energies

Article

IEC 62443 Standard for Hydro Power Plants

Jessica B. Heluany [1,*] and Ricardo Galvão [2]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2] PECE—Industrial Automation, University of São Paulo, São Paulo 2373, Brazil
* Correspondence: jessica.b.heluany@ntnu.no or jessica.heluany@gmail.com

Abstract: This study approaches cyber security in industrial environments focusing on hydro power plants, since they are part of the critical infrastructure and are the main source of renewable energy in some countries. The theoretical study case follows the standard IEC 62443-2-1 to implement a cyber security management system (CSMS) in a hydro power plant with two generation units. The CSMS is composed of six steps: (1) initiate CSMS, (2) high level risk assessment, (3) detailed risk assessment, (4) establish policies, procedures, and awareness, (5) select and implement countermeasures, and (6) maintain the CSMS. To perform the high-level risk assessment, an overview of the most common activities and vulnerabilities in hydro power plants systems is presented. After defining the priorities, the detailed risk assessment is performed based on a HAZOP risk analysis methodology focusing on hackable digital assets (cyber-HAZOP). The analysis of the cyber-HAZOP assessment leads to mitigations of the cyber risks that are addressed proposing modifications in the automation architecture, and this also involves checking lists to be used by the stakeholders during the implementation of the solution, emphasizing security configurations in digital assets groups.

Keywords: HPPs cybersecurity; cyber-HAZOP; IEC 62443; CSMS; smart grid

check for updates

Citation: Heluany, J.B.; Galvão, R. IEC 62443 Standard for Hydro Power Plants. *Energies* **2023**, *16*, 1452. https://doi.org/10.3390/en16031452

Academic Editors: Zhengwei Wang and Yongguang Cheng

Received: 25 November 2022
Revised: 18 January 2023
Accepted: 25 January 2023
Published: 1 February 2023

1. Introduction

The energy sector is a potential target for cyber-attacks given its role as critical infrastructure of a nation, which makes necessary the implementation of security strategies that hamper attacks such as ransomware, man-in-the-middle (MITM), denial-of-service (DoS), cross-site scripting (XXS), phishing, replay, false data insertion, jamming eavesdropping, spoofing, among others.

To facilitate the terminology understanding, in this paper, the common language established by the last release of NIST Framework and Roadmap of Smart Grid and Interoperability Standards (V4.0) [1] was adopted, where smart grids are conceptualized in a model with seven main domains: system transmission operators (TSOs); system distribution operators (DSOs); generation (including distributed energy resources (DERs); customer; markets; operations and service providers. Within each domain, actors and equipment have their respective roles and responsibilities in the electrical grid.

In countries where a considerable percentage of the produced energy comes from hydro power plants, it becomes very relevant to develop solutions and apply cybersecurity standards to this specific actor within the generation domain. The present paper is organized as follows: in Section 1, the motivation and the literature review are presented, justifying the purpose of this study and its contribution for the energy sector. In Section 2, some basic concepts are explained to give an overview of the steps that compose the study methodology, which involves the establishment of a cyber security management system (CSMS), which is detailed at Section 3. Then, a theoretical case study is developed in Section 4, and final considerations are discussed in Section 5.

1.1. Motivation

In recent discussions of cyber security in the energy world, considerable research attention has been directed toward smart grids. NIST conceptualization model makes clear that the term "smart grids" is broad and could be referring to any of the seven domains. On one hand, the high number of papers approaching cyber security in smart grids highlight the relevance of the topic. On the other hand, however, the broadness may hamper the applicability of such studies to specific actors within each of the seven domains. For this reason, attempting to collaborate by narrowing the topic in one of the domains, and this study focuses on generation, specifically hydro generation due to the background of the authors.

1.2. Literature Review

After identifying the energy market need for cyber security recommendations from practical experience, a brief review of the academic literature was conducted to better understand how the topic is being addressed and to acknowledge if there is a gap for the generation domain. Scopus was chosen as the database due to its broader range of publication sources. Filtering the field by "energy", format by "papers/articles", and running the query ((energy OR *grid) AND (cyber AND security)) in the title, 92 papers were collected for further screening.

Surprisingly, the first publications date from 2007, even before cyber-attacks rose in quantity and media attention. However, given that the aim of this study is to comprehend current approaches to smart grids, two exclusion criteria were applied to the set of papers: publication year was chosen from 2017 to 2022, and the content should be specific to any domain of smart grids, excluding end users of the "customers" domain, and other broad topics such as smart cities, smart homes, and electrical vehicles. This screening step resulted in 25 papers that were skimmed, resulting in 10 papers selected for detailed analysis.

In Table 1, the use case domain was identified and mapped against NIST domains together with the identified cyber security approach: risk vs. mitigation, attack vs. defence, network security, people management, and security management system. In some cases, the use case domain and the NIST domain coincide, while in others, the paper use case is referring to multiple NIST domains. It is interesting to note that, except for [2], the selected papers did not address an end actor within a domain, showing that there is a gap in the literature for narrower studies regarding cyber security in smart grid actors within each domain.

Table 1. Use case domain identified in analysed papers against NIST domains.

Paper title	Use Case Domain	NIST Domain	Cyber Security Approach
A microgrid ontology for the analysis of cyber-physical security	Microgrid	Generation; Distribution;	Attack vs. Defence
A novel actual time cyber security approach to smart grids	Substation	Distribution	Network security
Cyber security for multi-station integrated smart energy stations: Architecture and solutions	Smart Energy Stations (SESs)	Generation; Distribution;	Security management system
Cyber Security impact on energy systems	Virtual Power Plant (VPP)	Generation;	Risk vs. Mitigation; People management;
Cyber Security in the smart grid: challenges and solutions	Smart Grid	All	Risk vs. Mitigation
Cyber security in the energy world	Smart Grid	All	Network security
Grid cyber security strategy in an attacker–defender model	Power grid infrastructure	Distribution;	Attack vs. Défense
Improvement of cyber-security measures in national grid SA substation process control	Substation	Distribution;	Risk vs. Mitigation
Research on cyber security defence technology of power generation acquisition terminal in new energy plant	Power generation acquisition terminal	Generation;	Attack vs. defence
Smart grid cyber security enhancement: Challenges and solutions: a review	Smart Grid	All	Risk vs. Mitigation

