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
*Corresponding Author

Author Contributions

Conceptualization: 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.

1 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 2 provides background and section 3 reviews current literature and primary research. Section 4 elaborates upon the problem and explains the underlying methodology. Section 5 presents the case study, associated discussion and results. Section 6 offers concluding remarks and speaks to future work.

2 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.

3 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 'Cybersecurity 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 (Carías, 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.

4 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.

4.1 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.

4.2 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:	-Asset Reference (e.g., 001) -Asset Type -Criticality -Location Reference -Location Name -IP Address -MAC Address -Role -Manufacturer -Model -Host Name -Firmware V -OS Version -Client Protocols -Server Protocols -Purdue Level -Serial Number -Description -VLAN -Network Location (If known) -Protocol/Service, i.e., Modbus Eth/Ip -Date/Time
Risk Value Parameters (Critical to business operations): Vulnerability Assessment Parameters:	-High -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.

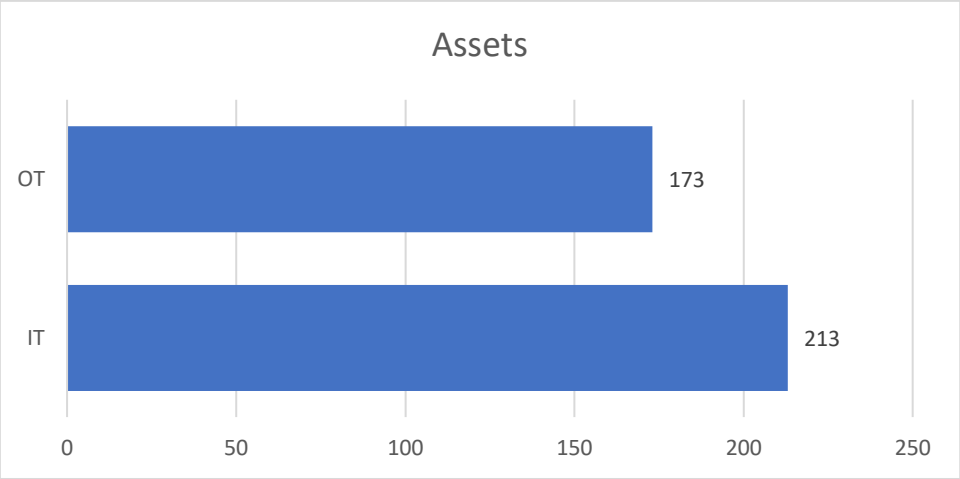

Figure 1 OT Assets to Purdue Level

Table 2 Architecture System Type, mapped to a physical location

Purdue Level	**Room Location**																						
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**
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
LEVEL 1				2	5			3		1	1			1		1			1	1	2	4	**22**
PLC				2	5			3		1	1			1		1			1	1	2	4	22
LEVEL 2	1	1			2	2	1		2			2	4	1			1	1		2	4	2	**26**
HMI	1	1			2	2	1		2			2	4	1			1	1		2	4	2	26
LEVEL 3		1	10																				**11**
Application Server			1																				1
EWS			2																				2
Historian			2																				2
Printer		1																					1
Terminal_server			5																				5
LEVEL 3.5			2		1																	1	**4**
IP_Camera																						1	1
Switch			2		1																		**3**
LEVEL 4			1																				**1**
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 2). Note the topology drawing is for visual understanding only and is purposely obfuscated to protect the identity of the organisation.

