b>IEC 62443-2-1 Requirements</b>	AVAIL 1.1 – AVAIL 1.3	Gov	2	ML-2
		Ops	1	Managed

*AVAIL 1 Findings:*

- The site has a BCP, but it is unclear whether OT equipment or security related incidents affecting OT equipment is considered.
- Network segmentation has been highlighted previously.
- Coverage for hardware failures was in place as spare resources were stored at site.

AVAIL 1 Recommendations:

- Network segmentation has been highlighted previously. This would cover some aspects of the requirements for this section as a denial-of-service attack on the network would unlikely impact the networked OT equipment in the correct VLANS however may affect the legacy OT network.
- Site DR policies and BCP should be updated to include OT equipment and consideration for a network OT outage. This would address actions required if a cyber incident affected the networked portion of the OT equipment.

AVAIL 2 – Backup / Restore / Archive

Table 5-29 AVAIL 2 maturity level (backup/restore/archive)

<b>Assessed Criteria</b>	OT Data required to recover from failure is backed up at suitable intervals.			✘
	The backup process is managed to avoid disruption to normal operations.			✘
	Backups are verified to ensure data validity and integrity.			✘
	Backups are protected ensuring access only to authorised personnel.			✘
	Recovery processes are defined and periodically validated.			✘
<b>IEC 62443-2-1 Requirements</b>	AVAL 2.1 – AVAIL 2.5	Gov	1	ML-1
		Ops	1	Initial

AVAIL 2 Findings:

- From Thales observations OT systems had a limited back up process, conversations with OT Engineers suggested that all backups for OT equipment configuration files sat on engineering laptops with no wider coverage from the IT backup solution in place. There were limited backup and restore capabilities for the Data OT system, but this was not fully understood within the Infrastructure Team. There were no integrity checks on backups that did exist and they were not periodically tested to ensure restore processes are in working order.
- Media used for the backup procedure is a mixture with heavier usage on USB drives. Media has not been considered for handling.
- Recovery Time Objectives /Recovery Point Objectives seemed undefined for OT assets but well covered for their IT counterparts.

*AVAIL 2 Recommendations:*

- Completion and further attention of inventory management combined with identification of critical OT assets will allow the creation of a process to define backup strategies for this environment including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). This information will determine which OT systems requires the most attention in relation to backups and restoration time against criticality to business continuity.
- Work should be carried out to assess whether the backup solution currently in place may be feasible to use in OT and that it covers any non-virtualised Windows operating system before Windows 7. Coverage for this system should be investigated and if a single central backup solution is not currently possible then research should begin into a solution that will cover OT assets. Immediate action should be taken to move currently backed up configurations from engineering laptops and onto a shared network space that is covered in the wider backup process, the health of the laptops currently holding backup configurations was not assessed – however it was discovered that they are likely older machines with mechanical hard drives which are assumed more prone to failure than more modern solutions.

### 5.3.2.3 Recommendations

Customer B has been evaluated as meeting the “Managed” maturity level from the IEC 62443 requirements. This can be improved by following a defined road map and security plan that documents the end state desired, current state and how to get from the current state to the desired end state. Thales recommend the following considerations to be taken to develop on the current maturity level.

#### *OT security program and policy generation*

An effective OT Cyber Security program formalises the company’s Cyber Security commitments and strategic goals at a senior level, communicates what is expected of all employees and empowers them to contribute toward achieving the desired state. It consists of a documented risk identification and risk assessment process and defined controls, including governance (e.g., policies and procedures) and technical measures, to address the risks identified.

IT security is often well defined but can have different business priorities and functional requirements to OT. For an OT focussed security program to be successful it must coordinate with applicable IT security elements and involve cooperation between different stakeholders (e.g., IT,

OT, procurement and safety) around the company to identify and address security risk, particularly where there are interconnections and interdependencies.

Building a security program is the most appropriate first step for Customer B as it will set out a vision of expectation ratified by security staff and senior leadership. Building out a detailed security program will ensure all strategic, tactical and operational objectives are considered and will define a clear path to an increased maturity level.

#### *Backup capability*

Reliable OT backups are an essential part of the business continuity and disaster recovery strategy ensuring that production capability can be restored quickly after a failure or cyber incident. This is particularly important where the system design does not employ a resilient architecture with built-in redundancies.

Were a cyber incident to occur at site in Customer B the capability to quickly restore operations may be hampered by the status of PLC and HMI backups.

#### *Network monitoring*

Many legacy OT systems use a 'flat' network where all devices occupy a single segment and can communicate with little or no restrictions. Segmentation refers to techniques that limit the flow of network traffic between networks and devices. The IEC 62443 'zones and conduits' approach is an effective way to implement segmentation whereby the network is segmented into zones containing assets. Zones can be based on various criteria, both physical and logical, e.g., location, device type (e.g., PLC), process area (e.g., Production Line 1) and function (e.g., process and safety). Conduits define the communication required between those zones and devices.

With this structure in place, controls can be applied to limit communication between zones and devices to the minimum communication necessary correct operation of the OT process. Network segmentation is often achieved by dividing OT systems into multiple networks (physical or virtual) connected by a Firewall. Dual homing of edge devices in different zones should be avoided.

Where trust can be reliably verified at device level, cryptographic controls on communications may be sufficient (e.g., authentication and integrity checks). However, all controls must remain effective in cases where previously trusted devices generate unauthorised traffic, for example in the case of a malware infection.



Given the nature of the network at the site in Customer B and the challenges posed to move the site network to a secure state it is recommended that Customer B consider as a minimum to monitor OT network traffic whilst network segmentation takes place.

#### *Secure remote access*

All connections into OT systems can be a security risk. Connections originating externally (i.e., from the Internet), especially by third parties, carry particularly high potential for harm and there are numerous documented cases of remote access technologies being exploited to gain unauthorised OT access. Solutions from popular reputable vendors can become vulnerable and insecure unless the operator regularly maintains it.

Customer B have several distinct methods of third-party direct access to the site in Customer B. This poses a challenge as any work undertaken as part of a security program could be bypassed as these controls may not apply to these connections. It is vital that the site in Customer B review and control third party ingress connections.

#### *Summary of Findings*

An overview on how the practices observed by Thales at the site compare against the requirements defined in the IEC 62443-2-1 standard is given in Table 5-30.

Table 5-30 IEC 62443-2-1 assessment scoring

Assessment Area	Description	Thales Scoring		IEC 62443-2-1
		Governance	Operations	Indicative Maturity
ORG 1	Security Related Organisation and Policies	2	2	2
ORG 2	Security Assessments and Reviews	2	2	2
ORG 3	Security of Physical Access	4	4	4
CM 1	<b>Inventory Management of Hardware / Software Components and Network Communications</b>			
CM 1. a	Documentation	3	3	3
CM 1. b	Configuration and Change Management	3	2	2
NET 1	System Segmentation	2	2	2
NET 2	Secure Wireless Networks	0	0	0
NET 3	Secure Remote Access	2	1	2
COMP 1	Devices and Media	1	1	1
COMP 2	Malware Protection	2	1	2
COMP 3	Patch Management	1	1	1
DATA 1	<b>Protection of Data</b>			
DATA 1. a	Data Management	2	1	2
DATA 1. b	Cryptographic Technologies	1	2	2
USER 1	Identification and Authentication	1	2	2
USER 2	Authorisation and Access Control	1	1	1
EVENT 1	<b>Event and Incident Management</b>			
EVENT 1. a	Detection and Logging	1	1	1
EVENT 1. b	Incident and Vulnerability Handling	2	1	2
AVAIL 1	System Availability and Intended Functionality	2	1	2
AVAIL 2	Backup / Restore / Archive	1	1	1

The next section provides the reader with the conclusions drawn for Case Study B.

### 5.3.3 Case Study B – Conclusion

The approach of Customer B site to OT Cyber Security is best described from a maturity perspective as ‘Managed’. This means that cyber risks are mostly addressed in a systematic manner. However, some risks may be outside of the corporate risk appetite. The site is at a medium risk of exposure to security events that could negatively affect operational activities and revenue. Thales allocated this maturity level based on assessment of the site findings against individual security practices

from IEC 62443-2-1 and their sub-categories. These security practices set the requirements for the standard and indicate what a 'good' OT Cyber Security standard looks like.

Although the IT Cyber Security practice was of a defined standard, many of the OT security practice elements brought this classification down because the site did not demonstrate an OT approach that was sufficiently aligned with industry best practice. Thales identified weaknesses around the following control areas:

- **Governance:** in several instances Customer B's IT Policies and Procedures was found to be inappropriate for the OT assets it applied to.
- **Network Segmentation and Remote Access:** while there was segmentation in place, the design and implementation contained a few shortcomings that would not provide sufficient protection in the case of a cyber-attack.
- **System controls:** vendor provided systems contained several weaknesses that would not provide sufficient protection against even low-skill adversaries. OT systems that were visually inspected were not patched regularly and or default or shared credentials were prevalent.
- **Logging and monitoring:** a network intrusion detection system was implemented. However, due to a few limitations and dependencies, the solution was found to be sub optimal.

OT security is a specialised endeavour. While the IT Cyber Security and networking teams may be able to take the lead on planned forecasting, with buy in from the OT engineering team and even shoulder some of their day-to-day work, the IT team will require additional resources to execute a plan. Thales recommends establishing a holistic OT CS programme based on IEC 62443-2-1. This will ensure that Customer B establish the appropriate governance and technical controls that are required for running any successful OT CS programme.

The next section will provide a comparative analysis of the case study A and case study B results.

## 5.4 Comparative Analysis of Case Study Results

As a finding of the various case studies, three specific problem areas were identified across both plants, regardless of their differences in Cyber Security maturity levels or the frameworks used to assess them. Each of the frameworks has notable security control grouping similarities that became evident in the results of both case studies.

In summary, although good Cyber Security hygiene was seen across some segments in the IT environment of both case studies, it was poor in the OT environment. Network Segmentation and Remote Access to the plant was problematic. In respect to the critical systems identified in both the plants, at least one or more of the system's, had poorly designed HMI input controls (PLC Security, 2021). In respect to the organisational elements observed, although both plants had some form of security monitoring, the SOC teams were primarily IT experts and lacked the expertise and processes required to understand OT protocols or alerts surrounding when to act in the event of an attack. These parallels between topic areas are summarised as mappings shown in Figure 5-5.

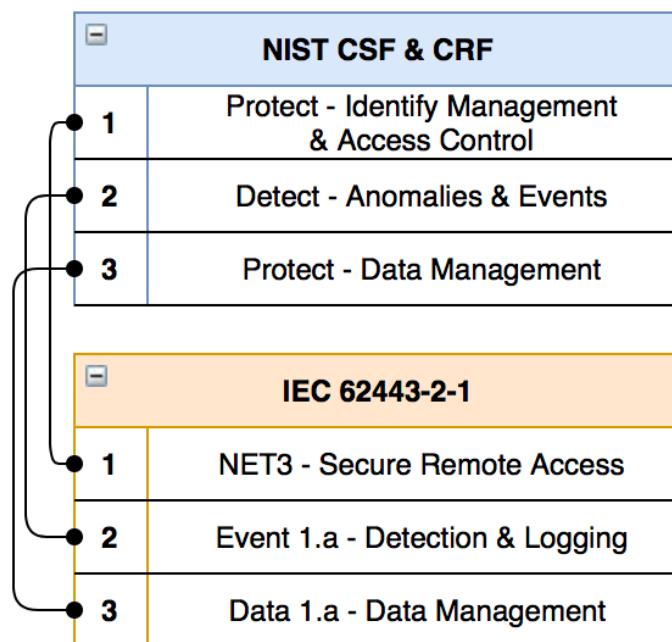


Figure 5-5 Mapping case study framework results

The results of each case study concluded that an organisation should have a well-established level of CS hygiene prior to undertaking a Cyber Resiliency assessment. Although the frameworks provided an approach to assessing each plant, the difficulty and resources needed to obtain a security and resilience baseline was not fit for purpose and would not provide a true measure of how a company had improved over time. The problems within each case study, although different, did share similarities across their problem spaces as described above. Conclusions derived from case study results show that an organisation should have a mature CS operation before a CR analysis can be performed appropriately.

Table 5-31 shows the comparative results between both case studies and mapped to IEC 62443.

Table 5-31 Case study results comparison mappings

Assessment Area	Description	Case Study B		IEC 62443-2-1 Indicative Maturity	Case Study A		IEC 62443-2-1 Indicative Maturity
		Governance	Operations		Governance	Operations	
ORG 1	Security Related Organisation and Policies	2	2	2	1	1	1
ORG 2	Security Assessments and Reviews	2	2	2	1	1	1
ORG 3	Security of Physical Access	4	4	4	4	4	4
<b>CM 1</b>	<b>Inventory Management of Hardware / Software Components and Network Communications</b>						
CM 1.a	Documentation	3	3	3	1	1	1
CM 1.b	Configuration and Change Management	3	2	2	1	1	1
NET 1	System Segmentation	2	2	2	2	2	2
NET 2	Secure Wireless Networks	0	0	0	0	0	0
NET 3	Secure Remote Access	2	1	2	1	1	1
COMP 1	Devices and Media	1	1	1	1	1	1
COMP 2	Malware Protection	2	1	2	1	1	1
COMP 3	Patch Management	1	1	1	1	1	1
<b>DATA 1</b>	<b>Protection of Data</b>						
DATA 1.a	Data Management	2	1	2	1	1	1
DATA 1.b	Cryptographic Technologies	1	2	2	1	1	1
USER 1	Identification and Authentication	1	2	2	1	1	1
USER 2	Authorisation and Access Control	1	1	1	1	1	1
<b>EVENT 1</b>	<b>Event and Incident Management</b>						
EVENT 1.a	Detection and Logging	1	1	1	1	1	1
EVENT 1.b	Incident and Vulnerability Logging	2	1	2	1	1	1
AVAIL 1	System Availability and Intended Functionality	2	1	2	2	1	2
AVAIL 2	Backup / Restore / Archive	1	1	1	2	2	2

## 5.5 Chapter Summary

The case study results show that a weak baseline Cyber Security always led to low Cyber Resilience results, rendering the initial CR baselines or enhancement measures ineffective. The significant difference of data elicited from these real-life studies provided a baseline dataset for the design of the testbed and is discussed in the next Chapter.

# Chapter 6

## Simulation & Modelling

### 6.1 Introduction

This section provides an overview of the simulation and modelling methods used in this experiment. The testbed is designed to replicate a real-world industrial system while avoiding interference with real-time services and without the need to encompass the entire plant. The simulation aims to represent a typical industrial scenario, which was informed by insights from various case studies (as discussed in Chapter 5).

To achieve an effective design and development of a Cyber Resilient system, it is essential to employ experimental methods that allow for quantitative measurement of Cyber Resilience. The testbed's purpose is to assess the performance of a critical system when equipped with Cyber Resilience enhancements based on the recommendations from case studies, best practices and requirements outlined in regulations, standards and guidelines. Examples of such standards and guidelines include ISA/IEC-62443, PLC Security – Top 20 and NIST Special Publication 800-82.

The primary objective of developing this Cyber Resilience testbed is to utilise real-world use cases employing physical OT equipment. By recreating a critical-safety Industrial Control System and measuring its performance both before and after implementing CR enhancements, the testbed serves as a platform to gauge the effectiveness of these improvements. Building upon the findings from the case studies, which highlighted three specific problem areas across both plants (discussed in Chapter 5), the testbed is specifically designed to replicate these weaknesses to evaluate the optimal outcomes.

The subsequent sections will provide a detailed description of the testbed setup.

## 6.2 Phase 2 - Testbed Design

This section describes the representative manufacturing system model used in this test bed. It includes the plant scenario description, the purpose and objective of the representative system and its operation, process flow and control.

### 6.2.1 Testbed Description and Scenario Use Case

The experimental testbed used in this research represents a typical manufacturing environment, specifically, in the production of Infant Milk Formula (IMF). Emulating a temperature control system with remote access functionality. The testbed is made up both physical and virtual components. The physical components (described in section 6.2.2.21) include a PLC (in particular, a Eurotherm 2000), an HMI Station, a Type K Thermocouple temperature sensor and a remote access router namely a EWON. All other components in the test bed are virtualised within the cyber range topology (as described in section 6.2.2.2).

In this given scenario, the IMF production line typically consists of six parts, Delivery of raw ingredients, Pre-treatment, Production, Filling, Packaging and Storage. Infant milk production is highly regulated and so quality assurance is completed at all levels throughout the process lifecycle. To record quality control results, access is granted to the corporate file share sever to collect and record all activities that relate to the quality and safety of the formula throughout its production process. Figure 6-1 depicts each stage of the production process.



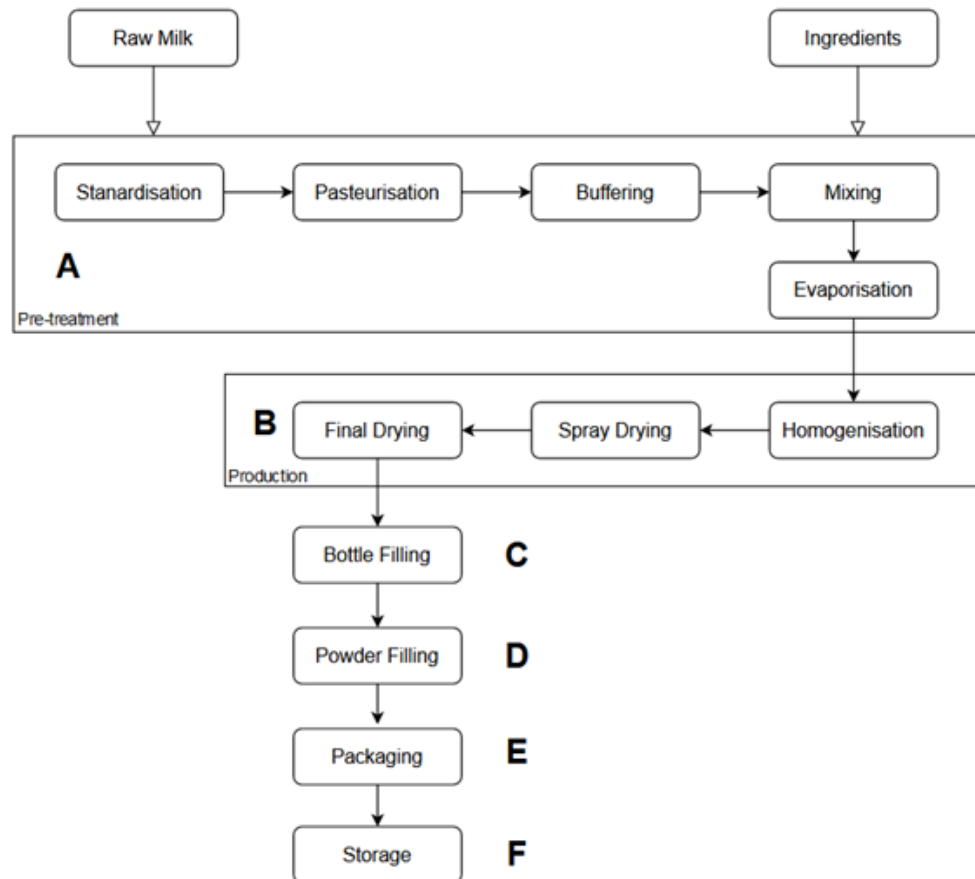


Figure 6-1 Production processing steps

Temperature levels are important in several areas of a milk processing plant, including:

- Milk reception and storage: when raw milk is delivered to the processing plant, it needs to be stored at a cool temperature to prevent bacterial growth and maintain the quality of the milk. The temperature in the milk reception area should be maintained at around 4°C.
- Before processing, the milk needs to be brought to a temperature between 20-26°C to facilitate the separation of cream and other processing steps.
- Pasteurisation: a critical part of the process as it reduces the risk of microbial contamination to ensure the product can be safely consumed by new-borns. Typically uses elevated temperatures (e.g., 78°C or above) for short periods.
- Powdered milk storage: milk powders are stored at temperatures below 55°C. Many chemical changes can occur if stored at higher temperatures, even for a brief time, which may induce deteriorative changes (Cheng et al., 2017) such as lactose crystallisation and browning reactions (Brownlee et al., 1984).

The optimal temperatures during the production of infant milk formula depend on the specific stage of the production process. The critical temperature levels and allowable time limits are set

to ensure the safety and quality of the infant formula. The maximum allowable time to operate either above or below the critical temperature levels can vary depending on several factors, including the specific stage of the production process, the type of equipment used and the quality and safety standards in place. Any deviations from the optimal temperature range must be addressed as quickly as possible to minimise any potential impact on the safety and quality of the infant formula.

The values of the temperature sensor readings are stored in the PLC (EPC 200) holding registers and are periodically polled by the HMI and EWON flexy (VPN) interfaces using the function code 0x03 (Read Holding Register). To control/monitor the testbed, an HMI software (Advanced HMI) is used to provide a graphical user interface to assess the PLC values and display the temperature readings via Modbus TCP communication. When temperature values require adjusting, this can be controlled using the HMI set point buttons via the Function Code 0x06 (write holding register). Data for the experiment is collected using a Network Probe/TAP and Wireshark and Excel used to analyse the data. A topology of the physical components is provided in Figure 6-2.

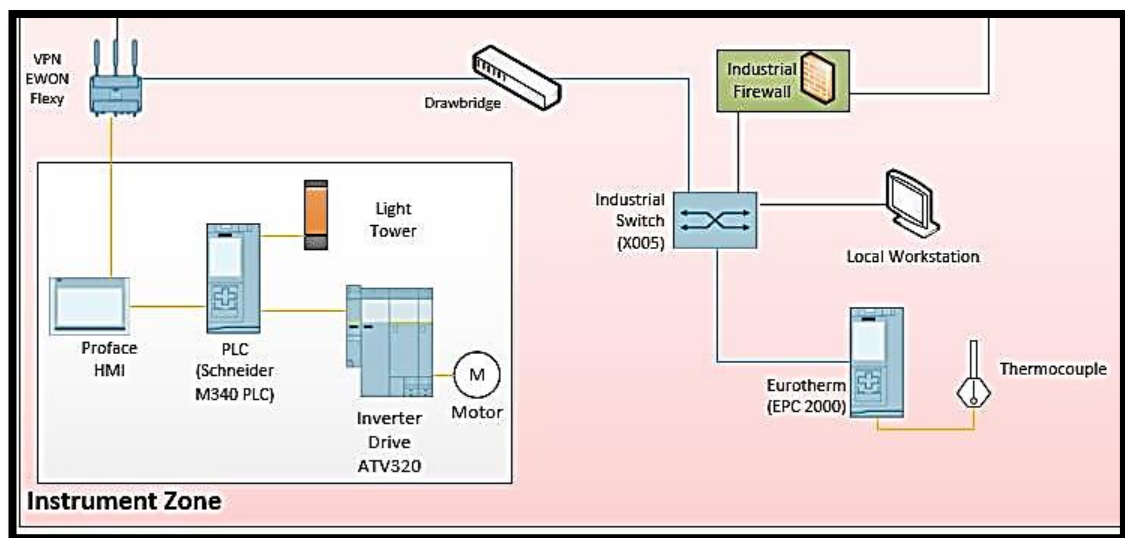


Figure 6-2 OT Network Architecture topology

The plant operator is required to enter the working temperature for the vessel to operate at. This may fluctuate slightly depending on the type of milk product being processed on any given day. Upon starting the HMI, the plant operator is provided with an overview of the set temperature value in the milk vessel and a numeric value of measured temperature. The set value is one that can be manually set by the operator and the measured value gives the actual temperature value inside the vessel. Once the vessel reaches the desired temperature, the measured temperature will be maintained within the vessel.

This is controlled at the PLC, which takes the measured temperature from the thermocouple and feeds it into the PID block. This block applies the PID algorithm to provide a physical heat output (IO1) based on the set point temperature in comparison to the measured temperature. The configuration is given in Figure 6-3.

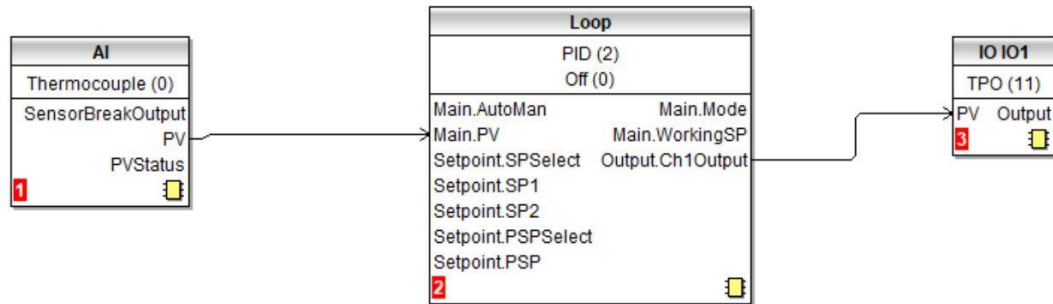


Figure 6-3 PLC threshold configuration

Within the PLC program, the set temperature limit value is compared against the measured temperature value. The safe operating temperatures for this part of the processing plant are defined as:

- Safe working limit = 20-25°C
- System warning level= 25.9°C
- System Critical level = >26°C

If the temperature set point within the PLC were modified to temperatures higher than these values, then a risk of contamination to the product could occur due to excessive temperatures within the vessel. If temperatures increase beyond the set limits the operator would be alerted by a series of visual alarms on the HMI.

As part of the system design, system engineers can configure additional programming that would apply limits in either the PLC logic, HMI or both to ensure temperature set points are set within a given validation criteria. This technique is referred to in the secure PLC coding guidance on best practice surrounding this topic however, this guidance has only recently been introduced in the Industrial Automation and Control domains since 2021 (PLC Security, 2021).

The configuration would need to be implemented within the PLC program itself as shown in Figure 6-4 and Figure 6-5. If the PLC configuration implemented this method of validation, the attack demonstrated in this experiment would not have been as damaging to the Infant Milk Production.

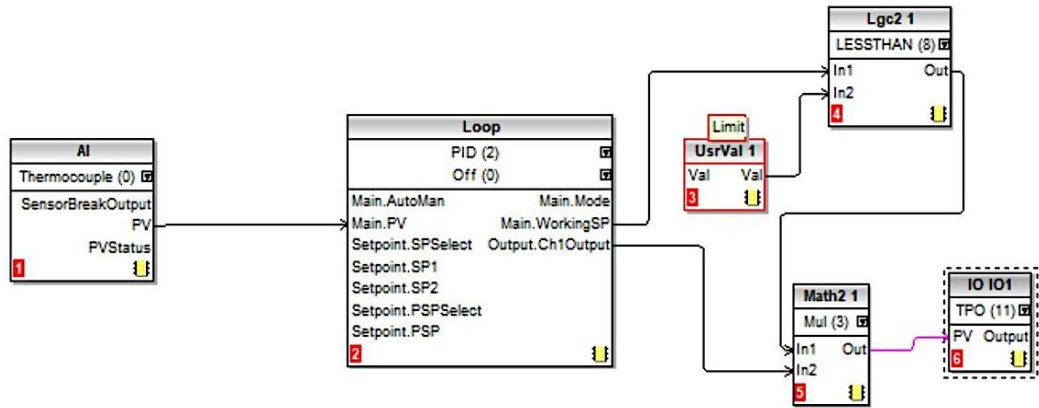


Figure 6-4 PLC threshold configuration

C:\Users\secadmin\Documents\Eurotherm\EPC2000\_Bench\_1.uic - Function Block View (L...

Function Block: Loop

Main Config Setpoint Feedforward Autotune PID Output Diagnostics

Name	Description	Address	Value	Wired From
RangeHigh	Loop upper operating point	12	1372.00	
RangeLow	Loop lower operating point	11	-200.00	
SPHighLimit	SP1/SP2 upper limit	111	1372.00	
SPLowLimit	SP1/SP2 lower limit	112	-200.00	
SPSelect	SP1 or SP2 select	15	SP1 (0)	
SP1	Setpoint 1	24	20.00	
SP2	Setpoint 2	25	0.00	
Program Setpoint	Select the program setpoint	1664	Off (0)	
Program Setpoint	Program Setpoint	1665	0.00	
RSPType	Selects the RSP configuratio	535	Setpoint (0)	
RSPHighLimit	RSP upper limit	1674	1572.00	
RSPLowLimit	RSP lower limit	1675	-1572.00	
RSP_En	Enable the RSP input	1666	Off (0)	
RSP	Remote Setpoint input	485	0.00	
SPTrimHighLimit	SPTrim upper limit	66	0.00	
SPTrimLowLimit	SPTrim lower limit	67	0.00	
SPTrim	Setpoint local trim value	27	0.00	
SPRateUnits	Rate limit units	531	PerSecond (0)	
SPRateUp	Setpoint up rate limit	35	Off (0)	

Figure 6-5 Eurotherm function block set-point

To replicate such scenario in an experimental test bed, the next section discusses the physical and virtual components used.

## 6.2.2 Physical and Logical Components

This section discusses the physical and virtual components used in the test bed.

### 6.2.2.1 Physical Components

The physical equipment used in this experiment is housed at Thales Ebbw Vale and described in Table 6-1.

*Table 6-1 Physical components in the testbed*

<b>Physical Component List</b>	<b>Description</b>
Network Switch Siemens	Industrial network switch (layer 2)
Schneider Modicon PLC software Control Expert	PLC software
Schneider Modicon PLC M340 CPU	CPU
Schneider Modicon PLC M340 PSU	Power supply unit
Schneider Modicon PLC M340 8IN 8 OUT	Input/output Module
Schneider Modicon PLC M340 4-way backplane	4-way backplane for PLC
Pro-face / Schneider HMI GP4000	Human machine interface
Eurotherm / Schneider EPC2000 Process control	Programmable Logic Controller
Schneider program lead	Physical cable
Pro-face program software GP PRO EX	Software for the HMI
Type K thermocouple	Temperature Sensor
Ewon Flexy 205	Remote router for industrial uses.
Allen Bradley PanelView	Human Machine Interface

The above equipment can be seen in Figure 6-6 and Figure 6-7.



Figure 6-6 Physical testbed (full)

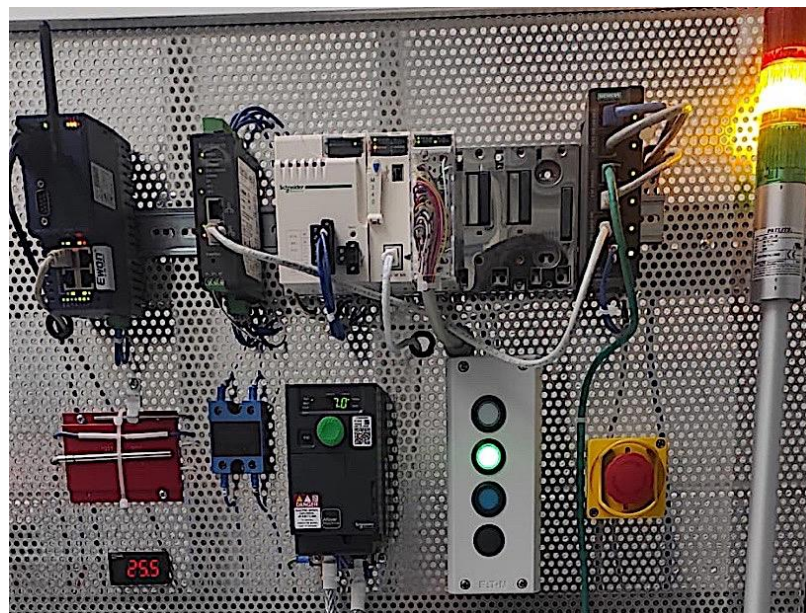


Figure 6-7 Physical Testbed (zoomed)

The equipment schematic diagrams are given in Figure 6-8, Figure 6-9 and Figure 6-10 to provide context on how the physical equipment is connected.

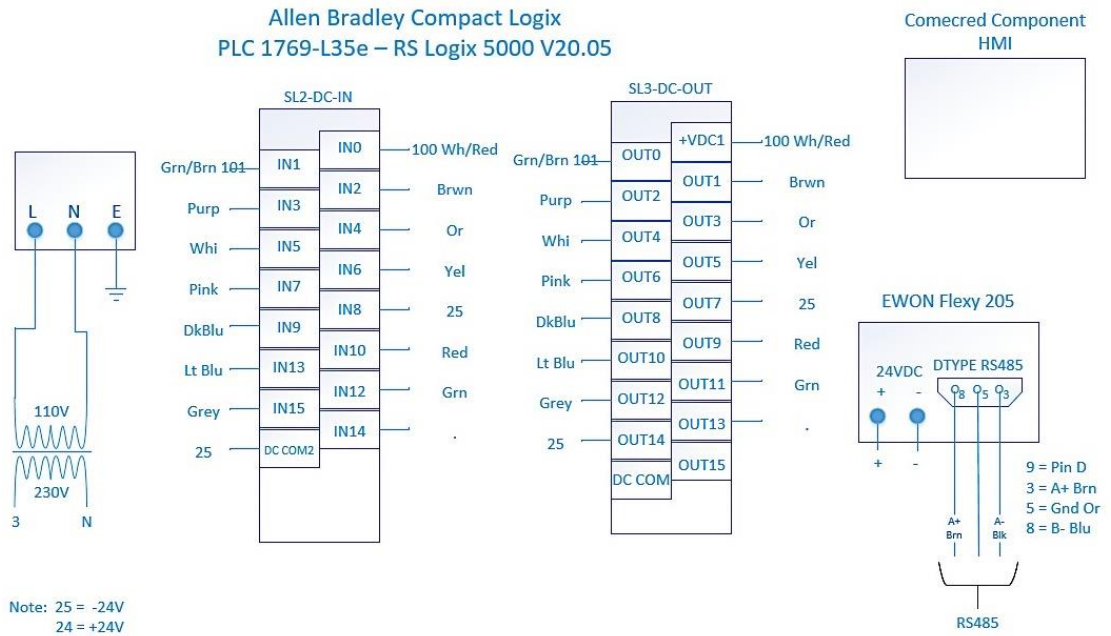


Figure 6-8 Schematic Diagram 01 drawn by Dene Yandle (2023)

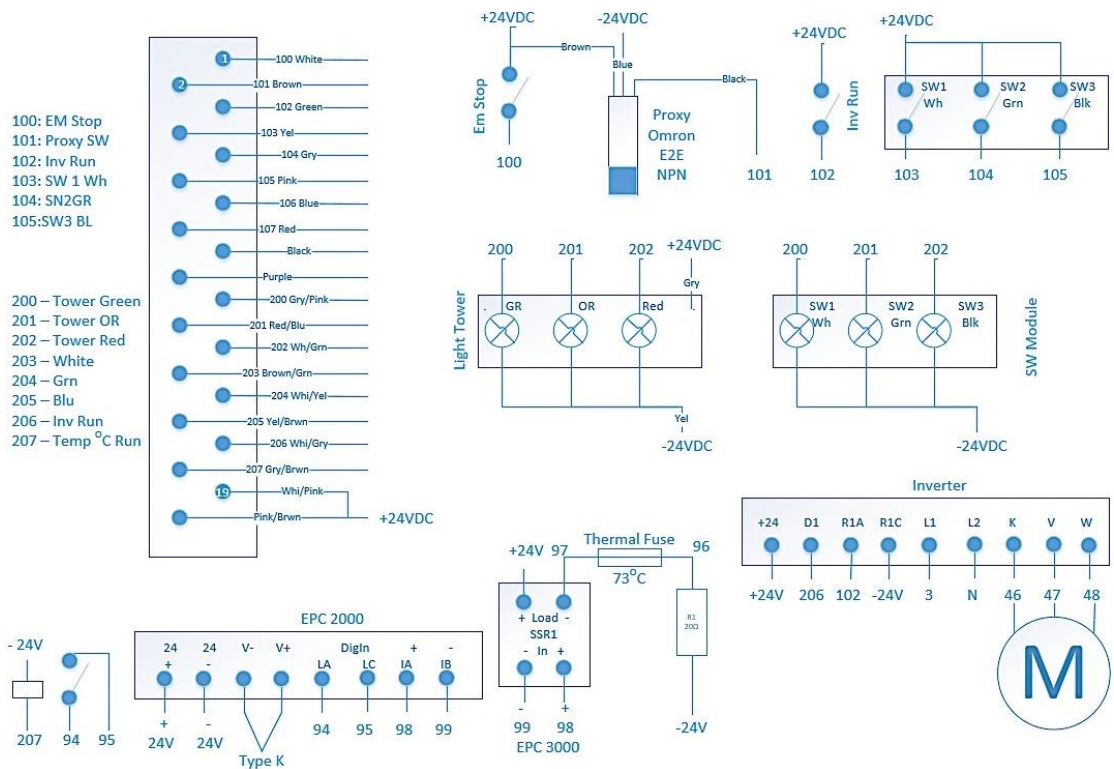


Figure 6-9 Schematic Diagram 02 drawn by Dene Yandle (2023)

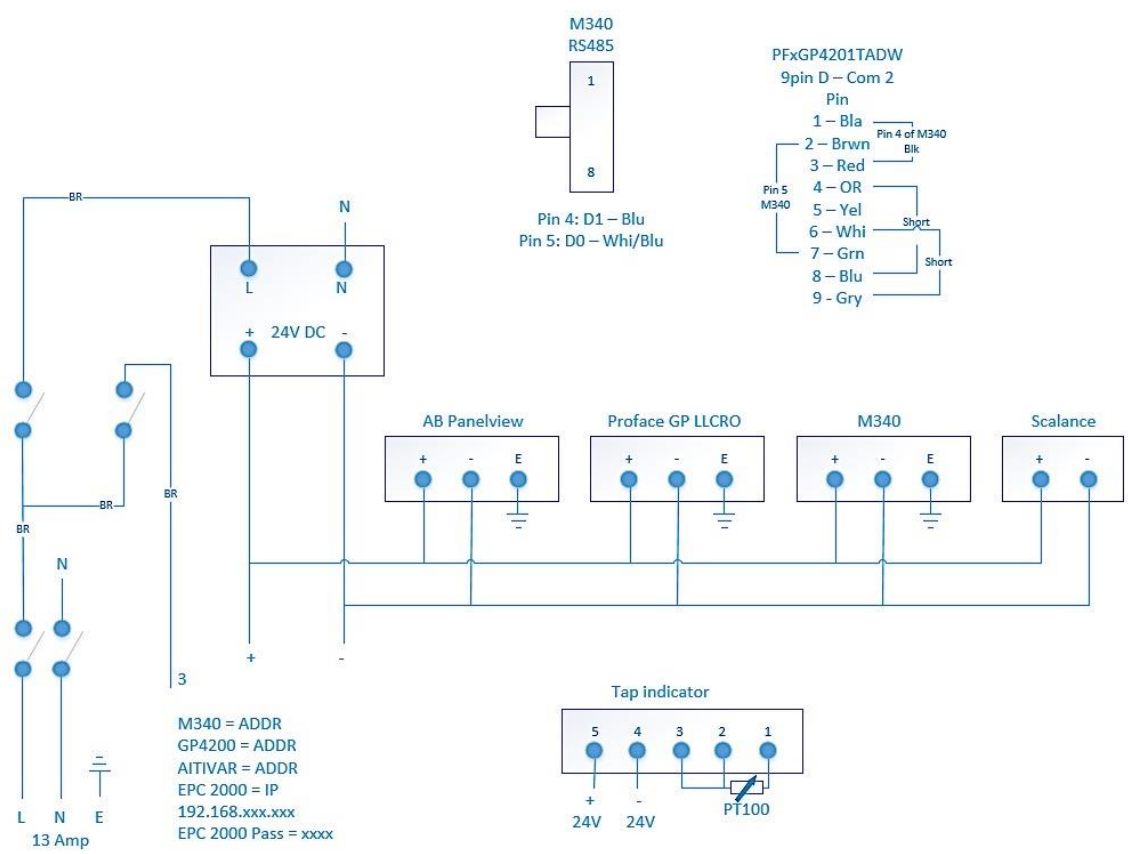


Figure 6-10 Schematic Diagram 03 drawn by Dene Yandle (2023)

**HMI:**

Within the HMI, the inbuilt web server is enabled to ‘mirror’ the functions of the HMI in real time and is typically used in manufacturing environments to enable remote access into the HMI using a standard web browser (see Figure 6-11).

