applied sciences

MDPI

Article

A Harmonized Information Security Taxonomy for Cyber Physical Systems

Johannes Hendrik Pool * and **Hein Venter**

Digital Forensic Science Research Group, Department of Computer Science, University of Pretoria, Pretoria 0002, South Africa

* Correspondence: cobus.pool@protonmail.com; Tel.: +27-(0)84-603-3090

Abstract: Cyber physical systems (CPSs) are found in many aspects of daily life, and they control and protect energy production, manufacturing and even healthcare. Due to long lifecycles and the use of legacy technologies, its associated security comes with many challenges. Security taxonomies are useful to classify and communicate security-related information and elements. Despite the existence of numerous taxonomies, they are fragmentary, limited to only specific lifecycle phases or cover only specific aspects. A harmonized taxonomy must be applicable to all lifecycle phases of the CPS. This paper presents well-established taxonomies that are combined into a single comprehensive and harmonized taxonomy and allows application throughout the different lifecycle phases. Application of the taxonomy to real-world scenarios requires a consistent implementation methodology. The use of the harmonized taxonomy methodology is demonstrated by applying it to an actual incident case study. The taxonomy is used to identify information security gaps through its implementation in the industrial facility in question. The identified gaps are then addressed as part of the security lifecycle of the CPS. The harmonized taxonomy can be expanded to apply it to industries with specific requirements.

Keywords: cyber physical systems; risk management; taxonomy; information security; industrial control and automation

check for updates

Citation: Pool, J.H.; Venter, H. A Harmonized Information Security Taxonomy for Cyber Physical Systems. *Appl. Sci.* **2022**, *12*, 8080. https://doi.org/10.3390/app12168080

Academic Editors: You-Jin Song, Howoon Kim and Hyun-Jong Cha

Received: 7 March 2022
Accepted: 24 March 2022
Published: 12 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cyber physical systems (CPSs) have become an essential part of modern society. They are utilized in a wide variety of applications from manufacturing, energy and transportation to building automation and home appliances. Securing CPSs requires a unique approach, as modern CPSs tend to be a hybrid of legacy systems with unsecured communication protocols, proprietary control equipment and commercial off-the-shelf hardware for human machine interfacing. This implies that the information security implementation for CPSs would need a hybrid approach as well. Due to fundamental differences in structure, including network topology, security objectives and availability requirements, security deployment in CPSs is much more restrictive than it would be in general IT systems [1].

Information security is primarily concerned with risk mitigation and management [2]. This is even more pertinent when considering CPSs, which can include industrial control and automation, safety and protection systems [3], where compromising the system can lead (and has in fact led) to damage to the plant [4] or even loss of life [5]. One way of contextualizing the information associated with information security implementation and management is by applying taxonomies.

Taxonomies are useful in information security to assist in the classification and grouping of information. This, in turn, assists in ensuring that users, decision makers and distributors of the security information all use the same terms of reference. A taxonomy is especially useful when it is comprehensive and relational [6], as this allows a relative or relational placing of every aspect of both information security implementation and incident management. Furthermore, this relative placing allows for specific information security implementation and incident management aspects to be uniquely categorized. Because of this, taxonomies form an important part of information management frameworks [7].

A comprehensive and consistent information security management framework for CPSs that addresses the full lifecycle—without unnecessary complication—is not available. Taxonomies related to information security tend to address limited aspects of security management. More comprehensive taxonomies for CPSs [8] have been proposed, but these taxonomies still concentrate on specific aspects, like incidents, and are not applicable throughout the system's lifecycle. The main goal of the current paper is to address the fragmented coverage of this dilemma by providing a broad, harmonized taxonomy for CPSs. This is accomplished by investigating the existing taxonomies in both the information and operational technology fields and combining them into a cohesive whole.

The rest of this paper is constructed as follows. The background section analyzes the leading standards and considers the typical lifecycles described by these standards. This is followed by a discussion of the established taxonomies. In the next section, the taxonomies are grouped into core elements, followed by a section that provides the harmonized taxonomy. The latter is validated by mapping a well-known case study to the taxonomy in the penultimate section, which is followed by the conclusion of the paper.

2. Background

Due to the nature of CPSs, it is natural to focus primarily on cybersecurity instead of on information security. Although there are differences in definition, information security generally entails safeguarding all information important to a business's operation, irrespective of the format or storage location. Cybersecurity, on the other hand, focuses on information in electronic format and on the devices responsible for storing, transferring and securing this information [9]. Theft of intellectual property through industrial espionage by deploying custom-developed tools like Duqu [10,11] against companies is problematic. Duqu is a modular piece of malware focused on collecting and extracting information that can be used to carry out targeted attacks on CPSs. Combating such threats requires a wider information security focus, and the guidance of accepted standards assists in this.

The following section provides an overview and comparison of the most well-known standards. This is followed by a discussion on the lifecycles presented in the standards, a risk overview and an analysis of some established taxonomies.

2.1. Focus and Limitations of the Leading Standards

Several standards are available that can be utilized as guiding frameworks to implement information security management systems, but there are limitations to each of them. The standards' focuses and limitations are shown in Table 1.

Table 1. Overview and comparison of standards and frameworks and their limitations.

Standard	Body	Focus	Limitation
ISO27000 suite	ISO	General information technology as found in the business and consumer markets.	Limited applicability to CPS as it does not consider the limitations of industrial systems, such as extended lifecycles and the inability to frequently apply patches.
IEC62443 suite	ISA	Specific to industrial systems like supervisory and data acquisition systems (SCADA).	Incomplete, as important modules such as the system lifecycle have still not been published.
NERC CIP	NERC	Specific to bulk electricity supply systems (BESs).	Many of the more generic equipment and technology types found in CPSs are not covered, as they do not apply to BESs.
NIST 800	NIST	Broadly applicable to information systems, with SP800 82R2 specific to CPSs.	NIST 800 SP 82R2 references many other standards, resulting in inconsistencies, such as with the lifecycle module reference.

2.2. Standards' Lifecycles

The following sections examine the lifecycles considered to be the best practices by each of the major standards. These standards are the following:

- ISO27000: Information security management systems;
- IEC62443: Security for industrial automation and control systems;
- NERC CIP: North American Electric Reliability Corporation Critical Infrastructure Protection;
- NIST 800-82R2: Guide to industrial control systems (ICS) security;

Since the standards differ in approach and intent, there are some unique aspects to each. Where applicable, these inconsistencies are highlighted.

2.2.1. ISO27000: Information Security Management Systems

The ISO27000 suite covers an extensive range of topics, and while there is no single or definitive security lifecycle, there is an application flow, shown in Figure 1. This resembles the economics-based Deming cycle to ensure continuous quality improvement [12].

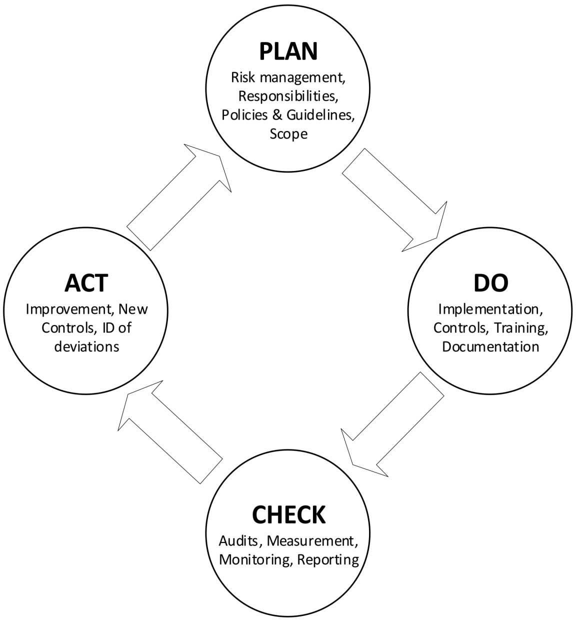
PLAN
Risk management, Responsibilities, Policies & Guidelines, Scope
DO
Implementation, Controls, Training, Documentation
CHECK
Audits, Measurement, Monitoring, Reporting
ACT
Improvement, New Controls, ID of deviations

Figure 1. The ISO27000 PDCA cycle for ISMS [13].

Though widely applied, it does not provide a specific focus on CPS implementation. For CPSs, availability and integrity—rather than confidentiality—are the primary concerns. For IT information security, on the other hand, confidentiality has the highest priority. A similar iterative process is found in other standards.

2.2.2. IEC62443 Suite: Security for Industrial Automation and Control Systems

The IEC 62443 suite is under development by the International Society for Automation (ISA) workgroup for industrial cybersecurity. The suite is envisioned to eventually cover the full spectrum of industrial cybersecurity management systems. While being a widely applied standard for industrial systems, it is still incomplete. The IEC62443-1-4 module has been in development since 2013. Unlike the ISO27000 cycle, this standard presents three distinct lifecycles:

- Security development lifecycle assurance, which focuses on the equipment manufacturers, as detailed in IEC62443-4-1 (it falls outside the scope of this paper and is therefore not discussed further here);
- The automation solution lifecycle;
- The cybersecurity lifecycle.

