





Article

When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method

Mostafa Shokry ¹, Ali Ismail Awad ^{2,3,*}, Mahmoud Khaled Abd-Ellah ⁴ and Ashraf A. M. Khalaf ⁵

¹ Department of Infrastructure and Information Security, Ministry of Electricity and Renewable Energy, Cairo 11517, Egypt; mostafa.shokry@moere.gov.eg

² College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 15551, United Arab Emirates

³ Centre for Security, Communications and Network Research, University of Plymouth, Plymouth PL4 8AA, UK

⁴ Faculty of Artificial Intelligence, Egyptian Russian University, Cairo 11829, Egypt; mahmoud-khaled@eru.edu.eg

⁵ Department of Electrical Engineering, Faculty of Engineering, Minia University, Minia 61519, Egypt; ashkhalaf@yahoo.com

* Correspondence: ali.awad@uaeu.ac.ae; Tel.: +971-3713-5531

Abstract: Leading risk assessment standards such as the NIST SP 800-39 and ISO 27005 state that information security risk assessment (ISRA) is one of the crucial stages in the risk-management process. It pinpoints current weaknesses and potential risks, the likelihood of their materializing, and their potential impact on the functionality of critical information systems such as advanced metering infrastructure (AMI). If the current security controls are insufficient, risk assessment helps with applying countermeasures and choosing risk-mitigation strategies to decrease the risk to a controllable level. Although studies have been conducted on risk assessment for AMI and smart grids, the scientific foundations for selecting and using an appropriate method are lacking, negatively impacting the credibility of the results. The main contribution of this work is identifying an appropriate ISRA method for AMI by aligning the risk assessment criteria for AMI systems with the ISRA methodologies' characteristics. Consequently, this work makes three main contributions. First, it presents a comprehensive comparison of multiple ISRA methods, including OCTAVE Allegro (OA), CORAS, COBRA, and FAIR, based on a variety of input requirements, tool features, and the type of risk assessment method. Second, it explores the necessary conditions for carrying out a risk assessment for an AMI system. Third, these AMI risk assessment prerequisites are aligned with the capabilities of multiple ISRA approaches to identify the best ISRA method for AMI systems. The OA method is found to be the best-suited risk assessment method for AMI, and this outcome paves the way to standardizing this method for AMI risk assessment.

Keywords: advanced metering infrastructure; information security risk assessment; smart grids; smart cities; risk assessment methods; OCTAVE Allegro; CRAMM



Citation: Shokry, M.; Awad, A.I.; Abd-Ellah, M.K.; Khalaf, A.A.M. When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method. *Sustainability* **2023**, *15*, 9812. <https://doi.org/10.3390/su15129812>

Academic Editors: Iqram Hussain, MD Rashedul Hasan Sarker and Md Azam Hossain

Received: 10 April 2023

Revised: 8 June 2023

Accepted: 12 June 2023

Published: 20 June 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

One of today's most important information infrastructure technologies, advanced metering infrastructure (AMI), can be seen as the first step in digitizing the conventional electricity grid [1]. The integration of information technology (IT) with current critical infrastructure, such as AMI, presents vulnerabilities that could be exploited in cybersecurity attacks. The security, economics, and public safety of a country are all at risk if any of its vital infrastructure systems are compromised [2]. Because of the significance of cybersecurity risks to critical infrastructure, the U.S.'s Cybersecurity Enhancement Act of 2014 updated the role of the National Institute of Standards and Technology (NIST) with respect to developing a cybersecurity framework. This framework focuses on providing a flexible,

performance-based, and cost-effective approach to the organizations that own the critical infrastructure, and it requires them to identify, assess, and manage cybersecurity risks [3].

The deployment of a security perimeter for an AMI system should start with an information security risk assessment (ISRA) being conducted. Due to the significance of the function of an AMI system and the sensitive data that are transmitted over it, the ISRA process must be carried out in advance. Therefore, it is important to choose an ISRA method that is capable of handling large amounts of data, is adaptable to the specific needs of AMI systems, and can provide accurate and reliable results. There are various ISRA methods that are currently available, such as OCTAVE Allegro (OA), CRAMM, CORAS, and COBRA [4]. Thus, determining the appropriate ISRA method to apply to an AMI system is a crucial challenge, as it requires careful consideration of various factors such as the nature of the AMI system, the types of data being processed, and the potential risks and threats associated with them. One of the biggest differences between AMI systems and other critical infrastructure systems is the huge amount of data that flows through them. These data include electricity consumption data, meter data management system (MDMS) data, and even commands that can be sent from the MDMS to a smart meter (SM) or data concentrator (DC) [5].

Numerous research studies have been conducted regarding the security of AMI systems and ISRA. For instance, one study by Hansen et al. [6] analyzed some of the security flaws that are currently present in AMI systems. Sgouras et al. [7] assessed the resilience of an AMI system against a potential botnet attack by employing a generic risk assessment methodology. Yao et al. [8] limited their investigation to the AMI system's network topology and evaluated security concerns using a general methodology for risk assessment. The only comparative study between ISRA methods using various comparison criteria was provided by Agrawal [9]. Despite the fact that a number of studies have been carried out in this field, no study has been conducted to establish the specific risk assessment needs of AMI systems or to ascertain the most suitable approach for conducting such assessments.

