A Framework to Support ICS Cyber Incident Response and Recovery

Alexander Staves
Lancaster University, UK
a.staves@lancaster.ac.uk

Harry Balderstone
Lancaster University, UK
h.balderstone@lancaster.ac.uk

Benjamin Green
Lancaster University, UK
b.green2@lancaster.ac.uk

Antonios Gouglidis
Lancaster University, UK
a.gouglidis@lancaster.ac.uk

David Hutchison
Lancaster University, UK
d.hutchison@lancaster.ac.uk

ABSTRACT

During the past decade there has been a steady increase in cyber attacks targeting Critical National Infrastructure. In order to better protect against an ever-expanding threat landscape, governments, standards bodies, and a plethora of industry experts have produced relevant guidance for operators in response to incidents. However, in a context where safety, reliability, and availability are key, combined with the industrial nature of operational systems, advice on the right practice remains a challenge. This is further compounded by the volume of available guidance, raising questions on where operators should start, which guidance set should be followed, and how confidence in the adopted approach can be established. In this paper, an analysis of existing guidance with a focus on cyber incident response and recovery is provided. From this, a work in progress framework is posited, to better support operators in the development of response and recovery operations.

Keywords

ICS, CNI, Cyber Incident, Guidance, Response and Recovery

INTRODUCTION

The importance of defending Critical National Infrastructure (CNI) against cyber attacks has developed rapidly over the past decade. CNI can be defined as infrastructure on which a nation is reliant to function (e.g. power generation and water treatment) (Green, Krotofil, et al. 2016). In many instances, CNI is underpinned by Industrial Control Systems (ICS). These provide an interface between operational real-world processes and digital systems, providing operators, commonly referred to as Operators of Essential Services (OES), with monitoring, control, and automation capability; these need to be a focal point for protective efforts.

Historically, ICS were considered immune to network-based attacks due to their reliance on proprietary network protocols and hardware (Byres and Hoffman 2004). There is some truth to this notion, with isolated networks being intrinsically secure from most forms of attack due to their lack of external connectivity. However, a continued drive for interconnection has been prioritised due to the benefits it yields (e.g. process optimization, energy efficiencies, and proactive maintenance) (Galloway and Hancke 2013). The introduction of widely adopted protocols to support interconnectivity (i.e. TCP/IP) within this context can be considered the most significant technical evolution of recent years, while also the greatest catalyst of risk; this effect can be observed through an increase in attacks originating from the Internet (Kaspersky Lab ICS CERT 2018).

To begin ensuring consistent control of CNI security, governmental bodies have started to implement similar strategies. The United States of America (USA) assigned, in 2013, the National Institute of Standards and Technology

(NIST) the task of providing guidance on CNI Cyber-Security to OES (Office of the Press Secretary 2013). The European Union (EU) approved the introduction of the Network and Information Systems (NIS) Directive in 2016 into national laws of all of its member states (European Commission 2019). The United Kingdom (UK) created the National Cyber Security Centre (NCSC) in 2016 to provide advice and support to the public and private sector alike (NCSC 2020). However, while guidance supporting the evolution of ICS security, and compliance with regulations, equips operators with a starting point, it may not be complete and actionable. This is of particular interest for cyber incident response and recovery (R&R) best practice, where CNI and its supporting ICS are used in a variety of ways.

This paper explores existing guidance related to cyber incident R&R for CNI – more specifically, for CNI where ICS acts as a foundational base for its operation. We provide the following contributions:

- An overview of cyber incident R&R guidance for ICS.
- A breakdown of key cyber incident R&R phases.
- A criteria set used to evaluate the completeness of guidance across identified phases.
- A critical analysis of existing guidance based on the defined criteria.
- A work in progress framework to support OES in their development of cyber incident R&R activities.

The remainder of this paper first presents an overview of cyber incident R&R guidance. This is used to define key R&R phases, before a criteria set is defined. Using this criteria set, an analysis of existing guidance is undertaken. Finally, we present our work-in-progress framework, conclusion, and areas for future work.