Automation System Operational Lifecycle

The intention of the automation solution and CPS lifecycle is to show the phases that are found in the design, implementation, and operation of a CPS (see Figure 2).

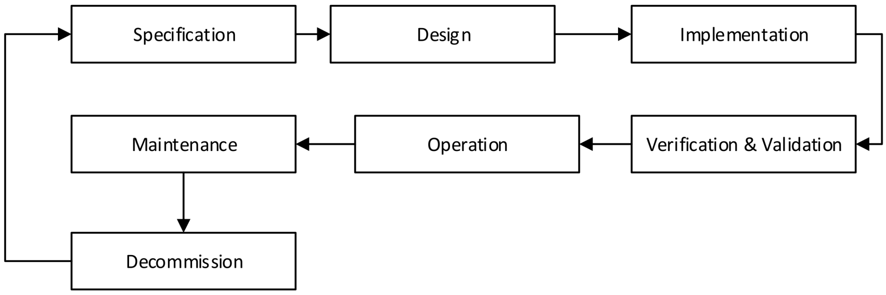

Figure 2. Automation solution (CPS) lifecycle as per ISA99 [14].

Changes to or incidents on the system should trigger the responsible party to initiate a security review for the system. The recommended triggers for re-evaluation are well defined in IEC62443-2-4, but in summary, they include the following common occurrences:

- Changes in system communication design or methodology;
- Process operational changes that impact the control or safety systems;
- Any modification of safety parameters or changes to the safety system;
- Expansion of or changes to the system hardware.

The CPS Security Lifecycle

The security lifecycle consists of three main phases:

- Risk assessment;
- Design and implementation of countermeasures;
- Monitoring and maintenance.

These phases are shown in Figure 3.

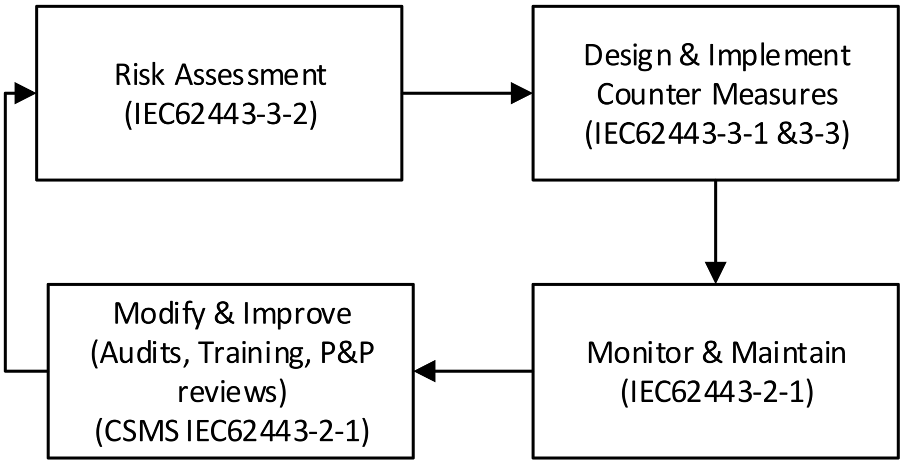
Risk Assessment (IEC62443-3-2)
Design & Implement Counter Measures (IEC62443-3-1 &3-3)
Modify & Improve (Audits, Training, P&P reviews) (CSMS IEC62443-2-1)
Monitor & Maintain (IEC62443-2-1)

Figure 3. CPS security lifecycle.

The security lifecycle is applied during the first three phases of the automation solution lifecycle and then on a periodic or triggered basis during the maintenance phase.

2.2.3. The NERC CIP Standard

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard is an extensive suite of modules that are frequently used across the world. In South Africa, Eskom (a national electricity provider) uses it as the basis for its cybersecurity specifications. While it applies general security concepts and principles, it is focused on bulk electricity supply (BES) applications.

The lifecycle presented by NERC CIP, as shown in Figure 4, is found in CIP-013-1. This lifecycle is focused on supply chain management and on ensuring the minimum levels of procured device security.

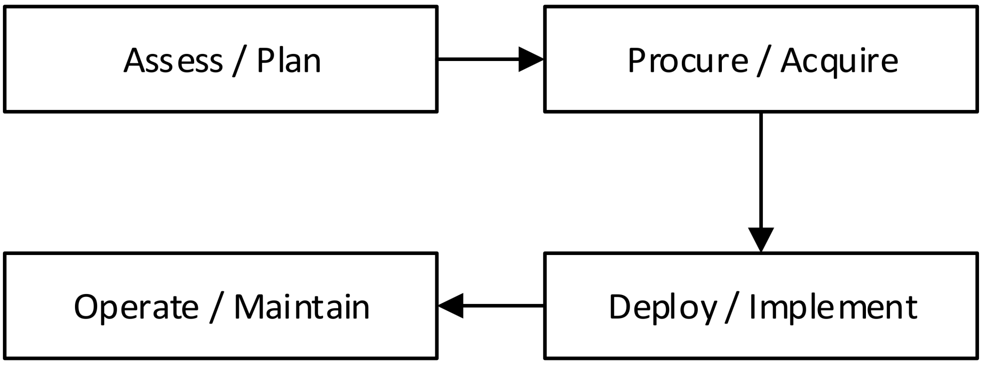

Figure 4. Notional BES cyber system lifecycle [15] NERC-CIP-013-1.

This lifecycle is like the ISA system lifecycle presented earlier. Periodic reassessment is required during the maintenance phase, although the exact requirements for this are not defined.

2.2.4. NIST SP 800-82R2: Guide to Industrial Control Systems (ICS) Security

The National Institute of Standards and Technology (NIST) 800 series of standards focuses on security, and 82R2 details the requirements for industrial systems or CPSs. The lifecycle is not defined in this standard. It references NIST SP 800-64, but this has been superseded by NIST SP 800-160V1. The cycle is shown in Figure 5.

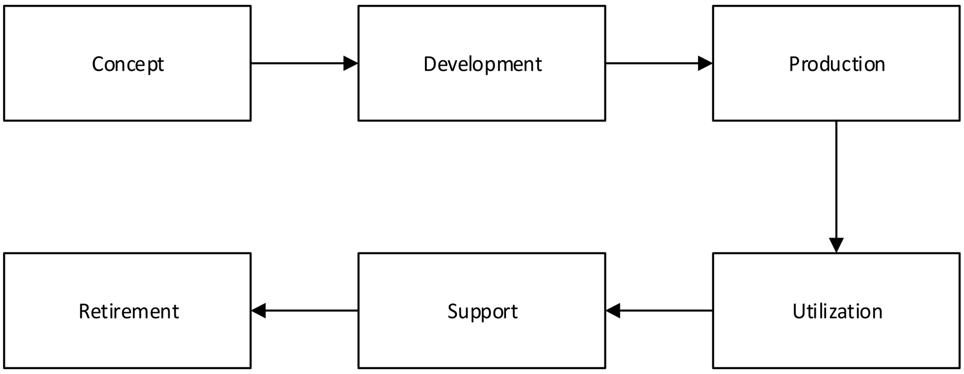

Figure 5. Recommended lifecycle by NIST SP 800-160-V1.

As can be observed, the standards present certain elements that are common to all the lifecycles:

- An initial or concept phase that includes assessment and planning for the systems and associated security (the first risk assessment should take place here);
- Implementation of the system and security design;
- Operating the asset with periodic reassessments and adjustment of the security implementation;
- Decommissioning of the asset, which includes sanitization of information to ensure information security.

If one considers that risk assessment and management feature prominently in the lifecycle phases, there needs to be an understanding of what is meant by risk. The following section provides such a definition.

2.3. Risk Defined

Risk can be quantified as follows:

$$\text{Risk} = \text{Impact} \times \text{Likelihood} \tag{1}$$

Price et al. [16] broke it down further:

$$\text{Risk} = \text{Impact} \times \text{Threat} \times \text{Vulnerability} \tag{2}$$

To control risk, the following actions can be taken:

- Assess business and system risk;
- Manage threats;
- Reduce vulnerabilities;
- Support risk reduction through protection measures (technology) and by implementing analyses (digital forensics) and improvement cycles in response to incidents.

Thus, the taxonomies selected and utilized should enable or facilitate the above risk assessment and reduction actions. The following section contains a discussion of the established taxonomies that have a bearing on this research.

2.4. Established Taxonomies

This section serves as an introduction and overview of some selected established taxonomies, and a detailed discussion follows in Section 3.

Since risk management is a fundamental aspect of information security, business risk taxonomies were considered. The taxonomy by Young et al. [17] (see Figure 6) was selected due to the comprehensive coverage it provides for business risk assessment.

