applied sciences

MDPI

Article

An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System

Halima Ibrahim Kure [1,*], Shareeful Islam [1,*] and Mohammad Abdur Razzaque [2]

[1] School of Architecture, Computing and Engineering, University of East London, London E16 2RD, UK
[2] School of Computing, Media and Arts, Teesside University, Middleborough TS1 3BX, UK; m.razzaque@tees.ac.uk
* Correspondence: h.kure@uel.ac.uk (H.I.K.); shareeful@uel.ac.uk (S.I.); Tel.: +44-208-223-7273 (H.I.K. & S.I.)

Received: 30 March 2018; Accepted: 16 May 2018; Published: 30 May 2018

Abstract: A cyber-physical system (CPS) is a combination of physical system components with cyber capabilities that have a very tight interconnectivity. CPS is a widely used technology in many applications, including electric power systems, communications, and transportation, and healthcare systems. These are critical national infrastructures. Cybersecurity attack is one of the major threats for a CPS because of many reasons, including complexity and interdependencies among various system components, integration of communication, computing, and control technology. Cybersecurity attacks may lead to various risks affecting the critical infrastructure business continuity, including degradation of production and performance, unavailability of critical services, and violation of the regulation. Managing cybersecurity risks is very important to protect CPS. However, risk management is challenging due to the inherent complex and evolving nature of the CPS system and recent attack trends. This paper presents an integrated cybersecurity risk management framework to assess and manage the risks in a proactive manner. Our work follows the existing risk management practice and standard and considers risks from the stakeholder model, cyber, and physical system components along with their dependencies. The approach enables identification of critical CPS assets and assesses the impact of vulnerabilities that affect the assets. It also presents a cybersecurity attack scenario that incorporates a cascading effect of threats and vulnerabilities to the assets. The attack model helps to determine the appropriate risk levels and their corresponding mitigation process. We present a power grid system to illustrate the applicability of our work. The result suggests that risk in a CPS of a critical infrastructure depends mainly on cyber-physical attack scenarios and the context of the organization. The involved risks in the studied context are both from the technical and nontechnical aspects of the CPS.

Keywords: cybersecurity; risk management; cyber-physical systems; cybersecurity attack scenario; supervisory control and data acquisition (SCADA) systems; cascading effect

1. Introduction

Generally, cyber-physical systems are real-time and robust independent systems with high performances requirements [1]. They are used in many application domains, including critical infrastructures, such as the national power grid, transportation, medical, and defense. These applications require the attainment of stability, performance, reliability, efficiency, and robustness, which require tight integration of computing, communication, and control technological systems [2]. CPSs of critical infrastructures have always been the target of criminals and are affected by security threats [3] because of their complexity and cyber-physical connectivity. These CPSs face security breaches when people, processes, technology, or other components are being attacked or risk management systems are missing, inadequate, or fail in any way. The attackers target confidential

data, such as customer information or other valuable records [4]. It is likely that the threats of CPSs will only increase in the future as the use of these systems become widespread. However, there are sensible safety measures that organizations can consider to minimize losses from their destruction. It is possible to control damages and recover from an attack and its consequences with the appropriate insight through research and a domain expert's assistance [5]. Managing CPS security risk is not about eliminating all risks; it is about determining and understanding the risk rating of events and putting the right processes or controls in place to manage them in accordance with the organization's risk tolerance level. Risk management is a continuous process, not a one-time event [3]. In response to an event(s), there is an urgent need for organizations to truly understand their cyber-physical security status and employ the necessary and urgent corrective actions to rectify weaknesses [6].

Risk can be defined as an uncertain event that may occur due to a system malfunction or failure that could harm assets, such as human beings or the environment, and also influence the organization's achievement on strategic, operational, and financial objectives [7]. Risk management is a key discipline for making effective decisions and communicating the results within organizations. It proactively identifies potential managerial and technical problems so that appropriate actions can be taken to reduce or eliminate the probability and/or impact of these problems [8]. There are many existing risk management methods for CPSs [9–12] However risk management in CPSs is challenging because of the increased complexity of the systems, the evolution of risk levels, human factor threats comprising of unintentional breaches of security, the unsuspicious use of infected information media giving away sensitive information, and lack of awareness and human errors [13]. In addition, cascading failures occur because of interdependencies among components and infrastructures. Importantly, threats affecting one part of a CPS can propagate to other parts through the network, which interconnects different parts of the CPS and affects other parts. As security threats grow, the organization needs a comprehensive cybersecurity risk management system to identify unique cybersecurity threats and their trends. The authors of a previous paper [14] discussed the challenges for securing CPS and analyzed security mechanisms for prevention, detection and recovery, resilience, and deterrence of attacks for securing CPS. A previous work [15] proposed a layered approach for evaluating risk based on security to prevent, mitigate, and tolerate attacks both on physical power applications and cyber infrastructures. The paper identifies the importance of combining both power application security and supporting infrastructure security into the risk assessment process and provides a methodology for impact evaluation. Also, another paper Ref. [11] provides an overview of a number of important real-life issues of cybersecurity and risk assessment for supervisory control and data acquisition (SCADA) and distributed control systems (DCS). The paper discussed the various compromise graphs and augmented vulnerability trees that quantitatively determine the probability of an attack, impact of the attack, and the reduction in risk as a result of a particular countermeasure. All these works, and more, are presented in the related work section emphasize: the importance of cybersecurity risks management for CPSs. However, comprehensive and integrated risk management practice is not sufficiently addressed in these works.

The novel contributions of this paper are: (i) A comprehensive integrated cybersecurity risk management framework that explicitly considers risk from a holistic perspective of the stakeholder model, cross functions risks, and existing risk management frameworks; (ii) the integration of the cascading effect from interdependent CPS components considering vulnerability, threats, and risks to an asset; and (iii) an evaluation of the proposed integrated risk management approach into a real cyber physical system. The result from this case study outlines the applicability of the proposed approach. We also compared the identified results with the existing results to demonstrate the impact of integrated risk management as approach to the CPS.

The remainder of the paper is structured as follows. Section 2 outlines state-of-the-art cyber security risk management practices for the cyber physical system and existing framework and standards. Section 3 provides the rationale for the integrated risk management approach. Section 4 presents the proposed cyber security risks management framework including the concepts and

algorithms. Section 5 demonstrates the evaluation results of the implementation of the proposed approach into a real smart grid system. This section also discusses of the various parts of the approach and compares it with other works. Section 6 provides the validity of the study, and finally Section 7 concludes the work and presents a few directions for future work.

2. Related Work

Cybersecurity risk management in CPSs is a very active research area, and a significant number of research works have been published in this area. We divided these works into three categories: (1) security risks management methods for CPS; (2) cyber security in smart grid; and (3) security risk management frameworks/standards/guidelines and presented the summary in the following.

2.1. Security Risks Management for Cyber-Physical System

A Risk Breakdown Structure (RBS) approach was proposed for managing the risks of CPS as previously described [16]. Countermeasures were proposed on the basis of the risk matrix method and classified. Risk values were introduced in an information security management system (ISMS) and quantitative evaluation was conducted for detailed risk assessment. The quantitative evaluation showed that the proposed countermeasures could reduce risk to some extent. Investigation into the cost-effectiveness of the proposed countermeasures is an important future work. Cherdantseva et al. [9] reviewed the state-of-the-art practices in cybersecurity risk assessment of the SCADA systems using aim, application domain, stages of risk management, risk management concepts, impact measurement, and sources of probabilistic data, evaluation, and tool support. Despite a large number of risk assessment methods for SCADA systems, the need for a comprehensive method that would cover all stages of risk management process is missing. The authors of a previous paper [10] proposed a new approach for assessing the organization's vulnerability to information-security breaches using the threat-impact index and cyber-vulnerability indexes based on vulnerability trees. This helps managers determine the current level of security and helps them select security mechanisms. However, probability added to each damage category would help to further quantify the risk associated with information systems. Hahn et al. [11] provided an overview of smart grid security, including the set of controls, communication, and physical system components required to provide an accurate cyber-physical environment. Several attack-impact evaluations were performed on the system such as availability and integrity attacks. There are other works that [12] focus on detecting computer attacks which change the behavior of the targeted control systems by understanding the consequences of the attack for risk assessment. Wu et al. [1] proposed a quantitative risk assessment model that focuses on the CPS running conditions and calculates risk in real-time using users' responses to risk at certain times. It provides users with attack information such as the type of attack, frequency, and target host ID and source host ID. Ten et al. proposed a cyber-security framework of the SCADA system as a critical infrastructure using real-time monitoring, anomaly detection, and impact analysis with an attack tree-based methodology, and mitigation strategies [17].

2.2. Cyber Security in Smart Grid

There are other works that focus on the security of smart grid. For instance Gai et al. [18] proposed an attack strategy approach using spoofing and jamming in order to interfere with the maximum number of signal channels. The approach used distributed power usage on both spoofing and jamming attacks by applying dynamic programming and was evaluated by subsequent experiments. However, this approach is most applicable to the power grid infrastructure. The authors of a previous paper Ref. [19] proposed a dynamic energy-aware cloudlet-based mobile cloud computing model (DECM) that focuses on solving additional energy consumptions during wireless communication in a power grid environment. The approach contributed to solving energy wastage problems within a dynamic networking environment, however, the applicability of the model needs to be tested in multiple industries with other service requirements. A fully homomorphic encryption for blend

operations (FHE-BO) model was proposed Ref. [20] which focuses on calculating encrypted real numbers. The encryption-decryption approach successfully acquired correct outputs from decrypting cypher-results of blend operations. The authors of a previous paper Ref. [19,21] discussed different unified approaches for security risk management in the context of the smart power grid. Risk assessment methodologies proposed included threat and vulnerability modeling schemes which help in identifying and categorizing threats, analyzing their impacts, and prioritizing them. A previous work Ref. [22] surveys the risk assessment methods, major challenges, and controls for various aspects of the smart grid such as SCADA systems and communication networks, in order to address the challenges facing the smart grid technologies. However, smart grids, as a provider, require a comprehensive cyber security solution by supporting stakeholders and assessing vulnerabilities and cyber threats and integrating systems to provide guidelines for effective risk management. The authors of Ref. [23] discussed the risk of cyber-attack on smart metering systems by applying methods and concepts from cyber-attack scenarios in a smart grid system.

2.3. Frameworks/Standards/Guidelines

There are widely accepted risk management standards such as ISO 31000 that provide guidelines for risk management activities which also consider risk management as an integral part of the overall organizational processes, including strategic planning and management processes [24]. IEC 31010 is also another recognized risk management method and technique [25]. The NIST framework focuses on managing cyber-security risk and NERC CIP standards for the identification and protection of critical cyber assets that support the reliable operation of the electric power grid. The NIST framework [26] is a risk-based approach for managing cyber-security risk. It is applied to deliver a complete platform that identifies relevant paths, providing guidance that ranges from requirements to implementation. Critical infrastructure organization can use the NIST framework alongside their existing frameworks to systematically identify, manage, and assess cybersecurity risk. It can serve as the basis for a new cybersecurity program or a mechanism for improving its existing programs. The outcome of the framework will serve as the basis for the on-going operation of the system, which includes reassessment to verify that the cybersecurity requirements are fulfilled [27]. A particular goal driven risk management approach [28,29] emphasizes the identification of goals as objectives specific to the organization mission. Risks are considered as an obstruction to the goal so that identified risks are assessed based on which goals they oppose. The approach is applied in various domains such as software development project and cloud computing.

