signals

MDPI

Review

CS Measures for Nuclear Power Plant Protection: A Systematic Literature Review

Nabin Chowdhury

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway; nabin.chowdhury@ntnu.no

Abstract: As digital instrumentation in Nuclear Power Plants (NPPs) is becoming increasingly complex, both attack vectors and defensive strategies are evolving based on new technologies and vulnerabilities. Continued efforts have been made to develop a variety of measures for the cyber defense of these infrastructures, which often consist in adapting security measures previously developed for other critical infrastructure sectors according to the requirements of NPPs. That being said, due to the very recent development of these solutions, there is a lack of agreement or standardization when it comes to their adoption at an industrial level. To better understand the state of the art in NPP Cyber-Security (CS) measures, in this work, we conduct a Systematic Literature Review (SLR) to identify scientific papers discussing CS frameworks, standards, guidelines, best practices, and any additional CS protection measures for NPPs. From our literature analysis, it was evidenced that protecting the digital space in NPPs involves three main steps: (i) identification of critical digital assets; (ii) risk assessment and threat analysis; (iii) establishment of measures for NPP protection based on the defense-in-depth model. To ensure the CS protection of these infrastructures, a holistic defense-in-depth approach is suggested in order to avoid excessive granularity and lack of compatibility between different layers of protection. Additional research is needed to ensure that such a model is developed effectively and that it is based on the interdependencies of all security requirements of NPPs.

Keywords: systematic literature review; cyber-security; critical infrastructure; nuclear power plant

check for updates

Citation: Chowdhury, N. CS Measures for Nuclear Power Plant Protection: A Systematic Literature Review. *Signals* **2021**, *2*, 803–819. https://doi.org/10.3390/signals2040046

Academic Editors: Chin-Ling Chen and Francesco de Paulis

Received: 5 May 2021
Accepted: 26 October 2021
Published: 4 November 2021

1. Introduction

The digitalization of many of today's Critical Infrastructure (CI) sectors has been extended to nuclear power plants (NPPs). The main control rooms of NPPs have integrated new digitalized human–system interfaces to facilitate the previously paper-based work and analog controls used by personnel [1]. Nonetheless, the digitalization of Instrumentation and Control (I&C) systems and the adoption of open-system architectures have escalated the threat of cyber attacks into a serious CS issue [2].

One of the most well-known cyber attacks against NPPs in the last decade is the cyber warfare weapon known as Stuxnet [3]. According to reports, hundred of thousands of computers in multiple countries were affected by this worm attack, with 58% of the infected systems being located in Iran [4]. Stuxnet used intermediary devices, such as USB sticks, to gain access to the victim systems. It has been reported that almost one-fifth of Iran's nuclear centrifuges have been damaged by the attack [5].

To tackle cyber threats affecting NPPs and to prevent attacks similar to Stuxnet from happening, safety regulations and standards have been published for digital safety system development and protection [6] in order to be used to protect NPPs' Critical Digital Assets (CDAs), which are the assets that are fundamental to the functioning of the nuclear plant and, therefore, are most sensitive to cyber attacks [7]. An example of a CS plan and related activities for NPP protection is shown in Figure 1.

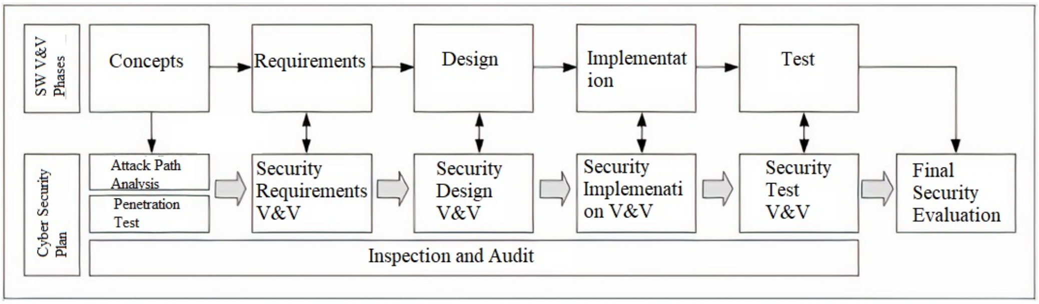

Figure 1. CS plan and activities for NPP protection, from "Implementation of cyber security for safety systems of nuclear facilities" by Park, J.; Suh, Y.; Park, C., 2016, Prog. Nucl. Energy, 88, 88–94. Copyright 2021 by Elsevier [6].

The United States Nuclear Regulatory Commission (USNRC) has published various regulatory guidelines and specific guides for the design and construction of nuclear plant facilities that are internationally referenced. CS risk assessment practices involving system, asset, threat, vulnerability risk analysis, and intrusion tests [8,9] to reduce the number of vulnerabilities and potential damage have also been developed and proposed.

The definition of standards and policies and the installation of security software alone are often not sufficient to ensure the security of nuclear facilities, or of any other critical infrastructure. In fact, many of the recent CS incidents were linked to human carelessness and unpreparedness of the personnel in detecting and preventing cyber attacks.

A great deal of research has been done to demonstrate the correlation between systems' security and the human factor. The authors of [10] showed in their study how a number of personality traits and attitudinal predispositions, such as impulsiveness, can affect an individual's ability in CS assurance. It was suggested by the authors that to address this issue, focused training that accounts for the human attributes should be given to personnel. The authors of [11] highlighted the importance of effective communication among individuals in attaining safety and security in an NPP. To achieve this, they suggested using an integrated training approach based on consultation with experts in each relevant discipline on a continuous basis.

All of these procedures and others that will be discussed in this work are defined herein as *CS measures* for NPP safety and security, meaning any type of method or instrument that has been developed and applied for NPP CS. Specifically, these measures include all types of CS procedures, tools, or other instrumentation, such as Intrusion Detection and Protection Systems (IDPSs), CS awareness and training campaigns, and any other type of solution used for CS assurance in NPPs.

Unfortunately, the lack of a comprehensive analyses and evaluations of current measures for NPP CS presents a challenge in the development of an effective and comprehensive CS framework. Additionally, current research focused on surveying the literature on solutions for NPP CS is noted to have proved very limited information on the attributes of each proposal.

For this reason, in this work, we will be describing all of the CS measures proposed in the literature for NPP protection based on their characteristics. This will later allow for comparisons of these solutions and identification of gaps and challenges.

In more detail, we reviewed the literature to identify the state of the art in standards, guidelines, and other security approaches developed for NPP CS. Furthermore, we analyzed all of these measures to understand the interdependencies among them and the current limitations, as well as to suggest potential improvements. Aside from providing an up-to-date analysis of NPP CS measures, this work is meant to serve as a basis for the development of holistic CS frameworks for NPP protection.