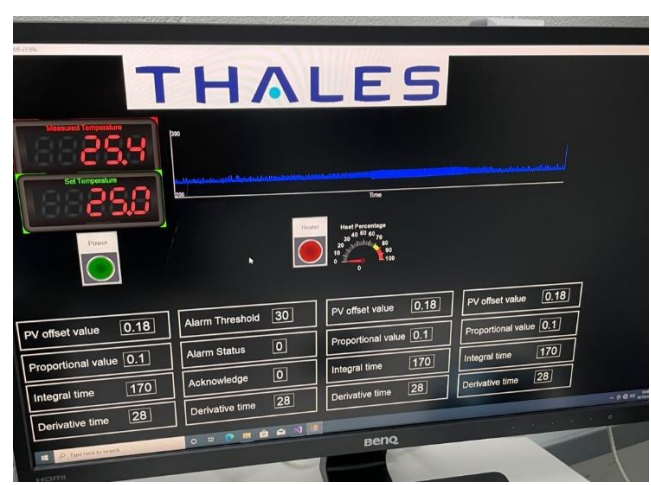


Figure 6-11 Representative physical system – HMI



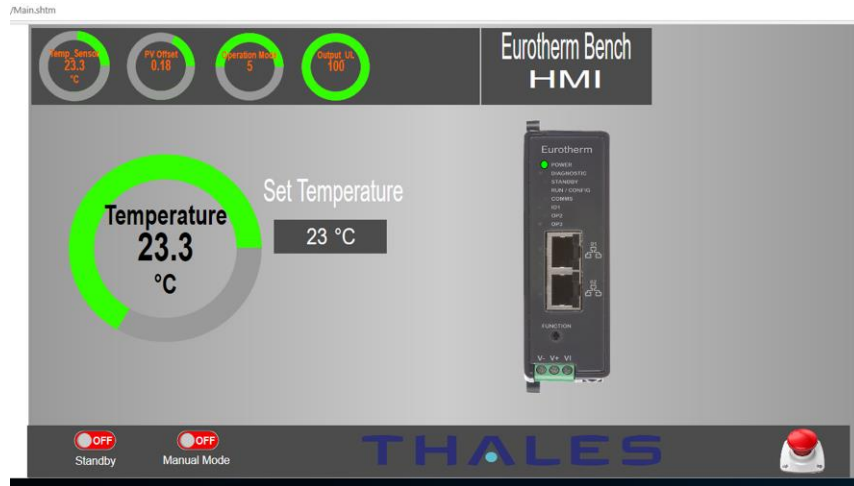


Figure 6-12 The EWON server interface

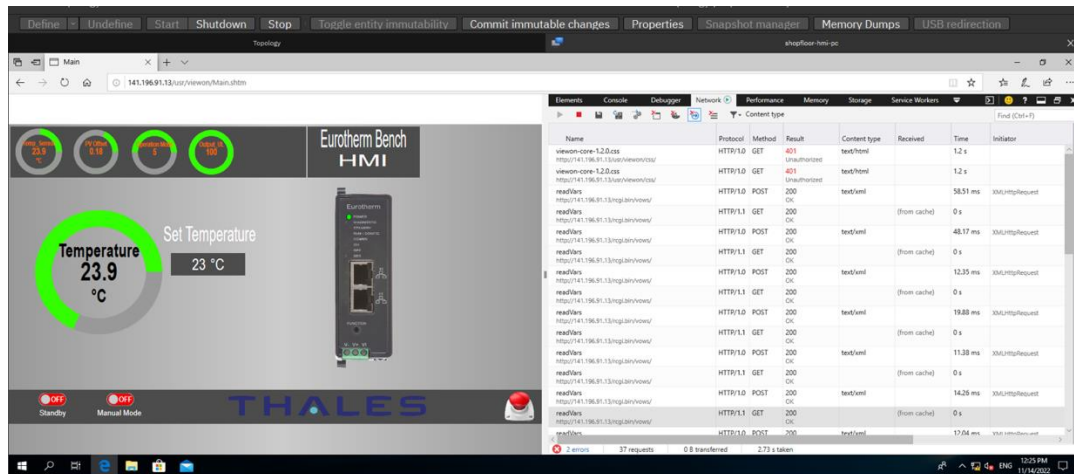


Figure 6-13 The EWON VPN remote Interface

This section described all the physical hardware and connections used in this testbed. The next section describes the logical components such as the virtual machines and software used, communication protocols and configuration of the systems.

### 6.2.2.2 Logical Components

This section details the software, configuration, communication protocols and the system design.

#### Cyber Range Integration

The following section will provide an overview of the cyber range testbed and its setup. It details the virtual components used, a description of their OS types and how they interconnect to the physical manufacturing system.

The cyber range platform is installed at the National Digital Exploitation Centre (NDEC) Cyber Lab in the UK. The National Digital Exploitation Centre (NDEC), operated by Thales, opened in South Wales in 2019. Built in partnership with Welsh Government and the University of South Wales, it provides a facility where Industry, Government and Academia work together to create a world class centre of excellence in digital technology and cyber-security. The virtual simulation platform is powered by DIATEAM and natively designed to demonstrate attack and defence cyber-security scenarios in a hyper realistic hybrid environment. The platform consists of a library of embedded ISO Images, virtual machines and allows the creation of topologies or scenarios for different use cases.

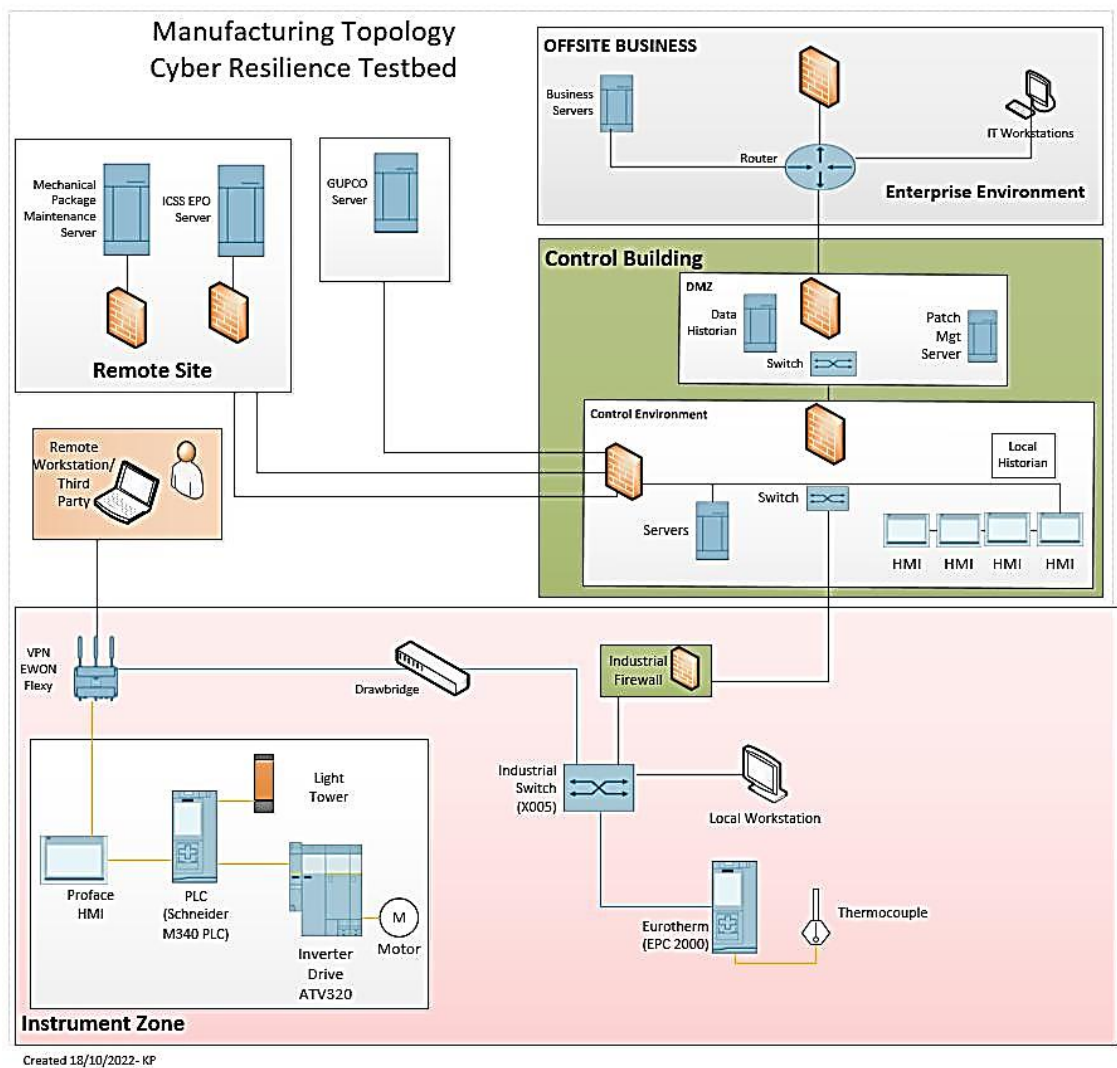


Figure 6-14 Topology of the representative environment created on the cyber range.

The testbed environment used in this thesis is based on the representation of a systems logical network. This representation is called a topology. A topology is composed of several entities which are connected through a network simulation tool using virtual wires. These entities can be either

Virtual Machines (VMs) or physical components utilising real network interfaces that connects the real world and the virtual one as shown in Figure 6-14.

Based on the representation of a manufacturing system. The topology above depicts the different layers of the Purdue Model (as discussed in Chapter 3), all assets represented in the above topology are virtual components apart from those identified in the red area labelled 'Instrument Zone'; which depicts the physical equipment (described in Section 6.2.2.1).

The following virtual machines are included in the cyber range topology:

- Kali Linux (Attackers Machine)
- Windows 10 Machine (the third-party contractor)
- Windows Server (As the Quality Control Machine)
- pfSense Virtual Firewalls
- Virtual Switching (including VLANS)
- Advanced HMI

#### *Advanced HMI*

This virtual machine can be identified as the first 'HMI' displayed in the green area labelled 'Control Environment' on the Topology in Figure 4-9. Using Advanced HMI with Visual Studio enabled the creation of a bespoke graphical user interface. The user interface depicts a typical industrial setting and has been connected to the OT equipment using Ethernet.

#### *Industrial Communication Protocols*

Various industrial protocols are employed throughout the testbed including routable and non-routable IP protocols. Routable protocols include Internet Protocol (IP)-based protocols (e.g., Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)) as well as industrial application layer protocols (e.g., Modbus/TCP).

#### *PLC Program*

Configuration of the PLC was achieved using 'Allen Bradley RSLogix Micro' software. The report can be seen in Appendix 1 and was generated within RSLogix showing the details of the programs function through ladder logic programming techniques. The code contained within 'LAD 8' is specifically related to the Industrial process depicted on the HMI. It is the PLC tags & variables within LAD 8 that the HMI is interacting with to provide the process feedback to the operator.

### *Interconnection between the physical and virtual components*

External components that cannot be virtualised within the cyber range virtual topology are connected using real network interfaces, this ensures communication is shared between the real world and the virtual one. The use of a hybrid port enabled this interconnection between the non-virtualised elements and the virtual topology. The integration, verification and validation tests are crucial while building any complex information and communication technology solution. To perform the corresponding tasks, a dedicated test bench, linked to a testing environment, to ensure the environment is as realistic as possible. A span Port (port mirroring capability or RSPAN) is a port on a network switch that allows traffic on a switch to be mirrored and fed into a monitoring tap or probe to capture the network traffic. The next section will describe the cyber-attack design.

### 6.2.3 Cyber-Attack Design

This section describes the disturbance source and description of the cyber-attack (remote attack) and the motivation for this attack design. It details the approach on how the attacker attempts to compromise the representative manufacturing system. A diagram of the attack sequence can be seen in Figure 6-15.

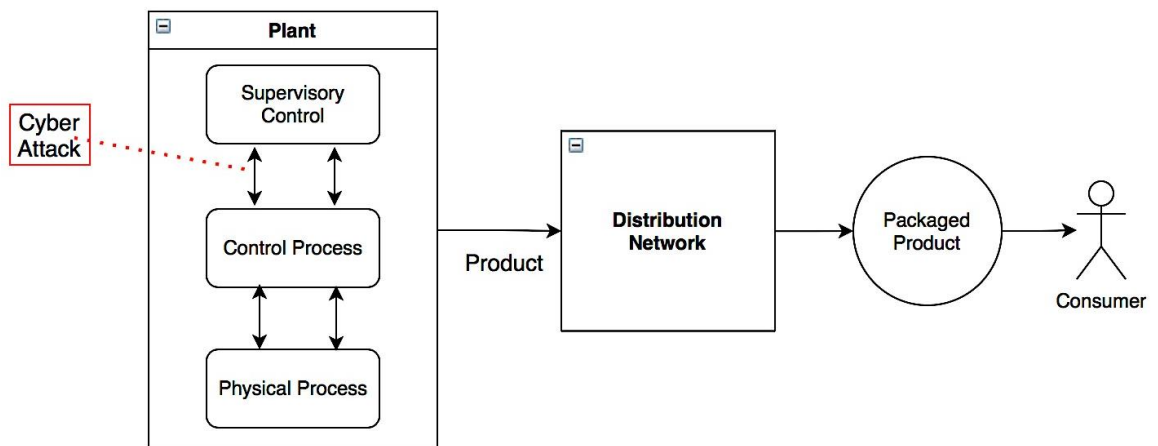


Figure 6-15 Diagrammatic structure of the remote attack

The motivation for designing this cyber-attack came about from the finding of the various case studies discussed in the next chapter, three specific problem areas were identified across both plants, discussed in Section 5.4. The attack was specifically designed to target the three weaknesses identified from the case studies undertaken.

Furthermore, the selection of an ARP poisoning attack, was chosen due to the reported number of ARP poisoning attacks targeting the industrial control sectors, particularly in critical infrastructure

systems such as power plants, water treatment facilities and manufacturing plants. These attacks can have severe consequences, as they can disrupt the operation of industrial control systems and cause physical damage to equipment or endanger human lives.

One well-known example of an ARP poisoning attack in the industrial control sector is the Stuxnet worm discussed in Section 2.4.1. Stuxnet was a sophisticated malware designed to specifically target industrial control systems, particularly those used in Iran's nuclear program. The malware used a combination of techniques, including ARP poisoning, to compromise the target systems and cause physical damage to centrifuges used in the uranium enrichment process. In another instance, researchers from the Cyber Security firm Dragos reported an ARP poisoning attack on a petrochemical plant in Saudi Arabia in 2017 (Dragos, 2022). The attack was part of a broader campaign targeting industrial control systems in the Middle East, which involved the use of custom malware and other advanced techniques. These incidents highlight the importance of securing industrial control systems against cyber threats, including ARP poisoning attacks.

The attacker wishes to compromise the plant data; however, the plant is air gapped. The attacker targets an external contractor who supports the plant and has remote access which make it possible for engineers to access the plant remotely. The attacker packages a payload inside a word document created using Villain (T3l3machus , 2022). Villain is a Windows & Linux backdoor generator that can embed a reverse shell in an email with the ability to bypass Windows defender. A phishing email requiring an urgent security update is sent to the third-party contractor containing the payload. The email arrives in the victim's inbox and the attachment is opened, immediately starting the malicious exe that spawns a reverse shell to the attacker. Unaware, the victim proceeds to access the plant network via a remote VPN tunnel, which is normal day-to-day activity. The attacker uses the reverse shell to route through the VPN tunnel identifying as the victim. This deception would bypass any of the security mechanisms the plant has in place since the connection is seen as legitimate.

The attacker uses NMAP to scan the plant network and can find interesting ports namely 139 NETBIOS and 445 SMB on an asset inside the OT segment of the plant. These ports indicate some sort of file share and is the quality assurance computer located in the plant enabling them to update their highly regulated quality records. The attacker enumerates the SMB asset and discovers an fs root mount. They then proceed to put the Secure Shell (SSH) Public Key in the authorised keys and log in using the stolen SSH credentials. Once on the quality assurance computer, the tool 'Ettercap' is used to obtain an absolute list of devices/macs in that subnet. The attacker moves the PyModbus

and Modbus TCP scripts to the quality assurance computer and stores them inside the user area. The SSH credentials are used to log in once again and 'su' escalates privileges.

Scripts are then run to read PLC values (since the attacker knows the PLC IP address from an earlier NMAP scan). The attacker analyses the traffic and identifies behaviourally, that the 2nd and 3rd Modbus registers are the read values and set values that control the temperature within the milk vessel. Using the quality assurance computer, the attacker performs an 'ARP poisoning attack' and acts as a man in the middle to obtain and redirect the traffic between the PLC and the HMI (avoiding spoofing any mac address to avoid detection). The attacker changes the read and write values.

The sequence of the attack is provided in Figure 6-16.

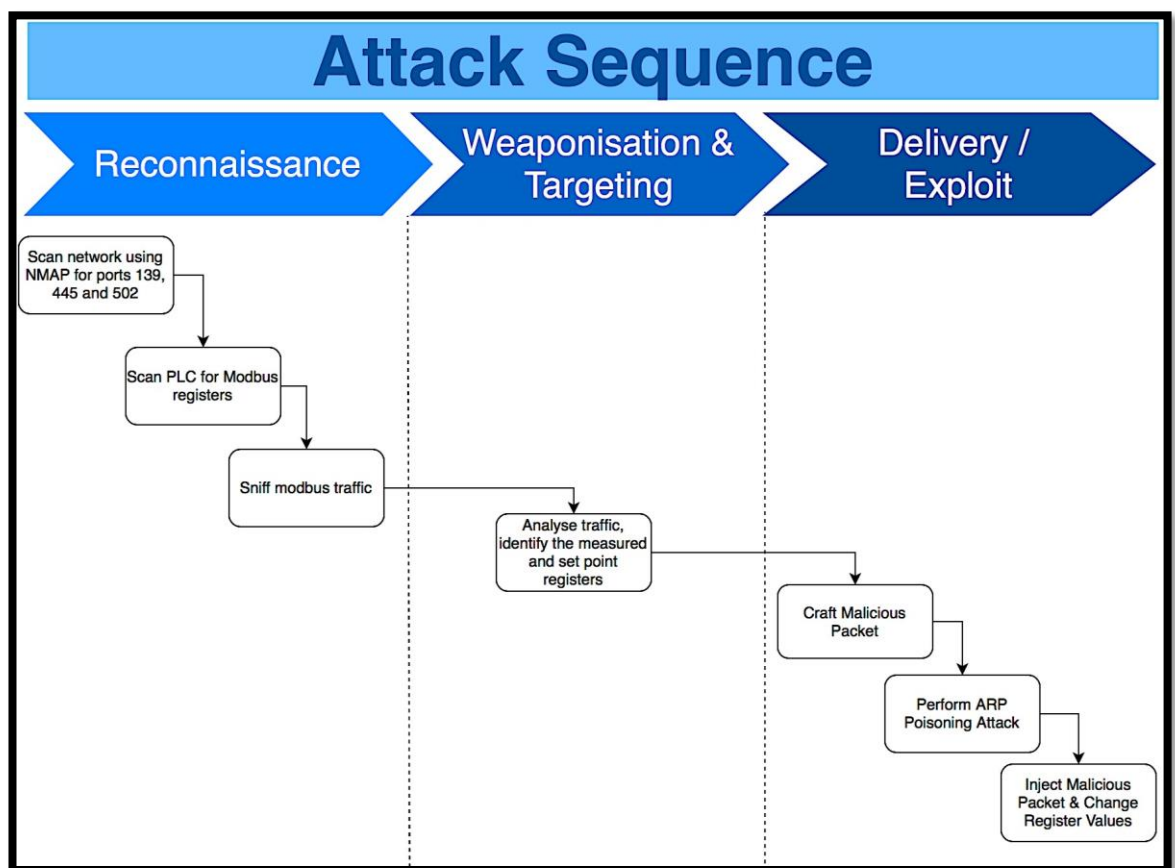


Figure 6-16 Cyber-attack sequence

The attacker could go on to change the password of account/disable others to lock plant out, change thresholds in the PLC, removing the ability for the plant to amend the set point. This could force the plant into shut down. Important documents that are essential to the safe operation of the plant (quality and risk assessment, historical data, safety testing records) could be lost or

encrypted, which would bring the entire plant to a halt and stop production until the problem can be remedied.

## 6.3 Phase 3 – Definition of Metrics and Specification of Tests

Phase 3 provides the definition of selected CR attributes and metrics, the reasoning behind each metric choice and the specification of the experiments. The next section discusses the resilience enhancements.

### 6.3.1 Selection of Resilience Enhancements

As a finding of the various case studies described in Chapter 5, three specific problem areas were identified.

1. There was external remote access to OT systems and a lack of network segmentation.
2. Monitoring and understanding of industrial specific logs were inadequate.
3. The PLC design relating to secure input controls was poorly considered.

In response to the three problem areas specified above, recommendations for enhancing resilience were provided (see section 6.3.1.1-3) which in summary include:

- Network Segmentation: Segment the system into smaller networks with restricted access, so that if any attacker can gain access to the manufacturing system, they will not be able to gain access to other areas of the system.
- Monitoring and understanding OT logs: Properly monitor and understand the logs of the manufacturing system for any suspicious user activity. This includes monitoring for any sudden changes in login timings, logins from unexpected geographic locations, unusual user activity and the OT communication protocols.
- Adopt Secure PLC system configuration practices (as described in Chapter 3) and control eight, in particular, which states: “Validate HMI input variables at the PLC level, not only at the HMI” (PLC Security, 2021).

These recommendations are explored further in the following sections.

#### 6.3.1.1 Network Segmentation

Network segmentation is a crucial step in securing both OT and IT environments but implementing it in an industrial control setting can be challenging due to the incompatibility of IT technologies with OT environments (General Electrics, 2017). However, network segmentation is essential for a mature Cyber Security profile and can significantly enhance reliability and safety. According to (ISA, 2020), system operators and integrators should define and implement segmentation specific to



their OT environments. This involves isolating systems into functional groups with similar security requirements, establishing proper zones and conduits. Such isolation makes unauthorised access and exploitation of critical devices more difficult and helps minimise the impact of a breach.

As also summarised in Chapter 2, an effective network segmentation solution, in OT environments, should allow for easy zone-level separation without physically relocating equipment, which is often impractical due to the size or remote location of critical devices. Therefore, a virtual or logical network segmentation approach is necessary, even when equipment is distributed across different sites (see Figure 6-17). Importantly, the segmentation process should not require reconfiguration or re-engineering of the OT network, as network changes causing disruptions or downtime are unacceptable (International Electrotechnical Commission (IEC), 2021); (General Electrics, 2017).

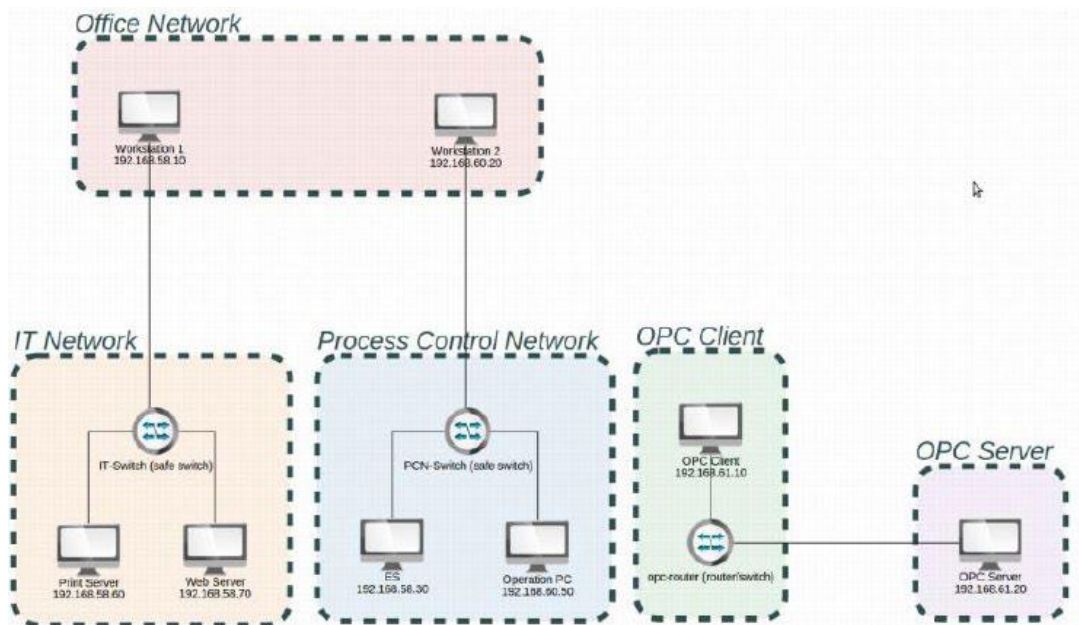


Figure 6-17 Zoning example, adopted from (General Electrics, 2017)

### 6.3.1.2 Training for SOC staff (Monitoring OT logs):

For effective analysis and filtering of network traffic in industrial environments, it is essential to have a solution that understands the communication protocols used, such as Modbus, DNP3 and OPC. The first step is protocol recognition, followed by deep protocol inspection. This level of scrutiny is necessary because even legitimate protocol commands can be exploited for malicious purposes, including web network-based exploits, insider attacks or denial of service attacks. To prevent potential physical damage to critical network assets, every aspect of the data flow, including packet bits, headers and payloads, must be thoroughly examined. The solution should make informed decisions based on the complete context of the packet, considering factors like the protocol used,

industrial application, addressing, sessions and distinguishing normal from malicious traffic (International Society of Automation (ISA), 2020).

Furthermore, collaboration between security analysts, IT professionals, plant operators and system engineers are essential for effective Cyber Resilience. Bridging the gap between IT and OT personnel is necessary to ensure a comprehensive understanding of control system design principles, Cyber Security risks and operational drivers (Syrmakeisis, et al., 2022). The convergence of professional knowledge and expertise enables the development of secure engineering practices and real-time IT/OT support for industrial manufacturing systems.

To ensure security in OT environments, specific policies must be enforced within each zone. These zones can have different combinations of protocols, devices and locations, requiring tailored security policies for each network. Organisations should employ a solution with baselining capabilities that can record and analyse network traffic to establish a baseline of normal behaviour (National Institute of Standards and Technology, 2021). This allows for protection against both malicious and unintentional activities, ensuring a customised security policy for OT environments.

### 6.3.1.3 HMI input variables validation at the PLC level

As examined in Section 3.4.3.3, PLCs are commonly used in Industrial Control Systems to automate the operation of machinery and equipment and are critical to the functioning of many industries. It is therefore important to ensure that they are secure and protected from cyber threats. The (PLC Security, 2021) guidance provides a framework for securing PLCs by outlining a set of best practices that organisations can follow. Table 3-9 outlines a summary of these practices. Using this framework, control eight was applied to enhance the CR of the representative system.

*Table 6-2 Enhancements made to the testbed - adopted from (PLC Security, 2021).*

Control Eight	Description
Validate HMI input variables at the PLC level, not only at HMI.	HMI access to PLC variables can (and should) be restricted to a valid operational value range at the HMI but further cross-checks in the PLC should be added to prevent or alert on, values outside of the acceptable ranges which are programmed into the HMI.

A potential threat actor could create or replay modified packets to transmit arbitrary values to the variables within the PLC that can be influenced externally, such as values passed from an HMI. Furthermore, the protocols used by PLCs are considered "open" protocols and are publicly available. As demonstrated in the cyber-attack designed in Section 6.2.3, an intruder can identify

the mapping of PLC variables by analysing the network traffic during the initial stages of an attack. This knowledge enables the intruder to craft malicious traffic, specifically tailored to the target, allowing them to manipulate a process using unauthorised tools.

Implementing the control specified in Table 6-2 will enhance the 'Reliability' attribute of CR, since it can identify non-malicious human errors in programming. In addition, this control will also enhance the 'Security' attribute of CR, since it ensures the integrity of the process by cross verifying the values passed into the PLC prior to implementing them. This will mitigate the risk of receiving invalid data in memory locations. The next section will discuss the definition of metrics used in this experiment.

### 6.3.2 Definition of Metrics

The enhancements discussed in the previous section were categorised into CR attributes to determine which metrics to use in the experiments. The following sections will expand on how this is done.

To incorporate each of the Cyber, Physical and Organisational domains associated with Cyber Resilience (as explored in Section 3.4), each enhancement technique selected represents at least one of the domains (see Figure 6-18 and Table 6-3).

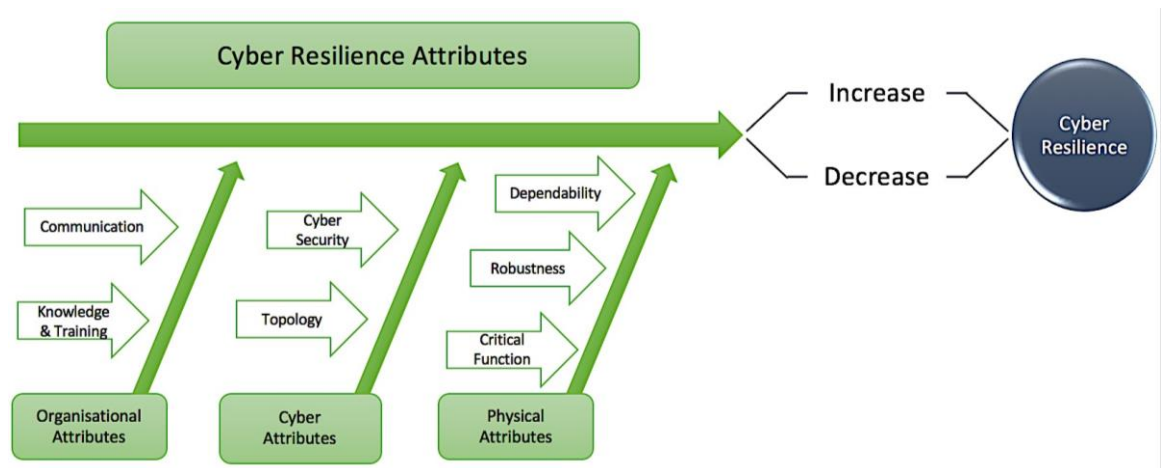


Figure 6-18 Experiment Cyber Resilience Attributes

Each of the attributes were categorised to the stages of resilience (as discussed in NIST and Linkov). Specifically, for these tests:

- The Cyber Domain attributes will provide a means to measure the organisation/systems ability to *Prevent*.

- The Physical Domain attributes will provide a means to measure the system’s ability to *Withstand/Adapt*.
- The Organisational Domain attributes will provide a means to measure the Organisation’s ability to *Detect/Recover*.

Table 6-3 shows how each test was mapped to the relevant attributes and how each attribute was mapped to the relevant domains.

*Table 6-3 CR Domains mapped to relevant attributes in this research.*

<b>Experiment Label</b>	<b>Experiment Parameters Description</b>	<b>Cyber Resilience Attributes</b>	<b>Cyber Resilience Domain</b>	<b>Functions/Stages of Resilience</b>
<b>Test 1</b>	<b>% of nominal system performance</b>	System’s Critical Function	Physical	N/A
<b>Test 2</b>	<b>% of system performance after disruption, without CR enhancements</b>	Topology – Network Segmentation Cyber Security - Secure Remote Access	Cyber	Prevent
<b>Test 3</b>	<b>Protection time after disruption, without CR enhancements</b>	Robustness and Reliability - Validate Inputs Inherent Safety	Physical	Withstand/Adapt
<b>Test 4</b>	<b>Protection time after disruption, with CR enhancements</b>	Robustness and Reliability - Validate Inputs Inherent Safety	Physical	Withstand/Adapt
<b>Test 5</b>	<b>Average discovery time after disruption, without CR enhancement</b>	Adequate Training Communication	Organisational	Detect/Respond
<b>Test 6</b>	<b>Average discovery time after disruption, with CR enhancement</b>	Adequate Training Communication	Organisational	Detect/Respond

The system enhancements and metrics discussed above, align directly with the following techniques described in various standards & frameworks (see Table 6-4).

*Table 6-4 Enhancement techniques mapped to standards/frameworks.*

<b>Standard/Framework</b>	<b>Mapping</b>
Mitre ATT&CK for ICS	<b>Tactic:</b> TA0110 – Impair Process Control <b>Technique:</b> T0836 – Modify Parameter
ISA 62443-3-3	<b>SR 3.5:</b> Input Validation <b>SR 3.6:</b> Deterministic Output
ISA 62443-4-2	<b>CR 3.5:</b> Input Validation <b>CR 3.6:</b> Deterministic Output
ISA 62443-4-1	<b>SI-2:</b> Secure Coding Standards <b>SVV-1:</b> Security Requirement Testing
MITRE CWE	<b>CWE-1320:</b> Improper Protection for out-of-bounds signal level alerts

The Cyber Resilience enhancements were applied to the representative system in tests 4 & 6, this was to determine if improvements were made to Cyber Resiliency. Additionally, each of the tests conducted in this study have been mapped holistically to the Cyber Resilience Matrix discussed in Chapter 3 (Linkov, et al., 2013). This ensured all aspects of CR were considered. Table 6-5 provides an overview of where this study relates to specific dimensions within the Cyber Resilience Matrix.

Table 6-5 Mappings between this study and the CR matrix set out in (Linkov, et al., 2013)

Plan and prepare for	Absorb	Recover from	Adapt to
<p><b>Physical</b></p> <p>(P1) Implement controls/sensors for critical assets <b>[Test 4 and Test 6]</b></p> <p>(P2) Implement controls/sensors for critical services <b>[Test 6]</b></p> <p>(P3) Assessment of network structure and interconnection to system components and to the environment <b>[Case Studies and Tests 2-4]</b>.</p>	<p>(1) Signal the compromise of assets or services <b>[Test 5]</b></p>	<p>(1) Investigate and repair malfunctioning controls or sensors <b>[Tests 4-6]</b></p> <p>(2) Assess service/asset damage <b>[Tests 2-6]</b></p>	<p>(1) Review asset and service configuration in response to recent event <b>[Tests 4 and 6]</b></p>
<p><b>Information</b></p> <p>(I1) Categorise assets and services based on sensitivity or resilience requirements <b>[Case Studies]</b></p> <p>(I5) Identify internal system dependencies <b>[Tests 1-6 and Case Studies]</b></p>	<p>(1) Observe sensors for critical services and assets <b>[Test 6]</b></p> <p>(2) Effectively and efficiently transmit relevant data to responsible stakeholders/ decision makers <b>[Test 6]</b></p>	<p>(1) Log events and sensors during event <b>[Tests 5 and 6]</b></p> <p>(2) Review and compare systems before and after the event <b>[All Tests]</b></p>	<p>1) Document incident's impact and cause <b>[All Tests]</b></p> <p>(2) Document time between problem and discovery/discovery and recovery <b>[All Tests]</b></p> <p>(4) Document point of entry (attack) <b>[All Tests and Case Studies]</b></p>
<p><b>Cognitive</b></p> <p>(C1) Anticipate and plan for system states and events <b>[Tests 4 and 6]</b></p>	<p>(2) The ability to evaluate performance impact to determine if mission can continue <b>[Tests 2-4]</b></p> <p>(3) Focus effort on identified critical assets and services <b>[All Tests and Case Studies]</b></p>	<p>(1) Review critical points of physical and information failure to make informed decisions <b>[All Tests and Case Studies]</b></p>	<p>(2) Determine motive of event (attack) <b>[All Tests]</b></p>
<p><b>Social</b></p> <p>(S1) Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish point of contact) <b>[All Tests and Case Studies]</b></p> <p>(S2) Educate/train employees about resilience and organisation's resilience plan. <b>[Test 6]</b></p> <p>(S4) Prepare/establish resilience communications <b>[Test 6]</b></p> <p>(S5) Establish a cyber-aware culture <b>[Test 6]</b></p>		<p>(1) Follow resilience communications plan <b>[Test 6]</b></p>	<p>(1) Evaluate employee's response to event to determine preparedness and communications effectiveness <b>[Tests 5 and 6]</b></p> <p>(2) Assign employees to critical areas that were previously overlooked <b>[Tests 5 and 6]</b></p>

Table 6-6 provides a description of each test demonstrating where each test links back to the hypotheses set out in Chapter 1.