The main contribution of this study is to identify the most appropriate risk assessment method to use with AMI systems. To accomplish this, several currently used ISRA methods were compared using various criteria, and their capabilities were then examined with reference to the specifications of the AMI risk assessment requirements. In this study, we primarily compared existing risk assessment methodologies, such as OA, CRAMM, CORAS, and COBRA. Even though there are numerous standards in the field of ISRA, such as NIST SP 800-37 [10], NIST SP 800-39 [11], and ISO 31000 [12], this study focused mainly on the specific methods that can be used for ISRA rather than the standards themselves.

1.1. Problem Statement and Contributions

According to the NIST Framework for Improving Critical Infrastructure Cybersecurity [13], critical infrastructure systems are “systems and assets, whether physical or virtual, so vital . . . that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”.

Several smart-infrastructure solutions are currently used that fall within the scope of the above definition of critical infrastructure, such as the Internet of Things (IoT), cyber-physical systems, and industrial control systems. In contrast to other intelligent infrastructure systems, an AMI network provides vast quantities of information, which is transmitted from all users to an electricity service provider's (ESP's) data center. Furthermore, a significant number of the parts of an AMI system does not reside within this data center, meaning that the data that are transmitted are crucial, and they change frequently [14].

Both the utility center and the end user depend heavily on the data that are transmitted via the AMI system. These data can be used to improve power quality, keep track of end users' energy consumption, and control the load [1]. Due to the high level of criticality of these data, a risk assessment procedure should be employed to pinpoint the flaws of the AMI system, establish any potential threats, determine the probability that an attack would

actually occur, and consider the effects that an attack would have on the AMI system. The key contribution of this research is the identification of an appropriate risk assessment methodology for examining the potential dangers associated with AMI systems [1].

There have been previous studies comparing ISRA methods and providing guidelines, such as that of Derakhshandeh and Mikaeilvand [15]. Two studies provided comparisons of some of the security risk assessment techniques currently in use by considering criteria such as accuracy and the amount of time needed to complete the risk assessment task. Kuzminykh et al. [16] provided an analysis of some of the existing risk assessment methods, focusing on the main features of each method. Pandey [17] focused on the relationship between an ISRA method and IT governance. However, these previous studies did not determine an appropriate ISRA method to use for AMI systems. Therefore, the contributions of this work are threefold, as follows:

- The various ISRA methods currently in use are compared by highlighting their key characteristics, such as the method of risk analysis that is used (qualitative or quantitative), how many steps are involved for each method, and whether or not the method complies with the three key security requirements: confidentiality, integrity, and availability (CIA).
- The AMI risk assessment requirements are demonstrated by including classifications of the crucial constituents of an AMI system into three main categories—information and data assets, resource assets, and service assets—that are essential to assessing an AMI system, determining its potential risks, and reducing them to acceptable levels.
- The main AMI risk assessment requirements and the capabilities of each risk assessment method are compared to determine the most appropriate method to apply to an AMI system to assess the potential risks that could threaten its critical assets and thus its overall performance.

1.2. Paper Structure

The rest of this article is organized into six sections, as shown in Figure 1; these are as follows. Section 2 examines the literature reporting works that were performed previously in the fields of both ISRA methods and the security of AMI systems. Section 3 provides a comparative analysis of a sample of existing ISRA methods, such as OA, CORAS, COBRA, and FAIR, under different criteria; the capabilities, advantages, and disadvantages of each ISRA method are illustrated. Section 4 gives an overview of AMI systems and the parameters required to carry out a risk evaluation on such a system, as well as considering the essential assets that could impact the system's performance. Section 5 focuses on the matching of the AMI assessment criteria with the features of existing ISRA approaches to establish the most suitable ISRA method for assessing any potential threats to an AMI system. Finally, Section 6 offers concluding statements and establishes prospective avenues for further exploration.



Figure 1. Mind map illustrating the structure of the paper.

2. Related Works

Numerous studies have been conducted regarding the current status of security and ISRA in the context of AMI systems, including comparisons between the most common existing ISRA methods and assessments of the potential risks to AMI systems, as illustrated in Table 1. For instance, Shokry et al. [18] conducted a survey of AMI security, including an examination of the existing vulnerabilities and threats for every stratum within AMI systems. Additionally, samples of security countermeasure techniques and present issues in each layer of the AMI were covered. Shokry et al. [19] employed the CORAS methodology to evaluate AMI systems with a focus on identifying their essential components, creating threat diagrams, and creating risk-scenario diagrams. Additionally, samples of countermeasure techniques were introduced.

Borenus et al. [20] examined smart grids (SGs) but only for four types of attack: erroneous data injection, ransomware, denial of service (DoS), and supply-chain attacks. However, this research relied on the ISO/IEC 27005:2018 standard [21], and an optimum ISRA method for an SG was not chosen through a comparative examination. Regarding samples of systems with critical infrastructure, Baig and Zeadally [22] analyzed the potential threats to SGs. Five SG elements and five risk events were taken into account using a generalized risk assessment approach. The key issues with this study were the adoption of a broad risk assessment approach and the limited number of risk scenarios that were considered.

Haider et al. [23] proposed a model to ascertain potential wireless threats to AMI resources. Their proposed model was based on two models; namely, they identified the digital security risks that can impact AMI systems, and they subsequently assessed and

prioritized these various threats through the use of an ordinal scale. Ali and Awad [24] used the OA method to assess IoT-based smart home systems to evaluate their current vulnerabilities and threats, and some countermeasure strategies were discussed to reduce the likelihood of possible hazards. Their study can provide a basis for augmenting the levels of security of smart homes that rely on IoT technology.