The rest of this paper is organized as follows: In Section 2, we describe the research method used to conduct the literature review. Then, in Section 3, we discuss competing or related surveys and other works discussing NPP CS, noting their limitations. Next, in

Section 4, we present the results of our literature review. As will be shown, the results have been grouped into three categories: Critical Digital Asset (CDA) discovery methods, risk assessment and threat analysis methods, and, finally, additional measures for NPP protection. Next, we summarize the findings from the literature review and analyze the results in Section 5. Finally, we provide closing remarks and future directions for research in Sections 6 and 7, respectively.

2. Research Method

The research method used to conduct this SLR is based on the guidelines proposed by [12] in the PRISMA statement and by [13] for conducting structured literature reviews in computer science fields. The authors of [13] indicated three main phases that should compose a review: (i) planning, (ii) conducting, and (iii) composing.

Each phase can be divided into steps. During the planning phase, the key steps to conduct are identifying whether there is a need for a review and, in that case, commissioning the review, defining the research questions, and developing and evaluating a review protocol. During the conducting phase, the focus should be on identifying articles to be included in the review through an initial search, and later, a quality assessment and screening. Once the final list of articles is obtained, data extraction and synthesis should be conducted. Finally, in the composing phase, the review should be formatted and evaluated.

This structure was also adopted for our work, with the integration of some other items to include when reporting a systematic review, as indicated in [12].

2.1. Objectives and Scope

The objective of this work can be summarized as follows: to *identify measures and solutions proposed for Nuclear Power Plant (NPP) CS and the interdependencies among them*, where CS "measures" are defined as all types of CS procedures, tools, or other instrumentation used for NPP CS. To achieve this goal, we conducted a systematic review to identify articles discussing CS standards, guidelines, best practices, and any other CS measures and solutions for NPP CS. Furthermore, we tried to analyze the attributes and factors that link these solutions together. More precisely, we investigated the beneficial attributes of each of these solutions to understand how these attributes can be used in a complementary way to provide comprehensive, effective, and multi-layered CS assurance in NPPs. The various objectives of this work can also be encapsulated as providing an answer to the following research questions:

- **RQ1:** What measures and solutions have been proposed in the literature for nuclear power plant CS?
- **RQ2:** What are the interdependencies among the measures and solutions?
- **RQ3:** How can these measures be utilized and implemented in NPPs to offer comprehensive and complementary CS?

2.2. Review Protocol

In order to make this work reproducible and expandable, a review protocol was established based on the recommendations for systematic reviews suggested in [12]. The protocol defines search methods for the identification of the studies, eligibility criteria, and data extraction and data analysis methods; these are described in detail in the following section.

2.3. Literature Search

To identify and collect scientific articles, three online databases were consulted: IEEE Xplore, Scopus, and ACM Digital Library. In order to maximize the number of results that may be pertinent to the goal of this study, only one query of keywords was utilized, namely, "CS + nuclear". Table 1 shows the number of results obtained by this search in each of the three databases.

Table 1. Results of the literature search from each online database.

	Scopus	IEEE Xplore	ACM	Total
CS + Nuclear	207	45	281	533

2.4. Practical Screening, Quality Assessment, and Selection of Studies

A set of inclusion and exclusion rules were put in place to screen the results of the literature search:

- Only articles written in English were selected;
- Only scientific articles published in conferences, workshops, and journals were selected;
- Articles published before January 2010 were excluded;
- Duplicates found through multiple databases were excluded;
- Articles that were not accessible to the author were excluded.

Any article that did not include the keywords "CS" and "Nuclear" in its title, abstract, or introduction was also excluded.

The number of articles remaining after two rounds of screening was 59.

After the screening, one last round of quality assessment was conducted. During this quality assessment, any article that did not pertain to the initial topic of "CS measures for NPP protection" or did not provide enough detail regarding suggested measures was excluded. After the quality assessment, the number of remaining articles was 36.

2.5. Data Extraction and Monitoring

We later developed a data extraction review form, which was utilized to map the articles selected for the review and the key findings described in each of these. The following attributes were selected for the review form:

- Title and Year: title of the paper and year of publishing;
- Authors: list of contributing authors;
- Domain: area or domain of focus of the article;
- Proposed/Discussed Method: CS measures proposed or analyzed by the authors;
- Description: brief description of the content of the paper;
- Conclusions: final conclusions and outputs presented by the authors;
- Discussion and Review: Our own analysis and evaluation of the content of the individual papers. This included any criticism and suggestions for potential improvements.

2.6. Composing the Review

The final step consisted in writing the review, which was conducted by using the method described in [12]. The topics included in the report are shown and summarized in Table 2.

Table 2. Sections and topics included in the composition of the systematic review based on the checklist of items proposed in [12].

Section/Topic	Checklist Item
– Title, abstract, and structured summary; – Research method; – Synthesis of data items; – Discussion and analysis of data items; – Synthesis of results of analysis; – Limitations and risks of bias; – Conclusion and future work.	– Provided a structured summary including background, objectives, and methods; – Indicated research methods, including protocols, screening and quality assessment rules, and data extraction formats; – Provided a summary of the data extracted from the literature, including results, discussion, and limitations; – Established attributes for comparison between the data extracted from each article and conducted a comparative analysis of the data; – Presented a synthesis of the main findings of the analysis of the data items; – Discussed any limitations at the study and outcome level and specified any assessment of risk of bias; – Provided a general interpretation of the results in the context of other evidence and implications for future research.

3. Related Work

To the best of the author's knowledge, only one work in the literature has reviewed CS measures for NPPs.

The authors of [14] discussed the history of the implementation and application of CS in nuclear power plants. A total of 51 studies on the subject were reviewed by the authors. The authors cited regulations, policies, guidelines, CS frameworks, and software security measures as some of the most adopted strategies for CS assurance in NPPs. A list of major issues to be addressed was pointed out by the authors:

- Development and testing;
- Secure design;
- Biological approaches to security;
- Usable security;
- CS metrics;
- Anomaly and misuse detection systems;
- Policy security;
- Cyber retaliation;
- CS related to legal issues;
- The economics of CS;
- In security cyber defense;
- Spam dealing.

While the authors raised relevant criticisms of software and CS hazards, their work was limited in providing an understanding of the interdependencies among preventive measures.

In addition to this work, a number of reviews were identified that focused on CS for other sectors of critical infrastructure. Many of the requirements and measures observed in these works can be applicable to the nuclear domain or could be adapted to serve as cyber defense tools for NPPs' I&C systems.

For example, the authors of [15] conducted a review of Smart Grid CS. In their work, the authors reviewed and categorized solutions based on the five categories that make up different components of the Smart Grid: Process Control System (PCS) Security, Smart Meter Security, Power System State Estimation Security, Smart Grid Communication Protocol Security, and Smart Grid Simulation for Security Analysis.