Several observations were made from reviewing the existing works.

- Cherdantseva et al. [9] reviewed existing cyber security risk assessment works and concluded that it is necessary to have a comprehensive risk management method which will cover all stages of the risk management process.
- Different risk management approaches for smart grid were also discussed in a previous work [21]. However, risk management from a holistic perspective that incorporates all aspects of a smart grid and their interdependencies is needed.
- Most of the risk management approaches emphasize assessing vulnerabilities and identifying threats but lack emphasis on the cascading effect of vulnerabilities and threats to the asset.
- The existing works provide limited efforts in considering the estimation of an accurate risk level for the organization.

Our work intends to fill these gaps by proposing an integrated cyber-security risk management approach. The novelty of this work is a comprehensive cyber-security risk management framework that considers all phases of the risk management process. We follow the existing risk management standard and framework with a holistic view of the risks and propose our approach. In particular, the proposed work is initiated by understanding of the business context and current risk management status of the organization. The approach considers cascading vulnerabilities and threats to generate

a cyber-attack scenario and the impact of the risks are considered from the CPS organization's key performance indicators (KPIs) to generate the accurate risk levels.

3. The Rationale for an Integrated Risk Management Approach

An integrated risk management includes a combination of various components of a CPS which are interdependent and necessary for successful risk management. It needs to be a part of an organization's strategy in order to address the organization's risk management principles. Critical infrastructure organizations (i.e., health, financial, telecommunications, transportation, energy, and water) are always the targets for attackers and face different types of risks [30]. An integrated risk management scheme enforces a constant assessment of potential risks at every level in an organization and gathers the results at the corporate level to enable priority setting and minimize risk. The identification, assessment, and management of risks throughout the organization help to avoid greater risks and foster improvement of the organization. Traditional security risk assessment methods only address IT security risk or compliance risk. The integrated risk management framework will build a holistic solution considering the technical and nontechnical aspects of the organization. Figure 1 shows several areas that will incorporate into an integrated risk management approach. The main components of the integrated risk management framework are:

- Integration of stakeholder's model: The integration of the stakeholder's model for risk management is a means of achieving greater inclusivity in an organization, and it is important for an organization to understand its own security risk management practices. This approach shows the importance of security from each and every area of the business enterprise of a critical infrastructure organization by making it clear to managers and subsequently enhancing employee commitment. In a traditional security risk assessment having just one stakeholder, which could be the compliance manager or security director, the value of the security risk assessment process is limited. An integrated risk management approach seeks to relate vulnerability findings and IT control gaps in the context of how such findings may affect attackers, users, government, shareholders, regulatory authorities, numerous individuals, or groups across an organization. It also deals with the human issues for risk management.
- Measurement of cross-functional risks from organizational context: An effective risk management method renders a successful management of various factors that prevent organizations from achieving their desired security objectives. Risks depicted through an integrated risk management approach become cross-functional (i.e., a system whereby people from different areas of an organization work together as a team considering both technical and nontechnical perspectives), and the approach draws an obvious conclusion on how risks affect regulatory requirements, the supply management chain, and the goals or KPSs of the organization and its security objectives. The approach will provide a better understanding of cross-functional risks amongst control objectives that may have been impacted by technical or process-based vulnerabilities and will give attention to any higher risks. Cross-functional risks include technical risks and nontechnical risks such as software risk, system complexity and vulnerabilities, environmental risk, legal security, etc. As the approach captures different information from different stakeholders, security issues are shared across the organization and weighed appropriately in light of the management's level of criticality for each business and control function.
- Builds upon existing frameworks/standards/guidelines: An integrated risk management approach builds upon existing frameworks by evaluating how the combination of neglected risk factors could yield minor to terrible outcomes. A state-of-the-art and well-known approach can smoothly lead an organization beyond simple compliance and reveal how to more effectively secure a particular information environment. The approach understands regulatory requirements and can translate them into control objectives for the organization. The existing frameworks and standards that will be considered for the risk management process will include, the NIST framework, ISO 31000:2009, ISO 27001:2013, and goal-driven risk management framework which

will provide guidelines for risk management activities and also considers risk management as an important aspect of the overall organizational process [24,25,28,29].

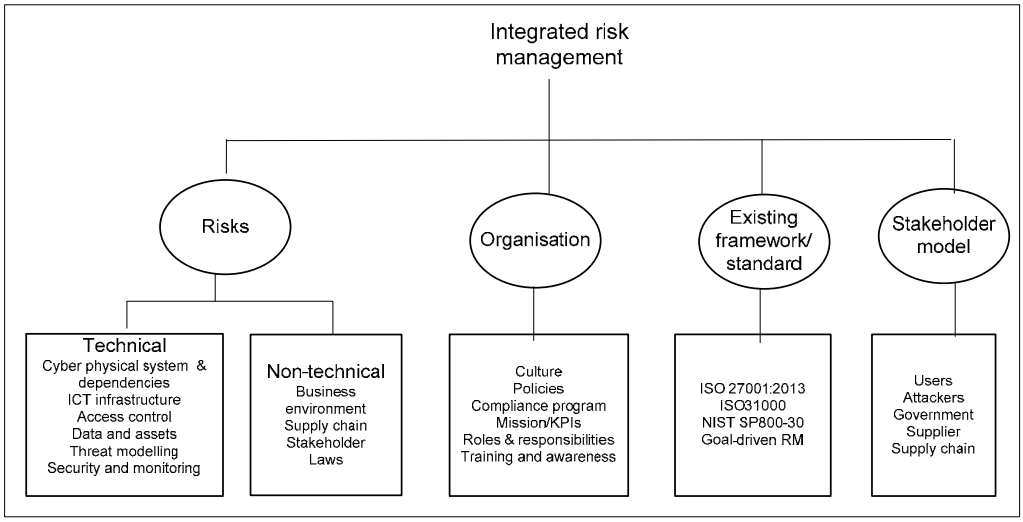

Figure 1. An integrated risk management approach.

4. An Integrated Risk Management Approach

The scope of the proposed integrated risk management approach is to understand, manage, monitor and communication of risks during operation in CPS for the benefit of a critical infrastructure organization. It includes many concepts that serve as a common language for describing the properties necessary for cybersecurity risk management. These concepts help us to systematically assess and manage risks proactively. In particular, we consider assets and their criticalities, relevant vulnerabilities and threats to model the cybersecurity attack scenario so that risk level can be quantified for the suitable countermeasure. This section presents an overview of the integrated risk management concepts of the proposed approach.

4.1. Modeling Concepts

The proposed approach includes a set of modeling concepts that are essential to understand, manage, and express cybersecurity risks. We have identified a few concepts necessary for the development of the cybersecurity risk management approach. Based on those concepts, an in-depth exploration of the numerous methods, tools, and techniques that can be used for a risk management approach in the CPS has been performed. An overview of the concepts used by the proposed approach is explained below:

- Actor: An actor is an entity, generally a human user, a system, an organization, or a process each with a specific strategic goal within its organizational setting and carries out specific activities to generate cybersecurity risk management actions or receive the generated cybersecurity risk management actions by another actor [31]. This requires the organization to appoint efficient actors to carry out various tasks to guide and lead in achieving its goals. The actors are identified as stakeholders, such as government employees, IT providers, and utilities, employees, consumers, owners and operators, customers, users, and providers with skills within a particular location.
- Goals: Goals signify the overall aims and objectives of an actor which supports the interest and continuity of the business. There are expectations to support the organization and include the KPIs of the organization, security, and organizational goals. KPIs allow the critical infrastructure organization actors to make a keen decision about the organization's continuity; they include confidentiality, availability, and integrity.

- Risks: Risk can be defined as the possibility of an unwanted outcome as a result of an incident, event, or occurrence, as determined by its likelihood and the associated consequences. The risk is inevitable in a business, however, it is the role of the actors to ensure that risks are kept to a minimum to achieve the goals. Once the risk has been identified, it is necessary to have a mitigation plan or any other solution to counterattack the risk. Risks are the potential consequences of the system and could possibly compromise the security of the CPS and not meet the actor's expectations. A CPS risk could be classified under security, operational, nontechnical, technical, and governance or regulatory parameters. These risks could obstruct the security of the CPS and require an appropriate assessment. The risk assessment will be based on likelihood, impact, and residual analysis, which helps in identifying which risk needs to be controlled by following different control strategies.
- Assets. Assets are defined as tangible or intangible entities which are necessary and have values to the CPS organization. Identification of key assets, and putting a value on each key asset, is an important process of risk management. These key assets could be people, services, facilities, processes, etc. It is important to identify critical assets as well as estimate their critical failure modes or impact of the loss. An asset has two features: (i) criticality and (ii) category. Criticality is defined as a measure of the consequences associated with the degradation or loss of an asset. It is the major indicator used by organizations to determine which asset is of more value to the business continuity. Category classifies assets according to its level of sensitivity and security requirements. The criticality of an asset category can be high, medium, or low, which means that assets with high rating are the most valuable to the organization.
- Controls. The set of security protections or countermeasures to avoid or minimize security risks in CPS critical infrastructure are called controls. Controls are also the mechanism used to provide security to the CPS, and they are characterized by combining technical and nontechnical controls which are used to deter anticipated and unanticipated threats from exploiting known vulnerabilities. They also describe the vital components and actions taken to protect the assets. The overall goal of risk assessment will be partly defeated if relevant controls are not applied.
- Compliance Programs: These are sets of requirements designed to secure the CPS to operate without any form of disturbance. Critical infrastructures are increasingly using compliance programs as a mechanism for demonstrating cybersecurity for CPS protection. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a compliance program designed to secure the assets necessary for operating a bulk electric system. In this case, the SCADA system of the CPS is an asset. Therefore, a significant sum of their budget and time is necessary to ensure security compliance with standards such as NERC CIP, NIST, NIPP, and other relevant standards.
- Cyber-attack scenario: A cyber-attack scenario is an event that leads to a negative impact on the organization's assets when it occurs. There are some certain components that determine a cyber-attack on a CPS. They include threat types, actor's skill, capability and location, assets, events, and time. With certain scenarios, the organization tends to think broadly by developing a range of possible outcomes to increase their readiness for a range of possibilities in the future.
- Policy: Policies are the principles of action adopted or proposed by an organization. There are a number of security policies, such as access control and backup that are necessary to formulate and implement the CPS security program.
- Threats and vulnerabilities: Vulnerability is the weakness in an organization security program that is exploited by a threat to gain unauthorized access to an asset. It has three properties. i.e., impact, type, and weight score.