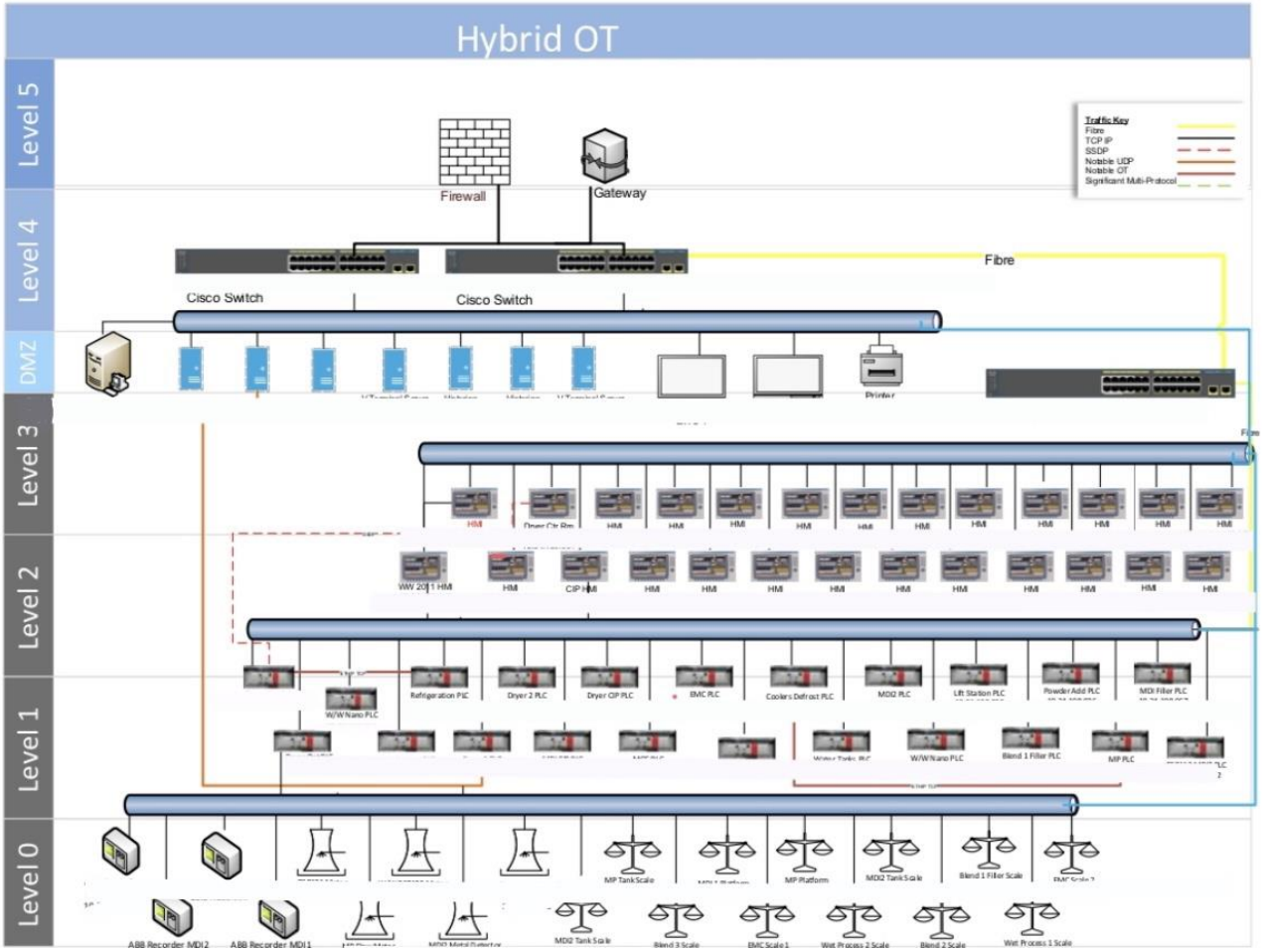

Figure 2 - Logical Topology with notable traffic concerns highlighted in red

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.

5 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.

5.1 Cyber Risk Analysis – Baseline Control Set

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.1.4 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.