The authors of [16] conducted a systematic review of countermeasures available to combat internal threats in healthcare critical infrastructure. According to their analysis, there was high heterogeneity across raw data, which indicated that the effectiveness of security measures varied significantly and that no single solution was able to totally mitigate an insider threat. For this reason, the authors suggested that a combination of security measures be utilized, which should grant an additional layer of protection according to the defense-in-depth model. The authors concluded by stating that significant work still needs to be undertaken to create more effective IDPS techniques. Further work also needs to be undertaken to create a model of threat mitigation that takes into account an unknown malicious insider, as well as to understand the nature of insider threats so that new technologies can be developed around potential further findings.

The authors of [17] conducted a survey of the risks, types of systems involved, and additional information used to develop and maintain a robust process control system for SCADA systems in critical infrastructure. The authors stated that an essential element and key factor of developing and implementing an SCADA CS program is the selection and implementation of a risk-based assessment method.

In Table 3, a summary of the recommendations from the authors of the above works is given, together with the domains of application and challenges/shortcomings noted in their works.

Table 3. Recommendations, challenges, and shortcomings of related survey works.

Work	Domain	Recommendations	Challenges	Shortcomings
Khattak et al. [14]	NPP CS	Establish SC framework composed of policies, CS team, security instrumentation, and a CS plan.	Lack of research and experience in NPP digital security and process control frameworks.	Work heavily relies on the outdated and regional RG 1.152 US regulation. The proposed NPP security framework is not very cohesive and is described at a high level of abstraction for various components.
Baumeister [15]	Smart Grid security	Used IDS in smart meters and other Smart Grid components; secure communication challenges; used a simulation to evaluate Smart Grid security.	Challenges due to the physical nature of Smart Grids, which causes them to be spread over large areas and be composed of many pieces. There is a need for advancements in current Smart Grid simulators.	The work describes various CS solutions for Smart Grids in a granular fashion instead of proposing a holistic model.
Walker-Roberts et al. [16]	Healthcare CI security	Use of multiple security measures at once. Ensured that confidential information is accessible only to authorized personnel. Improved the accuracy of current instrumentation.	Current machine learning techniques used to predict and prevent attacks and incidents are not accurate enough. Algorithms need optimization.	The work only considered certain aspects of healthcare CI CS, excluding others, such as personnel unawareness and lack of sophisticated policies.
Henrie [17]	SCADA CI security	Mitigation approach based on policies, procedures, technological solutions, standards, and best practices.	It is hard to prevent unintentional internal incidents. Risk analysis techniques sometimes do not consider the ratio of incident likelihood to possible damages.	While the work does suggest a well-structured and multi-layered mitigation approach, it does not describe the layers with enough detail to aid in developing an appropriate framework.

As can be noted from Table 3, many of the works described above provided limited descriptions of the analyzed solutions; this makes it challenging to compare them to each other, but also allows the development of a well-structured framework. For this reason, in the following sections, we will be describing all of the CS measures proposed in the literature for NPP protection based on their characteristics. This will later allow for comparisons of these solutions and identification of gaps and challenges.

4. Literature Review

The results of our literature review and the final selection of articles are depicted in Table 4.

After analyzing and extracting data from the articles, it was evidenced that these were distinguishable into three different categories of CS measures based on the focus of their findings: (i) **Critical Digital Asset (CDA) discovery methods**, (ii) **risk assessment and cyber attack taxonomies**, (iii) **protection measures for NPPs' I&C systems against vulnerabilities and attacks**. Based on this categorization, the selected works are described in further detail in the upcoming sections to better understand and compare the solutions proposed for each category.

Table 4. Domain and proposed CS measures of the works included in the literature review.

Work	Domain	Proposed Measure
Kim et al. [18]	Digital plant protection system; plant monitoring annunciator system	CS testbeds.
Symonov and Klevtsov [19]	Cyber threats in an NPP regulatory framework in the area of computer security of NPPs	Protection plans and attack mitigation; normative document.
Wang et al. [20]	NPPs' vulnerable components and failure points	Monte-Carlo-based exploration framework for identifying components vulnerable to cyber threats in NPPs.
Song et al. [21]	Technical definition control	Analysis of attack vectors and penetration tests.
Chung et al. [22]	Digital Instrumentation and Control (I&C) Systems	Implementable instrumentation and control system analysis model.
Peterson et al. [23]	Digital I&C systems	Review of past cyber-vulnerability incidents.
Park and Lee [24]	Digital I&C Systems	Quantitative assessment framework for evaluating NPP risk due to cyber attack scenarios.
Ibrahim and Al- Hindawi [25]	NPP modeling and verification	Attack graph modeling for a nuclear power plant modeled using the Architecture Analysis and Design Language (AADL).
Soupionis et al. [26]	Distributed Control Systems (DCSs)	Simulated the power grid network (including nuclear plant), but emulated the Information and Communications Technology (ICT).
Cho and Woo [27]	Cyber terror attacks	Defense-in-depth concept.
Shin et al. [28]	Digital equipment and digital systems	CS risk evaluation model.
Kim et al. [29]	Industrial Control Systems (ICSs) and Supervisory Control and Data Acquisition (SCADA)	Template for cyber attack taxonomy.
Cho et al. [30]	Digital and cyber-based systems	Levels/layers of protection to manage cyber/physical security.
Kim et al. [7]	Digital assets	Criteria for identifying digital assets.
Kim et al. [31]	CS incident affecting the NPP I&C	CS vulnerability checking system.
Cho and Woo [27]	Nuclear terror	Study of twelve nuclear terror cases.
Kim [2]	Digital control systems	Countermeasures for protecting nuclear power plants against cyber attacks.
Gupta et al. [32]	Electrical Power System (EPS) design and implementation	Cyber threat scenarios for the EPSs and EPS interfaces.
Lee et al. [33]	Digital I&C systems' regulatory documents	Quantitative method for evaluating the efficacy of security controls for DI&C systems in NPPs based on the intrusion-tolerant concept.
Vaddi et al. [34]	Digital I&C Systems	Event classifier for classifying abnormal events.
Jharko et al. [35]	Digital I&C Systems	Early fault diagnostic system (EDS).
Zhao et al. [36]	Risk assessment in NPPs	Finite-horizon semi-Markov general-sum game.
"IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations" [37]	NPP design requirements	Criteria for the design of an integrated security system for nuclear-power-generating stations.
Adams et al. [38]	CS attack prevention in NPPs	Cyber emulation of a digital control system.
Son et al. [39]	Digital assets	Approach to comparing and analyzing various methods used in the CS field to discover complementary points for the application of CS to critical systems in NPPs.
Boring et al. [40]	Role of reactor operators in detecting and mitigating cyber attacks in NPPs	Cyber concept of operations.
Park and Lee [41]	Digital assets	Importance analysis method for cyber attacks on an NPP.
Khattak et al. [14]	NPPs CS	Review of CS applications in nuclear power plants.
Zou [42]	NPPs CS	Security risk analysis of NPPs.
Zhang and Coble [43]	Digital I&C Systems	Localized kit for key equipment in a process as a complementary detection method to improve the robustness of key equipment under cyber attacks.
Jharko [44]	Faults of safety-critical software	Approach based on the "safety functions" for software verification of upper-level systems of automated process control systems.
Liu et al. [45]	Digital I&C Systems	General configuration and functions of a digital I&C system of an NPP.
Kim et al. [46]	Digital I&C Systems	Analysis of the effects of safety system unavailability on plant safety and human actions based on emergency operating procedures.
Jones et al. [47]	NPPs CS	Systems-engineering-focused approach for addressing NPP cyber threats.
Barker and Cheese [48]	NPP CS	Diode technology for providing corporate users with real-time plant data.
Li et al. [49]	Digital I&C Systems	Specific approaches to implementing a framework for I&C systems for prevention, detection, and response.