Yao et al. [8] focused explicitly on AMI communication links by investigating the existing vulnerabilities that may exist in an AMI network's topology. They applied a generic approach for risk assessment to the AMI system's mesh topology without specifying the risk assessment method. Line et al. [25] illustrated the difficulties that exist in relation to assessing the risks to AMI systems. They included the probable vulnerabilities and security threats that may exist in relation to AMI systems.

Shawly et al. [26] introduced a tool called SecAMI to calculate the relationship between the propagation speed of a distributed denial-of-service (DDoS) attack and the time required to detect such an attack on an AMI system. They applied this tool to the neighborhood area network (NAN) of the AMI system to improve the development and deployment of intrusion detection and prevention systems in this context.

Table 1. Comparison of the identified works related to AMI risk assessment found in the literature.

Ref.	Year	Objective	Remarks	Our Contribution
[18]	2022	This study focused on illustrating the structure of the AMI system, the existing vulnerabilities in each of its layers, samples of related attacks, and samples of countermeasure techniques that can be applied.	Neither the main risk assessment process, a comparative study between the existing risk assessment methods, nor an examination of the parameters required to apply the risk assessment procedure to an AMI system were included.	The main requirements to perform the risk assessment process for an AMI system and the main features of risk assessment methods are presented to decide on the best methodology for an AMI system.
[19]	2022	The CORAS risk assessment methodology was employed in the evaluation of AMI systems, determining samples of vulnerabilities in their elements, and creating threat and potential risk scenarios.	Neither a comparative study between samples of ISRA methods nor a determination of the AMI risk assessment requirements were included in this study.	The relevant characteristics of risk assessment methods are described, and these are considered in combination with the key needs of an AMI system in relation to completing the risk assessment process to find the optimal approach for an AMI system.
[20]	2022	The ISO/IEC 27005:2018 standard was used to evaluate any prospective risks for an SG.	The ISO/IEC 27005:2018 standard was applied to the SG without providing a comparative study between various risk assessment methods.	To choose the best method for AMI systems, the key elements of risk assessment methods are described along with the major needs of AMI systems in relation to carrying out the risk assessment procedure.
[22]	2019	By implementing a broad framework for risk assessment to examine possible risks for an SG as an extremely sensitive system, five risk scenarios were created.	A general risk assessment method was applied to the AMI system without determining the specific AMI risk assessment requirements or illustrating the pros and cons of various risk assessment methods.	A comparative analysis of the various risk assessment methods shows the key AMI requirements for implementing the risk-evaluation procedure to an AMI system. This helps choose the best risk assessment method for use with AMI systems.
[23]	2019	This work focused on attacks related to the wireless communication technology by applying a threat model based on the STRIDE and DREAR models.	Neither the main risk assessment process, a comparative study between the existing risk assessment methods, nor an examination of the parameters required to apply the risk assessment procedure to an AMI system were included.	To select the best approach for AMI systems, the key elements of risk assessment methods are laid out along with the essential criteria of AMI systems required to execute the risk assessment procedures.
[24]	2018	This study used the OA method for assessing the possible risks associated with IoT-based devices in smart homes.	The work covered only the customer side of the AMI system, excluding the SM and including only intelligent end devices (IEDs).	The AMI system is risk assessed, including the SM, DC, and MDMS within the ESP, and samples of mitigation techniques are included.
[8]	2017	This paper focused only on the AMI system's communication layer by implementing a methodology for risk assessment on its mesh topology to identify any current vulnerabilities.	This work focused only on the AMI communication layer without determining the risk assessment method that will be applied.	A comparative study between existing risk assessment methods demonstrating the main AMI requirements for applying a risk-evaluation procedure to an AMI system is conducted, and the most appropriate risk assessment method to apply to an AMI system is determined.
[25]	2015	This paper focused on determining the difficulties that are faced in the process of assessing the risks for an AMI system, including the potential threats and vulnerabilities that may exist.	The main assets and requirements of the risk assessment process and the appropriate risk assessment methods for the AMI system were not included.	Matching between the capabilities of some of the existing risk assessment methods and the required parameters for assessing the risks of AMI system is conducted to determine the most appropriate risk assessment method to meet these requirements.
[26]	2014	This work focused on the deployment of a tool that can be employed for the purpose of computing time between the initiation of a DDoS attack and its detection; this tool was then applied to the NAN of the AMI system.	This work did not demonstrate the risk assessment method that was used, and it focused mainly on one type of attack and AMI-system NAN topology.	The present work undertakes matching between the main requirements for applying a risk assessment process to an AMI system and the features of some existing risk assessment methods.

Research-Gap Analysis

As Table 1 illustrates, the issues of the risk assessment process for AMI systems have been a topic of discussion in several previous works in the literature; this is demonstrated by the reports of Borenius et al. [20], Shokry et al. [19], Baig and Zeadally [22], and Ali and Awad [24]. Additionally, numerous investigations have been presented in the field of security perspectives pertaining to AMI systems, as demonstrated in the reports of Shokry et al. [18], Haider et al. [23], and Yao et al. [8]. Numerous investigations have been carried out considering the security challenges associated with AMI systems.

Although several studies have been conducted in the domains of assessing the potential risks for AMI systems and their security, there are numerous research gaps in these studies. These can be summarized as follows:

- An optimum ISRA methodology for AMI systems has not been identified via a statistical comparison of ISRA methodologies.
- AMI systems have been evaluated using conventional risk assessment techniques rather than a well-known risk assessment methodology.
- Without explaining why it was selected or considering the AMI-specific risk-assessment requirements, the OA risk assessment approach has been employed to examine AMI systems.
- The CORAS risk assessment approach has also been employed for AMI systems without offering a comparative study with other risk assessment methods.