CYBER INCIDENT RESPONSE AND RECOVERY GUIDANCE

The following subsections provide an overview of government and industry guidance, created to support OES in the development and delivery of cyber incident R&R capability. Initial exploration will focus on UK-centric resources, and any supplementary documentation (i.e. referenced material from the UK guidance). International resources are then reviewed with a focus on North America and France. These countries were selected based on their global nuclear energy presence (i.e number of reactors currently in operation) (IAEA 2018); thus guidance from these is typically of a greater maturity level, and offers the availability of documents written in English.

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 (NCSC 2019a). Objective D relates to guidance on R&R, and is broken down into two sub-objectives: Response and Recovery Planning, and Lessons Learned. The CAF also recommends consulting additional external resources (Cichonski et al. 2012; ISO/IEC 2016a; Creasy and Glover 2013).

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, its aim is to provide OES with a framework for managing cyber security risks and incidents that could impact the quality or availability of drinking water. Furthermore, it allows the DWI to assess an operator's security measures for compliance with the NIS Directive (DWI 2019). The DWI CAF is constructed around four top-level objectives, objective D being related to R&R (DWI 2018). This guidance also recommends consulting additional external resources (ISO/IEC 2017a; IEC 2011; NIST 2017).

NCSC 10 Steps: Incident Management

The NCSC 10 Steps for incident management provides a light-weight resource covering key considerations aligned to incident R&R activities (NCSC 2018). 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 (ONR 2017). The assessment principles contain ten Fundamental Security Principles (FSyPs), two of which are directly relevant to cyber incident R&R (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 use by ONR inspectors covering eleven topics related to cyber security event response (ONR 2019). While TAGs explicitly state that they are not a resource for demonstrating adherence to SyAPs, they can provide additional insight into what OES high-level goals should be. This guide also recommends consulting external resources (IAEA 2013; IAEA 2011; IAEA 2015; ENISA 2010; Carnegie Mellon University 2019; Kral 2019; Sweigart 2003; CIS 2019).

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 (HMG 2018). Although brief, one section describes requirements when preparing for, and responding to, security incidents. This is discussed using generic, non-cyber terminology, and is targeted towards government organizations.

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 (HSE 2018). Discussion in relation to cyber incident R&R is present throughout this guide. Guidance surrounding cyber incident R&R 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 (IEC 2011; ISO/IEC 2017a).

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 (IAEA 2013). Cyber security is mentioned only 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 incident).

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 (IAEA 2011). Specific details on cyber incident R&R are limited to generic guidance such as describing relevant responsibilities and response planning.

IAEA NSS 23-G

The objectives of NSS 23-G (IAEA 2015) are defined across 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 R&R are limited; however, content such as that found in Annex 2 (i.e. examples of sensitive information) could be of use 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 (ENISA 2010). Covered topics include R&R through the explanation of 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 useful reference point in understanding core CSIRT requirements (Carnegie Mellon University 2019).

SANS Incident Handler's Handbook

The SANS Incident Handler's Handbook details key phases of incident R&R, their purpose, tools that can be used to support them, etc. (Kral 2019). While this is not ICS specific, it provides a comprehensive discussion on R&R broken down into the following core sections: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

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) (Sweigart 2003).

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

CIS CSC presents 20 security controls (CIS 2019). 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 R&R 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 (Cichonski et al. 2012). A focus is placed on exploring methods for ensuring essential service continuity and impact mitigation.

NIST SP 800-53 (USA)

SP 800-53 provides a "catalogue of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks" (NIST 2017). This includes twenty mandatory controls, mapped to ISO/IEC 27001 (ISO/IEC 2017a), for securing assets including R&R.

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 (Creasy and Glover 2013). 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 then 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 (ISO/IEC 2017a). 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 Learned, 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 (ISO/IEC 2017b).

BS EN ISO/IEC 27035:2016

ISO/IEC 27035 serves as a reference for fundamental principles that are 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 R&R: detecting, reporting, assessing and responding to incidents, and applying lessons learned (ISO/IEC 2016a). Part 2, Guidelines to plan and prepare for incident response, describes how to plan and prepare for cyber incident R&R. This covers the "Plan and Prepare" and the "Lessons Learned" phases presented in Part 1 of the standard (ISO/IEC 2016b).

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 reviewed. Part 2-1 of this series provides guidance for establishing an ICS security program including planning for incident R&R (IEC 2011). Part 4-2 of the series describes the technical security requirements for ICS components including guidance on how to ensure that systems respond in a timely manner to security violations by alerting the appropriate personnel and reporting details on the violation (IEC 2019).