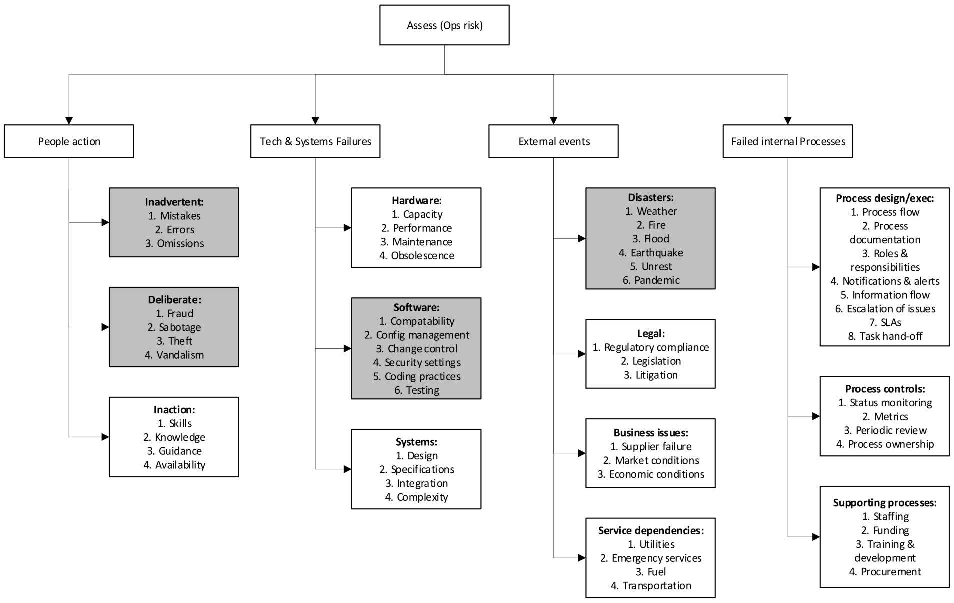

Figure 6. Operational cyber risk taxonomy [17].

The shaded areas are elements that are found in other taxonomies as well, such as those detailing threats and vulnerabilities. The presented taxonomies were selected either to support the operational risk taxonomy (as is the case with the threat and vulnerability taxonomies) or to expand on it (as with the technology and digital forensics taxonomies). Flowers et al. [18] compiled a selection of threat and vulnerability taxonomies related specifically to CPSs. These taxonomies, as well as the one by Bodungen et al. [19], were considered, and they classified threat scenarios in terms of the three categories shown in Figure 7.

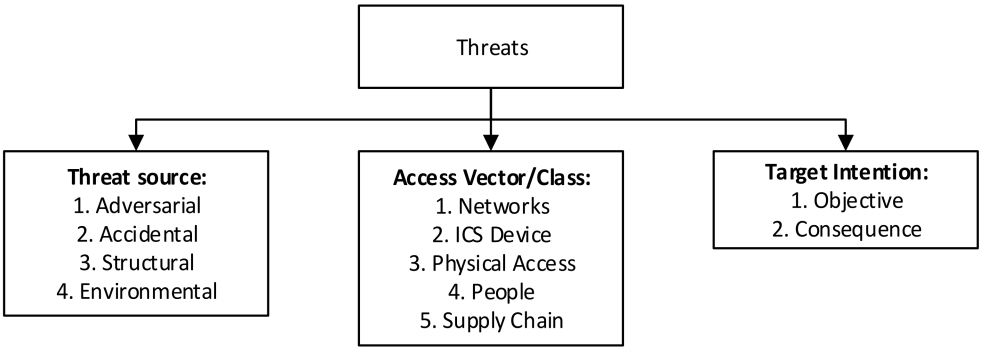

Figure 7. Threat taxonomy [19].

- The source: who or what is the origin of the threat?
- The access vector: what route is utilized to get into the system?
- Intention: what is the aim of the system compromise?

The vulnerability taxonomy by Bodungen et al. [19], as shown in Figure 8, postulates that there must be a weakness or failure of some kind that allows the threat scenario to take place. The vulnerabilities are grouped into the following categories:

- Policies and procedural failures;
- Nonadherence to standards (control failures);
- General cyber vulnerabilities exposed by a cyber vulnerability analysis (CVA).

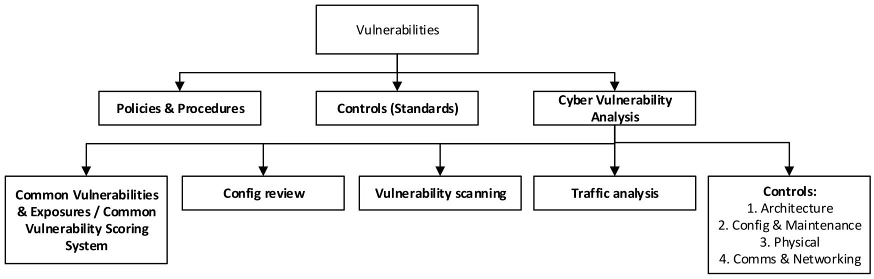

Figure 8. Vulnerability taxonomy [19].

The vulnerability taxonomy selected was that of Fleury [20], as this fit better with the operational risk taxonomy (see Figure 9).

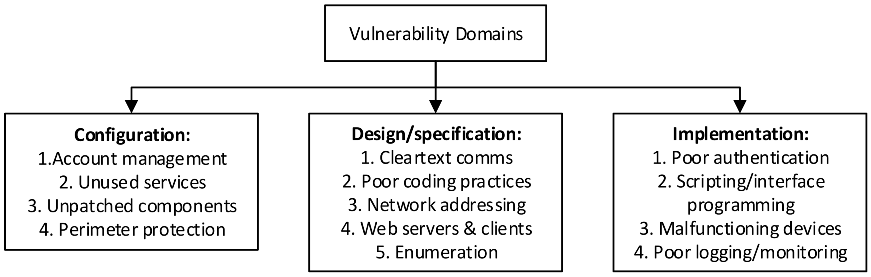

Figure 9. Vulnerability as an exploitable weakness [20].

Two additional taxonomy areas were investigated:

- Technology taxonomies;
- Digital forensic taxonomies.

Securing cyber systems and expanding on the risk management taxonomy, including CPSs, requires supporting technology and digital forensic information analysis. Two taxonomies were selected to represent these aspects (see Figures 10 and 11).

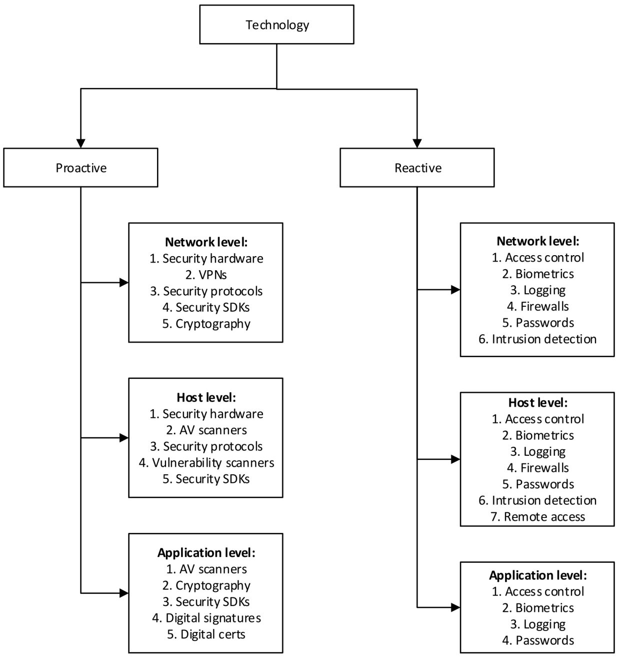

Figure 10. Information security technology taxonomy [21].

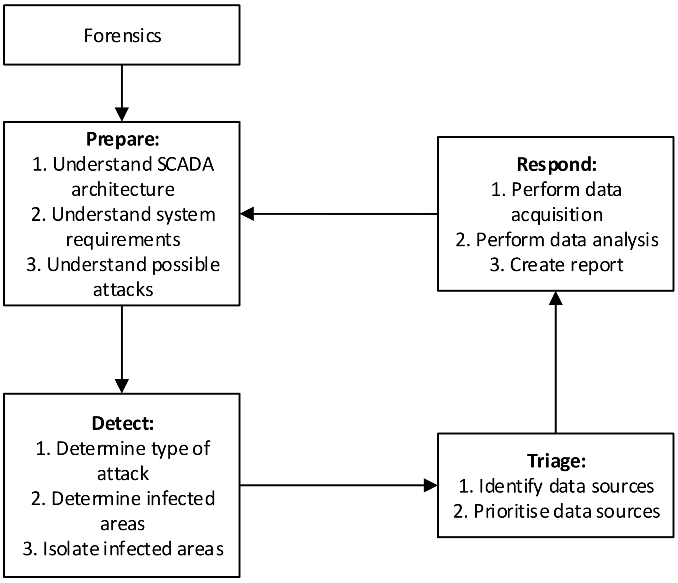
Forensics
Prepare:
1. Understand SCADA architecture
2. Understand system requirements
3. Understand possible attacks
Respond:
1. Perform data acquisition
2. Perform data analysis
3. Create report
Detect:
1. Determine type of attack
2. Determine infected areas
3. Isolate infected areas
Triage:
1. Identify data sources
2. Prioritise data sources

Figure 11. SCADA forensic incident response model [22].