Table 1 summarizes all relevant works that have been published in the AMI security and ISRA. This clearly shows that there is no previous work that has considered the problem of identifying the most appropriate ISRA method for security risk assessment in AMI networks. We were thus motivated to conduct this study, which is concerned with choosing the best risk assessment methodology for AMI systems to fill all of the aforementioned research gaps. The end result was attained by combining the capabilities of multiple risk assessment methodologies with the primary criteria of the AMI risk assessment procedure.

3. Security Risk Assessment Methods

Risk can be quantified as a function of the possibility that an attack will occur by taking advantage of an existing weakness and the influences of such attacks on a certain system's functionality [6]. The relationship between the three basic pillars of any risk—vulnerabilities, threats, and assets—is depicted in Figure 2. A threat can take advantage of an asset's flaws, and any asset that has weaknesses is susceptible to exploitation. The likelihood and frequency of a threat's recurrence can be used to assess the relationship between the threats and the assets' existing vulnerabilities. The sum of all the aforementioned factors results in the system's current potential risk.

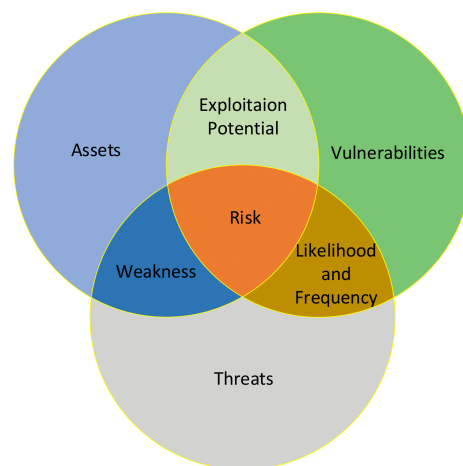


Figure 2. Risk component diagram illustrating the main risk components and their relationships.

The main goals of the ISRA are to assess a system's level of criticality, its critical assets, its vulnerabilities, prospective assaults that could put these assets at risk, and the effectiveness of its security measures [27]. Any of the current ISRA methods, such as OCTAVE Allegro (OA), CRAMM, CORAS, and COBRA, can be used to complete these tasks, but the results may vary from one method to another.

ISRA methods differ from each other in terms of their capabilities, which are represented by the availability of documentation, the risk-analysis approach, and the required number of steps. Additionally, some of these methods require external expertise, while others can be implemented by the internal employees of an organization [28]. Another difference between the methods is that some are compatible with all kinds of risks, while others can only be applied to a specific type of risk [28].

ISRA methods can be classified into three main categories: temporal, comparative, and functional. Temporal risk assessment methods focus on technical security and require a good system understanding. Comparative risk assessment methods focus on the management of nontechnical security risks. Functional risk assessment methods are a combination of both temporal and comparative methods; they have less focus on technical security than temporal methods but require more system-specific understanding than comparative approaches [9].

This section is devoted to a comparative study of some existing ISRA methods with different perspectives and features, such as OCTAVE, CRAMM, CORAS, FAIR, FRAP, MEHARI, and COBRA, which are the common and most famous methods in the literature. The strategy is to perform a comparative study using different criteria such as the simplicity of the method, the availability of its documentation, the purpose of the method, and its integration with the CIA security attributes.

3.1. CRAMM

The Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM) is one of the existing temporal ISRA methods. It is based on the structured systems analysis and design methodology, which is a set of standards that can be used to analyze a system's design, application, and method [29]. According to qualitative estimations given to assets, threats, and assets' vulnerabilities, CRAMM determines and evaluates risk levels before translating them into a quantitative assessment using these points [29].

CRAMM has its own complicated risk assessment software, the CRAMM v5.1 toolkit, which fully complies with the ISO 27001 standard [30]. ISO 27001 [31] focuses on asset-dependency modeling, the impact of a risk on business continuity, and the identification and assessment process for existing threats and vulnerabilities, then determining and assessing the level of the risk to identify the required security controls [32].

The three primary steps of the CRAMM ISRA method are: asset identification and valuation, threat and vulnerability assessment, and countermeasure selection and recommendation. These three stages are carried out in two phases: the analysis phase and the management phase [29].

As shown in Figure 3, the analysis phase of CRAMM determines the assets, threats, vulnerabilities, and resulting risks in accordance with these parameters. The management phase handles the risk-reduction countermeasures that will be used, the implementation plan, and the audit stage to track the risks and the efficiency of the countermeasures used [29].

CRAMM risk assessment has the advantages of being tool-supported and having a qualitative risk-analysis approach. However, it has several limitations, such as being very time-consuming, the difficulty of downloading its tool, the difficulty of locating its documentation, and the need for an expert team to execute the risk assessment process [29].

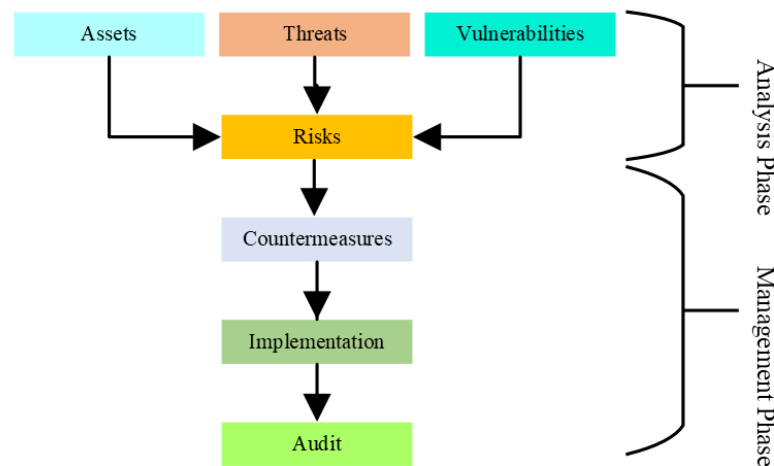


Figure 3. CRAMM risk assessment phases and stages.

