A Cyber Incident Response and Recovery Framework to Support Operators of ICS and Critical National Infrastructure

Alexander Staves, Tom Anderson, Harry Balderstone, Benjamin Green, Antonios Gouglidis, and David Hutchison

School of Computing and Communications, Lancaster University, Lancaster, LA1 4WA, United Kingdom

Abstract

Over the last decade, we have seen a shift in the focus of cyber attacks, moving from traditional IT systems to include more specialized Industrial Control Systems (ICS), often found within Critical National Infrastructure (CNI). Despite a push from governments to introduce appropriate legislation and guidance for such systems, operators of ICS and CNI still face multiple challenges in their cyber incident response and recovery capabilities, a theme that is often viewed as a last line of defence in minimizing the impact of cyber attacks. This paper provides the following contributions: Firstly, we analyze existing standards and guidelines within cyber incident response and recovery. This analysis provides a structure on key response and recovery phases, a foundational understanding of associated requirements for these, and identifies challenges that could affect the quality of in-practice response and recovery capabilities. Using this analysis as a baseline, we examine how response and recovery processes are currently undertaken in practice through engagement with UK-based CNI operators and regulators. Secondly, as a starting point towards improving identified challenges in existing standards and guidelines and their use in practice, we propose a framework, built using the outputs identified from the document analysis and the stakeholder engagement, for use by operators to support them in assessing and improving their response and recovery capabilities.

Keywords: ICS, CNI, OT, Cyber Security, Cyber Incident, Response and Recovery

1. Introduction

Critical National Infrastructure (CNI) is defined as "facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends" [26]. Examples sectors include water, energy, and civil nuclear, the majority of which are underpinned by Industrial Control Systems (ICS). These systems can be defined at a high-level through the Purdue Reference Architecture (Purdue Model) [31] shown in Figure 1. This model breaks ICS down into a set of zones and layers, each of which harbouring a set of sub-systems/devices responsible for the monitoring, control, and automation of operational processes (e.g. water treatment and distribution). More recently, the term Operational Technology (OT) has also been used to provide a high-level demarcation between conventional IT systems, found mainly within the Enterprize Zone, and bespoke ICS found within the Manufacturing and Safety Zones.

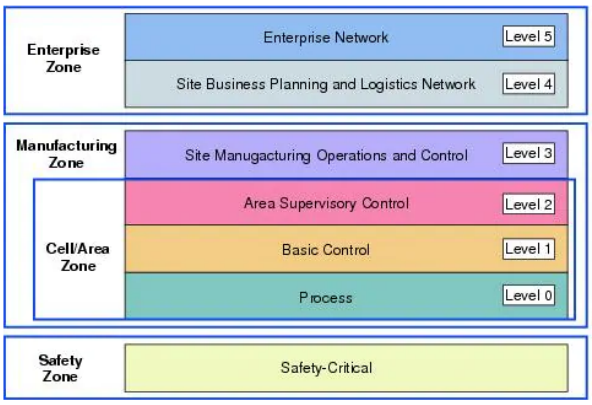

Figure 1: Purdue Enterprise Reference Architecture [31]

Over the last decade, a series of attack targeting ICS have been observed [36]. With one notable attack (Triton) even targeting safety level systems [37]. These at-

Email address: {a.staves, t.anderson1, h.balderstone, b.green2, a.gouglidis, d.hutchison}@lancaster.ac.uk (Alexander Staves, Tom Anderson, Harry Balderstone, Benjamin Green, Antonios Gouglidis, and David Hutchison)

tacks have acted as a catalyst for change in how we consider cyber defence within an industrial context. With organizational drivers and ever-evolving technical capabilities pushing the boundaries of safety and security to meet end-user goals, adoption, and increasing maturing of cyber security as a whole is becoming essential.

The importance of cyber security in CNI has not gone unnoticed by governments on an international level, many of whom have introduced strategies to drive change. For example, in 2016, European Union (EU) member states introduced the Network and Information Systems Directive (NIS-D) [44]. In the United Kingdom (UK), this was followed in 2016 by the creation of a National Cyber Security Centre (NCSC) [106], whose core role is to provide cyber security advice and support for public and private sector organizations, including focused advice on NIS-D compliance for CNI [107]. Similarly, in 2013 the United States of America assigned the National Institute of Standards and Technologies (NIST) the task of providing guidance on cyber security for CNI [119] Guidance from organizations such as the NCSC and NIST, primarily focus on five key principles; identify, protect, detect, respond, and recover [108]. The latter of which (respond and recover) can be considered as the last line of defence, designed to limit the impact of a cyber incident and promote a prompt recovery.

Although cyber incident response and recovery is crucial in most cyber security strategies, it is less explored than other areas. Given its last line of defence status, it presents a critical component that must be well understood by CNI operators. This paper provides an analysis of existing ICS focused standards and guidelines to identify the construct of response and recovery processes, their level of coverage, and potential challenges faced when using these documents. This analysis acts as a foundation in a set of semi-structured interviews with CNI operators and regulators to better understand current response and recovery practices, the use of existing standards and guidelines, and any associated challenges. These two studies then form a set of requirements from which a framework has been designed to support CNI operators in developing response and recovery capabilities through better use of standards and guidelines.

The core contributions of this paper are:

- An analysis of thirty-one international standards and guidelines
- An overarching construct of cyber security response and recovery processes
- An analysis of cyber security response and recovery process coverage
- Insight into operator/regular cyber security response and recovery processes
- A cyber security response and recovery framework

The remainder of this paper is structured as follow. Section 2 covers related work. Section 3 provides an analysis existing cyber security standards and guidelines. Section 4 describes the processes applied to the development of synthetic cyber attack scenarios, used within Section 5 to support a set of semi-structured interviews with UK-based CNI operators and regulators. Section 6 presents a discussion on key findings from the analysis of standards and guidelines and stakeholder engagement. Section 7 introduces our supportive cyber security response and recovery framework. Section 8 concludes the paper and offers areas for future work.

2. Related Work

Over the last decade, there has been an increasing volume of research activity targeted towards the holistic improvement of cyber security deficiencies within an ICS context. However, the field of cyber incident response and recovery has seen less focus [79], compared with risk assessment, for example. Here we provide a summary and review of literature spanning multiple aspects of response and recovery. The objective of this is to answer the following research questions:

- RQ1.1: How extensive is existing research on the improvement of ICS incident response and recovery?
- RQ1.2: How is literature on different topics related to ICS response and recovery (incident detection with cyber exercising for example) connected?
- RQ1.3: How does existing literature take into consideration industry recognised standards and guidelines?

Several works [57, 36, 167, 140] have explored historic cyber attacks against ICS. The work of Hassanzadeh et al., [57], for example, includes coverage of response, remediation, and lessons learnt. This can be used to better understand adversaries, their actions, and the actions of targeted organisations. All of which can support operators in the development of their own cyber security capabilities.

There exists a broad range of work on intrusion detection for ICS, all of which contribute towards the information set available to operators during initial incident response activities. For example, Jardin et al., [77] propose a non-invasive active monitoring approach, in contrast to more traditional passive techniques [50]. Taking an alternative approach, Urbina et al., [158] explore physics-based attack detection as a mechanism by which the impact of stealthy attacks can be minimised. A new metric is introduced to measure the impact of stealthy attacks, followed by a proposed combination and configuration of detection schemes towards stealthy attack mitigation. While Casalicchio and Gualandi [25] focus on the detection of changes to control logic. This is described as a self-protecting architecture for cyber-physical systems.

Going one step further from baseline detection techniques, Piedrahita et al., [125] apply software define networking into their detection and response system. This allows for automated network reconfiguration as a means of mitigation during an incident. With similar motivations, Ullah et al., [157] model an intrusion response system through the consideration of diverse attacker strategies. This model explores potential attack pathways, from which a response mechanism is designed to restrict attacker opportunities. Similarly, Cook et al., [33] define a seven-stage triage process to determine areas of priority where an attack's impact would be most significant.

Practical applied recovery work is also well covered. The work of Khalili et al., [83] for example, presents a recovery scheme for ICS, focusing on reducing the Mean Time To Recovery (MTTR). This work describes the use of physical backup hardware in recovering a system to its pre-attack state. Sesaki et al., [134] also explore system recovery and propose a novel approach by using a fallback and recovery ICS, the Fallback Control System (FCS). The FCS is not networked, and isolates controlled objected away from networked devices to manage them safely in isolation.

Butts and Glover [20] explore and describe limitations in current ICS security training. As part of this discussion, they describe the need for training to carry out response activities, develop training facilities with real-world environments, multiple interconnected systems, etc. An example of a response coordination syllabus is also outlined. Hirai et al., [61] begin to address these challenges by exploring incident response roles and responsibilities and introducing a framework for cyber incident response training. Further, Antonioli et al., [10] explore gamifying security training.

Cyber exercising is seen as a form of training, with the work of Asai et al., [12] proposing a framework that discusses exercise design, evaluation, and management. A practical exercise is provided as a means of validating the proposed framework. This is a theme explored by others in the creation of exercise platforms/testbeds for a variety of related activities [85, 129, 8].

ICS forensics has also been explored, including forensic readiness spanning data sources and tooling [42, 7, 16], case studies [160], and overarching forensic architectures [163].

Line at al., [98] engage with industry stakeholders to explore cyber situation awareness. This work focuses on comprehension of the current situation and understanding impact, situation evolution, attacker behaviour, and cause. From this, the authors provide a set of five recommendations (exercise, prepare for social engineering attacks, physical network separation, deploy anomaly detection, and use regulation as a means of ensuring improvements) focused on detection and response.

The work of He et al., [59] propose an ICS incident response decision framework across three phases (Descriptive, Predictive, and prescriptive).

In the closest work to ours, Jaatun et al., [76] propose a framework for incident response management in the petroleum industry. This work also includes engagement with industry stakeholders across multiple studies on incident response, risk and vulnerability assessment, security challenges at an installation, overall project findings, etc. These provide motivation and input into the resulting framework. The framework provides a high-level overview of factors one should consider as part of their overall response and recovery capabilities. However, it is a combination of just two (now outdated) standards and guidelines "with increased emphasis on proactive preparation and reactive learning". Line et al., [97] also interview industry stakeholders within an industrial context to better understand security incident management. This is focused on comparing small to large organisations but offers valuable insight into key challenges. Finally, our existing work in progress paper [145] forms a base for the work presented herein. This paper outlines existing standards and guidelines, then posits a set of objectives for future work, including stakeholder engagement and a holistic cyber security incident response and recovery framework. These objectives have been met throughout the remainder of this paper.

To summarise, concerning RQ1.1 and RQ1.2, cyber incident response and recovery has received limited attention from a holistic perspective, a critical gap noted by others [79]. While, collectively, existing litera-

ture spanning intrusion detection, historic attack analysis, training, exercising, etc., all contribute towards improvements in cyber incident response and recovery capabilities, a higher-level understanding of core requirements is still required. Furthermore, additional engagement with industry stakeholders and further understanding of challenges faced when using official standards and guidelines could add further towards understanding and addressing key challenges.

Industry standards and guidelines currently offer the most holistic and well-established view on response and recovery requirements. However, regarding RQ1.3, no comprehensive analysis of these has been undertaken to explore commonality in approach, coverage of key themes, use of technical vs non-technical content, etc. The following section therefore provides an analysis of these standards and guidelines to better understand each fundamental response and recovery phase and associated sub-phases; as well as to identify gaps in these documents that could negatively affect in-practice response and recovery capabilities.

3. Standards and Guidelines

3.1. Document Selection

The following subsections provide an analysis of selected government and industry standards and guidelines to support the development and delivery of cyber incident response and recovery capability used for our analysis. This guidance is primarily targeted at those responsible for the continued safe operation of ICS. Initial exploration focuses on UK-centric guidance and any supplementary documentation (i.e. referenced materials). International guidance is then investigated with a focus on North America and France, selected based on their accessibility (i.e. Open to the public and written in English), and their global nuclear energy presence, acting as an indicator of required cyber security guidance for one of the most critical elements of CNI [70]. The objective of this analysis is to answer the following research questions:

- RQ2.1: Which topics do standards and guidelines covering ICS incident response and recovery discuss?
- RQ2.2: How does using a subset of standards and guidelines affect the quality of guidance on ICS incident response and recovery?
- RQ2.3: What challenges can operators of ICS be faced with when consulting standards and guidelines?

A high level summary of the selected guidance documents can be found in Tables 1, 2, and 3 (UK guidance, supplementary/reference guidance and international guidance respectively). For more detail on the specific contents of each resource, a detailed summary of each document has been provided in Appendix A.

3.2. Critical Analysis

Across the aforementioned thirty-one standards and guidelines, a range of cyber incident response and recovery phases/sub-phases can be identified. While as a collective, the thirty-one standards and guidelines provide a comprehensive guidance base, should individual resources be used in isolation, a less than complete picture of requirements could be formed and, therefore, misused in practice. Consequently, The following sections provide an analysis of key phases and sub-phases and their coverage across each independent resource.

3.2.1. Methodology

When assessing the effectiveness of current guidance for ICS cyber security response and recovery, relevant requirements must first be identified. During our initial read-through of the selected documents, we identified and extracted response and recovery phases/sub-phases pertaining to RQ2.1 and used them as a base for our analysis. Table 4 takes each of these identified phase/sub-phase and aligns it to a criteria set. Additional criteria of technical and non-technical factors are also included, allowing for a clearer understanding of each resource's target audience. The resources from Tables 1, 2, and 3 were then independently compared against this criteria set, ensuring a structured analysis could be undertaken.

3.2.2. Results

Our analysis results have been compiled into Tables 5 and 6, offering a high-level snapshot of criteria coverage within each resource. In addition, key findings can be broken down across the four primary phases (Planning, Preparation, Mid-Incident, and Post-Incident) as follows:

- **Planning -** The majority of investigated guidance (~80%) discusses the importance of response plan documenting and role and responsibility assignment. There is, however, minimal discussion on Criticality Assessment and Threat Assessment (~53% and ~63% respectively). Also, Risk Management is inconsistently discussed (~53%).