The Metamodel illustrated in Figure 2 above shows the relationship between the concepts. The actor is represented as having an interest in SCADA system services offered by the CPS. The actor introduces security goals such as confidentiality, integrity, and availability, and organizational goals

such as business continuity and reputation of the organization and the key performance indicators such as authenticity, consistency, resilience, etc., and the attainment of one or more is always their focus. As concerns are raised in regards to risk which may impede the fulfilment of the goals, controls regarding security and the organization are introduced to help mitigate the risks. The actor has full control over its assets and needs to keep the assets secure for the continuity of the business, but these assets are prone to weaknesses in their systems, known as vulnerabilities. These vulnerabilities, when not addressed on time, can lead to a threat which will introduce risk, and this risk is likely to lead to the exploitation of the assets. Once the risk factors have been identified, risk assessment is carried out to mitigate them.

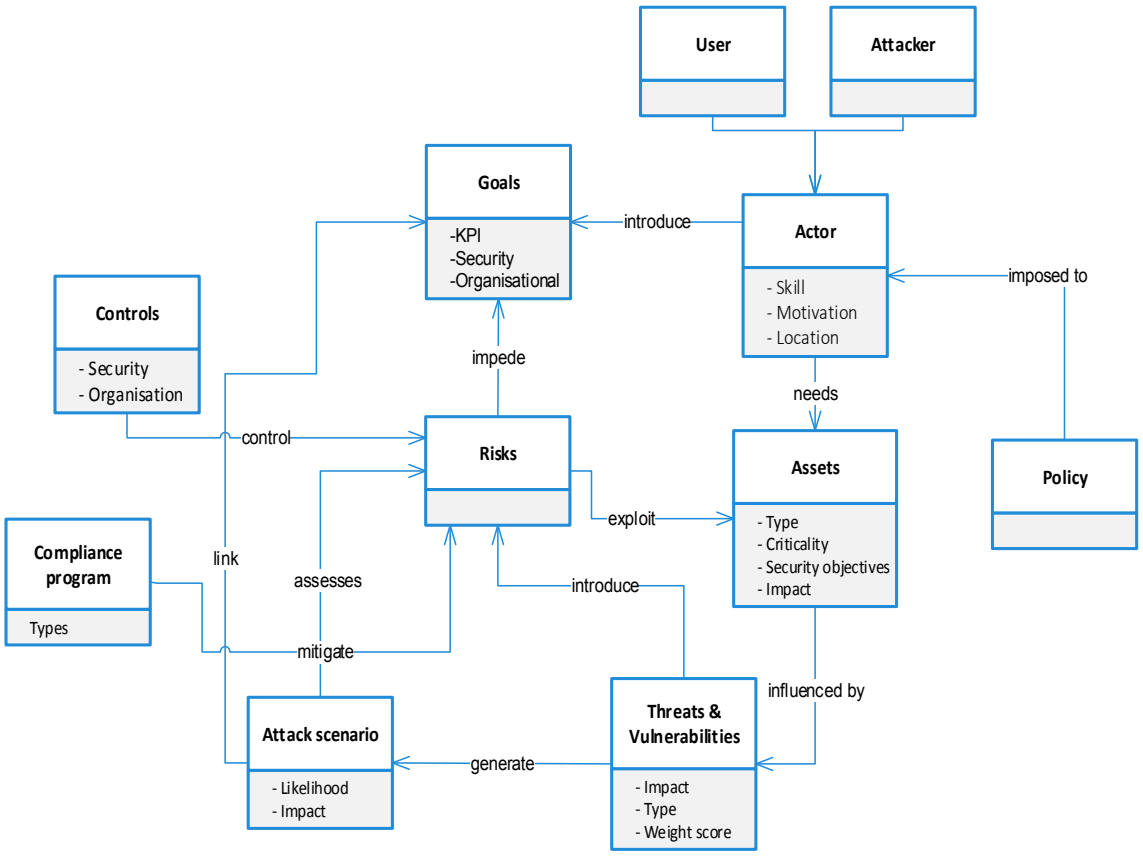

Figure 2. Metamodel.

4.2. Risk Management Process

The process of risk management comprises a systematic collection of activities. We follow the guidelines identified in the existing risk management standards ISO 310000 [32], NIST SP800-30 framework [26], and NERC CIP standards [33] to define our risk management process. The process consists of six different sequential activities which are linked with each other and every activity includes steps to support specific tasks relating to risk management.

4.2.1. Activity 1: Risk Management Context

The risk management context formally triggers the risk management activities. The purpose of this activity is to define the system and its components, scope, the KPI, and the risk acceptance level in which an organization will tolerate the residual risk to the overall business continuity. Active involvement of the actor's requirement is taken into account, risk managers and management representatives are also considered for successfully planning of risk management activities that focus on the cybersecurity of the CPS. The initiation of risk management is determined by the implementation

of the risk management scope, schedule, available resources, risk monitoring strategy, and risk treatment, based on the critical infrastructure organizations' objectives. It includes three steps which are given below.

Step 1: Identify the system and components and existing risk management practice

This step identifies the system and its associated components of a critical infrastructure. This step also identifies the current risk management practice for the CPS organization. We follow the NIST cyber security framework's implementation tiers for this purpose framework [28]. In particular, according to the framework, tiers range from 1 (partial) to 4 (adaptive). This allows us to understand the organization's current risk management practice and desired practice for future practice. Critical infrastructure is a unique system because of its complex, diversified, mutual interrelations among its systems, components, and other systems [34]. Due to the relationship between other components and systems, the state of one system is highly dependent on the state of the other system or component and thus these factors are called interdependencies. Interdependencies among the systems or components can be classified into four categories, as explained below.

- Physical interdependency: This refers to two or more infrastructures that are physically interdependent if the operation of one infrastructure depends on the physical output of the other.
- Cyber interdependency: Refers to the state of an infrastructure depending on the information communicated through the information infrastructure.
- Logical interdependencies: This type of interdependency occurs when the state of each infrastructure depends on the state of the other through controls, mechanisms, regulatory or otherwise, that cannot be considered cyber, physical, or geographical.
- Geographical independencies: This kind of interdependency occurs when elements of multiple infrastructures are in the same remote area. In this case, natural disasters can cause an element of one infrastructure to create failure in one or more infrastructures within close vicinity.

Step 2: Determine goals and key performance indicators (KPI)

This step identifies the organizational and security goals. The main goals are general confidentiality, integrity, availability, and reputation. Based on these goals, the key performance indicators for the organizational context are considered, as well as the strengths and weaknesses of the organization, which help to explain the need for cybersecurity risk management. It is also necessary to identify the key operational responsibilities of the critical infrastructure in order to support the cybersecurity activities. Key performance indicators play an integral role in risk management. They are the benefits and targets set by organizations and these goals must be achieved. A secure CPS should be able to provide the below KPI:

- Confidentiality (C): This KPI deals with the disclosure of sensitive data against unauthorized users, CPS internal users, external users, and malicious attackers. It involves the deletion and transfer of data between authorized users in a secure environment to prevent data leakage.
- High availability (A): Availability refers to ensuring that the assets of the critical infrastructure are made available and accessible to the end users as agreed, or when and where they need it. It defines the degree or extent to which the asset is readily usable along with the necessary IT and management procedures, tools, and technologies required to enable, manage, and continue to make it available.
- Integrity (I): Integrity refers to the ability of critical infrastructure organizations assets to perform their required functions effectively and efficiently without any disruption or loss of service. It includes the critical aspect of any asset which stores, processes, and retrieves data, its design, implementation, and usage. Integrity ensures that the data managed by systems and messages communicated over the network altered by unauthorized users.

- Resiliency (R): This KPI allows for the CPS to be able to work on an acceptable level of efficiency even when external or internal disturbances occur.
- Reputation (RE): Reputation is the trust and confidence the organization has gained by the public or given to the public.
- Authenticity (AUT): This KPI improves the identification and verification technology of an authorized user in order to provide security, ease of use, and administration. It has the capacity to identify an authorized user to its specific appropriate information and service type.
- Nonrepudiation (NR): This KPI provides certifiable evidence of a message being delivered to both communication endpoints in order to ensure that either the sender or the receiver does not deny sending and/or receiving the message.
- Maintainability (M): Maintainability is associated with the mean time to repair (MTTR) an asset and get it to work perfectly within a specified period of time. The time could be categorized as less than a day, several days, one week, several weeks, month(s), or even a year.

Step 3: Risk acceptance level

The risk acceptance level gives an organization a guideline with which risk needs to be controlled based on management decision linking with residual risks. With a proper risk management process, risk can be eliminated, but not to a zero level, therefore, the remaining risk is referred to as the residual risk and should be accepted to a certain level with reference to Table 1 below. Accepting risk to a certain level is really important for a critical infrastructure and organization and its surrounding context. There are no risk-free systems; therefore, the need to understand which level of acceptance of risk after control is important for an organization. A well secured CPS can resist any form of disturbances either internally or externally and is able to continue working on an acceptable efficiency level [34]. Based on the probability of occurrence and impact, the risk level will be categorized into five different risk levels. Therefore, the risk management approach decides what level of risk can be accepted for the organization.

Table 1. Asset weight score.

Category	Range
Extreme	0.81–1.00
High	0.61–0.80
Medium	0.41–0.60
Low	0.21–0.40
Very Low	0.0–0.20

4.2.2. Activity 2: Assets Identification and Criticality

This activity identifies the assets of the critical infrastructure organization which require more attention. For a successful risk management process, asset identification is critical due to the threats that impact on the assets. The activity identifies the assets and determines their criticality so that critical assets obtain adequate protection. We aware that threats are becoming more forward-thinking and attacks are targeted against CPS, with vulnerabilities are being exploited and attempts being made to destroy CPSs [35]. Therefore, the identification and protection of critical assets is necessary to avoid cyber-attacks on them and their subsequent destruction.

Step 1: Criticality identification

Criticality is a major indicator that determines the important assets of the CPS. This task combines the weight of an asset with the impact value of the asset to get the critical level of the asset. There is no standard way of combining information to determine which asset is relatively more important than others. The protection of all critical assets is almost impossible due to resource limitations and budgetary constraints. Thus, the effective identification of the most critical assets allows for ranking,

and an investment is made on those assets if the disruption could have a serious impact on national security, public health, safety, or business continuity. Asset criticality is determined based on the weight score and the impact value score. However, if a selected asset is considered more important, the weighting factor should be greater, but if the asset is considered less important, then it should be less. The asset critical level will be considered based in the description of following three categories: Noncritical, Reasonably Critical, and Extremely Critical. The categories are defined below.

- Noncritical level 0.01–3.99.
- A reasonably critical level 4.00–7.99.
- An extremely critical level 8.00–10.00.