Synthesizingpapers with a more generic smart grids security approach, refs. [3,4] report challenges and solutions using different perspectives. In [3], they conceptualize the smart grid and summarize the NIST security requirements regarding confidentiality, integrity, and availability to form the basis of the discussion about common risks and their corresponding mitigations according to the OSI layer. The following components are analysed: PMU (power metering unit), AMI (advanced metering infrastructure), smart meter, gateway, routing protocol, and control system. The risks mitigations recommended include input validation, DNSSEC, firewall, locking down ports, ICMP packet filtering, ARP inspection, disabling unused ports, and securing the physical infrastructure. Similarly, in [4], cyber attacks are mapped against confidentiality, integrity, and availability, but instead of suggesting techniques to overcome the security challenges according to the OSI layer, the countermeasures are classified according to an attack timeline divided into three steps: pre attack, under attack, and post attack. In addition to the mitigations listed in [3], this paper also explores more recent technologies, recommending IDS (intrusion detection system), blockchain, 5G, and AI (artificial intelligence). Both papers have an important role on demonstrating how vulnerable smart grids are and exemplifying some strategies to mitigate risks, but, at the same time, they emphasize that, besides the benefits brought by digital transformation, this also brings the need for a more robust security strategy.

In article [5], the authors mention diverse equipment that could be the target of cyber attacks, such as dispatch generators, electrical transformers, and circuit breakers. Moreover, one of the possible consequences cited, malfunction of a controller response, could lead to dangerous situations in terms of safety and security. Despite the use case is a microgrid, this equipment is also present in hydro power plants. The proposed solution, a combination of CIM (common interface model) and IEC 61850 for the development of an ontology, including AEGs (attack execution graphs), would allow the evaluation of cyber security issues through the generation of ADIVSE (ADVersary view security evaluation) models. Additionally, approaching network communication, ref. [6] examined standards and protocols most used in the power industry, highlighting IEC 60870-5 and DNP3 for SCADA systems and IEC 61850 for substations. In terms of substations security, in [7], the proposed solution is the implementation of homomorphic encryption in smart meters using MPI (message passing interface) with the Floyd-Warshall algorithm.

When it comes to the generation domain, ref. [8] recognized similar cyber attacks to the ones discussed so far, but also pointed that natural factors and human error/behaviour can lead to disruption in the energy supply. From a defence point of view, the authors claim that the responsibility of securing devices "is attached to the person" when, for example, applying patches or improving the company's personnel skills to manage incidents. For new power plants, ref. [9] applied an algorithm based on the Spark platform developed by AMP Laboratory of UCBerkeley to generate frequent item sets and extract association rules that were used to develop an anti-penetration strategy according to the results of the risk assessment. For lower impact systems, the strategy consisted of the packet filtering rule, while, for high-risk terminals with serious impact, the authors instantiated the anti-penetration strategy as address or port filtering rules.

Considering all these studies, but changing the perspective from risk vs. mitigation [2–4,8], attack-defence [5,9,10], or network security [6,7] to a security management view, only [11] proposed a holistic approach similar to the aim of this study. However, their focus is broader than generation, with the design a system architecture for smart energy stations composed of five entities: substation, photovoltaic station, energy storage station, electric vehicle charging station, and data centre station. Based on the data exchanges, they proposed cyber security protection solutions according to the principle of "security zoning, enhanced borders; dedicated network, multilayer protection; horizontal isolation, vertical authentication; classified storage, controlled sharing". Different zones are suggested, and the isolation devices range from industrial firewalls, forward/reverse isolators, and vertical encryption devices. Additionally, VLANs and service prioritization are addressed to guarantee real-time and no real-time communications.

1.3. Contribution

As observed in the literature review, there is limited research investigating cyber security in specific actors of smart grid domains. Nonetheless, given that knowledge building is complimentary, the previous studies analysed can be aggregated to transform approaches such as risk vs. mitigation or attack vs. defence into a holistic continuous security management approach, as suggested by IEC 62443-2-1 [12] with a cyber security management system (CSMS).

In the next topics, some basic concepts of safety, security, and risk analysis will be introduced to form the basis for the application of the IEC 62443-2-1 standard to a typical hydroelectric power plant, involving collaboration to cover the gap of domain/actor-focused studies. Systems and sub-systems of a two-generator hydro power plant will be evaluated considering the risk involved and the risk tolerance to make recommendations that are compliant with the IEC 62443-2-1 standard.

2. Conceptualization

2.1. Safety vs. Security

In the begging of the industrial revolution, plant safety was fundamental to strategic plans. The concern with injury or damage to the health of personnel, physical damage due to equipment incorrect operation according to input data, hardware failure, or error in operation were all taken into consideration to define the most appropriate technical solutions.

In industry 4.0, one of the main characteristics of the market solutions is the use of the internet to connect not only people, but systems themselves, being called IIoT (industrial internet of things). This technological evolution increases the cyber-attack surface. In this scenario besides safety, it is also important to focus on plant security, as well as investing in defence strategies of digital assets.

2.2. Risk Analysis

As defined at IEC 62443-1-1, risk is the “expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence” [13]. Risk origins can be either physical or digital. Risk analysis methodologies can be focused on these origins, what enables the reutilization of a safety analysis to a security analysis through the classification of assets into hackable or non-hackable.

2.3. HAZOP vs. Cyber-HAZOP

The HAZOP (hazard and operability) analysis is a highly systematic methodology. The facility is divided into systems (nodes) for which many scenarios are evaluated through the selection of parameters and guidewords. The objective is to identify the qualitative potential of hazards and operating problems associated with a system or piece of equipment caused by deviations [14].

Following the method proposed by [15], it is possible to turn the HAZOP into a cyber-HAZOP risk analysis by selecting hackable scenarios. In this case, the step-by-step equivalent procedure can be observed below:

1. Define premises about the plant;
2. Define parameters to be considered;
3. Select a system to be evaluated;
4. Briefly explain the process;
4.1. Specify a parameter;
4.1.1. Specify a guideword;
4.1.1.1. Undertake a threat analysis;
4.1.1.2. For each threat, identify if the system is vulnerable to an incident (scenarios);
4.1.1.3. Identify the worst consequences associated to each scenario without safeguards;
4.1.1.4. Specify existing safeguards for each consequence;
4.1.1.5. Determine the probability and severity of each consequence;

4.1.1.6. Make recommendations to mitigate consequences if the probability or severity of occurrence are inacceptable according to the level of risk acceptance stablished by the company;

4.1.2. Repeat step 4.1.1 for each guideword;

4.2. Repeat step 4.1 for each parameter;

5. Repeat step 4 for all plant nodes.

2.4. Hydro Power Plants Systems and Its Vulnerabilities

Usually, the scope of supply for a hydroelectric power plant (HPP) involves more than one company. Table 2 contains a typical case for an automation project.