The technology taxonomy is divided into proactive and reactive technologies that allow for a split into prevention and detection and response phases. This allows mapping to the lifecycle phases of CPSs.

The digital forensic taxonomy in Figure 11 also allows for detection and response phases. This links the digital forensic taxonomy to the technology taxonomy.

The selected taxonomies cover a wide range of aspects. Section 3 considers the logical grouping of these aspects into a complementary and comprehensive whole.

3. Core Taxonomy Elements

Although the approaches differ, the authors realized that the taxonomies presented in the previous section aim to address risk management.

The taxonomies discussed in Section 2 can now be integrated to create a harmonized approach for addressing the following specific core elements:

- Business and system risk identification;
- Management of threats;
- Reduction of vulnerabilities;
- Support of risk reduction through protection measures (technology) and implementation of analyses (digital forensics) and improvement cycles in response to incidents.

3.1. Elements

To address risk management and be usable, the taxonomies and elements must be adaptable and broadly applicable to various industries. If the taxonomies are not adaptable and can be used only in very specific applications or scenarios, they cannot facilitate risk management in a broader industry context and will only be applied in a specific niche.

The presented taxonomies represent either risk or risk mitigation. The definition of risk refers to impact, which is an operational or business rationale measure [3], as well as to threats and vulnerabilities. Mitigation requires addressing the threats and vulnerabilities through technology and analyzing incidents through digital forensics to improve processes.

This means that the taxonomies can be divided into the following risk management and support or analysis domains that contain so-called core elements:

- Risk
  a. Operational risk and risk assessment;
  b. Threats;
  c. Vulnerabilities.
- Risk mitigation (support and analysis)
  a. Technologies: proactive and reactive;
  b. Digital forensics.

The following sections discuss each of the core elements of the selected taxonomies shown above in more detail.

3.1.1. Operational Risk and Risk Assessment

The operational risk taxonomy presented here was developed by Young et al. [17] to address most elements that could potentially increase business risk.

This taxonomy uses ISO27000 elements to make it applicable to general business risk applications. This is important, as the Shamoon incident at Saudi Aramco [23] (for instance) had a devastating impact on the production plants. The storage and dispatch of products were interrupted due to the unavailability of the business systems.

The taxonomy presented by Young is split into the following four broad categories:

- People: specifically, the lack of resources, knowledge and training;
- System and technology failures: inadequacies in hardware and system deployments (this in turn relates to implemented supporting technology as well);
- Failed internal processes: policies and procedures, monitoring of metrics and support;
- External events: legislation, supply chain and external services.

3.1.2. Threats

Bodungen et al. [19] did not present threats and threat scenarios as a taxonomy but rather as a set of interrelated elements. This specifically covers threats to CPSs. They contended that each threat scenario has the following elements:

- Threat source (who or what?);
- How (vulnerability exploited?);
- Access vector (route?);
- Target (What is the intended target and consequence?).

The vulnerabilities in the system(s) are handled as a separate aspect but still integrated within the process as a whole.

The next section considers a vulnerability taxonomy.

3.1.3. Vulnerabilities

Fleury et al. [20] approached the problem by considering vulnerabilities as artifacts created during the lifecycle phases of CPS implementation. This allows for the incorporation of management failures and risks into the broader business risk that complements the operational risk taxonomy.

This taxonomy also allows for association with the system lifecycle phases.

The next sections consider the support elements that apply to more lifecycle phases.

3.1.4. Technology

The IEC62443-3-1 technical report provides guidance on implementing risk mitigation technologies for the following domains:

- Authentication and authorization;
- Filtering, blocking and access control (including firewalls);
- Encryption and data validation;
- Management, audit, measurement, monitoring and detection (including digital forensics);
- Industrial automation and control systems computer software (including embedded and operating systems);
- Physical security.

The presented technologies are intentionally broad to ensure applicability across a variety of industries. This does, however, present problems when attempting to associate the technology's implementation with the system lifecycle.

Venter et al. [21] provided an alternative taxonomy that allows for better lifecycle phase association. The technologies are grouped into proactive and reactive technologies that allow for system lifecycle association. It should be noted that although the categories remain broad, they are much better defined than those of the IEC62443 standard.

3.1.5. Digital Forensics

Digital forensics presents a challenge for industrial systems [24]. The digital forensics discipline is mature in the broad IT environment but not in the industrial environment. This is partially due to legacy hierarchies but primarily because CPSs still make use of more proprietary technologies at the control and field levels. This type of proprietary technology is typically not found in the IT domain. Thus, while techniques like fuzzing and intrusion detection systems can be used for network forensics in a CPS environment, a system-specific process might be required for control equipment and field equipment. This complication can be mitigated by ensuring close cooperation with the system manufacturer, as was the case with the Trisis incident [8]. In this incident, an unexplained protection system CPU failure led to the plant shutting down. The hardware was sent to the manufacturer for analysis, which determined that the failure had been due to a new strain of targeted malware called Trisis.

Eden et al. [22] presented a digital forensic response model specifically aimed at supervisory control and data acquisition (SCADA) systems which better defines the requirements.

The next section presents a comparison of the discussed taxonomies and indicates how they relate to one another.

3.2. The Relationship between the Taxonomies and Core Elements

The taxonomies address the core elements in different ways and with a certain degree of overlap. This relationship between the core elements and taxonomies is shown in Table 2.

Table 2. The relationship between the taxonomies and core elements.

Taxonomy Author(s)	Core Elements Addressed Operational Risk Assessment	Threats	Vulnerabilities	Technology	Digital Forensics
Young et al. [17]	X	X	X		
Bodungen et al. [19]	X	X			
Fleury et al. [20]	X		X		
Eden et al. [22]					X
Venter et al. [21]				X	

Table 2 makes it apparent that the first three taxonomies related to risk management cover overlapping areas, whereas the last two taxonomies, which are related to risk mitigation, expand on the other three. All the taxonomies and associated elements must be addressed to ensure broad coverage of information security in CPSs. This dictates the grouping of the taxonomies into core elements and the grouping of these elements—on a higher level—into domains.

4. Harmonized Taxonomy

The harmonized taxonomy captures the essential elements as defined in Sections 2 and 3. It is separated into three domains, where the central lifecycle domain serves to anchor the other two domains (i.e., the support and analysis domain as well as the risk assessment and management domain).

The discussion that follows references the labels (i.e., the blue circles enclosing a number or character) in Figure 12 to facilitate the explanation of the taxonomy.

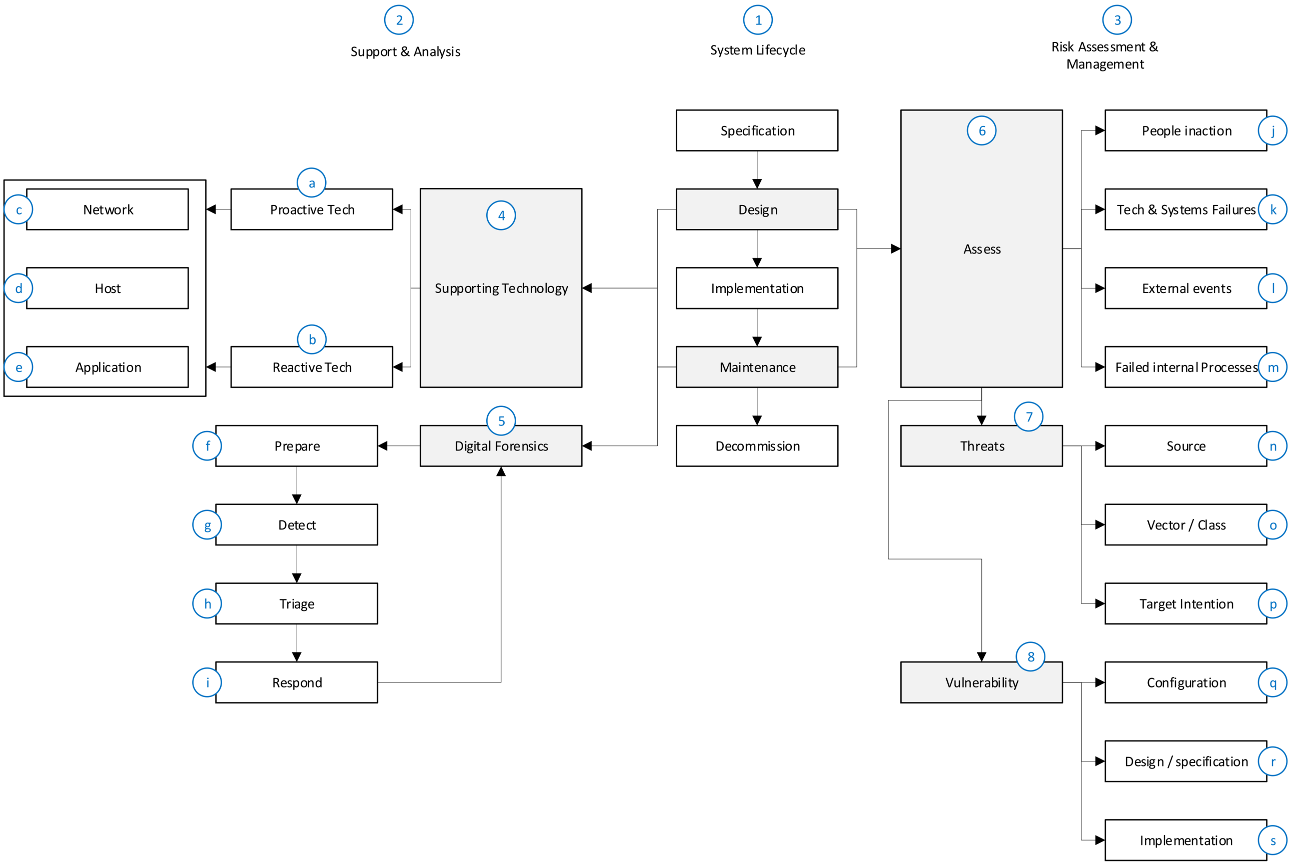

Figure 12. Harmonized information security taxonomy for cyber physical systems.