Step 2: Asset weight

The asset weighting score is determined according to the level in which an asset is important to the continuity of the CPS objective. The category does not fully define criticality; however, the criticality of an asset can be categorized into high, medium, or low depending on the asset weight assigned. Assets with high rating are considered more valuable to the continuity of CPS, those with a medium rating represent moderate value, and those with a low rating mean that the asset is of minor value to the CPS continuity. A weight score will be assigned to each asset based on the subjective judgment given by the organization's stakeholders. Weight scoring allows the allocating of scores to achieve a total score indicating the assets criticality as shown in Table 1 below; Equation (1) determines the asset criticality.

Asset criticality *(AC)* = Asset weight score × Impact value score

$$AC = \sum_{i=1}^{n_{10}} (W_i V_i) \quad (1)$$

Using a Simple Additive Weighting (SAW) method, asset criticality level can be determined for each asset. Where a summation of the:

- *IV* = Impact value will range from 1.00–10.0.
- *W* = Weight score will range from 0.01–1.00.

4.2.3. Activity 3: Vulnerability Assessment and Threat Identification

This activity identifies and assesses the vulnerabilities that could exploit and impact on the assets identified by the previous activity. Vulnerability assessment follows different techniques, in our case, we will follow a checklist of all possible vulnerabilities associated with each critical asset, how many different assets are affected by one or many vulnerabilities, and finally how vulnerability cascade to affecting another vulnerability, therefore, causing the occurrence of a threat. The vulnerability is an exposure to security that results in the weakness of a critical asset allowing for the compromise of any of the security objectives [36], and is defined as 'the measure of the susceptibility of a system to threat' [37]. Identification and assessing vulnerability is an important and a delicate task that has an impact on the successful operation of assets that provide CPS services. There are several ways in which an attacker can exploit CPS vulnerability and therefore causing severe damage, starting from an attacker only being able to view information and ending with a worst-case scenario. Regardless of any vulnerability discovered, the attacker has little or complete control over the system and any action taken is referred to as a cyber-attack. Summary of a checklist table of the possible vulnerabilities found in the critical assets of a CPS will be given in the evaluation section. The list does not capture all the vulnerabilities because it changes over time, which could be due to environmental or technical changes. The check-list of vulnerabilities [31] will be used for illustration and will be categorized into software, hardware, database, application, communication, and network of the of CPS. This activity will be divided into two steps, the first step will look at the vulnerability rating based on the impact of the vulnerability on critical assets, and the second step will assess the vulnerability impact on the assets.

Step 1: Vulnerability Impact Rating

The impact of vulnerability on critical assets will be assigned a vulnerability rating score of VR.1 to VR.5 from very high to very low for the vulnerability found on each critical asset. In the case of multiple vulnerabilities, vulnerability is assessed and a score is given. Description of the various levels of VR (Vulnerability Rating) will be explained in Table 2 below:

Table 2. Vulnerability rating table.

Score (VR)	Criteria	Description
VR.5	Very high	One or more major weaknesses have been identified that make the asset extremely susceptible to an attack. The organization has no capability of resisting the occurrence of a threat.
VR.4	High	One or more major weaknesses have been identified that make the asset highly susceptible to an attack. The organization has the low capability of resisting the occurrence of a threat.
VR.3	Medium	A weakness has been identified that makes the asset moderately susceptible to an attack. The organization has the reasonable capability of resisting the occurrence of a threat.
VR.2	Low	A minor weakness has been identified that slightly increases the susceptibility of the asset to an attack. The organization has a good capability of resisting the occurrence of a threat.
VR.1	Very low	No weaknesses exist. The organization has an excellent capability of resisting the occurrence of a threat.

Step 2: Asset Vulnerability Impact Assessment Model (A-VIAM)

We propose an Asset Vulnerability Impact Assessment Model (A-VIAM) to determine the vulnerability impact on an asset. The model is built upon mathematical multi-value theory and structured as a value model [38]. A-VIAM is an additive preference model that assigns a value on a scale of 0.01–10.0 for vulnerability impact. The Vulnerability Rating (*VR*) on a scale of 1–5 is used to assess the vulnerability of a critical asset component and will be divided by the total number of a vulnerability discovered. The total impact value of all the critical asset components will be summed together and divided by the total number of the critical assets considered to assess the vulnerability of the entire system. The different vulnerabilities identified for a software asset, for example, the *VR* score will be assigned based on its impact on the software critical asset. All the *VR* values will be summed together to get an impact value for the Software asset and divided by the total number of vulnerabilities identified. The same method is applied to every other critical asset. The calculation for the A-VIAM model is shown below;

$$VI(CA) = \sum_{VR=1}^{n} \frac{V_{VR1} + V_{VR2} \ldots + n_{vrn}}{total\ number\ of\ vulnerability} \quad (2)$$

where: *VI* = Vulnerability Impact. Scores range between 1.00 and 10.0, and will be assigned to a vulnerability impact on to the critical asset. Where 1.00–3.99 = low, 4.00–6.99 = medium and 7.00–10.0 = high. *VR* = Vulnerability Rating. A score of 1–5 is given for the *VR* as shown in Table 2. *V* = Vulnerability type, this will be the various vulnerability types associated with each critical asset as shown in Table 7. CA = Critical Asset.

For example, if three vulnerabilities (V3.1, V3.2, and V3.4) from the checklist above were identified as a Software asset, the vulnerabilities will be rated using the *VR* score to get the vulnerability impact on the software asset using Equation (3):

$$VI(CA) = \mathrm{V3.1}_4 + \mathrm{V3.2}_3 + \mathrm{V3.4}_4 = 11/3 = 3.67$$

In this case, the vulnerability impact of the software asset is low, therefore there is little possibility of a threat occurring. The more the vulnerability is identified as an asset, the higher the vulnerability impact on the asset. To calculate vulnerability impact of an entire system, the total Vulnerability Impact of each CA, $VI(CA)$ will be summed together and divided by the total number of assets identified using the equation below:

$$VI(S) \sum_{VA\ (CA)=1}^{n} \frac{VI\ (CA1) + VI(CA2) \ldots + VI(CAn)}{total\ number\ of\ assets} \quad (3)$$

where S = Overall Critical Infrastructure System.

The category of the overall vulnerability system will have a range between 10 and 100% indicating vulnerability.

Step 3: Identify threats

The final step of this activity identifies the threat caused by the existence of a vulnerability which affects the critical assets of a critical infrastructure and its ability to deliver its services. Critical Infrastructures can be remotely controlled over the internet by the implementation of IT systems [39]. This implementation of IT systems on critical infrastructures and the interconnection between the two has given room for cyber threats leading to security concerns. Vulnerabilities such as the denial of service or malware attacks, which are famous in Critical Infrastructures, can lead to threats thereby, causing security challenges to the interconnected devices [40]. This task will also look at the different threats that affect critical assets, consequently, creating the occurrence of a risk or risks.

4.2.4. Activity 4: Risk Assessment

Risk assessment is a challenging task for the overall risk management process due to difficulties in quantifying the risk, specifically in CPS domain. We advocate to identify and evaluate the critical assets and vulnerabilities of the assets so that it eases the risk assessment activity. The first step of this activity generated the cybersecurity attack scenario based on the asset and threat from the previous activity, followed by other steps which are given below.

Step 1: Generate cyber-security attack scenario

This step generates the cyber-security attack scenario based on the identified assets, threats, and potential vulnerabilities. The cyber-security attack scenario is a combination of threats, vulnerabilities, and assets. Typically those vulnerabilities and threats that have cascade-linked with each other are included in order to generate an attack scenario. Every attack scenario will have an impact to oppose the organizational goals of the critical infrastructure. Therefore, the cybersecurity attack scenario has interdependency between the vulnerabilities and threat to exploit risk. Due to the interdependency between components of a critical infrastructure organization, cascading effects are likely to occur. Vulnerabilities cascade through each other to trigger threat which eventually turns into a risk. In terms of the cascading effect, it could be a logical, cyber, physical, or geographical cascade subject, depending on its type of interdependency. The concept of the cyber-security attack scenario is used in the approach to clearly define the type of activities that occur during risk assessment.

Step 2: Determine the likelihood of a cyber-security attack scenario

This step determines the likelihood of the risk event of the attack scenario generated in step 1. To generate the likelihood of the attack scenario, we consider the access point, attacker's location and capability, entry and target point, numbers of vulnerabilities exploited by the attacker and the skill of the attacker. This assessment will be performed by estimating two quantities, which are the likelihood of the potential scenario S occurring multiplied by the vulnerability impact as a result of the number of vulnerabilities identified which is estimated using historical evidence, empirical data and other factors. The risk R is calculated by multiplying the likelihood of the cyber security attack scenario and

its impact as shown in Equation (4), where i refers to the number of each type of incident that could result in scenario S occurring and affecting the system. The Table 3 below shows three different levels that will determine the likelihood of the attack scenario occurring and the R_i likelihood.

$$R_i = L(S_i) \times VI \tag{4}$$

where,

- $L(S)$ = the likelihood of the occurrence of the scenario S.
- i = 1, 2, 3 . . . n. The number of each incident that could result in a scenario occurring.
- R_i = risk; S = a scenario; L = likelihood; VI = vulnerability impact.

Table 3. The likelihood scale.

Levels	$L(S)$	R_i
Almost certain	0.60–1.00	1.00–1.99
Likely	0.59–0.30	2.00–3.99
Unlikely	0.29–0.01	4.00–5.00

Step 3: Attackers' skill and location

The location and skill of the attacker are based on their knowledge and expertise in organizing, executing, and succeeding in an attack. The attacker's characteristics, capability, and possible location will be explained below. The attacker's location could be internal, end-to-end, external, or physical. An internal attacker's location is usually found within the network of the organization. We consider three different levels of attacker skill which are given below and a general procedure to determine the likelihood

- Level 1: At this level the attacker has insufficient knowledge, skill, and/or resources to perform a successful attack. This attacker is most likely to be found in any of the three locations mentioned above.
- Level 2: At this level, the attacker has moderate skill level and resources to exploit one known vulnerability successfully, and the attacker is most likely to be found in the three locations mentioned above.
- Level 3: In this level, the attacker is an expert with sufficient level of skills and resources to exploit at least one known vulnerability successfully and the attacker is most likely to be found within the network as an internal attacker, end-to-end, an external attacker, or a physical attacker.

Likelihood identification procedure
$L(S_i)$ = likelihood of the scenario
R_i = risk
VI = vulnerability impact of vulnerability V_i
AL = attacker level
For each identified vulnerability V_i
  Determine vulnerability impact VI
  Measure the likelihood of the scenario $L(S_i)$
For each R_i,
  Calculate $R_i = L(S_i) * VI$
    If ($R_i \leq 1.99$) AND AL =1 then
    $L(S)$ is unlikely to occur
    If ($R_i \leq 3.99$) AND AL = 2 or 3 then

L(S) is likely to occur
If ($R_i \leq 5.00$) AND AL = 2 or 3 then
L(S) is almost certain to occur.