Table 2. Main activities in HPPs automation projects and its typical suppliers.

Activity	Supplier
Engineering, tests, and commissioning of field network, process network, and supervisory system	Suppliers of automation and control systems
Communication between process data and office network	Suppliers of automation and control systems or information technology with customer participation, possibly involving IT and OT teams to support the activity
Communication link for remote access	Suppliers of automation and control systems or information technology with customer participation, possibly involving IT and OT teams to support the activity
Communication link with regulation agent	Automation and control systems suppliers generally subcontract telecommunications companies for this scope. Customer participation can involve IT and OT teams to support the activity.

In order to ease the implementation of defence in depth strategies, each activity can be associated to one or more configuration group of devices. To exemplify the vulnerabilities, Table 3 contains six group categories and its main vulnerabilities, highlighting that some of them are common to more than one group.

Table 3. Configuration categories and its potential vulnerabilities. Based on [16].

Category	Potential Vulnerabilities
Supervisory System	Poor physical security; lack of system hardening; inadequate security awareness; poor password policies; poor account management; social engineering susceptibility; lack of patch management; lack of authentication; zero-day vulnerabilities; ineffective anti-virus/application whitelisting; insufficient access control; use of vulnerable ICS protocols; untested third-party applications; insecure embedded applications;
Communication link with operation centre or regulation agent	Poor physical security; lack of system hardening; inadequate port security; lack of authentication; unnecessary firewall rules; lack of patch/firmware management; poor configuration management; configuration errors;
Communication between process data and office network	Poor physical security; lack of system hardening; inadequate port security; lack of authentication; unnecessary firewall rules; poor configuration management; lack of patch/firmware management; configuration errors; uncontrolled file sharing;
Network equipment	Poor physical security; configuration errors; poor configuration management; inadequate port security; lack of firmware management; unnecessary firewall rules; lack of intrusion detection capabilities; use of vulnerable ICS protocols;
Electrical protection system	Poor physical security; lack of firmware management; configuration errors; poor configuration management; lack of authentication; use of vulnerable ICS protocols;
Controllers	Poor physical security; lack of system hardening; lack of firmware management; untested application integration; configuration errors; poor configuration management; lack of authentication; use of vulnerable ICS protocols;

This rearrangement of vulnerabilities is deeply related in the modus operandi of HPPs automation project once this separation proposal enables one to address risk mitigation for specific suppliers.

3. CSMS Application Guide for HPP's According to IEC 62443

The IEC 62443 standard is organized in four groups: General, policies and procedures, system, and component. Together, they provide a vast amount of information for the implementation of a cyber security management system (CSMS) in industrial control systems (ICS). In the following sessions, a series of questions are suggested as a starting point for the implementation of a CSMS in a hydro power plant.

3.1. Initiate CSMS Program

It is necessary to develop a business plan, determine the desired scope and obtain support from the organization. Suggested concerns:

- What is the expected result taking into consideration that a CSMS does not generate ROI (return of investment)?
- Are there financial resources in short term to enable the application of resulting countermeasures?
- Are there financial resources available in short, medium, and long term for the maintenance of the CSMS?
- Are there specialists available for each HPP system that can participate in the detailed risk assessment?
- Is it possible to initiate the CSMS only by reallocation of personnel activities or is it necessary to contract new personnel?
- Will the program be applied only by internal efforts, or will there be third-part suppliers?
- Will the CSMS be developed for a single HPP or for a group of them? Will reference automation architecture be developed?
- What is the timeline expectation? Is it feasible?

3.2. High Level Risk Assessment

The high-level risk assessment should be performed to indicate priorities and support the strategy definition regarding personnel and financial resources. Suggested concerns:

- Which HPP's systems can cause personnel injury in case of inadequate operation?
- Which HPP's systems can cause environmental damage in case of inadequate operation?
- Which HPP's systems can cause equipment damage in case of inadequate operation?
- What is the impact on company's reputation due to a well succeeded cyberattack?
- What is the financial and social impact if one or more generator unities stop working due to a successful cyber attack?
- What is the actual and pretended risk tolerance?
- How is the IT × OT integration? Which team acts in case of incidents?
- What does the governments agents require regarding cyber security in critical infrastructures?

3.3. Detailed Risk Assessment

The detailed risk assessment should be performed in accordance with the priorities and resources defined in the high-level risk assessment. It is important to determine a methodology and apply it for the specified systems. Suggested concerns:

- Is there an incident database to guide systems prioritization?
- Is there a safety risk analysis that can be adapted to a security risk analysis?
- How many defence layers will be applied for priority systems?
- What is the impact of the countermeasures on the systems?

3.4. Establish Policies, Procedures and Awareness

It is necessary to create policies, procedures, and awareness trainings that mitigate the risks evaluated. Suggested concerns:

- What kind of trainings will be created: theoretical, practical or both?
- Which personnel should be involved: IT, OT, or both? From which specialty?
- Will an external company be hired for specific trainings?
- Will there be mandatory trainings? What will be the frequency?
- How will be the means of divulgation of the new policies and procedures inside the HPP?
- How will the integration between IT and OT departments be approached in the policies, procedures, and awareness program?
- What will be the frequency of policies and procedures revision?
- Will there be mandatory policies and procedures?

3.5. Select and Implement Countermeasures

Once the risk tolerance, priorities, probabilities, and severities are known, they must be carefully evaluated for the selection of the most adequate countermeasures, and it is important to take into consideration the concept of defence in depth for the countermeasure's definition. Suggested concerns:

- Will it be given emphasis for internal or externa attacks for the HPP under consideration (intentional or unintentional)?
- Can the selected countermeasures be implemented in a single step or is it necessary to divide the implementation in more steps due to financial restrictions?
- Recent cyber attack cases in similar plants occurred due to what kind of lack of security?
- What are the existing safeguards for the worst-case consequences? Is it possible to improve by applying more defence layers?

3.6. Maintain the CSMS

As can be observed in Figure 1, the activity of maintaining the CSMS can go back to any other activity, highlighting the cyclic nature of security management. It is necessary to monitor the CSMS results and the real adherence to the policies and procedures, check changes in government regulations, look for best practices continuously, and revise the activities according to lessons learned during the implementation and maintenance of the program.