The system lifecycle itself (1) is a simplified version of the ISA cycle, with the design and maintenance phases acting as core phases.

The design phase is important, as this is where the initial risk assessment for the CPS will be performed, considering threats and vulnerabilities. The envisaged risks will be addressed through a supporting technology and digital forensic implementation design. After CPS implementation, the maintenance phase becomes critical. This is where incidents will likely be experienced during active operation and where incident detection, response, analysis and defense optimization will need to take place.

The core element grouping within the support and analysis domain (2) as well as the risk assessment and management domain (3) reflects the relationship between analyzing and assessing the risks and scenarios in the risk assessment and management domain on the one hand and mitigating the risks and improving the processes contained in the support and analysis domain on the other hand. This paper discusses and highlights the following relationships:

- Actions and implementations to provide information security as required in the CPS lifecycle;
- Risk analysis domain:
    a. Risk assessment;
    b. Threat identification and assessment;
    c. Vulnerability identification and assessment.
- Risk mitigation domain:
    a. Supporting technology for prevention (proactive), detection and response (reactive);
    b. Information collection and incident analysis through digital forensics.

The harmonized taxonomy reflects these relationships in its design and layout. An overview of the harmonized taxonomy is given in Figure 12, while the finer details are presented in Section 3. Space constraints limit the amount of detail that can be presented in Figure 12.

While the core elements within the domains are treated as separate actions, this should never be performed in isolation. As shown in Section 3, there are overlaps and dependencies between the different elements, and ignoring this will lead to gaps in the coverage of the taxonomy. These gaps will in turn invalidate the comprehensive aim of the harmonized taxonomy. In the following paragraphs, the taxonomy structure and elements are discussed in more detail.

The support and analysis (2) domain consists of supporting technology (4) and digital forensics (5). The supporting technology (referring to proactive (a) and reactive (b) technology) is applicable throughout the life of the system. The proactive technology is required to limit intrusions, whereas reactive technology limits the spread and impact of intrusions. Both the proactive and reactive technologies are further divided into network (c), host (d) and application (e) level technologies, but the actual technologies are very different between the proactive and reactive technologies (see Figure 10 again).

Apart from the preparation phase (f), the digital forensic elements are almost purely reactive. They are initiated once an incident occurs, detected (g) and confirmed by either the supporting technology or the plant personnel. Detection is followed by a triage (h) where the data sources are identified and prioritized. Data collection and analysis form part of the response phase (i). The analysis might indicate that changes or updates are required in the supporting technology or even in the digital forensic processes to reduce future risk.

The execution of the risk assessment and management (3) domain is critical to information security. The assessment (6) considers the following:

- People or personnel failures (j);
- Technology or system failures (k);
- External events (l);
- Failures in internal processes (m).

Apart from the initial assessment during the system's design, there are two instances where re-assessment is recommended:

- Periodic re-assessment or audit as required by the applicable standard or legislation;
- As a result of the findings following an incident investigation.

The threat analysis (7) overlaps with the assessment and covers the following:

- Threat source (n): intentional or malicious, non-intentional and disaster-related;
- Access vector (o): the route used to gain entrance to the system;
- Target intention (p): what is the objective and expected consequence of the intrusion or incident?

Lastly, vulnerability (8) analysis is covered, and again there is overlap with the assessment, specifically with regard to technology and system failures (k). The following is considered in the vulnerability element:

- Configuration problems (q);
- Design or specification problems (r);
- Implementation problems (s).

To demonstrate the application of the harmonized taxonomy, the next section maps a well-known case study of incidents in CPSs to the harmonized taxonomy.

5. Mapping a Case Study to the Taxonomy

The case study selected for mapping was the Maroochy Shire water plant incident. The Stuxnet incident in Iran is available in Appendix A and applies the taxonomy to a nation-state adversary scenario. The mapping is not comprehensive but includes all the most prominent aspects to demonstrate the practical use of the harmonized taxonomy.

Before discussing the mapping, it is important to understand that applying the harmonized taxonomy requires a structured approach (i.e., an application methodology). This approach is discussed in the next section.

5.1. Harmonized Taxonomy Application Methodology

The application methodology only acts as a guide to the usage of the harmonized taxonomy. It cannot function in isolation. As discussed in the previous section, the taxonomy contains multiple detailed sub-elements below the elements listed in Table 3. It is important when applying the taxonomy to consider not just the high-level elements but also the detailed sub-elements to ensure that a full system analysis is performed. A specific example describing the relationship between the taxonomy elements and the methodology elements is provided at the end of this section.

Table 3. The links between the taxonomy and the application methodology elements.

Harmonized Taxonomy: Element	Harmonized Taxonomy: Element Number	Methodology: Element	Methodology: Element Number(s)
System lifecycle	1	System lifecycle	1, 3, 9, 10, 19
Risk assessment	6	Risk assessment	4, 12, 16
Threats	7	Threat source or agent	6, 14
Vulnerability	8	Vulnerabilities	5, 13
Supporting technology	4	Supporting tech and forensics	8, 12, 15, 17
Digital forensics	5	Supporting tech and forensics	8, 12, 15, 17

Two application methodologies are presented. The first (see Figure 13) details the generic process that will be followed by a plant owner over the lifecycle of a typical CPS. For the sake of completeness, this methodology is discussed in detail to illustrate the application of the taxonomy over the full lifecycle. The second methodology (see Figure 14) is a subset of the generic methodology and only considers the incident investigation actions. It was this simplified (second) methodology that was used for the case study analysis. This was because the incident occurred during the maintenance and operational phase of the plant lifecycle, and the information for the specification, design, and implementation phases was not available. The original design intent of the system and the operational constraints were not part of the papers used in the analysis.

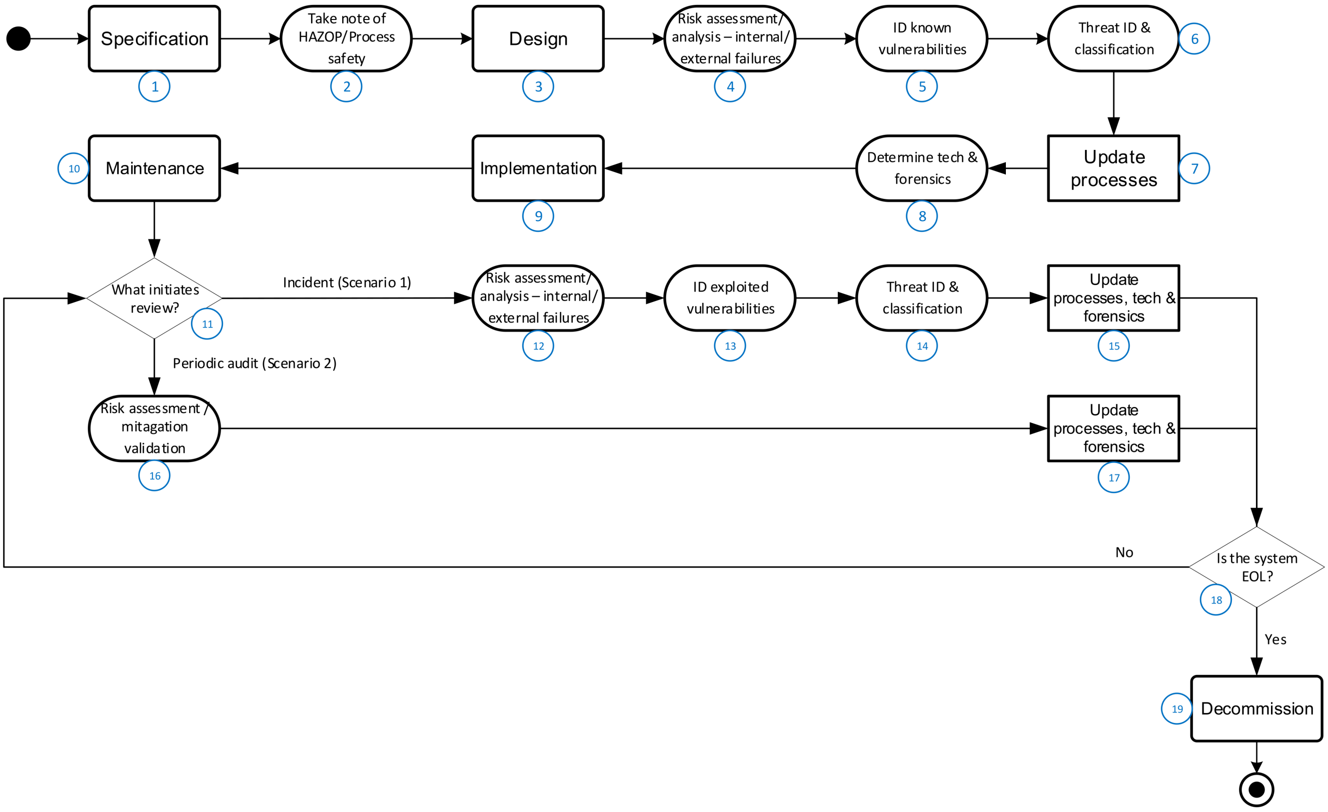
Specification
1
Take note of HAZOP/Process safety
2
Design
3
Risk assessment/ analysis – internal/ external failures
4
ID known vulnerabilities
5
Threat ID & classification
6
Update processes
7
Determine tech & forensics
8
Implementation
9
Maintenance
10
What initiates review?
11
Incident (Scenario 1)
Risk assessment/ analysis – internal/ external failures
12
ID exploited vulnerabilities
13
Threat ID & classification
14
Update processes, tech & forensics
15
Periodic audit (Scenario 2)
Risk assessment / mitagation validation
16
Update processes, tech & forensics
17
No
Is the system EOL?
18
Yes
Decommission
19