Guidance/Standard	Organisation	References
NCSC Cyber Assessment Framework	NCSC	[110]
DWI Cyber Assesment Framework	DWI	[40, 39]
10 Steps: Incident Management	NCSC	[109]
Security Assessment Principles (SyAPs)	ONR	[118]
Preparation for and Response to Cyber Security Events Technical Assessment Guide	ONR	[120]
HMG Security Policy Framework	HMG	[62]
Operational Guidance 86	HSE	[62]

Table 1: Overview of Selected UK Guidance and Standards

Guidance/Standard	Organisation	References
Nuclear Security Fundamentals	IAEA	[65]
Nuclear Security Series 17	IAEA	[64]
Nuclear Security Series 23-G	IAEA	[66]
Good Practice Guide for Incident Management	ENISA	[66]
Computer Security Incident Response Team FAQ	Carnegie Mellon University	[24]
Incident Handler's Handbook	SANS	[88]
Security Consensus Operational Readiness Evaluation	SANS	[147]
CIS Critical Security Controls	CIS	[30]
SP 800-61	NIST	[29]
SP 800-53	NIST	[116]
Cyber Security Incident Response Guide	CREST	[35]
ISO/IEC 27001/27002	ISO/IEC	[73, 74]
ISO/IEC 27035:2016	ISO/IEC	[71, 72]
IEC 62443 Series	IEC	[67, 68]

Table 2: Overview of Selected Supplementary Guidance and Standards

Guidance/Standard	Organisation	Country	References
ISO/IEC 27019:2017	ISO/IEC	N/A	[75]
RG 5.71	NRC	USA	[117]
NEI 08.09	NEI	USA	[112]
Framework for Improving Critical Infrastructure	NIST	USA	[108]
SP 800-82	NIST	USA	[146]
SP 800-83	NIST	USA	[143]
SP 800-100	NIST	USA	[18]
CIP-008-06	NERC	USA	[113]
REGDOC-2.5.2	CNSC	Canada	[32]
Managing Cyber Security for Industrial Control Systems	ANSSI	France	[9]

Table 3: Overview of Selected International Guidance and Standards

Requirement Type/Phase	Requirement	Criteria
Type	Non-Technical (NT)	Information provided is non-technical.
	Technical (Tec)	Information provided is technical.
Planning	Roles and Responsibilities (RR)	Contains information on assigning/defining roles and responsibilities.
	Response Planning (RP)	Contains information on response plan documenting.
	Criticality Assessment (CA)	Contains information on identifying and assessing key assets and infrastructure in terms of criticality.
	Threat Analysis (TA)	Contains information on conducting a continuous threat analysis for remediating identified vulnerabilities and minimising attack vectors.
	Risk Management (RM)	Contains information on creating and consulting risk management documents.
Preparation	Training (Tra)	Contains information on personnel training - including response team training/awareness training.
	Regular Testing and Auditing (RTA)	Contains information on testing and auditing- this includes red team exercises, penetration tests, and automatic testing.
	Incident Detection (ID)	Contains information on incident detection mechanisms.
Mid-Incident	Resource Availability (RA)	Contains information on resource allocation and accessibility in the event of a cyber incident (physical and non-physical resources).
	Incident Reporting (IRep)	Contains information on reporting incidents to the appropriate personnel (internal/external).
	Incident Containment (IC)	Contains information on procedures that should be implemented for containing the damage caused by an incident.
	Incident Eradication (IE)	Contains information on procedures that should be implemented for eradicating incidents.
	Incident Recovery (IRec)	Contains information on procedures that should be implemented for recovering from an incident.
	Evidence Collection/Handling (EC)	Contains information on evidence collection for use by external authorities.
	Public Relations Management (PRM)	Contains information on public information disclosure management.
Post-Incident	Root Cause Analysis (RCA)	Contains information on post-incident analysis; used to determine the root cause of the incident.
	Lessons Learnt (LL)	Contains information on lessons learnt from past incidents for improving current defensive capabilities.

Table 4: Requirements and Criteria for Document Analysis

- **Preparation -** The need for training is well covered (71%). However, discussion on testing and auditing, in addition to incident detection, is inconsistent (~59% and ~66%, respectively). This may be due to its inclusion within a larger series. For example, The NCSC CAF Objective D does not cover incident detection, as this is covered in Objective C [111].

- **Mid-Incident -** Incident Reporting, Containment, Eradication and Recovery are well covered (~88%, ~69%, ~72%, and ~81% respectively). However, Resource Availability guidance is limited (~34%). This level of coverage is surprising, as most post-incident activities are highly dependent on resource availability. If resources (human and non-human) are incorrectly allocated or unavailable, this can adversely affect an incident's impact. Additionally, Evidence Collection/Handling and Public Relations Management coverage is limited (~31%, and ~19%, respectively). This also is a cause for concern, especially considering the importance of these activities. For serious incidents, the collection and preservation of evidence for authorities is essential. Any accidental tampering of evidence during response and recovery activities could seriously affect the corresponding investigation. Similarly, maintaining an honest and trustworthy reputation with the general public is crucial, as this can affect operations in the long term.

- **Post-Incident -** Although Lessons Learnt are well covered (~66%), phases that directly impact the quality of this remain inconsistently discussed. Without consistent discussion of Root Cause Analysis (~31%), limited guidance is, in reality, available for ensuring that the output from Lessons Learnt is thorough enough.

3.3. Summary

The majority of analysed resources contain high-level details, with only ~54% providing technical guidance. Since ICS implementations can differ between environments, hardware-specific technical guidance is not always recommended. However, due to the subject area's technical nature, a lack of technical guidance may present a challenge for operators during practical implementation.

Through the analysis of our selected resources, and with respect to RQ2.2 and RQ2.3, a lack of consistency has been highlighted. Although the core topics surrounding cyber security response and recovery activities are discussed in most, including Roles and Responsibility assignment and Response Plan Documenting, less-common topic areas, Evidence Collection or Public Relations Management, for example, appear irregularly. Concerns arise where operators are recommended to consult guidance that does not discuss these topics, leading to overlooked critical activities. While our analysis of standards and guidelines allows for operators and researchers alike to better understand the requirements needed to develop a comprehensive ICS cyber incident response and recovery plan as well as identify which publications cover specific topics, the lack of consistency throughout available guidance highlights the need for amalgamation into a single resource, which operators can consult; ensuring complete coverage.

Having provided an analysis of a broad literature base to identify the current state of the art guidance for cyber incident response and recovery, the following sections detail the creation of synthetic cyber attack scenarios applied to a set of interviews with industry stakeholders. This provides a picture of current real-world practices and how the gaps identified in the resources discussed here can affect incident response and recovery capabilities in practice. Our goal for this is to establish a base from both theory (standards and guidelines) and practice (stakeholder interviews) for use in the creation of our framework; detailed in Section 7.

4. Synthetic Scenario Development

To support engagement with industry stakeholders (see Section 5) and avoid findings being tied directly to real-world infrastructure, creating realistic synthetic attack scenarios is required. This presents a generalisable foundation on which all participants can openly discuss their approaches to cyber incident response and recover while ensuring neither the research team nor the participant cross sensitive information boundaries. Discussion of these scenarios also enables interview participants to discuss how specific guidance and guidelines, discussed in Section 3, could positively or negatively affect ICS cyber incident response and recovery activities. The construction of these scenarios is outlined over the following subsections.

4.1. Overview of Historical Attacks

A set of historical attacks was reviewed to contextualise better the risk posed to ICSs and create realistic synthetic cyber attack scenarios for use in our stakeholder engagement. These ranged from simplistic co-

	Type		Planning					Preparation		
Guidance/Standard	**NT**	**Tec**	**RR**	**RP**	**CA**	**TA**	**RM**	**Tra**	**RTA**	**ID**
SyAPs (ONR)	✓		✓	✓	✓	✓	✓	✓	✓	✓
TAG (ONR)	✓		✓	✓	✓		✓	✓	✓	✓
CAF - Objective D (NCSC)	✓		✓	✓	✓		✓	✓	✓	
10 Steps: Incident Management (NCSC)	✓		✓	✓			✓	✓	✓	
OG 86 (HSE)	✓	✓	✓		✓		✓			
Security Policy Framework (HMG)	✓				✓	✓	✓			✓
CAF (DWI)	✓		✓	✓	✓		✓	✓	✓	
Cyber-Security Incident Response Guide (CREST)	✓	✓		✓	✓	✓				✓
Good Practice Guide for Incident Management (ENISA)	✓		✓	✓			✓			
Nuclear Security Fundamentals (IAEA)	✓		✓	✓	✓			✓	✓	✓
NSS 17 (IAEA)	✓	✓	✓	✓	✓	✓	✓	✓		
NSS 23-G (IAEA)	✓	✓	✓	✓			✓	✓	✓	
IEC 62443 (Parts 2-1 and 4-2)	✓	✓	✓	✓				✓	✓	✓
ISO/IEC 27001/27002	✓		✓	✓		✓			✓	
ISO/IEC 27035	✓	✓		✓		✓	✓	✓		✓
ISO/IEC 27019	✓		✓	✓		✓			✓	
RG 5.71 (NRC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NEI 08.09	✓	✓	✓	✓		✓	✓	✓	✓	✓
NIST Framework	✓		✓	✓	✓	✓	✓	✓	✓	✓
NIST SP 800-53	✓	✓	✓	✓		✓	✓	✓	✓	✓
NIST SP 800-82		✓		✓		✓				✓
NIST SP 800-83	✓	✓		✓		✓		✓		✓
NIST SP 800-61	✓	✓		✓		✓		✓		✓
NIST SP 800-100	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CIP-008-06 (NERC)	✓		✓	✓	✓				✓	✓
CSIRT FAQ (Carnegie Mellon University)	✓		✓	✓		✓		✓	✓	
Incident Handler's Handbook (SANS)	✓	✓	✓	✓	✓			✓		✓
SCORE (SANS)	✓	✓	✓	✓		✓				✓
Critical Security Controls (SANS)	✓		✓	✓		✓		✓	✓	✓
REGDOC-2.5.2 (CNSC)	✓	✓	✓	✓	✓	✓		✓	✓	✓
Managing Cyber Security for ICS (ANSSI)	✓	✓	✓	✓	✓	✓	✓	✓		✓

Table 5: Document Analysis Results (Part One)

incidental malware infections to more sophisticated targeted attacks. While there exist many a discussion across media outlets concerning cyber attacks targeting ICSs, many of these describe generic scanning tool traffic seen on the Internet. For this reason, the attacks listed here were more focused, with evidence of witnessed impact. Each contains a common name, year of occurrence, confirmed/suspected threat actor, and high-level method/s of attack and have been detailed in Table 7. In some instances, insufficient information is available to suggest attribution.

Using our investigation of these historical attacks, we derive the following key attributes, setting out areas for exploration in the development of synthetic scenarios.

4.1.1. Nation State

As nation-states appeared across sixteen of the twenty-nine historical attacks, including a level of sophistication into the proposed scenarios accounting for the complexity achievable by a nation-state is of great importance. Their potential ties across historical events demonstrate motivation in the targeting of ICSs.

	Mid-Incident							Post-Incident	
Guidance/Standard	**RA**	**IRep**	**IC**	**IE**	**IRec**	**ECH**	**ERM**	**RCA**	**LL**
SyAPs (ONR)	✓	✓							
TAG (ONR)		✓	✓	✓	✓	✓			
CAF - Objective D (NCSC)	✓	✓	✓	✓	✓			✓	✓
10 Steps: Incident Management (NCSC)	✓	✓			✓				✓
OG 86 (HSE)	✓	✓	✓	✓	✓			✓	✓
Security Policy Framework (HMG)		✓				✓			
CAF (DWI)	✓	✓	✓	✓	✓				✓
Cyber-Security Incident Response Guide (CREST)	✓	✓	✓	✓	✓			✓	✓
Good Practice Guide for Incident Management (ENISA)		✓							
Nuclear Security Fundamentals (IAEA)	✓								
NSS 17 (IAEA)					✓				
NSS 23-G (IAEA)		✓				✓	✓	✓	✓
IEC 62443 (Parts 2-1 and 4-2)		✓	✓	✓	✓				✓
ISO/IEC 27001/27002		✓	✓	✓	✓	✓			✓
ISO/IEC 27035		✓	✓	✓	✓				✓
ISO/IEC 27019		✓	✓	✓	✓	✓			✓
RG 5.71 (NRC)		✓	✓	✓	✓		✓	✓	✓
NEI 08.09		✓	✓	✓	✓				✓
NIST Framework	✓	✓	✓	✓	✓		✓	✓	✓
NIST SP 800-53		✓	✓	✓	✓		✓		
NIST SP 800-82			✓	✓	✓				
NIST SP 800-83		✓	✓	✓	✓	✓		✓	✓
NIST SP 800-61		✓	✓	✓	✓	✓		✓	✓
NIST SP 800-100)		✓	✓	✓	✓				✓
CIP-008-06 (NERC)		✓				✓		✓	✓
CSIRT FAQ (Carnegie Mellon University)	✓	✓	✓	✓	✓		✓		✓
Incident Handler's Handbook (SANS)	✓	✓	✓	✓	✓	✓			✓
SCORE (SANS)		✓	✓	✓	✓	✓	✓	✓	✓
Critical Security Controls (SANS)		✓	✓	✓	✓				
REGDOC-2.5.2 (CNSC)		✓	✓		✓				
Managing Cyber Security for ICS (ANSSI)					✓				

Table 6: Document Analysis Results (Part Two)

4.1.2. Insider Threat

- While insider threats appeared in just seven of the twenty-nine historical attacks, their ability to allow for the circumvention of security controls and value from a process comprehension perspective (i.e. "the understanding of system characteristics and components responsible for the safe delivery of service (e.g. treatment of water). This includes all relevant physical and computational attributes.") [52], makes them a significant threat in even the most complex and secure environments. Therefore, accounting for their ability to aid an attack should be considered within the proposed scenarios.

4.1.3. Purely Technical and Socio-Technical

- All attacks contain a technical component. This could be the exploration of a system vulnerability, exfiltration of data, etc. However, the prevalence of attacks containing social components (i.e. social engineering) has increased over recent years. In a similar way to insider threats, the exploitation of individuals can be used to circumvent technical controls, particularly a system's perimeter. Therefore, social vulnerabilities, alongside purely technical vulnerabilities, should

Attack Name	Year	Threat Actor	Attack Method	Reference(s)
Gazprom	1999	Insider	Technical	[103, 105, 115]
Maroochy Water System	2000	Insider	Technical	[139, 103, 15, 114]
California Independent System	2001	Nation State/Criminal Organization	Technical	[49, 153, 103, 104]
Red Worm Controller Crash	2002-2003	Unknown	Technical	[156, 152, 102, 93]
Slammer Worm	2003	Insider	Technical	[82, 103, 105, 114, 45, 27]
SoBig Virus	2003	Spammers	Email/Technical	[2, 103, 126]
Nachi (Welchia) Virus	2003	Unknown	Technical	[156, 142]
Zotob Worm	2005	Criminal Organisation	Technical	[14, 17, 56, 17]
Browns Ferry Nuclear Plant	2006	Unknown	Technical	[114, 82, 94]
Tehama-Colusa Canal Authority	2007	Insider	Technical	[103, 154, 114]
City Tram Attack	2008	Prankster	Technical	[13, 3]
Spies in US Power Grid	2009	Nation State	Technical	[114]
Dallas Hospital HVAC	2009	Insider	Technical	[114, 4, 159]
Night Dragon	2009	Nation State/Criminal Organization	Email/Technical	[101, 114]
Stuxnet	2010	Nation State/Insider	USB/Technical	[103, 46, 95, 144]
Duqu	2011	Nation State	Technical	[103, 28]
Flame	2012	Nation State	USB/Technical	[103, 164, 21, 5]
Shamoon	2012	Nation State/Hacktivist	Technical	[166, 123, 19]
Havex	2013	Nation State	Email/Technical	[60, 115, 148, 161]
Blackenergy	2014	Criminal Organization	Email/Technical	[84, 81, 84]
German Steel Mill	2014	Unknown	Email/Technical	[100, 92, 91]
Ukraine Energy	2015	Nation State	Email/Technical	[96, 165, 41]
CrashOverride	2016	Nation State	Email/Technical	[54, 38]
Shamoon 2	2016	Nation State/Hacktivist	Email/Technical	[80, 150]
Wolf Creek	2017	Criminal Organization/Nation State	Email/Technical	[99, 124, 132, 58]
Triton/Petro Rabigh	2017	Criminal organization/Nation state	Technical	[78, 6, 87]
U.S. Utility Sectors	2018	Criminal Organization/Nation State	Email/Technical	[141, 149]
Norsk Hydro	2019	Unknown	Technical	[1, 155, 151]
Triton	2019	Criminal Organization/Nation State	Technical	[55, 6]

Table 7: Overview of Historical Attacks

be included within the proposed scenarios.

There were at least one or more intended attack effects that the attacker, or attack group, was pursuing within each attack. Here the chosen effect terms are aligned with those provided by Rid [131].

4.1.4. Espionage: Data Exfiltration

- Across many of the historical attacks, there exists an element of espionage, that is, to extract useful information. Information acquisition might be the ultimate desired effect of the attacker or act as a precursor to other attacks. There is considerable value to the information held on ICS networks. For example, chemical process information for the manufacture of complex compounds.