*Table 6-6 Specification of modelling metrics and tests*

<b>Test Number</b>	<b>Metric Description</b>	<b>With reference, too:</b>
Test 1	% of nominal system performance and product quality (baseline).	This test is performed to obtain a baseline of how the system performs (as is) prior to Cyber Resilience enhancements and prior to a disruption.
Test 2	% of system performance & product quality after disruption (without CR enhancements).	Cyber Security – Hypothesis 2.
Test 3	Protection time – the time the system can withstand an incident without degradation to product quality (without CR enhancements).	Cyber Resilience – Dependability. Hypothesis 1.
Test 4	Protection time – the time the system can withstand an incident without degradation to product quality (with CR enhancements).	Cyber Resilience – Dependability. Hypothesis 1.
Test 5	Average time between start of adversary activities and their discovery (without CR enhancements).	Cyber Security, Complexity, Human Factors and Organisational aspects of CR. Hypothesis 2.
Test 6	Average time between start of adversary activities and their discovery (with CR enhancements).	Cyber Resilience, Complexity, Human Factors and Organisational aspects of CS. Hypothesis 1 + 2.

The next section discusses the experiments conducted.

### 6.3.3 Specification of Tests

This section discusses each of the tests (as summarised in the previous section) along with a diagrammatic structure of the experimental tests given in Figure 6-19.

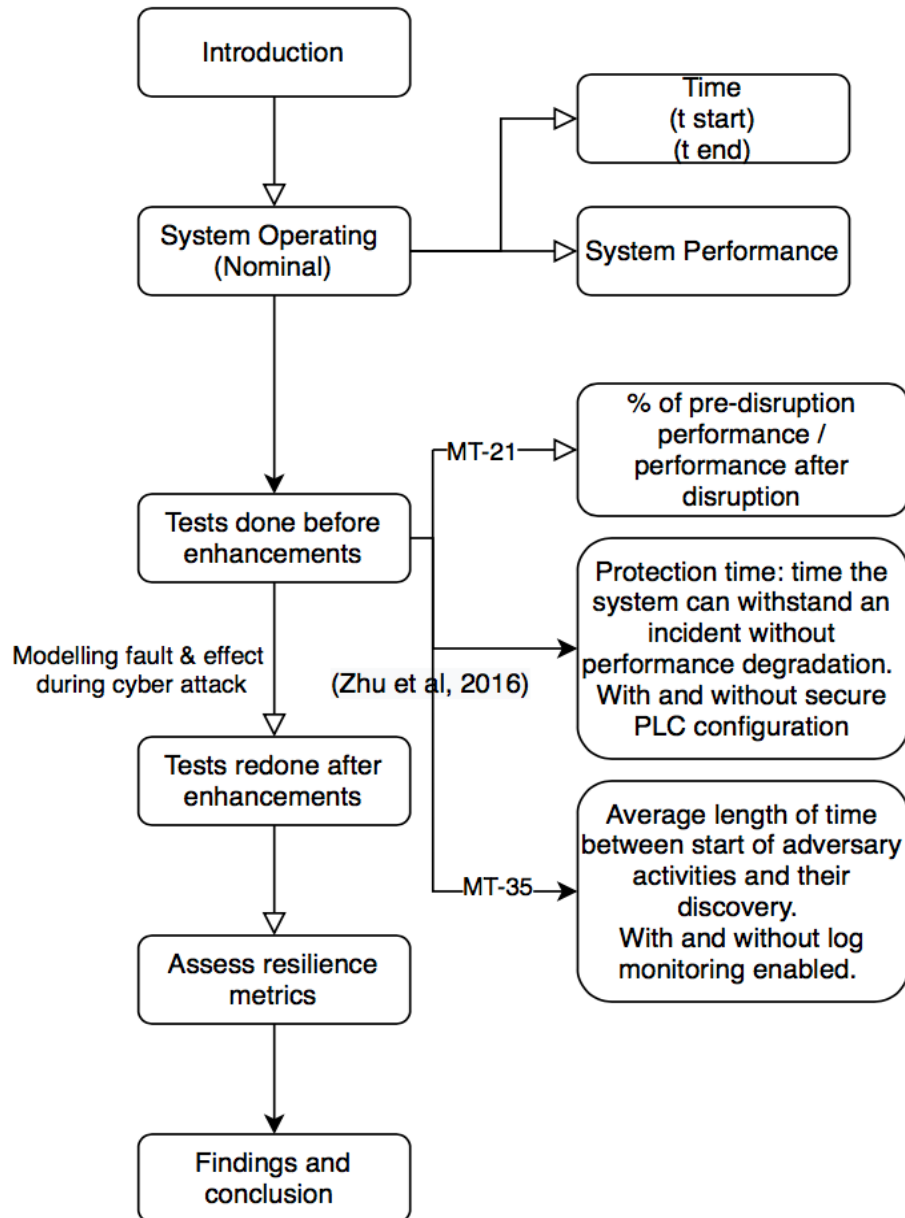


Figure 6-19 Diagrammatic structure of tests performed



### 6.3.3.1 % of nominal system performance and product quality (Test 1)

In this test, the % of system performance and time is analysed in its normal operating environment, without any cyber disturbance and without any recommended Cyber Resilience improvements. This test is done to obtain a baseline measure of a systems typical operating level. This test refers specifically to Hypothesis 2. In that Cyber Resilience relies on a foundation of Cyber Security.

The operator selects 23°C as a reasonable set point temperature required for the milk vessel to run at. Temperature within the vessel continues to climb until the set point value of 23°C is reached. Once the vessel reaches the desired temperature, the measured temperature is maintained within the vessel (see Figure 6-20).



Figure 6-20 HMI temperature reading

This is controlled at the PLC, which takes the measured temperature from the thermocouple and feeds it into the PID block. This block applies the PID algorithm to provide a physical heat output (IO1) based on the set point temperature in comparison to the measured temperature. The configuration is given in Figure 6-21.

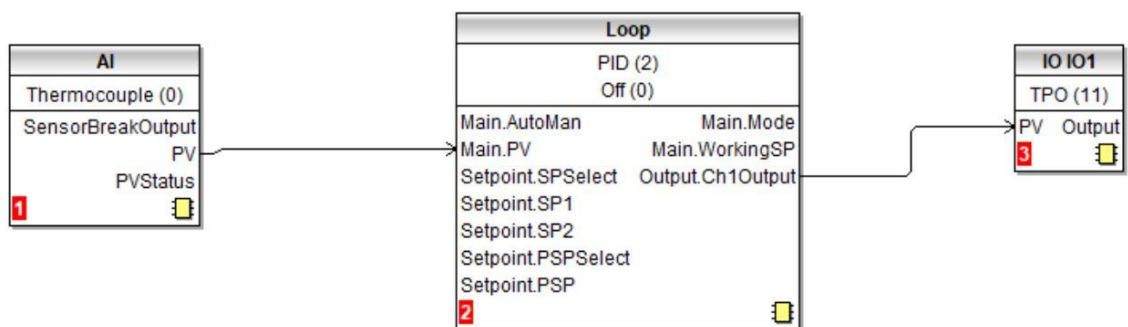


Figure 6-21 PLC configuration logic

Within the PLC program, the set temperature limit value is compared against the measured temperature value. The safe operating temperatures for this part of the processing plant are defined as:

- Safe working limit = 20-25°C
- System warning level= 25.9°C
- System Critical level = >26°C

If the temperature set point within the PLC were modified to temperatures higher than these values then a risk of contamination to the product could occur due to excessive temperatures within the vessel. If temperatures increase beyond the set limits the operator would be alerted by a series of visual alarms on the HMI.

#### 6.3.3.2 % of system performance after disruption before CR enhancements (Test 2)

In this test, the % of system performance and time is analysed following a successful cyber-attack. The system is measured as is, without recommended CR enhancements. This test is done to obtain a baseline measure of a systems operating level following a successful cyber-attack. This measure will determine how the system is impacted during a successful cyber-attack.

The operator selects 23°C as a reasonable set point temperature required for the milk vessel to run at. Temperature within the vessel continues to climb until the set point value of 23°C is reached. Once the vessel reaches the desired temperature, the measured temperature is maintained within the vessel for 120 minutes.

At 120 minutes the attack starts. Modbus read values are requested by the attacker at 125 minutes and malicious write value packets are sent at 2 hours 9 and 2 hours 10 minutes. These readings continue for 4 minutes until the attack ends. The values of the malicious temperature are maintained until 180 minutes.

#### 6.3.3.3 Protection time following disruption before CR enhancements (Test 3)

In this test, the Protection time is analysed as the time the system can withstand an incident without degradation and without CR enhancements (adequate PLC secure coding applied). The PLC configuration for this test is shown in Figure 6-22:

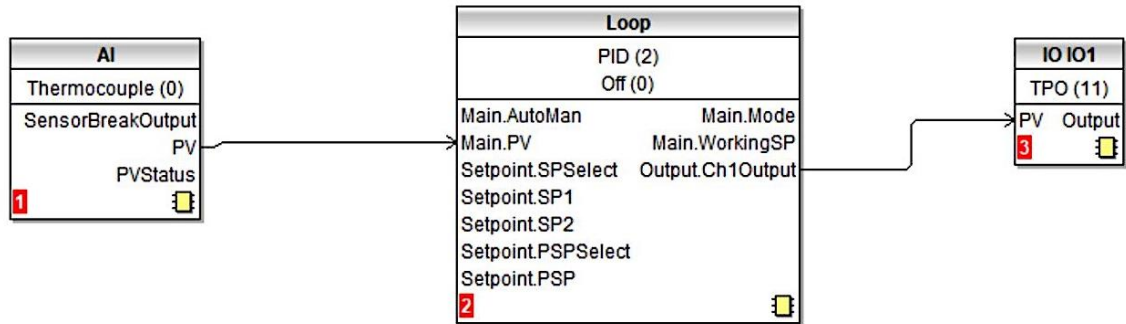


Figure 6-22 PLC logic

The safe temperature values are considered as % of system performance over time and analysed following a successful cyber-attack. Much like the test before, the system is measured as is, without recommended enhancements. This measure will determine how the system adapts during a successful cyber-attack.

#### 6.3.3.4 Protection time and product quality following a disruption with CR enhancements (Test 4)

In this test, the Protection time is analysed as the time the system can withstand an incident without degradation and with adequate PLC secure coding applied. The safe temperature values are considered as % of system performance over time and analysed following a successful cyber-attack. This measure will determine how the system adapts during a successful cyber-attack. Unlike the test before, the system is measured this time with a Cyber Resilience enhancement recommendation applied. The following enhancements were made to the system before the test was conducted.

- a. Validate HMI input variables at the PLC level, not only at the HMI.

As part of the PLC system design, system engineers can configure additional programming that would apply limits in either the PLC logic, HMI or both to ensure temperature set points are set within a given validation criteria. This technique is referred to in the secure PLC coding guidance on best practice surrounding this topic however, this guidance has only recently been introduced in the Industrial Automation and Control domains since 2021 (PLC Security, 2021). The recommended configuration was implemented within the PLC program prior to the test, as shown in Figures 6-23 and 6-24 below:

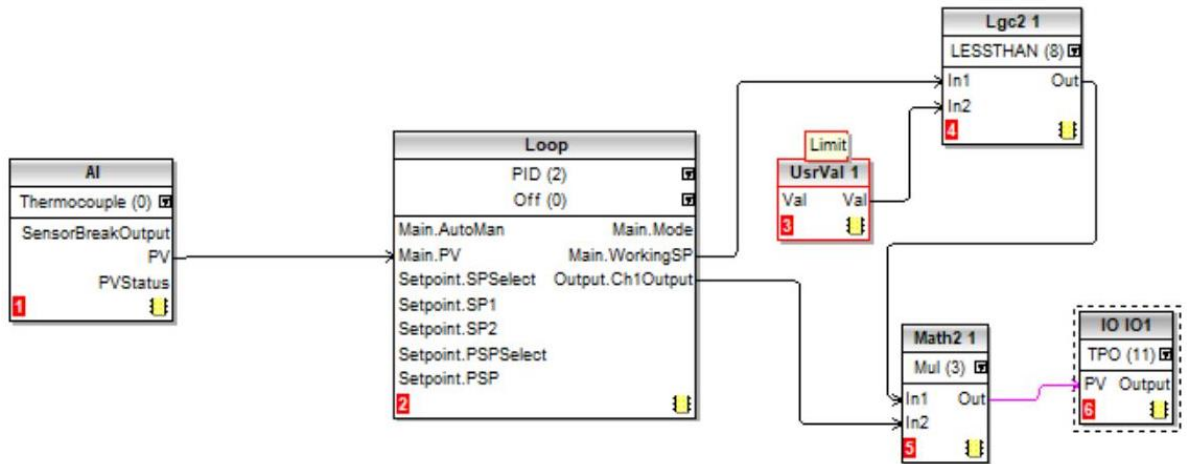


Figure 6-23 Secure Limits configuration set in the PLC

C:\Users\secadmin\Documents\Eurotherm\EPC2000\_Bench\_1.uic - Function Block View (L... [Close] [Maximize] [Minimize]

Function Block: Loop [Refresh]

Main Config Setpoint Feedforward Autotune PID Output Diagnostics

Name	Description	Address	Value	Wired From
RangeHigh	Loop upper operating point	12	1372.00	
RangeLow	Loop lower operating point	11	-200.00	
SPHighLimit	SP1/SP2 upper limit	111	1372.00	
SPLowLimit	SP1/SP2 lower limit	112	-200.00	
SPSelect	SP1 or SP2 select	15	SP1 (0) ▾	
SP1	Setpoint 1	24	20.00	
SP2	Setpoint 2	25	0.00	
Read/write access	Select the program setpoint	1664	Off (0) ▾	
	Program Setpoint	1665	0.00	
RSPTtype	Selects the RSP configuratio	535	Setpoint (0) ▾	
RSPHighLimit	RSP upper limit	1674	1572.00	
RSPLowLimit	RSP lower limit	1675	-1572.00	
RSP_En	Enable the RSP input	1666	Off (0) ▾	
RSP	Remote Setpoint input	485	0.00	
SPTrimHighLimit	SPTrim upper limit	66	0.00	
SPTrimLowLimit	SPTrim lower limit	67	0.00	
SPTrim	Setpoint local trim value	27	0.00	
SPRateUnits	Rate limit units	531	PerSecond (0) ▾	
SPRateUp	Setpoint up rate limit	35	Off (0) ▾	

Figure 6-24 Secure limits configured in the PLC.

### 6.3.3.5 Discovery time after a disruption without CR enhancements (Test 5)

In this test, the time between start of adversary activities and their discovery is considered and analysed following a successful cyber-attack. The system is measured as is, without recommended CR enhancements. This measure will determine how fast the organisation responds to the identification of malicious activity. The measure also considers the distinction between a cyber-attack and plant failure or maintenance, highlighted in (Syrmakesis, et al., 2022). Differentiating cyber-attacks from plant failures is crucial as both events negatively impact the system. It is

essential to identify whether a degradation in system performance is the result of a cyber-attack or a plant failure/maintenance to implement appropriate countermeasures. Making this distinction poses significant challenges and has received limited attention (Syrmakesis, et al., 2022). Organisations are encouraged to prioritise efforts in distinguishing between cyber-attacks and plant failures to enable the application of suitable discovery and recovery methods. Investigating the unique characteristics of each unplanned event is necessary for effective differentiation.

During the test, the SOC team is alerted that Modbus traffic is changed. However, the analysts do not fully understand Modbus traffic. Since this Modbus traffic is constant in their logs showing the normal PLC temperature changes daily, the attack goes unnoticed. The SOC team is unaware the values being changed are outside of the normative acceptance set points and no follow up is taken, the incident is ignored.

When a cyber-attack occurred the SOC team supposed it was a normal change and that the alert was a false positive, consequently, did not follow up with the engineer on shift.

#### 6.3.3.6 Discovery time following a disruption with CR enhancements (Test 6)

In this test, the time between start of adversary activities and their discovery is considered and analysed following a successful cyber-attack. The system is measured with the recommended enhancements. This measure will determine how fast the organisation responds to the identification of malicious activity. As described in Test 5, this measure also considers the distinction between a cyber-attack and plant failure or maintenance, highlighted in (Syrmakesis, et al., 2022).

Engineers provide the SOC team with the plant maintenance schedules that show any planned maintenance such as downtimes and the safe temperature limits. Once the cyber-attack commences, the SOC team identify the malicious behaviour in the logs and follow this up with the plant engineers.

## 6.4 Phase 4 - Functions of Resilience - Simulation Results

This section presents the results of the tests set out in the previous section. The simulation results form the basis for assessing the functions of resilience.

- This should reduce the impact of a cyber-attack on product quality.
- Help withstand the effects of a cyber-attack.
- Recover and learn from the effects of a cyber-attack.
- Detect an event and respond to it (time to resolve and restore functionality).

The functions of resilience are measured using the following approach given in Figure 6-25.

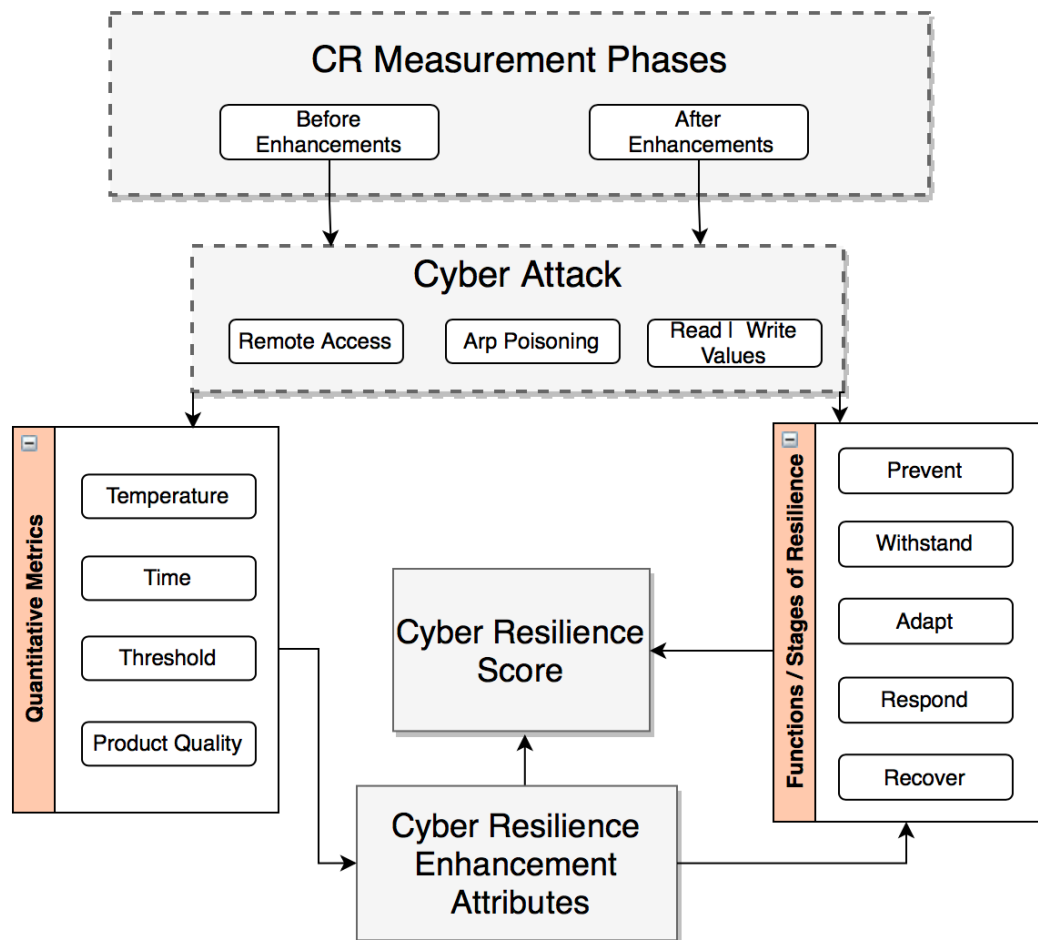


Figure 6-25 Physical System CR Measurement

Based on the tests specified in the previous section, the following formula is used to estimate the time a system can withstand a cyber-attack incident without dropping to a below a critical temperature threshold level:

$$t = \left( \frac{(T_{max} - T_{nom})}{(T_{max} - T_{min})} \right) * t_{max} \quad (1)$$

Where:

- $t$  is the estimated time that the system can withstand a cyber-attack incident without dropping to a below critical temperature efficiency level (minutes)
- $T_{max}$  is the maximum temperature reached by the manufacturing system during the incident (°C)
- $T_{min}$  is the minimum safe temperature required for the product (°C)
- $T_{nom}$  is the average nominal operating temperature of the manufacturing system (°C)
- $t_{max}$  is the maximum allowable time for the manufacturing system to operate above the safe temperature level (minutes)

Note that this formula assumes a linear relationship between the temperature increase and time. It is also important to note that this is only an estimation and that the actual time may vary depending on several factors such as the severity of the cyber-attack, the resilience of the system, the requirements of the system thresholds and the effectiveness of the response measures taken.

The next section discusses the results.

#### 6.4.1 Introduction to Results

All data related to this test bed is freely available for research purposes at: <https://github.com/KPMarie/PhD-CyberResilience-Datasets-OT-ICS->.

The dataset was created by collecting 3 hours' worth of PCAP logs using Wireshark. The data shows nominal operating performance logs for 120 minutes. Then the start of malicious activity on the plant network immediately after which lasts until 140 minutes into the PCAP. The PCAP continues to monitor the system until 180 minutes. The PCAP contains a total of 45368 data points for use by the research community. A csv copy of the PCAP is also provided.

### 6.4.1.1 Test 1 Results

This test shows the systems nominal temperature values (or operating performance) as shown in Figure 6-26 and the quality of the Infant Milk formula % (Figure 6-28).

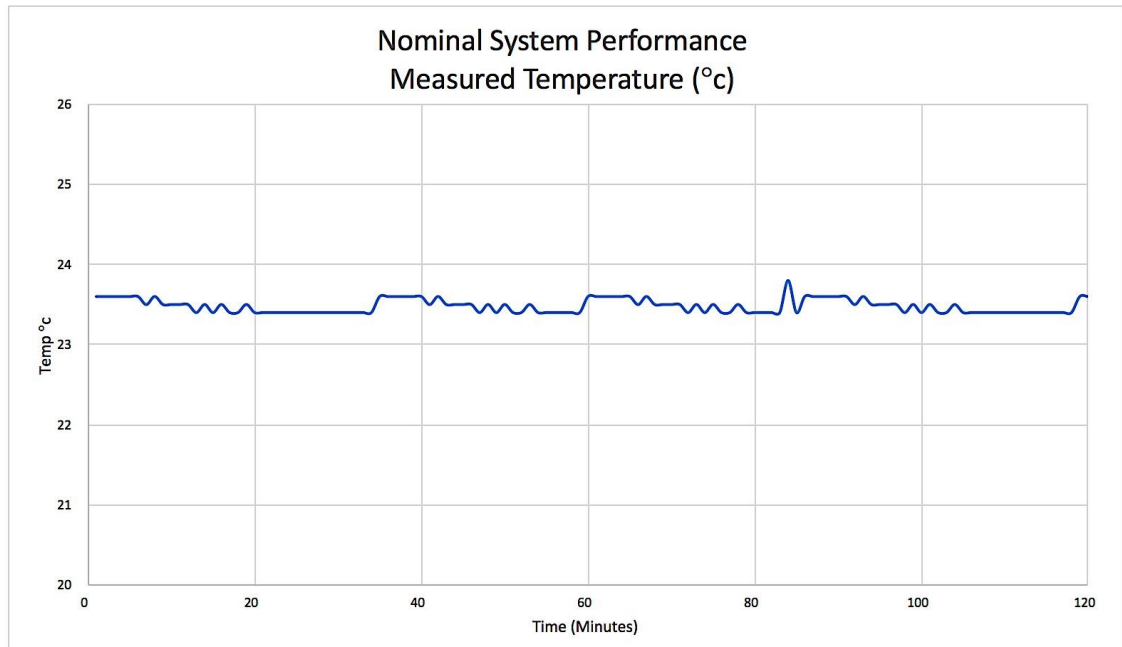


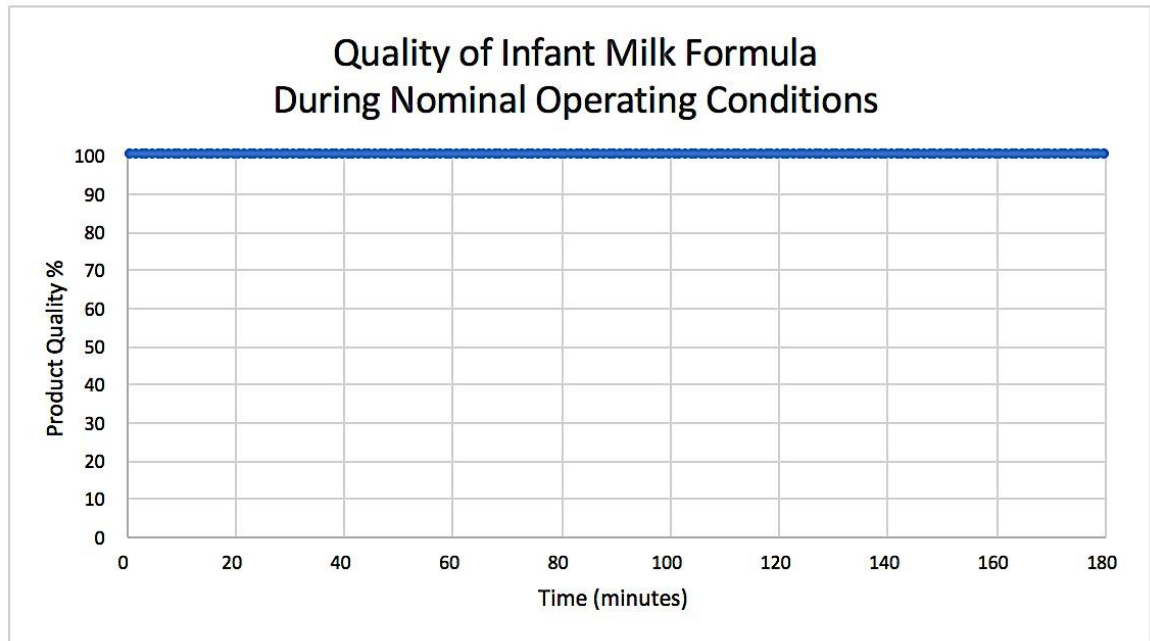
Figure 6-26 Nominal system performance measured temperature test

Figure 6-26 shows the normal system performance in terms of temperature fluctuations over a two-hour period. Figure 6-27 shows the same results for the physical HMI interface.



Figure 6-27 HMI interface





*Figure 6-28 Quality of infant milk formula during normal operating conditions*

Figure 6-28 shows the quality of the Infant Milk formula when the system operates in nominal conditions. Here, the IMF remains at an acceptable quality for 180 minutes during this test.

#### 6.4.1.2 Test 2 Results

This test shows the systems measured temperature values during the attack compared to the systems nominal temperature values (shown in Figure 6-29). Additionally, Figure 6-30 shows the impact to the quality of infant milk formula percentage. The results provide the following information:

- The time the attacker gains access to the plant network.
- The systems measured temperature values during the attack compared to the systems nominal temperature performance.
- The quality of the infant milk formula (%).

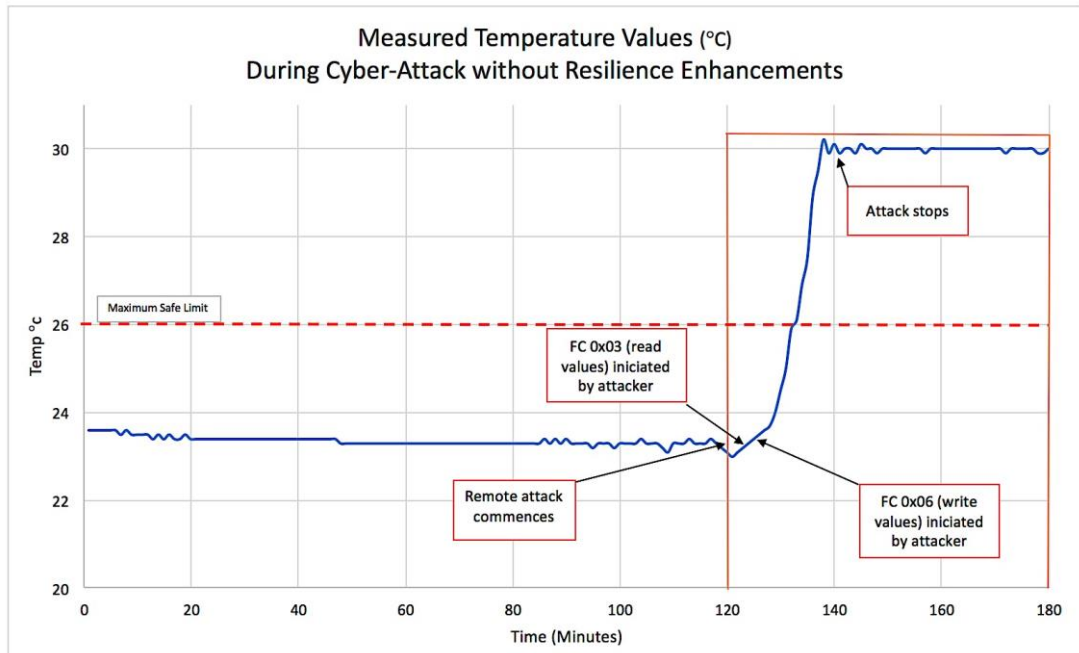


Figure 6-29 System performance showing the measured temperature following a cyber-attack.

The average nominal operating temperature is 23.25°C and the average value following disruption is 30.5°C. Therefore, the system performance shows a 31% increase in temperature compared to the nominal operating temperature of the vessel and a 17% increase above the maximum safe limits set for this process. The quality of product over time is shown in Figure 6-30.

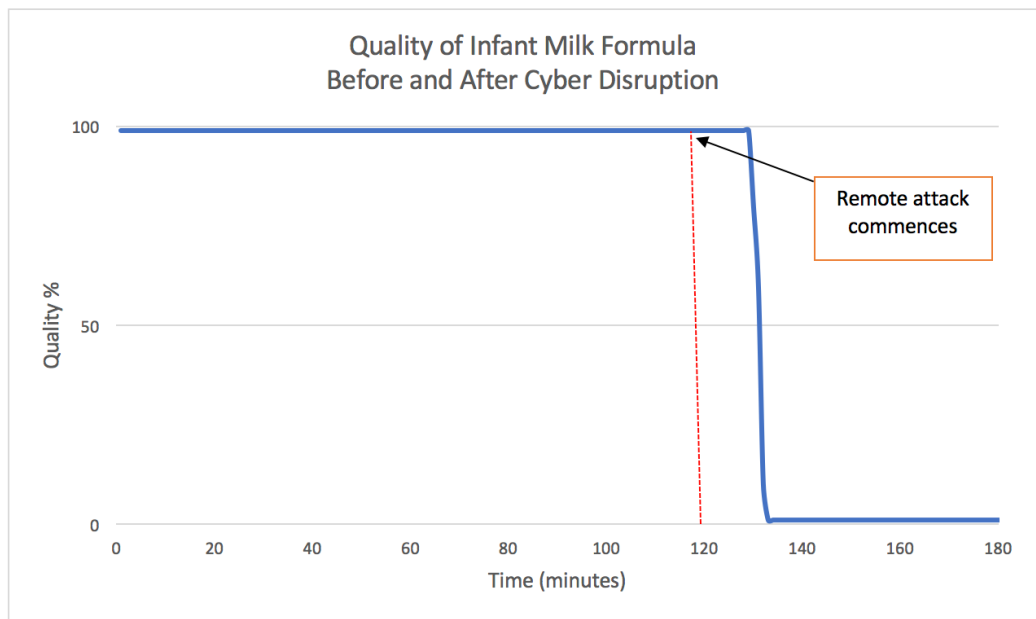


Figure 6-30 Quality of infant milk formula before and after a cyber disruption

The following formula is used to estimate the time this system can withstand a cyber-attack incident without dropping to a below critical temperature efficiency level (as set out in equation 1 in Section 6.4). Substituting the results of this test:

$$t = \left( \frac{(30.5 - 23.25)}{(30.5 - 20)} \right) * 5$$

$$t = \left( \frac{7.25}{10.5} \right) * 5$$

$$t = 3.41 \text{ minutes (approx)}$$

The estimated time this manufacturing system can withstand the cyber-attack incident without dropping to a below critical temperature efficiency level (with 5 minutes deviation time allowed) is approximately 3.41 minutes.

#### 6.4.1.3 Test 3 Results

This test shows the protection time or the time the system can withstand an incident without degradation prior to CR enhancements. The results show the:

- time the attacker gains access to the plant network;
- system's measured temperature values during the attack compared to the systems nominal temperature performance;
- quality of the infant milk formula (%);
- system's protection time without degradation.

This test does not consider the human factors I.E SOC team. It only measures the ability to withstand a cyber-attack without secure coding practices. Changes to set points are made and the attack is successful.

The average nominal operating temperature can be calculated as 23.25°C and the average value following disruption is 30.5°C. Therefore, a comparison of system performance shows a 30% increase in temperature to the vessel compared to its nominal operating temperature and a 17% increase, above the maximum safe limits set for this process, for 4 minutes. The system took a total of seven minutes for the temperature to return within the set safe limits.

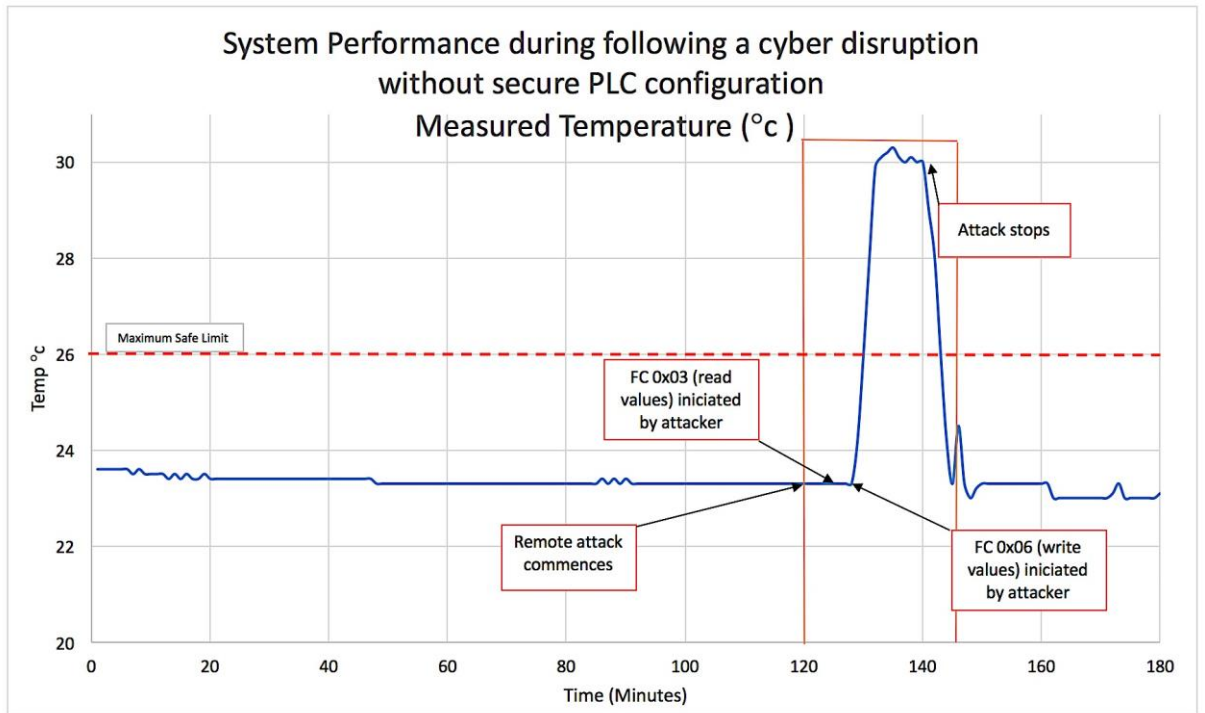


Figure 6-31 System performance following a cyber disruption - without CR enhancements.

Once the attack stops at 141 minutes, the plant engineer can communicate with the PLC and change the system set point back to its nominal temperature value. The system takes three minutes for the temperature to adjust. The quality of product over time is shown in Figure 6-32.