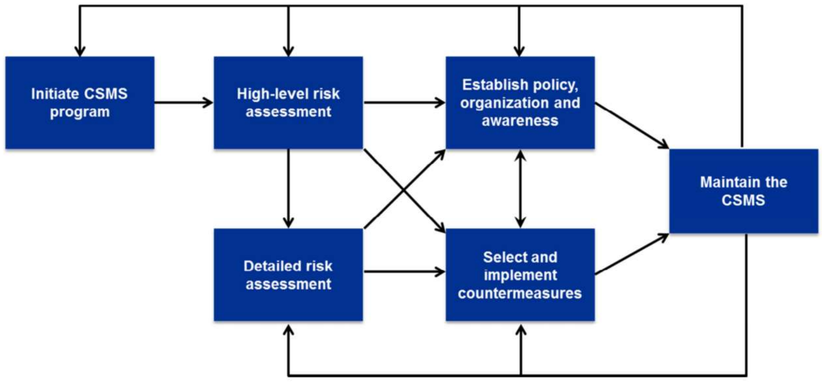
Initiate CSMS program
High-level risk assessment
Establish policy, organization and awareness
Maintain the CSMS
Detailed risk assessment
Select and implement countermeasures

Figure 1. Top level activities for establishing a CSMS [12].

4. Study Case for a Typical HPP

4.1. Methodology and Contextualization

As detailed in the Section 2.3, ref. [15] proposed a generic method to turn a HAZOP into a cyber-HAZOP risk analysis by selecting hackable scenarios. In this paper, some basic concepts involving hydro power plants systems and CSMS were introduced to contextualize the theorical application of this method based on a real HPP with two Pelton generator unities that produce approximately 300 MW.

Some simple modifications were applied to the automation architecture shown in Figure 2 in order to represent a more typical solution of distributed automation and control system.

The devices are based on Siemens solutions, where the main controllers are from S7 400 family configured with hot stand-by redundancy. The field I/O devices are based on ET 200M and ET 200S solutions, and subsystems have S7 300 as the controller. The protection system is based on SIPROTEC equipment.

It is a client/server architecture where the operation network contains a historian, two operation stations, and tow engineering stations all communicating through proprietary protocol. The process network has double ring topology and optical fiber as physical mean for proprietary and non-proprietary communication protocols. The systems connected to the process network are: generator units, auxiliary systems (mechanical and electrical), and substation and electrical protection communicating through IEC 61850 protocol. Lastly, the field network is based on RS 485 as physical mean and Profibus DP as communication protocol. Moreover, there are two external connections: one with the office network and a gateway for the connection with the government regulation agent.

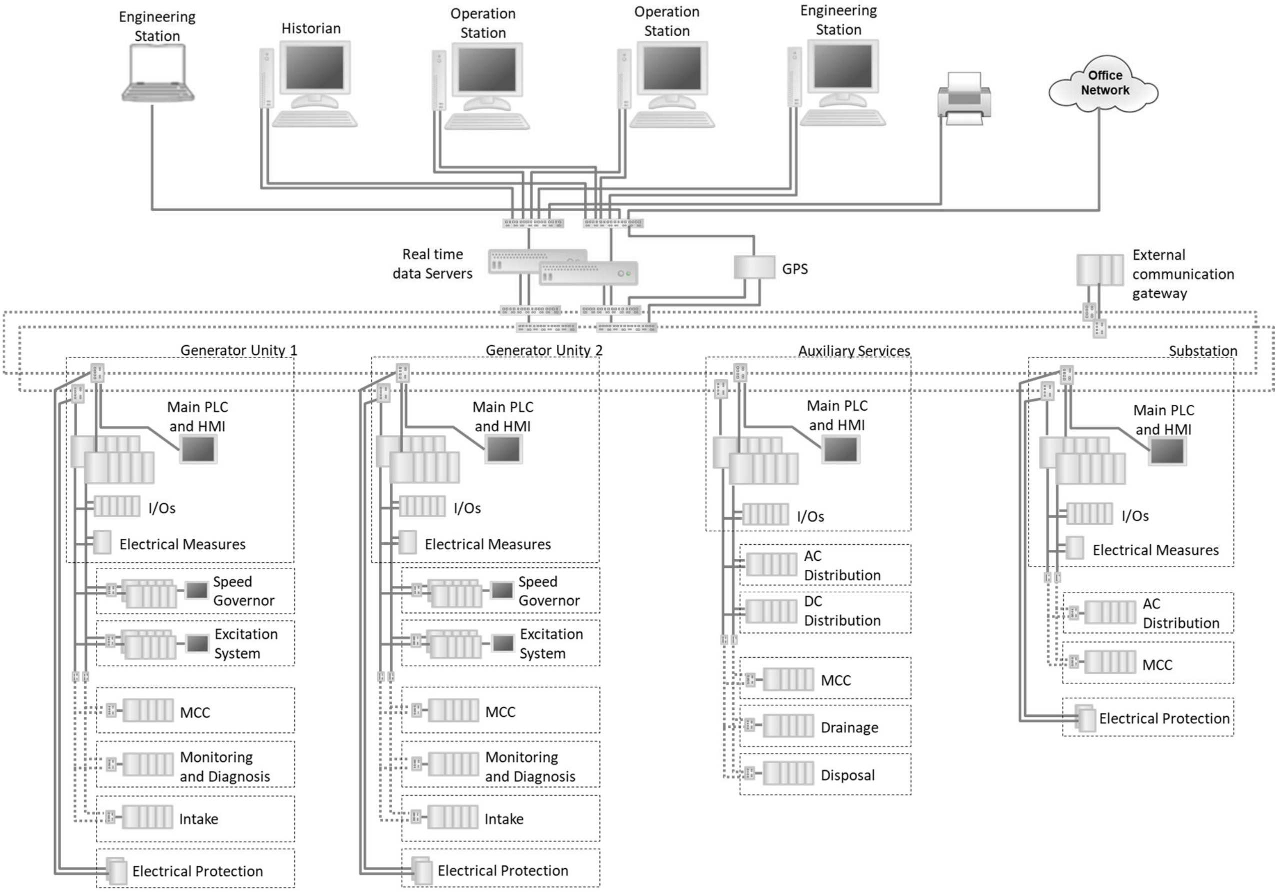

Figure 2. Study case automation architecture based on real HPP with two generator units.