4.1. Critical Digital Assets in Nuclear Power Plants

Prior to developing a risk-informed CS strategy, an analysis of the system should be conducted to identify significant CDAs. Digital assets are classified and managed as CDAs that have safety, security, and emergency preparedness functions if they are the most sensitive to cyber attacks in terms of the functioning of the plant. On average, CDAs represent 70–80% of all digital assets, and applying and managing the same security control for all assets is inefficient [7]. The identification of these assets is necessary for the development of CS systems, which will be dependent on numerous factors, such as attack paths, methods, and potential target systems [41].

In the US, RG 5.71 is the regulatory guide that has been put forth to provide a framework to aid in the identification of these CDAs. The goal of this regulatory guide is to harmonize the set of security controls (based on NIST CS standards) that address potential cyber risks to CDAs.

RG 5.71 defines a level-based defensive architecture and a set of security controls addressing the potential cyber risks of CDAs. More specifically, RG 5.71 defines different levels of protection and divides the security controls into three categories: (1) technology, (2) operation, and (3) management.

That said, RG 5.71 only offers a general overview of tools and criteria for the identification of these CDAs. For this reason, much research has been conducted to develop and discuss methods in order to aid in the identification of assets that should be considered critical.

The authors of [7] presented criteria for identifying digital assets, which were classified as Vital Digital Assets (VDAs) by the authors. Their proposed criteria for selecting VDAs followed a step-based procedure. The procedure consisted of the following steps: first, gathering information for selecting VDAs; then, selecting initial events that could be caused by cyber attacks, and finally, selecting and analyzing accident mitigation facilities and selecting VDAs from target sets. The authors found that it is more economically and operationally efficient to manage the application of graded security controls to VDAs than to apply equivalent security controls to a number of CDAs. The authors concluded by indicating that further research should be conducted to understand how to apply and regulate the VDA approach in actual nuclear power plants.

The authors of [39] suggested a selection of complementary points of CS to be used to understand the requirements of nuclear regulations and to find complementary considerations in nuclear CS. The authors believe that further work in this direction could aid in resolving the nuclear CS issues and could help discover the deficiencies in nuclear CS schemes.

4.2. Risk Assessment and Threat Analysis for NPPs

The CS guides and regulations formulated by international organizations and countries, such as RG 5.71, mostly provide general guidance for CS risk assessment.

According to [19], international regulatory guides present a series of shortcomings:

- Lack of assessment methods for computer security conditions and identification of security vulnerabilities;
- Lack of assessment methods for computer risks and threats;
- The development stage does not consider computer security issues;
- Lack of consideration for aspects of training and attestation of personnel concerning computer security.

The authors of [50] suggested classifying attacks by their format/character:

- Information-gathering attacks;
- Active attacks to disable or compromise the proper functioning of one or several computers or other devices critical to a facility's safety or security;
- Concurrent modes of attack.

The authors of [23] argued that the vulnerability assessment methodologies proposed by the US Nuclear Regulatory Commission (NRC) require several key additions and changes to increase their efficacy. Some of the changes suggested by the authors include conducting and storing a comprehensive inventory of digital systems and components, conducting more penetration testing, using vulnerability databases and analysis software, and improved use of vulnerability assessment methods.

The authors of [19] suggested categorizing threats to NPPs into cyber threats at the stage of development of I&C systems and cyber threats at the stage of operation of I&C systems at NPPs. Additionally, these threats could also be sub-divided based on whether they are internal or external.

To identify possible risks and overcome the gaps found in the current regulatory frameworks, many vulnerability assessment methodologies have been proposed in the literature. A potential security risk analysis of NPPs should include probability of attack by the adversary, attack purpose, and attack ability [42].

To evaluate CS risk in accordance with regulatory guides such as RG 5.71, the authors of [28] proposed a CS risk model using a Bayesian Network (BN) for a Reactor Protection System (RPS) of a nuclear reactor, as well as a methodology for applying analytical results from a BN model to an event tree model. The model was developed to overcome the limitations of previously used fault trees as a Probabilistic Safety Assessment (PSA) method.

Another risk assessment framework was proposed by [24]. The framework proposed by these authors evaluates risk by defining the difficulty and consequences of a cyber attack, basing assessment methods on Bayesian belief networks and probabilistic safety assessment methods. The authors demonstrated the feasibility of the proposed framework by quantitatively evaluating several cyber attack scenarios based on the developed models for difficulty and consequences as a case study. Finally, the authors suggested that the framework may be used for risk-informed regulation of cyber attack scenarios and CDAs with quantitative goals, as well as risk-informed CS strategies and related evaluation efficiencies.

According to RG 5.71, periodic checking of the I&C systems should be conducted to identify any possible CS vulnerabilities. For this reason, CS vulnerability checking systems, such as the one proposed by [31], should be used to reduce the impact of vulnerabilities, as well as to ensure compliance with the automatic check regulatory guidelines. A fundamental requirement of these scanning tools is that they should not generate excessively high network traffic or overhead on the objects to be scanned.

The work by [45] determined the levels of CS protection for the subsystems and equipment of a digital I&C system of an NPP. These levels were determined using the CS defense-in-depth model, an example of which is shown in Figure 2. The authors tried to identify the potential CS risk factors, namely, assets, threats, and vulnerabilities. The proposed risk analysis was then carried out each of the identified levels.

The authors of [41] proposed an importance analysis method for cyber attacks against an NPP using the Probabilistic Safety Assessment (PSA) method. The authors started by identifying possible cyber attacks with failure modes. The authors demonstrated the proposed PSA method with two case studies. In the case studies, the risks of two cyber attack scenarios were quantitatively evaluated with two risk metrics: Core Damage Frequency (CDF) and Conditional Core Damage Probability (CCDP). The authors concluded that by identifying significant CDAs and classifying cyber attacks using quantifiable measures, it should be possible to develop a defense strategy against cyber attacks on NPPs that is both reliable and efficient.