4.1.5. Sabotage: Denial of Service (DoS)

- While often considered simplistic in execution, the impact of denial of service (DoS) attacks can be significant. As the level of knowledge required to execute a successful DoS is lower than operational process manipulation, it becomes obtainable to a broader range of threat actors (i.e. low and high skilled). Here, sabotage is defined as an observable destructive act that prevents ICSs from functioning as intended. Additionally, acts of sabotage have a lower barrier to enact than acts of subversion. Therefore, its inclusion within the proposed scenarios presents an alternate, widely applicable objective.

4.1.6. Subversion: Operational Process Manipulation

- Subversion is the act of subtle process disruption (operational process manipulation), which is difficult to detect and may not result in the ultimate destruction of operational equipment. The level of process comprehension required to achieve targeted operational process manipulation is high [52]. However, where historical attacks highlighted the inclusion of nation-state or insider threat actors, the ability to achieve this can be realised. The proposed scenarios should, where possible, also look at options for the manipulation of operational processes by lower-skilled threat actors. This would allow for a broader perspective to be obtained around more strategic, targeted attack objectives.

The baseline requirements derived through this investigation of historical cyber attacks form a key starting point in developing synthetic scenarios. However, to ensure they remain valid at a practical level and to better understand their technical construct and execution, they must be developed in a safe/controlled environment. This is discussed in the following section.

Techniques Used	**Tools Used**
Brute Forcing	Wireshark
Enumeration	Nmap
Exploitation	Metasploit
Lateral Movement	Snap7 (Python Library)
Social Engineering	Custom Scripts
Data Injection	Burp Suite
DoS	
Command and Control	
Device Reconfiguration	
Data Exfiltration	

Table 8: Techniques and Tools Used for Scenario Development

4.2. Testbed Proof of Concept

Over the last eight years, Lancaster University has developed a comprehensive ICS testbed environment [53, 51]. To summarise, it has been constructed through the procurement and implementation of physical, real-world hardware and software produced by major ICS vendors, including Siemens, Schneider, Allen Bradley, and ABB. This has been leveraged in the physical testing and subsequent construction of our synthetic scenarios outlined in Section 4.3, achieved through the practical development and deployment of each attack. This activity was undertaken to solidify our synthetic scenarios' realism further and develop a better understanding of their practical end-to-end execution should it be questioned during the interview process. Table 8 presents, at a high-level, the fundamental techniques applied across the development of our synthetic attack scenarios and the tools used to deliver these techniques.

During the practical development of each attack, we explored the devices in use to identify new vulnerability which could be exploited to achieve an impact similar to those observed in historical attacks. This resulted in the discovery of two Zero-Day vulnerabilities. These have been appropriately disclosed to the vendors in question. In addition, for ethical reasons, we will not opensource the attack code developed as part of this exercise.

4.3. Synthetic Scenarios

The following diagrams and supporting text provide an overview of our baseline synthetic system architecture, onto which the attack scenarios are applied, including the core operational functionality delivered at a device level. Each attack scenarios is broken down into stages, depicted through the use of high-level attack paths.

4.3.1. Baseline Infrastructure

Figure 2 presents our simplified ICS baseline infrastructure. This includes a set of devices and mapped to the Purdue model colour scheme (see Figure 1).

The Sensors and Actuators within our baseline infrastructure are hardwired to the Programmable Logic Controller (PLC), operating using traditional electronic signalling (i.e. current/voltage based). We exclude the use of protocol-based sensors (e.g. Profibus, WirelessHART, EthernetIP) to simplify this layer of the infrastructure, as it does not form a core component of our attack scenarios.

The PLC is a Siemens ET200S [137]. This device interacts with the sensors and actuators autonomously through pre-defined control logic and manually via human interaction with the Human Machine Interface (HMI) and centralised Supervisory Control and Data Acquisition (SCADA) system.

The HMI is a Siemens KTP700F [138]. This device is responsible for the localised monitoring and control of operational processes via the PLC.

The Remote Terminal Unit (RTU) is a Schneider SCADAPack32 [136]. This device is responsible for collecting and forwarding critical sensor data to the centralised SCADA system from the PLC.

The Data Historian is a Windows 7 workstation running Kepware [128]. This device is responsible for collecting and forwarding operational data from the PLC to the Data Analytics system.

The router is a PEPWave [122], and the switch is a Westermo Lynx [162]. These devices are responsible for passing data between each of the Cell/Area Zone devices and the data-centre. While the switch acts passively, the router enforces basic security controls by filtering traffic between its local and remote interfaces. This filtering comes in the form of a rule-set allowing the Centralised SCADA and Data Analytics systems to communicate with any device across the Cell/Area Zone. All other communications are blocked.

The centralised SCADA is a Windows Server 2016 based system running Schneider's ClearSCADA [135]. This application collects and depicts data from the RTU. Its primary purpose is operational alarm generation.

The data analytics systems operate on Ubuntu Server 18.04, running ThingWorx [69]. This application collects, augments, and depicts data from the Data Historian. Its primary purpose is the delivery of in-depth analytical and processing capability of operational data.

The two workstations run Windows 7 and have access to the Data Analytics and Centralised SCADA systems via their web interfaces. One of the two workstations (lighter shade of blue) also operates a client application (ViewX [135]), allowing for a greater level of interaction with the Centralised SCADA system. There are no network-level security controls between these four systems.

4.3.2. Synthetic Reference Scenario One: Technical - Espionage and Sabotage

The following points describe each stage of attack scenario one. These have been developed and tested within our testbed environment, harnessing tooling described within section 4.2:

- Stage 1: Compromise router through the use of password brute-forcing. Once accessed, leverage existing VPN configuration functions and reconnect as a trusted user.
- Stage 2: Enumerate devices on the Cell/Area Zone network. Where possible, extract relevant data (e.g. device configuration and process control logic) for offline analysis.
- Stage 3: Take external monitoring systems offline (i.e. RTU and Data Historian).
- Stage 4: Take the PLC offline.

4.3.3. Synthetic Reference Scenario Two: Socio-Technical - Subversion

The following points describe each stage of attack scenario three. Each stage has been developed and tested within our testbed environment, harnessing tooling described within section 4.2:

- Stage 1: Setup an HTTPS listener on a public-facing system. Send an email to a workstation user containing a malicious file. Once opened, an HTTPS session back to the attacker will be established.
- Stage 2: Via the HTTPS session, leverage the compromised user's access to interact with the Centralised SCADA system using its associated client application.
- Stage 3: Via the HTTPS session and access to the Centralised SCADA system, use the inbuilt capability to control the PLC, resulting in operational impact.

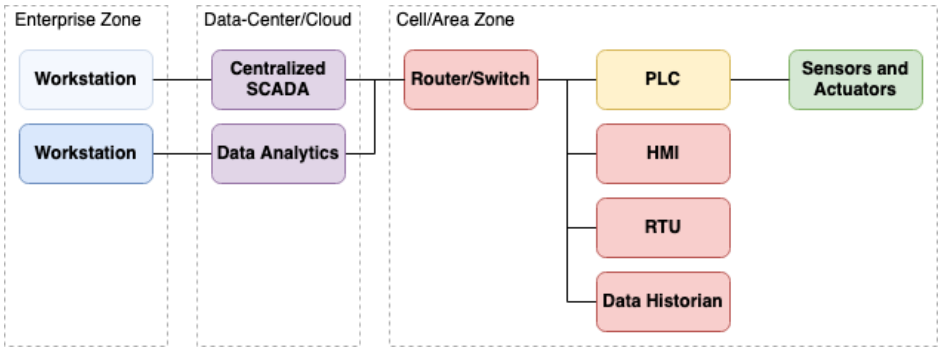

Figure 2: Core Infrastructure

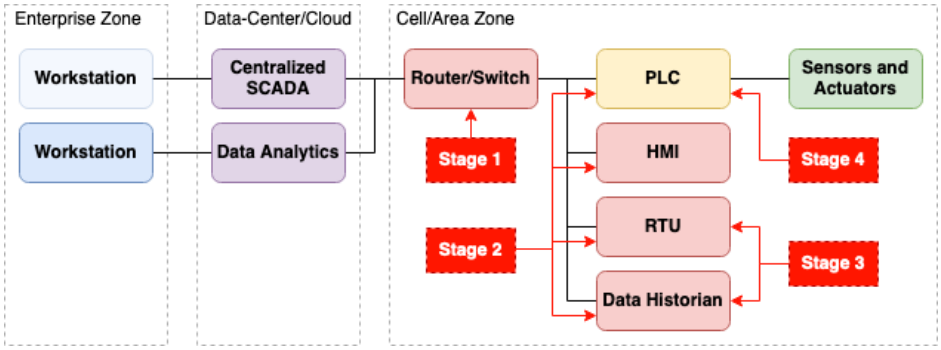

Figure 3: Scenario 1

4.4. Summary

The synthetic attack scenarios described across the previous sections were presented at an abstract level. When transforming these for inclusion in the subsequent interviews, the level of detail required may increase supporting participant understanding. In addition, it may be appropriate to provide evidence of the tooling used during our testbed proof of concept activities, to further participant's depth of understanding around each stage of an attack's execution.

While the testbed itself has been reviewed to ensure it accurately represents a real-world system through the practical development of each scenario affords a high degree of confidence in applicability to a real-world context, we sought additional validation through informal engagement with industry experts. We approached five experts with experience in the field of cyber security consultancy. Each expert was presented with the synthetic scenarios and asked to provide comments on their practical applicability to real-world systems. We explained how these had been tested using real-world hardware and software in our testbed environment and how the use of exploits targeting Zero-Day vulnerabilities had been appropriately disclosed. Besides minor changes to the terminology used to describe each scenario, they were accepted as good working examples of attacks that could be executed against an ICS environment.

The following section describes how the developed synthetic scenarios have been utilised in a series of interview with industry stakeholders to stimulate discussion on cyber incident response and recovery processes and the use of standards and guidelines in practice; discussed in Section 3.

5. Stakeholder Engagement

The following subsections provide an overview of an empirical study with industry stakeholders operating/regulating elements of European CNI. Using semi-structured interviews and synthetic cyber attack scenarios, this study explores current cyber incident response and recovery practices, the adoption of existing standards and guidelines, and challenges in their use. The goal of these interviews is to further investigate the findings from Section 3 and to assess whether the challenges from using standards and guidelines are observable in

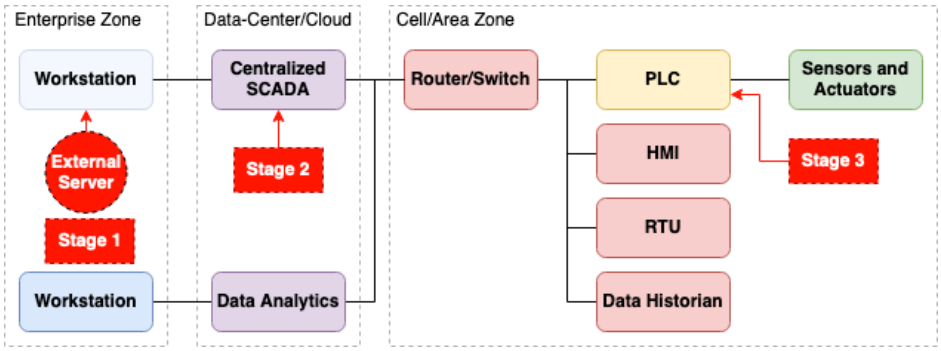

Figure 4: Scenario 2

practice. Our research questions reflect this, and are as follows:

- RQ3.1: How extensive is the use of standards and guidelines in practice?
- RQ3.2: How do operators use standards and guidelines in their incident response and recovery capabilities?
- RQ3.3: What challenges do operators face when making use of standards and guidelines in their incident response and recovery processes?

5.1. Methodology

In search of appropriate research techniques, interviewing key stakeholders working across the topic area was applied. A simple ethnographic observation would prove extremely challenging and time-consuming, particularly when considering the sensitive nature of systems and processes being evaluated and the requirement to seek approval from both participants and the organisation in which they work. Interviewing was selected as an appropriate alternative [121], enabling each participant to discuss response and recovery activities without direct reference to a specific organisation or system. The ability to explore meanings, routines, behaviours, etc. [133] all adds towards appropriate focusing, particularly when discussing complex topics, and confirmation of meaning from both parties (the interviewer and interviewee) may also be required [23].

Interviewing typically falls within three core categories, viz. structured, semi-structured, and unstructured. Here a semi-structured approach has been adopted, often seen as the most common form of qualitative research methods. This approach provides adequate flexibility with a pre-defined core question set, options to include improvised follow-up questions, and explore meanings should they be required [11]. Where existing cyber incident response and recovery guidance discussed across Section 3 highlighted deviations in provided detail, the possibility of a repeat scenario was considered in the selection of an interviewing technique. The flexibility offered through a semi-structured approach presents significant benefits, allowing for additional probing where little detail is provided and further exploration of more comprehensive approaches where required. The following sub-sections break down points considered through the application of this approach.

5.1.1. Sample

In selecting an appropriate participant sample, the aim is to understand the topic area from all relevant perspectives. To achieve this, a broad approach to the targeting of participants was applied. This resulted in a diverse collection of role-profiles. More specifically, those engaging in cyber incident response and recovery processes across multiple systems, with varying levels of responsibility. This sampling approach provides multiple perspectives, building a broader picture of how cyber incident response and recovery activities are conducted.

To summarise, we selected eight participants holding the following roles:

- Chief Information Security Office (x2)
- Operational Technology Manager
- Information Technology Manager
- Information Assurance Manager
- Engineering Delivery Manager
- Emergency Arrangements Coordinator
- Operational Technology Software Engineer

- Operational Technology Cyber Security Inspector

The levels of experience varied amongst participants within each of the defined roles. The majority of which, however, had been working with industrial systems for over ten years.

5.1.2. Threats to Validity

The work of Campbell & Stanley [22] discusses common threats to the validity of the collected data. To address these issues, attention was initially focused on the participant sample, as previously discussed. From this, interviewing techniques applied to build rapport, trust, and openness were adopted, with questions covering all relevant topics and those topics alone (i.e., no irrelevant questioning). As this set of interviews is designed to complete orientation on cyber incident response and recovery, included questions were drawn from initial understandings achieved through the analysis of standards and guidelines in Section 3.

Where Powney & Watts [127] discuss the emergence of interesting content upon completion of interviews (i.e., when the recorder is switched off), notes were taken and added to the interview protocol/guide. Subsequently, additional prompts were included for potential re-interviews of the same interviewee, for inclusion within other interviews, or simply as salient content worth exploring as part of further focusing efforts. This approach allowed the interview process to evolve in a structured and managed way while eliciting pertinent information.

5.1.3. Reliability

Of primary concern to the reliability of collected data is interviewer bias. This is the ability to trust that findings are not derived from research instruments or as a result of an interviewer's quirks and improvisations. Concerning this is the perspective of "insiders". Insiders can be defined as interviewers who share similar cultural, ethnic, linguistic, national, and religious heritage to interviewees [47]. More simply, where the interviewer and interviewee are part of the same organisation (i.e., work colleagues) [11]. This can prove highly valuable when seeking additional participants, understanding organisational structures, etc. [11]. However, it can also increase the risk of data reliability issues, with a higher probability of assumptions and general interviewer bias, based on an interviewer's perspective of "the way things are". While the research team may or may not be considered insiders by these standardised definitions, having collectively spent over thirty years working for CNI operators, we too have our perspective on "the way things are", from organisational culture to policies, power relationships, etc. The positive attributes of these experiences were utilised in the interview protocol/guide design. However, to account for the possibility of negative attribute inclusion, this guide was read and understood by all project members prior to the start of interviews.

Rubin & Rubin [133] refers to transparency and consistency; this accounts for consistency and evidence of inevitable inconsistencies in data. These were appropriately handled and included within the analysis phase.

Neutrality beyond the aforementioned "insider" bias was also considered throughout the interview protocol/guide design process and during each interview. As an interviewer, acknowledgement of personal background, age, class, etc., can all influence an interview's direction and output.