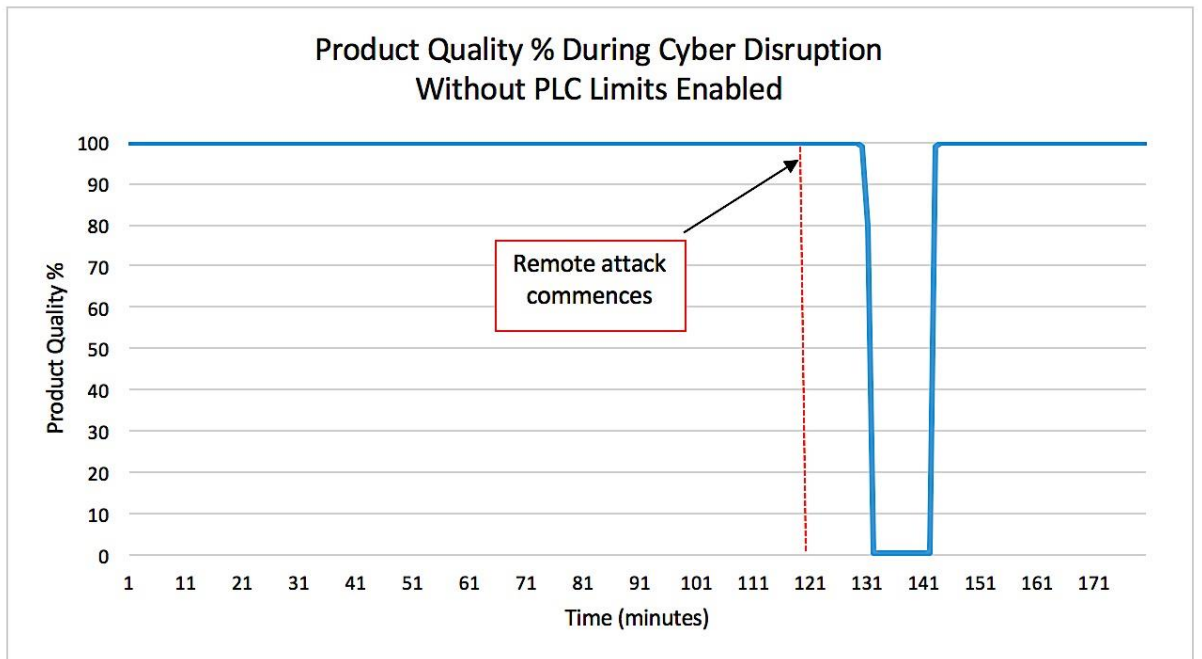


Figure 6-32 Product quality % following a cyber disruption (without CR enhancements)

The following formula is used to estimate the time this system can withstand a cyber-attack incident without dropping to a below critical temperature efficiency level (set out in Equation 1, Section 6.4). Substituting the results of this test:

$$t = \left( \frac{(30.5 - 23.25)}{(30.5 - 20)} \right) * 5$$

$$t = \left( \frac{7.25}{10.5} \right) * 5$$

$$t = 3.41 \text{ minutes (approx)}$$

The estimated time this manufacturing system can withstand the cyber-attack incident without dropping to a below critical temperature efficiency level (with 5 minutes deviation time allowed) is approximately 3.41 minutes.

#### 6.4.1.4 Test 4 Results

Protection time – the time the system can withstand an incident without degradation and with CR enhancements (PLC secure coding techniques applied). The results show the following:

- The time the attacker gains access to the plant network.
- The system's measured temperature values during the attack compared to the system's nominal temperature performance.
- The quality of the infant milk formula as a percentage (%).

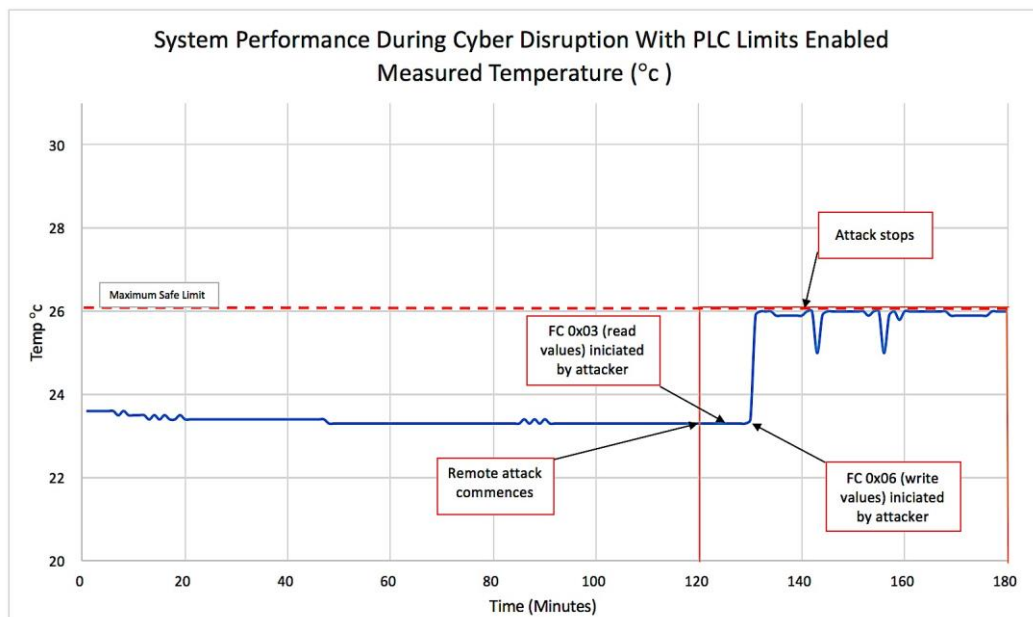


Figure 6-33 System performance during a cyber disruption - with CR enhancements

The average nominal operating temperature can be calculated as 23.25°C and the average value following disruption is 25.9°C. Therefore, a comparison of system performance shows an 11% increase in temperature to the vessel for a total of thirty-five minutes. This temperature however, remains within the safety limitations of the system and will therefore not have an impact on the production of milk formula. Although the attack goes ahead it is unsuccessful at altering PLC set points and the system continues to operate without degradation. The quality of product over time is shown in Figure 6-34.

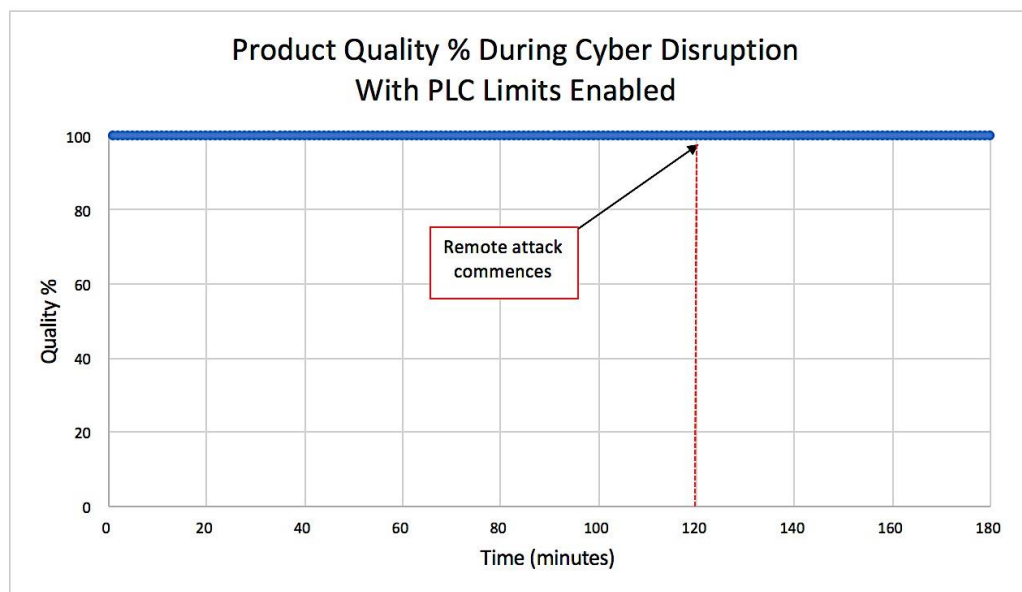


Figure 6-34 Test 4 - quality % of product following a cyber disruption - with CR enhancements

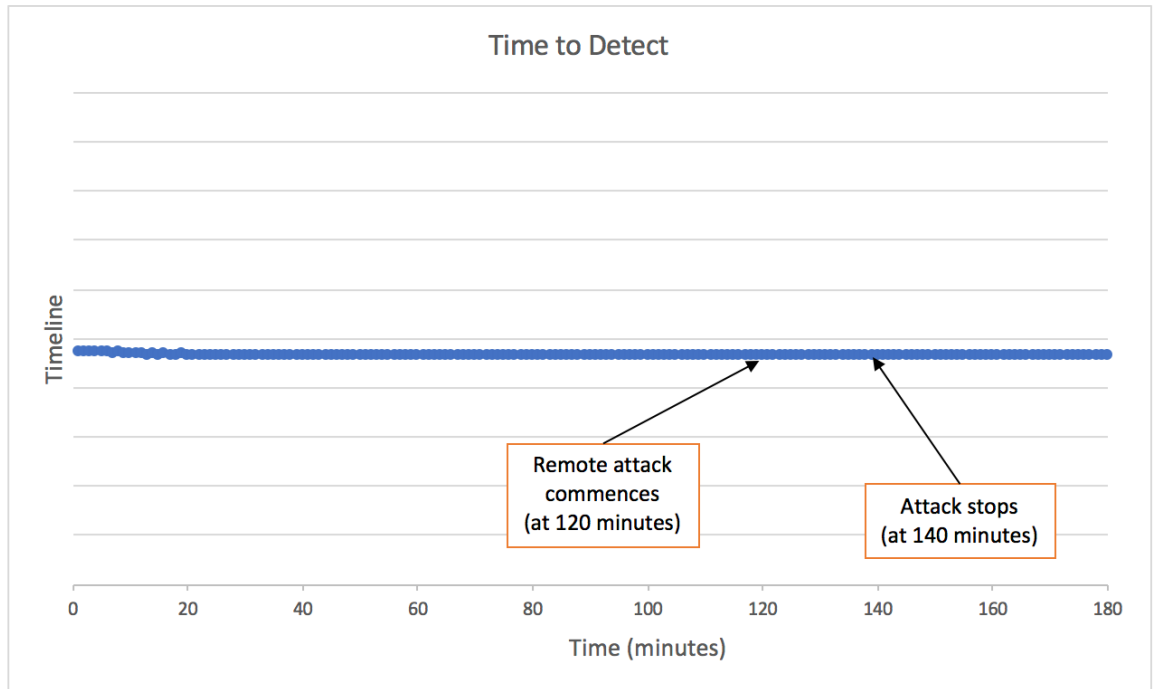
In summary, the guidance provided in (PLC Security, 2021) is an effective approach in securing PLCs in Industrial Control Systems and results show that it can be successfully implemented on physical industrial testbeds. By following these practices, organisations can improve the security of their PLCs and reduce the risk of cyber-attacks on their ICS. It is important to note that the specific implementation of these practices may vary depending on the unique needs and requirements of each organisation.

#### 6.4.1.5 Test 5 Results

This test shows the time between start of adversary activities and their discovery (without adequate training). The results show the:

- time the attacker gains access to the plant network;
- time the adversary activities were first discovered;
- time between start of adversary activities and their discovery.

The SOC team is alerted that Modbus traffic has changed. However, the SOC team is only familiar with IT related protocols and do not fully comprehend Modbus traffic. Since Modbus traffic is continual and is not unusual for PLC temperatures to change daily, the attack goes unnoticed (as shown in Figure 6-35).



*Figure 6-35 Test 5 – time between start of adversary activities and their discovery - without CR enhancements*

The SOC team are unaware the values being changed are outside of the normative acceptance set points. No follow up is taken and the alert logs are ignored. The SOC team believed it was a normal change and presumed the alert was a false positive, therefore did not follow up with the engineer on shift.

#### 6.4.1.6 Test 6 Results

This test shows the time between start of adversary activities and their discovery (with adequate OT training). The results show the:

- time the attacker gains access to the plant network;
- time the adversary activities were first discovered;
- time between start of adversary activities and their discovery.

The SOC team are provided with the plant maintenance schedules that show any planned maintenance such as downtimes or expected changes. Once the Cyber-attack commences, the SOC team identify the malicious behaviour in the logs (see Figure 6-36 and Figure 6-37).

10

## MITM attack

14:25:26.665 | Status: open

...

---

<b>Source</b>	
MAC	cc:6b:f1:51:dd:56
Zone	
Is security	true
Protocol	unknown

---

**What happened?**

Attacker identified by MAC address cc:6b:f1:51:dd:56 is acting as a MITM, its victims are: 141.196.91.4, 141.196.91.68

**Possible cause**

A potential MITM attack has been detected. The attacker is ARP-poisoning the victims. The attacker node could alter the communication between its victims.

**Suggested solution**

Investigate on the network configuration and the possible presence of malicious actors.

**Attack analysis**

This alert could be:

- A **Execution** tactic (technique *MITM*, T0830)

[Open details >](#)

Figure 6-36 SIEM alert following enhancements.

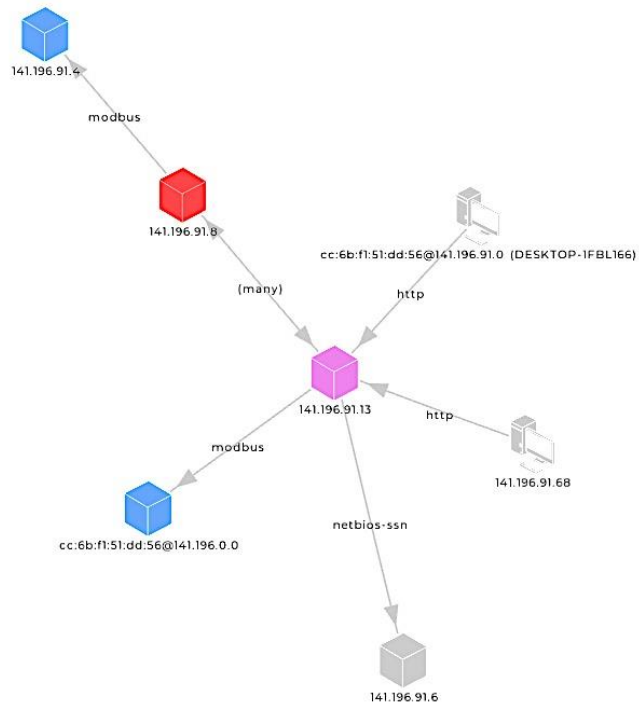


Figure 6-37 SIEM attack logs



Figure 6-38 shows the discovery time.

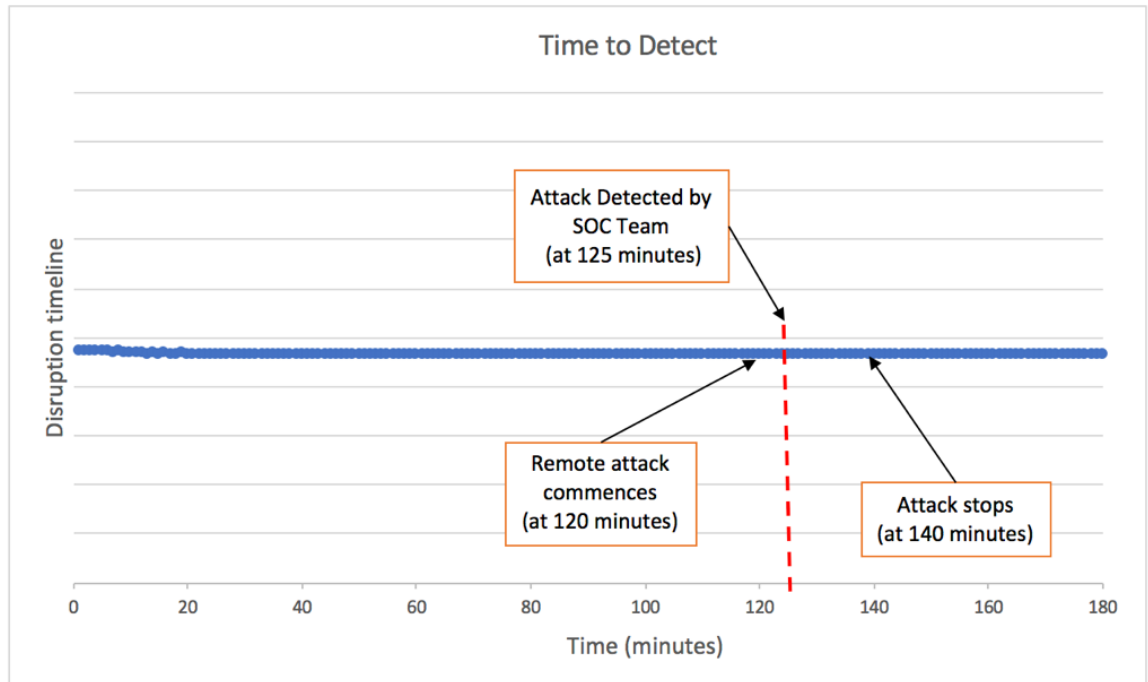


Figure 6-38 Test 6 – time between start of adversary activities and their discovery - with CR enhancements.

The results from tests 5 and 6 show that that even with good cyber hygiene practices in place, such as monitoring, a cyber-attack to a critical manufacturing system can still go undetected without Cyber Resilience initiatives being in place. This Cyber Resilience control relates specifically to the SOC team’s prior knowledge and understanding of the normal OT values and what to look for. With good Cyber Resilience and good Cyber Security, response time to identifying an attack is significantly improved.

## 6.5 Chapter Summary

In this chapter, the ICS test bed environment was summarised, as well as the scenarios and metrics measured, as also summarised in Chapter 4, additionally the results of the experiments conducted was provided. Simulations of the system before and after a cyber-attack were performed to analyse the system performance. Analysis of the data collected during the experiments were used to evaluate and validate the system performance. Results are discussed in the Chapter 7.

# Chapter 7

## Discussion

### 7.1 Introduction

This chapter discusses each of the results and the limitations of the research. The experiments conducted in this study were informed from first-hand case study evidence on the application of Cyber Security and Resilience in practice and the physical testbed demonstrates how to objectively model Cyber Resilience enhancement strategies to determine their effectiveness when applied to a critical manufacturing system.

The field of Cyber Resilience measurement in industrial manufacturing systems is crucial for ensuring the security and safety of critical infrastructure. This PhD thesis has made a valuable contribution to this field by employing both qualitative assessments from real case studies and the construction of a physical testbed to obtain quantitative measures. By combining these two approaches, the thesis provides a more comprehensive understanding of the factors that contribute to Cyber Resilience in industrial control systems. The utilisation of real case studies allows for an in-depth analysis of the challenges and vulnerabilities faced by organisations in securing their systems. On the other hand, the physical testbed enables the collection of quantitative data, which can be used to develop more accurate and reliable metrics for measuring Cyber Resilience.

Additionally, the research has resulted in the creation of a novel cyber-attack and a labelled dataset obtained from the industrial manufacturing testbed. This dataset is a valuable resource for researchers in this field, as it provides a real-world example of a cyber-attack on an industrial control system. Moreover, it is currently the only known research that provides a testbed specifically designed to produce Infant Milk Formula, enabling the development and testing of new models and approaches for measuring Cyber Resilience in such systems.

As set out in Chapter 4, the approach followed in this research is given again in Figure 7-1.

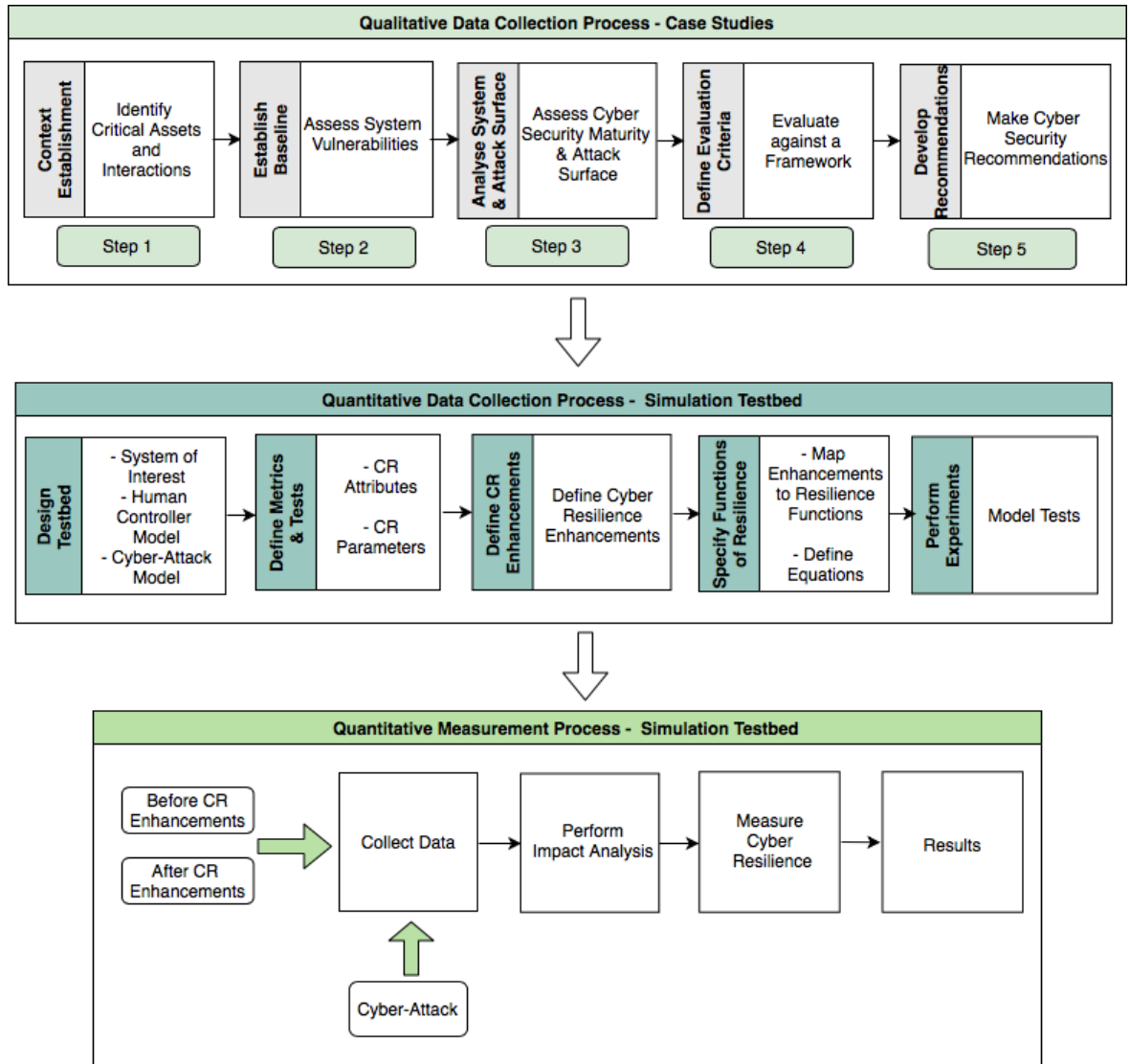


Figure 7-1 Research approach to obtaining CR metrics

The next section will discuss the findings of the case studies.

## 7.2 Case Study Discussion

A wide variety of frameworks exist that aid organisations with techniques and approaches to improving Cyber Resilience. However, there is a sparsity of real-life case studies that speak to the adoption and measurement of these novel approaches within a manufacturing environment.

The case studies presented in this research assessed the contribution of various frameworks and offered findings derived from two industrial plant consultations undertaken with Thales. The case studies draw on key themes that appeared from the literature to analyse Cyber Security gaps, to what degree constructs can be adopted to improve Cyber Resilience and to determine if an evaluation of the results could provide a baseline measure of an organisation’s resilience.

Based on the findings from each study, three specific problem areas were identified in both plants (discussed in Chapter 5), regardless of their differences in Cyber Security maturity levels or assessment frameworks. While each framework had unique characteristics and differences, there were noticeable similarities in security control groupings that were evident in the results of both case studies and discussed in Chapter 5.

To summarise, while certain segments of the IT environment demonstrated good Cyber Security practices in both case studies, the OT environment showed poor practices. Issues were found in network segmentation and remote access to the plants. Additionally, poorly designed HMI input controls were identified in at least one or more of the critical systems in both plants. Furthermore, regarding the organisational elements, although both plants had some form of security monitoring, the SOC teams primarily consisted of IT experts lacking the expertise and processes required to understand OT protocols or respond to alerts during an attack.

Conclusions drawn show that although the frameworks did aid with the qualitative subjective analysis, the accompanying evaluation processes was not sufficient to quantitatively measure the overall Cyber Resilience maturity for each case study. Consequently, the creation of a physical testbed was necessary to obtain a quantitative measure.

The next section will discuss the physical testbed and simulation findings.

### 7.3 Simulation Discussion

This section presents an overview of the simulation and modelling used in this experiment. The testbed emulates a real-world industrial system as closely as possible without affecting real-time systems. The testbed models a typical industrial scenario that were informed by the results of several case studies (as discussed in Chapter 5).

To achieve effective design and development of a Cyber Resilient system, it is crucial to employ experimental methods that allow for quantitative measurement of Cyber Resilience. In accordance with the case study recommendations, best practices and guidance set out in various frameworks, the aim of the testbed was to measure the performance of a critical system when instrumented with a cyber-attack both before and after Cyber Resilience enhancements were implemented.

As a result of the case study findings, whereby three specific problem areas stood out across both plants (discussed in Chapter 5), the testbed was designed to specifically mirror these weaknesses to gauge the optimal results.

The testbed illustrates the production of Infant Milk Formula and consisted of a temperature control process, managed by a PLC (Programmable Logic Controller), which takes a measured temperature from a thermocouple and feeds it into a PID (Proportional-Integral-Derivative) block. The PID block applies a PID algorithm to generate a physical heat output (IO1) (based on the set temperature and the measured temperature). Inside the PLC program, the set temperature limit value is then compared with the measured temperature value. The safe operating temperatures for the processing plant in this model was defined as: Safe working limit: 20-26°C. If the temperature set point within the PLC is modified to values higher or lower than these defined limits, there is a risk of product contamination due to excessive temperatures in the vessel.

During the experiments, malicious packets disguised as Modbus client queries were successfully injected into the Modbus TCP communication protocol, as described in Chapter 6 for tests 2-6.

In all tests, the impact of the attack meant that the PLC was unable to respond to legitimate requests from the HMI during the period of attack. Consequently, the HMI was unable to communicate or control the PLC until the attack ended. Tests 2-4 considered the Cyber and Physical domains of resilience with particular focus to the following attributes: Topology, Security and Dependability – Safety; Inherent resilience. A comparison of the results is given in Figure 7-2 and Figure 7-3. Figure 7-2 shows the nominal system temperature compared to the system temperature during the attack, both before and after resilience enhancements were implemented.

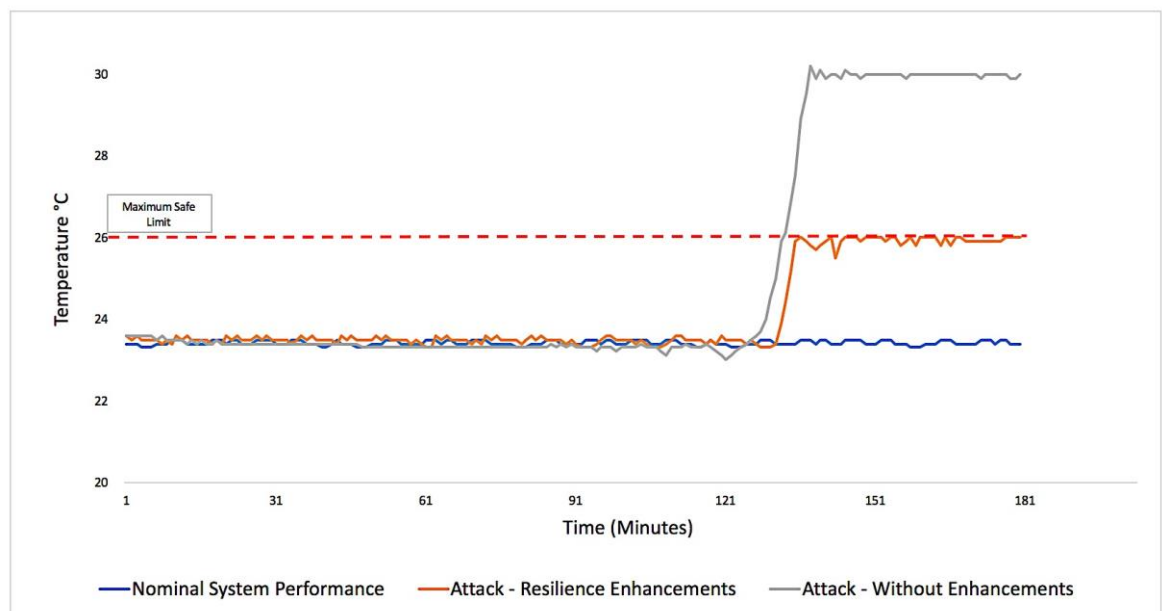


Figure 7-2 Comparison of system performance during tests 1, 3 and 4

Figure 7-3 shows the quality % of Infant Milk Formula during nominal system operating compared to the quality % following the attack, both before and after resilience enhancements were implemented.

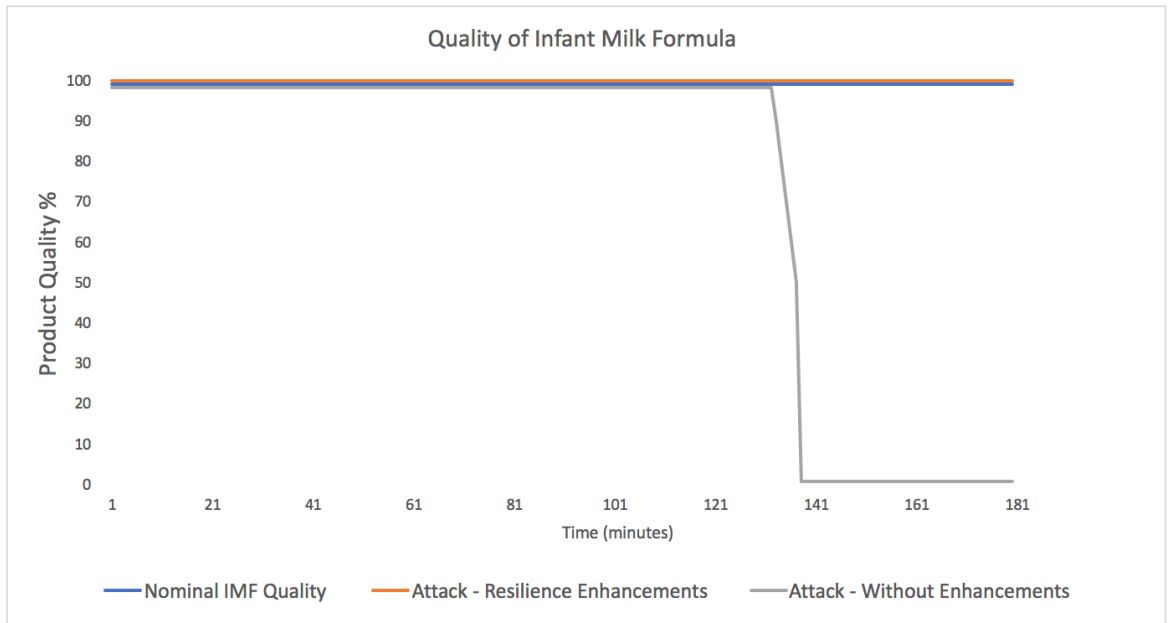


Figure 7-3 Quality % of IMF following a cyber-attack - with and without CR enhancements

On the other hand, tests 5-6 considered the Organisation and Social domains of Cyber Resilience including adequate training for the SOC personnel in order to make the distinction between a cyber-attack, plant failure and planned maintenance (Syrmakeisis, et al., 2022). These final tests focused on the following attributes: Security; Monitoring, Process and Procedures, Communication, Training and Knowledge.

The following sections will further discuss each of the experiments undertaken and their findings.

### 7.3.1 Discussion - Test 1

In this test, the system's performance was analysed under normal operating conditions, without cyber disturbances or recommended resilience enhancements applied. The purpose of this test was to establish a baseline measurement of the system's typical operating level. This test specifically related to Hypothesis 2, which states that Cyber Resilience is built on a foundation of Cyber Security.

In the test scenario, the operator sets the temperature of the milk vessel to 23°C, which is considered a reasonable set point. The temperature inside the vessel gradually rises until it reaches

the desired temperature. Once the desired temperature is reached, the measured temperature is maintained within the vessel.

### 7.3.2 Discussion - Test 2

In this test, the system's performance was analysed following a successful cyber-attack. The system was assessed 'as-is' prior to any enhancements or modifications. The objective of this test was to establish a baseline measurement of the system's operating level following a successful cyber-attack. This measurement helped to determine the impact on the system during the attack. This test specifically related to Hypothesis 2, which states that Cyber Resilience is built on a foundation of Cyber Security.

Like the previous test, the operator set the temperature of the milk vessel to 23°C as the desired set point. The temperature inside the vessel gradually increased until it reached the desired set point value. Once the desired temperature was reached, the measured temperature was maintained within the vessel for 120 minutes. At the 120-minute mark, the cyber-attack began. The attacker requested Modbus read values at 125 minutes and sent malicious write value packets at 2 hours 9 minutes and 2 hours 10 minutes. These manipulated temperature readings persist for 4 minutes until the attack concludes. The malicious temperature values, introduced by the attacker, were maintained until the 180-minute mark.

This test allowed for the observation and analysis of how the system operates and performs following a successful cyber-attack, without any additional countermeasures or improvements implemented. By comparing the results of this test to the baseline measurement obtained in the first test, the impact of the cyber-attack on the system could be evaluated.

### 7.3.3 Discussion - Test 3

The focus of this test was on analysing the protection time, which refers to the duration that the system can withstand an incident without degradation prior to CR enhancements I.E., without applying appropriate PLC secure coding techniques.

The analysis of protection time involved considering the safe temperature values as a percentage of the system's performance over time. This analysis was conducted following a successful cyber-attack. Like the previous test, the system was evaluated without any recommended enhancements or modifications. The purpose of this test was to assess how the system responded and adapted during a successful cyber-attack under its current configuration.

By measuring the system's performance over time and comparing it to the safe temperature values, the impact and effectiveness of the system's defences or lack thereof can be evaluated. The analysis of protection time provided insights into how long the system could sustain its performance and withstand an incident without experiencing degradation or compromising its intended functionality.

#### 7.3.4 Discussion - Test 4

The focus of this test was on analysing the time a system can withstand an incident without degradation. Unlike the previous test, in this case, CR enhancements were made to the system. Which involved validating HMI input variables at the PLC level, in addition to the HMI itself. As discussed in Chapter 6, system engineers can configure additional programming in the PLC logic, the HMI or both, to impose threshold limits/validation criteria. This technique, which ensures in this case, that temperature set points are within specified validation criteria, is considered a best practice in (PLC Security, 2021).

The recommended configuration, based on the secure coding guidance, was implemented within the PLC program prior to conducting the test. The specific details of these enhancements, including the PLC program configuration, are depicted in Chapter 6 Figures 6-24 and 6-25 (not included in the provided text). The purpose of these enhancements is to enhance the system's Cyber Resilience and evaluate its ability to withstand a cyber-attack while maintaining performance and functionality.

Following the cyber-attack disruption, the average temperature in the vessel increases to 25.9°C. which showed a relative increase of 11.39% compared to nominal operating temperatures. This increase in temperature lasted for a total of thirty-five minutes. However, despite the temperature rise, it remained within the safety threshold limitations established for the milk production process. Consequently, it does not have an impact on the quality of the milk formula produced.

In summary, although the cyber-attack was successful in causing a disruption, it did not alter the safe temperature values outside of the acceptable threshold limit. Thus, the system continued to operate without any degradation to the product quality. It is therefore, in this specific circumstance, classed as resilient as the system was able to withstand a cyber-attack. This outcome suggests for this specific use case, that by applying Secure PLC controls (PLC Security, 2021), it prevented the system from being tampered with outside of safe limits through the HMI interface. It is also important to highlight that this control did not prevent the cyber-attack causing disruption,



it only prevented the attacker from increasing safe temperature limits, the attacker was still able to modify the system. To increase the system's resilience, it is recommended that several CR attributes and enhancements should be considered, as a single enhancement alone may not be enough to keep the system resilient. Although not demonstrated in this test, it is important to note that although a good outcome was witnessed in this scenario, variations between the results in a different use case or with a different attack type may vary. For instance, if the cyber-attack had originated from a human controller inside the plant and had direct access to the PLC controller, then results may differ. Furthermore, if an external attacker gained access to the plant network and manipulated values in the quality control system logs. This echoes Jacobs, et al., (2018) on the significance of evaluating each individual system to determine which of the Cyber Resilience attributes are being measured and against what disturbance source. (Jacobs, et al., 2018) stated:

“Various measures and approaches have their places in a comprehensive assessment of a system, yet each on their own fail to capture the holistic picture.”

This test demonstrates that even with mature Cyber Security practices, such attacks could impair process control and alter temperatures. This could lead to the production of unsafe infant milk if not spotted by quality procedures. By applying Cyber Resilience enhancements, the system was able to withstand the malicious attempts to modify parameters outside of the allowed threshold and ensure its performance, although in a degraded manner.

### 7.3.5 Discussion - Test 5

Test 5 results indicate that the SOC team responsible for monitoring and detecting cyber threats in the industrial environment lacked sufficient understanding of Modbus traffic, which is a commonly used protocol in these systems. As a result, when the Modbus traffic showed changes, the SOC team did not recognise it as abnormal because they were only familiar with IT protocols and not specifically with Modbus. The attack went unnoticed because the changes in Modbus traffic were consistent and aligned with the daily temperature variations of the PLC (Programmable Logic Controller). Since these changes occur daily as part of normal operations, the SOC team did not realise that the values being altered were outside of the acceptable threshold. Consequently, no follow-up actions were taken and the logs indicating the changes were ignored. It is worth noting that the SOC team did identify suspicious activity prior to this test however, it turned out to be a false positive. This activity involved normal changes to values performed remotely by engineers as part of their regular activities. Although the SOC team followed up on this initially, considering it

suspicious, it was later determined to be a false positive. In the case of a cyber-attack, the SOC team treated it as a normal change and assumed that the alert indicating the attack was also a false positive. As a result, they did not take any further action or communicate with the engineer on duty regarding the incident. These results highlight the need for SOC teams to have a comprehensive understanding of the protocols and traffic patterns specific to industrial control systems, such as Modbus. Without this knowledge, they may overlook or misinterpret suspicious activities, leading to missed opportunities for detecting and responding to cyber-attacks.