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 (ISO/IEC 2017c). 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 R&R guidance for nuclear operators (NRC 2010). Guidance is provided under high-level requirements for establishing a cyber security plan in relation to incident R&R.

Nuclear Energy Institute (NEI) 08.09 (USA)

NEI 08.09 is closely linked to NRC RG 5.71 (NEI 2010). R&R 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 (NIST 2018). It provides a common organising structure for multiple approches to cybersecurity by assembling standards, guidelines and practices into one document. Five core functions are defined, two of which are related to R&R.

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 (Stougger et al. 2015). ICS-specific guidelines for R&R 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 OES understand and mitigate risks associated with malware incidents, including associated practical guidance on response activities (Souppaya and Scarfone 2013).

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 (Bowen et al. 2006). Guidance on R&R 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" (NERC 2019).

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" (CNSC 2014). While this section provides a set of guiding principles focused on ties to safety, the inclusion of cyber specific incident R&R guidance is limited.

ANSSI Managing Cyber Security for Industrial Control Systems (France)

Coverage of cyber incident R&R 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 (ANSSI 2012).

Response and Recovery Phases

In order to provide a critical analysis of the reviewed documents, the key phases and sub-phases that OES are advised to adopt must first be defined. From these, a criteria set can be built and its coverage can then be measured.

Using the reviewed documents, the following key phases and sub-phases have been extracted. This provides a complete overview of elements identified within the reviewed guidance:

- Planning Phase:
  - Define Roles and Responsibilities
  - Document Response Planning Activities
  - Conduct Asset Criticality Assessment
  - Document Risk Management Process
  - Perform Threat Analysis
- Preparation Phase:
  - Conduct Personnel Training
  - Perform Regular Tests and Audits
  - Implement Incident Detection Capabilities
- Mid-Incident Phase:
  - Ensure Resource Availibility
  - Conduct Incident Reporting
  - Perform Incident Containment
  - Perform Incident Eradication
  - Perform Incident Recovery
- Post-Incident Phase:
  - Conduct Root Cause Analysis
  - Document Lessons Learnt
  - Collect Evidence
  - Manage Public Relations Communication

CRITICAL ANALYSIS

The following section provides a critical analysis of the guidance discussed across the previous section, making use of established R&R phases as a base. This highlights the value of each resource, and identifies areas that are in need of further development.

Methodology

When assessing the effectiveness of current guidance for ICS R&R, relevant requirements must be identified. These are chosen based on the identified R&R phases from the previous section: Planning, Preparation, Mid-Incident and Post-Incident. A breakdown of these is illustrated within Table 1. A criteria set has been defined alongside these, to ensure a structured and in-depth analysis can be undertaken. Additional criteria of technical and non-technical factors have also been included allowing for a clearer understanding of the target user. Operators may favor technical documents, whereas those in management roles may prefer higher level non-technical documents, for example.

Table 1. Requirements and Criteria for Document Analysis

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.
	Risk Management (RM)	Contains information on creating and consulting risk management documents.
	Threat Analysis (TA)	Contains information on conducting a continuous threat analysis for remediating identified vulnerabilities and minimising attack vectors.
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.
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.
	Evidence Collection (EC)	Contains information on evidence collection for use by external authorities.
	Public Relations Management (PRM)	Contains information on public information disclosure management.

Results

The results of the analysis have been compiled into Tables 2 and 3. At a high-level, topic areas with substantial coverage can be identified, and a clear disparity across the reviewed guidance set is evident.

The majority of documentation reviewed contains high level details, with only ~54% of these providing technical guidance. Since ICS implementations can differ between environments, hardware specific technical guidance is not always recommended. However, due to the technological nature of the subject area, a lack of technical guidance may present a challenge, or indeed a problem, for OES during practical implementation.

To provide a clearer discussion on findings, the following subsections provide a breakdown across each of the key R&R phases.

Table 2. Document Analysis Results (Part One)

	Type		Planning					Preparation		
Guidance/Standard	**NT**	**Tec**	**RR**	**RP**	**CA**	**RM**	**TA**	**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)	✓	✓	✓	✓	✓	✓	✓	✓		✓

Planning Phase

The majority of publications (~80%) discuss 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%).