5.1.4. Primary Practical Technique (In-Person Interviewing)

In-person interviewing provided the mechanism for engagement, as this allowed for clear and in-depth data collection. This interviewing technique provides additional information compared to remote interviewing, mainly due to facial expressions and visual cues. In-person interviews can also be considerably longer than remote interviews since participants have provided greater commitment to participate and are less likely to be distracted during the interview process [11].

5.1.5. Interview Protocol/Guide

Each interview was broken down into the following six stages, providing a logical structure to the interview protocol/guide:

- Preface
- Establishing Demographics
- Scenario Familiarization
- Response and Recovery Analysis
- Guidance Analysis
- Conclusion

The core focus of these interviews was to build upon Section 3, providing a broader understanding of cyber incident response and recovery practices within an ICS context. More specifically, how key stakeholders broach cyber incidents. Taking direction from Section 3, the questions aligned to these interview stages

are aided through the inclusion of probes and definitions. Due to time limitations, additional probes were only used to provide a greater depth of understanding to directly-related, salient points of discussion. The following provides a summary of primary interview questions. Our complete protocol/guide can be found on Github [90].

Establishing Demographics
The following question-set was applied to the demographics phase.

- Please can you tell us your job title and provide a very brief overview of your core roles and responsibilities?
- How many years of experience do you have working in this role?
- At a high level, please can you explain to us what you understand the term Response and Recovery to mean within the context of an Operational Technology (Industrial Control Systems) cyber security incident?

Response and Recovery Analysis
The following question-set was applied during the response and recovery analysis phase, once the participant had been shown the first synthetic cyber attack scenario. Upon completing these questions, the participant was then shown the second scenario and asked if anything would be done differently.

- Given your role in the organisation, at a high level, what are the core steps you would go through as part of response and recovery operations in the example scenario?
- How many individuals within the organisation would work directly with you on these steps, so performing the same role as you?
- Who else would you have direct engagement with during response and recovery processes?
- How many individuals across the organisation would be involved in response and recovery operations more generally speaking?
- When undertaking a response and recovery operation to this scenario, what do you consider the primary goal to be?
- When you are undertaking individual response and recovery actions, how do you factor in risk evaluation as part of the decision-making process?
- Typically, what are the expected outputs post-incident, once you have appropriately recovered from an incident and everything is back to normal?

Guidance Analysis
The following question-set was applied during the external guidance analysis phase.

- In your opinion, which standards or guidelines best cover response and recovery in relation to Operational Technology cyber-attacks?
- As a final question, what is your opinion on currently available standards and guidelines within the context of cyber incident response and recovery?

Conclude
The following question was applied during the conclusion phase.

- Would you like to add anything which may be relevant?

5.1.6. Analysis

In search of an appropriate methodology by which captured interview data could be analysed, template analysis was selected. Also referred to as "codebook analysis" and "thematic coding", template analysis offers a highly flexible method to the analysis of qualitative data [86]. Sitting between the relatively rigid approach of content analysis in which analytical codes are all pre-defined [130], and the opposite approach of grounded theory in which all analytical codes must be derived from the data [48]. This approach was initially conceived by Crabtree & Miller [34], and was later adopted by King et al., [86], from which it saw an increase in adoption across a variety of fields. Considering participant numbers and their diverse roles, the flexibility offered through template analysis provided significant value over alternative approaches, allowing us to create an initial code-set aligned to core areas of interest, with relevant additional codes added as they emerged.

While template analysis has fewer specified procedures, offering greater flexibility to statistical and qualitative analysis of the same data, recommendations are proposed by King et al., [86], these were followed within the analysis of interview data here. For example, through the use of the previously described interview protocol/guide, an initial code-set was constructed but was limited to allow for further granularity or abstraction if required. Where too many pre-defined codes may constrain/confuse analysis, too few may cause a lack of direction. Undertaking a brief review of initial

transcripts allowed additional codes to be added. This helped us build confidence in the code-set before starting the complete data codification.

5.2. Results

Key findings from the interviews with stakeholders are summarised here. These have been grouped based on identified themes and key points of interest. It is worth emphasising that all of the points discussed here have been identified from the contents of the interviews. These, therefore, reflect the generalised opinions of participants but may differ from person to person. A detailed narrative of these key points can be found in Appendix B.

1. Primary Goals of R&R:
    - Make the system safe.
    - Preserve evidence during response and recovery actions.
    - Establish communications between relevant parties.
    - Make appropriate decisions for providing safety, security and business continuity based on the specifics of the incident.
2. Key Phases and Tasks:
    - Incident identification (system error, or cyber attack ..?).
    - Escalate the incident to management.
    - Form an Incident Response Team.
    - Log response decisions and actions.
    - Collect evidence while preserving safety.
    - Engage in response actions such as examining logs, isolating impacted systems, removing external connectivity etc.
    - Review logs and forensic data after the incident.
    - Conduct internal review for lessons learned and communication with legal or regulating organisations.
3. Risk Evaluation:
    - Ensure decisions are made quickly.
    - Engage with subject-matter experts with full understanding of the associated risks.
    - Use formal risk evaluation procedures for specific scenarios; and semi-formal decision making based on collective agreement otherwise.
    - Follow formal processes for dangerous actions.
    - Exercise regularly to pre-emptively capture as much as possible of the risk that could arise.
4. Human Capital:
    - Organisation structure adjusted and accounted for loss of coverage.
    - Every individual on site should be at the disposal of the response team during an incident.
    - Possibility to pull in additional resources from external organisations.
    - If an incident is critical enough to affect multiple sectors, regulatory bodies and government could convene to decide upon the best course of action.
5. Use of Standards and Guidelines:
    - There are generally mixed opinions on this topic.
    - Some considered them to have matured over recent years, while others believe they are too focused on one specific domain and are inefficient.
    - Prevalence of existing standards and guidelines felt to be limited.
    - Organisations responsible for providing guidance (NIST for example) were generally mentioned, as opposed to specific standards and resources.
    - No approaches were identified from academic work.
    - Awareness of standards and guidance was limited prior to the period 2011-2021.
    - Reluctance to reinvent from the ground up when resources already exist.
    - No single resource was deemed appropriate for all aspects of incident response and recovery.
    - OT-based participants believed that existing resources lack tooling and frameworks to adequately cover OT.
    - Participants with an IT background raised questions around the requirement for independent guidance, stating similarities that exist between concepts from both IT and OT domains. This led to an unnecessary separation and isolation of guidance, resulting in a counter-productive use of time and resources.

- Volume and depth of existing resources raised concerns from a usability perspective and could result in inconsistencies.
- Training derived from standards and guidelines could be of benefit.

5.3. Summary

Across the previous sections, we have outlined the methodology applied to a set of interviews with individuals working in and around ICS from both IT and OT backgrounds. This included a pre-defined question-set, allowing for a degree of flexibility through semi-structured in-person interviews. The output of which was analysed using template analysis, a suitable technique given the nature of our research objectives.

During each interview, several themes emerged, covering key topics from existing response and recovery practices to the level of internal and external personnel engagement and opinions/use of existing standards and guidelines within a response and recovery context. These, along with findings from our initial analysis of existing standards and guidelines in Section 3, will be discussed in more detail across the following section.

6. Discussion

The following discussion is broken down into existing standards and guidelines and engagement with industry stakeholders. These two studies, the former focusing on the theory behind incident response and recovery and the latter focusing on its implementation in practice, offer input into improving ICS cyber incident response and recovery capabilities. The goal of these studies was to identify the challenges faced when using standards and guidelines documents to improve and/or assess ICS cyber incident response and recovery capabilities. These findings are summarised here.

6.1. Guidance

The analysis of existing guidance across Section 2 captured thirty-one resources in total. This was made up of both UK and International standards and guidelines from governmental organisations (NCSC, NIST, HSE, DWI, NRC, CNSC and ANSSI); non-statutory organisations (ONR and NERC); international organisations (ISO/IEC, ENISA and IAEA); educational institutions (Carnegie Mellon University and SANS); and industry institutions (NEI and CREST).

This vast array of material demonstrates an abundance of guidance ICS operators can consult towards developing their own internal processes and overall capability. Furthermore, it was found that these resources are often interwoven with one another, acting as key multi-directional reference points.

Our analysis of the thirty-one identified resources found a lack of consistency in the breadth of content when aligned to a holistic criteria set (See Tables 4, 5, and 6). While consulting a single resource could lead operators to review multiple additional cited resources, this may not always be possible. Paywalls, for example, can impact accessibility to cited resources. Furthermore, where baseline information is included around a specific cyber incident response and recovery phase, it may be misunderstood as complete, with additional cited materials considered optional.

The adoption of processes supporting cyber incident response and recovery can be both technical and/or procedural in nature. While guidance must adapt to its intended audience (e.g. non-technical managerial positions versus engineer-level security specialists), it is also vital that topics are covered at an appropriate level of detail to enact meaningful paths of progression. In reviewing existing resources for technical versus non-technical content, we found several instances where the required level of technical detail was limited or not present. We acknowledge the value of non-technical discussion in conveying critical concepts; however, implementation can be challenging without supporting technical specifications and direction.

A wealth of information can be found across the resources reviewed here. However, the isolated selection of a single resource to drive change within an organisation will likely result in a less than complete picture. The quantity of available resources also presents a challenge for operators. How does an operator know they have selected the most comprehensive resource or set of resources? Beyond regulatory interaction, how does an operator know they have implemented cyber incident response and recovery processes at an appropriate level of technical depth? Without a clear overview and understanding of a broad resource pool, as provided here, answering these questions can present a significant challenge.

6.2. Stakeholder Engagement

During our initial demographic question base, it was established that most participants had only ever worked in an industrial sector. Career opportunities to develop pathways into specific technical and managerial roles were commonplace. The in-house/in-sector development of personnel is logical; however, it can lead to isolated viewpoints without external engagement. While

external engagement can be a challenge due to the justifiably closed nature of operational facilities, engagement with relevant third parties can prove to be highly valuable when developing holistic cyber security capability.

Some participants described the in-house development of tailored cyber incident response and recovery approaches. It is unclear on the level of external engagement being undertaken to obtain a third-party viewpoint. However, it was noted by several participants that reinventing the wheel is undesirable, and taking input from existing standards and guidelines is a preferred approach, with internally developed approaches using well-known materials (e.g. from NIST). This provides confidence and credibility to the development of tailored internal guidance.

The processes outline towards a central incident response team's formation, and operations were well understood by all participants. The ability to leverage all internal, and bespoke external resources where necessary, appeared almost limitless, with contracts in place to support every eventuality. Given the cause-agnostic nature of central incident response team processes, a clear understanding of procedures/requirements allowed for a smooth, well-orchestrated establishment process. The level of internal resources to support cyber incidents from an OT perspective was unclear with all participants; this could cause delays in identifying an attack's progression and maturity but would not cause significant challenges in reacquiring control and, therefore, the integrity of systems from a safety perspective.

During response and recovery activities, the documentation of system state, decision-making processes, actions, and their subsequent effect, were well described by all participants. The value of documenting actions during an incident was clearly articulated, from future use during legal or regularity challenges, to root cause analysis/the technical understanding of how an event occurred. Having such a comprehensive approach supports not only an understating of how something happened but what can be done to mitigate a similar event occurring in the future and what decisions helped/hindered response and recovery efforts. Findings of this nature can be fed into future hypothetical exercises and overarching processes to enhance skill-sets and an organisation's overall ability to effectively respond and recover to previously unseen incidents.

When considering the evaluation of risk during response and recovery decision making, a semi-formal approach based on input from a broad range of experts was adopted. While this was focused mainly on the implication actions could have on safety, they also considered environmental impact, forensic data integrity, and reputational damage. Formal evaluation techniques were applied to specific scenarios, where a situation dictates a requirement for personnel to enter potentially hazardous areas, for example. However, it was deemed impractical in a time-critical situation to cover every eventuality, thus opting for a semi-formal, cause agnostic, expert input-based approach.

Regarding the research questions posed in Section 5, there existed some conflicting views on standards and guidelines, with IT-focused participants stating that they could see direct similarities between IT and OT tailored resources, whereas OT focused participants believed them to be too information focused (as opposed to function-focused), their value was considered significant towards maturing existing cyber security processes. This was echoed throughout with a desire to take existing, proven approaches rather than reinvent them from the ground up.

Lessons learnt from an OT cyber security perspective appeared less mature than other areas. This is unsurprising due to its relatively recent formation when compared with conventional engineering and safety-focused cases. The involvement of individuals with a broad range of skill-sets within central incident response teams, and subsequent follow-up lessons learnt, is currently the closest way to comprehend OT focused aspects, with input from security and engineering personnel. The use of lessons learnt reports within cyber exercising could also be seen as a pathway to the overall development and understanding of cyber security challenges across an organisation.

The engagement from participants in internal and national-level cyber incident exercising can be seen as a positive step in developing capability and overall preparedness. Although some operators are mandated to perform exercising, some of the participants engaged voluntarily. This commitment forms the most practical route to test new cyber-focused response and recovery practices, whether derived from standards and guidelines or lessons learnt.

6.3. Summary

Sections 3 and 5 have provided a window into cyber security incident response and recovery guidance, alongside a high-level overview of processes adopted by operators. In extending the scope of Section 5 to capture opinions on existing guidance, an understanding of how they are currently viewed and used in practice has been provided.

While significant effort has been invested by reputable organisations in the creation and continued evo-

lution of guidance to support operators develop cyber security incident response and recovery capabilities, its uptake could be improved. The volume of guidance, its intertwined nature, and varying levels of scope present three primary challenges in its adoption. Selecting a guidance set that provides only high-level non-technical information, coupled with the exclusion of supplementary cited materials and limited coverage across our defined criteria-set, could leave operators lacking core skills, implementing under-developed supporting technologies, and operating limited overarching processes.

When we consider the internal growth of talent within industrial organisations, it becomes critical to provide comprehensive guidance allowing for new roles and career paths to form. The use of existing standards and guidelines to develop internal processes provides a primary conduit towards identifying required skills, and general human capital, further highlighting their importance.

Based on our findings, providing a framework that could be used to identify/assess an organisation's existing overarching cyber security incident response and recovery process coverage would directly benefit operators. Where gaps are identified in existing practices, it becomes vital to better understand how they can be developed. In the interest of avoiding the recreation of existing material, a framework's coverage of response and recovery phases should be based on those detailed in existing standards and guidelines. Furthermore, specific section numbers from within each of the references standards and guideline should be highlighted to avoid the requirements for a comprehensive and resource-heavy review by each framework user. A framework of this nature would complement existing processes, offering a high degree of credibility, instilling confidence in its use.

As all personnel can be used during an incident, including the involvement of third parties, through an enhanced cyber security understanding, gaps in human capital may be identified. For example, during exercising, an organisation will be able to identify that while key response and recovery phases would significantly benefit decision-making processes within central incident teams, increasing the efficiency of activities, preserve forensic data, etc., they require additional personnel to be recruited, or existing personnel to undergo additional training.

Initial framework concepts were discussed with interview participants and received a positive response. Therefore, the following section introduces our framework, acting as a starting point towards supporting operators in developing their cyber incident response and recovery capabilities.

7. Response and Recovery Framework

The following cyber incident response and recovery framework has been created based on the findings of our two subsequent studies discussed across the previous sections. From these studies, we identified two key points, (1) existing guidance lacks consistency in the breadth and depth of information provided, and (2) a single resource by which existing cyber incident response and recovery processes could be reviewed for completeness and further developed, would offer significant value to ICS operators. In the interest of avoiding the recreation of existing material, an undesirable option raised during our stakeholder engagement, the framework presented here focuses on aggregating information across the previously investigated thirty-one international standards and guidelines. The core output of which provides a centralized, credible resource used to review, support, and enhance an organization's cyber incident response and recovery capabilities.