The authors of [51] presented a qualitative methodology for CS assessment that is appropriate for nuclear I&C systems. The authors conducted an assessment based on a questionnaire comprising 162 questions divided into five categories. An evaluation of the questionnaires was then conducted by weighting each response depending on whether the results showed the overall CS status for each category, and they conducted an evaluation of the system as a whole. The authors suggested that this methodology could serve as a CS index at an initial phase of the system development for the CS assessment of nuclear

I&C systems. Nonetheless, further research needs to be conducted to assign detailed CS countermeasures in each category.

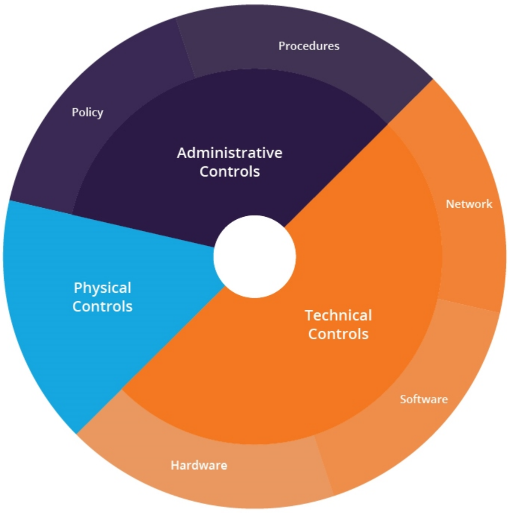

Figure 2. Example of the layered security architecture of the defense-in-depth model.

Possible attacks may also be categorized into taxonomies to facilitate both their identification and preventive action planning. The authors of [7] highlighted that it is difficult to study cyber attack taxonomies for NPPs considering the characteristics of ICSs and the inadequacy of research compared to such issues in information technology. The authors suggested a template for a cyber attack taxonomy based on the characteristics of NPPs, exemplified a specific cyber attack case in the template, and proposed a systematic countermeasure selection strategy by matching the countermeasures with CDAs and security control in RG 5.71. The taxonomy included the attack procedure, attack vector, attack consequence, vulnerability, and countermeasure selection.

The authors of [34] noted the importance of correctly classifying cyber attacks and distinguishing them from fault-induced safety events. For this purpose, the authors developed an event classifier to classify abnormal events in NPPs as either fault-induced safety events or cyber attacks. While the classifier was proven to be successful in distinguishing different types of abnormal events, more work is needed to enable the classification of combinations of safety events and cyber attacks.

The authors of [20] proposed a Monte-Carlo-based exploration framework for generating cyber attack scenarios in Cyber–Physical Systems (CPSs). The method takes into account various failure modes of attacked components of the CPSs and outputs the possible effects of the cyber threats on the system. According to their analysis, actuators are the most vulnerable CPS components, as their failures may lead to the loss of system functionality and integrity.

The authors of [22] proposed a method for calculating the degree of risk to a nuclear reactor's systems based on multiple factors for the purpose of safety. The authors presented a security threat mapping table, which was used to define and specify security problems. An important observation noted by the authors is that to create security profiles, environmental elements, security assumptions, and the organization's security policy must be analyzed. The model developed by the authors has already been implemented in reactor protection systems that are operating in the Republic of Korea. Nonetheless, additional research on I&CS protection profiles and security functions is suggested.

A possible way to study attack vectors is by simulating threat scenarios both theoretically and with the aid of simulation platforms. The authors of [32] presented three threat scenarios related to the Electric Power Systems (EPSs) of NPPs. This type of modeling is believed by the authors to be a useful input for security analysis and closed-loop virtual validation via simulation and Fault Tree Analysis (FTA).

Another effective way of understanding threats to NPPs is by modeling attack scenarios or attack graphs; this can be done by either taking the security-related details of the NPP system into consideration or not [25].

The authors of [21] described methods of defining attack vectors in NPP systems. Additionally, techniques for reviewing and selecting requirements in RG 5.71 were also described. Finally, methods of integrating the results of the previous techniques to identify possible technical security controls to counter respective attack vectors were also described. To conduct the attack vector analysis process, analysis of the system architecture and of attack vectors, modeling of the target system, assignment of the security level of its CDAs, and investigation of the known vulnerabilities of these CDAs are all suggested.

The authors acknowledged that further studies are needed to research the details of the practices of those control requirements and to develop security devices and technologies best fitted to NPP I&C systems.

Study of attack procedures, vectors, and consequences should not be conducted only on a theoretical basis, but should be supported by real-life occurrences. An example of such a study is the analysis of the cyber terror attacks against NPPs that occurred in South Korea conducted by [27]. This type of analysis aids in understanding the factors motivating the attackers, and also gives a concrete outlook of the consequences of successful attacks on these critical systems.

Another study that used historical incident analysis as a basis for developing a quantitative CS assessment method was discussed in [52]. The authors proposed organizing initiating threats and their bounding groups for NPPs to determine threats based on actual industrial incidents. It was also suggested to apply the same criteria to Probabilistic Safety Assessments (PSAs) in order to describe scenarios and models of NPP cyber risk. Nonetheless, the authors argued that the quantification of the probability of each scenario should also be conducted in order to understand the likelihood of each attack.

4.3. Measures for NPP Protection

After obtaining an understanding of the threats and vulnerabilities that afflict the digital systems of NPPs, it is necessary to establish measures to protect them from computer threats and techniques for the mitigation of cyber attacks. As indicated by [30], the cyber/physical security of NPPs may require the management of different levels/layers of protection in accordance with the standard set by RG 5.71. According to [19], standards of minimum acceptable risks are challenging to develop due to the constant progress and modernization of information technology and digital systems, in addition to the new threats and tools that are constantly being developed. For the same reason, standardized measures for protection from or mitigation of cyber attacks are just as arduous to define.

In the series of documents published by the International Atomic Energy Agency (IAEA) [50], it was suggested that the basic principle to follow to protect against computer threats is the use of the defense-in-depth model. This model is based on the idea of using multiple layers of often independent protection measures to guarantee multi-level protection without single points of failure.

The authors of [19] described an action list of activities to conduct during the development, implementation, maintenance, and improvement of computer security in NPPs in accordance with the procedures defined in the international standards and regulatory guides.

Approaches to CS threat prevention, detection, and response of (IT) systems that have proven to be successful have also been suggested to be used for I&C systems of NPPs. Naturally, differences in real-time operational requirements, distinct communication protocols, and requirements for continuous availability of the systems need to be considered when adapting these approaches for I&C systems in NPPs.