4.2. Initiate CSMS Program

The company assumed that cyber security should be considered in all levels with a top-down strategy. Table 4 shows the topics selected and the decisions made regarding each one.

Table 4. Company decisions to initiate the CSMS.

Topic	Decision
Business plan	Enough investment for a dedicated team and for the implementation of a CSMS in this pilot plant.
CSMS scope	Complete automation architecture with selection of priority countermeasures according to the established risk tolerance and detailed risk analysis to be performed.
Stakeholders	Head office of the electrical company, regional unities, services, and product providers.
Organization support	Full support of all organization, given that cyber security has become a priority in the company's strategy.

Given that the business plan allows a dedicated team, the following departments are considered:

- Electrical maintenance and operation;
- Mechanical maintenance and operation;
- Electrical engineering;
- Mechanical engineering;
- Automation engineering;
- Information technology;

4.3. High Level Risk Assessment

Given the period of this study, the high frequency of ransomware attacks led to the conclusion that they have medium probability of occurrence in the supervisory system and should be considered in the program. Besides, there is also a medium probability of non-authorized remote access focusing on turning down the HPP more than aiming to destroy it, once it would require a deeper knowledge of the systems and existing solutions in the HPP.

Regarding regulations, although, in some countries, there is no mandatory government regulation on cyber security for critical infrastructures, the loss of revenue due to a non-operating unity generator, costs to restore the system, or possible taxes due to non-availability justify the investment in more defence layers. Given this context, the company also changed its risk tolerance from high to medium.

4.4. Detailed Risk Assessment

The following premises were adopted:

- Plant personnel would not attack or pass information to outside attackers intentionally because besides it is easier to detect, and, in the case of a dangerous incident, they would be exposed to possible injuries, so it is assumed that the leak of internal information is due to social engineering, reinforcing the need of trainings and awareness.
- Differently from process data that contains industrial secrets, it is assumed that data from a HPP is not the focus, reducing the need of defence layers related to data itself. Before applying solutions such as deep packet inspection (DPI), other defence layers would be priority.
- Taking the previous premises into consideration, it is presumed that the focus of a cyber attack on a HPP is to take control of the substation and/or generator unities to turn the system down, in other words, it is assumed that it would be an attack more similar to Blackenergy than to Stuxnet.

This plant already had a HAZOP analysis available, so it was decided to turn it into a cyber-HAZOP by filtering the hackable scenarios.

Table 5 exemplifies cases of the excitation system for two parameters: isolation and control system. If the isolation is inadequate and this event is not alarmed in the SCADA, the machine can be damaged. This is a hackable scenario because a cyber-attack can block alarms to the SCADA letting the excitation system under risk. The complete analysis can be found on [17].

Table 5. Company decisions to initiate the CSMS.

Subsystem	Guideword	Param.	Deviation	Possible Causes	Conseq.	P	S	R	Existing Safeguards
Excitation system	No/Low	Isolation	Low or inexistent isolation	Dust on the generator brushes. Damage in the internal equipment of the excitation system that are connected to the power electronics circuits.	Unity stops	0.1	5.0	0.5	SCADA alarm. Protection relay 64R
Excitation system	No	Control System	Control system out of work	CLP damage. Cabling failure. Failure on the 125Vcc powering system	Unity stops	0.1	3.0	0.3	Control system redundancy

4.5. Establish Policies, Procedures and Awareness

The IEC 62443 standard does not specify trainings frequency, so the suggestions are open to adaptations according to each plant needs and level of knowledge of personnel.

4.5.1. Awareness Trainings

Table 6 shows the trainings content that HPPs personnel must attend with 3 h of duration each 12 months.

Table 6. Training's content.

Topic	Content
Risks, threats and vulnerabilities	Conceptual definitions and approach of risks associated to the HPP's cyber assets.
Risk analysis	Conceptual definitions of the risk analysis utilized in the HPP (cyberHAZOP) to prepare the team for continuous documentation revision.
Standards	General view of the main international standards used as base for the HPP's policies: NERC CIP, IEC 62443 and NIST 800-82.
Social Engineering	Focus on behaviour issues exemplifying well succeeded social engineering attacks to promote awareness and improve the level of responsibility when dealing with internal data

4.5.2. Policies and Procedures

Once the HPP may have legacy systems, the policies and procedures are mandatory for all applicable systems. Table 7 shows the contents for each topic.

4.6. Select and Implement Countermeasures

Given that the cyber-HAZOP did not result in high-risk scenarios, the medium risk cases were filtered and commented with recommendations:

Discharge channel: The discharge channel level is measured through a sensor. If the level is very high, it can lower the turbine efficiency, damage it, and, in the worst case, inundate the powerhouse. Once this sensor can be physically targeted to send a wrong value to the system, it is recommended to be installed in a restricted area under access control.

Stator: if an overvoltage occurs and is not detected, the isolation system can be damaged. Besides project considerations that take this risk into consideration, some devices are also responsible to detect this situation: excitation digital control and protection relay, so it is recommended to control physical and configuration access to these assets.

Table 7. Policies and procedures content.

Topic	Content
Use of removable media	Policy describing allowed and forbidden attitudes and its respective procedures. If the utilization of removable media is absolutely necessary, before being connected to the system, it must be verified and sanitized
Backup	All applicable systems must have an associated document with the backup procedure, which must be conducted every three months or when some change is applied
Restore	The restore procedure must be tested every 12 months for all applicable systems. Examples: PLCs multi-project, servers' images, historian data, operation station images, devices configuration (e.g., firewall and protection relays), among others
Incidents	Incident report policy containing a procedure to be followed in case of compromised systems
Change	Change management policy with examples and templates to keep the documentation always in the last revision.
Inventory	Inventory policy containing a template document. The inventory procedure must be revised each 12 months or in case of change for both physical and cyber assets.
Patches	Patch management policy and related procedures focusing relevant systems to keep the plant safe. Only security patches should be applied for whatever system: Windows platforms, firmware, or automation software. The CSMS responsible must verify available patches every week and filter the applicable ones to include in the updates planning
Access control	Access control policy for both physical and cyber assets according to minimum privilege philosophy. Access levels must be documented with responsible names and the document must be revised every six months or in case of change
Logs	Policy describing which logs should be monitored for each system

Spherical valve: Inadequate pressure conditions during valve opening and closing can collapse the penstock. Theses sensors should be in a restricted area under access control with regards to the speed governor controller to avoid wrong configurations and commands.