Moreover, to test the communication aspects between personnel such as operators/engineers and SOC team. Differentiating cyber-attacks from plant failures is crucial as both events negatively impact the system. It is essential to identify whether a degradation in system performance is the result of a cyber-attack or a plant failure/maintenance to implement appropriate countermeasures. Making this distinction poses significant challenges and yet has received limited attention (Syrmakeisis, et al., 2022). Organisations are encouraged to prioritise efforts in distinguishing between cyber-attacks and plant failures to enable the application of suitable discovery and recovery methods. Investigating the unique characteristics of each unplanned event is necessary for effective differentiation.

### 7.3.6 Discussion - Test 6

In test 6, the system was tested again with the recommended resilience enhancements made and the SOC team was provided with the relevant contact information for the plant engineers on-duty and plant maintenance schedules, which included information about planned maintenance activities, downtimes and expected changes. During the cyber-attack, the SOC team was able to identify the malicious behaviour in the system logs and escalate accordingly. These findings demonstrate that even with good cyber hygiene practices in place, a cyber-attack on a critical manufacturing system can still go undetected unless there are Cyber Resilience initiatives in place. Specifically, the Cyber Resilience control in this case refers to the SOC team's prior knowledge and understanding of normal operational technology (OT) values and what to look for in terms of abnormalities. Having both good Cyber Resilience and good Cyber Security measures in place significantly improves the response time to identify and recover from an attack. By leveraging their understanding of the normal OT values and actively monitoring for any deviations or malicious behaviour, the SOC team was able to detect the cyber-attack in a timely manner.

These results emphasise the importance of incorporating Cyber Resilience measures alongside cyber-security and safety practices. Cyber Resilience initiatives, such as providing the SOC team

with knowledge about normal system behaviour and appropriate response procedures, play a critical role in enhancing the detection and response capabilities of organisations, even when they have implemented strong cyber-security measures. By modelling a remote attack against the system, we were able to enhance Cyber Resilience through the tools and techniques recommended in the case studies informed from various frameworks (Linkov, et al., 2013); (Mitre Corp., 2012); (National Institute of Standards and Technology, 2021); (International Electrotechnical Commission (IEC), 2021). Furthermore, whilst a SOC team ticks the box for good cyber hygiene practices, most SOC analysts are IT professionals who often have little involvement or understanding of the people who operate, manage, design, implement, monitor and integrate production control systems. Conversely, many control system engineers do not fully understand the features and cyber risks of devices. In addition, IT support personnel who provide the communications paths and network defences do not always grasp the systems' operational drivers and constraints. In the same way OT and IT systems converged to coevolve. So too should the traditional IT personnel and OT engineers to both fully understand the design principles underlying control systems and how to support those systems in a manner that ensures cyber availability and integrity. In parallel, the need for control system engineers and operators to better understand the important role they play in cyber-security. This starts by ensuring that a control system is designed and engineered with cyber-security built into it and that cyber-security has the same level of focus as system reliability throughout the system lifecycle (Sans 2022).

When these distinct groups of professionals work together, they spoke a common language that enabled them to work together to secure their industrial control system environments. They will help develop cyber-secure-aware engineering practices and real-time control system IT /OT support carried out by professionals who understand the physical effects of actions in the cyber world. The next section will discuss how the research questions were answered.

## 7.4 Answering the Research Questions

Specifically, there are three questions this thesis aimed to answer, these were:

### 7.4.1 In response to Question 1

#### **What are the current methods employed to analyse the level of Cyber Resilience in manufacturing systems?**

The significance of this topic has grown among researchers due to the widespread adoption of digital and online technologies by businesses (Rehmani, et al., 2018). Consequently, there exists a vast body of literature on Cyber Resilience measurement, encompassing various theoretical, technical and organisational perspectives (Tiwari et al., 2020). Broadly speaking, these approaches can be categorised into qualitative and quantitative methods, with a few utilising a combination of both. A comprehensive review of the relevant literature on Cyber Resilience and its measurement is presented in Chapter 3.

Although Cyber Resilience is a compelling concept, imprecise usage can lead to counterproductive outcomes. The ambiguity and misconception surrounding the term pose challenges in defining, designing, implementing and measuring it (Manyena, 2006), which hampers its adoption uptake by policy makers (Linkov & Kott, 2018). Despite the existence of numerous approaches, frameworks and metrics, a lack of consistency prevails as each approach tends to be domain-specific (Benson & Craig, 2014); (Zhu, et al., 2016); (Davidson, et al., 2016). Consequently, experts remain sceptical, dismissing it as one of the passing trends in Cyber Security (Dupont, 2019).

To address the limitations highlighted in the preceding paragraphs, this research began by conducting a multidisciplinary literature review in Chapter 3, which explored the multiple dimensions of Cyber Resilience and the criteria necessary for its implementation and measurement. Specifically, three critical areas were examined in Chapter 3 in response to this research question:

- The current Operational Technology landscape and the need for a shift in thinking towards Cyber Resilience.
- The various interpretations and applications of the term across different disciplines.
- The existing approaches to Cyber Resilience that are relevant to the OT sectors.

Furthermore, Chapters 4 and 6 outline the approach and tests conducted to measure the Cyber Resilience of a manufacturing system, both before and after implementing resilience

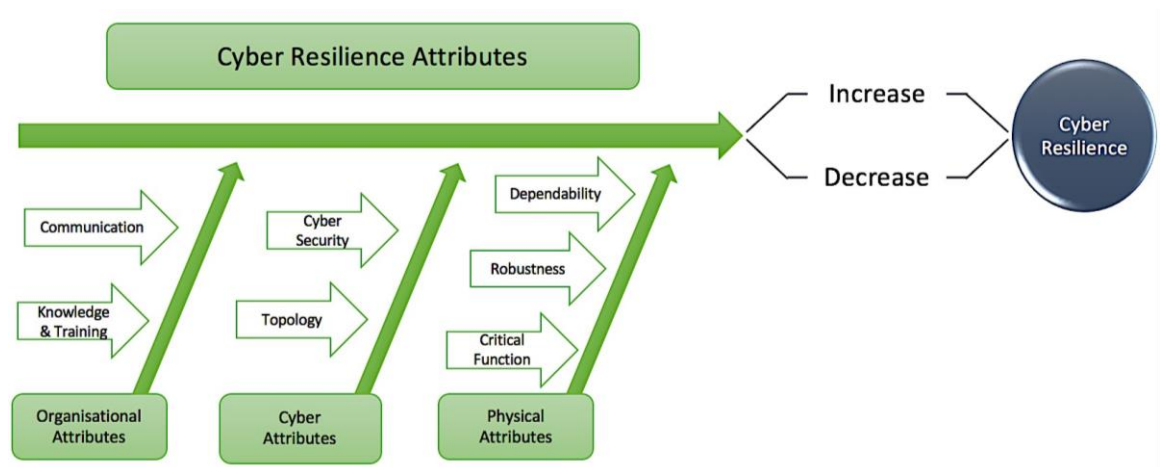
enhancements. The hypotheses, case studies and simulations demonstrate that the most effective approach for obtaining an objective quantitative metric for Cyber Resilience, without jeopardising real-life critical systems, involves a combination of qualitative assessments and quantitative modelling of disruption impacts. However, this approach entails significant costs, time, resources and a comprehensive understanding of the interconnected dependencies, components, systems and organisational complexities involved.

## 7.4.2 In response to Question 2

**Which attributes and parameters are suitable for Cyber Resilience and which of the attributes stood out in the results?**

Chapter 3, specifically Sections 3.5.1 and 3.5.2, extensively discusses the attributes and parameters associated with Cyber Resilience. A comprehensive and holistic approach to Cyber Resilience is emphasised, necessitating organisations to consider various attributes and relevant parameters to develop tactics that address the most pertinent attributes. Attributes in the context of Cyber Resilience pertain to the characteristics or features of a system that contribute to its ability to withstand and recover from cyber-attacks, disruptions and failures. Examples of Cyber Resilient attributes include redundancy, flexibility, efficiency, security, diversity and complexity (Berger, et al., 2021).

The specific attributes that stood out during the experiments conducted for this research (as explored in Section 6.3.2), included: Critical Function, Inherent Safety, Topology, Cyber Security, Communication and Training. Each attribute incorporated across each of the Cyber, Physical and Organisational domains (see Figure 7-4).



*Figure 7-4 Experiment Cyber Resilience Attributes*

Conversely, Cyber Resilient parameters are specific metrics or measurements used by organisations to evaluate the resilience of their systems. These parameters quantify the effectiveness of the CR attributes and facilitate the systematic and quantitative assessment of a system's overall resilience. Diagrams illustrating high-level attributes are provided in Chapter 3.3 to demonstrate how each attribute can impact a system's Cyber Resilience. It is important to note that the attributes selected for enhancing cyber resilience should be carefully considered. As discussed in Chapter 3, context

matters and each system should be looked at in intricate detail prior to selecting which of the attributes to enhance.

A list of potential Cyber Resilience metrics relevant to the manufacturing industry is also presented in Chapter 3.3. These attributes and parameters are integral components of Cyber Resilience in the manufacturing sector. While each attribute and parameter possess distinct characteristics, they often exhibit interdependence and synergistic effects, enhancing the industry's ability to prevent, detect, respond and recover from cyber disruptions. When each of the attributes selected for the experiment were categorised to the stages of resilience, it became apparent that the cyber specific attributes provided a means to measure the organisation/systems ability to *Prevent*. The physical attributes provided a means to measure the system's ability to *Withstand/Adapt* and the organisational attributes provided a means to measure the organisation's ability to *Detect/Recover*. Results show that when attributes existed in a single domain without cooperation from attributes in the other domains, cyber resilience was not achieved, when an attribute existed in all 3 of the domains at the same time, results demonstrated the system's ability to prevent, withstand, adapt, detect and recover from a cyber-disruption, thus, significantly increasing the systems overall cyber resilience.

Finally, Chapter 6 (section 6.3.2) and Chapter 7 (section 7.4.3) illustrate an approach to determine the most relevant attributes and parameters for the system being examined.

### 7.4.3 In response to Question 3

#### **How to provide a level of assurance that a manufacturing system is Cyber Resilient using this research approach?**

To determine if the approach stipulated in this thesis is relevant, example use cases, taken from actual events, are theoretically analysed and executed using the method proposed in Chapter 6. Examples are necessary to provide a clear understanding of the approach. Here, for instance, the use case of the cyber-attack on the Oldsmar Florida water treatment plant (discussed in chapter 2) is used.

Water treatment plants typically manage the release of sodium hydroxide (NaOH), which is commonly used as a chemical reagent in water treatment processes. Sodium hydroxide is added to the water to stabilise the PH values and usually released at one hundred parts per million (ppm), although may fluctuate depending on the pre-treated water's pH value.

As a reminder to the reader and to save page flicking, in the Oldsmar water attack, the assumed attacker or human operator (since the course of events leading up to the assumed attack are still unclear), gained access to the plant remotely and changed the values to 11000 ppm. This amount of Sodium Hydroxide is dangerous to human health and if consumed could cause vomiting, illness or in rare cases, even death.

An example of a topology (created on the cyber range) for this use case is given in Figure 7-5.



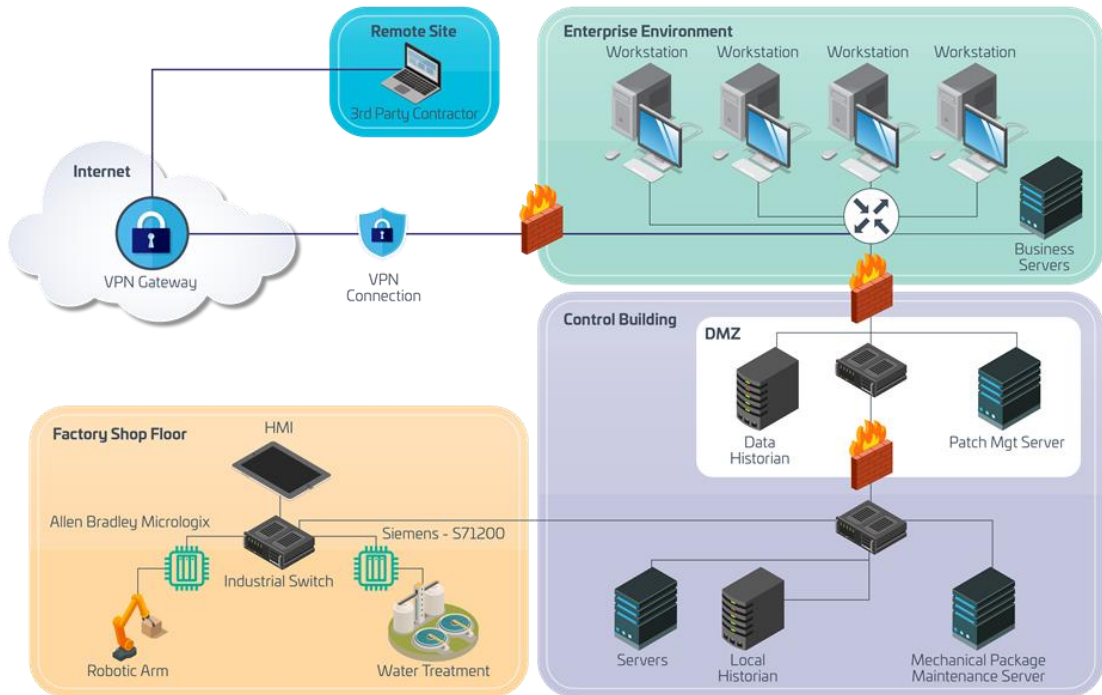


Figure 7-5 Oldsmar Water Attack - hypothetical use case

To understand which CR metrics to select for this use case, a general overview of how a water treatment plant manages the release of sodium hydroxide is given (Imran, et al., 2016):

- Dilution and Mixing: Sodium hydroxide is a highly caustic substance and can be hazardous if released directly into the environment. Therefore, water treatment plants typically dilute and mix sodium hydroxide with water or other chemicals to reduce its concentration and neutralise its caustic properties.
- Controlled Dosage: Sodium hydroxide is added to the water treatment process in controlled amounts to adjust the pH levels. The dosage is calculated based on the water quality and treatment requirements. By maintaining precise control over the addition of sodium hydroxide, the plant can minimise the risk of excess or uncontrolled releases.
- Automated Systems and Alarms: Water treatment plants often employ automated systems and alarms to monitor and control the addition of chemicals, including sodium hydroxide. These systems can detect deviations in dosing rates, pH levels or other parameters and trigger alarms to alert operators. Swift response to such alarms helps prevent overfeeding or accidental releases.
- Secondary Containment: Water treatment plants have measures in place to contain and capture any accidental releases or leaks. Secondary containment systems, such as bunds, basins or collection tanks, are designed to capture spilled sodium hydroxide and prevent it

from reaching the environment. These systems allow for the safe clean-up and disposal of the spilled material.

- **Training and Safety Procedures:** Water treatment plant operators undergo training on the safe handling, storage and disposal of chemicals. They follow strict safety procedures to minimise the risk of accidental releases. This includes wearing appropriate personal protective equipment (PPE) and following established protocols for handling sodium hydroxide. However, it is apparent that this training does not include Cyber Security awareness.
- **Disposal and Wastewater Treatment:** After the water treatment process, any residual sodium hydroxide that is not consumed or reacts with water is typically removed during the wastewater treatment phase. Water treatment plants employ various techniques, such as pH adjustment, coagulation, flocculation and sedimentation to remove and neutralise chemicals from the treated water before it is released back into the environment.

It is important to note that the specific procedures and technologies employed by water treatment plants may vary depending on factors such as local regulations, plant size and treatment processes used.

The metrics that could be selected for enhancing system resilience in this hypothetical scenario are given in Figure 7-6.

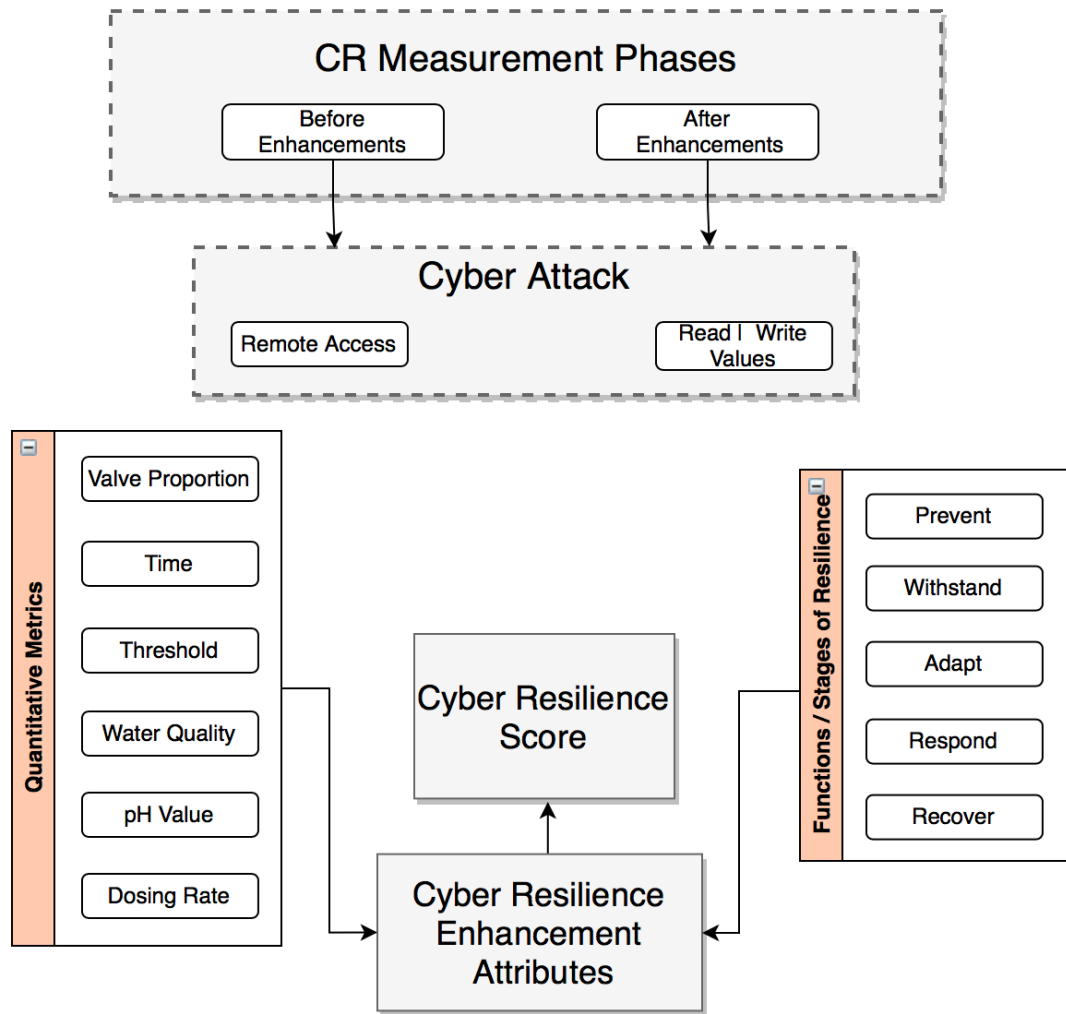


Figure 7-6 The Cyber Resilience attributes selected for theoretical use case.

An analysis of the system design process and the method of attack for this use case highlighted three issues.

- There are poor access controls for remote connections into the plant.
- There is an inadequate, or lack of, security monitoring of industrial logs.
- There is little or no validation of thresholds limits configured within the PLC set points which would prevent data input error.

These are like the problem themes that were evident within the case studies undertaken in this research (discussed in chapter 5). Figure 7-7 shows two attack routes into the water treatment plant system (presented by blue/red arrows).

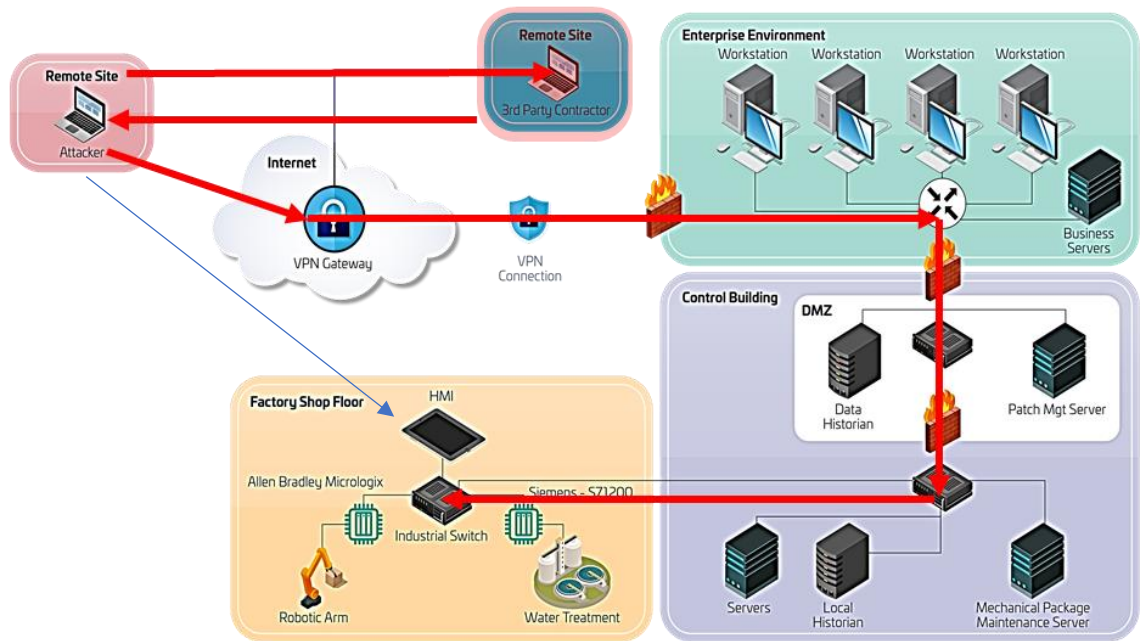


Figure 7-7 Attack steps into the plant.

In response to the three problem areas specified above, recommendations for enhancing resilience are comparable with the experiment undertaken in this research (Chapter 6), which in summary include:

- Network Segmentation: Segment the system into smaller networks with restricted access, so that if any attacker can gain access to the manufacturing system, they will not be able to gain access to other areas of the system.
- Monitoring and understanding OT logs: Properly monitor and understand the logs of the manufacturing system for any suspicious user activity. This includes monitoring for any sudden changes in login timings, logins from unexpected geographic locations, unusual user activity and monitoring of the OT communication protocols.
- Adopt Secure PLC system configuration practices (as described in Chapter 3) and control eight, in particular, which states: “Validate HMI input variables at the PLC level, not only at the HMI” (PLC Security, 2021).

The next section will discuss the limitations of this research.

## 7.5 Limitations

The case studies conducted for this thesis faced several challenges, including the difficulty in obtaining confidential data and the reluctance of organisations to participate in the research. Additionally, conducting and reporting on such studies was time-consuming. The analysis of the case studies relied on qualitative expert opinions and subjective assessments.

In terms of the physical testbed and simulations, this thesis only modelled three specific topic areas. It suggests that future work should encompass all Cyber Resilience controls within a particular framework to obtain a comprehensive measure of a system's CR maturity level. The thesis primarily focused on the CR of critical systems and components within the manufacturing sector. While some consideration was given to organisational and human elements of CR, the main emphasis was on the system itself. This decision was made due to the substantial challenges associated with addressing CR at the organisational level, which was deemed out of scope for this research.

## 7.6 Chapter Summary

The research objectives, which aimed to determine if Cyber Resilience can mitigate the impact of a successful cyber-attack on a manufacturing system and if it can be quantitatively measured, has been affirmatively addressed. This was accomplished through real-life case studies utilising established frameworks, as well as the modelling of a critical subset system as a holistic soft system. The thesis brings attention to non-holistic issues arising from incomplete knowledge about the overall system interactions within complex system-of-systems. It underscores the significance of analysing all scenarios and emerging properties that could impede the system's intended functionality and lead to adverse consequences. While the studies by (Carias, et al., 2018) and (Min et al, 2007) demonstrate the benefits of using System Dynamics as a modelling technique and also made a significant contribution towards the approach of the experiments undertaken in this research, it is also important to consider that while simulation models like System Dynamics offer valuable insights in understanding the complexities of enhancing CR in the manufacturing OT industry, they should be regarded as a starting point (as discussed in Chapter 3). The authors acknowledged that real-world validation and accounting for environmental factors are crucial to ensure the model's reliability and practicality in guiding actual decision-making and policy implementation and as such this research built upon this foundation by adding in these crucial factors.

Highlighting the unique insights from the study, this research presents a novel approach to quantitatively measure Cyber Resilience in manufacturing systems by comprehensively analysing all system interactions, encompassing digital and mechanical connectivity along with human controllers and selecting appropriate attributes and parameters. The practical indicators of a systems resilience include the interplay between secure control practices and inherent resilience mechanisms. Demonstrating that security, engineering and safety practices must work together collaboratively in order to achieve Cyber Resilience in a manufacturing system. The findings of this study can help guide practitioners into understanding the criticality of integrating security, system and safety engineering practices to enhance Cyber Resilience in safety-critical complex-systems.

While no recorded instances of cyber-attacks targeting infant milk production plants have been reported, the results highlight the importance of taking Cyber Resilience seriously in the food and beverage industry. A cyber-attack could have severe implications for the safety and quality of products manufactured in such plants. The findings validate that Cyber Resilience is a crucial aspect of digital systems; however, it must be exercised with caution. For example, in the production of infant milk formula, different areas of the plant have varying temperature requirements. A temperature fluctuation that may be tolerable in one area could be catastrophic in another. For example, the pre-processing area must consistently maintain a specific temperature and any drop below the critical value renders the system non-resilient, even if the temperature recovers. Conversely, the storage area may allow for some temperature variation outside the assigned value if it is rectified within a specified period. If the temperature capacity recovers within that time, the system remains resilient. However, it acknowledges that achieving and measuring Cyber Resilience can be challenging and beyond the capabilities of certain organisations due to limitations in budgets, resources, expertise and the rapid pace of technological advancements.

The study concludes that the most practical approach to obtaining empirical quantitative metrics without impacting critical real-life systems involves a combination of qualitative assessments and quantitative modelling of disruption impacts. Nevertheless, this approach entails costs, time requirements, resource allocation and an extensive understanding of the interconnected dependencies, components, systems, organisation and complexity involved.

The next chapter concludes this research.

# Chapter 8

## Conclusion and Future Work

### 8.1 Introduction

The industrial manufacturing sector is experiencing rapid growth and undergoing significant transformation, driven by factors such as sustainability, process streamlining, cost-cutting pressures and the need for safer working environments. However, these positive advancements also come with challenges, including the increasing threat of cyber-attacks on control systems. The convergence of Operational and Informational Technology has become crucial, yet the traditional security approach is insufficient to tackle the unique challenges faced by this industry.

The concept of Cyber Resilience has gained momentum as a promising solution to address these challenges. Nevertheless, confusion surrounding its application, multiple definitions and scope variations have led to debates in the literature. While efforts have been made to develop resilience metrics, they often lack suitability for specific cases, such as critical manufacturing systems. The research also ascertains the lack of research on quantitative Cyber Resiliency measurements, particularly in the context of combined OT and IT systems (Kott & Linkov, 2021).

The aim and objectives established in the introductory chapter, along with the findings presented in individual chapters, support the hypotheses and conclusions drawn. This chapter provides a summary and evaluation of the findings derived from the research conducted in this thesis.

### 8.2 Summary of Findings

The literature review, discussed in Chapter 3, reveals significant gaps in defining Cyber Resilience metrics due to its dependence on various factors specific to each scenario or use case. This research addresses this gap by demonstrating the need to develop a more practical and customisable

approach in measuring Cyber Resilience. As a result, this thesis takes a significant step towards providing a framework for objectively and quantitatively measuring a critical manufacturing system's Cyber Resilience.

Through two case study evaluations at real-world manufacturing plants and the development of an experimental testbed, this research captures valuable data related to a manufacturing system's resilience. The Cyber Resilience metrics proposed in this thesis offer insights into the impact of cyber-attacks and the effectiveness of resilience enhancements. This research demonstrates how enhanced Cyber Resilience can mitigate the impact of cyber-attacks on critical manufacturing systems validating **Hypotheses 1 and 2**. The combination of qualitative and quantitative approaches in measuring Cyber Resilience provides valuable insights based on real-world case study evidence and objective modelling of resilience attributes and enhancement strategies. The findings highlight essential attributes and parameters that serve as practical indicators of a system's Cyber Resilience. Notably, the study reveals that when secure control practices are combined with various resiliency measures, the system's ability to endure and recover from a disruption is enhanced. Furthermore, the thesis examines the relevance of its proposed approach by analysing and theoretically executing example use cases based on real events. One such case is the cyber-attack on the Oldsmar Florida water plant discussed in Chapter 2 and analysed in Chapter 7. The analysis highlighted three major issues, specifically:

- There are poor access controls for remote connections into the plant.
- There is an inadequate, or lack of, security monitoring of industrial logs.
- There is little or no validation of thresholds limits configured within the PLC set points which would prevent data input error.

These are comparable with those identified in the real-life studies conducted for this research and suggests potential attack routes into the system.

The findings highlight the need to base resilience metrics on the purpose, intended functionality and requirements of each system. Since different systems within the same environment may have varying resilience requirements based on specific factors, such as temperature fluctuation tolerance. These observations lead to two conclusions. First, the systems are no longer identical. Despite having the same components and setup, external dependencies beyond the temperature make each system distinct. Second, the temperature behaviour can be relaxed in some production areas and yet this may be detrimental in others. It is therefore crucial to base resilience metrics on each system's purpose. Furthermore, collaboration between security analysts, IT professionals, plant operators and system engineers is essential for effective Cyber Resilience. The convergence



of these professionals' knowledge and expertise enables the development of secure engineering practices and real-time IT/OT support for industrial manufacturing systems.

The conclusions drawn from each case study emphasise the importance of having a well-established level of Cyber Security hygiene before conducting a Cyber Resiliency assessment. While the frameworks provided an assessment approach for each plant, they were not suitable for obtaining an accurate CR baseline and therefore could not measure how a company had improved over time. Despite the different problems in each case study, they shared similarities in their respective areas of concern as described above. The results suggest that an organisation should have a mature Cyber Security operation before performing a Cyber Resiliency analysis effectively. The case study findings satisfied **Hypothesis 2**, which states that Cyber Resilience is built on a foundation of Cyber Security.

The conclusions drawn from the Simulation Testbed, both the experimental and hypothetical results corroborate **Hypothesis 1** in that Cyber Resilience is a crucial aspect of ICS systems (Jacobs, et al., 2018); (INCOSE Resilient Systems Working Group, 2020); (Kott & Linkov, 2019); (M. A. Haque, et al., 2018); (DiMase, et al., 2015); (Dupont, 2019). Conversely, caution must be exercised in its application.

Overall, this thesis provides a philosophical foundation and a holistic approach to obtaining a quantitative metric of Cyber Resilience for a manufacturing system. It acknowledges the complexity and diversity of contexts in which resilience is measured and highlights the importance of core security and safety controls as a foundation for effective CR. The presented CR landscape contributes to the knowledge base in obtaining useful metrics for cyber manufacturing systems and offers an approach to obtaining both qualitative and quantitative measurements.

Highlighting the unique insights from this study, this research presents a novel approach to quantitatively measure Cyber Resilience in manufacturing systems by comprehensively analysing all system interactions, encompassing digital and mechanical connectivity along with human controllers and selecting appropriate attributes and parameters. The practical indicators of a systems resilience include the interplay between secure control practices and inherent resilience mechanisms. This research underscores the importance of integrating security, system and safety engineering practices to enhance Cyber Resilience. It demonstrates how Cyber Resilience can effectively address the emerging complexities associated with safety-critical complex systems. In conclusion, this thesis contributes significantly to the understanding of Cyber Resilience in the context of manufacturing systems. Its findings shed light on the importance of proactive measures and informed decision-making to bolster the industry's ability to withstand and recover from cyber-

attacks. As the manufacturing sector continues to evolve, implementing Cyber Resilience strategies will be a key factor in ensuring sustained growth, security and operational continuity in the face of an ever-changing threat landscape.

The next section discusses the research objectives answered in this thesis.

### 8.3 Research Objectives

The research objectives explored existing OT architecture design spaces to understand how cyber-applied safety practices may impact the availability of a critical system and modelled a novel architecture design to facilitate a more resilient system architecture so that cyber and safety can coevolve. Specifically, the research objectives were to:

1. Establish the various definitions of ‘Resilience’ and clearly identify how definitions vary between domains and contexts (answered in Chapter 3).
  - a. Establish a definition of Cyber Resilience in the context of this research for an industrial manufacturing system (answered in Chapter 3).
2. Define the characteristics and parameters of Cyber Resilience (answered in Chapter 3);
3. Conduct a literature study of CR in safety-critical complex-systems focused on the manufacturing industry to establish the current state of the art (answered in Chapter 3).
  - a. Establish current approaches in literature toward the measurement of CR and to define which of the approaches are most relevant and meaningful (answered in Chapter 3);
4. Conduct primary research by way of case studies to collect original datasets from various sources across the industrial manufacturing sectors (answered in Chapter 5).
  - a. Analyse case study results, with focus on the most critical systems, zones and communications; establish qualitative baseline maturity levels and provide a series of recommendations through various frameworks and best practice guidance on how each study can enhance their CR maturity.
  - b. Identify limitations with the selected frameworks (answered in Chapter 6).
5. Design and build a representative physical test bed emulating a critical manufacturing system informed from case study observations (answered in Chapter 4).
  - a. Develop a cyber-attack to target the representative system; informed by case study evaluations (answered in Chapter 4).

- b. Define a series of metrics to quantitatively measure Cyber Resilience of a representative manufacturing system in the event of a cyber-attack (answered in Chapter 4).
- c. Implement and test simulation and modelling techniques to determine if the metrics and approaches defined enable a manufacturing system to achieve sustainability in a degraded situation (answered in Chapter 6 and Chapter 7).
- d. Analyse, record and discuss the results (answered in Chapter 6 and Chapter 7).

## 8.4 Future Work

The methodology employed in this thesis involved conducting in-depth analysis, which required a significant amount of time and effort. However, it is important to note that the metric obtained from this analysis represents a single point in time. Future work should focus on enhancing this approach by incorporating autonomous methods, such as AI, to continually monitor Cyber Resilient systems and provide notifications of any changes in maturity.

The case studies conducted in both plants revealed three common problem areas, irrespective of their differences in Cyber Security (CS) maturity levels and assessment frameworks. The simulation model and tests were specifically targeted at addressing these areas of concern. However, future research should adopt a holistic approach and explore a broader range of problem areas beyond these three specific topics. It is essential to consider industry-specific areas that were outside the scope of this thesis, such as on/offshore structures, oil rigs and wind farms, to gain a comprehensive understanding of Cyber Resilience in various contexts.

## 8.5 Contribution to knowledge

The field of Cyber Resilience measurement on industrial manufacturing systems is crucial for ensuring the security and safety of critical infrastructure. This PhD thesis makes valuable contributions to this field.

- It provides a detailed evaluation on the characteristics and parameters of Cyber Resilience (presented in Section 3.3).
- It uses case studies to validate qualitative approaches, which themselves are a contribution to knowledge given the sparsity of examples in literature (described in Chapter 5).
- It documents the creation of a physical testbed to perform analysis and obtain quantitative metrics, which other can emulate (presented in Section 6.2).
- It documents the development of an original cyber-attack with a labelled dataset, collected from the industrial manufacturing testbed, which provides an invaluable resource for researchers working in this field (explained in Section 6.2.3).
- It provides a comprehensive evaluation of the factors that contribute to Cyber Resilience in industrial control systems (described in Section 6.3.1).
- It includes a Cyber Resilience milk formula production use case (expressed in Section 6.4).
- It proposes and documents an approach to obtaining a quantitative, objective, Cyber Resilience metric for a critical manufacturing system (described in Section 6.4.1).

Overall, this PhD thesis represents a significant contribution to the field of Cyber Resilience measurement on industrial control systems. Its use of both qualitative and quantitative approaches, as well as the physical test bed, provision of an original cyber-attack and labelled dataset, makes it a valuable resource for researchers and practitioners alike.

# References

- Ahmad, A., Johnson, C. & Storer, T., 2015. An Investigation on Organisation Cyber Resilience. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, Volume 9, pp. 1661-1666.
- Albasrawi, M. N., Jarus, N., Joshi, K. A. & Sarvestani, S. S., 2014. Analysis of Reliability and Resilience for Smart Grids. In: *IEEE 38th Annual Computer Software and Applications Conference*. Vasteras, Sweden: IEEE, pp. 529-534.
- Assante, M. J. & Lee, R. M., 2015. *The ICS Cyber Kill Chain*. [Online] Available at: <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297> [Accessed 2019].
- Avizienis, A., Laprie, J. C., Randell, B. & Landwehr, C., 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), pp. 11-33.
- Axelsson, J., 2022. *What Systems Engineers Should Know About Emergence*. USA: INCOSE.
- Ayyub, B. M., 2014. Systems resilience for multihazard environments: Definition, metrics and valuation for decision making. *Risk Analysis*, 34(2), p. 340–355.
- Bagheri S, R. G., 2017. *Organisational Cyber Resilience: research opportunities*. Australia, ACIS2017.
- Bagheri, S. & Ridley, G., 2017. *Organisational cyber resilience: research opportunities*. Hobart, Australasian Conference on Information Systems.
- Bagheri, S., Ridley, G. & Williams, B., 2023. Organisational Cyber Resilience: Management Perspectives. *Australasian Journal of Information Systems*, Volume 27.
- Banerjee Ruths, M., 2009. The Lesson of John Snow and the Broad Street Pump. *Virtual Mentor*, Volume 11, pp. 470-472.
- Barbacci, M., 1995. Quality Attributes. *Software Engineering Institute*, p. 16.
- Baumgart, S., Froberg, J. & Punnek, S., 2018. *Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site*. Rome, IEEE, pp. 1-8.