The authors of [49] proposed specific approaches to implementing a framework for prevention, detection, and response for I&C systems. For prevention, the authors suggested monitoring and auditing I&C systems to meet the real-time requirements. For detection, an intrusion detection approach based on physical data was proposed in order to deal with the distinct communication protocols. Finally, for response, the intrusion-tolerant control was proposed to maintain continuous availability. According to the authors, this overall solution, when combined with a safety design principle, should provide an overall solution for CS of I&C systems.

In addition to to adapted frameworks for CS, a number of approaches specifically developed for the CS of I&C systems of NPPs have appeared in the literature.

The authors of [35] proposed a framework for CS assessment using an Early Fault Diagnostics System (EDS) during the operational stage. The EDS aims to prevent the evolution of the incident/accident by using a troubleshooting process in any plant operational mode. This would allow plant operators to identify any significant deviation of plant parameters from their normal value, well before reaching any undesired threshold that would potentially lead to a prohibited plant state, together with the cause that generated the deviation.

The authors of [47] laid out a new systems-engineering-focused approach for addressing threats to NPPs, which they named System-Aware Security (SAS) for NPPs. The authors theoretically demonstrated a possible application of the methodology in order to address cyber attacks employed via embedded infections in NP systems. The authors highlighted that the approach still has several limitations, and further work in component integration and security analysis may be necessary to improve the model.

To improve the robustness of key equipment under cyber attacks, the authors of [43] proposed a localized kit for key equipment in a process as a complementary detection method. The authors highlighted that the proposed model reduced the total number of variables used and improved the computational speed when compared to other models.

The authors of [33] proposed a quantitative method for evaluating changes in CS when specific CS controls are applied in NPPs. The amount of improvement achieved by security controls was defined as the reduction of the probability that the system would fail to protect essential functions from a cyber attack. Additionally, the authors applied the concept of the intrusion-tolerant system. According to this concept, the tolerance to intrusion of a system is defined as the extent to which the system is able to provide the minimum level of safe operation when facing unexpected intrusions. The authors then constructed an event tree with the investigated intrusion-tolerant strategies for the case of protecting the availability of essential functions. The authors concluded that there still exist some limitations in estimating the efficacy of CS controls due to the lack of detail in the methods for obtaining the probability of the detection strategy and the GD strategy.

Many researchers have realized in recent years that the concept of having a multi-layered CS defense system should not be exclusive to the implementation of safety and security measures, such as firewalls, intrusion detection systems, and fail-safe safety systems. It is not wise to expect that these measures will be able to anticipate all attack vectors and, as such, it is highly recommended that operators are readily responsive when it comes to detecting and preventing these types of incidents.

The authors of [40] reviewed the role of reactor operators in detecting and mitigating cyber attacks in nuclear power plants. The authors introduced the idea of a cyber concept of operations, in which operators treat cyber intrusions in the same way that they would other hardware faults at the plant. A pilot study was conducted, in which reactor operators were asked to and succeeded in navigating the plant to a safe state despite cyber spoofing across multiple scenarios. The findings from the experiments confirmed that having dedicated operators can help ensure plant resilience to cyber attacks.

By using n-conventional Fault Tree (FT) analysis, the author of kim2017systematic conducted a study on the effects of safety system unavailability on plant safety and analyzed human actions based on emergency operating procedures. Based on this combined analysis, the authors suggested a novel method of systematically developing cyber attack propagation scenarios, where a cyber attack is linked to its consequences. The analysis was focused on the operator's actions and the effects on the system in case of the failure of action. Future research should focus on the study of the generation of the initiating event of a cyber attack, which was not discussed in this author's work. In addition, operator behavior should also be analyzed in future studies in order to understand the effects of different types of training and any other factors that may influence their behavior.

When it comes to evaluating the operator's ability to successfully respond to malicious attacks or undesired events, the authors of [38] suggested using a cyber emulation of a digital control system coupled with a training simulator of a Generic Pressurized Water Reactor (GPWR). In an experiment set up by the authors, licensed operators were asked to complete a series of scenarios on the simulator, some of which were purposefully obfuscated. The results from the experiments showed that even after obfuscating certain indicators, the combination of security systems and operator actions was sufficient to detect the attack and protect the system. Limitations in the number of participants and indicator values should be overcome in later iterations of such experiments to allow for more realistic evaluations.

To support cyber attack response and effective risk assessment, reduce the risk of cyber attacks, and improve the resilience of NPPs, the authors of [36] proposed a finite-horizon semi-Markov general-sum game between a defender and an attacker to obtain the time-sensitive attack response strategy and the real-time risk assessment in NPPs. By applying the model and the method to a simplified digital feedwater control system for a generic pressurized water reactor, the authors showed that the defender's optimal strategy varies with different system states and different amounts of time remaining in the game. The authors concluded that more research must be conducted in order to collect datasets, understand real-world defender—attacker interactions, and integrate changes in operation due to malfunctioning or other unexpected occurrences.

Unfortunately, it is not possible to conduct vulnerability tests directly on NPPs; this is because of the risks of adverse effects, which could provoke serious damages to the systems and interrupt their functioning. To circumvent this issue, testbeds are often used to test technical solutions.

The authors of [18] suggested the design of a CS testbed for a Digital Plant Protection System (DPPS) and Plant Monitoring and Annunciator System (PMAS). Network connectivity was considered an important element for the analysis and design of the cyber security testbed. Unfortunately, the testbed has yet to be completed. Once completed, the authors have planned the development of a test to detect malware, such as APT for control systems, as well as a vulnerability test.

The authors of [26] also presented the implementation of a cyber–physical testbed. Their testbed included the implementation of two simulated and interconnected Critical Infrastructures (CIs), namely, a power grid and a nuclear plant. Additionally, the following components were included in the testbed:

- A simulated power market for providing the cost of the provided energy;
- An actual Programmable Logic Controller (PLC), which is interconnected with a specific bus of the power network;
- An emulated cyber network that interconnects and controls all of the aforementioned elements.

The novelty of this system comes from interconnecting this diverse range of elements and, by doing so, aiding the understanding of the consequences of the interdependencies between the different systems. The authors showed that the effects of network parameters on a coordinated attack could be significant. The authors are planning to make use of the implementation to run more advanced experiments, which will include the actions of real operators in the cyber–physical testing/simulation process. Additionally, they plan to implement a set of countermeasures to tackle and mitigate the attacks based on the exchanged signals and their statistical analysis to detect anomalies.

5. Discussion

According to our analysis and the data extraction from the articles selected for this review, CS of NPPs requires three sequential phases: (i) identifying critical digital assets using discovery methods; (ii) establishing and conducting a risk assessment and threat analysis; (iii) installing a layer of protective measures for NPPs' I&C systems against vulnerabilities and attacks.