Preparation Phase

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 (NCSC 2019b).

Mid-Incident Activities

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 drastically and adversely affect the impact of an incident.

Table 3. Document Analysis Results (Part Two)

	Mid-Incident					Post-Incident			
Guidance/Standard	**RA**	**IRep**	**IC**	**IE**	**IRec**	**RCA**	**LL**	**EC**	**PRM**
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)					✓				

Post-Incident Activities

Of all the phases undertaken during R&R operations, post-incident activities contains the greatest level of inconsistencies. Lessons Learned are well covered (~66%); however, Root Cause Analysis, Evidence Collection, and Public Relations Management coverage is limited (~31%, ~31%, and ~19%, respectively). The reduced level of discussion on Post-Incident topics is surprising, 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 R&R 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.

Analysis: Concluding Remarks

Through the analysis of these publications, a lack of consistency has been highlighted. Although the core topics surrounding R&R activities are discussed in most documents, such as Roles and Responsibility assignment and Response Plan Documenting, less-common topic areas, such as Evidence Collection or Public Relations Management appear irregularly. Concerns will surely arise if OES are recommended to consult documents that do not discuss these topics, meaning that important topic areas may be unintentionally overlooked. The lack of consistency throughout available guidance highlights the need for amalgamation into one resource that OES are able to use reliably. This will give them the confidence that they are consulting the most in-depth material on R&R activities. The following section will cover the design of a work-in-progress framework, constructed to address the limitations in existing guidance.

FRAMEWORK PROPOSAL

In order to remediate the inconsistencies discovered in current available guidance, a framework that aims to make guidance on R&R more accessible and comprehensible has been drafted. The current progress on this framework can be seen in Figure 1. The purpose of this framework is to break OES' R&R capabilities into a more granular and

manageable set of processes and controls. The contents for this framework are based on the information presented throughout the reviewed standards and guidelines.

As shown in Figure 1, our framework is broken down into the four R&R processes, as per the criteria table used during the analysis of existing guidance (see Table 1). Within each, processes and/or controls are defined. The framework will be composed of two main sections: an in-depth explanation of the controls and related sub-controls/processes; and a summary table used for quick referencing. The table will contain a list of all the controls, each containing a set of sub-controls/processes, accompanied by a short explanation. Each of these will then be mapped to a data source, which provides methods or tools used to aid OES in following the framework. Furthermore, external resources on these sub-controls/processes will be referenced should additional information be required. Table 4 demonstrates what a portion of the final framework will look like.

As an example of its use, the control "Criticality Assessment" (belonging to the Planning phase) is composed of four sub-controls/processes. The sub-control "ID Non-Physical Assets" can be achieved by obtaining database meta-data and software version numbers. Additional resources available for this sub-control are ISA 62443-2-1 4.2.3.4/6, ISA 62443-3-3 SR 7.8 and more.

This framework is still under development and is presented in its current version. It is subject to change based on the findings of future work, as discussed in the next section.

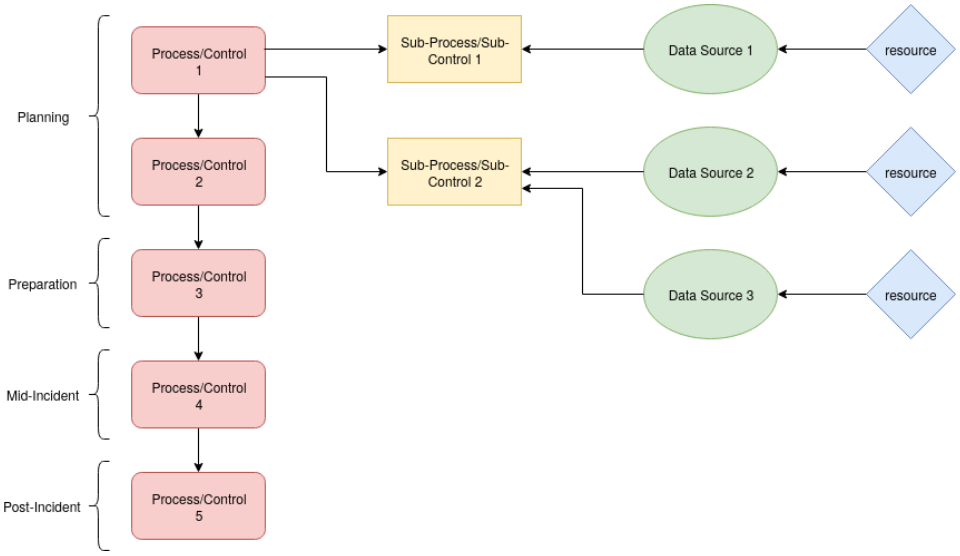

Figure 1. Framework Design - each process/control has an associated set of sub-processes/controls, data sources and resources