- Benson, M. H. & Craig, R. K., 2014. The end of sustainability. *Society & Natural Resources*, 27(7), pp. 777-782.
- Berger, C., Peichhammer, P., Hans, P. & Domaschka, P., 2021. A Survey on Resilience in the IoT: Taxonomy, Classification and Discussion of Resilience Mechanisms. *ACM Computer Surveys (CSUR)*, September, 54(7), pp. 1-39.
- Biringer, B., Vugrin, E. & Warren, D., 2013. *Critical Infrastructure, System Security and Resiliency*. 13 ed. New York: CRC Press.
- Björk, F., Henkel, M., Stirna, J. & Zdravkovic, J., 2015. Cyber Resilience – Fundamentals for a Definition. In: A. Rocha, A. Correia, S. Costanzo & L. Reis, eds. *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*. Cham: Springer International Publishing, pp. 3-4.
- Bodeau, D., Graubart, R., Heinbockel, W. & Laderman, E., 2015. *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*, Bedford, MA: Mitre Corporation.
- Bodeau, G., 2011. *Cyber Resiliency Engineering Framework*. Bedford, The MITRE Corporation.
- Bronk, C. & Tikk, E., 2013. The Cyber Attack on Saudi Aramco. *Survival*, Volume 55.
- Brtis, J. S. & McEvilley, M. A., 2019. *Systems Engineering for Resilience*, Colorado Springs: The MITRE Corporation.
- Bruneau, M. et al., 2003. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake spectra*, 19(4), pp. 733-752.
- Bryson, R., 2018. *Building Cyber Resilience*. [Online] Available at: <http://www.rjmcgregor.com/wp-content/uploads/2018/09/Building-Cyber-Resilience.pdf> [Accessed 2 4 2021].
- Cambridge Dictionary, 2023. *Resilience*. [Online] Available at: <https://dictionary.cambridge.org/dictionary/english/resilience> [Accessed 15 January 2023].
- Caralli, R. et al., 2016. *CERT Resilience Management Model*, USA: CERT.
- Cariás, J. F., Arrizabalaga, S., Labaka, L. & Hernantes, J., 2021. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access*, 9(1), pp. 80741-80762.

- Cariás, J. F., Arrizabalaga, S., Labaka, L. & Hernantes, J., 2021. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access*, 9(1), pp. 80741-80762.
- Cariás, J., Labaka, J., Sarriegi, J. & Hernantes, J., 2018. *An approach to the modeling of CR management*. Bilbao, Spain, IEEE, pp. 1-6.
- Census-Records, 1831. *Census-Records*. [Online] Available at: <https://www.nationalarchives.gov.uk/help-with-your-research/research-guides/census-records/> [Accessed 2022].
- Chang, V. et al., 2015. A resiliency framework for an enterprise cloud. *International Journal of Information Management*, 36(1), pp. 155-166.
- Cherdantsevaa., Y. et al., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56(1), pp. 1-27.
- Cherdantsevaa, Y. et al., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56(1), pp. 1-27.
- Chittister, C. G. & Haimés, Y. Y., 2011. The Role of Modeling in the Resilience of Cyber infrastructure Systems and Preparedness for Cyber Intrusions. *Econ Papers*, 8(1), p. 22.
- Choudhury, S., Rodriguez, L., Curtis, D. & Oler, K., 2015. *Action Recommendation for Cyber Resilience*. New York, ACM, pp. 3-8.
- Clark, A. & Zonouz, S., 2017. Cyber-Physical Resilience: Definition and Assessment Metric. *IEEE Transactions on Smart Grid*, Volume 99, pp. 1-1.
- Clark-Ginsberg, A., 2016. *Whats the difference between Reliability and Resilience*, Stanford: Stanford University.
- Collier, Z. A. et al., 2016. Security Metrics in Industrial Control Systems. In: E. J. Colbert & A. Kott, eds. *Cyber-security of SCADA and Other Industrial Control Systems*. Cham: Springer, pp. 167-185.
- Coulouris, G., Dollimore, J. & Kindberg, J., 2021. *Distributed Systems: Concepts and Design*. 5th Edition ed. USA: Addison-Wesley.
- Creese, J., 2019. Cyber protection of public assets. *ITNOW*, 61(3), p. 36–37.
- Cybenko, G., 2019. Metrics based on the System Performance Perspective. In: A. Kott & I. Linkov, eds. *Cyber Resilience of Systems and Networks*. Cham: Springer, pp. 29-40.

Dakwat, A. L. & Villani, E., 2018. System safety assessment based on STPA and model checking. *Safety Science*, Volume 109, pp. 130-143.

Davidson, J. L. et al., 2016. Interrogating Resilience: toward a typology to improve its operationalisation. *Ecology and Society*, 21(2), pp. 1-15.

Davies, P., 2021. *How the Security You Chose Affects Functional Safety*. [Online] Available at: <https://the26262club.com/2021/11/10/how-the-security-you-chose-affects-functional-safety/> [Accessed 10 10 2022].

Department of Homeland Security, 2018. *Publications*. [Online] Available at: [https://www.dhs.gov/sites/default/files/publications/dhs\\_resilience\\_framework\\_july\\_2018\\_508.pdf](https://www.dhs.gov/sites/default/files/publications/dhs_resilience_framework_july_2018_508.pdf) [Accessed January 2021].

DiMase, Z., Collier, K., Heffner, K. & Linkov, I., 2015. Systems Engineering framework for Cyber Physical Security and Resilience. *Environment Systems and Decisions*, June, Volume 35, pp. 291-300.

Donnelly, P., Abuhmida, M. & Tubb, C., 2022. The Drift of Industrial Control Systems to Pseudo Security. *International Journal of Critical Infrastructure Protection*, Volume 38.

Dragos, 2022. *Dragos 2021 year in review*. [Online] Available at: <https://www.dragos.com/year-in-review/#section-threats> [Accessed 26th June 2022].

Dubois, D. & Prade, H., 2012. Possibility Theory. In: *Computational Complexity*. Boston: Springer, p. 2240–2252.

Dunigan O'Keeffe, H. S. A. S. T. D., 2021. *Bain & Company - Getting Business Resilience Right*. [Online] Available at: <https://www.bain.com/insights/getting-business-resilience-right/> [Accessed 25th August 2022].

Dupont, B., 2019. The Cyber-Resilience of financial institutions: significance and applicability. *Journal of Cyber-security*, 11 October, 5(1), pp. 1-17.

Easley, D. & Kleinberg, J., 2010. *Networks, Crowds and Markets: Reasoning About a Highly Connected World*. 1st ed. USA: Cambridge University Press.



- Elebute, K., 2018. A Grounded Theory of Security and Technical Barriers to the Continuance Use of Cloud Storage by SMEs. *Information Security and Computer Fraud*, 6(1), pp. 1-7.
- Espinoza-Zelaya, C. & Bai Moon, Y., 2022. Resilience Enhancing Mechanisms for Cyber Manufacturing Systems against Cyber Attacks. *IFAC Paper Online*, pp. 2252-2257.
- Estay, D. A., Sahay, R., Barfod, M. B. & Jensen, C. D., 2020. A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 97(1), p. 101996.
- European Central Bank, 2021. *Cyber Resilience*. [Online] Available at: <https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html>
- European Commission, 2022. *European Commission Website*. [Online] Available at: <https://digital-strategy.ec.europa.eu/en/news/new-funding-calls-under-digital-europe-programme-boost-cyber-resilience> [Accessed 15th December 2022].
- Evans, S., 2018. *Mondelez's NotPetya cyber attack claim disputed by Zurich*, US: Reinsurance News.
- Eves, D., 2014. *Two steps forward, one step back: A brief history of the origins, development and implementation of health and safety law in the United Kingdom*. Birmingham, UK, The Royal Society for the Prevention of Accidents.
- Ferdinand, J., 2015. Building organisational cyber resilience: a strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning*, 9(2), p. 185–195.
- Firesmith, D., 2022. *System Resilience Part 2: How System Resilience relates to other Quality Attributes*. [Online] Available at: <http://insights.sei.cmu.edu/blog/resilience-part-2-how-system-resilience-relates-to-other-quality-attributes/> [Accessed 09th May 2023].
- Fisher, R. & Norman, M., 2010. Developing measurement indices to enhance protection and resilience of critical infrastructures and key resources. *Journal of Business Continuity and Emergency Planning*, 4(3), pp. 191-206.
- Florin, M. & L. I., 2016. *IRGC resource guide on resilience*. USA: IRGC.
- Ford, R., Carvalho, M. & Mayron, L., 2012. *Toward Metrics for Cyber Resilience*. USA, Florida Institute of Technology University of California at Davis.

Fox-Lent, C., Read, L. & Allen, C., 2018. Tiered Approach to Resilience Assessment. *Risk Analysis*, Volume 38.

Friedburg, I. et al., 2017. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, 34(2), pp. 183-196.

Gartner, 2020. *Operational Technology (OT)*. [Online] Available at: [https://www.gartner.com/en/information-technology/glossary/operational-technology-ot#:~:text=Operational%20technology%20\(OT\)%20is%20hardware,Research](https://www.gartner.com/en/information-technology/glossary/operational-technology-ot#:~:text=Operational%20technology%20(OT)%20is%20hardware,Research) [Accessed 2021].

Gates, D. & Bremicker, M., 2017. *Beyond the hype. Separating ambition from reality in i4.0*. Switzerland: KPMG International.

General Electric, 2017. *Network Segmentation for Industrial Control Environments*. [Online] Available at: [https://www.ge.com/digital/sites/default/files/download\\_assets/network-segmentation-for-industrial-control-environments-whitepaper.pdf](https://www.ge.com/digital/sites/default/files/download_assets/network-segmentation-for-industrial-control-environments-whitepaper.pdf) [Accessed 05th January 2021].

Giacomello, G. & Pescaroli, G., 2019. Managing Human Factors. In: A. Kott & I. Linkov, eds. *Cyber Resilience of Systems and Networks*. New York: Springer International Publishing, pp. 381-401.

Goldbeck, N., Angeloudis, P. & Ochieng, W. Y., 2019. Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. *Reliability Engineering and Systems Safety*, March, Volume 188, pp. 62-79.

Goodman, P. & Haisley, E., 2007. Social comparison processes in an organizational context: New directions. *Organizational Behavior and Human Decision Processes*.

Google Books, 2022. *Ngram Viewer*. [Online] Available at: [https://books.google.com/ngrams/graph?content=cyber resilience&year start=1800&year end=2019&corpus=0&smoothing=3](https://books.google.com/ngrams/graph?content=cyber%20resilience&year_start=1800&year_end=2019&corpus=0&smoothing=3)

Goss, D. A., 2009. Johannes Amos Comenius (1592-1670) and his depiction of lenses and spectacles in the first children's picture book. *Hindsight Journal of Optometry History*, 40(1), pp. 25-28.

GOV.UK, 2020. *Cyber Resilience*. [Online] Available at: <https://www.gov.uk/government/collections/cyber-resilience>

Groenendal, J. & Helsloot, I., 2021. Cyber Resilience during the COVID-19 Pandemic crisis: A case study. *Journal of Contingencies and Crisis Management*, 29(4), pp. 439-444.

- Groenendal, J. & Helsloot, I., 2021. Cyber Resilience during the COVID-19 Pandemic crisis: A case study. *Journal of Contingencies and Crisis Management*, 29(4), pp. 439-444.
- Haimes, Y. Y., 2009. On the Definition of Resilience in Systems. *Risk Analysis*, 29(4), pp. 498-501.
- Haque, M. A., Teyou, G. K. D., Shetty, S. & Krishnappa, B., 2018. *Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics and Insights*. Miami, IEEE, pp. 25-30.
- Hassell, S. et al., 2012. *Evaluating network cyber resiliency methods using cyber threat, Vulnerability and Defense Modeling and Simulation*. Orlando, IEEE, pp. 1-6.
- Heeks, R. & Ospina, A., 2018. Conceptualising the link between information systems and resilience: a developing country field study. *Information Systems Journal*, 29(1), p. 70–96..
- Holling, C. S., 1973. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4(1), pp. 1-23.
- Holling, C. S., 1996. Engineering Resilience versus Ecological Resilience. In: P. Shultz, ed. *Engineering with ecological constraints*. Washington: National Academies Press, p. 32.
- Hollnagel, E., 2015. *Introduction to the Resiliency Analysis Grid (RAG)*. [Online] Available at: <https://www.erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf> [Accessed 2021].
- Hollnagel, E., Hounsgaard, J. & Colliga, L., 2014. *FRAM-the Functional Resonance Analysis Method: a handbook for the practical use of the method*. Southern Denmark: Centre for Quality.
- Hollnagel, E., Paries, J., Woods, D. & Wreathall, J., 2011. *Resilience Engineering Perspectives Volume 3: Resilience Engineering in Practice*. 1 ed. Farnham: Ashgate Publishing Limited.
- Hollnagel, E., Woods, D. D. & Leveson, N. C., 2006. *Resilience engineering: Concepts and precepts*. 1 ed. Aldershot, UK: Ashgate Publishing Limited.
- Hotz, R. L., 1999. *Mars Probe Lost Due to Simple Math Error*. [Online] Available at: <https://www.latimes.com/archives/la-xpm-1999-oct-01-mn-17288-story.html> [Accessed 30 1 2021].
- Imran, B., Khan, S. J. & Qazi, I. A., 2016. Removal and recovery of sodium hydroxide (NaOH) from industrial wastewater by two-stage diffusion dialysis (DD) and electro dialysis (ED) processes. *Desalination and Water Treatment*, 57(17), pp. 7926-7932.
- INCOSE Resilient Systems Working Group, 2020. *Annual Incose International Workshop 2020*. Torrance USA, Incose.org.

International Electrotechnical Commission (IEC), 2021. *Understanding IEC 62443*. [Online] Available at: <https://www.iec.ch/blog/understanding-iec-62443> [Accessed 2022].

International Society of Automation (ISA), 2020. *ISA/IEC 62443 Series of Standards*. [Online] Available at: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> [Accessed 22 September 2022].

IRRIIS, 2006. *Integrated risk reduction of information-based infrastructure systems*. [Online] Available at: <https://cordis.europa.eu/project/id/027568> [Accessed 07th January 2023].

ISA, 2020. *Cyber-security Fundamentals*. [Online] Available at: [http://www.isaca.org/knowledgecenter/documents/glossary/cyber-security\\_fundamentals\\_glossary.pdf](http://www.isaca.org/knowledgecenter/documents/glossary/cyber-security_fundamentals_glossary.pdf) [Accessed 15 Jan 2021].

Jackson, S. & Ferris, T., 2016. *Proactive and Reactive Resilience: A Comparison of Perspectives*. South Australia: Insight Magazine of the International Council on Systems Engineering.

Jacobs, N., Hossain-McKenzie, S. & Vugrin, E., 2018. *Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example*. USA: Sandia National Laboratories.

Janbu, A. F., 2009. *Treatment of uncertainties in reliability assessment of safety instrumented systems*. Trondheim: Norwegian University of Science and Technology.

Johnson, C., 2016. *Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems*. Brighton, Safety-Critical Systems Club, pp. 171-182.

Kagermann, H., Wahlster, W. & Helbig, J., 2013. *Recommendations for implementing the strategic initiative Industrie 4.0 – Final report of the Industrie 4.0 Working Group*, Berlin, Germany: Forschungsunion.

Kaspersky, 2018. *Threat Landscape for Industrial Automation Systems for H1 2018*. [Online] [Accessed 29 July 2019].

Keys, B. & Shapiro, S., 2019. Frameworks and Best Practices. In: A. Kott & I. Linkov, eds. *Cyber Resilience of Systems and Networks*. New York, NY: Springer International Publishing, pp. 381-401.

Kott, A. & Abdelzaher, T., 2014. Resiliency and robustness of complex systems and networks.. *Adaptive Dynamic and Resilient Systems*, Volume 67, pp. 67-86.

- Kott, A. & Linkov, I., 2019. *Cyber Resilience of Systems and Networks*. 1st ed. Cham: Springer.
- Kott, A. & Linkov, I., 2021. To Improve Cyber Resilience, Measure It. *Computer*, Feb, 54(2), pp. 80-85.
- Leandros, A. & Maglaras, K., 2018. Cyber Security of Critical Infrastructures. *IEEE*.
- Levenson, E., 2021. *Florida water hack highlights risks of remote access work without proper security*. [Online]  
Available at: <https://edition.cnn.com/2021/02/13/us/florida-hack-remote-access/index.html>  
[Accessed 18th July 2021].
- Leversage, D. & Byres, E., 2008. *Estimating a system's mean time-to-compromise*. s.l.:IEEE Security Privacy.
- Leversage, D. J. & Byres, E. J., 2008. Estimating a system's mean time-to-compromise. *IEEE Security and Privacy*, 1 1, pp. 52-60.
- Leveson, N., 2011. *Engineering A Safer World*. 1st ed. London: MIT Press.
- Leveson, N., 2020. An Improved Design Process for Complex, Control-Based Systems Using STPA and a Conceptual Architecture. *Engineering Systems Lab, Aeronautics and Astronautics Dept.*.
- Leveson, N., 2020. Safety III: A Systems Approach to Safety and Resilience. *MIT ENGINEERING SYSTEMS LAB*, 07 01.
- Leveson, N. G., 2009. The need for new paradigms in safety engineering.. *Safety-critical systems: Problems, process and practice.* , pp. 3-20.
- Leveson, N. G., 2017. Rasmussen's legacy: A paradigm change in engineering for safety.. *Applied Ergonomics.*, Volume 59, pp. 581-591.
- Ligo, A., Kott, A. & Linkov, I., 2021. *How to Measure Cyber Resilience of an Autonomous Agent: Approaches and Challenges*. Paris, AICA 202.
- Linkov & Eisenberg, e. a., 2013. Measurable Resilience for actionable policy. *Environmental Science and Technology*, September, Volume 47, pp. 10108-10110.
- Linkov, I., Bridges, T. & Creutzig, F., 2014. *Changing the resilience paradigm*. s.l.:Nature Climate Change.
- Linkov, I. et al., 2014. Changing the resilience paradigm. *Nature Climate Change*, 4(1), pp. 407-409.

- Linkov, I. et al., 2013. Resilience metrics for cyber systems. *Environment Systems and Decisions*, Nov, 33(1), pp. 471-476.
- Linkov, I., Eisenberg, D., Plourde, K. & Seager, T. P., 2013. Resilience Metrics for Cyber Systems. In: *Environmental Systems and Decisions*. USA: s.n., pp. 471-476.
- Linkov, I. & Kott, A., 2018. *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. Cyber Resilience of Systems and Networks ed. USA: Springer.
- Linkov, I. & Kott, A., 2018. Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: I. Linkov & A. Kott, eds. *Cyber Resilience of Systems and Networks*. Cham: Springer, pp. 1-25.
- Li, T., Feng, C. & Hankin, C., 2020. Scalable Approach to Enhancing ICS Resilience. *MaxSAT Evaluation 2019 (affiliated with SAT 2019)*, pp. 32-33.
- M. A. Haque, G. K. De Teyou, Shetty, S. & B. Krishnappa, 2018. Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics and Insights. In: *IEEE International Conference on Intelligence and Security Informatics (ISI)*. s.l.:IEEE, pp. 25-30.
- M. McEvilley, M. W., 2022. *Functionally Interpreting Security*. s.l.:Wiley Online Publishing.
- Ma'ayan, A., 2017. Complex Systems Biology. *Journal of the Royal Society Interface*, 14(134).
- Magee, C. & De Weck, O., 2004. Complex System Classification. *INCOSE International Symposium*, Volume 14.
- Maglaras, L. A. et al., 2018. Cyber security of critical infrastructures. *ICT Express*, 4(1), pp. 42-45.
- Maglaras, L. A. et al., 2018. Cyber security of critical infrastructures. *Ict Express*, 4(1), pp. 42-45.
- Manyena, S. B., 2006. The concept of resilience revisited. *Disasters*, December.30(4).
- Manyena, S. B., 2006. The concept of resilience revisited. *Disasters*, 30(4), pp. 434-450.
- Meloeny, S., 2022. *What is Industry 4.0?* [Online] Available at: <https://www.calsoft.com/what-is-industry-4-0/> [Accessed 2023 July 2023].
- Merton, R. K., 1936. The Unanticipated Consequences of Purposive Social Action. *American Sociological Review*, 1(6), pp. 894-904.
- Meyer, R. & Kunreuther, H., 2017. The Ostrich Paradox: Why we underprepare for disasters. *University of Pennsylvania Press*, 07th February.

Michael. A. McEvelley, M. W., 2022. *Functionally Interpreting Security*, USA: INCOSE - Wiley Online Library - <https://doi.org/10.1002/inst.12380>.

Min, H.-S. J., Beyeler, W., Brown, T. & Son , Y. J., 2007. Toward modeling and simulation of critical national infrastructure interdependencies. Jan, 39(1), pp. 57-71.

Mitre Corp., 2012. *Cyber Resiliency Metrics, Measures of Effectiveness and Scoring*, Bedford, MA: Mitre Corporation, Department No. T8A2.

MITRE, 2017. *ATT&CK Matrix for Enterprise*. [Online] Available at: <https://attack.mitre.org> [Accessed 15th Jan 2021].

Moore, T. J. & Cho, J.-H., 2019. Applying Percolation Theory. In: A. Kott & I. Linkov, eds. *Cyber Resilience of Systems and Networks*. Basel: Springer International Publishing, pp. 107-133.

Mthunzi, S. N., Benkhelifa, E., Bosakowski, T. & Hariri, S., 2019. A Bio-inspired Approach To Cyber Security. In: Q. Z. S. Brij B. Gupta, ed. *Machine Learning for Computer and Cyber Security*. 1st Edition ed. Boca Rattan: CRC Press.

National Institute of Standards and Technology, 2012. *Guide for Conducting Risk Assessments*. NIST SP 800-30 Rev 1 ed. Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST SP 800-53 ed. Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2014. *Framework for Improving Critical Infrastructure Cyber-security (Version 1.0)*, Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cyber-security*, Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cyber-security (Version 1.1)*, Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST SP 800-37 ed. Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2021. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. NIST SP 800-160 ed. Washington, D.C.: U.S. Department of Commerce.

Novak, J. D., 1990. Concept maps and Vee diagrams: Two metacognitive tools to facilitate meaningful learning.. In: s.l.: *Instructional Science*, 19(1), pp. 29-52.

Office of Cyber-security, Energy Security and Emergency Response, 2012. *Cyber-security Capability Maturity Model (C2M2)*. [Online]  
Available at: <https://www.energy.gov/ceser/cyber-security-capability-maturity-model-c2m2>  
[Accessed 1 June 2021].

Office of Cyber-security, Energy Security and Emergency Response, 2012. *Cyber-security Capability Maturity Model (C2M2)*. [Online]  
Available at: <https://www.energy.gov/ceser/cyber-security-capability-maturity-model-c2m2>  
[Accessed 1 June 2021].

OffSec, 2018. *Metasploit Unleashed*. [Online]  
Available at: <https://www.offsec.com/metasploit-unleashed/client-side-exploits/>  
[Accessed 14 4 2022].

Oxford English Dictionary, 2013. *Resilience*. [Online]  
Available at: [www.oed.com](http://www.oed.com)  
[Accessed 30 1 2021].

Patriarca, R., Simone, F. & Di Gravio, G., 2022. Modelling cyber resilience in a water treatment and distribution system. *Reliability Engineering and System Safety*, 09th June, Volume 226, p. 108653.

Perrow, C., 1984. *Normal Accidents; Living with High Risk Technologies*. USA: Basic Books.

PLC Security, 2021. *Secure PLC Coding Practices: Top 20 List*. [Online]  
Available at: [https://www.plc-security.com/content/Top\\_20\\_Secure\\_PLC\\_Coding\\_Practices\\_V1.0.pdf#page17](https://www.plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf#page17)  
[Accessed 09th August 2021].

Rahman, S. et al., 2021. Assessing Cyber Resilience of Additive Manufacturing Supply Chain: data fusion technique. *CIRP Journal*, Volume 35, pp. 911-928.

Ramuhalli, P., Halappanavar, P., Coble, J. & Dixit, M., 2013. Towards a theory of autonomous reconstitution of compromised cyber-systems. In: *2013 IEEE International Conference on Technologies for Homeland Security (HST)* . Greater Boston, Massachusetts: IEEE, pp. 577-583.



- Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. *Safety Science*, Volume 27, pp. 183-213.
- Reeder, J. R. & Hall, T., 2021. Cyber-security's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defence Review*, 1 August, pp. 15-39.
- Reeder, J. R. & Hall, T., 2021. Cyber-security's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defence Review*, 1 August, pp. 15-39.
- Regmedia, 2023. *Reg Media*. [Online] Available at: [https://regmedia.co.uk/2023/06/20/mondelez\\_data\\_breach\\_notification\\_june\\_2023.pdf](https://regmedia.co.uk/2023/06/20/mondelez_data_breach_notification_june_2023.pdf) [Accessed 03rd July 2023].
- Rehmani, M., Akhtar, F., Davy, A. & Jennings, B., 2018. *Achieving Resilience in SDN-Based Smart Grid: A Multi-Armed Bandit Approach*. Montreal, QC, Canada, IEEE, pp. 366-371.
- Rogers, P., 2020. *Connections: The Quarterly*, Volume 3, pp. 13-32.
- Rohit Singh, Shaun T. Hutton, Donahoo, M. J. & Sicker, D., 2021. *Toward Grading Cyber-security & Resilience Posture for Cyber Physical Systems*. s.l.:s.n.
- Ross, R., Graubart, R. & Bodeau, D., 2018. *Systems Security Engineering: NIST*, Washington DC: NIST.
- S. Bologna, A. F. a. M. M., 2013. Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures. In: *Cyber Security*. s.l.:Springer 2013, pp. 57-72.
- Saaty, T., 2008. Reactive measurement and its generalisation in decision making. Why pairwise comparisons are central in mathematics for the measurement of intangible far the analytic hierarchy/network process. *Mathematical Principles of decision making*, Volume 2, pp. 251-318.
- Saaty, T. L., 2009. *Mathematical Principles of Decision Making*. 1st ed. Pittsburgh, PA, USA: RSW Publications.
- Schlaepfer, R., Koch, M. & Merkofer, P., 2015. Industry 4.0. Challenges and Solutions for the Digital Transformation and Use of Exponential Technologies.. *Deloitte*, p. 1–30.
- Scoblic, J. P., 2020. *Learning from the Future: Essays on Uncertainty, Foresight and the Long Term*, USA: Harvard.
- Seligman, M. & Csikszentmihalyi, M., 2000. Positive psychology: an introduction. *Am Psychol*, Volume 55, pp. 5-14.

Sikula, N., Mancillas, J., Linkov, I. & McDonagh, J., 2015. Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments'. *Environment Systems & Decisions*, 35(2), pp. 219-228.

Simonovich, L., 2020. *Thriving in a Digitized Environment*. [Online] Available at: <https://www.securitymagazine.com/articles/93849-leo-simonovich-thriving-in-a-digitized-environment>

[Accessed 1 October 2021].

Singh, R., Hutton, S. T., Donahoo, M. J. & Sicker, D., 2021. *Toward Grading Cyber-security & Resilience Posture for Cyber Physical Systems*. McKinney, TX, Elsevier.

Smith, S. C., 2023. Towards a Scientific Definition of Cyber Resilience. In: R. L. Wilson & B. Curran, eds. *International Conference on Cyber Warfare and Security*. Baltimore County, Maryland, USA: Academic Conferences International Limited, pp. 379-386.

Stoddart, K. et al., 2016. *Forensic Readiness for SCADA/ICS Incident Response*. UK, BCS.

Sugden, A. M., 2001. Resistance and resilience. *Science*, Volume 293.

Syrmakesis, A., Alcaraz, C. & Hatziaargyriou, N., 2022. Classifying Resilience approaches for protecting smart grids against cyber threats. *International Journal of Information Security*, Volume 21, pp. 1189-1210.

T3l3machus, 2022. *Villain*. [Online] Available at: <https://github.com/t3l3machus/Villain> [Accessed 23rd November 2022].

Tasan-Kok, T., Stead, D. & Lu, P., 2013. Conceptual overview of resilience: history and context. In: T. T. Eraydin A, ed. *Resilience Thinking in Urban Planning*. New York: Springer, p. 39–51.

Tedim, F. & Leone, V., 2017. Enhancing resilience to wildfire disasters; from 'the war against fire' to coexist with fire'. Disaster Resilience: An integrated approach. In: D. Paton & D. Johnston, eds. *Disaster resilience: an integrated approach*. Springfield, USA: Charles C Thomas Pub Ltd, pp. 233-263.

Thales Group, 2020. s.l.:s.n.

Theron, P., 2013. ICT Resilience as Dynamic Process and Cumulative Aptitude. In: P. Theron, Bologna & Sandro, eds. *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. Hershey, Pennsylvania: IGI Global, pp. 1-35.

Tusher, H. et al., 2022. Cyber Security Risk Assessment in autonomous shipping. *Maritime economics & logistics*, January, 24(2), pp. 208-227.

TUVSUD, 2022. *Functional Safety ISO-13849 - IEC-62061*. [Online] Available at: <https://www.tuvsud.com/en-us/services/functional-safety/iso-13849-iec-62061> [Accessed 24th Jan 2023].

Vescuso, P., 2022. *Manufacturing Leadership Council*. [Online] Available at: <https://www.manufacturingleadershipcouncil.com/manufacturing-tops-industrial-ransomware-hit-list-in-2021-26932/> [Accessed 23rd July 2022].

Volos, C., Akgul, A. & Pham, V., 2017. A simple chaotic circuit with a hyperbolic sine function and its use in a sound encryption scheme. *Nonlinear Dynamics*, Volume 89, p. 1047–1061.

Walker, B., Holling, C., Carpenter, S. & Kinzig, A., 2004. Resilience, adaptability and transformability in social–ecological systems. *Ecology and Society*, 9(2), p. 5.

Walser, A., 2023. *FBI and former city manager say Oldsmar cyberattack never happened*. [Online] Available at: <https://www.abcactionnews.com/news/local-news/i-team-investigates/fbi-and-former-city-manager-say-oldsmar-cyberattack-never-happened> [Accessed 01st May 2023].

Watkins, L. & Hurley, J., 2015. Cyber Maturity as measured by scientific risk-based metrics. *Journal of Information Warfare*, Volume 14, p. 384.

Wei, D. & Ji, K., 2010. Resilient industrial control system (RICS): Concepts, formulation, metrics and insights. In: *2010 3rd international symposium on resilient control systems*. Idaho Falls: IEEE, pp. 15-22.

Westrum, R., 2006. A Typology of Resilience Situations Resilience Engineering: An Integrative Review of Fundamental Concepts and Directions for Future Research in Safety Management. *Open Journal of Safety Science and Technology*, 7(4), pp. 55-66.

Wilamowski, G. C., Dever, J. R. & Stuban, S. M., 2017. Using AHP to create cyber security metrics. *Resilience Metrics formulation using AHP*, Volume 24.

Williams, T., 1992. *The Purdue Enterprise Reference Architecture, A Technical Guide for CIM Planning and Implementation I*. First ed. Research Triangle: Instrument Society of America.

Wordsworth, D., 2014. *Why does everything suddenly need ‘resilience’? Schoolchildren, flood defences, press regulators... it's time to resilie*. [Online]

Available at: <https://www.spectator.co.uk/article/why-does-everything-suddenly-need-resilience/>  
[Accessed 20th June 2022].

World Economic Forum, 2022. *World Economic Forum - Risk and Resilience 2022 agenda*. [Online]  
Available at: <https://www.weforum.org/agenda/2022/07/how-organizations-accelerate-resilience-journey/>  
[Accessed 15th August 2022].

Xu, Y. et al., 2023. Physics-informed machine learning for reliability and systems safety applications: State of the art and challenges. *Reliability Engineering & System Safety*, Volume 230, p. 108900.

Yi, C. & Jackson, N., 2021. A review of measuring ecosystem resilience to disturbance. *Environmental Research*, 14th May, 16(5), p. 053008.

Young, W. & Leveson, N., 2013. Systems thinking for safety and security. In: *29th Annual Computer Security Applications Conference*. New Orleans, Louisiana, USA: ACM, pp. 1-8.

Zhu, Q., Wei, D. & Ji, K., 2016. Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics and Design Principles. In: *Cyber Security for Industrial Control Systems*. Boca Raton, Florida: CRC Press, pp. 161-192.

# Appendix 1

## Case Study Framework

The following sections provide an overview of the requirements defined in the IEC 62443-2-1 standard and was adopted during the case study analysis.

### Reference Explanations for IEC 62443-2-1 Requirements

#### **ORG 1 – Security Related Organisation and Policies**

- Coordination between stakeholders

An effective CS program formalises the company's CS commitments and strategic goals at a senior level, communicates what is expected of all employees and empowers them to contribute toward achieving the desired state. It consists of a documented risk identification and risk assessment process and defined controls, including governance (e.g., policies and procedures) and technical measures, to address the risks identified.

IT security is often well defined but can have different business priorities and functional requirements to OT. For an OT focussed security program to be successful it must coordinate with applicable IT security elements and involve cooperation between different stakeholders (e.g., IT, OT, procurement and safety) around the company to identify and address security risk, particularly where there are interconnections and interdependencies.

- Background Checks

Insider threat can be a significant operational risk, vetting can help reduce this risk. The nature of the business and the industry it operates in is a contributing factor. Examples may include malicious actions by disgruntled employees, corporate espionage (i.e., intellectual property theft) and sabotage (i.e., compromise of production or product integrity).

- Roles and Responsibilities

Establishing security roles and points of contact are a key to an effective OT security program. Where this is not clearly defined, it can hinder detection, response and recovery from cyber

incidents. It may cause confusion between business IT and process OT stakeholders and can undermine the open CS culture that is essential to encourage reporting of suspicious or potentially dangerous occurrences.

- Security Training

CS is a complex area and is not necessarily intuitive, even for engineers and technically experienced operators. Security risks in computerised systems are not always immediately obvious in the way that other risks might be, e.g., safety defects. Likewise, IT professionals typically have a good understanding of the CS but are less likely to understand the functional characteristics of specialised OT processes.

Appropriate general awareness training for all personnel who work with OT systems and specialist training for key security roles and responsibilities builds an understanding of cyber risk and informs stakeholders how their actions help manage that risk. This helps reduce inconsistencies or failures in the design, integration and operation of IT and OT systems, as well as in implementing and adhering to risk reduction controls that might otherwise interfere with correct function and leave systems vulnerable to compromise.

- Supply Chain

Knowing the provenance of assets, how they are supported and to what extent, is essential in managing their security and operational lifecycle. OT systems may have a single supplier or be integrated using components from multiple suppliers. Suppliers will also have their own suppliers and sub-contractors. Suppliers can also be third party service providers to whom a particular function is outsourced. Every supplier has the potential to affect OT CS. Organisations must understand their supply chain, assess the risk it may pose to OT security and communicate clearly defined contractual security requirements and expectations to their suppliers.

## **ORG 2 – Security Assessments and Reviews**

Effective CS is not achieved overnight, nor is it an ‘all or nothing’ proposition. Threats, like safety hazards, represent a potential for harm to the company’s people, assets, reputation and to the environment. The company must assess those risks, establish what level of risk is tolerable and implement controls to control the risk to that level.

Quantitative assessment of likelihood can be difficult for cyber threats. Cyber risk assessment will often be qualitative, identifying the applicability and severity of threats (i.e., ‘could this affect us?’ and ‘how bad would the anticipated outcome be for us?’). The severity should consider quantitative

factors (e.g., lost revenue and cost to recover). The business can then identify where controls are required to reduce risk to an acceptable level and justify where investment is required.

The risk management approach must be formalised and documented to ensure it is objective and repeatable. The organisation may develop a bespoke framework for risk management or implement a generic or cyber specific standard methodology including ISO 27005, Octave Allegro, ISA/IEC 62443-3-2 or STPA (Leveson, 2011).

The core principle of robust CS defences is one of *defence in depth*, i.e., the coordinated implementation of multiple complementary controls covering different threats, addressing vulnerabilities and reducing risk. Failure to coordinate controls leaves gaps where significant risks are not addressed. This will reduce the efficacy of the controls that are implemented.

Security management is not static. To be effective it must be applied continually throughout the lifecycle of systems and assets from design, into operation and through to decommissioning. All elements of the security program, including governance, risk assessment and applied controls, need to be periodically reviewed and updated where needed.

During development, components, their functions and characteristics should be tested against security requirements before they are integrated into production systems. Testing provides assurance that components will not disrupt system operation, introduce vulnerabilities, or reduce the efficacy of existing security controls. Vendor 'secure by design' certifications can help when selecting a product, but these products can still be integrated and operated in ways that are not secure.

In-service monitoring for security anomalies to help assess the adequacy of applied security controls is vital. Security anomalies are when the configuration or behaviour of the OT system deviates from designed and documented norms. It is important that these anomalies are identified and investigated as they may indicate deficiencies with current security controls.

### **ORG 3 – Security of Physical Access**

Physical access to systems and equipment can overcome many logical security controls so controlling this access is important. A variety of controls may be part of a physical access strategy including fences, guards, ID badges, locked doors, cameras and conduits to enclose and protect cabling related to critical functions.

Effective physical access controls are balanced provide a robust deterrent to unauthorised persons but enable authorised access with minimum disruption. Where practicable, both authorised and

unauthorised access attempts should be identified and recorded, particularly to critical and sensitive areas.

- CM1.a – Documentation

Accurate suitably detailed asset inventory and documentation are one of the most crucial parts of a security strategy. Without knowing what components should be present, how they function and their configuration, operators would face an impossible task to maintain them and identify security deficiencies. The implementation of most technical security controls is also highly dependent on the accuracy of these records.

Meeting this requirement requires that records be complete and continually reviewed and updated to ensure accuracy. The complex characteristics of CS risk mean that the same type of asset may have exhibit different risk when used in different ways. Differences in hardware and software, including versions of firmware or installed programs is also a factor in determining exposure to security vulnerabilities. The asset inventory must be appropriately detailed to consider these characteristics.