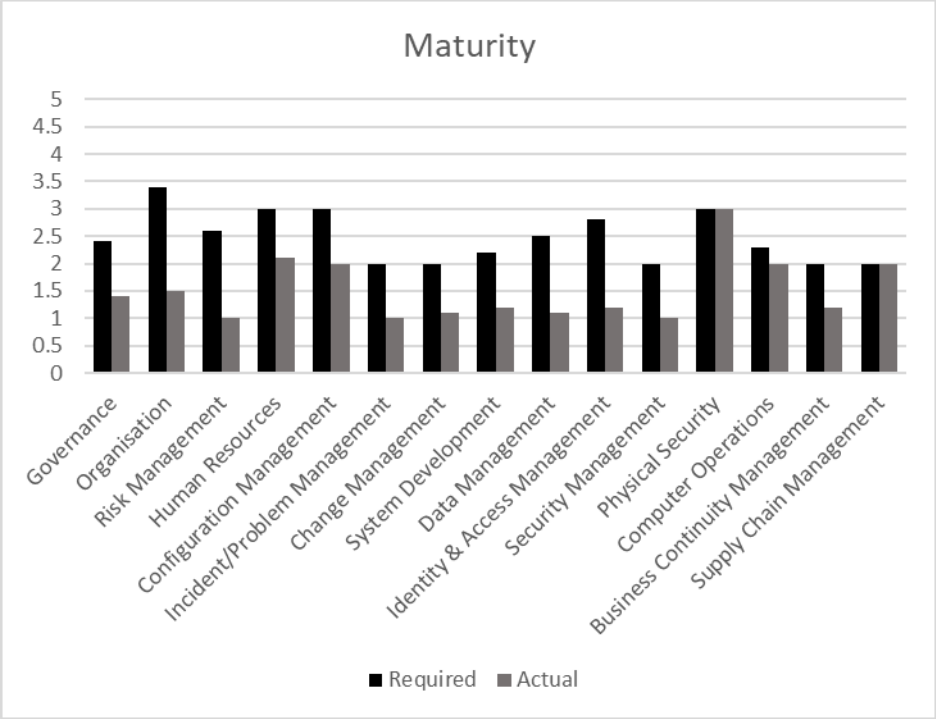

Figure 3 Summary of Required vs Actual Maturity Level Indications per Area

The next section outlines examples of vulnerabilities and practices discovered during the analysis that represent weaknesses in the organisations approach to cyber resilience.

5.2 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 2 network architecture	No network segmentation or 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 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. 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. 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 a wormable 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

5.3 Recommendations

This section provides observations & recommendations (summarised in Table 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	The business should develop a sufficient security audit plan to measure compliance against, and 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 firewalls strategically would reduce the ability for a single asset compromise to impact wider sections of the factory.	High

	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. 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.	
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 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

5.4 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**
PRIVILEGE RESTRICTION **Definition:** Restrict privileges based on attributes of users and system elements as well as on environmental factors. **Discussion:** Apply existing capabilities more stringently to deliver a trusted and complete response.	**TRUST-BASED PRIVILEGE MANAGEMENT** **Definition:** Define, assign, and maintain privileges based on established trust criteria consistent with the principles of least privilege. **Informal description:** Trust no more than necessary. **Discussion:** Separate roles and responsibilities, and use dual authorisation.	Implement least privilege. Employ location-based account restrictions. Employ time-based restrictions on automated processes. Require dual authorisation for critical actions.
REALIGNMENT **Definition:** Structure systems to meet business missions and reduce current anticipated risks. **Discussion:** Look for restructuring opportunities related to new assets and any upgrades to current assets.	**PURPOSING** **Definition:** Ensure that cyber resources are used consistently with business function purposes and approved uses, thereby avoiding unnecessary sharing and complexity. **Informal description:** Ensure that resources are used consistently with mission or business function purposes and approved uses.	Ensure that no resource is designated as trusted unless a business reason justifies it Ensure that privileged accounts are not used for non-privileged functions. Use allow-listing to prevent the installation of unapproved applications. Use allow-listing to restrict communications to a specified set of addresses.

REDUNDANCY **Definition:** Provide multiple protected instances of critical resources. **Discussion:** Redundancy is integral to system resilience, however manage carefully to avoid vulnerabilities and increasing the attack surface	**PROTECTED BACKUP AND RESTORE** **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. **Informal description:** Back up resources securely and defend the restore process from adversary exploitation.	Maintain and protect system-level backup information (e.g., operating system, application software, system configuration data). Increase monitoring and analysis during restore operations.
SEGMENTATION **Definition:** Define and separate system elements based on criticality and trustworthiness. **Discussion:** Reduce the adversary's scope for lateral movement or command and control (C2).	**PREDEFINED SEGMENTATION** **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. **Informal description:** Separate OT and IT Networks at the very least.	Use virtualization to maintain separate processing domains based on user privileges. Use cryptographic separation for maintenance. Partition applications from system functionality. Isolate security functions from non-security functions. Use physical separation (air gap) to isolate security tools and capabilities. Isolate components based on organisational mission.

6 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 cybersecurity 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.

7 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.

8 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.

Carías, 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.

Leversage, 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 Cybersecurity (Version 1.0),* Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity (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 Cybersecurity, Energy Security, and Emergency Response, 2012. *Cybersecurity Capability Maturity Model (C2M2).* [Online]
Available at: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
[Accessed 1 June 2021].

Reeder, J. R. & Hall, T., 2021. Cybersecurity'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 Cybersecurity & 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.