Figure 13. Harmonized taxonomy and generic methodology.

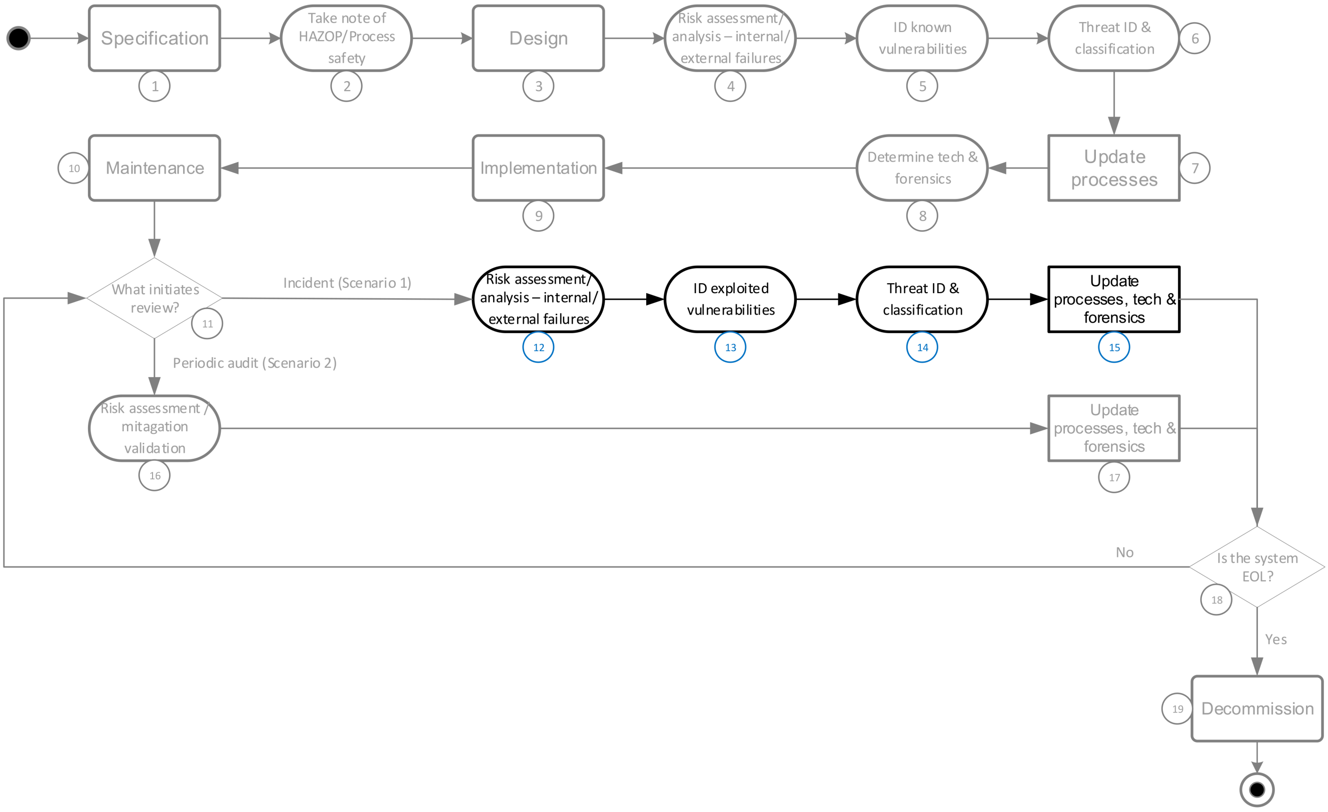
Specification
1
Take note of HAZOP/Process safety
2
Design
3
Risk assessment/ analysis – internal/ external failures
4
ID known vulnerabilities
5
Threat ID & classification
6
Update processes
7
Determine tech & forensics
8
Implementation
9
Maintenance
10
What initiates review?
11
Incident (Scenario 1)
Risk assessment/ analysis – internal/ external failures
12
ID exploited vulnerabilities
13
Threat ID & classification
14
Update processes, tech & forensics
15
Periodic audit (Scenario 2)
Risk assessment / mitagation validation
16
Update processes, tech & forensics
17
No
Is the system EOL?
18
Yes
Decommission
19

Figure 14. Harmonized taxonomy and case study methodology.

The application methodology follows the CPS lifecycle as per the harmonized taxonomy. It starts with the specification (1) phase. While this phase is not generally used to address security concerns, several activities influence the security and system design. Specifically, hazardous operation studies and process safety requirements (2) provide information to quantify risk, including monetary loss and environmental and safety impacts, as well as to impose restrictions on safety system integrity. The design phase (3) requires the initial risk assessment (4), where the internal and external risks are evaluated, as discussed in Section 4. The adequacy of existing protection measures, possible threat sources (5) and existing system vulnerabilities (6) is checked and documented. Completing the full risk assessment will allow for the identification of gaps that will be addressed through updating of policies and procedures (7), adding supporting protection technology and a digital forensic analysis (8) process. In some cases, it might be found that the specified CPS cannot meet the security requirements due to inherent constraints, and alternative systems might have to be considered.

During the implementation phase (9), the complete CPS (including digital forensics and supporting technology) will be evaluated, typically during factory acceptance testing, to ensure that it meets the security design requirements. This evaluation will also include an evaluation of the failed processes element in Figure 6 to ensure the company processes do not introduce additional business risk.

After commissioning, the CPS enters the commercial operation or maintenance phase (10). This phase is the longest in the CPS lifecycle. Due to the time duration involved, this is typically where security incidents occur or system design changes and modifications are made to allow for changes in the process requirements. Standards like IEC62443 might specify that periodic risk reviews are required to maintain security integrity. Thus, the two different scenarios (11) are the following:

- Incident analysis;
- Periodic audit and review.

The harmonized taxonomy caters to both these different scenarios but with a difference in application methodology. The first and arguably more serious scenario will occur due to a security incident. It was this scenario that was analyzed in the selected case study. The risk assessment (12) is conducted to determine the failures and to evaluate all the elements as shown in Figure 6. The analysis determines failures or gaps in the digital forensic processes or techniques and supporting technologies that allowed the incident to take place. An attempt is made to determine and classify the vulnerability (13) and the threat source (14) associated with the incident. As was performed during the design phase, gaps are identified in the supporting technology and digital forensic processes or techniques (15), and these elements are updated to mitigate the risk.

The second scenario is more proactive and will be initiated in response to either a change in the process's operational requirements or as part of periodic auditing to comply with the implemented standard. The documented risk assessment, along with existing mitigation measures, will be evaluated (16) to determine whether the assumptions are still valid and whether the threats and vulnerabilities are still adequately addressed. If gaps are found, the required processes and mitigation measures (17) will be updated to address the risks associated with such gaps. Both scenarios mentioned can occur multiple times during the operational life of a CPS. Their occurrence will depend on whether the system is expected to remain operational or whether it has reached the end of its useful life (18). For the former, the scenarios as presented will be repeated until the latter case is reached. Once the CPS reaches the end of its operational life, it will be decommissioned (19). In this phase, the system must be disposed of in such a way that no confidential information can be leaked from, for example, application software or design configuration.

It is crucial for the harmonized taxonomy to be the master reference for each step in the application methodology. This ensures that the taxonomy meets the desired criteria for being a part of a comprehensive and consistent security framework.