7.1. The Framework

From our analysis of thirty-one international standards and guidelines, we were able to identify four high-level cyber incident response and recovery phases, aligned to seventeen sub-phases. These were summarized in Table 4, and are used as a base for expansion in our framework. Our second study, the stakeholder engagements, discussed in Section 5, provided us with an in-depth practical understanding for developing the process-flow and contents of the framework. Due to the size of this framework (See Figure 6), we have turned it into an interactive HTML resource available on Github [89]. The following subsections provide a breakdown of the information aligned to each sub-phase within the framework and its overarching modes of operation.

7.1.1. Overview

A high-level description of each sub-phase, allowing framework users to view their core functions. This helps in the selection of sub-phases for further development.

7.1.2. Dependencies

While each sub-phase has its own unique set of outputs, those outputs may feed directly into subsequent sub-phases as pre-requisites. The high-level view of such dependencies ensures framework users account for sub-phase interplays.

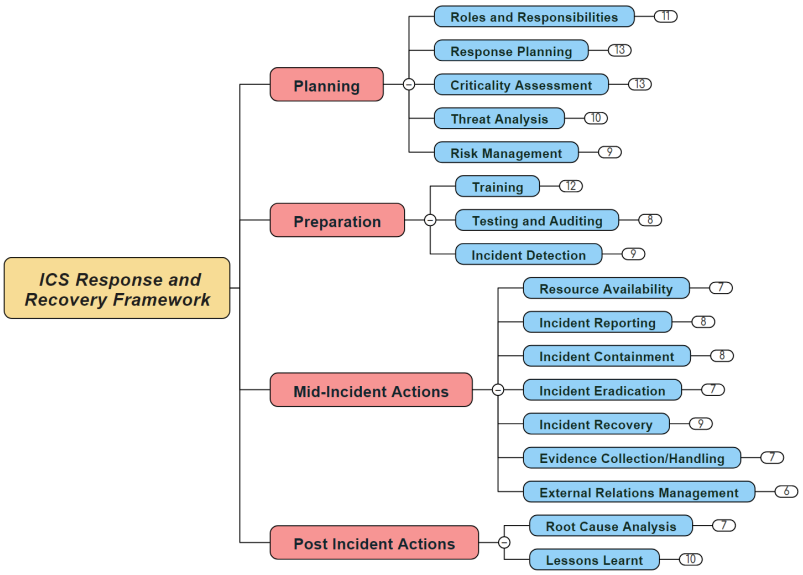

Figure 5: Cyber Incident Response and Recovery Framework [89]

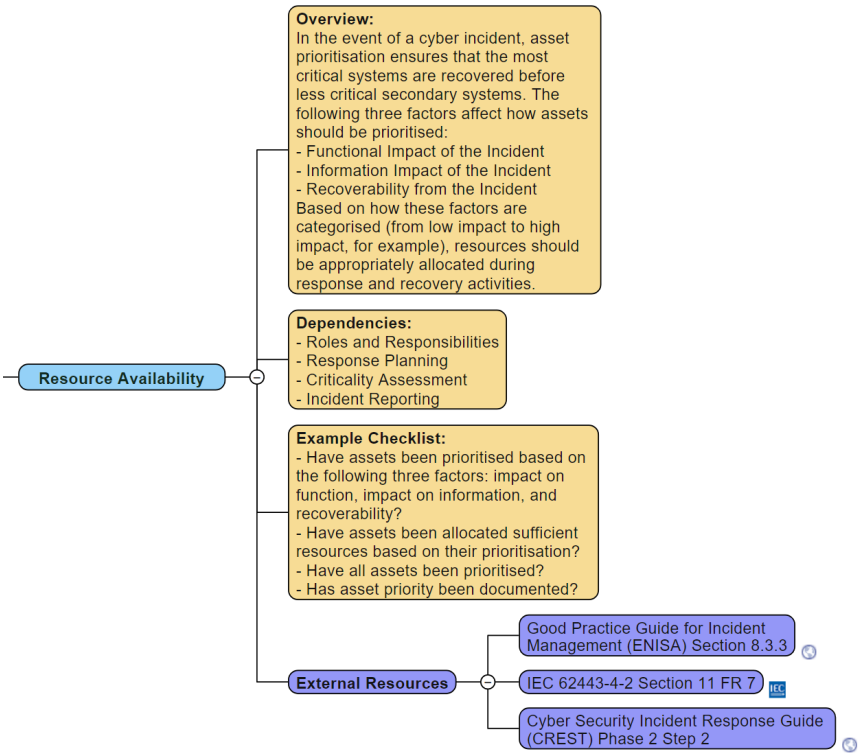

Figure 6: Resource Availability sub-phase of R&R Framework [89]

7.1.3. Example Checklist

Sub-phases can be highly detailed, taking time to understand and develop. However, the inclusion of example checklists offers an initial starting point for framework users to explore their existing capability.

7.1.4. Additional Resources

Providing the most critical element of the framework are additional resources. Here, each sub-phase is mapped to specific sections of the thirty-one standards and guidelines, saving framework users time in their inception/continued development.

7.1.5. Framework Operation

Our framework provides a light-weight, highly accessible resource that can be used in two primary ways: (1) to review each of the identified cyber incident response and recovery phases/sub-phases against existing capabilities, supporting the identification and development of existing gaps, and (2) as a quick reference guide to understand, assess, and develop, specific phases/sub-phases.

While the framework does not provide a quantifiable methodology towards assessing existing capability, its use as defined within this section offers a high-level, flexible approach to identify gaps and deficiencies in existing practices. More importantly, it provides highly-focused direction to credible resources allowing for the continued development of cyber incident response and recovery capability. These resources provide guidance on the creation of policies and process, including those directly associated with practical security controls, affording framework users not only with comprehensive scoping coverage but depth in practical detail. We are confident that the framework can be of significant added value to CNI operators in carrying out their everyday tasks and can guide them and their managers in selecting the suitable implementation for their environment. As such, to not be prescriptive, the framework is defined as a means to guide operators towards the appropriate tools rather than to define specific rules and processes.

Figure 7 has been created to support user understanding of the framework's operation. This figure depicts a process flow aligned to the two primary methods of use. The first of which would see a cyclic flow from the initial cyber incident response and recovery phase (Roles and Responsibilities) to the last (Lessons Learnt), whereas the second would involve a single pass on the relevant sub-phase of particular interest to the user (i.e. to further develop know issues in related current practices). The stages of this process flow are as follows:

- To begin, the relevant cyber incident response and recovery sub-phase should be selected from the framework using its associated title. This action can be supported by using the high-level overview, included as part of each sub-phases supporting text. Where an initial sub-phase has been identified but does not match the user's requirements (a possibility with the second method of framework use), a step back to re-review alternative sub-phases will be required.
- Using the provided checklist aligned to the sub-phase under review, the user should conduct an assessment of current capabilities. This activity provides a high-level view of current capabilities vs sub-phase requirements and acts as a starting point to better understand the associated sub-phase and whether it has been considered within existing cyber incident response and recovery processes.
- From the initial baseline checklist, associated dependencies should be reviewed. This begins to build a more comprehensive picture of the sub-phase under review, its key characteristic, and how it fits within the broader cyber incident response and recovery life-cycle. If they are met and understood, no further action is required. Alternatively, a loop back to review each dependency within the framework could be conducted.
- Where the information provided within the framework is sufficient, the sub-phase review process may end. However, it is strongly recommended that the highlighted sections within external resources (extracted from our initial pool of thirty-one standards and guidelines) are used to better understand the interplay between the current sub-phase and its dependencies, low-level implementation details, etc. Without this, only a high-level understanding of sub-phase requirements is formed; this is insufficient to practically develop cyber incident response and recovery capability.

8. Conclusion and Future Work

Section 3 and Appendix A provide an analysis of thirty-one individual standards and guidelines to better understand the current state-of-the-art for cyber incident response and recovery. As seen in Tables 5 and 6, the level of information coverage across these resources varies, leaving users exposed to potentially incomplete processes. This presents a significant challenge when

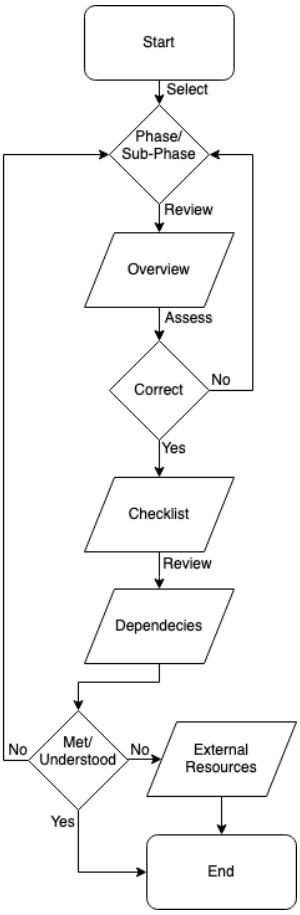

Figure 7: Framework Process Flow

developing cyber incident response and recovery capabilities, compounded by the technical vs non-technical nature of available resources.

Engagement with key industry stakeholders in Section 5 and Appendix B introduced additional challenges, with a focused view on the applicability of standards and guidelines in practice, discussed in Section 3. In taking a concentrated approach to using specific standards and guidelines, an appreciation of discrepancies in the quantity and type of information available across a broader set of resources may be lacking. Where time limitations prevent broader reviews from being undertaken, it is clear why focused approaches are adopted. However, in discussing initial framework concepts with industry stakeholder, positive feedback was received, affording those in industry with a short-cut/lower barrier to entry when reviewing resources outside their current scope.

A key output from the stakeholder engagement noted that any framework developed to support cyber incident response and recovery processes should not seek to "reinvent the wheel". This viewpoint, and the aforementioned challenges, provided a driving force behind our framework's design. While Tables 5 and 6 provide a snapshot of standard and guideline coverage, included domains, and a technical vs non-technical focus, industry stakeholders would still be required to identify key characteristic aligned to each sub-phase, relevant sections within each resource, dependencies, etc. Therefore, while these tables provide a valuable resource in identifying standard and guideline content, when used in parallel with our framework, a lower barrier to adoption and thus an increased likelihood of uptake is achieved.

When designing the foundational base upon which our framework sits, it was essential to avoid obstacles in its use while still offering value in the development of existing and new practices. The framework's lightweight construct presents a clear and meaningful way for its users to map existing practices to key cyber incident response and recovery phases/sub-phases and assess their completeness using base-line overviews and example checklists before progressing into granular details via specific sections of additional related resources. However, more importantly, the framework does not mandate each sub-phases' inclusion but offers a clear view of their holistic benefits derived through dependency mapping. This allows users to pick and choose sub-phases based on their existing practices and objectives (i.e. improve existing practices or introduce new practices).

A key characteristic of our framework is the inclusion of dependencies between sub-phases. This is currently presented at a high-level, with limited descriptive details outlining dependency parameters outside of the specified resources. We believe undertaking a more detailed analysis, and write-up of these dependencies within the framework would support further development of each sub-phase and provide an increased motivation towards the broader inclusion of all sub-phases (due to their directly observable value across the cyber incident response and recovery lifecycle). This offers an initial starting point for future work, which will be extended further through additional engagement with industry stakeholders, taking their feedback on our framework, and any additional features they would like to see in its continued development.

From our initial analysis of related work (see Section 2), we were able to identify a range of research activity that collectively contributes to multiple response and recovery phases/sub-phases. As part of our future work, we will also look to provide references to

academic work similar to the standards and guidelines in our current version. We believe this will further strengthen the level of technical guidance available to framework users.

9. Acknowledgements

The authors would like to acknowledge the UK Government's Department for Business, Energy, and Industrial Strategy (BEIS), which provided the funding for this research. The authors would also like to thank all industry stakeholders for their participation.

References

[1] Security primer – lockergoga. https://www.cisecurity.org/wp-content/uploads/2019/03/LockerGoga-Security-Primer-1.pdf.

[2] Sobig virus strikes csx train signalling system. https://www.risidata.com/Database/Detail/sobig-virus-strikes-csx-train-signalling-system, 2003.

[3] Tv remote control derails trams. http://www.h-online.com/security/news/item/TV-remote-control-derails-trams-Update-735805.html, 2008.

[4] Feds: Hospital hacker's 'massive' ddos averted. https://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested/, 2009.

[5] W32.flamer information. https://www.symantec.com/connect/forums/w32flamer-information, 2012.

[6] Triton attribution: Russian government-owned lab most likely built custom intrusion tools for triton attackers. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html, 2019.

[7] I. Ahmed, S. Obermeier, S. Sudhakaran, and V. Roussev. Programmable logic controller forensics. *IEEE Security & Privacy*, 15(6):18–24, 2017.

[8] U. P. D. Ani, J. M. Watson, B. Green, B. Craggs, and J. R. Nurse. Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. *Journal of Cyber Security Technology*, pages 1–49, 2020.

[9] ANSSI. Managing Cybersecurity for Industrial Control Systems. Technical report, Agence Nationale de la Sécurité des Systèmes d'Information, 2012.

[10] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa, and N. O. Tippenhauer. Gamifying ics security training and research: Design, implementation, and results of s3. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 93–102, 2017.

[11] H. Arksey and P. T. Knight. *Interviewing for social scientists: An introductory resource with examples*. Sage, London, 1999.

[12] H. Asai, T. Aoyama, Y. Ota, Y. Hashimoto, and I. Koshijima. Design and operation framework for industrial control system security exercise. In *Security of Cyber-Physical Systems*, pages 25–51. Springer, 2020.

[13] G. Baker. Schoolboy Hacks into City's Tram System. http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html, 2008. Retrieved 11/09/2017.

[14] M. O. Balitanas, S.-H. Jeon, and T.-h. Kim. Retrofit to cain of ip-based supervisory control and data acquisition system. In *International Conference on Information Security and Assurance*, pages 211–218. Springer, 2011.

[15] C. Beggs and M. Warren. A proposed cyber-terrorism scada risk framework concept for australia. In *ECIW2008-7th European Conference on Information Warfare and Security: ECIW2008*, page 17. Academic Conferences Limited, 2008.

[16] M. Betts, J. Stirland, F. Olajide, K. Jones, and H. Janicke. Developing a state of the art methodology & toolkit for ics scada forensics. In *The International Conference on Information Security and Cyber Forensics*, 2016.

[17] C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt, and K. Wilhoit. *Hacking Industrial Control Systems Exposed: ICS and SCADA Security Secrets & Solutions*. McGraw-Hill Education, London, first edition, 2017.

[18] P. Bowen, J. Hash, and M. Wilson. NIST Special Publication 800-100: Information Security Handbook - A Guide for Managers. Technical report, National Institute of Standards and Technology, 2006.

[19] C. Bronk and E. Tikk-Ringas. Hack or attack? Shamoon and the Evolution of Cyber Conflict. *Survival, Glocal Politics and Strategy*, 2013. Retrieved 02/03/2017.

[20] J. Butts and M. Glover. How industrial control system security training is falling short. In *International Conference on Critical Infrastructure Protection*, pages 135–149. Springer, 2015.

[21] E. Byres. Flame Malware and SCADA Security: What are the Impacts? https://www.tofinosecurity.com/blog/ flame-malware-and-scada-security-what-are-impacts, 2012. Retrieved 31/08/2017.

[22] D. T. Campbell and J. C. Stanley. *Experimental and quasi-experimental designs for research on teaching*. Ravenio Books, 1963.

[23] D. Canter, J. Brown, and M. Brenner. *The research interview: Uses and approaches*. Academic Press, New York, 1985.

[24] Carnegie Mellon University. The CERT Division. https://www.sei.cmu.edu/about/divisions/cert/index.cfm, 2019.