CONCLUSION AND FUTURE WORK

As shown, an (over)abundance of available guidance exists for OES to consult. Reviewed resources include publications 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). An analysis of the guidance from these sources concluded that a lack of consistency exists between the disseminated information. Because of this, if OES fail to consult a comprehensive set of resources, their processes run a risk of being incomplete. This lack of consistency highlights the need to amalgamate all essential elements of guidance for R&R activities into one resource. A draft version of a more complete resource has been created to address this limitation in existing guidance. Its continued evolution will be supported by future work, including the development of an ICS testbed and attack scenarios, used to obtain an industry perspective from key stakeholders, in parallel to an ongoing in-depth review of existing academic literature.

Over the past five years, Lancaster University has constructed an ICS testbed through the procurement and implementation of physical real-world hardware and software, produced by major ICS vendors including Siemens, Schneider, Cisco, PTC, etc. This ensures that the testbed is able to accurately represent a real-world network of ICS devices, and therefore affords a high degree of confidence in applicability to real-world environments (Green, Le, et al. 2017). Using the testbed, synthetic attack scenarios are currently being developed. Creation of these attack

Table 4. Excerpt from the Proposed Framework (subject to change)

Phase	Control	sub-control / process	Data Source	
Planning	**1) Criticality Assessment:** identify and assess criticality of all assets	**1.1) ID Physical Assets:** Identify and assess criticality of Physical Assets (hardware, infrastructure)	hardware inventory, building plans	CIS CSC 1 13, 14, COBIT 5 BAI09.01/02 ISA 62443-2-1 4.2.3.4/6 ISA 62443-3-3 SR 7.8 ISO/IEC 27001 A.8.1.1/2, A.8.2.1 NIST SP 800-53 CM-8, PM-5
		1.2) ID Non-Physical Assets: Identify and assess criticality of Non-Physical Assets (software, data)	database meta-data, software version number	CIS CSC 2, 13, 14 COBIT 5 BAI09.01/02/05 ISA 62443-2-1 4.2.3.4/6 ISA 62443-3-3 SR 7.8 ISO/IEC 27001 A.8.1.1/2, A.8.2.1, A.12.5.1 NIST SP 800-53 CM-8, PM-5
		1.3) ID Human Assets: Identify and assess criticality of Human Assets (employees, external)	employee records, employee timesheets, list of employed third party companies	*WiP*
		1.4) Map Communication and Data Flows	*WiP*	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1 4.2.3.4 ISO/IEC 27001 A.13.2.1/2 NIST SP 800-53 AC-4, CA-3, CA-9, PL-8
	2) Threat Analysis: conduct continuous Threat Analysis on all assets	**2.1) Vulnerability Scanning:** Regularly conduct (known) vulnerability scans on all assets	vulnerability scanning tool information, CVE database, scan scheduling	CIS CSC 3 *WiP*
		2.2) Firmware Updates: Update firmware for systems obtained from a trusted source (vendor)	firmware version number, communication method for obtaining new firmware, update scheduling	CIS CSC 3 *WiP*
		2.3) ID Zero Days: Identify potential zero day vulnerabilities (internal testing team, bug bounty program)	test scheduling, bug bounty funding	*WiP*

scenarios will serve as a means of testing the thoroughness and effectiveness of the proposed framework. These scenarios will be tested and modified using the University ICS testbed in an attempt to mimic real-life scenarios. One of the currently developed scenarios corresponds to a Denial of Service Attack, which is broken down into the following four stages (See Figure 2 for a graphical representation of the attack scenario):

- Stage 1: Compromise a router through the use of password brute-forcing. Once access is gained, leverage existing VPN configuration and reconnect as a trusted user.
- Stage 2: Enumerate devices in the Industrial Zone. Where possible, extract relevant data (e.g device configuration and process control logic) for offline analysis.
- Stage 3: Take external monitoring systems offline.
- Stage 4: Take the PLC offline.