The simplified methodology in Figure 14 addresses only incident response, as indicated by the highlighted steps (i.e., scenario 1). The entire harmonized taxonomy is, for easy reference, repeated as indicated by the gray steps. The occurrence of an incident implies that there was a failure or multiple failures (12) in either the internal or external processes or the supporting systems, as detailed in Figure 6. The primary aim of an incident investigation is to identify these failures or gaps and address them. In addition, there must either have been a vulnerability (13) in terms of access that allowed the incident to occur or someone or something initiated the incident (14) as a threat actor. Very important (although not applicable in the analyzed case study) is that the threat agent does not have to be malicious or the incident intentional. However, the security measures put in place must protect against the non-malicious, unintentional scenario as well, as that can be just as devastating as an adversary-driven incident [5].

It is important to understand how the elements in the methodology link to the elements in the taxonomy. Table 3 summarizes this link. The numbering references used refer to Figure 12 for the taxonomy and Figure 13 for the methodology.

To illustrate the practical application, one could consider an instance where the supporting technology core element (see Figure 13) needs to be analyzed in step 8 of the methodology. To conduct this analysis, one would need to refer to element 4 (i.e., supporting technology) of the harmonized taxonomy in Figure 12 and the detailed elements presented in Figure 10. This same analysis and the associated reference to the harmonized taxonomy will be repeated in steps 12, 15 and 17 of Figure 13 by simply reapplying the harmonized taxonomy supporting the technology elements.

The next section applies this simplified methodology to the mapping of the selected case study (i.e., the Maroochy Shire case study).

5.2. The Maroochy Shire Incident

The Maroochy Shire case study was selected because it provided an example of a malicious insider, whereas the Stuxnet case study provided an example of a malicious outsider. The insider case is more typical of the type of incident that companies usually can expect [25] to experience.

The specific incident took place in early 2000 at the Maroochy water services plant in Queensland, Australia. Because it was one of the first definitively confirmed malicious industrial cyber incidents, the Maroochy Shire incident has since been extensively analyzed. The analyses conducted by Weiss et al. [26] and Slay et al. [27] were used for mapping purposes.

The incident occurred when a disgruntled contracted ex-employee, Vitek Boden, accessed the plant control system remotely through an unsecured radio link over several months. He disrupted the plant's operation and caused a discharge of effluent into the local stream. Detection of the incident occurred when personnel noticed a discrepancy between the actual pump state and what was shown on the operator display. An investigation followed, which led to the identification of a wireless connection as the attack vector. Analysis of this incident is provided below by means of using the harmonized taxonomy. The numbering references used were as indicated in Figure 14, with the assessment core element details as indicated in Figure 6.

The incident occurred during the plant maintenance and operational lifecycle phase (10). The primary cause or threat agent (14) was the disgruntled ex-employee who exploited vulnerabilities in the system configuration and security perimeter (13). Considering the risk assessment as detailed in the harmonized taxonomy (see Figures 6 and 12), there were several internal and external failures (12) and gaps in the supporting technology and digital forensics. These gaps are noted below.

When the risk assessment (12) element of the taxonomy was considered, several internal failures (identified gap 1) appeared. These included failures in process design and execution, specifically notifications and alerts, SLA management and, to a lesser extent, process documentation. Furthermore, internal process control failed due to status monitoring and periodic reviews being inadequate. Lastly, regarding internal failures, the staffing supporting process resulted in a dismissed contract employee retaining his access to the system.

Moving on to external events revealed the next unaddressed risk (identified gap 2) in that the plant could not adhere to regulatory operating requirements and caused environmental damage through the discharge of effluent, which in turn required extended clean-up.

The system and technology failures element highlighted a design (identified gap 3) problem, with the logical plant security perimeter permitting wireless remote access for authorized equipment. The scenario of the equipment being stolen and then used was not envisioned.

The final element of the risk assessment identified a knowledge inaction risk (identified gap 4). Even though the discrepancy and intrusion were identified by an employee, it took some time and required tacit knowledge that had not been codified or generally available. Formal knowledge of the system configuration and structure could potentially have allowed for earlier identification.

Consideration of the risk mitigation core elements led to the identification of additional gaps. There was a general lack of supporting technology (identified gap 5), with some of the most obvious being inadequate or missing intrusion detection, access control and logging. If any of these had been adequately addressed, it could have made the intrusion much more complex and may have allowed for earlier detection. The digital forensics element was completely dependent on individual knowledge, with no formalized process in place (identified gap 6). Detection and triage took place because a site engineer could identify discrepancies in the assigned station numbers and, from there, locate a wireless intrusion. The response, specifically performing and analyzing data acquisition, resulted in the intrusion being identified and locked out. Then, with the assistance of the police, the perpetrator was located and arrested. None of this, however, was due to a structured and formalized process, and success depended solely on the skills and knowledge of individuals.

Classifying the threat (14) showed that it was adversarial, using the wireless network as an access vector to cause environmental, monetary and possibly reputational damage.

Two specific vulnerabilities (13) were exploited. This involved the system configuration, specifically account management and perimeter protection, and implementation with regard to poor authentication, logging and monitoring. It is interesting to note that the vulnerability could, for this incident, already be identified in the assessment core element, with it being confirmed by the vulnerability assessment.

Following the methodology and applying the harmonized taxonomy allowed for the identification of system, process, and mitigation gaps, as well as for the accurate classification of the threats and exploited vulnerabilities. The six gaps identified covered every core element of the harmonized taxonomy but required application of the core and sub-elements.

Section 6 contains a discussion on the harmonized taxonomy, its benefits, usage and shortcomings.

6. Discussion

The harmonized taxonomy brings together a variety of existing taxonomies into a harmonized, single-reference taxonomy. It links the core elements to the CPS lifecycle phases and allows the specific aspects of risk and incident response management to be uniquely classified in the taxonomy.

Utilizing the taxonomy has the following advantages:

- It supports a common reference framework between the information technology (IT) and operational technology disciplines, especially with regard to business risk. This is an effect of utilizing a hybrid approach to the taxonomy, as the impact of IT risks on CPSs and vice versa can be analyzed and assessed without changing the harmonized taxonomy structure.

- The classification and grouping of risk- and incident-related information can be consistently and accurately applied. This can then be used to improve the security management programs and update the required supporting risk mitigation technologies. Lessons learned from IT or CPS incidents can be applied without having to change the harmonized taxonomy. If the IT or broader business risk aspects do not apply to the CPSs, these aspects will simply not be applied. This flexibility also allows for broad industry application. A less comprehensive taxonomy that was (for example) developed for the petrochemical industry would require customization if it were to be applied to heavy manufacturing. This is because the CPSs being utilized and the process requirements are very different, even though similar business risks can be experienced. Flexibility is enabled by not specifying the process or system requirements as part of the harmonized taxonomy elements or structure and by rather capturing them in the assessment of broad business risk. For example, the batch and source tracking information of a pharmaceutical plant is critical. Thus, securing information is a critical part of threat assessment, whereas batch information security for the coal supply to a power station will be much less critical. The harmonized taxonomy is equally applicable to both scenarios.
- Utilizing the taxonomy allows for its application as a reference framework during any stage of the system lifecycle. This is demonstrated in Section 5, where the generic application methodology shows the repeated application of the same taxonomy elements in different steps and at different lifecycle stages.
- Applying the harmonized taxonomy elements during incident investigations allows the easy identification of risk and risk mitigation gaps (as demonstrated by the case study mapping). This facilitates focused updates and changes to protection measures to close any possible gaps and reduce overall company risk.

The harmonized taxonomy as presented is deficient in the following respect.

The digital forensics taxonomy core element does not provide a high level of detail for supervisory and field equipment, since proprietary technologies are still being used at these levels. This deficiency can be partially mitigated, however, if the correct support relationship with the system manufacturer is in place. The digital forensics core element as presented is still usable as a guide but might require additional detailed sub-elements based on industry or business requirements. This requirement will be addressed in future work.

Section 7 next concludes this paper.

7. Conclusions

This paper provided a background analysis of CPS lifecycles and established risk taxonomies. The taxonomies presented followed a hybrid approach to match the configuration of modern CPSs and the overlap between the IT and operational technology worlds.

This paper also addressed the fragmentary and incomplete nature of established taxonomies by combining several of these taxonomies into a single harmonized taxonomy. The taxonomy is divided into two main areas. The first area is risk assessment, including threat and vulnerability identification. The second area is risk mitigation by using supporting technology and forensic processes.

The practical use of the taxonomy was demonstrated by analyzing a case study and identifying security gaps. Continued research on the application of the harmonized taxonomy is being conducted on case studies and real-world industrial facilities.

Further research into the following areas could be considered:

- Testing the usability of the harmonized taxonomy during system definition (i.e., before the design and procurement of the system). This should focus on the integration of process safety and information security into the system definition.
- Possible refinement of the digital forensic taxonomy while still maintaining its broad applicability.