[25] E. Casalicchio and G. Gualandi. Asimov: A self-protecting control application for the smart factory. *Future Generation Computer Systems*, 115:213–235, 2021.

[26] Centre for the Protection of National Infrastructure. Critical National Infrastructure. https://www.cpni.gov.uk/critical-national-infrastructure-0, 2021.

[27] CheckPoint. SQL Slammer Comeback. http://blog.checkpoint.com/2017/02/02/sql-slammer-comeback/, 2017. Retrieved 30/08/2017.

[28] E. Chien, L. O'Murchu, and N. Falliere. W32. Duqu: The Precursor to the Next Stuxnet. https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet, 2011. Retrieved 13/04/2015.

[29] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. NIST Special Publication 800-61: Computer Security Incident Handling Guide. Technical report, National Institute of Standards and Technology, 2012.

[30] CIS. CIS Critical Security Controls. Technical report, Center for Internet Security, 2019.

[31] Cisco and Rockwell Automation. Ethernet-to-the-Factory 1.2 Design and Implementation Guide. Technical report, 2008.

[32] CNSC. REGDOC-2.5.2 Design of Reactor Facilities: Nuclear Power Plants. Technical report, Canadian Nuclear Safety Commission, 2014.

[33] A. Cook, H. Janicke, R. Smith, and L. Maglaras. The industrial control system cyber defence triage process. *Computers & Security*, 70:467–481, 2017.

[34] B. F. Crabtree and W. F. Miller. *A Template Approach to Text Analysis: Developing and Using Codebooks*. Sage, Thousand Oaks, CA, US, 1992.

[35] J. Creasy and I. Glover. Cyber Security Incident Response Guide. Technical report, Council for Registered Ethical Security Testers, 2013.

[36] R. Derbyshire, B. Green, D. Prince, A. Mauthe, and D. Hutchison. An analysis of cyber security attack taxonomies. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 153–161. IEEE, 2018.

[37] A. Di Pinto, Y. Dragoni, and A. Carcano. Triton: The first ics cyber attack on safety instrument systems. In *Proc. Black Hat USA*, pages 1–26, 2018.

[38] Dragos. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. Technical report, 2017. Retrieved 29/12/2017.

[39] DWI. Guidance on the Implementation of the NIS Regulations 2018 - The Cyber Assessment Framework (CAF). Technical report, Drinking Water Inspectorate, 2018.

[40] DWI. CAF Information. `http://dwi.defra.gov.uk/nis/caf/index.html`, 2019.

[41] E-ISAC and SANS. Analysis of the Cyber Attack on the Ukrainian Power Grid. Technical report, 2016. Retrieved 27/09/2017.

[42] P. Eden, A. Blyth, P. Burnap, Y. Cherdantseva, K. Jones, H. Soulsby, and K. Stoddart. Forensic readiness for scada/ics incident response. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, pages 142–150, 2016.

[43] ENISA. Good Practice Guide for Incident Management. Technical report, European Network and Information Security Agency, 2010.

[44] European Union Agency for Cybersecurity. NIS Directive, 2021.

[45] F-Secure. Worm:W32/Slammer. `https://www.f-secure.com/v-descs/mssqlm.shtml`, 2003. Retrieved 30/08/2017.

[46] N. Falliere, L. Murchu, and E. Chien. W32. stuxnet dossier. Technical Report February, 2011. Retrieved 18/02/2015.

[47] D. Ganga and S. Scott. Cultural" insiders" and the issue of positionality in qualitative migration research: Moving" across" and moving" along" researcher-participant divides. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, volume 7, 2006.

[48] B. Glaser and A. Strauss. Grounded theory: the discovery of grounded theory. *Sociology The Journal Of The British Sociological Association*, 12:27–49, 1967.

[49] C. Glenn, D. Sterbentz, and A. Wright. Cyber threat and vulnerability analysis of the us electric sector. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2016.

[50] J. Gonzalez and M. Papa. Passive scanning in modbus networks. In *International Conference on Critical Infrastructure Protection*, pages 175–187. Springer, 2007.

[51] B. Green, R. Derbyshire, W. Knowles, J. Boorman, P. Cihola s, D. Prince, and D. Hutchison. {ICS} testbed tetris: Practical building blocks towards a cyber security resource. In *13th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 20)*, 2020.

[52] B. Green, M. Krotofil, and A. Abbasi. On the significance of process comprehension for conducting targeted ics attacks. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 57–67. ACM, 2017.

[53] B. Green, A. Lee, R. Antrobus, U. Roedig, D. Hutchison, and A. Rashid. Pains, gains and plcs: ten lessons from building an industrial control systems testbed for security research. In *10th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 17)*, 2017.

[54] A. Greenberg. "Crash Override": The Malware That Took Down A Power Grid. `https://www.wired.com/story/crash-override-malware/`, 2017. Retrieved 02/09/2017.

[55] A. GREENBERG. The highly dangerous 'triton' hackers have probed the us grid. `https://www.wired.com/story/triton-hackers-scan-us-power-grid/`, 2019.

[56] L. Haines. Zotob perp jailed: Hard time for bot ne'er-do-well. `https://www.theregister.co.uk/2006/09/13/zotob_perps_jailed/`, 2006. Retrieved 31/08/2017.

[57] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld, and M. K. Banks. A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, 146(5):03120003, 2020.

[58] T. Hatmaker. Nuclear facility hacks remain fairly superficial for now, say dhs and fbi, 2017.

[59] Y. He, L. A. Maglaras, H. Janicke, and K. Jones. An industrial control systems incident response decision framework. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 761–762. IEEE, 2015.

[60] K. E. Hemsley, E. Fisher, et al. History of industrial control system cyber incidents. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[61] H. Hirai, T. Aoyama, N. Davaadorj, and I. Koshijima. Framework for cyber incident response training. *Safety and Security Engineering VII, Rome, Italy*, pages 273–283, 2017.

[62] HMG. HMG Security Policy Framework. Technical report, Her Majesty's Government, 2018.

[63] HSE. Cyber Security for Industrial Automation and Control Systems (IACS). `http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf`, 2018.

[64] IAEA. IAEA Nuclear Security Series No. 17. Technical report, International Atomic Energy Agency, 2011.

[65] IAEA. Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime. Technical report, International Atomic Energy Agency, 2013.

[66] IAEA. IAEA Nuclear Security Series No. 23-G. Technical report, International Atomic Energy Agency, 2015.

[67] IEC. BS IEC 62443-2-1:2011, 2011.

[68] IEC. BS EN IEC 62443-4-2:2019, 2019.

[69] P. Inc. ThingWorx IIoT Platform, 2019.

[70] International Atomic Energy Agency. Nuclear Share of Electricity Generation in 2019. https://pris.iaea.org/pris/worldstatistics/ nuclearshareofelectricitygeneration.aspx, 2021.

[71] ISO/IEC. BS ISO/IEC 27035-1:2016, 2016.

[72] ISO/IEC. BS ISO/IEC 27035-2:2016, 2016.

[73] ISO/IEC. BS EN ISO/IEC 27001:2017, 2017.

[74] ISO/IEC. BS EN ISO/IEC 27002:2017, 2017.

[75] ISO/IEC. BS EN ISO/IEC 27019:2017, 2017.

[76] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2(1-2):26–37, 2009.

[77] W. Jardine, S. Frey, B. Green, and A. Rashid. Senami: Selective non-invasive active monitoring for ics intrusion detection. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, pages 23–34, 2016.

[78] D. Kapellmann and R. Washburn. Call to action: Mobilizing community discussion to improve information-sharing about vulnerabilities in industrial control systems and critical infrastructure. In *2019 11th International Conference on Cyber Conflict (CyCon)*, volume 900, pages 1–23. IEEE, 2019.

[79] F. Kargl, R. W. van der Heijden, H. König, A. Valdes, and

M. C. Dacier. Insights on the security and dependability of industrial control systems. *IEEE security & privacy*, 12(6):75–78, 2014.

[80] Kasperky. From Shamoon to Stonedrill. Technical report, 2017. Retrieved 07/01/2018.

[81] Kaspersky. BlackEnergy APT Attacks in Ukraine. `https://www.kaspersky.co.uk/resource-center/threats/blackenergy`, 2015. Retrieved 01/09/2017.

[82] B. Kesler. The vulnerability of nuclear facilities to cyber attack. *Strategic Insights*, 10(1):15–25, 2011.

[83] A. Khalili, A. Sami, M. Keikha, and A. A. Safavi. Recovery scheme for industrial control systems. In *The 5th Conference on Information and Knowledge Technology*, pages 279–283. IEEE, 2013.

[84] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In *ICS-CSR*, 2016.

[85] J. Kim, K. Kim, and M. Jang. Cyber-physical battlefield platform for large-scale cybersecurity exercises. In *2019 11th International Conference on Cyber Conflict (CyCon)*, volume 900, pages 1–19. IEEE, 2019.

[86] N. King, C. Cassell, and G. Symon. Qualitative methods in organizational research: A practical guide. *The Qualitative Research Interview*, 17, 1994.

[87] E. Kovacs. Triton ics malware developers likely copied code from legitimate libraries. https://www.icscybersecurityconference.com/triton-ics-malware-developers-likely-copied-code-from-legitimate-libraries/, 2018.

[88] P. Kral. Information Security Reading Room: Incident Handler's Handbook. Technical report, SANS Institute, 2019.

[89] Lancaster University. ICS Response and Recovery Framework. `https://ics-rr-framework.github.io/`, 2021.

[90] Lancaster University. Interview Protocol. `https://github.com/ICS-RR-Framework/Stakeholder-Engagement-Protocol`, 2021.

[91] R. M. Lee. Article on German Steel Mill Attack "Inside Job" is Just Hype. http://www.robertmlee.org/article-on-german-steel-mill-attack-inside-job-is-just-hype/, 2015. Retrieved 01/09/2017.

[92] R. M. Lee, M. J. Assante, and T. Conway. German Steel Mill Cyber Attack. Technical report, SANS, 2014. Retrieved 02/02/2015.

[93] S. Left. Code Red virus traced to China. `https://www.theguardian.com/technology/2001/aug/31/viruses.security`, 2001. Retrieved 04/09/2017.

[94] R. Lemos. 'Data storm' blamed for nuclear plant shutdown: Malfunctioning control device causes fatal spike in traffic. `https://www.theregister.co.uk/2007/05/21/alabama_nuclear_plant_shutdown/`, 2007. Retrieved 31/08/2017.

[95] J. Leyden. Mystery lingers over stealthy Stuxnet infection: Cloak and dagger. `https://www.theregister.co.uk/2010/09/27/stuxnet_analysis/`, 2010. Retrieved 31/08/2017.

[96] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318, 2017.

[97] M. B. Line, I. A. Tøndel, and M. G. Jaatun. Current practices and challenges in industrial control organizations regarding information security incident management–does size matter? information security incident management in large and small industrial control organizations. *International journal of critical infrastructure protection*, 12:12–26, 2016.

[98] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer. Targeted attacks against industrial control systems: Is the power industry prepared? In *Proceedings of the 2nd Workshop on Smart Energy Grid Security*, pages 13–22, 2014.

[99] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis. Threats, protection and attribution of cyber attacks on critical infrastructures. *arXiv preprint arXiv:1901.03899*, 2019.

[100] T. D. Maiziere. Die Lage der IT-Sicherheit in Deutschland 2014. Technical report, 2014. Retrieved 03/02/2015.

[101] McAfee. Global Energy Cyberattacks : " Night Dragon ". Technical report, 2011. Retrieved 14/02/2014.

[102] C. Meinel. Code red: Worm assault on the web, 2001.

[103] B. Miller and D. Rowe. A Survey SCADA of and Critical Infrastructure Incidents. In *Proceedings of the 1st Annual Conference on Research in Information Technology*, RIIT '12, pages 51–56, New York, NY, USA, 2012. ACM.

[104] D. Morain. Hackers Victimize Cal-ISO. `http://articles.latimes.com/2001/jun/09/news/mn-8294`, 2001. Retrieved 30/08/2017.

[105] S. Mustard. Security of distributed control systems: The concern increases. *Computing & Control Engineering Journal*, 16(6):19–25, 2005.

[106] National Cyber Security Centre. About the NCSC. `https://www.ncsc.gov.uk/section/about-ncsc/what-we-do`, 2021.

[107] National Cyber Security Centre. NCSC CAF Guidance. `https://www.ncsc.gov.uk/collection/caf`, 2021.

[108] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Technical report, 2018.

[109] NCSC. 10 Steps to Cyber Security: Incident Management. `https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/incident-management`, 2018.

[110] NCSC. NCSC CAF Guidance. `https://www.ncsc.gov.uk/collection/nis-directive?curPage=/collection/nis-directive/introduction-to-the-nis-directive`, 2019.

[111] NCSC. NCSC CAF Guidance Objective C - Detecting Cyber Security Events. `https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-c-detecting-cyber-security-events`, 2019.

[112] NEI. NEI 08-09 Cyber Security Plan for Nuclear Power Reactors. Technical report, Nuclear Energy Institute, 2010.

[113] NERC. CIP-008-6 - Cyber Security - Incident Reporting and Response Planning. Technical report, North American Electric Reliability Corporation, 2019.

[114] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4):418–436, jun 2012.

[115] R. Nigam. (Known) SCADA Attacks Over the Years. `https://blog.fortinet.com/2015/02/12/known-scada-attacks-over-the-years`, 2015. Retrieved 24/08/2017.

[116] NIST. Draft NIST Special Publication 800-53, Revision 5, Initial Public Draft. Technical report, National Institute of Standards and Technology, 2017.

[117] NRC. RG 5.71 Cyber Security Programs for Nuclear Facilities. Technical report, Nuclear Regulatory Commission, 2010.

[118] Office for Nuclear Regulation. Security Assessment Principles for the Civil Nuclear Industry. Technical report, 2017.

[119] Office of the Press Secratary. Executive Order - Improving Critical Infrastructure Cybersecurity. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, 2021.

[120] ONR. Office for Nuclear Regulation (ONR) Permissioning Inspection - Technical Assessment Guides. http://www.onr.org.uk/operational/tech_asst_guides/, 2019.

[121] M. Q. Patton. *Qualitative evaluation and research methods*. SAGE, London, 1990.

[122] Peplink. MAX Outdoor Router. https://www.peplink.com/products/max-cellular-router/outdoor/{\#}hd2, 2019.

[123] N. Perlroth. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, 2012. Retrieved 01/09/2017.

[124] N. Perlroth. Hackers are targeting nuclear facilities, homeland security dept. and f.b.i. say. https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html, 2017.

[125] A. F. M. Piedrahita, V. Gaur, J. Giraldo, A. A. Cardenas, and S. J. Rueda. Leveraging software-defined networking for incident response in industrial control systems. *IEEE Software*, 35(1):44–50, 2017.

[126] H. W. Poole, L. Lambert, C. Woodford, and C. J. P. Moschovitis. *The Internet: a historical encyclopedia*, volume 1. Abc-Clio Inc, Oxford, 2005.

[127] J. Powney and M. Watts. *Interviewing in educational research*. Routledge & Kegan Paul, Ablingdon, 1987.

[128] PTC Inc. KEPServerEX - Solving Your Communications Challenges. https://www.kepware.com/en-us/products/, 2019.

[129] G. Ravikumar, B. Hyder, and M. Govindarasu. Next-generation cps testbed-based grid exercise-synthetic grid, attack, and defense modeling. In *2020 Resilience Week (RWS)*, pages 92–98. IEEE, 2020.

[130] W. RI. *Basic Content Analysis*. Beverly Hills, CA: Sage Publications, 1985.

[131] T. Rid. Cyber war will not take place. *Journal of strategic studies*, 35(1):5–32, 2012.

[132] M. Rosenberg. Wolf creek nuclear plant hit by cyberattack. https:// www.theenergytimes.com/cybersecurity/wolf-creek-nuclear-plant-hit-cyberattack, 2017.