- CM1.b – Configuration and Change Management

Managing configuration of systems and assets is an important factor in maintaining a robust CS posture. It also contributes to maintaining the integrity and correct operation of OT processes, which can be affected by unauthorised or unplanned changes.

Maintaining a record of the correct and approved configuration for all devices and software supports the ability to recover in the event of a fault, failure, or incident and acts as a basis for comparison to enable the identification of unauthorised changes.

Changes should only be permitted via a formal management of change (MoC) process. This process must consider CS implications of a change (e.g., addition or removal of assets, change of configuration, installing new or updated software). have potential to reduce the overall security posture. Effective change control is a fundamental control that integrates with and informs other requirements in the standard. The change process should: require approval and oversight by designated responsible persons, trigger the updating of records including documentation and drawings and monitor process performance by detecting and investigate unauthorised / unscheduled changes.

## **NET 1 – System Segmentation**

- OT and non-OT network boundary control



Connections between OT and non-OT networks and their devices can be a significant OT CS risk. This includes business IT networks, third-party networks, remote connections and the Internet, which should be considered less trusted from the perspective of OT. Communications with less trusted networks is a prominent threat vector by which OT systems are compromised and every data flow permitted can increase the risk.

This risk is controlled by limiting communication between networks and assets on different sides of this boundary, enforcing restrictions that permit only the minimum communication identified as legitimately required for correct operation of the OT process. This is commonly achieved utilising network security devices (gateways, firewalls and proxy servers) featuring a 'default deny' policy and specific rules permitting required traffic.

- Documentation of Networks

Maintaining accurate documentation of the network architecture including how and where devices are configured is important for the same reasons as those relating to asset inventory. Additionally, a detailed understanding of the network topology is a key step underpinning the implementation of the IEC 62443 'zones and conduits' approach. This involves identifying boundaries (e.g., based on location, function, ownership, trust, or a combination) and defining controls to restrict communication flows to the minimum required for correct function of the system. Documentation must be maintained to ensure it reflects the reality of the network 'as fitted' and not just the 'as designed' or 'as built' architecture.

It is vital that the identification, documentation and risk assessment of interconnections between assets is undertaken across all OT networks and assets to ensure the OT process is fully understood.

- Safety System Network Communications

Safety systems are responsible for detecting and preventing dangerous occurrences in a process that could result in physical damage or harm to people or the environment. IEC 61508 and IEC 61511 are the industry standards applicable to functional safety. In these standards systems, components and functions are defined as either 'Safety Instrumented Systems' (SIS) or 'Basic Process Control Systems' (BPCS). Safety systems can be independent or integrated / combined. Unless safety critical functions have been completely engineered out of the process, IEC 62443-2-1 requires that safety systems connected to OT process systems have controls in place to prevent interference with safety critical functions.

- External Networks and Dependencies

Some functions of OT processes may be dependent on external network services (e.g., a cloud hosted ERP system). However, there can be instances when OT processes are isolated from external networks, for example because of fault/failure, or as a protective measure when a cyber incident occurs. Operators need to identify the desired behaviour of the OT process in this eventuality and if continued independent operation is required, take steps to identify and document interdependencies that impede this. Best practice guidance in the standard is that essential functions must continue to operate at a minimum, if only in a degraded or less-optimised way. Manual control may be acceptable if sufficient documentation and operator training is in place to support it. To support cyber incident response and maintenance activity, a documented procedure should detail why, when and how the OT process can be disconnected intentionally from external networks and the functional implications.

- Internal OT Network Segmentation

Many legacy OT systems use a 'flat' network where all devices occupy a single segment and can communicate with little or no restrictions. Segmentation refers to techniques that limit the flow of network traffic between networks and devices. The IEC 62443 'zones and conduits' approach is an effective way to implement segmentation whereby the network is segmented into zones containing assets. Zones can be based on various criteria, both physical and logical, e.g., location, device type (e.g., PLC), process area (e.g., Production Line 1) and function (e.g., process and safety). Conduits define the communication required between those zones and devices.

With this structure in place, controls can be applied to limit communication between zones and devices to the minimum communication necessary correct operation of the OT process. Network segmentation is often achieved by dividing OT systems into multiple networks (physical or virtual) connected by a firewall. Dual homing of edge devices in different zones should be avoided. Where trust can be reliably verified at device level, cryptographic controls on communications may be sufficient (e.g., authentication and integrity checks). However, all controls must remain effective in cases where previously trusted devices generate unauthorised traffic, for example in the case of a malware infection.

- Identify Connected Devices

It is important that mechanisms be in place to detect and identify undocumented or unauthorised devices that are connected to OT networks. Every connected device contributes to the overall system-level attack surface (i.e., the sum of potential points that an attacker can target). It is unlikely that undocumented legitimate assets will benefit from regular maintenance, meaning they

will gradually become more outdated and vulnerable. Unauthorised devices are a significant security risk, whether intentionally or accidentally, they can provide a foothold for malicious actors and may bypass other security controls designed into the system.

Network segmentation within OT (e.g., with firewalls) typically only applies at the boundary between zones formed of different network segments and may not have visibility over all devices and communications within the zones. The most effective device discovery approach combines continual automated network-based checks with a program of periodic manual inspections of physical equipment locations. Network access control (NAC) and similar solutions can be highly effective, they provide the ability to deny connectivity to unidentified devices but can be difficult to design and configure to minimise unintentional disruption and impose a technical burden for ongoing maintenance.

- Protect Network Accessible Services

All services or functions enabled on OT devices that are accessible over the network need to be protected from unauthorised access. The most common methods of achieving using IPsec or TLS protocol suites to provide authentication, integrity, confidentiality and anti-replay protection for payload data. TLS is increasingly prevalent and applies to many modern industrial control protocols (e.g., OPC UA and Secure-CIP). The use of network services and protocols without authentication or with plaintext authentication should be avoided. Where insecure services or protocols are necessary (e.g., HTTP, FTP, Modbus TCP), additional controls should be used to augment their security, at a minimum the use of a firewall or access control list.

- Segregate OT and Non-OT Data Business Functions and Data

It is desirable for OT devices to be dedicated to supporting OT systems, functions and data. OT servers and operator workstations should not be used for general business activity (e.g., web browsing, user messaging and email) as this significantly increases the risk of compromise by malware and other threats.

As per NET 1.a, IT and OT functions and data should not share the same internal network segments. Instead, separate networks should be used. With correct configuration, it can be practical for the same physical infrastructure (e.g., network switches) to support both IT and OT services, however OT data should use separate dedicated logical network (e.g., VLANs).

- Network Time

In some processes, precise time may be a crucial component for operational, safety, or health reasons. Examples include the synchronisation of electrical grids and radio communications protocols and the recording of manufacturing data for products such as foods, beverages and pharmaceuticals. Accurate time synchronisation across the system is important even when time precision is not crucial to the production process.

Time stamping of logs across discrete system assets is an important to support operational and security incident investigation by allowing correlation of events from different devices. Where systems include Microsoft Active Directory domains, domain members can only communicate correctly and securely when they are synchronised to a common time source. Trusted servers should distribute time, use a protocol offering protection against tampering wherever possible.

### **NET 2 – Secure Wireless Networks**

Wireless networks cover a diverse range of radio frequency protocols including 802.11 Wi-Fi, Bluetooth, ZigBee, LP-WAN, line-of-sight microwave and proprietary radio protocols. The nature of wireless networks means they can allow access to systems from beyond the physical boundaries of a site. This means that sensitive data transmitted wirelessly may be leaked if it is not protected with encryption. Wireless communications are also more susceptible to interference, both unintentional and malicious, which can result in a denial of service unless the data has authentication, integrity and anti-replay protection mechanisms.

Rogue Wi-Fi access points can also pose a risk of compromise to OT systems. This is when unauthorised wireless access points are connected to OT networks. They may be installed by a staff member looking to make their work easier but without an appreciation of the risks, or by a motivated attacker with physical access to provide a means for future covert network access.

Where 802.11 Wi-Fi networks are used, the most secure method is EAP-TLS mutual authentication where both the network and the client authenticate one another using digital certificates. Physical layer precautions for protecting wireless transceivers can including surveying site wireless propagation characteristics and the tuning transmitter power to limit the physical range to the minimum required for correct operation.

### **NET 3 – Secure Remote Access**

All connections into OT systems can be a security risk. Connections originating externally (i.e., from the Internet), especially by third parties, carry particularly high potential for harm and there are numerous documented cases of remote access technologies being exploited to gain unauthorised

OT access. Solutions from popular reputable vendors can become vulnerable and insecure unless the operator regularly maintains it.

Many different technologies can provide remote access to OT systems and some have more effective security controls than others. The general minimum good practice is that:

- a company approved standard solution is used;
- the solution is controlled by the company and maintained/updated by the vendor;
- the credentials for access are linked to named individuals;
- multi-factor authentication is used (e.g., username, password and one-time code);
- connections and activity are logged;
- once connected, network access is limited to the minimum required;
- connections for third parties are enabled only when required for approved activity.

### **COMP 1 – Devices and Media**

Every device has an individual attack surface, the number of ways it is potentially vulnerable to attack or compromise typically increases as more features are enabled such as the number of network ports or the protocols and connections that are permitted. Device hardening is a process that reduces the attack surface to a minimum by removing or disabling unnecessary and unused features and/or installed software.

Components certified 'secure by design' typically disable potentially insecure features and behaviour by default, but this does not mean they cannot be enabled when integrated into the system. Best practice is to maintain a standard baseline configuration template for commonly deployed device families. However, the attack surface of an asset will increase when security vulnerabilities are discovered in enabled features or installed software. It can also be degraded by maintenance activities. Regular review is necessary to ensure the device remains hardened over time.

Portable media connections are sometimes necessary but are a threat. Portable media can be easily moved and used between different systems including those not controlled by the organisation. There is a risk that portable media may be infected with malware on one computer and then spread that infection to another computer. This threat vector can result in compromise of systems even where network-based security controls are well designed. USB drives are the near ubiquitous portable storage media today, but other older types of portable media including optical and magnetic disks can still be a threat. Standard USB flash drives can be susceptible to malicious modification of the firmware, programming them to interfere with the connected system. This type

of modification can be harder to detect and is not resolved by formatting the drive. The most effective control is for organisations to restrict portable media use only to specific situations where it is necessary and to use dedicated media owned and catalogued by them.

## **COMP 2 – Malware Protection**

Malware protection is a control that helps to prevent compromise of the system by malicious software which could occur from infected downloads or by connection of infected devices or portable media. Traditional anti-virus relies heavily on signatures to identify known malware variants. This is unlikely to offer a high degree of protection against rapidly changing malware and ransomware developed today. The most effective solutions combine the traditional signature-based detection with monitoring of the system for suspicious and high-risk behaviour indicative of malware or ransomware infection.

Other mechanisms that may be used for malware protection include verification of authenticity with digital signatures (aka 'whitelisting'). However, this approach effectively outsources the designation of trust to the software publisher and may not be desirable as the sole method of protection.

Anti-malware should be continually monitored and regularly reviewed to ensure protective features are operating correctly. Although the use of malware prevention technologies that do not rely solely on regular signature updates to remain effective is recommended, updates are still important. Solution vendors continually update their detection processes in response to the latest malware and ransomware variants they encounter to provide the maximum level of protection.

As with all changes, malware protection software updates carry a potential to disrupt OT assets and processes due to incompatibility with some devices and software. This is typically more problematic for legacy software. Current versions from reputable OT vendors who follow best practice software coding practices are less likely to be affected. However, it may still be prudent to test and deploy updates in stages to production environments. Care is required to ensure this process occurs in a timely fashion that does not introduce intolerable risk from outdated protection.

Not all devices used in OT systems support malware protection mechanisms. These devices should be documented and alternative controls applied to reduce the level of risk where appropriate. It is also advisable that removable devices (e.g., USB drives) and newly supplied or third-party managed devices should be tested for malware using a stand-alone malware scanner (aka 'sheep dip') before being connected to OT networks and systems.

### **COMP 3 – Patch Management**

Updates are an important aspect of CS management. Typically, software vulnerabilities can only be resolved fully by applying a security update or ‘patch’ from the vendor. However, patching is also a contentious topic in OT and may be avoided over concerns of disruption to the function or reliability of OT processes. The operator should have a defined process for managing updates. Even if their policy is to carry the risk by not applying patches (or applying alternative controls), they should document their exposure to known vulnerabilities.

Vendors typically test their updates prior to release; however, this may occur in isolation and only consider incompatibilities or regression relating to their own products. Updates from one vendor (e.g., operating system or anti-malware products) may not be compatible with OT process software (e.g., SCADA products).

Updates should be tested for compatibility with the organisation’s production system configuration, prior to being deployed on live production systems. Major OT software vendors will test their products with the latest updates from Microsoft and provide a list of those they have verified as being compatible. Unless a managed support contract is in place from an OT system vendor, it will be necessary for the process operator to test updates before applying to their system.

Software and software update installers may come from a variety of sources. This is increasingly likely to be the vendor website but may still include optical media and USB drives as part of the process. There is a potential that packages being installed may be malicious or corrupt copies, which could disrupt the OT process. Verification of authenticity and integrity is essential to prevent this.

Software from major vendors will include digital signatures enabling authenticity and integrity to be verified. This may not be the case for all software and is not a complete guarantee because it relies on the vendor’s security, so care must be taken. This requirement also applies to firmware and other low-level updates (e.g., computer BIOS) that may be applied to OT assets including PLCs.

It may not always be possible or practicable to install an update or patch. This may be because incompatibilities are identified, because the vendor has not yet released an update, or because the affected asset is end-of-life (EOL) and no longer supported by the vendor. It may simply be that potential disruption from update application is considered an intolerable business risk.

In all cases, the justification and residual risk must be documented. Wherever possible alternative compensating controls should be identified and implemented if the residual risk is unacceptable.

- DATA1.a – Data Management

There is a common misconception that data management is not relevant to OT processes. OT processes contain many different types of sensitive data that may need to be managed. Data classification is a key part of data management, unclassified data must be managed on a case-by-case basis, which can become an overwhelming task and can lead to mistakes. The operator should have defined governance and processes for data management.

Examples of sensitive OT data requiring classification include:

- communications and commands between operator interfaces and PLCs/controllers
- intellectual property, proprietary information and production recipes
- system documentation e.g., drawings and manuals which could assist a cyber-attacker.
- authentication information, e.g., user databases
- backup data for business continuity and disaster recovery.

Once data has been identified and classified controls are applied to protect it according to its value, critical data is given the most protection. The most crucial operational data in OT systems is usually the configuration and communications of SCADA and PLCs controlling the process, it is vital that this data can be trusted. Data that relates to Safety Instrumented Functions (SIF) that are responsible for detecting and preventing unsafe process states requires particularly robust protection. This must ensure that safety systems and their data are protected from interference and unauthorised modification. CS consideration for safety data should include a failsafe design that halts to a safe default state when inconsistent safety data means in-service safety cannot be maintained.

Other data, such as backups, may not be critical for routine process operation, but becomes vital in the event of a failure to ensure systems can be restored promptly (AVAIL 2). When a cyber incident does occur, then having assurance of availability and integrity of this data is paramount.

The nature and function of different classifications data requires that it remain available for different lengths of time, this is data retention. This is often a business decision, but there may be a legal requirement to maintain an audit trail. Appropriate retention of event logs (EVENT 1.a) is a key requirement enabling cyber incident investigation.

At the end of the retention period when data is no longer required, it is important that sensitive data be securely disposed of. This could be commercial information or intellectual property where disclosure may affect competition and profitability. It can also be technical information that is



useful to a cyber-attacker such as password databases and configuration files. There should be documented procedures for securely erasing sensitive data from OT assets.

- DATA1.b – Cryptographic Technologies

Cryptographic technologies can provide several security functions in systems, including authentication, confidentiality, integrity checks, anti-replay and non-repudiation. However, cryptographic implementation requires careful design and maintenance to be effective, resistant to exploitation and not inadvertently interfere with availability.

Cryptographic functions used should meet commonly regarded acceptable standards (e.g., current NIST and/or FIPS). Deprecated protocols (e.g., SSL and TLS 1.0/1.1) and ciphers (e.g., DES, MD5, SHA-1) should not be used.

Where public key cryptography is used (e.g., TLS with RSA or ECDSA certificates) it should use securely generated private keys with valid PKI certificates with reasonable validity periods that have been issued by and validated against a managed and trusted root certificate authority. Self-signed certificates should not be used because they cannot be easily validated and revoked.

- USER 1 – Identification and Authentication

User accounts and passwords are a common way for users identify themselves for access to assets and systems. In addition to human users, networked devices and other components may need to identify and authenticate themselves to other devices before communications can be established. The organisation should have defined policies, procedures and standards governing the creation of user accounts and granting of access.

Wherever supported, accounts should be created and allocated to named individual users, or specific service or device-to-device functions. If OT system users are not individually identified and authenticated there may be an increased CS risk.

Accounts should be assigned specific roles to suit the organisation's OT process (e.g., operator, supervisor and engineer). Roles should grant the minimum access required for legitimate business activity, the Principle of Least Privilege (PoLP).

Allocation of access rights that are too broad can increase the likelihood of unintentional disruption and makes a cyber incident from malware infection or direct action by a malicious actor more likely to spread throughout the system without check. Granting the minimum permissions to an account or role allows users to carry out their duties without interference but limits the potential for harm

should an account be compromised. Additionally, the legitimate user is less likely to cause accidental damage with limited permissions.

Accounts that are no longer required but have been left active they increase the likelihood that an attacker may use them to gain access to OT systems. Because these accounts are no longer routinely used by legitimate users, their subversion by an attacker is also more likely to go unnoticed.

Multifactor authentication uses additional checks to confirm a user's identity above a simple password. Although not universally available, multifactor authentication is a powerful authentication tool that enhances a security by making it harder for stolen or guessed passwords to be used, whilst not significantly decreasing ease of use for genuine authorised users. MFA should always be enforced on externally accessible services.

User access should be logged and this information should be actively monitored for suspicious activity or confirmed unauthorised access.

- USER 2 – Authorisation and Access Control

The configuration of devices and services should ensure that functions are only accessible to authorised defined user accounts. The use of guest, anonymous and 'everyone' access settings should be avoided. This is particularly important for high privilege level functions, e.g., for administration and maintenance.

The granting of full administrator rights should be minimised and carefully controlled. A computer administrator account may be able to bypass restrictions in process control software (e.g., SCADA) and influence the process without being specifically authorised to do so. This may be inadvertent, (e.g., during maintenance) or an intentional action by a malicious actor.

Routine use of administrative accounts also presents an increased risk that a malware infection may occur. Routinely accessing infected systems with administrative privileges (e.g., domain administrator accounts) increases the likelihood that compromise is spread throughout the OT environment. Routine accounts should have low privileges and be escalated only when required. Delegated administrative accounts are recommended (i.e., not domain administrator).

For particularly high-risk activity (e.g., changing of set-points related to safe operation), organisations may consider adopting a multiple authorisation process requiring two people (e.g., operator and supervisor) to enter their credentials to authorise the change.

- EVENT 1.a – Detection and Logging

Recording of activity and events occurring on OT assets enables the monitoring of performance and helps to identify deviation from normal operating parameters. It is also a key function underpinning the ability to detect and investigate CS incidents.

Many OT processes will have at least basic operational event detection. When combined with physical observations, is sufficient to enable experienced operators and maintainers to identify control system faults and failures, e.g., sensors out-of-range. However, this is not sufficient to enable reliable detection of cyber incidents. Such incidents may affect correct operation of the process, but it may be impossible to identify the root cause as being a cyber incident unless the appropriate security related events are recorded.

Detection of such incidents may also not be immediate; in some cases, an attacker can have a presence in the network for a long time before being detected. Suitably detailed and separately stored archival event data is necessary to establish the nature and extent of compromise in this scenario.

Central collection of event and log data from multiple system components over time allows automated alerting of suspicious occurrences. The correlation of data trends over time also provides improved ability to identify characteristics of more sophisticated cyber incidents and enables effective incident investigation and response once a security problem is detected.

- EVENT 1.b – Incident and Vulnerability Handling

Historically in OT systems, incident management has been limited to fault, failure, or dangerous occurrences pertaining to the physical characteristics of the process (e.g., electrical power loss, mechanical defect and fire).

Investigation and response to identified CS incidents requires a different response. This will require escalation to experienced specialists and will involve different approaches to resolve dependent on the nature of the cyber threat. For example, the response to event detection indicating malware infection may be quite different to that if an event detection indicates an active attacker inside the system.

Organisations should ensure that CS incidents are considered within the Incident Response Plan (IRP) for the OT production process. These plans should consider the cyber threats and incident types and document the standard approach the organisation will take to respond to them. This should also detail key roles, responsibilities and escalation points.

Incident response should aim to determine root cause through forensic investigation. Where investigation identifies a deficiency or vulnerability in the way the system is currently designed, maintained, or operated this should be captured. Captured lessons then feed into a process for continuous improvement re-assess risk and implement changes where required.

- AVAIL 1 – System Availability and Intended Functionality

Organisations should have policies and procedures for restoring operations when they have been disrupted by an incident. Typically, this will be a business continuity plan (BCP) and/or disaster recovery plan (DRP). Historically these plans may not have included OT or may include OT but not consider the specific actions required to recover from a cyber incident.

As with all policies and procedures, BCP/DRP must be regularly reviewed to ensure they remain applicable and effective. This is particularly relevant for cyber threats, which are very dynamic by their nature.

Process disruption can occur because of hardware failures in OT devices and supporting auxiliary and ancillary systems (e.g., power supplies, heating and cooling). Physical failures occur naturally and can be modelled statistically, with an element of probabilistic uncertainty, to measure likelihood. Resilience and redundancy of critical components should be considered in the original design. This is typically achieved using (High Availability) system architectures with resilient sources of power, e.g., UPS.

However, CS incidents can also result in physical failures e.g., by causing operation of devices significantly outside manufacturer specified tolerances. Unlike natural failures, cyber incidents are more likely to result in damage to multiple components of a HA architecture. In this case, the stores holding of sufficient critical spare parts (cold-standby) may be crucial to restoring process operations in a timely fashion.

- AVAIL 2 – Backup / Restore / Archive

Regular backups ensure that OT assets can be quickly recovered to a stable state with minimum disruption and loss of data should an incident occur. The frequency of backups configured by an organisation will depend on how much data loss is tolerable. This is referred to as the recovery point objective (RPO). Depending on the criticality of an asset and its data this may range from hours or minutes to weeks and months.

Backups can also be manually triggered outside of scheduled windows as part of a change control process. For example, backup before a change is made to provide a means to roll back and revert

to the previous state. Backups may be the only means of recovering from a cyber incident, so they require a high degree of protection. Appropriate data protection classification and controls are essential. Generally, accepted good practice for backups includes:

- scheduling backups so they do not disrupt production;
- conducting backups regularly;
- testing the backup once complete to ensure it can be recovered if needed;
- checking backup integrity and availability continually for online backups (i.e., backup server) and periodically for offline backups (i.e., removable disks or tapes);
- protecting backup data from unauthorised access and from any modification (i.e., 'write once').

The process of correctly restoring a backup should be clearly documented so it can be followed successfully by staff when required. It is advisable to test the process periodically as part of incident response and business continuity exercises to ensure the process works and that familiar with it.

# Appendix 2

## Testbed PLC Configuration

Configuration of the PLC can be seen in Appendix 1 and was generated within RSLogix showing the details of the programs function through ladder logic programming techniques. The code contained within 'LAD 8' is specifically related to the Industrial process depicted on the HMI. It is the PLC tags & variables within LAD 8 that the HMI is interacting with to provide the process feedback to the operator.



<b>Processor Type: Bul.1763    MicroLogix 1100 Series B</b>		
Processor Name: THA0766		
Total Memory Used: 436 Instruction Words Used - 224 Data Table Words Used		
Total Memory Left: 6220 Instruction Words Left		
Program Files: Data Files: 12 Program ID: b3f3		
I/O Configuration		
0	Bul.1763	MicroLogix 1100 Series B

1	1762-IF2OF2	Analog 2 Chan. Input, 2 Chan. Output			
Channel Configuration					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex Edit Resource/Owner Timeout: 60					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex Passthrough Link ID: 1					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex Write Protected: No					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex Comms Servicing Selection: Yes					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex Message Servicing Selection: Yes					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex 1st AWA Append Character: \d					
CHANNEL 0 (SYSTEM) - Driver: DF1 Full Duplex 2nd AWA Append Character: \a					
Source ID: 1 (decimal)					
Baud: 19200					
Parity: NONE					
Control Line: No Handshaking					
Error Detection: CRC					
Embedded Responses: Auto Detect					
Duplicate Packet Detect: Yes					
ACK Timeout(x20ms): 50					
NAK Retries: 3					
ENQ Retries: 3					
CHANNEL 1 (SYSTEM) - Driver: Ethernet					
CHANNEL 1 (SYSTEM) - Driver: Ethernet Edit Resource/Owner Timeout: 60					
CHANNEL 1 (SYSTEM) - Driver: Ethernet Passthrough Link ID: 1					
CHANNEL 1 (SYSTEM) - Driver: Ethernet Write Protected: No					
Name	Number	Type	Rungs	Debug	Bytes
[SYSTEM]	0	SYS	0	No	0

1	SYS	0	No	0	
2	LADDER	7	No	92	
3	LADDER	9	No	261	
4	LADDER	3	No	81	
5	LADDER	11	No	399	
6	LADDER	9	No	313	
7	LADDER	13	No	203	
VIRT_HMI	8	LADDER	16	No	358
CHANNEL 1 (SYSTEM) - Driver: Ethernet Comms Servicing Selection: Yes					
CHANNEL 1 (SYSTEM) - Driver: Ethernet Message Servicing Selection: Yes					
Hardware Address: 00:0F:73:03:7C:4D					
IP Address: 10.x.x.x					
Subnet Mask: 255.255.255.0					
Gateway Address: 10.x.x.x					
Msg Connection Timeout (x 1mS): 15000					
Msg Reply Timeout (x mS): 3000					
Inactivity Timeout (x Min): 30					
Bootp Enable: No					
DHCP Enable: No					
SNMP Enable: No					
HTTP Enable: Yes					
Auto Negotiate Enable: Yes					
Port Speed Enable: 10/100 Mbps Full Duplex/Half Duplex					
Contact:					
Location:					
Program File List:					



Name	Number	Type	Scope	Debug	Words	Elements	Last
OUTPUT		0	O	Global	No	18	6 O:5
INPUT	1	I	Global	No	36	12	I:11
STATUS	2	S	Global	No	0	66	S:65
BINARY	3	B	Global	No	20	20	B3:19
TIMER	4	T	Global	No	18	6	T4:5
COUNTER		5	C	Global	No	3	1 C5:0
CONTROL		6	R	Global	No	3	1 R6:0
INTEGER		7	N	Global	No	40	40 N7:39
FLOAT	8	F	Global	No	2	1	F8:0
VHMI	9	B	Global	No	36	36	B9:35
	10	N	Global	No	40	40	N10:39
VHMI_INT		11	N	Global	No	8	8 N11:7

See document 'Appendices' in email for further expansion of PLC Config as file is too big.

# Appendix 3

## Equations

The following formula is used to estimate the time a system can withstand a cyber-attack incident without dropping to a below critical temperature efficiency level:

$$t = ((T_{max} - T_{nom}) / (T_{max} - T_{min})) \times t_{max}$$

Where:

- ***t*** is the estimated time the system can withstand a cyber-attack incident without dropping to a below critical temperature efficiency level (minutes)
- ***T<sub>max</sub>*** is the maximum temperature reached by the manufacturing system during and after the cyber-attack incident (°C)
- ***T<sub>min</sub>*** is the minimum temperature required for the product to remain within safe limits (°C)
- ***T<sub>nom</sub>*** is the nominal operating temperature of the manufacturing system (°C)
- ***t<sub>max</sub>*** is the maximum allowable time for the manufacturing system to operate above the critical temperature level (minutes)

Note that this formula assumes a linear relationship between the temperature increase and time. It is also important to note that this is only an estimation and that the actual time may vary depending on several factors such as the severity of the cyber-attack, the resilience of the system, the requirements of the system and the effectiveness of the response measures taken.

# Appendix 4

## Research Output

A Cyber Resilience Analysis Case Study of an Industrial Operational Technology Environment

**Kirsty Perrett**

**Researcher, Cyber Security, University of South Wales, CF37 1DL, UK**

**Ian David Wilson\***

**Professor (Associate), Computing and Mathematical Sciences, University of South Wales, CF37 1DL, UK**

**<https://orcid.org/0000-0002-3550-049X>**

**[ian.wilson@southwales.ac.uk](mailto:ian.wilson@southwales.ac.uk)**

**\*Corresponding Author**

### **Author Contributions**

Conceptualisation: Kirsty Perrett, Ian Wilson; Methodology: Kirsty Perrett, Ian Wilson; Formal analysis and investigation: Kirsty Perrett; Writing - original draft preparation: Kirsty Perrett; Writing - review and editing: Ian Wilson; Project/funding facilitator: Ian Wilson; Supervision: Ian Wilson

### **Abstract**

Cyber resilience is an active research area offering a novel approach to Cyber Security. The term appeared due to the concerning number of cyber-attacks on critical infrastructure. The National Institute of Standards and Technology (NIST) developed a framework to assist organisations with techniques and approaches to improving cyber resilience. However, there is a sparsity of case studies that speak to the adoption or measurement of these novel approaches within a complex industrial control environment. This paper presents a case study analysis of a manufacturing plant assessment drawing on key themes from the NIST literature.

The paper presents how well NIST constructs can be adopted to find cyber resilient enhancement opportunities and to decide if an evaluation of the results could supply a quantitative baseline measure of an organisation's overall resilience. Conclusions drawn show that although the

framework did partially aid with the analysis process, the frameworks ease of adoption assumes an organisation has a conventional cyber security foundation; NIST should make this clear within their guidance. Furthermore, the accompanying evaluation process was not sufficient to quantitatively measure the overall cyber resilience maturity for this case study.

**Keywords:**

Cyber Resilience, NIST, Case Study, Industrial Control Systems, Operational Technology, Critical Infrastructure

**Acknowledgements**

The authors acknowledge the support of the Knowledge Economy Skills Scholarships (KESS) and Thales Ltd. KESS is a pan-Wales higher level skills initiative led by Bangor University on behalf of the HE sectors in Wales. It is part funded by the Welsh Government's European Social Fund (ESF) convergence programme for West Wales and the Valleys.

Introduction

Digital innovation is shaping our world. As technology and big data processes are increasingly used to deliver critical services, Operational Technology (OT) systems have evolved to collectively work with enterprise IT networks to provide operational data to a centralised management platform. Whilst this convergence brings many advantages to industry and society, OT systems, historically, have not been planned or executed with cyber security as a priority.

The conventional risk assessment approach to cyber security has proven to be unmanageable in OT environments (Linkov, et al., 2013), (Groenendal & Helsloot, 2021) and there is a rising threat to the cyber security of traditional OT systems (Johnson, 2016). An example is the high-profile attack on the Colonial Pipeline in May 2021 where hackers successfully shut down the largest petroleum pipeline in the United States (Reeder & Hall, 2021). A wide variety of Cyber Resiliency frameworks exist that aid organisations with techniques and approaches to improving cyber resilience. However, there is a sparsity of real-life case studies that speak to the adoption and measurement of these novel approaches within an OT environment.

The study presented in this paper assesses the contribution of the NIST Cyber Resilience (CR) framework (National Institute of Standards and Technology, 2021) and offers findings derived from a case study of an industrial plant consultation undertaken with the Thales Group. The case study draws on key themes that appeared from the literature to analyse CR gaps, to what degree constructs can be adopted to improve CR and to determine if an evaluation of the results could

provide a measure of an organisation's resilience. The presented case study and conclusions drawn afford a baseline for future research into cyber resilient improvements.

The paper is organised as follows. Section 0 provides background and section 0 reviews current literature and primary research. Section 0 elaborates upon the problem and explains the underlying methodology. Section 5 presents the case study, associated discussion and results. Section 0 offers concluding remarks and speaks to future work.

## Background

Critical infrastructure, industrial and manufacturing industries are primarily enabled by Industrial Control Systems (ICS) commonly referred to as Operational Technology, which enable us to go about our daily lives. Here, OT is as any system outside of the enterprise network and include equipment such as Programmable Logic Controllers (PLCs), embedded systems and Supervisory Control and Data Acquisition (SCADA) systems. OT systems are different from typical IT systems. OT support complex interconnectivity between physical and logical infrastructure often communicating through propriety protocols that rely on computational equipment such as PLCs. PLCs typically don't allow remote access unless interconnected with another industrial asset known as a Human Machine Interface (HMI) (Cherdantsevaa., et al., 2016). The implementation of IT security policies is problematic in OT safety-critical systems. Whilst regulators and engineers understand the fundamental safety requirements of such systems, cyber security requirements do not easily follow on and this increases the risk of compromise (Maglaras, et al., 2018).

Cyber resilience refers to the ability of the system to prepare, absorb, recover and adapt to adverse effects; especially those associated with cyber-attacks (Linkov & Kott, 2018) (National Institute of Standards and Technology, 2021). Resilience Engineering has underpinned other domains for decades and its proven approach has now made its way into the cyber domain (see (National Institute of Standards and Technology, 2021) for a detailed account).

Risk management, cyber security and cyber resilience, although intertwined, are very different. Risk management quantifies the probability and impact of cyber risks and cyber security defends against those risks, whereas cyber resilience is essential when cyber risk is ineffective, such as "when hazardous conditions are a complete surprise when the risk analytic paradigm has been proven ineffective" (Linkov & Eisenberg, 2013). While risk has been a constant feature of human existence, never before in human history have leaders needed to prepare for such a multitude of shocks and while risk management in cyber security is concerned with the minimisation of hazards, cyber resilience seeks to maintain high performance levels "irrespective of the pre-sense of absence of

hazards” (Bagheri S, 2017). The traditional concept of cyber security focuses primarily on protecting systems from cyber-attacks known as “fail-safe”. Cyber resilience focuses on the business mission as a whole and the events that follow in the aftermath of a cyber-attack known as “safe-to-fail” (Björk, et al., 2015). In other words, cyber resilience takes over when risk management has been unsuccessful at guarding an organisation from disruptive threats and implies a constant cycle of undertakings and reactions to implement the adaptive measures needed to come to the next unpredictable shock.

#### Literature Review

A plethora of standards, frameworks and directives on the topics of cyber security and cyber resilience have appeared over the last decade. The following introduces these topics with a particular emphasis on cyber resilience.

The U.S. Department of Commerce published a framework (National Institute of Standards and Technology, 2014) to promote the protection of critical infrastructure and to support operators to manage cyber security related risks (National Institute of Standards and Technology, 2013), (COBIT 5), (ISA 62443) and ISO/IEC 2700. NIST subsequently released a framework for developing CR systems (National Institute of Standards and Technology, 2021) updated in August 2021 to align to the MITRE Att&ck Framework (MITRE, 2017). ISA-95 is the international standard for the integration of enterprise and control systems. ISA-95 consists of models and terminology (Williams, 1992). One example widely used across OT environments is the Purdue Model which incorporates layers of technology and business practice used by industrial corporations and incorporates them as levels for the standard (Simonovich, 2020). The US energy sector developed a ‘Cyber-security Capability Maturity Model’ (C2M2) in 2012 to help organisations running critical infrastructure. The model comprises 10 domains, objectives and practices aligned to maturity indicator levels (Office of Cybersecurity, Energy Security, and Emergency Response, 2012). An updated version (released in July 2021) aligned with the main changes to NIST cyber security framework (National Institute of Standards and Technology, 2018).

One of the major requirements of a cyber analysis is to supply a basis for relative comparison so that decision makers can make well-informed actions based on in-depth knowledge of both the system and business environment (Leversage & Byres, 2008). Tools such as capability maturity models form the basis for cyber security metrics in literature. Capability maturity models (widely used in the cyber security domain) typically depict existing practices within an organisation as a basis for comparison. However, although there are attempts in literature to provide a method for measuring cyber resilience, few offer a method to achieve a baseline maturity measure of an

organisation's resilience during the context establishment stage and, of the few that do, only qualitative metrics are offered.

Cyber Resiliency and its importance has been highlighted (Linkov, et al., 2013), (Linkov, et al., 2014), (Linkov & Kott, 2018), (Kott & Linkov, 2019), (Kott & Linkov, 2021). The most recent work highlights that there is insufficient research on cyber resiliency measurements and only recently have researchers begun to investigate quantitative measures (Kott & Linkov, 2021). We, therefore, rely on qualitative approaches to measure cyber resilience (Groenendal & Helsloot, 2021). Another challenge is that organisations may find it difficult to translate CR frameworks and models into roadmaps since there is no easy-to-follow process on how an industry can adopt and measure CR. This supports early findings (Haque, et al., 2018) which states that “although many of the frameworks provide some subjective guidance of resilience study, they all lack clear explanation on the quantitative resilience metrics formulation”. Recent research attempts to resolve such challenges (Cariás, et al., 2021) produced a Cyber Resilience Assessment tool to aid Small and Medium Enterprises (SMEs) in their CR operationalisation. Three case studies formed the basis for this study with reported success. However, the study related to SMEs with a limited level of cyber resilience. The need for this type of tool within OT environments would be of benefit. Subsequently, a study proposed a method of grading a system’s cyber resilience (Singh, et al., 2021). The paper only considers the system technology rather than the whole organisation, which is the underlying focus for a cyber resilience analysis. The metric criteria are not yet consistent or repeatable. The authors recognise this and aim to improve this in their future work.