Author Contributions: Conceptualization, J.H.P.; methodology, J.H.P.; validation, J.H.P. and H.V.; formal analysis, J.H.P. and H.V.; investigation, J.H.P. and H.V.; writing—original draft preparation, J.H.P.; writing—review and editing, H.V.; visualization, H.V.; supervision, H.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Nation State Adversary Case Study: Stuxnet

The first time an early variant of Stuxnet was identified was in early 2007, but at that time, no one realized the importance of the code. Stuxnet was designed and deployed as a cyber weapon with one specific aim in mind: to damage the enrichment centrifuges at the Natanz nuclear facility in Iran. It has become one of the most well-known industrial cyber incidents, and portions of the code have been found in other pieces of malware like Duqu and Flame [28]. The initial incident was followed by another apparent attack in 2021 [29]. For mapping of the Natanz Stuxnet incident, papers by Rao [30] and Langer [4] were used.

Due to the secretive nature of the Natanz facility, actual information about the incident is limited. What is presented here is based on information from the selected papers that used a variety of sources and malware analysis.

The methodology in Figure 14 and the harmonized taxonomy shown in Figure 12 were referenced for this analysis. The incident occurred during the plant's maintenance and operational lifecycle phase (10). The primary cause or threat agent (14) was a nation-state adversary that used zero-day vulnerabilities (13) in the control hardware and support systems.

Evaluating the assessment core element (12) highlighted several failures that resulted in gaps in the security of the plant and CPSs. Internal process failures occurred on all sub-elements. The process design and execution had notification and alert failures. Process control failed at status monitoring, specifically the monitoring of traffic between the controller and the operator station. The supporting processes failed due to staffing problems, as the personnel were not technically proficient enough to detect abnormalities. Procurement also posed a challenge, since the equipment used had hard-coded system passwords that allowed access. This issue is still a widespread concern in many systems [31].

External events played a role in as far as the geopolitical situation resulted in nation-states launching a weaponized cyber-attack on the facility.

Technology and system failures admittedly occurred, but the sophisticated nature of the attack would have caused most defenses to have a limited effect. Moreover, the people failures in terms of skills, which allowed the detection of the activity, were more serious and eventually aggravated the impact of the incident.

Classification of the threat (14) showed this to have been adversarial, using physical access by means of a USB port to cause physical damage to the enrichment centrifuges.

A variety of vulnerabilities (13) were exploited. These included several zero-day vulnerabilities in Windows and poor system account management by utilizing the hard-coded passwords on the CPS. Poor logging in the implementation allowed abnormal communication between the field CPS and the operator station to go undetected.

It is not clear what supporting technology and digital forensics processes (15) were in place, but it is safe to say that they were insufficient, as the malware operated for some time before it was detected. After detection, analyses of the malware and its effects continued for several years. To be clear, had the correct systems and processes been in place, it is still unlikely that the incident would have been prevented, but the detection and recovery period would very likely have been shortened.

The harmonized taxonomy identified the following gaps:

- Like the Maroochy incident, there were definite management and procedural failures, and the plant personnel could not match the sophistication of the adversary.
- This case highlights the relative lack of defense that plant owners have against a well-resourced and very sophisticated enemy.
- Vulnerability management would have had little effect because of the use of multiple zero-day exploits. An effective information security management system with the associated support technology would likely have enabled quicker detection of the abnormal communications between the control and SCADA levels (digital forensics detection).
- A proper risk assessment would likely have identified the hard-coded passwords as a concern. These system-level accounts could then have been monitored for any abnormal activity.

References

1. Neitzel, L.; Huba, B. Top 10 Differences between ICS and IT Cybersecurity. Available online: https://blog.isa.org/top-10-differences-ics-cybersecurity (accessed on 16 June 2021).
2. *ISO27000*; Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. International Organization for Standardization: Geneva, Switzerland, 2005.
3. *IEC62443*; Industrial Communication Network—Networks and System Security. Part 1-1. Terminology, Concepts and Models. IEC/ISA: Durham, UK, 2009.
4. Langner, R. *Stuxnet Malware Analysis Paper*; Langner Group: Hamburg, Germany, 2013.
5. Weimer, C. Bellingham's Pipeline Explosion—A Decade of Healing. Available online: https://pstrust.org/docs/pstnewsletter_spring09.pdf (accessed on 23 March 2014).
6. Smith, S. *A Proposal for a Taxonomy for Vulnerabilities in Supervisory Control and Data Acquisition (SCADA) Systems*; Army Research Lab Aberdeen Proving Ground: Aberdeen, MD, USA, 2014.
7. Fouche, M.L. The Role of Taxonomies in Knowledge Management. Ph.D. Thesis, University of South Africa, Pretoria, South Africa, 2006.
8. Ahmadian, M.; Shajari, M.; Shafiee, M. Industrial control system security taxonomic framework with application to a comprehensive incidents survey. *Int. J. Crit. Infrastruct. Prot.* **2020**, *29*, 100356. [CrossRef]
9. Althonayan, A.; Adronache, A. Shifting from information security towards a cybersecurity paradigm. In *ACM International Conference Proceeding Series*; ACM: Washington, DC, USA, 2018; pp. 68–79.
10. Johnson, A. W32.Duqu: The Precursor to the Next Stuxnet. Available online: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=933c68f1-6ee7-473e-9eb6-6c8459f790f2&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (accessed on 18 November 2021).
11. Paganini, P. Duqu 2.0: The Most Sophisticated Malware Ever Seen. Available online: https://resources.infosecinstitute.com/topic/duqu-2-0-the-most-sophisticated-malware-ever-seen/ (accessed on 15 July 2020).
12. Patel, P. Application of Plan-Do-Check_Act Cycle for Quality and Productivity Improvement—A Review. *Int. J. Res. Appl. Sci. Eng. Technol.* **2017**, *1*, 197–201.
13. Mödinger, M. *Metrics and Key Performance Indicators for Information Security Reports of Universities*; Hochschule Augsberg: Welden, Germany, 2018.
14. ISA Global Cybersecurity Alliance. *Security Lifecycles in the ISA/IEC 62443 Series*; ISA: Durham, UK, 2020.
15. NERC. Reliability Standards Complete. 2020. Available online: https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf (accessed on 22 November 2021).
16. Price, P.; Marufuzzaman, M. *Industrial Control System Risk*; Idaho National Laboratory: Idaho Falls, ID, USA, 2019.
17. Young, L.; Cebula, J. *A Taxonomy of Operational Cyber Security Risks (Version 2)*; Carnegie Mellon University: Pittsburgh, PA, USA, 2014.
18. Flowers, A.; Smith, S.; Oltramari, A. Security Taxonomies of Industrial Control Systems. In *Cyber-Security of SCADA and Other Industrial Control Systems*; Colbert, E., Kott, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 111–132.
19. Bodungen, C.; Singerm, B.; Shbeeb, A.; Wilhoit, K.; Hilt, S. *Hacking Exposed: ICS and SCADA Security Secrets & Solutions*; McGraw Hill Education: New York, NY, USA, 2017.
20. Fleury, T.; Khurana, H.; Welch, V. *Towards a Taxonomy of Attacks against Energy Control Systems*; Critical Infrastructure Protection II; Springer: Boston, MA, USA, 2008; Volume 290, pp. 71–85.
21. Venter, H.; Eloff, J. *A Taxonomy for Information Security Technologies*; Computers & Security: Amsterdam, The Netherlands, 2003; Volume 22, pp. 299–307.
22. Eden, P.; Blyth, A.; Burnap, P.; Jones, K.; Stoddart, K. *A Forensic Taxonomy of SCADA Systems and Approach to Incident Response*; BCS Learning & Development: Swindon, UK, 2015.
23. Bronk, C.; Tikk-Ringas, E. Hack or Attack? In *Shamoon and the Evolution of Cyber Conflict. Survival*; James, A., Ed.; Baker III Institute for Public Policy of Rice University: Houston, TX, USA, 2013.

24. Amad, R.A.; Beztchi, S.; Smith, J.M.; Lyles, B.; Prowell, S. Tools, techniques, and methodologies: A survey of digital forensics for SCADA systems. In *ACM International Conference Proceeding Series*; ACM: New York, NY, USA, 2018; pp. 1–8.
25. Giandomenico, N.; de Groot, J. Insider vs. Outsider Data Security Threats: What's the Greater Risk? Available online: https://digitalguardian.com/blog/insider-outsider-data-security-threats (accessed on 12 December 2021).
26. Weiss, J.; Abrams, M. *Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia*; MITRE: McLean, VA, USA, 2008.
27. Slay, J.; Miller, M. Lessons learned from the Maroochy water breach. In *Critical Infrastructure Protection*; Stewart, J., Ed.; Springer: Boston, MA, USA, 2011; pp. 781–791.
28. Bencsath, B.; Pek, G. The cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet* **2012**, *4*, 971–1003.
29. Corera, G. Iran Nuclear Attack: Mystery Surrounds Nuclear Sabotage at Natanz. Available online: https://www.bbc.com/news/world-middle-east-56722181 (accessed on 12 April 2021).
30. Rao, S. *Stuxnet—A New Cyberwar Weapon*; Aalto University: Espoo, Finland, 2014.
31. Oxana, A. Strangelove Github. Available online: https://github.com/scadastrangelove/SCADAPASS/blob/master/scadapass.csv (accessed on 8 November 2021).