[133] H. J. Rubin and I. S. Rubin. *Qualitative interviewing: The art of hearing data*. Sage, London, 2011.

[134] T. Sasaki, K. Sawada, S. Shin, and S. Hosokawa. Fallback and recovery control system of industrial control system for cybersecurity. *IFAC-PapersOnLine*, 50(1):15247–15252, 2017.

[135] Schneider Electric. ClearSCADA: Software for Telemetry and Remote SCADA Systems and Applications. https://www.schneider-electric.co.uk/en/product-range-presentation/61264-clearscada/, 2019.

[136] Schneider Electric. SCADAPack 100, 300, 32. https://www.schneider-electric.com/en/product-range/61247-scadapack-100{\%}2C-300{\%}2C-32/189048704-scadapack-32/?subNodeId=189048704en{_}WW, 2019.

[137] Siemens. ET200S. https://mall.industry.siemens.com/goos/catalog/Pages/mmpdata.ashx?lang=en{\&}MLFB1=6ES7151-8AB00-0AB0{\&}MLFB2=6ES7151-8AB01-0AB0{\&}, 2019.

[138] Siemens. KTP700F. https://mall.industry.siemens.com/mall/en/uk/Catalog/Product/6AV2125-2GB23-0AX0, 2019.

[139] J. Slay and M. Miller. Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection*, pages 73–82. Springer, 2007.

[140] J. Slowik. Evolution of ics attacks and the prospects for future disruptive events.

[141] R. Smith. Russian hackers reach u.s. utility control rooms, homeland security officials say. https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110, 2018.

[142] Sophos. Nachi worm tries to undo Blaster damage - but no virus is a good virus, says Sophos. https://www.sophos.com/en-us/press-office/press-releases/2003/08/va_nachi.aspx, 2003. Retrieved 30/08/2017.

[143] M. Souppaya and K. Scarfone. NIST Special Publication 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops. Technical report, National Institute of Standards and Technology, 2013.

[144] Spiegel Online. The NSA and Its Willing Helpers. http://www.spiegel.de/ international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html, 2013. Retrieved 31/08/2017.

[145] A. Staves, H. Balderstone, B. Green, A. Gouglidis, and D. Hutchison. A framework to support ics cyber incident response and recovery. In *the 17th International Conference on Information Systems for Crisis Response and Management*, 2020.

[146] K. Stougger, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security, Revision 2. Technical report, National Institute of Standards and Technology, 2015.

[147] C. Sweigart. SCORE Security Checklist. Technical report, SANS Institute, 2003.

[148] Symantec. Emerging Threat: Dragonfly / Energetic Bear – APT Group. https://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group, 2014. Retrieved 29/08/2017.

[149] Symantec. Dragonfly: Western energy sector targeted by sophisticated attack group. https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks, 2017.

[150] Symantec. Shamoon: Multi-staged destructive attacks limited to specific targets. https://www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets, 2017. Retrieved 01/09/2017.

[151] Symantec. Targeted ransomware: Proliferating menace threatens organizations. https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat, 2019.

[152] A. Tham. What is Code Red Worm? Technical report, 2001. Retrieved 01/02/2015.

[153] The Associated Press. Hackers Attacked California Power. http://www.nytimes.com/2001/06/10/us/hackers-attacked-california-power.html?mcubz=1, 2001. Retrieved 30/08/2017.

[154] The Repository of Industrial Security Incidents. California Canal System Hack. https://www.risidata.com/Database/Detail/California_Canal_System_Hack, 2015.

[155] TREND MICRO. What you need to know about the lockergoga ransomware. https://www.cisecurity.org/wp-content/uploads/2019/03/LockerGoga-Security-

Primer-1.pdf, 2019.
[156] R. J. Turk. Cyber incidents involving control systems. Technical report, 2005. Retrieved 18/07/2014.
[157] S. Ullah, S. Shelly, A. Hassanzadeh, A. Nayak, and K. Hasan. On the effectiveness of intrusion response systems against persistent threats. In *2020 International Conference on Computing, Networking and Communications (ICNC)*, pages 415–421. IEEE, 2020.
[158] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1092–1105, 2016.
[159] U.S. Department of Justice. Arlington Security Guard Arreseted on Federal Charges for Hacking into Hospital's Computer System. https://www.justice.gov/archive/usao/txn/PressRel09/mcgraw_cyber_compl_arrest_pr.html, 2009. Retrieved 02/09/2017.
[160] P. Van Vliet, M.-T. Kechadi, and N.-A. Le-Khac. Forensics in industrial control system: a case study. In *Security of Industrial Control Systems and Cyber Physical Systems*, pages 147–156. Springer, 2015.
[161] J. Vávra and M. Hromada. An evaluation of cyber threats to industrial control systems. In *Military Technologies (ICMT), 2015 International Conference on*, pages 1–5. IEEE, 2015.
[162] Westermo. Managed Ethernet Switch. https://www.westermo.com/products/ethernet-switches/layer-2/l110-f2g, 2019.
[163] T. Wu, J. F. P. Disso, K. Jones, and A. Campos. Towards a scada forensics architecture. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*, pages 12–21, 2013.
[164] K. Zetter. Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. http://www.wired.com/2012/05/flame/all/, 2012. Retrieved 17/02/2015.
[165] K. Zetter. Everything We Know About Ukraine's power Plant Hack. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, 2016. Retrieved 2/09/2017.
[166] S. Zhioua. The Middle East under Malware Attack Dissecting Cyber Weapons. In *Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on*, pages 11–16. IEEE, 2013.
[167] B. Zhu, A. Joseph, and S. Sastry. A taxonomy of cyber attacks on scada systems. In *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, pages 380–388. IEEE, 2011.

Appendix A. Detailed Overview of Standards and Guidelines

The following subsections provide a detailed overview of the standards and guidance used for our analysis in Section 3.

Appendix A.1. UK Guidance

NCSC Cyber Assessment Framework (CAF)

Created in response to the NIS Directive, the CAF consists of four objectives, each focusing on a different stage of an organisation's security planning [110]. Objective D relates to guidance on response and recovery and is broken down into two sub-objectives: Response and Recovery Planning and Lessons Learned. The CAF also recommends consulting additional external resources [29, 71, 35].

Drinking Water Inspectorate (DWI) Cyber Assessment Framework

The DWI have published their own guidance tailored towards the water sector in the UK. Based on the NCSC's CAF, it aims to provide operators with a framework for managing cyber security risks and incidents that could impact drinking water quality or availability. Furthermore, it allows the DWI to assess operators' security measures for compliance with the NIS Directive [40]. The DWI CAF is constructed around four top-level objectives, objective D being related to response and recovery [39]. This guidance recommends consulting additional external resources [73, 67, 116].

NCSC 10 Steps: Incident Management

The NCSC 10 Steps for incident management provides a light-weight resource covering key considerations aligned to incident response and recovery activities [109]. These include establishing a response capability, providing training, and usage of lessons learned.

Office for Nuclear Regulation (ONR) Security Assessment Principles (SyAPs)

SyAPs aid regulatory judgements and recommendations when undertaking assessments (for compliance) of nuclear facilities [118]. The assessment principles contain ten Fundamental Security Principles (FSyPs), two of which are directly relevant to cyber incident response and recovery (FSySP 7 and 10). These cover the following topics: Counter-Terrorism Measures, Emergency Preparedness, Response Planning, Testing and Exercising of the Security Response, and Clarity of Command, Control and Communications Arrangements During a Post Nuclear Security Event.

ONR Preparation for and Response to Cyber Security Events Technical Assessment Guide (TAG)

This TAG provides guidance for ONR inspectors' use covering eleven topics related to cyber security event response [120]. While TAGs explicitly state that they are not a resource for demonstrating adherence to SyAPs, they can provide additional insight into what operators' high-level goals should be. This guide also recommends consulting external resources [65, 64, 66, 43, 24, 88, 147, 30].

Her Majesty's Government (HMG) Security Policy Framework

The HMG Security Policy Framework covers several topic areas, from culture and awareness to risk management and personnel security [62]. Although brief, one section describes requirements when preparing for, and responding to, security events. This is discussed using generic, non-cyber terminology.

Health and Safety Executive (HSE) Operational Guidance (OG) 86

OG 86 is closely aligned to the NCSC CAF and is formed around its core security objectives and corresponding principles [63]. Discussion on cyber incident response and recovery is present throughout this guide. Guidance surrounding cyber incident response and recovery is provided in direct alignment to CAF objective D. This can be summarised as the development of a clear and concise, well-articulated cyber incident response plan. OG 86 also recommends consulting additional external resources [67, 73].

Appendix A.2. Supplementary Guidance

International Atomic Energy Agency (IAEA) Nuclear Security Fundamentals

The IAEA Nuclear Security Fundamentals outlines 12 essential elements required to support a state's nuclear security regime [65]. Cyber security is only mentioned once within this document, linked to a requirement on assurance activities. Essential element 11 relates directly to response (i.e. planning for, preparedness for, and response to, a nuclear security event).

IAEA Nuclear Security Series (NSS) 17

NSS 17 is designed to guide operators in establishing and improving programmes of work to protect computer systems, networks, and other (critical) digital systems responsible for the safe and secure operation of nuclear facilities [64]. Specific details on cyber incident response and recovery are limited to generic guidance, such as describing relevant responsibilities and response planning.

IAEA NSS 23-G

The objectives of NSS 23-G [66] are defined over four areas: establishing a framework for ensuring the confidentiality, integrity, and availability (CIA) of sensitive information; identifying sensitive information; considerations for sharing/disclosing sensitive information; and guidelines/methodologies for ensuring CIA. Therefore, its ties to cyber incident response and recovery are limited; however, content such as that found in Annex 2 (i.e. examples of sensitive information) could be used when categorising information related to "contingency and response plans and exercises".

ENISA Good Practice Guide for Incident Management

While not directed towards ICS, this guide provides a comprehensive discussion on cyber incident management for conventional IT systems [43]. Covered topics include response and recovery by explaining the incident handling process and basic codes of practice.

Carnegie Mellon University - Computer Security Incident Response Team FAQ

This FAQ provides a high-level discussion on CSIRTs. Although not targeted towards ICS, it acts as a helpful reference point in understanding core CSIRT requirements [24].

SANS Incident Handler's Handbook

The SANS Incident Handler's Handbook details key phases of incident response and recovery, their purpose, tools that can be used to support them, etc. [88]. While this is not ICS specific, it provides a comprehensive discussion on response and recovery broken down into the following core sections: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learnt.

SANS Security Consensus Operational Readiness Evaluation (SCORE)

The SANS SCORE security checklist is highly summarised in the form of six bullet points, each corresponding to the six steps presented within the Incident Handler's Handbook. It is designed to support all forms of incidents, including those from Advanced Persistent Threats (APT) [147].

The Center for Internet Security (CIS) Critical Security Controls (CSC)

CIS CSC presents 20 security controls [30]. Although defined as controls, these are more closely linked with high-level groups/objectives, to which mapping against the NIST Cyber Security Framework is performed. CSC 10, 19 and 20 discuss response and recovery topics covering guidance for both small and large organisations.

NIST Computer Security Incident Handling Guide (SP 800-61)

SP 800-61 details the need for incident prioritisation, stating that the handling and subsequent recovery of systems affected by these incidents should be determined by the potential impact on service functionality and information integrity [29]. A focus is placed on exploring methods for ensuring essential service continuity and impact mitigation.

NIST SP 800-53

SP 800-53 provides a "catalogue of security and privacy controls for federal information systems and organisations to protect organisational operations and assets, individuals, other organisations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks" [116]. This includes twenty mandatory controls, mapped to ISO/IEC 27001 [73], for securing assets, including response and recovery.

CREST Cyber Security Incident Response Guide

This guide is split into three core areas: preparing for, responding to, and recovering from a cyber security incident [35]. Each of these areas contains a step by step guide offering potential avenues for an organisation to follow during incident response, including methods for identifying potential incidents, conducting triage, and effectively containing and recovering from a state of containment.

BS EN ISO/IEC 27001/27002

ISO/IEC 27001 provides non-technical guidance for implementing and maintaining systems that are well protected from cyber threats, including a table in Annex A listing all the objectives that an asset owner should achieve [73]. Section A.16 of this table refers to incident management and consists of the following objectives: Responsibilities and Procedures, Incident Reporting, Vulnerability/Weakness Reporting, Event Assessment, Incident Response, Lessons Learnt, Evidence Collection. These objectives are described in more detail within ISO/IEC 27002, which serves as a "best practices" guidance for implementing the requirements in ISO/IEC 27001 [74].

BS EN ISO/IEC 27035:2016

ISO/IEC 27035 serves as a reference for fundamental principles designed to ensure that the correct tools, techniques and methods are appropriately selected in the event of a cyber incident. Part 1, Principles of incident management, presents fundamental concepts of information security incident management. These concepts are combined with principles from the five phases of response and recovery: detecting, reporting, assessing and responding to incidents, and applying lessons learnt [71]. Part 2, Guidelines to plan and prepare for incident response, describes how to plan and prepare for cyber incident response and recovery. This covers the "Plan and Prepare" and the "Lessons Learnt" phases presented in Part 1 of the standard [72].

BS EN IEC 62443 Series

The IEC 62443 catalogue defines procedures for implementing secure ICS. However, while the entirety of the catalogue was recommended by UK guidance, due to paywall restrictions, only parts 2-1 and 4-2 of the series were selected. Part 2-1 of this series provides guidance for establishing an ICS security program, including planning for incident response and recovery [67]. Part 4-2 of the series describes the technical security requirements for ICS components, including guidance on how to ensure that systems respond promptly to security violations by alerting the appropriate personnel and reporting details on the violation [68].

Appendix A.3. International Guidance

BS EN ISO/IEC 27019:2017

ISO/IEC 27019 provides guidance to fulfil the objectives set out in ISO/IEC 27001 and 27002 for ICS within the energy utility industry [75]. This is similar to that provided in ISO/IEC 27001, with subtle modifications to better suit ICS.

Nuclear Regulatory Commission (NRC) RG 5.71 (USA)

RG 5.71 provides a comprehensive overview of cyber incident response and recovery guidance for nuclear operators [117]. Guidance is provided under high-level requirements for establishing a cyber security plan concerning incident response and recovery.

Nuclear Energy Institute (NEI) 08.09 (USA)

NEI 08.09 is closely linked to NRC RG 5.71 [112]. Response and recovery activities/requirements are discussed across multiple high-level topic areas surrounding contingency planning.

NIST Framework for Improving Critical Infrastructure 2018 (USA)

This framework focuses on improving cyber security risk management for CNI [108]. It provides a standard

organisational structure for multiple cybersecurity approaches by assembling standards, guidelines, and practices into one document. Five core functions are defined, two of which are related to response and recovery.

NIST SP 800-82 (USA)

SP 800-82 provides guidance on securing ICS. It presents a general overview of system architectures, associated vulnerabilities, and recommendations on how to counteract these in order to reduce the associated risk [146]. ICS-specific response and recovery guidelines include Incident Detection, Incident Classification, Response Actions, and Recovery Actions.

NIST SP 800-83 (USA)

Based on SP 800-61, SP 800-83 provides a Guide to Malware Incident Prevention and Handling for Desktops and Laptops. Although not ICS specific, it is intended to help operators understand and mitigate risks associated with malware incidents, including associated practical guidance on response activities [143].

NIST SP 800-100 (USA)

SP 800-100 provides high-level guidance for management personnel tied to general information security themes, including risk management, service acquisition, and planning [18]. Guidance on response and recovery includes topics such as Incident Preparation, Incident Prevention, Incident Eradication, Incident Recovery, and Post-Incident Activities.