Step 4: Determine the impact of the cyber-security attack scenario

The impact I of a cyber-security attack scenario S is determined based on the likelihood L of the scenario S occurring and its impact on the organizations KPI K. For example, in a power grid system, if a cyber-security attack scenario should occur, there is a higher likelihood that its impact will be on the critical infrastructure organizations KPI (availability). Risk impact will depend on the affected KPI. If risk affects KPI impact will certainly be high. The relative importance of the KPI depends on its level of risk impact on the business. If there is a risk on the KPI of the system that has a high impact on the business, the risk impact will be high. Therefore, KPI, measured based on a subjective judgment of the actors, is needed to provide previous records of risk events that must have occurred and the impact of the cyber-security attack scenario. KPI importance level will follow a weight score scale of 0.01–1.00; extreme (1.00–0.81), high (0.80–0.61), medium (0.60–0.41), low (0.40–0.21) and very low (0.20–0.01) to identify the relative weight of each KPI. The impact of overall risk scale will be; low (0.01–3.99), medium (4.00–7.99), high (8.00–10.0).

$$I = \sum_{w=1}^{n_{10}} (L_S + K_{w1} \ldots K_{wn}) \tag{5}$$

where KPI (K): Key Performance Indicator; W: Weight score; L: Likelihood; I: Impact; S: Scenario; K_n: number of KPIs; K_w: weight of *KPI*; C = confidentiality, A = availability, I = integrity, R = resilience, AUT = authenticity, REP = reputation, NR = Nonrepudiation, M = maintainability.

In order to determine the impact of a cyber-security attack scenario, several preassumptions have been made for this purpose:

Preassumption 1. *Attacker is an expert and familiar with one of the vulnerabilities and exploits it for the attack.*

Preassumption 2. *Attacker is an expert and familiar with all possible vulnerabilities and exploits them all for the attack.*

Preassumption 3. *The attacker is an expert and familiar with all possible vulnerabilities and exploits one for the attack.*

Preassumption 4. *Attacker is an intermediate and familiar with possible vulnerability and exploits all for the attack.*

Preassumption 5. *The attacker is a novice and familiar with only one of the vulnerabilities and therefore exploits just that one for the attack.*

Preassumption 6. *The attacker is a novice and familiar with none of the vulnerabilities and therefore exploits nothing for the attack.*

Step 5: Identify the risk level

This final step identifies the risk level for each cyber-security attack scenario generated, the likelihood of the scenario occurring and the impact of the Scenario on KPI when it occurs. Risk level value is the addition of the likelihood of the cyber-security attack scenario resulting in a risk event and the impact of the risk event on the KPI of the organization using the Equation (6). We consider various risk level as shown in Table 4.

$$RL = L\,(S) + I \tag{6}$$

Table 4. Risk level description.

Risk Level	Score	Description
Extreme	10.0–8.00	The risk level is extremely critical and requires the implementation of the control measures to mitigate risk almost immediately. The risk level is extremely critical when both the likelihood and the impact of the risk event is extreme. Could result in serious damage that could obstruct the operations of the organization.
High	7.99–6.00	The risk level is highly critical and requires the implementation of the control measures for mitigating risk that has to be immediately within a short time frame. The risk impact is highly critical when both the likelihood and impact of the risk event are extreme and/or high. Expected to have a serious impact on the organization's reputation.
Medium	5.99–4.00	The risk level implies that the risk has an adversarial effect on the organization and effective actions need to be applied to the contingency plan of the organization and within a specific period of time. It is likely to result in a short-term disruption of the organization's services.
Low	3.99–2.00	The risk level from the risk event requires the organization to take effective actions and may require the need for a new contingency plan as well as corrective measures.
Very low	1.99–1.00	This risk level indicates that a corrective measure needs to be implemented and a contingency plan needs to be developed.

4.2.5. Activity 5: Risk Control

This activity identifies the possible control measures that could mitigate and eliminate identified risk related to the critical assets. No system is risk-free, therefore, in order to reduce security breaches to protect assets from the various types of threats and vulnerabilities, effective controls must be applied. In some cases, weaknesses in the controls make it impossible to protect the assets completely. Therefore, risk assessment is a crucial step for the management of risk in Critical Infrastructures. We follow five main risks control strategy as shown below:

- Avoidance: Risk avoidance involves eliminating risks that can negatively affect an organizations asset. Risk avoidance looks for ways to avoid compromising events completely by taking measure to ensure that threats do not occur. However, it is almost impossible to avoid all risks completely.
- Reduction: Risk reduction involves the lessening of vulnerabilities and threats events that affect the continuity of a critical process by creating contingency plans to enable critical infrastructure organizations to continue operating under recovery management. With risk reduction, the impact of a risk is limited so that it does not occur, and if it does occur, the problem will be easier to repair. The reduction can be against the impact and likelihood of the event occurring and implementing controls to reduce the risk to an acceptable level.
- Prevention: This measure should deter or avoid the risk event that can cause a negative impact on the critical infrastructure organization. Realistic preventive actions such as business continuity are put in place for effective risk control during cybersecurity risk management.
- Acceptance: This control strategy mainly involves taking no action by accepting the present level of the evaluated risk. Risk acceptance is a good strategy when the impact of the risk to the organization is very small.
- Transfer: The risk transfer measure basically shifts risks to other contract partners or enterprises, mainly to reduce the financial impact on the critical infrastructure organization or the responsibility of implementing the mitigating controls.

4.2.6. Activity 6: Risk Monitor and Residual Risk

This activity monitors the existing risk and identifies new risks which could emerge from the CPS. We consider residual risk as a remaining risk after putting any control to determine the effectiveness of the control. Residual risks procedure: Residual risk is the risk left untreated after a risk assessment has been carried out and the risk has been identified and controls implemented. After the risk has been identified, we mitigate the unacceptable risk, the remaining risk is called the residual risk,

and therefore, the risk assessment will have to be initiated from the start considering the influence of the controls to reduce the likelihood and impact of an incident. Residual risks are tightly connected to the acceptable level of risk, if the risk level is below acceptable risk, then nothing is done, and the management accepts those risk. If the risk level is above the acceptable level of risk, then new ways to mitigate those risk must be implemented.

5. Evaluation

We follow an empirical investigation through a case study and action research to determine the usefulness of the integrated risk management approach. We follow an empirical investigation through a case study and action research to determine the usefulness of the integrated risk management approach. For any empirical investigation, it is necessary to confirm the various factors, such as availability of resources, appropriate investigation questions relating to the method and study context, participant knowledge towards the study area, and many more. In our case, we confirmed all these factors and action research for this context contributes to the understanding of the risks and provides solutions to mitigate the risks. We investigated the study context and compared the study results with other studies to generalize our findings and validity of the research results.

5.1. Study Goal

The goal of the study is to:

- understand the risks associated with a CPS.
- identify suitable control management methods for the risks in a proactive manner.
- achieve feasibility of the integrated risk management method for CPS.

5.2. Data Collection and Analysis

The data collection process started with understanding the system context and interviewing the selected staff. We also reviewed various organizational documents in order to understand the existing policies and practices relating to risk management and information security. Note that, we provided an overview of the integrated risk management approach before starting any data collection. The collected data were analyzed by following both qualitatively and quantitatively methods. In particular, the unit of analysis considered the existing risk management process, no of identified risks and effectiveness of risk control. Finally we have taken the participants" view relating to the integrated risk management approach.

5.3. Study Context

The Power Holding Company of Nigeria (PHCN), formerly the National Electric Power Authority (NEPA), is an organization that generates, distributes, and transmits electricity in Nigeria. DIStribution COmpany (Disco) has acquired a license to distribute electricity and currently has 11 branches across Nigeria that serves at least 30,000 customers within an area. The main business process of Disco is to provide last-mile services in the electricity supply value chain, transforming or stepping down electricity from high voltage at the transmission level to lower voltage depending on the category of the customer, and is responsible for the marketing and sale of electricity to customers, providing tax to the government, collecting bills, and collection and customer care functions its geographical area.

The whole underlined infrastructure of Disco is a cyber-physical system. It consists of a supervisory control and data acquisition (SCADA) system which monitors processes that take place within the facility, as well as the storage and distribution components of the system to the surrounding area. Other components include communication and networks, distribution systems, server systems, control layers, field devices, smart devices, users, and operators of SCADA systems. The specific functions of the SCADA system include historical data logging for analysis and trending, alarming, controls, and process visualization. Disco also provide laptops for employees for emails, analysis,

and scheduling while at work or at home, remote access and project planning. There are Local Area Networks (LANs) within Disco for conducting business operations (i.e., file sharing, emails, databases, and web portals), operating the SCADA system. It consists of components such as the workstation, alarm management, and data control (gateways). Finally, the secondary LAN is used for stimulation, testing, and development. The existing systems (computers and servers) and the SCADA use a Windows-based operating system.

Recently, several incidents happened at Disco. All branches of Disco deployed a new SCADA system in order to improve power reliability, cyber security, and resilience to disruption. These use a SCADA consisting of 5 generic machine types connected to a local Ethernet LAN to support their services. There was a vulnerability found in the RTU (remote terminal unit) of the SCADA system in one of the branches. The RTU that controls the physical state of the equipment in the field lacked firewall up-gradation that caused data loss and operational disruption. For that reason, the other branches have decided to perform a risk management to assess vulnerabilities, such as the lack of firewalls, lack of identification and authentication mechanism, unprotected communication lines, single point of failure, flooding of local network from external sources, and to also identify other vulnerabilities that might affect its assets in the present or future. So our work focuses on assisting the mitigation of the risks and improving the cybersecurity practice. The first author of the paper and two members of Discos, including the head of IT, investigated the situation as part of a common research interest.

5.4. Introduction to the Integrated Risk Management Process

5.4.1. Activity 1: Risk Management Context

The risk management context identified the system components and determined its goals and KPI for the Disco Company. The systems include SCADA systems, communications and networks, SCADA users and operators, smart devices, software's, server systems, database, operating systems, and field devices. These systems are physical, geographically, and logically independent to support overall business operations (Figure 3). The KPIs (i.e., Confidentiality, Integrity, Availability, Authenticity, Maintainability, Resiliency, Reputation, and Nonrepudiation) were discussed and agreed with the management team. Currently, the risk management practice at Disco follows an ad hoc approach mainly in a reactive manner, there is a very limited awareness among the staff relating to cyber security risk management, the risk management process is not comprehensive and Disco does not collaborate with any of its external stakeholders relating to risk management. The risk management team ranked the existing practice as tier 1 partial. The management team agreed that, depending on the discussion, those risks having risk a level of more than three are considered the controls and those risk levels below three are considered within the acceptance level.