3.2. FAIR

Factor Analysis of Information Risk (FAIR) is one of the quantitative and comparative risk assessment methods that focuses on determining accurate probabilities for the frequency of threat occurrence and the magnitude of the potential loss [33]. FAIR focuses on assessing the risk in financial terms by comprehending how time and money affect systems after the occurrence of a security risk [33].

FAIR has its own tool that can be applied to at least one object in the entity. The risk assessment process is then performed by determining the strengths and weaknesses in the current security controls [34]. This step is performed in a quantitative manner by determining the authentication controls, authorization controls, and then the structural integrity [34].

The four primary stages of the FAIR risk assessment methodology are as follows: identify the scenario's elements, evaluate the loss-event frequency, evaluate the probable loss magnitude, and derive and articulate the risk. The first phase of the FAIR risk assessment method focuses on obtaining an identifier for each asset in the system and the community of the threats [34].

The second phase of the FAIR risk assessment method includes estimation of the threat-event frequency and how a threat can affect an asset, measuring the effectiveness of the existing security controls, deriving the potential vulnerabilities, and deriving the loss-event frequency. The third phase involves estimating the worst-case scenario for asset loss. The final phase of the FAIR method is deriving the risk matrix based on the relationships between the probable loss magnitude and loss-event frequency that were determined in the previous phases [34].

The quantitative risk-analysis approach used by the FAIR risk assessment method has the advantage of producing accurate results for the risk assessment process. However, it has a number of drawbacks, including the time required to implement quantitative risk analysis, the comparative risk assessment method's lack of attention to the technical aspects of the system, the lack of documentation required to carry out this risk assessment method, and the absence of a risk-mitigation phase [33].

3.3. CORAS

The Consultative Objective Risk Analysis System (CORAS) is a risk assessment method that adheres to ISO 27005 requirements and complies with ISO 27005 standards [35]. The CORAS risk assessment method is a semi-quantitative, temporal, and object-oriented ISRA method that is built on the unified modeling language (UML) [35]. Its operating approach is based on creating diagrams to represent the connections and interconnections between resources, risks, and threats, as shown in Figure 4 [35].

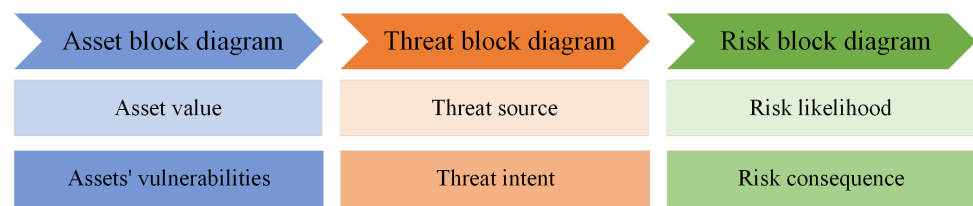


Figure 4. Diagram showing the basic structure of CORAS, which requires creating block diagrams for assets, threats, and risks.

CORAS is made up of the following eight successive steps: readiness for analysis, the target's consumer presentation, enhancing the description of the intended objective with asset diagrams, confirmation of the target description, identifying the risks with threat diagrams, estimating the risk with threat diagrams, risk assessment with risk diagrams, and risk mitigation using a treatment diagram [36].

The "readiness for analysis" step should concentrate on having the resources and information accessible to be administered in the risk assessment procedure. The primary goal of the "target's consumer presentation" is to learn as much as possible from the customer about the system that has to be evaluated, along with any required presumption. Then, asset diagrams are used to pinpoint the crucial assets that are essential for the operation and that need to be safeguarded. To pass the target-description phase, the preset assets must be ranked according to their severity level, likelihood and consequence scales must be determined, and each asset must have a risk-evaluation matrix that distinguishes between desirable and undesirable risks [36].

The main advantages of CORAS are its free tool, the ease with which the method's documentation can be found, and the fact that it is a semi-quantitative risk assessment method that combines the benefits of both quantitative and qualitative risk analysis. In addition, the CORAS risk assessment approach suffers from significant shortcomings, such as the numerous procedures that must be undertaken, their associated time and expense, and the fact that a professional security team is still required to complete the process.

3.4. COBRA

Consultative, Objective, and Bi-functional Risk Analysis (COBRA) is a risk assessment method that is supported by a tool to enhance the risk assessment process [37]. COBRA is an example of a comparative ISRA method that emphasizes the business assets rather than the technical aspects. The three standard processes for using COBRA risk assessment are as follows: questionnaire development, risk surveying, and report preparation [37].

For the first stage, the base questionnaire is built to ascertain the entity's infrastructure design and the user requirements [38]. The second stage involves the client providing clarification and answers to the earlier questionnaires; these responses must be shielded from disclosure. The third stage involves producing risk evaluations and "scores" for specific risk categories, making specific suggestions, offering remedies, and explaining potential business ramifications [38].