Using the developed attack scenarios, key industry stakeholders will be consulted in order to explore adopted methodologies for R&R operations, including the use of existing guidance. The following roles have been included as a starting point for exploration: cyber security personnel, system operators, system managers, system engineers,

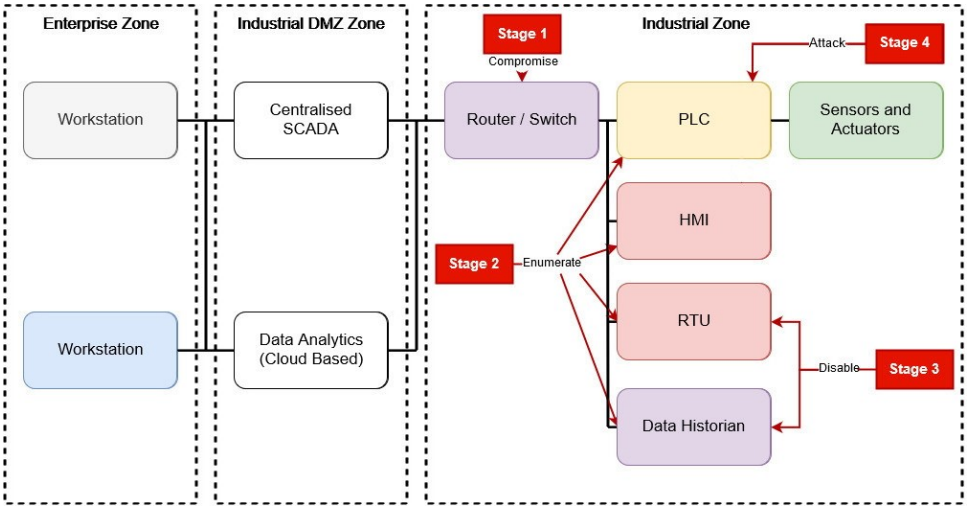

Figure 2. DoS Attack Scenario

safety managers, and regulators. Obtaining an industry perspective will provide key additional information, giving an important practical support to the framework.

To ensure a comprehensive analysis of current guidance has been undertaken, existing academic literature will also be investigated. Relevant works will be reviewed for thematic similarities, to both reinforce our previous findings and to gain an understanding of how/where identified gaps may have been addressed by the academic community.

The findings from both industry engagement and existing literature will be used to support the development of our proposed framework, aiming to ensure in future a more comprehensive and robust set of processes and controls.

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 as part of the UK's Nuclear Innovation Programme.

REFERENCES

ANSSI (2012). *Managing Cybersecurity for Industrial Control Systems*. Tech. rep. Agence Nationale de la Sécurité des Systèmes d'Information.

Bowen, P., Hash, J., and Wilson, M. (2006). *NIST Special Publication 800-100: Information Security Handbook - A Guide for Managers*. Tech. rep. National Institute of Standards and Technology.

Byres, E. and Hoffman, D. (2004). "The myths and facts behind cyber security risks for industrial control systems". In: *In Proc. of VDE Kongress*.

Carnegie Mellon University (2019). *The CERT Division*. URL: https://www.sei.cmu.edu/about/divisions/cert/index.cfm (visited on 01/20/2020).

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2012). *NIST Special Publication 800-61: Computer Security Incident Handling Guide*. Tech. rep. National Institute of Standards and Technology.

CIS (2019). *CIS Critical Security Controls*. Tech. rep. Center for Internet Security.

CNSC (2014). *REGDOC-2.5.2 Design of Reactor Facilities: Nuclear Power Plants*. Tech. rep. Canadian Nuclear Safety Commission.

Creasy, J. and Glover, I. (2013). *Cyber Security Incident Response Guide*. Tech. rep. Council for Registered Ethical Security Testers.

DWI (2018). *Guidance on the Implementation of the NIS Regulations 2018 - The Cyber Assessment Framework (CAF)*. Tech. rep. Drinking Water Inspectorate.