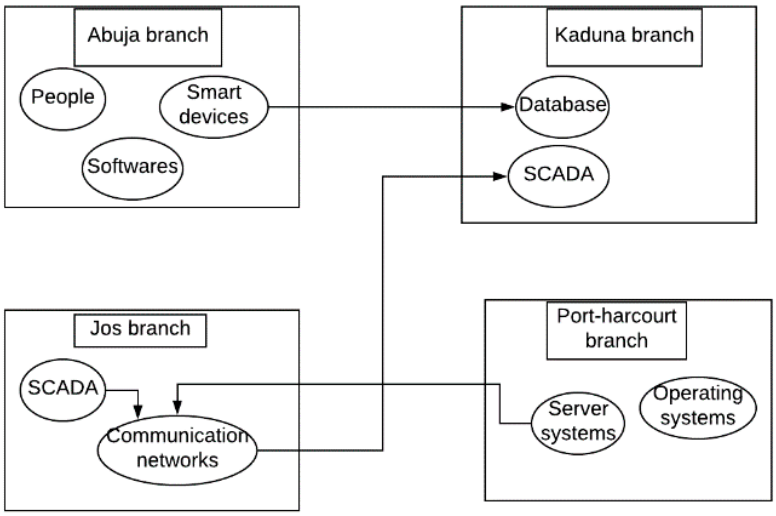

Figure 3. Geographical interdependency.

5.4.2. Activity 2: Assets Criticality

Based on the risk management context and identified main systems, the following Table 5 shows the asset criticality of the system components:

Table 5. Asset criticality.

Sub-System	Component	Impact	Weight	Equation (1)	Criticality
SCADA application software	MS Office Excel Human–machine interface	9	0.81	(9 × 0.81) = 7.29	Reasonably critical
Operating systems	Windows 7	9	0.97	(9 × 0.97) = 8.73	Extremely critical
Field devices	Programmable logic controller (PLC) Sensors Actuators Remote terminal units (RTU)	7	0.69	(7 × 0.69) = 4.83	Reasonably critical
Smart devices	Smart meter	8.7	0.99	(8.7 × 0.99) = 8.81	Reasonably critical
SCADA operators and users	Human resource manager IT personnel Senior engineer Security advisers Maintenance crew Developers	4	1.00	(4 × 1.00) = 4.00	Reasonably critical
	Customers Government	5	0.82	(5 × 0.82) = 4.10	Reasonably critical
Communication and Network infrastructure	Telephones Radio Cables Satellites Power lines	8.5	0.75	(8.5 × 0.95) = 8.08	Extremely critical
Host computers	Master terminal unit (MTU) Servers	8.0	0.89	(8.0 × 0.89) = 7.12	Extremely critical
Hardware's	Supervisory computers	7	0.69	(7 × 0.69) = 4.85	Reasonably critical

5.4.3. Activity 3: Vulnerability Assessment and Threat Identification

Depending on the incident that happened, we discovered several vulnerable areas of the system, such as metering challenges (estimating bills, poor meter maintenance), lack of maintenance of the network infrastructure, and lack of firewall configuration and systems updates. By identifying the weak points, Table 6 shows the vulnerability assessment and threats for the study context which

affected critical assets and caused the existence of a threat which led to risk. Table 7 highlights the impact of vulnerability for the Disco.

Table 6. Vulnerability identification checklist.

Assets Affected	Potential Vulnerability	Vulnerability Ranking (VR)	Threats
1. SCADA operators and users	V1.1 Absence of IT personnel	VR3	Breach of availability
	V1.2 Insufficient security training	VR3	Error in use
	V1.3 Lack of monitoring mechanisms	VR4	Illegal processing of data
	V1.4 Lack of operator awareness	VR3	Asset compromise
	V1.4 Absence of maintenance crew	VR3	Breach of availability
2. Communication and networks	V2.1 unprotected communication lines	VR5	Eavesdropping
	V2.2 lack of authorization and authentication	VR5	Authorization violation
	V2.3 failure to segment network	VR4	Network compromise
	V2.4 Lack barrier and control mechanism	VR4	Bypassing controls
3. SCADA system	V3.1 No logouts when leaving the workstation	VR3	Abuse of right
	V3.2 Metering challenges	VR3	Cheating meter reading
	V3.3 Poorly designed API, website or mobile app	VR3	Compromise
	V3.3. Lack of documentation	VR3	Error in use
	V3.4 widely distributed software	VR2	Corruption of data
	V3.5 weak firewall	VR3	Access control/forging or right
	V3.6 weak user password	VR3	Access control
	V3.6 Denial of service	VR4	Authorization violation
4. Hardware	V4.1 Unprotected storage	VR2	Theft of media or document
	V4.2 No spare management	VR3	Breach of availability
	V4.3 Equipment failure	VR4	Breach of availability
5. Database	V5.1 Data leakage	VR3	Abuse of right
6. physical	V6.1 Unstable power grid	VR5	Loss of power supply
7. Organization	V7.1 Lack of disaster recovery plan	VR5	Equipment failure
	V7.2 lack of proper allocation of information security responsibilities	VR2	Denial of actions
	V7.3 Lack of change control procedure	VR3	Breach of information system maintainability
	V7.4 Inadequate service maintenance response	VR2	Breach of information system maintainability

Table 7. Vulnerability impact assessment.

Asset Name	Vulnerability Type	Vulnerability Rating Score (*VR*)	Equation (3)	Vulnerability Impact (*VI*)
Hardware	V4.1, V4.2	3, 4	7/2 = 3.50	Low
SCADA system	V3.1, V3.3, V3.5	3, 2, 4	9/3 = 3.00	Low
Communication and networks	V2.3	5	5/1 = 5.00	Medium
People	V1.2, V1.3	3, 4	7/2 = 3.50	Low

5.4.4. Activity 4: Risk Assessment

Step 1: Generate cyber-security attack scenario

After the identification of vulnerabilities and threats, we noticed some weaknesses in the system, including the lack of firewalls and improper/irregular systems updates. We focused on the most critical vulnerabilities to demonstrate some cyber-attack scenarios. Seen in Figures 4–6.

- **Scenario 1:** A highly skilled external attacker gained access to the master terminal unit (MTU) of the power grid system through a remote access point exploiting the weak password and firewall. The attacker was able to disrupt communications, access critical data such as passwords and operating plans, and thereby, monitor the status of the system and inject malicious control commands as well as forge data into the control center. This action led the system operators into taking inappropriate actions that interrupted the availability of electricity.
- **Scenario 2:** Due to a heavy rainfall, a fallen tree branch damaged the overhead power lines feeding the substation. This interrupted the supply causing the socket breaker for this line to trip at the primary substation, leading to a total power outage to some parts of the area including the local ports and few hospitals. However, the operator did not get any notification of the socket

breaker trip and therefore did not assign the maintenance crew to the specific area of the faulty network; this left customers without supply for 18 h.

- **Scenario 3:** An endpoint skilled customer who has a bakery and requires (uses more electricity), the biggest running cost for such an operation is the electricity bill. The customer, therefore, modifies the meter reader by cracking the smart meter password and was able to reprogram and reset the smart meter. The dishonest customer was able to change the meter reading to a lower value than the actual one to reduce his electricity bill.

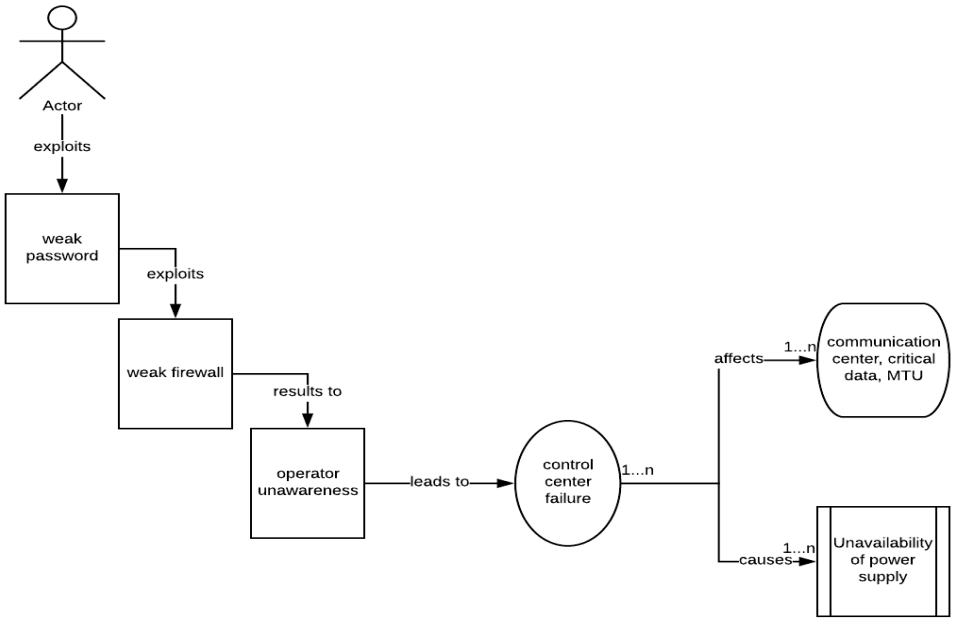

Figure 4. Scenario 1 attack sequence.

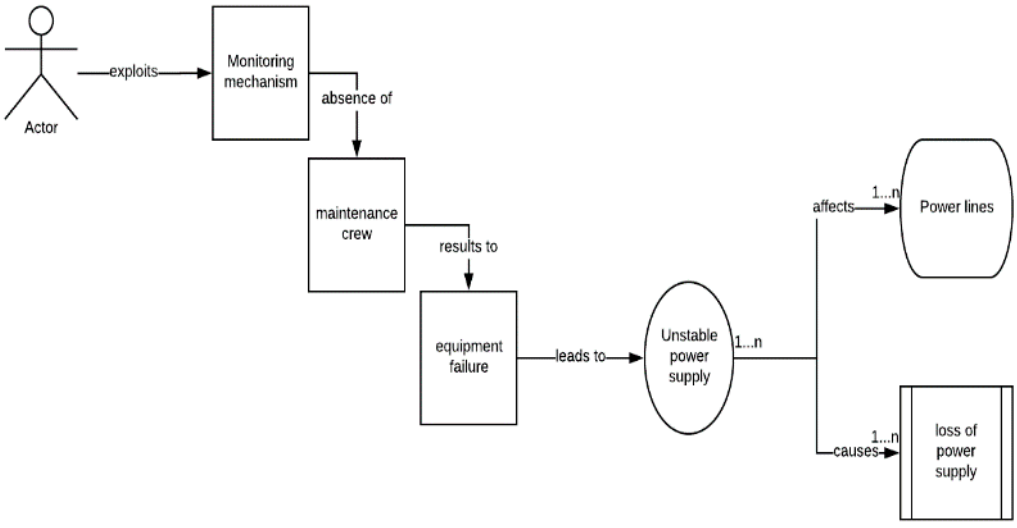

Figure 5. Scenario 2 attack pattern.