While the COBRA risk assessment method has the benefits of having relatively few steps and tool support, it also has several drawbacks, including a lack of implementation documentation and the inability to choose between a quantitative or qualitative risk-analysis approach [38].

3.5. MEHARI

The MEthod for Harmonized Analysis of Risk (MEHARI) is a semi-quantitative ISRA approach based on the, ISO 27001 [31], and ISO 27005 [21] standards. MEHARI can be classified as a scenario-based risk assessment method, as its principle of operation is based on creating multiple scenarios in a database that can be compiled and documented either by using tables or through specialized software [16,39].

The following steps must be considered while implementing a risk assessment task using the MEHARI method. Risk analysis determines the risks' severity levels by identifying the sources of risk inside an entity. A risk assessment is performed to determine whether the current danger may be accepted. To overcome the unaccepted risk, risk treatment is used to determine the best countermeasure approach. Then, the action plan that the entity will use to address any potential risks is executed. Development of an action plan for any additional risks is then found, and the last step is monitoring of the outcomes to determine whether the risk-mitigation approach used is adequate or needs improvement [39,40].

Although the MEHARI risk assessment method has advantages, such as being a free semi-quantitative risk assessment method that is compatible with ISO standards, it also has significant disadvantages, such as the need for a substantial initial risk knowledge base and a challenging MEHARI worksheet that necessitates the use of a skilled security team to conduct the risk assessment process on a given system [16].

3.6. OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is currently a widely used ISRA academic method. OCTAVE methods can be classified into three main subcategories: the OCTAVE, OCTAVE-S, and OA risk assessment methods [41]. The risk in OA can be expressed as follows [41]:

$$\text{Risk} = \text{impact} \times \text{likelihood}. \quad (1)$$

Equation (1) illustrates how to calculate the risk in accordance with the OA risk assessment method, which is the multiplication of the risk's impact by its likelihood of occurrence [41].

For both OCTAVE and OCTAVE-S, the following three stages need to be fulfilled: building asset-based threat profiles, identifying infrastructure vulnerabilities, and developing a security strategy and plans [42]. To identify existing threats, a threat profile is created for each critical asset in the organization using a threat-tree approach [42]. Figure 5 shows the tree structure of the OCTAVE methods, which is used for each asset currently in an organization. The vulnerability, threat agent, attacker purpose, and effect of the attack on the asset are all identified using the tree structure [42].

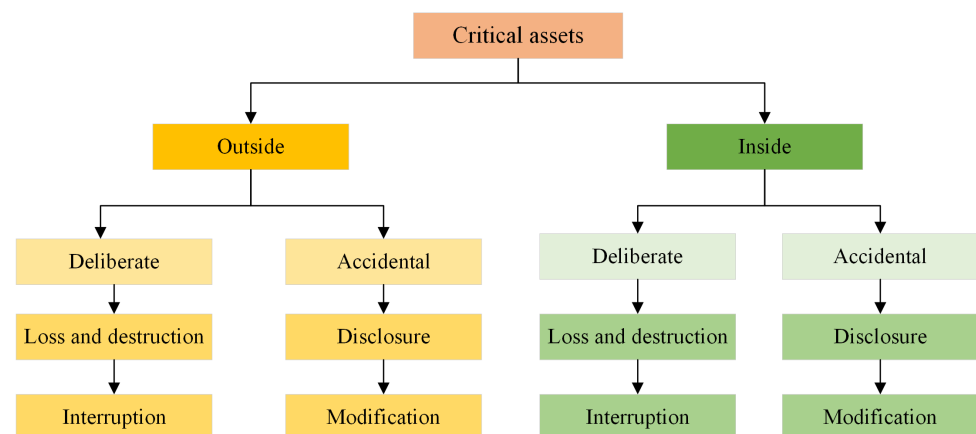


Figure 5. Example of the tree structure for the OCTAVE risk assessment method.

The goal of the OA is the same as that of OCTAVE and OCTAVE-S, but it has the additional benefit of targeting the information assets [43]. The OA applies the container idea to the evaluation procedure. This concept focuses on the information assets, including whether they are used and where they are stored, transported, and processed [43]. The OA differs from the two other OCTAVE risk assessment methods in the number of phases required to perform the risk assessment task: the OA consists of eight steps that are broken down into four phases [43].

The OA risk assessment method's first phase focuses on developing the risk-measurement standards. This step's two main goals are to determine the potential system impact areas and rank those areas according to how important they are to the system. Multiple impact categories, including fines, customer satisfaction, productivity, reputation, and finances, can be included [44].

The OA method's second phase is developing an information-asset profile and identifying an information-asset container. An information-asset profile is created by noting the salient features of every crucial information asset, for instance, the individual who possesses it, the level of safeguarding required, and its importance to the system. Identification of the information-asset container involves focusing on the location of the information assets, and OA introduces the notion of the "container" within which the data resource is retained, conveyed, and manipulated [44].

The OA method's third phase entails identifying areas of concern and threat scenarios. Identifying areas of concern involves focusing on detecting potential threats that may affect each critical asset in the system. Identifying threat scenarios provides more information about the threats that were identified in the previous phase [44]. Threat-scenario identification includes consideration of the threat actor, their motivation, the resulting effect on the information asset, how the information asset's security requirements are breached, and the probability of the occurrence of this threat [44].

The last phase of the OA method for risk assessment is to detect the risks, analyze the risks, and choose mitigation strategies. Detection of the risks focuses on determining the consequences of the threats that are mentioned in the earlier steps on the system or the owner of the critical information asset in a qualitative manner. Analyzing the risks focuses on evaluating the impact of the threat and then calculating a risk score for each impact area [44].