Hydraulic governor: High pressure can cause pipes rupture. In addition to the existing SCADA alarm, the pressure sensor should be in a restrict area under access control.

Speed governor: If the PLC is unavailable or if there are failures for sending and receiving data, the unity must be stopped. A common safeguard is the system redundancy, but it is also recommended to control physical, configuration, and command access to this asset.

Electrical protection system: If there is a problem with input data, unknown devices status requires stopping the system, and the non-actuation of electrical protection can cause serious damages. It is recommended to apply many defence layer restriction for physical and configuration access, separate network, and constant security firmware updates.

Supervisory and control system: If this system is unavailable or if there are failures for sending and receiving data, the HPP must be stopped. It is recommended to control physical and configuration/operation access, follow the policies and procedures, and update Windows security patches and antivirus signatures.

Open cooling system: If the cooling system presents low flow or pressure, the circuit temperature can increase and/or the supply of services water can decrease. These sensors should be in a restricted area under access control.

Drainage: The HPPs drainage is performed through pumps whose commands are from a PLC or local operation. If this system does not work when needed, the powerhouse can inundate, so it is recommended to control physical, configuration, and command access to this system.

Services water: If there is no services water flow, many systems are affected, justifying restricting physical and operation access to this system.

Ventilation: If there is no ventilation flow, it is impossible to regulate the environment temperature and air quality, which can inhibit the permanency of the operators inside the powerhouse. It is recommended to control physical and command access to these assets.

As can be observed in the medium risk cases, most risks can be mitigated through physical access control, minimum privilege philosophy for configuration and operation, security patch updates, security firmware updates, antivirus, trainings, and personnel awareness.

Regarding the automation architecture, the following measures are suggested:

- Division into security cells protected through firewall to control activities that occur within and between then.
- Inclusion of a server with security functionalities: antivirus and Windows patches.
- Inclusion of a centralized log management system.
- Configuration of a DMZ (demilitarized zone) to limit data flow from process to office network containing the historian server, antivirus, Windows patch update server, and log management server.

Cell 1 contains the operation and engineering stations, while Cell 2 contains the real time data servers. The process and operation networks are physically distinct and, by separating them into different security cells, it is necessary to configure firewall rules to be compliant with IEC 62443 requirements. As a result, the modular switches must provide technical features that enable security configurations, or the PCs must have embedded security options such as firewall and VPN.

The communication gateway with the Operation Centre or Government Agent is extremely relevant, and it is an external connection. To be IEC 62443-compliant, another DMZ should be configured, but given that it involves a government agent and some countries still do not have a national mandatory standard, it is considered in Cell 3 without DMZ characteristics, but configured according to the government agent rules requirements.

As cited in the high-level risk assessment, it is admitted that external ransomware attacks and non-authorized remote access probability is higher than intentional internal attacks probability. For this reason, all systems connected to the process network (generator unities, auxiliary services, and substation) are considered in Cell 4.

In addition to the modifications suggested for the automation architecture, in order to keep a minimum security level, it is suggested to develop check lists for the six groups of devices configuration stated in Table 2:

- Supervisory system;
- Communication link with operation centre or regulation agent;
- Communication between process data and office network;
- Network equipment;
- Electrical protection system;
- Controllers.

The check lists should approach measures to mitigate identified vulnerabilities. Although Table 8 refers only to controllers, similar check lists should be developed for the other devices groups, taking into consideration Table 3 contents regarding common ICS vulnerabilities.

It can be said that the architecture suggest in Figure 3 is an intermediate solution. The architecture division into security cells can follow many criteria, and it impacts the amount and costs of security devices, and there must be at least one firewall for each cell. Figure 4 is an example of a lower level of security with only two security cells and a DMZ, while Figure 5 considers seven security cells and a DMZ.

Table 8. Controllers check list.

Controllers				
Item	**Description**	**Yes**	**No**	**Comments**
1	Physical security: allocation of controllers inside cabinets with access control			
2	Hardening: disable non-utilized functionalities			
3	Hardening: disable logical and physical (USB and others) nonutilized ports.			
4	Firmware: guarantee that the device is running with the last homologated firmware version			
5	Configuration: keep the controllers configuration tool with physical access control and restrict users able to change configurations			