North American Electric Reliability Corporation (NERC) CIP-008-06 (USA)

Targeted towards power systems in North America, CIP-008-06 encompasses cyber security incident reporting and response planning requirements and associated recommendations. Its purpose is to "mitigate the risk of reliable operation of the Bulk Electric System as the result of a cyber security incident by specifying incident response requirements" [113].

Canadian Nuclear Safety Commission (CNSC) REGDOC-2.5.2 (Canada)

Cyber security requirements feature throughout this document within discussions on design management, design documents, and the instrumentation of the control life-cycle. One section is dedicated to cyber security under "Robustness Against Malevolent Acts" [32]. While this section provides a set of guiding principles focused on ties to safety, the inclusion of cyber specific incident response and recovery guidance is limited.

ANSSI Managing Cyber Security for Industrial Control Systems (France)

Coverage of cyber incident response and recovery activities within this document is limited, appearing briefly as part of a discussion on defence-in-depth strategies and across one section focusing on the "Incident Handling Alert Chain". This section is brief, with best practices established in the form of three questions [9].

Appendix B. Detailed Overview of Interview Results

The following subsections provide a detailed breakdown of key findings from section 5.2. These are grouped based on identified themes and key points of interest.

Appendix B.1. Primary Goal

Before identifying core phases individuals enact during the cyber incident response and recovery process, it is important to understand what participants believe the primary goal should be. As one would expect, a fundamental focus on safety through incident containment and the preservation of critical system integrity rose to the forefront, with a couple of additional notable points raised once the system was safe.

'The primary goal for us on site would be to make it safe.'

Preserving evidence allowing for subsequent investigations to better understand how the attack happened was raised by many participants in varying forms. This was also tied to appropriate chains of custody.

'Preserving evidence so that we can ensure then that we don't lose how it happened.'

Establishing communications between all relevant parties as quickly as possible was deemed highly important, from the person who detected an incident to shift managers and beyond. From this point onwards, participates felt entire pre-prepared response and recovery arrangements would fall into place.

Those in technical roles followed up on these goals with practical actions based on the two hypothetical scenarios. For example, removing all external communications points to prevent the continued manipulation of systems.

An emphasis was made by the participating inspector on the balance that was required between providing

safety, security, and business continuity and that a risk-based decision needed to be made based on the type of incident that was being responded to.

'The following questions need to be asked: do I continue operation? Is there a safety issue? Or is there a security issue where information or material and the protection of it can be undermined?'

Appendix B.2. Key Phases/Tasks

As a reminder, the identified phases/tasks are a direct output of discussion formulated through our hypothetical scenarios.

'. . . if it comes from operators, the first response is probably "something's broken" as opposed to "something's been hacked". . . '

Incident identification could come from several parties. For example, Security Operations Centres (SOCs) may have detected suspicious behaviour based on various data capture points. Alternatively, operators using impacted processes may be the first to highlight suspicious activity due to a loss of control. In the instance where operators are the first to raise concerns, it would likely be viewed as a system error instead of a cyber attack.

'Our arrangement would require the team that discovered the breach to contact our 24/7 site shift manager. . . '

Upon a system issue/incident being raised, escalation processes would be enacted. These typically involve notifying senior site managers in the first instance. A central incident control team would be formed, including key personnel to support decision-making processes. As scenario one is diverse, spanning both IT and OT systems, forming a centralised response team would include individuals from both sides of the organisation. In addition, specialised external support would be brought in. This support could come in the form of cyber security specialists, forensic analysis from third-party companies, for example. Alternatively, it might be operational engineering or safety-focused resources from partner or parents organisations.

'. . . he would need to know a high-level summary: what does it mean to the site, what could the impacts be, how long until you get it fixed, is it going to spread, etc.'

As a collective, the central incident control team would provide a diverse skill-set and knowledge-based to those in charge. Therefore, translating technical information into a language all parties can understand regarding the capabilities of the threat and what the potential impact could be, was deemed of great importance. This would provide a platform for response and recovery decision making moving forwards, including the initial formation and continuing involvement of appropriate personnel.

'We encourage the reasoning for decision making to be including on these log pads.'

Participants referred to priority systems, ticketing systems, logging systems, etc., as part of the fundamental setup of centralised incident control centres. These systems are brought in to allow for a coherent understanding, management, and recording of all subsequent response and recovery actions. This includes the criticality of the incident, reasoning behind decision making, and timings of actions taken and their resulting output.

'First of all, get it safe and secure. Preserve the evidence. And then look for how it happened with a view to then prevent it from happening again.'

Regarding the general operation of systems under attack, several factors came into focus aligned to the continued running vs shutdown of processes. These were naturally driven by safety; however, forensic data to support follow-up investigations was considered beyond this. The value of evidence was viewed as critical to better understand how the attack took place, where the gaps in system defences lie, and thus where additional focus is required moving forwards. This was also considered critical to subsequent recovery processes, giving confidence to the execution of follow-up actions, e.g. reloading backup configuration and knowing that will have the desired effect. Furthermore, the criticality of specific systems to the success of the business may be high. This could again deter from a complete shutdown where there is no risk from a safety perspective.

'We'd be looking for things on the intrusion prevention system and we'd be engaged directly with the SOC team to identify whether they've identified malicious activity.'

Response documents would be used to guide decision making throughout an incident. However, based on the hypothetical scenarios posed to participants, several key actions were noted from a technical perspective. These include, but are not limited to:

- Examine operational system logs.
- Examine intrusion prevention system and firewall logs.
- Examine web-proxy logs.
- Engage with SOC teams.
- Engage with forensic teams/conduct an analysis.
- Identify impacted workstations.
- Isolate impacted workstations.
- Block access to the attackers IP/Domain.
- Remove external connectivity.
- Check systems are up to date (e.g., OS and AV).
- Erase/replace devices and restore from backups.

These actions can all be used to support decision-making within the centralised incident control centre and would be communicated promptly to ensure all parties are kept up-to-date with each team's overall process. Thus, providing a complete picture of the incident and add assurance to the actions taken and their ability to restore normal, safe operations.

'The investigations are generally based on how wide an impact another incident like that could have. It starts at purely local to that plant. Then it's across the site as a whole. The highest level is anything that could happen to other sites.'

Considering post-incident outcomes, several relevant points have been raised throughout this section. However, a more comprehensive analysis of an incident would be undertaken. Differing levels of analysis and investigation would occur based on the impact of an incident or potential impact of a similar incident in the future.

'After every incident we do a lessons learned and implement actions on how to improve the resilience of our systems. We raise what we call a learning report and then a manager is assigned to that and then actions are put in.'

As a starting point, all logs taken during an incident would be reviewed. These, along with forensic and more technical details, can be used to form the basis of a lessons-learn/incident report. In addition to lessons-learn for internal review, these sources could also be included within any legal challenge or regulator inquiry, providing a clear timeline of events and rationale for every decision that was made. The report would typically provide an executive summary and an action-based output to address the root cause, offering suggested additional measures that could be applied to prevent any reoccurrence.

'There's no point in recovering and then being in the exact same position and them doing the same thing.'

The participating inspector explained that he would expect dutyholders to follow a playbook to take appropriate response actions in a timely manner.

'A lot of our dutyholders have playbooks to contrast which behaviours are anomalous and help them identify what is going wrong.'

A point was also made on how response actions could have adverse effects on evidence collection, highlighting that if a timely response was not critical, delaying the recovery process in favour of collecting evidence was recommended.

'There would have to be a decision made based on how much time can be dedicated to evidence gathering which would be A) to conduct a criminal or internal investigation and B) to inform Lessons Learnt since we would need to turn on the industrial zone and get it moving again as quickly as possible.'

Appendix B.3. Risk Evaluation

During response and recovery processes, it was widely acknowledged that important decisions must be made quickly to ensure systems remain stable, ensuring no safety-related risks are realised. Several interesting points were raised concerning the evaluation of risk during decision making, from risk owners to formal and semi-formal processes. However, it is important to note that risk evaluation was deemed cause agnostic. Therefore, the following points are mainly applicable to incidents caused through any means, malicious or otherwise.

'It's the job of the shift manager in the operational centre and the job of the controller of the day in the tactical centre to surround themselves with a team of specialists who provide advice to them.'

Starting with those involved in crucial risk decision making roles, while central teams are formed to manage an ongoing incident, they rely on subject matter expert knowledge from across the organisation. For example,

each operating system may have a supervisor; this role is ultimately responsible for ensuring its safe operation. As a result, supervisors will have an in-depth knowledge of operational processes, response documentation, the potential impact given actions could instigate, etc. Therefore, they would be called on to provide advice to central teams throughout an incident.

'We would have a response document and follow the right protocol.'

The processes for evaluating risk were mixed, formulated around understanding the consequences of all possible actions. Formal risk evaluation procedures did exist for specific scenarios, in addition to response documents with defined protocols. However, evaluation techniques, on the whole, were described mainly as semi-formal decisions made on the collective agreement of key stakeholders (as previously described), with the operational centre acting as a primary responsible party. However, each operational process's pre-existing assessments indicate their criticality and the impact that could be realised during an incident. Should an incident escalate to the point where individuals would be required to enter potentially hazardous areas of a facility, rigorous formal processes would be followed.

'There's a formal process including a briefing, agreement, and sign off, at different levels of authority before we'd send someone into a potentially hazardous situation.'

Safety formed the key consideration of risk evaluations. This was supported by environmental factors, the integrity of forensic resources/maintaining the chain of custody, and finally, reputational damage. Adding a reputational viewpoint was described as an attribute that could impact public perception, stimulating negative rhetoric on facilities' continued operation, and therefore should be considered where possible.

'The consequence of the risk would be based on safety first including environmental factors, and then reputation.'

As previously noted, pre-existing risk assessment documentation is used during decision-making processes. In addition to these, emergency arrangement teams regularly exercise incident response processes, refining them to pre-emptively capture all risks that could arise during an incident and improve the organisations ability to effectively minimise impact.

'Our emergency arrangements team would have exercises on this sort of thing to improve it and test it.'

Risk-based decisions would also change based on circumstances which could affect the impact of specific actions. For example, within the energy sector, an abundance of power is available during the summer as opposed to winter. The amount of risk associated with shutting down a power plant would, therefore, differ depending on the time of year.

Appendix B.4. Human Capital

Considering the human capital required during an incident, the previous sections have offered an initial insight. However, it is an important point for which additional detail is required.

'If I wasn't on duty, my line manager would take on my role as he is the senior C and I engineer.'

Considering the role profiles of participants, there existed very few examples of identical roles. However, each organisation's structure was constructed to account for loss of coverage, i.e., although in differing roles, individuals could step into their colleagues' shoes and perform the role required both up and down-stream.

'If there's an emergency on site, we always say that the whole site is at our disposal. Everyone understands that there's a responsibility to do what they need to do.'

Taking a more holistic view, it was considered that every individual working on a site would be at the disposal of the central emergency response team during an incident, with 24-hour on-call personnel covering key role profiles.

'We also have a contract with an external company. To do things like investigations and forensics. . . '

Extending out from localised on-site resources, all participants raised the possibility of pulling in additional resources from specialised third-party organisations (e.g., cyber security practitioners and forensic investigator), in addition to operational and engineering personnel from across the wider business, partner, or parent organisations, dependant upon the skill-set required.

'I would probably become more of a support to the OT side of things....My role would shift a little bit to lace the forefront.'

The aforementioned measure makes it hard to define precise numbers or skill-sets required during an incident, particularly given our scenarios' diverse nature. However, it was noted that specific roles could act in more of an advisory capacity where an incident has occurred on systems outside of their control or direct expertise.

If an incident were critical enough to affect multiple sectors or bring about danger to civilian life, then a range of stakeholders in the private sector, the regulatory body and the government would convene and decide upon the most appropriate action to take.

'Legislation and cooperation between stakeholders would allow timely decisions to be made to ensure that a safe outcome would be achieved.'

Appendix B.5. Use of Standards and Guidelines

Opinions of existing standards and guidelines were mixed amongst the participants. Some considered them to have matured over recent years, provide a valuable base of expertise. Others believed they were too focused on one specific domain and failed to capture similarities between IT and OT, resulting in inefficient activities.

The prevalence of existing standards and guidelines for use during the planning and execution of response and recovery activities was limited. Throughout the interviews, examples were discussed mainly from a higher-level viewpoint. This was achieved by identifying specific organisations responsible for standard and guideline development, as opposed to individual resources (e.g., The National Institute of Standards and Technology (NIST), not NIST SP800-82, SP800-53, etc.).

One participant also discussed an internal framework currently under development by centralised teams within their organisation, incorporating cyber incident response and recovery. However, the participant could not advise on its creation at a technical level and the level of concept/methodological coverage from existing standards and guidelines beyond an alignment to NIST.

No approaches derived from academic works were discussed.

Where existing standards and guidelines were discussed positively, highlighted attributes focused on an increased drive towards their adoption and increasing levels of maturity.

'. . . awareness was very limited prior to 2011-2012.'

The awareness level of appropriate standards and guidelines was noted as limited before 2011-2012. However, in parallel to the increased awareness over recent years, the level of standard and guideline maturity is also believed to have developed, increasing its value to this new audience.

'What's the point in us reinventing stuff when someone's already done it?'

Through the use of internal reviews, participants felt they had demonstrated good coverage across multiple aspects of cyber incident response and recovery. However, acknowledgement was made towards the use of existing expertise through the adoption of documented approaches rather than reinventing from the ground up.

'Historically, cyber was just considered to be "for the IT guys"; it's not anything to do with us.'

A broader acknowledgement of cyber security and related standards amongst non-IT-based personnel demonstrates an increased maturity level from an operational perspective. This involved conducting reviews as a collective group from multiple business areas to better understand requirements and the importance of cyber security from the more common health and safety viewpoint.

'It's not something that we could just say that "it's the geek stuff, you sort it out". . . I align it very much with an important health and safety focus.'

Where existing standards and guidelines were viewed in a negative light, a variety of points were raised. These were aligned mainly to variety, length, applicability, and complexity.

'There isn't particularly one that's the "magic" one'. . . '

Initial insights identified that no single resource was deemed appropriate for all aspects of cyber incident response and recovery and that, as a result, internally developed sector-specific approaches were under development using existing standards and guidelines as a base.

'. . . they're very IT focused and therefore very information focused as opposed to function.'

Participants with an OT background believe that existing standards and guidelines often lacked tooling and frameworks to adequately cover OT systems, applying an IT focus based on information instead of function. These were seen as barriers to their adoption.

'We'll have some guidance that is created for IT and then we'll end up having to do exactly the same work but created for OT. There's a lot of parallels and similarities.'

In contrast, participants with an IT background raised questions around the requirement for independent guidance, stated similarities exist between concepts from both IT and OT domains. This leads to a feeling of continued isolation, resulting in a counter-productive use of time and resources.

'I think that better guidance on how to implement said guidance and best practices would definitely help take the pain out of it all.'

The volume and depth of existing standards and guidelines from a usability perspective raised concerns about their application. With resources stretched, the ability to explore, understand and implement existing standards and guidelines dramatically increase the barrier to entry. This could result in inconsistencies, with participants demonstrating a desire to know everyone is efficiently pulling in the same direction, with approaches suitable for their organisation's size and scale/risk profile.

'. . . some of the guidance goes into too much detail rather than what we actually need.'

In more general discussions with key cyber security personnel, it was acknowledged that non-cyber security-focused colleagues would have a lower awareness level, but thanks to broader work programmes, it was now at a higher level of maturity than in previous years. In addition, processes and time allocation for reviewing existing standards and guidelines had been established.

The participating inspector argued that exercising and training, which can be derived from standards and guidelines, provides a significant benefit to dutyholders as it pushes them to be more familiar with processes thanks to hands-on experiences.

'As an engineer, what appears to be the best way is to get groups of people together and exercising them to develop muscle memory that can be used during real incidents.'