Previous studies have supported the validity of the OA risk assessment technique. For instance, Ali and Awad [24] used the SM, one of an AMI system's home area network (HAN) levels, to apply the eight phases of the OA risk assessment technique. Their study identified ten risk scenarios using this technique. Some examples of the risks that were identified included information exposure, user impersonation, DoS attacks, and identity theft. Zia and Chauhan [43] used smart houses, a component of AMI systems, to validate the OA approach. Their article primarily focused on web-related attacks that took advantage of the weakness of remote connections to smart devices from the client side.

The main benefits of the OA risk assessment method are its ease of use, the availability of free and open-source documentation that can be used to follow the risk assessment procedures, the use of both quantitative and qualitative approaches in risk assessment tasks, and the lack of a requirement for external experts to perform the risk assessment task on an entity. However, there are many steps that must be taken, which adds time and expense [44].

Table 2 compares the aforementioned risk assessment methods based on a variety of factors, including the integration of threats and vulnerabilities, data assets, software assets, hardware assets, service assets, integration of the CIA security attributes, simplicity, the method's intended use, the cost and accessibility of its documentation, tool support, standards compliance, the type of approach, the level of expertise required, and the method type. This table demonstrates that the CRAMM, CORAS, FAIR, and COBRA risk assessment methods are supported by tools and provide additional benefits. Furthermore, it has been demonstrated that CRAMM and OA support the data assets, software assets, and hardware assets—essential components of AMI-system risk assessment.

Table 2. Comparison between the existing risk assessment methods.

Criteria	CRAMM	FAIR	CORAS	COBRA	MEHARI	OA
Threat and vulnerability integration	Supported	N/A	Supported	Not supported	N/A	Supported
Including critical assets	Not supported	N/A	Supported	N/A	N/A	Supported
Data assets	Supported	N/A	N/A	N/A	N/A	Supported
Software assets	Supported	N/A	N/A	N/A	N/A	Supported
Hardware assets	Supported	N/A	N/A	N/A	N/A	Supported
Service assets	Supported	N/A	N/A	N/A	N/A	Supported
CIA integration	Does not clearly talk about the security attributes	N/A	Included	Does not clearly talk about the security attributes	N/A	Included
Simplicity	Systematic analysis	N/A	Uses no mathematical equations	N/A	N/A	Uses no mathematical equations
Purpose of the method	N/A	Commercial	N/A	N/A	Commercial	Academic
Price and availability of documentation	Expensive and not available	Expensive	Expensive	N/A	N/A	Free
Tool supported	Supported	Supported	Supported	Supported	N/A	Not supported
Standards compliance	Yes	No	Yes	No	Yes	No
Risk-analysis approach	Qualitative	Quantitative	Qualitative	N/A	Qualitative & Quantitative	Qualitative & Quantitative
Level of expertise required	High-level expert	N/A	UML and Security team	N/A	N/A	Internal team
Method type (temporal, functional, comparative)	N/A	N/A	Functional	N/A	N/A	Functional

4. AMI Risk Assessment Requirements

AMI is a major component of an SG. It is represented by a network that connects IEDs, SMs, and DCs, which are linked through either the HAN or NAN [45]. These devices are then connected to the ESP's control center via wide area networks (WANs). The main item in the ESP's data center is the MDMS, which is used to observe and control the data received from the end devices [45]. Numerous communication methods that employ wired or wireless technologies are used to interact between the MDMS and end devices [45].

An AMI system provides advanced features to the traditional electricity grid, such as energy tracking, data gathering, load management, and sophisticated control features [46]. These features enhance the performance of the grid and thus enable its customers to easily manage their electricity usage. The major objectives of an AMI system are to collect the data from the end customers, send it to the ESP to be further analyzed, and send control commands from the ESP to the end devices such as a DC or SM for remote management, updating firmware, or remotely shutting down power [46].

Due to the significant role of AMI systems and their high level of criticality, risk assessment procedures must be implemented to identify their current vulnerabilities, possible threats, and the influence of such dangers upon their performance. The risks will then be reduced to an acceptable level for an AMI system's regular functioning using mitigation techniques.

As demonstrated in Figure 6, the first step in applying a risk assessment process to any system is the risk-identification step, which focuses on identifying the primary critical resources within the system that necessitate evaluation; this is considered the major step in any risk assessment process [16]. Thus, determining the primary and crucial assets for an

AMI system is the main aim of this section, which will be used further for determining the main requirements for assessing the potential risks to an AMI.

An AMI system’s assets are defined as the items that need to be protected, are targeted to be exposed, and could negatively affect the overall performance and objective of the AMI [47]. An AMI system’s assets can be divided into intangible and tangible assets. An AMI’s tangible assets start from the end customers in the entity, which are homes or industrial premises, and data from these pass through the SM, DC, and MDMS in the data center of the ESP [48]. Another vital asset of an AMI system is the data that are transferred through the communication links or exist on the SM, DC, and MDMS, which can be represented by the firmware [48]. Intangible assets can be represented by the ESP’s reputation, which may be affected by the availability and confidentiality security attributes [48].