An equivalent procedure is described in the current standards and guidelines that define the CS risks, as well as the defensive architectures and security controls necessary to address these risks, as is the case for the RG 5.71 regulatory guide [19].

The articles discussed in Section 4.1 offered more detailed instruments and methods for identifying CDAs of NPPs, while in Section 4.2, we analyzed the various methods and procedures suggested in the literature for risk assessment and threat analysis for NPPs. Finally, defensive measures for detection and prevention of threats were discussed in Section 4.3.

One of the main limitations noted during this analysis is that the majority of measures proposed for NPP CS were not developed using this sequential approach. The lack of holistic CS cyber defense based on the interdependences of critical assets, risks, and threats, as well as different layers of protection requirements and results in accordance with the defence-in-depth model, has been established.

Supplementing software-based security solutions with human competence development and readiness has also been found to be lackluster. These two security components are often developed separately; this limits the complementary aid that each can provide to both the other component and to the security of the system as a whole.

Limitations to holistic approaches for cyber defense strategies for NPPs were often motivated by the novelty of research specific to the nuclear domain and its intrinsic requirements. Many of the models discussed were, in fact, adapted from the IT CS domain and require further improvement in order to become fully applicable to NPP cyber defense.

6. Conclusions

The CS of NPPs is a growing concern. The digitalization of I&C systems has caused cyber threats to be as dangerous as physical threats to the functioning and damages that could be caused to nuclear facilities. In this work, we reviewed the literature to establish the state of the art in CS measures for NPP protection. More specifically, we highlighted both standards and regulations, as well as proposals for measures to identify CDAs, analyze risks and threats, and establish cyber defense mechanisms and measures against these threats.

It has been noted that the development of solutions specific to the nuclear domain has been mostly a recent focus of researchers, and as such, many of the proposed solutions are often limited in their functionality or applicability in real-life NPP I&C systems.

Based on the findings of this work, the main challenge in current NPP CS is providing a holistic security approach based on a layered Defense-in-Depth (DiD) model. While such an approach is not novel and has, in fact, been adopted in many other industries and CI sectors, both adoption and research specific to its development in NPPs were found to be lacking.

Limitations in resources and the novelty of the research area have been identified as the two main reasons for the current shortcomings.

Nonetheless, researchers are showing continuous efforts to adapt DiD models developed for different CI sectors to NPP protection, with additional promising software solutions currently in progress.

7. Future Research

This work presents a theoretical study on current CS measures for NPP protection. Many of the solutions described in this work have not been validated through experimentation. For this reason, future research should concentrate on both expanding the capabilities of current proposals and conducting tests to assess both the effectiveness and applicability of these in the nuclear domain. Additionally, further work should be conducted to harmonize the proposals to be in accordance with a holistic defense-in-depth model, where requirements are built based on the interdependent security needs and objectives of each layer of protection. Finally, it is recommended to continue research that is focused on improving the performance and reliability of IDPSs, the algorithms used in risk assessment and communication channel security, and the capabilities and performance of NPP simulators.

Funding: This research was funded by the Norwegian University of Science and Technology (NTNU).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Porthin, M.; Liinasuo, M.; Kling, T. Effects of digitalization of nuclear power plant control rooms on human reliability analysis–A review. *Reliab. Eng. Syst. Saf.* **2020**, *194*, 106415. [CrossRef]
2. Kim, D.Y. Cyber security issues imposed on nuclear power plants. *Ann. Nucl. Energy* **2014**, *65*, 141–143. [CrossRef]
3. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Comput. Secur.* **2011**, *9*, 49–51. [CrossRef]
4. Chen, T.M.; Abu-Nimeh, S. Lessons from stuxnet. *Computer* **2011**, *44*, 91–93. [CrossRef]
5. Farwell, J.P.; Rohozinski, R. Stuxnet and the future of cyber war. *Survival* **2011**, *53*, 23–40. [CrossRef]
6. Park, J.; Suh, Y.; Park, C. Implementation of cyber security for safety systems of nuclear facilities. *Prog. Nucl. Energy* **2016**, *88*, 88–94. [CrossRef]
7. Kim, S.; Kim, S.; Nam, K.H.; Kim, S.; Kwon, K.h. Cyber Security Strategy for Nuclear Power Plant through Vital Digital Assets. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 224–226.
8. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
9. Ganin, A.A.; Quach, P.; Panwar, M.; Collier, Z.A.; Keisler, J.M.; Marchese, D.; Linkov, I. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Anal.* **2020**, *40*, 183–199. [CrossRef]
10. Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* **2017**, *3*, e00346. [CrossRef] [PubMed]
11. Gupta, D.; Bajramovic, E.; Hoppe, H.; Ciriello, A. The need for integrated cybersecurity and safety training. *J. Nucl. Eng. Radiat. Sci.* **2018**, *4*, 041006. [CrossRef]
12. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med.* **2009**, *6*, e1000097. [CrossRef] [PubMed]
13. Kofod-Petersen, A. How to Do a Structured Literature Review in Computer Science. Ver. 0.1. 1 October 2012. Available online: https://docplayer.net/43782220-How-to-do-a-structured-literature-review-in-computer-science.html (accessed on 10 May 2021).
14. Khattak, M.A.; Shaharuddin, M.K.H.; Islam, M.S.; Ahmad, M.H.N. Review of cyber security applications in nuclear power plants. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2017**, *7*, 43–54.
15. Baumeister, T. Literature Review on Smart Grid Cyber Security. Available online: https://csdl.ics.hawaii.edu/techreports/2010/10-11/10-11.pdf (accessed on 10 May 2021).
16. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access* **2018**, *6*, 25167–25177. [CrossRef]
17. Henrie, M. Cyber security risk management in the SCADA critical infrastructure environment. *Eng. Manag. J.* **2013**, *25*, 38–45. [CrossRef]
18. Kim, Y.S.; Moon, I.S.; Lee, S.I. A design of cyber security test-bed for DPPS and PMAS in Korean operating nuclear power plant. In Proceedings of the 2016 16th International Conference on Control, Automation and Systems (ICCAS), Gyeongju, Korea, 16–19 October 2016; pp. 1480–1483.
19. Symonov, A.; Klevtsov, A. About the problem of regulatory activity for computer security of NPP instrumentation and control systems in Ukraine. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, UKraine, 24–27 May 2018; pp. 6–11.
20. Wang, W.; Cammi, A.; Di Maio, F.; Lorenzi, S.; Zio, E. A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliab. Eng. Syst. Saf.* **2018**, *175*, 24–37. [CrossRef]
21. Song, J.G.; Lee, J.W.; Park, G.Y.; Kwon, K.C.; Lee, D.Y.; Lee, C.K. An analysis of technical security control requirements for digital I&C systems in nuclear power plants. *Nucl. Eng. Technol.* **2013**, *45*, 637–652.
22. Chung, M.; Ahn, W.; Min, B.; Seo, J.; Moon, J. An analytical method for developing appropriate protection profiles of Instrumentation & Control System for nuclear power plants. *J. Supercomput.* **2018**, *74*, 1378–1393.