DWI (2019). *CAF Information*. URL: http://dwi.defra.gov.uk/nis/caf/index.html (visited on 01/20/2020).

ENISA (2010). *Good Practice Guide for Incident Management*. Tech. rep. European Network and Information Security Agency.

European Commission (2019). *The Directive on Security of Network and Information Systems (NIS Directive)*.

Galloway, B. and Hancke, G. P. (Second 2013). "Introduction to Industrial Control Networks". In: *IEEE Communications Surveys Tutorials* 15.2, pp. 860–880.

Green, B., Krotofil, M., and Hutchison, D. (2016). "Achieving ICS Resilience and Security Through Granular Data Flow Management". In: *Proceedings of the 2Nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, pages 93–101.

Green, B., Le, A., Antrobus, R., Roedig, U., Hutchison, D., and Rashid, A. (2017). *Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research*. Tech. rep. Lancaster University.

HMG (2018). *HMG Security Policy Framework*. Tech. rep. Her Majesty's Government.

HSE (2018). *Cyber Security for Industrial Automation and Control Systems (IACS)*. Tech. rep. Health and Safety Executive.

IAEA (2011). *IAEA Nuclear Security Series No. 17*. Tech. rep. International Atomic Energy Agency.

IAEA (2013). *Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime*. Tech. rep. International Atomic Energy Agency.

IAEA (2015). *IAEA Nuclear Security Series No. 23-G*. Tech. rep. International Atomic Energy Agency.

IAEA (2018). *Nuclear Share of Electricity Generation in 2018*.

IEC (2011). *BS IEC 62443-2-1:2011*.

IEC (2019). *BS EN IEC 62443-4-2:2019*.

ISO/IEC (2016a). *BS ISO/IEC 27035-1:2016*.

ISO/IEC (2016b). *BS ISO/IEC 27035-2:2016*.

ISO/IEC (2017a). *BS EN ISO/IEC 27001:2017*.

ISO/IEC (2017b). *BS EN ISO/IEC 27002:2017*.

ISO/IEC (2017c). *BS EN ISO/IEC 27019:2017*.

Kaspersky Lab ICS CERT (2018). *Threat Landscape for Industrial Automation Systems: H1 2018*.

Kral, P. (2019). *Information Security Reading Room: Incident Handler's Handbook*. Tech. rep. SANS Institute.

NCSC (2018). *10 Steps to Cyber Security: Incident Management*. URL: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/incident-management (visited on 01/21/2020).

NCSC (2019a). *NCSC CAF Guidance*. URL: https://www.ncsc.gov.uk/collection/nis-directive?curPage=/collection/nis-directive/introduction-to-the-nis-directive (visited on 01/21/2020).

NCSC (2019b). *NCSC CAF Guidance Objective C - Detecting Cyber Security Events*. URL: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-c-detecting-cyber-security-events (visited on 01/21/2020).

NCSC (2020). *About the NCSC: What We Do*. URL: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do (visited on 01/21/2020).

NEI (2010). *NEI 08-09 Cyber Security Plan for Nuclear Power Reactors*. Tech. rep. Nuclear Energy Institute.

NERC (2019). *CIP-008-6 - Cyber Security - Incident Reporting and Response Planning*. Tech. rep. North American Electric Reliability Corporation.

NIST (2017). *Draft NIST Special Publication 800-53, Revision 5, Initial Public Draft*. Tech. rep. National Institute of Standards and Technology.

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Tech. rep. National Institute of Standards and Technology.

NRC (2010). *RG 5.71 Cyber Security Programs for Nuclear Facilities*. Tech. rep. Nuclear Regulatory Commission.

Office of the Press Secretary (2013). *Executive Order - Improving Critical Infrastructure Cybersecurity*.

ONR (2017). *Security Assessment Principles for the Civil Nuclear Industry*. Tech. rep. Office for Nuclear Regulation.

ONR (2019). *Office for Nuclear Regulation (ONR) Permissioning Inspection - Technical Assessment Guides*. URL: http://www.onr.org.uk/operational/tech_asst_guides/ (visited on 01/21/2020).

Souppaya, M. and Scarfone, K. (2013). *NIST Special Publication 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. Tech. rep. National Institute of Standards and Technology.

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

Sweigart, C. (2003). *SCORE Security Checklist*. Tech. rep. SANS Institute.