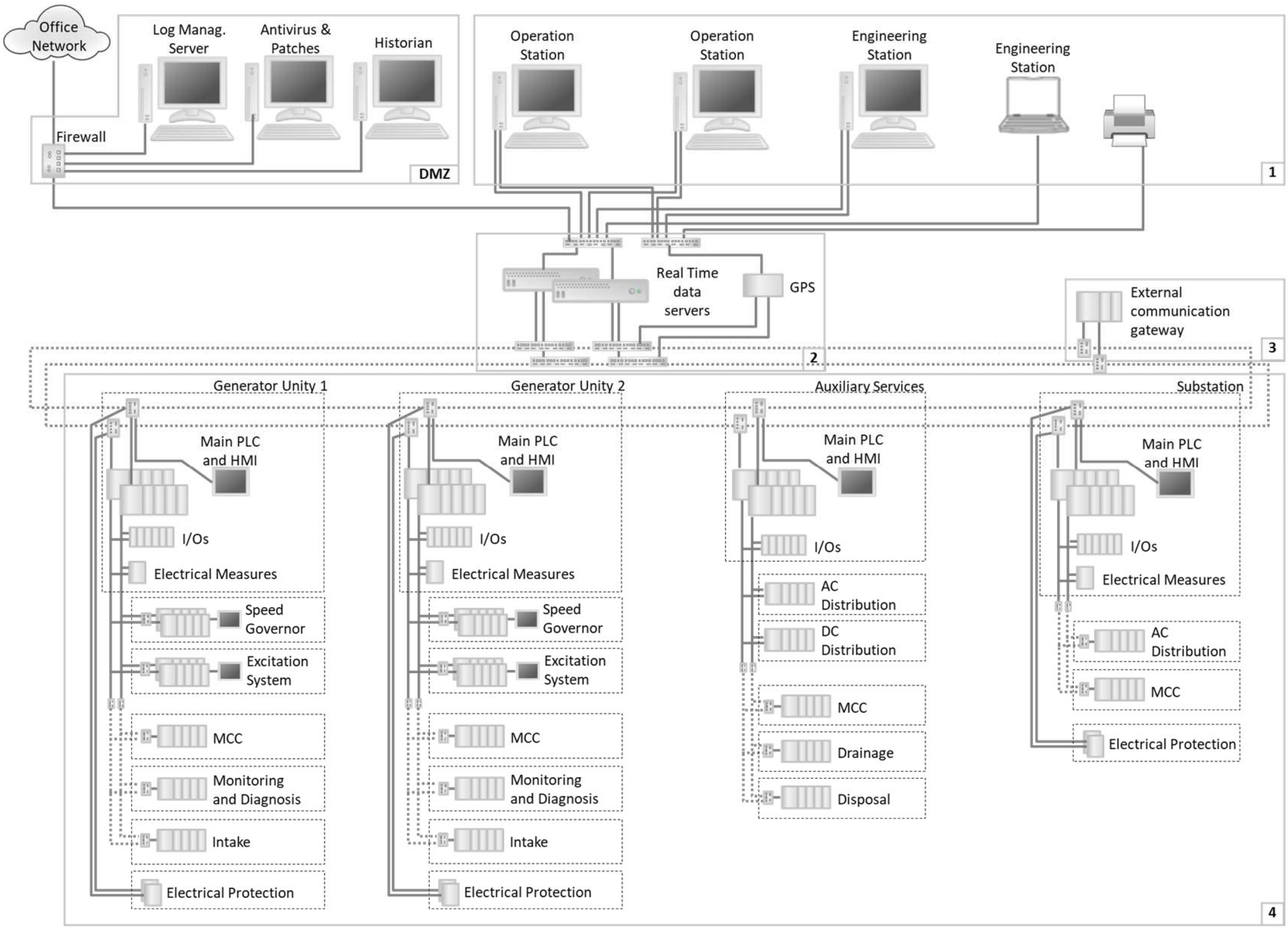

Figure 3. Architecture containing a DMZ and four security cells.

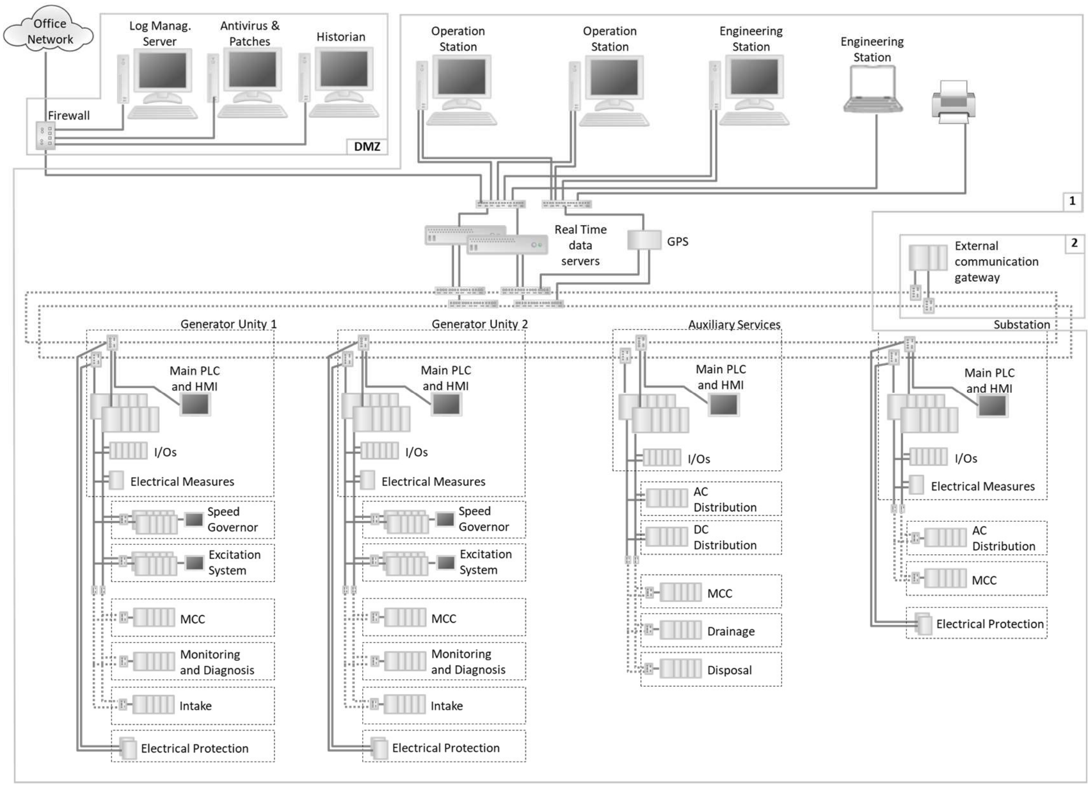

Figure 4. Architecture containing a DMZ and two security cells.