23. Peterson, J.; Haney, M.; Borrelli, R. An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. *Nucl. Eng. Des.* **2019**, *346*, 75–84. [CrossRef]
24. Park, J.W.; Lee, S.J. A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence. *Ann. Nucl. Energy* **2020**, *142*, 107432. [CrossRef]
25. Ibrahim, M.; Al-Hindawi, Q. Attack graph modeling for nuclear power plant. In Proceedings of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018; pp. 1–6.
26. Soupionis, Y.; Piccinelli, R.; Benoist, T. Cyber security impact on power grid including nuclear plant. In Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS), Gdansk, Poland, 1–14 September 2016; pp. 767–773.
27. Cho, H.S.; Woo, T.H. Cyber security in nuclear industry–Analytic study from the terror incident in nuclear power plants (NPPs). *Ann. Nucl. Energy* **2017**, *99*, 47–53. [CrossRef]
28. Shin, J.; Son, H.; Heo, G. Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nucl. Eng. Technol.* **2017**, *49*, 517–524.
29. Kim, S.; Heo, G.; Zio, E.; Shin, J.; Song, J.g. Cyber attack taxonomy for digital environment in nuclear power plants. *Nucl. Eng. Technol.* **2020**, *52*, 995–1001. [CrossRef]
30. Cho, C.S.; Chung, W.H.; Kuo, S.Y. Cyberphysical security and dependability analysis of digital control systems in nuclear power plants. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *46*, 356–369. [CrossRef]
31. Kim, J.H.; Choi, Y.S.; Na, J.C. Cybersecurity Vulnerability Scanner for Digital Nuclear Power Plant Instrumentation and Control Systems. In Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, Shenzhen, China, 8–10 December 2018; pp. 463–467.
32. Gupta, D.; Bajramovic, E.; Parekh, M.; Waedt, K. Cyber threat scenarios for electrical systems of nuclear power plants. In Proceedings of the 2018 26th International Conference on Nuclear Engineering, London, UK, 22–26 July 2018.
33. Lee, C.; Yim, H.B.; Seong, P.H. Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept. *Ann. Nucl. Energy* **2018**, *112*, 646–654. [CrossRef]
34. Vaddi, P.K.; Pietrykowski, M.C.; Kar, D.; Diao, X.; Zhao, Y.; Mabry, T.; Ray, I.; Smidts, C. Dynamic bayesian networks based abnormal event classifier for nuclear power plants in case of cyber security threats. *Prog. Nucl. Energy* **2020**, *128*, 103479. [CrossRef]
35. Jharko, E.; Promyslov, V.; Iskhakov, A. Extending Functionality of Early Fault Diagnostic System for Online Security Assessment of Nuclear Power Plant. In Proceedings of the 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 8–14 September 2019; pp. 1–6.
36. Zhao, Y.; Huang, L.; Smidts, C.; Zhu, Q. Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants. *Reliab. Eng. Syst. Saf.* **2020**, *201*. [CrossRef]
37. *692-1997—IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations*; IEEE: Piscataway, NJ, USA, 1997; ISBN 978-0-7381-0711-0. [CrossRef]
38. Adams, S.S.; Murchison, N.; Bruneau, R.J. Investigating Cyber Threats in a Nuclear Power Plant. Available online: https://www.osti.gov/servlets/purl/1593630 (accessed on 10 May 2021).
39. Son, J.; Choi, J.; Yoon, H. New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants. *IEEE Access* **2019**, *7*, 78379–78390. [CrossRef]
40. Boring, R.L.; Ulrich, T.A.; Medema, H.M.; Lew, R. Operator Resilience to Cyber Interdictions in Nuclear Power Plants. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; pp. 247–251.
41. Park, J.W.; Lee, S.J. Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants. *Nucl. Eng. Technol.* **2019**, *51*, 138–145. [CrossRef]
42. Yan, Z.Y.; Chun, Z.J.; Liu, G.J.; Zou, L.L. Risk analysis of cyber security in nuclear power plant. In *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. SICPNPP 2017. Lecture Notes in Electrical Engineering*; Springer Nature Singapore Pte Ltd.: Singapore, 2017.
43. Zhang, F.; Coble, J.B. Robust localized cyber-attack detection for key equipment in nuclear power plants. *Prog. Nucl. Energy* **2020**, *128*, 103446. [CrossRef]
44. Jharko, E.P. Safety Functions in the Software Quality Assurance of NPP Safety Important Systems. In Proceedings of the 2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russia, 25–29 March 2019; pp. 1–6.
45. Liu, D.; Chen, Y.; Shi, J.; Chen, D. Study on Cyber Security Risk Assessment of Digital Instrumentation &Control System of Nuclear Power Plant. In Proceedings of the 2018 International Conference on Power System Technology (POWERCON), Guangzhou, China, 6–8 November 2018; pp. 4742–4750.
46. Kim, H.E.; Son, H.S.; Kim, J.; Kang, H.G. Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 290–301. [CrossRef]
47. Jones, R.A.; Nguyen, T.V.; Horowitz, B.M. System-aware security for nuclear power systems. In Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 15–17 November 2011; pp. 224–229.
48. Barker, R.; Cheese, C. The application of data diodes for securely connecting nuclear power plant safety systems to the corporate it network. In Proceedings of the 7th IET International Conference on System Safety, Incorporating the Cyber Security Conference 2012, Edinburgh, UK, 15–18 October 2012

49. Li, J.; Guo, C.; Si, W.; Huang, X. The Approaches of Prevention, Detection, and Response for Cybersecurity of I&C Systems in NPPs. In *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems. SICPNPP 2018. Lecture Notes in Electrical Engineering*; Springer Nature Singapore Pte Ltd.: Singapore, 2018; pp. 283–290.
50. International Atomic Energy Agency. *Computer Security at Nuclear Facilities: Reference Manual: Technical Guidance*; International Atomic Energy Agency: Vienna, Austria, 2012. (In Chinese)
51. Kang, Y.D.; Chong, K.T. Development of cyber security assessment methodology for the instrumentation & control systems in nuclear power plants. *J. Korea Acad.-Ind. Coop. Soc.* **2010**, *11*, 3451–3457.
52. Han, S.M.; Seong, P.H. Suggestion of Initiating Threats and Bounding Groups for NPP Cyber Risk Assessment. In Transactions of the Korean Nuclear Society Autumn Meeting, Yeosu, Korea, 25–26 October 2018.