The ‘Cyber Resiliency Metrics, Measures of Effectiveness and Scoring’ framework (Mitre Corp., 2012) supplies ideas for cyber resilience metrics and considers the problem domain overlap. It discusses the large overlap between each problem domain and state “As cyber resilience techniques mature and are more widely adopted, the disciplines of cyber resilience, cyber security and conventional security will merge”. Since many of the traditional cyber security analysis approaches and metrics can be repurposed in a cyber resilience analysis then, in principle, an industry should be able to reach some sort of baseline metric through use of multiple frameworks and existing maturity models. Mitre updated this framework in May 2015 to include challenges this case study acknowledges in Section 3 (Bodeau, et al., 2015).

The U.S. Department of Commerce approach to conducting CR analysis includes the Anticipate, Withstand, Recover and Adapt goals, along with the x8 objectives and x14 techniques (National Institute of Standards and Technology, 2021). Prerequisites of the framework suggest the architectural, programmatic, operational and threat context must be identified. The Architectural

context identifies the type of system being analysed including its patterns, how it interacts with other assets, asset locations and layers in the architecture. The type of system is important as it determines which approach or technique is most appropriate for the analysis. The Programmatic context identifies how the system is being acquired, developed and maintained. This also identifies the stakeholders responsible for the system. The Operational context identifies how the system will be used and maintained and how it interacts with other systems. The Threat context identifies the threat events, sources and scenarios of concern. However, the framework offers little guidance on how to obtain the prerequisite context and does not make clear the analysis ease of adoption assumes that an organisation already has a mature cyber security foundation; NIST should address this. Mitre updated their 2012 framework to address this.

A mature cyber security foundation for this case study did not exist and, for this reason, a mix of frameworks and maturity models were used in conjunction with the NIST framework to evaluate the organisation. The overhead for obtaining the prerequisite information needed to start a CR analysis was significant. This overhead could have been avoided if the organisation had an established level of cyber security. The following section outlines the methodology and methods used to perform a cyber resilience analysis for this case study.

## Methodology

This case study provides a high-level analysis of an industrial factory belonging to a globally established company with presence in multiple countries. The business (anonymised to protect their identity) manufactures products used in the Aerospace and Defence industries as well as many other industrial marketplaces. The analysis is based on the (National Institute of Standards and Technology, 2021) framework and tailored to the organisation through use of other frameworks and standards, such as the Purdue Model and NIST CNI guidance, to evaluate the outcome. The study focuses on the business mission, its OT infrastructure, its current cyber risk posture and recommendations provided to the customer.

## Outline methodology

The applied methodology is set out in five steps.

### Step 1: Context establishment

Identify key stakeholders, OT assets, system categorisation, Netflow discovery and other capabilities from functional areas such as cyber security, cyber defence and contingency planning.

### Step 2: Establish a baseline and identify gaps and critical business resources



Using the data collected, identify critical resources and any gaps. Gaps can also be identified from historical reviews such as penetration test reports, after action or risk management reports and vulnerability assessments with respect threat/attack events.

#### Step 3: Analyse the system and attack surfaces

Graphically map logical and physical systems. In this step, the system is analysed from two perspectives (architectural improvements can then be identified), specifically:

Identify the critical business resources through a graphical analysis of network assets communicating.

Identify high value targets of APT (Advanced Persistent Threat) actors and develop attack scenarios.

#### Step 4: Define evaluation criteria and threat/vulnerability assessment

Cyber resiliency can be evaluated in multiple ways and should be distinguished before the assessment can begin. See (National Institute of Standards and Technology, 2021) for further evaluation criteria. A typical evaluation criterion could be a cyber risk assessment especially if the organisation already makes use of a Risk Management Framework such as (National Institute of Standards and Technology).

#### Step 5: Develop recommendations (plan of action)

Make recommendations following the NIST framework guidelines.

#### Case study

The following describes the application of the steps described above within the context of the case study and the time and resources used to conduct this study.

Two expert consultants from Thales Ltd and a research student spent a total of 18 hours at the customer site. In addition, the team spent a further 30 hours analysing the data and another 20 hours finalising the findings in the form of a report.

#### Step 1 – Context establishment

This stage is twofold and included:

a planning stage where the scope of this case study is assessed and key stakeholders are identified;

a data collection stage where personnel are interviewed, OT Network architectures/floor plans are reviewed, the connection of passive monitoring equipment is established and other metrics found

during a physical walkthrough such as configuration assessment of factory end points is documented (summarised in Table 1).

*Table 1 Data types collected.*

Architectural Analysis	
System Field Parameters - Metadata:	<ul style="list-style-type: none"> <li>-Asset Reference (e.g., 001)</li> <li>-Asset Type</li> <li>-Criticality</li> <li>-Location Reference</li> <li>-Location Name</li> <li>-IP Address</li> <li>-MAC Address</li> <li>-Role</li> <li>-Manufacturer</li> <li>-Model</li> <li>-Host Name</li> <li>-Firmware V</li> <li>-OS Version</li> <li>-Client Protocols</li> <li>-Server Protocols</li> <li>-Purdue Level</li> <li>-Serial Number</li> <li>-Description</li> <li>-VLAN</li> <li>-Network Location (If known)</li> <li>-Protocol/Service, i.e., Modbus Eth/Ip</li> <li>-Date/Time</li> </ul>
Risk Value Parameters (Critical to business operations):	-High
Vulnerability Assessment Parameters:	-Medium
	-Low

Log data variables criteria:	- Timestamp
	- Asset ID
	- Title / Event
	- Impact level
	- Sensor / Trigger
	- User (optional)
	- Unique Identifier

### Step 2 - Data Examination and Gap Analysis

Analysing the data collected in Step 1 established a baseline and identified the gaps in cyber resiliency that may directly cause harm to the organisation. An analysis of data sources contributed to understanding how the customer’s OT communicated with their IT and external networks including third party suppliers and maintenance contractors. An OT vulnerability assessment for each of the assets was completed to determine how likely they could be targeted by Advanced Persistent Threat, followed by a risk assessment (National Institute of Standards and Technology, 2018) of critical assets to determine their Purdue level and value to the business. Figure 1 shows the total number of OT and IT assets.

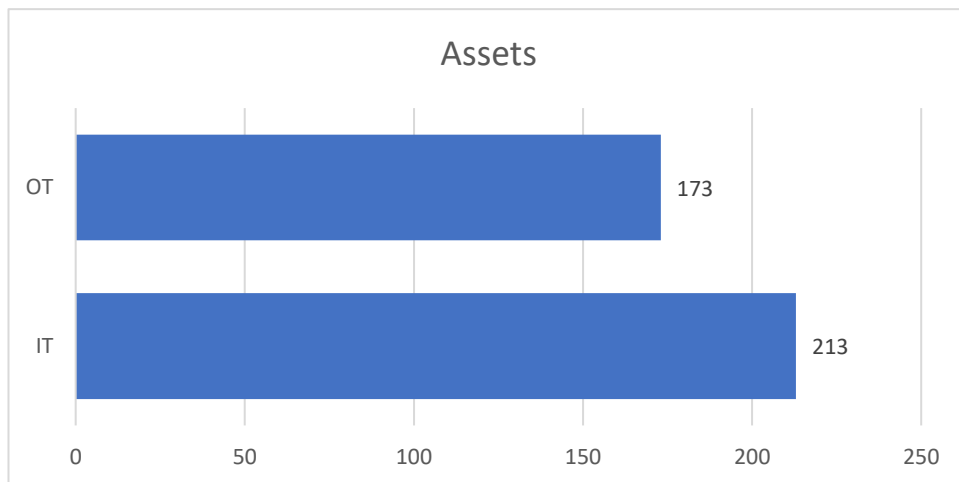


Figure 1 OT Assets to Purdue Level

Table 2 Architecture System Type, mapped to a physical location

Purdue Level	Room Location																				Total		
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T		U	V
LEVEL 0						2			1			1	4		1	1	3		1		4	3	21

Scale						2			1			1	2			1	2				3		12		
Sensor													2			1		1			1		1	3	9
<b>LEVEL 1</b>				2	5			3		1	1			1		1				1	1	2	4	<b>22</b>	
PLC				2	5			3		1	1			1		1				1	1	2	4	22	
<b>LEVEL 2</b>	1	1			2	2	1		2			2	4	1			1	1			2	4	2	<b>26</b>	
HMI	1	1			2	2	1		2			2	4	1			1	1			2	4	2	26	
<b>LEVEL 3</b>		1	10																					<b>11</b>	
Application Server			1																					1	
EWS			2																					2	
Historian			2																					2	
Printer		1																						1	
Terminal_server			5																					5	
<b>LEVEL 3.5</b>			2		1																		1	<b>4</b>	
IP_Camera																							1	1	
Switch			2		1																			<b>3</b>	
<b>LEVEL 4</b>			1																					<b>1</b>	
Gateway			1																					1	

Each OT asset is mapped to its Purdue level (shown in bold) by system type (see Table 2).

### Step 3 - Mapping Logical and Physical Networks

A logical and physical topology arrangement of assets provided a graphical representation of critical assets and data flows. The logical topology representation classifies the network and illustrates the subnets and traffic flows. Each asset is identified (where possible) with their criticality to business, host names, IP addresses and their roles with any notable traffic communications highlighted in red (see Figure 2Figure ). Note the topology drawing is for visual understanding only and is purposely obfuscated to protect the identity of the organisation.

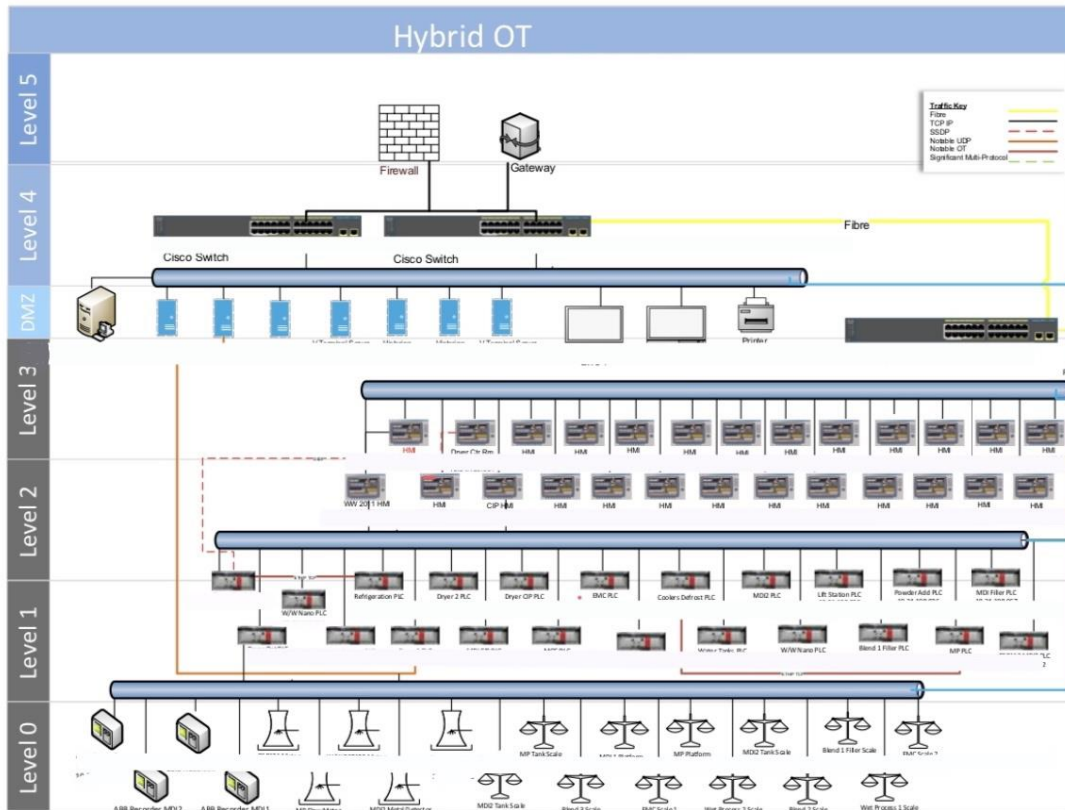


Figure 2 - Logical Topology with notable traffic concerns highlighted in red

Using the data triaged in stages 1 and 2, the Logical Network Infrastructure is mapped to a physical location for each asset (see Table 3). The physical topologies mapped each asset to the geographical location using the business’s floorplans (not included to protect the identity of the customer).

Table 3 Physical Topology - Mapping assets to geographical location

Location	Asset Ref	Description
A	243	Engineer Workstation
B	001	Gateway
	002	Switch
	003	PLC
	100	Application server
	104	Terminal server
	105	Historian
	106	HMI
	107	Sensor
	199	EWS

	200	Firewall
--	-----	----------

#### Step 4 - Define evaluation criteria and threat/vulnerability assessment

Other elements of the Operational business processes were audited to complete the evaluation. The results presented each of the findings as prioritised risks. The associated mitigating recommendations and a set of objectives needed to drive a cyber resiliency approach were assessed incorporating the data identified from the gap analysis and discovered during the site walk-round which summarised:

operational issues (e.g., failed Modbus connections, device restarts);

security Threats (e.g., port scans, login attempts);

networking problems (e.g., unstable connections, unanswered requests);

connection attempts to public IP addresses;

contextual analysis of information;

deep dives into any areas of concern;

samples of single assets of high risk.

#### Step 5: Develop recommendations (plan of action)

The next section discusses the case study baseline results and recommendations.

#### Baseline Results

This section is an objective view of what security controls are in place at the factory using the (National Institute of Standards and Technology, 2018) baseline set of activities framework. This framework provided a baseline control set to perform a gap analysis. Due to the lack of any comprehensive Cyber Security Risk Assessment analysis, this section does not make any determinations as to if such controls are necessary, just if they appear to exist and how they are used.

#### Cyber Risk Analysis – Baseline Control Set

##### Identify

##### Asset Management

A functioning system exists based on an excel inventory. Many of these required human interaction to ensure data integrity is coordinated and is potentially prone to data inconsistencies. The list of recorded assets does not include asset priority ratings based on criticality, business value, or supply

chain availability (given the number of legacy systems). No overarching strategy for managing and or maintaining the configuration of assets was apparent. There did not appear to be a list of external dependencies or critical business assets – this could mean that they either have none or that a determination has not been conducted. There did not appear to be a formalised process for ensuring a consistent supply of engineering spares, conversely the onsite teams appeared both knowledgeable and capable of ensuring critical assets could be replaced and maintained. The process was expert driven rather than documented and process driven. There was no clear RACI structure in place for cyber resilience; primarily due to the fact it was not a significant concern for the factory.

#### Business Environment

The staff and organisation were clear about their role in the successful operation of their business. The mission for the factory and staff appeared to be well articulated and of the people we talked to, they agreed on similar missions and objectives (e.g. on time delivery in a safe and reliable manner). Dependencies and critical functions were identified and managed from a physical and supply chain perspective, but not clearly from an information or digital perspective. Resilience was not a key priority or addressed maturely from a digital or cyber perspective. Physical resiliency within the factory was possible through component/system & production line reuse. Although there is awareness about the importance of an OT cyber resiliency approach, a consistent approach had not been adopted. There is no standalone separate network environment for OT infrastructure.

#### Governance

It was acknowledged that no governance or risk management process for OT cyber security had been put in place. Cyber was treated in a similar fashion to other large corporate risks and managed through the same management process. The roles & responsibilities for cyber security seemed to align with those for the IT operation of the factory (e.g. cyber wasn't treated any differently to other engineering aspects). It was clear who staff would communicate with should an issue arise with the factory (cyber or otherwise). There was acknowledgement that specific cyber security legislative or regulatory requirements are not tracked at the factory level, instead it was assumed that the corporate IT both on / off-site were likely to provide that info to the factory.

#### Risk Assessment

There is a process in place to identify, track or respond to asset vulnerabilities, providing the assets are managed by the corporate AV. This does not cover unknown or unregistered devices onsite that client IT are unaware of. There is no formal method of receiving cyber threat intelligence – the

factory relies on corporate IT to inform them of any issue. But there was no method of tracking response to that issue. And it was acknowledged that IT does not provide threat or vulnerability intelligence for OT assets. No business-aligned OT cyber continuity plan has been defined. There was no formal method of reviewing threats and their potential business impacts (cyber or otherwise). Therefore, new risks are not consistently identified, scored, or addressed. Cyber risks are only identified or prioritised when informed by corporate IT.

#### Risk Management Strategy

There is no formal cyber security risk management process or strategy, beyond the corporate risk management approach. The organisational risk tolerance is determined on an ad-hoc basis. The approach to risk seems to be divorced from the wider business.

#### Protect

##### Identity Management and Access Control

Identity is not comprehensively managed within the factory infrastructure. The majority of access is through shared role-based access, limited audit capability to identify critical actions carried out by an individual. Access to critical resources is limited to IT staff. There is external remote access into the facility. Enterprise remote access is limited to IP addresses through Firewall rules. There is limited network segregation through a DMZ. The firewall is managed remotely by another site through an external software defined firewall on the external to internal interface and controlled through a software/VM firewall on the internal to external interface. A zone & conduit approach to network integrity is not in effect. Identities are handled through corporate access to assets and first-hand knowledge of those people. Access to engineering laptops is controlled through informal process. There didn't appear to be any central authentication OT management solution or multi-factor solution – especially when it came to OT assets. Everyone has access to the factory assets and any information critical assets reside on the IT enterprise network.

#### Awareness and Training

There is no regular or formal training on cyber security from an OT or factory perspective, just in regard to the corporate IT Roles & responsibilities are inherited from existing work structures rather than explicit RACI charts. There is some engineering reliability on external 3rd. parties. Senior executives understand their roles and make themselves available to the team. There are no dedicated cyber-security personnel for OT.

#### Data Security



There did not appear to be any whole disk encryption products in use. Therefore, within the factory there was limited to no data-at-rest protection. There did not appear to be any data-in-transit protection in use – except where the default protocols/configurations use it. There was limited to no ability or approach to detecting or controlling for information leakage, disposition, or removal of information from the factory domain. There was no formal method for checking the integrity of vendor supplied software/firmware.

#### Information Protection Process and Procedures

The concept of least functionality is not routinely or consistently deployed. There did, however, appear to be a consistent or deliberate use of baseline configurations from the IT side. There is a formal approach to configuration change management. This is routinely handled through IT coordination between individuals and logged via their IT Helpdesk. There is no comprehensive or tested method for backups. There appeared to be confusion between the IT teams about which critical assets were being backed up. There did not appear to be a well-known and followed process for data destruction when not required. Protection technologies and processes are not regularly checked or validated. Response plans and recovery plans do not include cyber or cyber incidents directly.

#### Maintenance

Maintenance is performed by engineering experts as required. There is a ticketing system in place to log and track issues. Remote access for maintenance is permitted as discussed.

#### Protective Technology

Audit logs are not reviewed according to business needs or risks. Removable media is not currently restricted but plans for this are underway. Technology resilience is in place for some critical assets (e.g. core switches, virtualised servers) – but the conditions and resiliency requirements driving them were not clearly articulated.

#### Detect

##### Anomalies and Events

Security event logs are not collected on the OT equipment. There was an absence of an event monitoring and reporting systems. Therefore, a baseline knowledge of expected data flows & volumes was not known. There is no vulnerability management process or solution for OT. There was an expert led approach to reviewing events and their impacts.

#### Security Continuous Monitoring

There is an absence of automated vulnerability assessment (VA). There did not appear to be a regular or routine review of critical security functions such as credential reuse/compromise. There was no detection or audit of security credentials to detect unauthorised creation or use. There was some use of anti-malware solutions in place to help detect the deployment of malicious code. There was no regular audit for the use of unauthorised connections, devices, or software.

#### Detection Processes

Security IT related management procedures for firewalls, security appliances, network segmentation and intrusion detection are managed by the IT Network to authorise access and control information flows from and to networks, however no security in place on the OT LAN Network. Almost everything on the OT infrastructure is done manually system by system. Detection processes do not appear to be regularly tested, evaluated or continuously improved.

#### Respond

##### Response Planning

No network security policy in place for the OT Network No procedure or guidelines. There haven't been any significant cyber issues – therefore response plans have not been tested in anger.

##### Communications

No adequate follow-up actions or playbooks are defined for indications of inappropriate or unusual activities. Staff rely on IT and engineers to report anomalies in an ad-hoc manner. Information sharing between stakeholders (internal & external) is done in an ad-hoc manner.

##### Analysis

Ad hoc risk analysis and use of measures by individuals. No incidents have occurred requiring forensics or impact analysis.

##### Mitigation

No incidents have occurred requiring containment or mitigation. New vulnerabilities are not mitigated but may be documented as accepted risks.

##### Improvements

Response plans have not been required to be enacted for OT, therefore no lessons learned to be included.

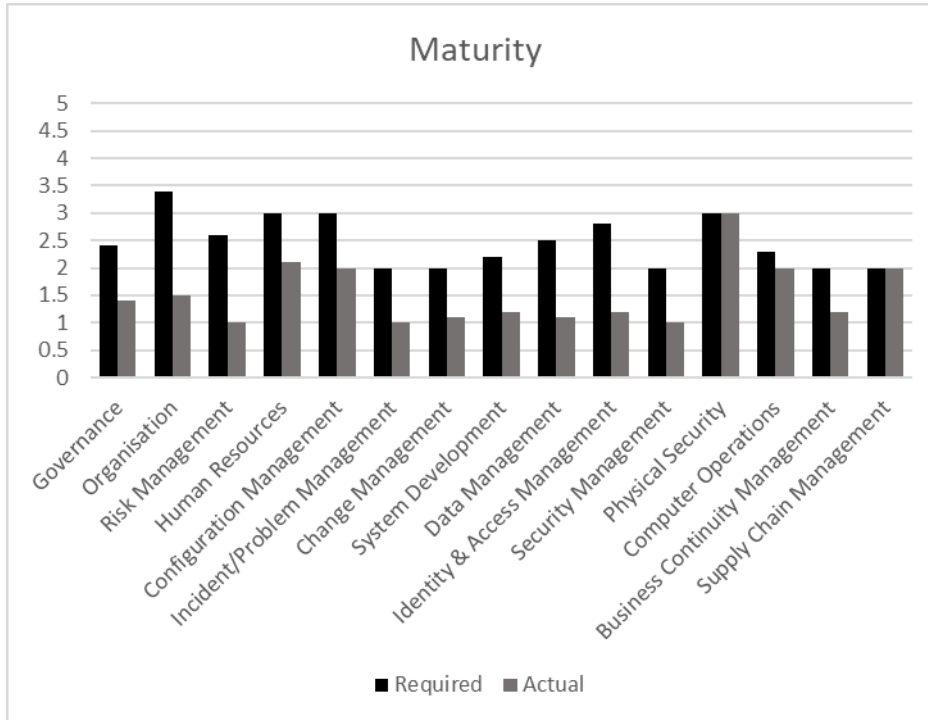


Figure 3 Summary of Required vs Actual Maturity Level Indications per Area

The next section outlines examples of vulnerabilities and practices discovered during the analysis that represent weaknesses in the organisations approach to cyber resilience.

#### Threat/Impact Analysis

The described vulnerabilities (shown in Table 4) were assessed based on whether they could be exploited by a reasonable attacker. They represent the most likely avenues for compromise or use as part of a wider campaign. Each impact rating is scored based on an assessment of an attacker’s ability to turn that finding into a severe, major or minor impact to factory operations. Each rating is based on expert opinion and, although impartial, it should be validated by a wider risk and impact assessment that includes on-site factory personnel.

Table 4 Vulnerability Assessment

Area	Control	CR Weakness	Impact to Business	Impact Rating
Architectural Analysis	Flat layer network architecture	No network segmentation defences within the Operational Technology factory network.	If one asset is compromised – every asset can be compromised. It would be very easy to access an OT system in the event of an untargeted or enterprise compromise. Should any part of the interlinked assets fail (such as loss of power) it could impact other parts of the OT network. The introduction of malware into the factory would not be inhibited	Severe

			from spreading throughout the network to other HMIs/x86 devices and even to the IT enterprise assets.	
Programmatic Analysis	Inconsistent use of software versions, or hardware. AV Malware control	There are multiple OS versions, types and software builds in use throughout the factory including Windows XP. There is good use of end-point protection controls in place such as AV however not been deployed to all assets.	Untargeted attacks such as crypto-malware leverage well-known software vulnerabilities. The wide range of OS versions and legacy software make the factory pre-disposed to having significant compromise, should any be introduced accidentally. Coupled with the wide variety of legacy OS's & applications, the ability for malware (even widely known & signature friendly instances) to spread is high once compromise occurs. End-points without AV are extremely vulnerable to well-known attacks.	Major
	Windows XP used as HMI's	Windows XP machines were frequently found to be operating as HMI's to the OT machines.	BlueKeep is a recent but well publicised vulnerability in Microsoft's RDP service (CVE-2019-0708). Patches are available for legacy OSs including XP. It is advised that the systems are patched, as XP machines are critical within the factory and wormable exploits are in the wild.	Major
Operational Analysis	Good use of change control	There does appear to be a patching / configuration change management approach in place. However, OT assets appeared to be running versions of firmware that contain known vulnerabilities.	The wide range of insecure OS systems such as XP makes it very easy for unsophisticated attackers to use off-the-shelf attack kits to compromise the factory. Regular exploits for much of these systems exist in toolkits such as Metasploit.	Major
	No backup plans	There seemed to be some confusion between what the factory thought was being backed up and what was actually backed up.	Traffic identified to/from a server IP address appear to allow a wide range of services traversing the network to across all VLANs including test to communicate between any device in the factory network.	Severe

		Backups of configuration changes were accomplished through file-sharing over FTP.	Whilst this allows file-sharing to occur, it would also allow any compromise of those assets to spread into the OT factory.  This is a typical example of how a wormable exploit such as Eternal Blue (e.g. WannaCry) could spread from the enterprise IT network to the factory network.	
	Reliability on experienced staff	The factory is increasingly reliant on IT staff. Critical information is stored on the enterprise ERP system.	If you cut off or impact enterprise connectivity then the factory is quickly constrained by what it can do. Just as with the NotPetya attacks it is clear how a severe impact to enterprise systems would have knock on consequences to the factory operations.	Major

### Recommendations

This section provides observations & recommendations (summarised in Table 5-5) based on what was seen. Note: that no in-depth threat or risk assessment was performed, therefore recommendations are given from an informed point of view, rather than an outcome from a formal risk management process. Overall, it is fair to say that the organisation did have some basic protections in place. However, they had no systemic ability to detect, respond or recover from a cyber-attack and no resiliency to an insider attack or accidental compromise.

Table 5 Recommendations

Area	Recommendation	Priority
Strategy	The business should have a defined cyber security strategy for factory OT infrastructures separate to the IT strategy.	High
Governance	The business should ensure that a clear RACI structure is in place for governing cyber resilience and cyber incident response.	High
Risk Management	The business should establish and use a common approach for performing risk identification, assessment and management. This does not have to be in-depth, but it should be consistent to allow for improvement.	High

Security Audit	<p>The business should develop a sufficient security audit plan to measure compliance against and effectiveness of its security controls</p> <p>The business should then start to perform regular security audits of its controls and approaches.</p>	Medium
Identity & Access Management	<p>The business should have a user-auditable method for accessing critical systems, consider segregation of duties to reduce the likelihood of single individuals compromising critical processes.</p> <p>Consider restricting the broad access into the factory network, to only those necessary services. Regularly review and validate the rules and authorisations into the factory domain through the firewall.</p>	High
Change Management	<p>The business should formalise an OT change management process to ensure the current configurations and assets builds are known. This includes OT endpoints such as engineering terminals and HMIs.</p>	Medium
Security Architecture	<p>The business should take a zone &amp; conduit approach to network architecture within the factory. Deploying industrial firewalls strategically would reduce the ability for a single asset compromise to impact wider sections of the factory.</p> <p>The business should institute a segregation between the factory and enterprise networks. Boundary segregation devices should monitor and restrict services not just IPs through application firewalls.</p> <p>The business should review its network architecture from a OT/IT resiliency perspective and determine if it is sufficient for the business expectations in the event of a cyber-incident and ensure that there are no single points of failure.</p>	High
External Supplier Management	<p>The business should ensure remote visitors are strictly monitored for the entire session or restricted entirely from accessing factory machines until more robust security controls</p>	Medium

	are implemented to reduce the potential impact from accidental/intentional infection or data infiltration.	
Threat Intelligence	The business should require factories to include cyber in its high-level threat assessment. Provide an appropriate feed of threat intelligence relevant to the factories and their assets and establish a routine method of reviewing and evaluating that threat intelligence as it pertains to their operations.	Low
Incident Management	Capabilities to react and recover from cyber security incidents should be routinely tested and exercised. Accidental or insider compromises are assessed to be the most likely cause of cyber incidents. Swift recovery will minimize impacts to operations.	Medium
Business Continuity	The business should require factories to include significant cyber incidents in its business continuity plans, including recovery from APT or other destructive cyber consequence.	Medium
Human Resources	The business should review the limited succession planning and staff backup for key/critical individuals and/or departments.	Medium

#### Cyber Resiliency Evaluation

A number of techniques reiterated from (National Institute of Standards and Technology, 2021), deemed most applicable to this case study, are outlined in Table 6. These techniques are based on a general objective view of the selection of approaches that could be taken to enhance the subject's overall cyber resilience that were not derived directly from this case study but, rather, given as relevant in general.

Table 6 Cyber Resilience Evaluation

Techniques	Approaches	Examples
------------	------------	----------

<p><b>PRIVILEGE RESTRICTION</b></p> <p><b>Definition:</b> Restrict privileges based on attributes of users and system elements as well as on environmental factors.</p> <p><b>Discussion:</b> Apply existing capabilities more stringently to deliver a trusted and complete response.</p>	<p><b>TRUST-BASED PRIVILEGE MANAGEMENT</b></p> <p><b>Definition:</b> Define, assign and maintain privileges based on established trust criteria consistent with the principles of least privilege.</p> <p><b>Informal description:</b> Trust no more than necessary.</p> <p><b>Discussion:</b> Separate roles and responsibilities and use dual authorisation.</p>	<p>Implement least privilege.</p> <p>Employ location-based account restrictions.</p> <p>Employ time-based restrictions on automated processes.</p> <p>Require dual authorisation for critical actions.</p>
<p><b>REALIGNMENT</b></p> <p><b>Definition:</b> Structure systems to meet business missions and reduce current anticipated risks.</p> <p><b>Discussion:</b> Look for restructuring opportunities related to new assets and any upgrades to current assets.</p>	<p><b>PURPOSING</b></p> <p><b>Definition:</b> Ensure that cyber resources are used consistently with business function purposes and approved uses, thereby avoiding unnecessary sharing and complexity.</p> <p><b>Informal description:</b> Ensure that resources are used consistently with mission or business function purposes and approved uses.</p>	<p>Ensure that no resource is designated as trusted unless a business reason justifies it</p> <p>Ensure that privileged accounts are not used for non-privileged functions.</p> <p>Use allow-listing to prevent the installation of unapproved applications.</p> <p>Use allow-listing to restrict communications to a specified set of addresses.</p>
<p><b>REDUNDANCY</b></p>	<p><b>PROTECTED BACKUP AND RESTORE</b></p>	



<p><b>Definition:</b> Provide multiple protected instances of critical resources.</p> <p><b>Discussion:</b> Redundancy is integral to system resilience, however manage carefully to avoid vulnerabilities and increasing the attack surface</p>	<p><b>Definition:</b> Back up information and software in a way that protects its confidentiality, integrity and authenticity. Enable safe and secure restoration in case of disruption or corruption.</p> <p><b>Informal description:</b> Back up resources securely and defend the restore process from adversary exploitation.</p>	<p>Maintain and protect system-level backup information (e.g., operating system, application software, system configuration data).</p> <p>Increase monitoring and analysis during restore operations.</p>
<p><b>SEGMENTATION</b></p> <p><b>Definition:</b> Define and separate system elements based on criticality and trustworthiness.</p> <p><b>Discussion:</b> Reduce the adversary's scope for lateral movement or command and control (C2).</p>	<p><b>PREDEFINED SEGMENTATION</b></p> <p><b>Definition:</b> Define enclaves, segments, micro-segments, or other restricted types of resource sets based on criticality and trustworthiness so that they can be protected separately and, if necessary, isolated.</p> <p><b>Informal description:</b> Separate OT and IT Networks at the very least.</p>	<p>Use virtualization to maintain separate processing domains based on user privileges.</p> <p>Use cryptographic separation for maintenance.</p> <p>Partition applications from system functionality.</p> <p>Isolate security functions from non-security functions.</p> <p>Use physical separation (air gap) to isolate security tools and capabilities.</p> <p>Isolate components based on organisational mission.</p>

## Conclusion

This paper introduced the reader to the subject by supplying some background context and a literature review including primary research. This was followed by a problem statement, a methodology and a discussion of the case study and its results. Finally, a conclusion is offered.

This paper presented a case study of a cyber resilience qualitative analysis of a manufacturing plant based on key themes from the NIST Cyber Resilience framework; highlighting the CR gaps, to what degree the adoption of its constructs might improve CR and to determine if an evaluation of the results could supply a measure of an organisation's CR. Conclusions drawn demonstrate that although the framework did assist with some of the analysis process, the framework's ease of adoption assumes an organisation has a conventional cyber-security foundation; NIST should make this clear within their guidance. Furthermore, the accompanying evaluation process was not sufficient to quantitatively measure the overall CR maturity for this case study and as such the limitations of the NIST CR Framework are clearly described. For this reason, the assessor utilised elements of different frameworks and maturity models alongside NIST to evaluate the organisation. Furthermore, the authors agree that there is insufficient research on cyber resiliency measurements (Kott & Linkov, 2021), especially where applied to case studies in the literature, of which this paper is positioned to fill a research gap. The result of this in-depth analysis adds an important data point for others developing CR analysis on combined OT and IT systems. Clearly identifying that applying only a subjective qualitative framework without modelling the recommended enhancements in an OT-IT environment cannot guarantee an enhanced cyber resilience maturity overall and further analysis is required. A digital twin of the organisation, simulated in a cyber range, to enhance the analysis and assessment of its cyber resiliency might better facilitate the quantitative measurement of resilience of an organisation under different attack strain thresholds and is the subject of the authors' further research.

#### Declarations

This work was supported by KESS in collaboration with Thales Ltd. (Grant number 21439). The authors have no financial or proprietary interests in any material discussed in this article.

#### References

- Björk, F., Henkel, M., Stirna, J. & Zdravkovic, J., 2015. Cyber Resilience – Fundamentals for a Definition. In: A. Rocha, A. Correia, S. Costanzo & L. Reis, eds. *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*. Cham: Springer International Publishing, pp. 3-4.
- Bodeau, D., Graubart, R., Heinbockel, W. & Laderman, E., 2015. *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*, Bedford, MA: Mitre Corporation.

- Cariás, J. F., Arrizabalaga, S., Labaka, L. & Hernantes, J., 2021. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access*, 9(1), pp. 80741-80762.
- Cherdantsevaa., Y. et al., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56(1), pp. 1-27.
- Groenendal, J. & Helsloot, I., 2021. Cyber Resilience during the COVID-19 Pandemic crisis: A case study. *Journal of Contingencies and Crisis Management*, 29(4), pp. 439-444.
- Haque, M. A., Teyou, G. K. D., Shetty, S. & Krishnappa, B., 2018. *Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics and Insights*. Miami, IEEE, pp. 25-30.
- Johnson, C., 2016. *Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems*. Brighton, Safety-Critical Systems Club, pp. 171-182.
- Kott, A. & Linkov, I., 2019. *Cyber Resilience of Systems and Networks*. 1st ed. Cham: Springer.
- Kott, A. & Linkov, I., 2021. To Improve Cyber Resilience, Measure It. *Computer*, Feb, 54(2), pp. 80-85.
- Leverage, D. J. & Byres, E. J., 2008. Estimating a system's mean time-to-compromise. *IEEE Security and Privacy*, 1 1, pp. 52-60.
- Linkov, I. et al., 2014. Changing the resilience paradigm. *Nature Climate Change*, 4(1), pp. 407-409.
- Linkov, I. et al., 2013. Resilience metrics for cyber systems. *Environment Systems and Decisions*, Nov, 33(1), pp. 471-476.
- Linkov, I. & Kott, A., 2018. Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: I. Linkov & A. Kott, eds. *Cyber Resilience of Systems and Networks*. Cham: Springer, pp. 1-25.
- Maglaras, L. A. et al., 2018. Cyber security of critical infrastructures. *ICT Express*, 4(1), pp. 42-45.
- Mitre Corp., 2012. *Cyber Resiliency Metrics, Measures of Effectiveness and Scoring*, Bedford, MA: Mitre Corporation, Department No. T8A2.
- MITRE, 2017. *ATT&CK Matrix for Enterprise*. [Online] Available at: <https://attack.mitre.org> [Accessed 15th Jan 2021].
- National Institute of Standards and Technology, 2012. *Guide for Conducting Risk Assessments*. NIST SP 800-30 Rev 1 ed. Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST SP 800-53 ed. Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2014. *Framework for Improving Critical Infrastructure Cyber-security (Version 1.0)*, Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cyber-security (Version 1.1)*, Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2021. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. NIST SP 800-160 ed. Washington, D.C.: U.S. Department of Commerce.

Office of Cyber-security, Energy Security and Emergency Response, 2012. *Cyber-security Capability Maturity Model (C2M2)*. [Online] Available at: <https://www.energy.gov/ceser/cyber-security-capability-maturity-model-c2m2> [Accessed 1 June 2021].

Reeder, J. R. & Hall, T., 2021. Cyber-security's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defence Review*, 1 August, pp. 15-39.

Simonovich, L., 2020. *Thriving in a Digitized Environment*. [Online] Available at: <https://www.securitymagazine.com/articles/93849-leo-simonovich-thriving-in-a-digitized-environment> [Accessed 1 October 2021].

Singh, R., Hutton, S. T., Donahoo, M. J. & Sicker, D., 2021. *Toward Grading Cyber-security & Resilience Posture for Cyber Physical Systems*. McKinney, TX, Elsevier.

Williams, T., 1992. *The Purdue Enterprise Reference Architecture, A Technical Guide for CIM Planning and Implementation I*. First ed. Research Triangle: Instrument Society of America.