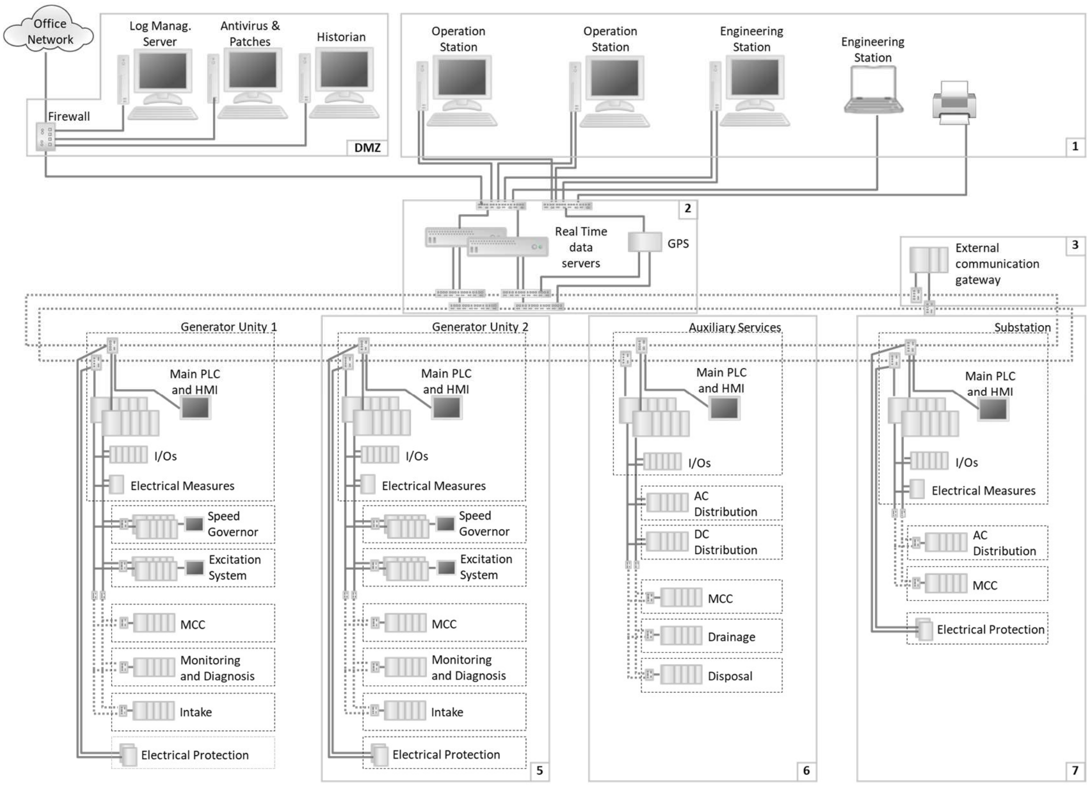

Figure 5. Architecture containing a DMZ and seven security cells.

5. Conclusions and Future Work

This study proposes the application of IEC 62443 concepts for hydro electrical power plants. As discussed in the literature review session, it adds value to the energy market given the gap for more domain/actor-based studies, and, in this case, the contribution is focused on hydropower owners and network operations. It is expected that the methodology developed in this paper can contribute to a better understanding of how to start a security management program, what are the implications of the chosen risk tolerance, and how it may change technical solutions and network equipment and configuration.

Before analysing the study case, common ICS vulnerabilities were considered in groups of devices according to a typical modus operandi of suppliers in an HPP automation project. To illustrate the application guide, a theoretical study case based on a real HPP was developed, and some premises were adopted to develop the CSMS. Once the HPP had a HAZOP risk analysis available, it was filtered for hackable cases exemplifying how to transform a safety risk analysis into a security risk analysis: cyber-HAZOP.

The medium risk cases were detailed, showing that most of them can be mitigated through physical access control, minimum privilege philosophy for configuration and operation access, security patch updates, security firmware updates, antivirus, trainings, and personnel awareness.

Regarding the automation architecture, it was suggested to implement a DMZ and divide the devices into four security cells. The DMZ was considered with the historian and servers for antivirus, Windows security patches, and log management. The external communication gateway was not considered in a DMZ because it would involve the government agent and, in many countries, there are no mandatory regulations regarding cyber security in critical infrastructures.

To exemplify other solutions, two more architectures were designed considering lower and higher risk tolerances. The lower the risk tolerance, more security cells should be implemented, thus increasing the solution costs and maintenance efforts.

Future studies on the energy generation domain could further investigate the cost—benefit relation resulting of the risk tolerance that each company is committed and how it impacts the cyber risks countermeasures implementation. For example, some mitigations from the literature review, such as IDS (intrusion detection system), blockchain, 5G, and AI (artificial intelligence) were not considered in this study due to the high implementation cost. Besides, limited budgets are common in smaller power plants, and more relevant plants may have a different scenario, being able to apply more security layers and invest in more expensive solutions. Furthermore, the literature review also shows little research on real case applications, where the results could be evaluated and improved according to this or other methodologies, deepening the analysis of different technical solutions and their efficacy to meet the challenge that the energy sector faces regarding cyber security.

Author Contributions: Writing and editing, J.B.H.; supervision, R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The only external data source is the HAZOP safety assessment, which was obtained from 3rd party for study purposes and restrictions apply to these data, which is not publicly available.

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

References

1. Gopstein, A.; Nguyen, C.; O'Fallon, C.; Hastings, N.; Wollman, D.A. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0, Special Publication (NIST SP)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. Available online: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-206.pdf (accessed on 27 December 2022).
2. Jahil, A.A.A.; Giarratano, D. *Improvement of Cyber-Security Measures in National Grid SA Substation Process Control*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2017.
3. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. *Cyber Security in Smart Grid: Challenges and Solutions*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019; pp. 546–551.

4. Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solution—A Review. *Sustainability* **2022**, *14*, 14226. [CrossRef]
5. Backes, M.; Keefe, K.; Valdes, A. *A Microgrid Ontology for the Analysis of Cyber-Physical Security*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2017.
6. Ang, C.K.G.; Utomo, N.P. *Cyber Security in the Energy World*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2017; pp. 1–5.
7. Buyuk, O.O.; Camurcu, A.Y. *A Novel Actual Time Cyber Security Approach to Smart Grids*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2018.
8. Chobanov, V.; Doychev, I. Cyber Security impact on energy systems. In Proceedings of the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 9–11 June 2022; pp. 1–5.
9. Liu, Y.; Qin, H.; Chen, Z.; Shi, C.; Zhang, R.; Chen, W. *Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019; pp. 25–30.
10. Chen, Y.C.; Mooney, V.; Grijalva, S. *Grid Cyber-Security Strategy in An Attacker-Defender Model*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020.
11. Chen, Y.; Li, J.; Lu, Q.; Lin, H.; Xia, Y.; Li, F. Cyber security for multi-station integrated smart energy stations: Architecture and solutions. *Energies* **2021**, *14*, 4287. [CrossRef]
12. *IEC 62443-2-1*; Industrial Communication Networks–Network and System Security—Part 2-1: Establishing an Industrial Automation and Control System Security Program. IEC: Geneva, Switzerland, 2010.
13. *IEC 62443-1-1*; Industrial Communication Networks–Network and System Security—Part 1-1: Terminology, Concepts and Models. IEC: Geneva, Switzerland, 2009.
14. Nolan, D.P. *Safety and Security Review for the Process Industries–Application of HAZOP, PHA, What-If and SVA Reviews*; Elsevier: Amsterdam, The Netherlands, 2014.
15. Marszal, E. Security process hazard analysis review. *ISA InTech Mag.* **2016**. Available online: https://www.isa.org/intech-home/2016/march-april/features/security-process-hazard-analysis-review (accessed on 24 November 2022).
16. Knapp, E.D.; Langill, J.T. *Industrial Network Security–Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*; Syngress: Rockland, MA, USA, 2015.
17. Heluany, J.B. Application of Cyber Security Standards in HPPs. Master's Thesis, University of São Paulo, São Paulo, Brazil, 2018.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.