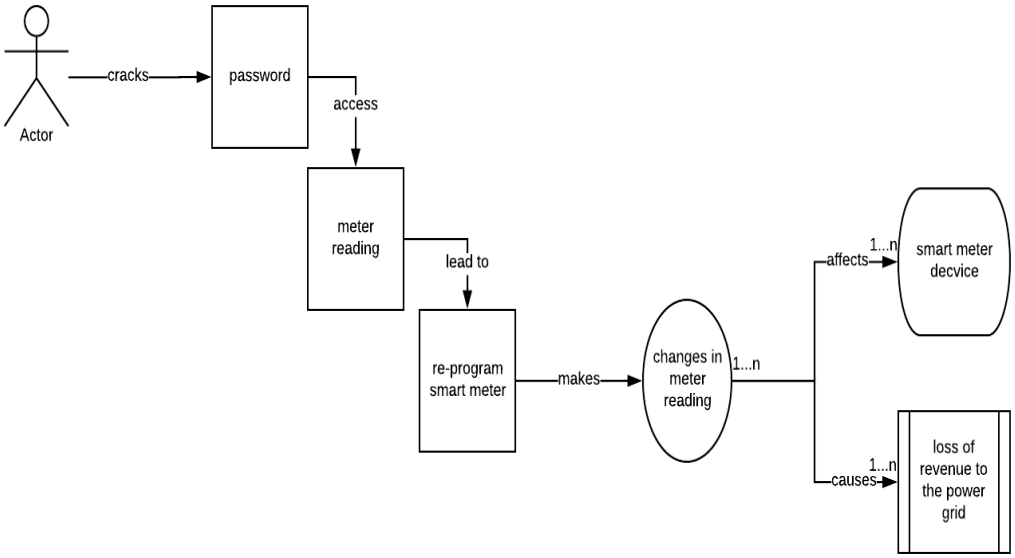

Figure 6. Scenario 3 attack pattern.

Step 2: Determine the likelihood of a cyber-security attack scenario

This step determines the likelihood, by estimating the potential attack scenario occurring multiplied by the vulnerability impact when it occurs by following Equations (2) and (4).

- **Scenario 1:**

$$VI = \text{V3.5}_{\text{VR5}} + \text{V3.6}_{\text{VR4}} + \text{V1.4}_{\text{VR3}}/3$$
$$VI = 13/3 = 4.33$$
$$R_i = 0.93 \times 4.33 = 3.85$$

Based on scenario 1, three vulnerabilities were identified and the impact of the vulnerability is 4.33, which means that the vulnerability is medially rated. Therefore, the likelihood of the attack scenario occurring is 3.85 and it is almost certain to occur.

- **Scenario 2:**

$$VI = \text{V3.6}_{\text{VR4}} + \text{V3.4}_{\text{VR2}} + \text{V3.5}_{\text{VR3}}/3$$
$$VI = 9/3 = 3.00$$
$$R_i = 0.78 \times 3.00 = 2.34$$

Based on scenario 2, three vulnerabilities were identified and the impact of the vulnerability is 3.00, which means that the vulnerability is average. Therefore, the likelihood of the attack scenario occurring is 2.34 and it is likely to occur.

- **Scenario 3:**

$$VI = \text{V3.2}_{\text{VR3}} + \text{V1.3}_{\text{VR4}} + \text{V2.2}_{\text{VR5}}/3$$
$$VI = 12/3 = 4.00$$
$$R_i = 1.00 \times 4.00 = 4.00$$

Based on scenario 3, three vulnerabilities were identified and the impact of the vulnerability is 4.00. Therefore, the likelihood of the attack scenario occurring is 4.00 and it is almost certain to occur.

Step 3: Determine the impact of the cyber-security attack scenario

- Scenario 1: The attacker bridged confidentiality, availability, and integrity by disrupting communications and gaining access to passwords, and authenticity by gaining access to the communication systems; the reputation of the organization is at stake. The impact will be based on the KPI bridged, and the KPI is assigned a weighted score based on a subjective judgment by the stakeholders. Impact of the scenario is the sum of all the KPI affected and the likelihood of the scenario occurring.

$$I = 0.93 + 0.61 + 0.55 + 0.71 + 0.33 = 3.13$$

  Therefore, impact on the KPI from the likelihood of the cyber-attack scenario generated is 3.13, which means that the impact is low.
- Scenario 2: The attack bridged the organization's availability, confidentiality, integrity, authenticity, maintainability, and reputation. The weight assigned to each KPI is based on the extent to which the attack impacted the organization negatively.

$$I = 0.97 + 0.75 + 0.60 + 0.65 + 0.68 + 0.49 = 4.14$$

  which means the attack impact on the organization was average.
- Scenario 3: The attacker bridged availability, confidentiality, nonrepudiation, integrity, and authentication by resetting the smart meter and adjusting it for his own financial benefit.

$$I = 1.00 + 0.45 + 0.56 + 0.63 + 0.71 = 3.35$$

  This means the attack impact is low impact to the organization, and the organization can operate without any major breakdown.

Step 4: Identify the risk level

The risk level for each scenario generated will be the likelihood of the attack scenario generated and the impact of the attack on the organizations KPI, by following Equation (6). Discos have agreed to accept any risk below 3, but anything from 3 and above, the risk is controlled. The risk level for each scenario is identified as shown below:

- Scenario 1:

$$RL = 3.85 + 3.13 = 6.98 \text{ (high)}$$

- Scenario 2:

$$RL = 2.34 + 4.14 = 6.48 \text{ (high)}$$

- Scenario 3:

$$RL = 4.00 + 3.35 = 7.35 \text{ (high)}$$

5.4.5. Activity 5: Risk Control

Key staff of the Discos Company, including IT, were involved in this step in order to identify control to mitigate the risks. Different controls are considered to the risks depending on the type of KPI they have impacted and also the level of damage it has caused. The following controls were proposed and an action plan was given to them to implement the controls in the next two months. The controls were also discussed with the management. Seen in Table 8.

Table 8. Security controls.

Scenario	Controls
Scenario 1	C1.1 User training is required C1.2 Strong and secure firewall configuration C1.3 Advanced control access for data provided to ensure limited access to assets C1.4 Strong combination of password and username C1.5 Regular vulnerability assessments should be carried out C1.6 Encryption of data at all times and restricted access.
Scenario 2	C2.1 Notification of events relating to occurrences is sent to customers when a power outage occurs or likely to occur C2.2 IT personnel security awareness programs should be I place every 6 months or yearly C2.3 Electricity suppliers should not go out of business C2.4 Necessary testing to confirm that the service, control process, alarm handling are functioning and protected from risk.
Scenario 3	C3.1 Violation will lead to a legal penalty C3.2 Monitoring users pattern and history C3.3 Reset the default password by the provider C3.4 Monitoring systems C3.5 Procedure to reset passwords for the smart meter after every 6 months. C3.6 Sign agreement with the customers C3.7 Accurate customer usage estimation C3.8 Tools to monitor usage of electricity accurately.

5.4.6. Activity 6: Risk Monitor and Residual Risk

The previous activity identified control actions. This activity identified the initial monitoring activity that should be taken into consideration and the risk factors that do not have adequate controls. However, the complete risk monitoring will be done in the future and not proposed in this paper. Seen in Table 9.

Table 9. Risk monitor.

Risk Name	Attack Scenario	Affected Asset	Likelihood
Unavailability of the power supply	Scenario 1	Communication systems	Likely
Loss of power supply	Scenario 2	Power lines	Likely
Loss of revenue to the grid	Scenario 3	Smart meter	Almost certain

6. Discussion

The staffs of Discos observed that the integrated risk management approach is very obliging and detailed for asset identification, assessing potential vulnerabilities and risks. It provides a comprehensive and holistic analysis of the critical assets, cascading vulnerabilities, and risks based on the cyber-attack scenario generated that is relevant to the study context. Based on the studied evaluation, the following observations have been made.

6.1. Applicability of the Approach

Several observations have been identified in regards to the applicability of the approach. The activities presented in the process are functional and acceptable. The integrated risk management approach provides the basics for identifying critical assets, assessing their vulnerabilities and potential threats, and the possible risk that could disrupt the business operations. This approach has made stakeholders aware of the possible threats that could impact their critical functions and business operations, therefore taking the necessary actions to control threats and risk events from occurring. Furthermore, understanding the current risk management practice within Disco, rating it, and proposing improvements certainly created awareness at the overall organizational level. The management of Disco planned to achieve tier 2 (risk informed) from tier 1 (partial) by implementing the integrated risk management process in a proactive manner, prioritizing cyber security activities,

sharing information an informal basis, and involving all departments and collaboration with external stakeholders.

The approach is a systematic process that integrates all areas from a holistic perspective of identifying risk which includes the stakeholders, risk types, frameworks, and the organization. It evaluates the impact of a cyber-attack on business values, organizational functions, operations, and other technical areas of the power grid system. There are three cyber security attack scenarios considered from seven assets and 18 controls, that are proposed, which is comprehensive compared to Disco's previous risk management results. However, some of the risks that could disrupt organizations operations include denial of service attack and unprotected communication lines. In order to understand the risk level, the approach can assess vulnerabilities and the impact level of an attack on the organization, using a semi-quantitative risk analysis technique.

6.2. Comparison with Existing Study Results

The results of our case study were compared with existing study results in the literature. The integrated cyber-security risk management approach is a comprehensive approach compared to other works from literature. A previous author Ref. [3] presented various security threats and incidents that occurred on different critical infrastructure domains. The work introduces some security measures including vulnerability assessments and penetration testing approaches for critical infrastructure; however, the focus of this paper was not only on vulnerability assessment, but on how clearly risk needs to be assessed, mitigated, and controlled. Asset identification and cascading vulnerabilities were not considered as a result of the interdependency between assets. A previous work [36] offers an insightful review of the possible solution paths to understand the industrial control systems security trends in relation to cyber threats, vulnerabilities, attacks, and impacts on the industrial control system (ICS). The work did not implement any practical approach to identify assets, assess vulnerabilities, threats, and mitigate risks, but only suggested some techniques. Authors of a previous paper Ref. [41] proposed a risk and vulnerability analysis method for critical infrastructure which focuses on serious events, emphasizing dependencies between critical infrastructure sectors. However, no detailed analysis has been carried out to uniquely identify critical assets and vulnerabilities of those assets, or to identify those particular chains of events (cascading vulnerabilities). A previous paper Ref. [21] proposed a unified risk management approach for a power grid system. Risk assessment, including threat and vulnerability, as well as categorizing, was discussed, but assets were not critically identified, cascading vulnerabilities were not considered, and controls were not put in place to mitigate the risk. The authors of a previous paper Ref. [9] emphasized the need for a comprehensive risk management method which covers all stages of the risk management process, our work focuses on this to improve the cyber-security of the CPS. The authors of a previous paper Ref. [10] proposed a quantitative method for mitigating cyber-security risk in information systems, our work quantified risk by identifying critical assets first, then assessing vulnerabilities. Likelihood of cyber-attack scenarios were generated to further identify the risk level and apply proper controls. The authors of a previous paper Ref. [13], in their risk assessment process, identified some risks such as unsuspicious use of infected information media, giving away of sensitive information, and lack of awareness. Our work identified all these risks, including human errors, loss of power supply, unavailability of power supply, loss of revenue to the power grid, and breach of security goals. The authors of a previous paper Ref. [15] proposed a layered approach that evaluates risks based on security, our work evaluated risks based on cyber-attacks as well as physical attacks and evaluates risk level and proper controls. The authors of a previous paper Ref. [14] discussed a mechanism for preventing, detecting, and recovering attacks for securing CPS, our work provided a mechanism for identifying critical assets, assessing cascading vulnerabilities, generating cyber-attack scenarios, impact of the attack occurring, and provided mitigation controls to properly secure the CPS.

None of the works provide a systematic risk management process that identifies critical assets before assessing vulnerabilities, and also focuses on the initial vulnerability impact that leads to

the cascading vulnerabilities effect. Our work identifies and compares the existing risk mitigation strategies for CPS in critical infrastructure, and therefore, gives critical infrastructure organizations a chance to perform an in-depth analysis for cyber-security on CPS. In terms of risk identification and mitigation, there are common findings between our study and other works. The authors of a previous paper Ref. [34] addressed risk by taking into account interdependencies and risk monitoring. These results are completely or partly similar to the findings in our work. However, some risks, such as energy wastage and deploying mobile cloud computing challenges, as identified [19], are not directly similar to our studied context. Some unique risk factors that were not mentioned in other studies include: lack of contingency plans, lack of disaster recovery, lack of monitoring mechanisms, lack of comprehensive risk management, and initial impact of cascading vulnerability. Cascading risk effect is the major risk in our study context, which does not match any other work. We advocated to users and operators to not ignore their IT responsibilities because the risks in critical infrastructure organizations depend on the context of the organization. It is also necessary to create awareness about cyber security risks throughout the whole organizational level and its supply chain environment as well as continuously improving and using advanced cyber security technologies to practice managing risks and the evolution of those risks.

6.3. Limitations of the Framework

One of the observations from the participants was that it is difficult to understand the calculations for assessing vulnerability and assuming the probability value and impact value for risk level. Furthermore, the participants also commented about the KPIs and their link to determining impact. It could be more challenging if the numbers of KPIs increased. We are planning to automate the calculation and tailoring the KPI depending on the CPS context. The risk monitoring activities and residual risks were not investigated due to the lack of time with the organization.

6.4. Study Validity

Threats relating to validity are always important for any empirical investigation. We tried to reduce the bias of our study finding by actively involving the staff throughout the process. Data was collected from various sources such as interviewing participants, reviewing the existing documentation, and the organization's internal and external context. The active of participation of key staff of the organization also supported the precondition for action research. The management commitment to achieve tier 2 for an informed cyber security risk management practice demonstrated the importance of the risk management for overall business continuity. However, there is a possibility of culture bias as data was gathered from a single geographical location. To mitigate this, we compared our findings with other study results and observed several common and unique issues to generalize our findings.

7. Conclusions

Critical infrastructures are increasingly facing many challenges, including cybersecurity attacks. Importantly, there are many security challenges faced by infrastructure service providers, which tend to bring down their business operations and disrupt the continuity of their operation. An integrated cyber-security risk management framework for the CPS of a critical infrastructure can systematically analyze the risks and offer plans to control the risks so that business continuity can be ensured. Every critical infrastructure should implement an effective risk management process to protect the stakeholders from financial, organizational, and reputational loss. Our work contributes to the existing literature by providing a comprehensive risk management approach. To demonstrate the applicability of the work, we applied the proposed approach to a smart grid CPS. The example shows that the approach sufficiently supports the organization to analyze their security issues, identify critical assets, assess vulnerabilities and potential threats, and to also identify risk levels with proper controls to mitigate risks. The results show that the approach provides information about possible vulnerabilities, how they can cascade, and result in a bigger issue if not addressed on time. The approach considered

seven main KPIs of the organization, and impact was calculated based on the effect of an attack on the KPIs. Risks were analyzed using a semi quantitative approach and influenced by the likelihood of the cyber-attack scenario occurring and the impact on the KPI of the organization to provide accurate risk levels. The results of the risk management outcome were integrated into the study context. The organization planned to achieve a risk-informed approach for managing overall cyber security risks. We advocate for the creation of cyber security risk management awareness within all organizational levels; staff must not ignore their IT responsibilities. Our future plan is to apply the proposed approach into other case studies in order to generalize our findings and validate the applicability of the approach. We are also planning to develop a tool to automate risk management activities. Furthermore, it is also necessary to create a process for integrating advanced cyber security technologies and practice for managing the risk and its evolutions.

Author Contributions: H.I.K. and S.I. contributed to the design and development of the proposed integrated risk management framework, concepts, and process. H.I.K. has set up the case study and performed the case study. M.A.R. contributed to the review the whole paper and provided feedback within the given framework.

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

References

1. Wu, W.; Kang, R.; Li, Z. Risk assessment method for cyber security of cyber physical systems. In Proceedings of the 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, China, 21–23 October 2015.
2. Kim, K.-D.; Kumar, P. An overview and some challenges in cyber-physical systems. *J. Indian Inst. Sci.* **2013**, *93*, 341–352.
3. Abouzakhar, N. Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. In Proceedings of the European Conference on Information Warfare and Security, Jyväskylä, Finland, 11–12 July 2013.
4. Marvell, S. *The Real and Present Threat of a Cyber Breach Demands Real-Time Risk Management*; Acuity Risk Management: London, UK, 2015.
5. Adar, E.; Wuchner, A. Risk management for critical infrastructure protection (CIP) challenges, best practices & tools. In Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05), Darmstadt, Germany, 3–4 November 2005.
6. Marvell, S. Real-Time Cyber Security Risk Management. *ITNOW* **2015**, *57*, 26–27. [CrossRef]
7. Harvey, J.; Service, T.I. Introduction to Managing Risk. Available online: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf (accessed on 29 May 2018).
8. Georgieva, K.; Farooq, A.; Dumke, R.R. Analysis of the Risk Assessment Methods–A Survey. In *International Workshop on Software Measurement*; Springer: Berlin, Germany, 2009.
9. 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]
10. Patel, S.C.; Graham, J.H.; Ralston, P.A. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *Int. J. Inf. Manag.* **2008**, *28*, 483–491. [CrossRef]
11. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
12. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks against process control systems: Risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011.
13. Peng, Y.; Lu, T.; Liu, J.; Gao, Y.; Guo, X.; Xie, F. Cyber-physical system risk assessment. In Proceedings of the Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 6–18 October 2013.
14. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In Proceedings of the Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, USA, 23–24 July 2009.

15. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]
16. Yoneda, S.; Tanimoto, S.; Konosu, T.; Sato, H.; Kanai, A. Risk Assessment in Cyber-Physical System in Office Environment. In Proceedings of the 2015 18th International Conference on Network-Based Information Systems (NBiS), Taipei, Taiwan, 2–4 September 2015.
17. Ten, C.-W.; Manimaran, G.; Liu, C.-C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2010**, *40*, 853–865. [CrossRef]
18. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Trans. Smart Grid* **2017**, *8*, 2431–2439. [CrossRef]
19. Gai, K.; Qiu, M.; Zhao, H.; Tao, L.; Zong, Z. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. *J. Netw. Comput. Appl.* **2016**, *59*, 46–54. [CrossRef]
20. Gai, K.; Qiu, M. Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. *IEEE Trans. Ind. Inform.* **2017**. [CrossRef]
21. Ray, P.D.; Harnoor, R.; Hentea, M. Smart power grid security: A unified risk management approach. In Proceedings of the 2010 IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5–8 October 2010.
22. Yadav, D.; Mahajan, A.R. Smart Grid Cyber Security and Risk Assessment: An Overview. *Int. J. Sci. Eng. Technol. Res.* **2015**, *4*, 3078–3085.
23. Rice, E.B.; AlMajali, A. Mitigating the risk of cyber attack on smart grid systems. *Procedia Comput. Sci.* **2014**, *28*, 575–582. [CrossRef]
24. ISO. *Risk Management—Principles and Guidelines*; ISO 31000:2009; International Organization for Standardization: Geneva, Switzerland, 2009.
25. GOST-R. *Risk Management. Risk Assessment Methods*; ISO/IEC 31010-2011; International Organization for Standardization: Geneva, Switzerland, 2009.
26. Cybersecurity, C.I. Framework for Improving Critical Infrastructure Cybersecurity. Available online: http://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed on 29 May 2018).
27. Purdy, G. ISO 31000:2009—Setting a new standard for risk management. *Risk Anal.* **2010**, *30*, 881–886. [CrossRef] [PubMed]
28. Islam, S.; Fenz, S.; Weippl, E.; Mouratidis, H. A Risk Management Framework for Cloud Migration Decision Support. *J. Risk Financial Manag.* **2017**, *10*, 10. [CrossRef]
29. Islam, S.; Mouratidis, H.; Weippl, E.R. An empirical study on the implementation and evaluation of a goal-driven software development risk management model. *Inf. Softw. Technol.* **2014**, *56*, 117–133. [CrossRef]
30. Berg, H.-P. Risk management: Procedures, methods and experiences. *Risk Manag.* **2010**, *1*, 79–95.
31. CISO. Information Risk Assessment Handbook. Available online: http://www.nationalarchives.gov.uk/documents/information-management/risk-assessment-handbook.pdf (accessed on 29 May 2018).
32. AIRMIC; ALARM; IRM. *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*; The Public Risk Management Association: London, UK, 2010.
33. NERC, CIP. *Standards as Approved by the NERC Board of Trustees May 2006*; North American Electric Reliability Corporation: Atlanta, GA, USA, 2006.
34. Bialas, A. Risk management in critical infrastructure—Foundation for its sustainable work. *Sustainability* **2016**, *8*, 240. [CrossRef]
35. Rahman, A.A.L.A.; Islam, S.; Kalloniatis, C.; Gritzalis, S. A Risk Management Approach for a Sustainable Cloud Migration. *J. Risk Financial Manag.* **2017**, *10*, 20. [CrossRef]
36. Ani, U.P.D.; He, H.; Tiwari, A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *J. Cyber Secur. Technol.* **2017**, *1*, 32–74. [CrossRef]
37. Ezell, B.C. Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Anal.* **2007**, *27*, 571–583. [CrossRef] [PubMed]
38. Parnell, G.S.; Conley, H.W.; Jackson, J.A.; Lehmkuhl, L.J.; Andrew, J.M. Foundations 2025: A value model for evaluating future air and space forces. *Manag. Sci.* **1998**, *44*, 1336–1350. [CrossRef]
39. Blank, R.; Gallagher, P. *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012.

40. Baldoni, R. *Critical Infrastructure Protection: Threats, Attacks, and Counter-Measures*. Technical Report. Available online: http://www.dis.uniroma1.it/~tenace/download/deliverable/Deliverable4a.pdf (accessed on 29 May 2018).
41. Utne, I.B.; Hokstad, P.; Kjølle, G.; Vatn, J.; Tøndel, I.; Bertelsen, D.; Fridheim, H.; Røstum, J. Risk and vulnerability analysis of critical infrastructures-The DECRIS approach. In Proceedings of the SAMRISK Conference, Oslo, Norway, 6–7 March 2008.