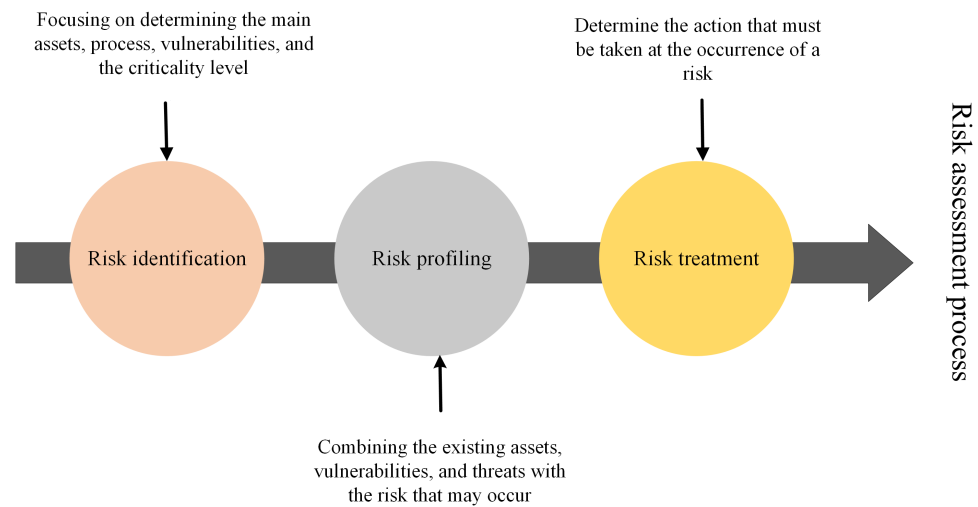


Figure 6. The three primary phases of risk assessment are risk identification, risk profiling, and risk treatment.

An AMI system’s assets can be classified into three main categories, as shown in Table 3. These are information and data assets, resource assets, and service assets [49]. Information assets for an AMI system can be determined as the audit data, the information about the energy usage by the customers, any policies or configurations in the MDMS of the ESP, locally protected information in the main data center, and the data that are transmitted, whether through the HAN, NAN, or WAN [49].

Table 3. Major assets of an AMI system that should be included in any risk assessment process.

Asset Type	Examples
Information and data assets	<ul style="list-style-type: none"> — Audit data. — Customer energy-consumption data. — Existing policies and configuration in the MDMS. — Local data existing in the data center.
Resource assets	<ul style="list-style-type: none"> — SMs. — DCs. — Bidirectional communication links. — Software and applications installed in the MDMS. — Smart appliances in the customer domain. — Tokens used for the authentication process and access control services.
Service assets	<ul style="list-style-type: none"> — Public-key infrastructure service. — Remote configuration service. — Phishing attacks. — Initialization steps that are performed for the SM. — Access-control services. — Confidentiality, integrity, accountability, and availability.

The AMI resource assets can be represented by the main AMI components, which are SMs, DCs, and communications links. The installed software and applications in the ESP's data center are considered as AMI resource assets [50]. They also include other hardware existing in the AMI system, such as smart appliances on the customer side and any hardware in the main data center that is essential for the operation of the AMI. Finally, if tokens are used in the AMI system for authenticating customers, these are also included in the AMI resource assets [50].

The service assets of an AMI may include the public-key infrastructure service, which can be used as an authentication technique for the system's fundamental elements. Remote upgrading and configuring of the firmware of SMs or DCs is an AMI service [50]. The initialization steps that are performed for a SM can also be included as an AMI service asset. The access-control services, whether those protecting the MDMS in the main data center or those protecting the end devices from unauthorized access, are also service assets [50]. The main services that are provided by the AMI are the CIA services that can be provided to secure the customer data [1]. The availability of the system and the primary security services that are applied by the main data center administrator also can be included as AMI service assets [1].

5. Appropriate Risk Assessment Method for an AMI System

Determination of the most appropriate risk assessment method to apply to an AMI system is the main contribution of this paper. Table 4 presents a matching of the main requirements for applying a risk assessment method to an AMI system and the capabilities of each risk assessment method.

Table 4. Comparison of the capabilities of the ISRA methodologies with the criteria for risk assessment of an AMI system.

AMI RA Requirement	CRAMM	FAIR	CORAS	COBRA	MEHARI	OA
Audit data	Supported	N/A	N/A	N/A	N/A	Supported
Customer energy-consumption data	Supported	N/A	N/A	N/A	N/A	Supported
Existing policies and configuration in the MDMS	Supported	N/A	N/A	N/A	N/A	Supported
Customer energy-consumption data	Supported	N/A	N/A	N/A	N/A	Supported
Locally existing data in the data center	Supported	N/A	N/A	N/A	N/A	Supported
Smart appliances in the customer domain	Supported	N/A	N/A	N/A	N/A	Supported
CIA integration	Does not clearly talk about the security attributes	N/A	Does not clearly talk about the security attributes	Does not clearly talk about the security attributes	N/A	Considers the CIA attributes
AMI hardware assets	Supported	N/A	N/A	N/A	N/A	Supported
Risk-analysis approach	Qualitative	Quantitative	Qualitative	N/A	Qualitative and Quantitative	Qualitative and Quantitative

As demonstrated in Table 4, the OA method is the only approach that fully complies with the AMI risk assessment requirements; the other methods only comply partially with these requirements. The OA method is thus found to be the most suitable risk assessment approach for an AMI system for the following reasons:

- The OA focuses mainly on the management of information assets, and it encompasses an evaluation of the various information containers, including hardware, databases, and human resources. The OA also focuses on information assets wherever they are stored, transported, or processed, locations that are distributed in AMI systems.
- The OA is an academic risk assessment approach and a temporal risk assessment method that targets technical security issues and requires a good understanding of the system, which is necessary for performing a risk assessment for an AMI system.

- The OA can be used to assess the data assets, software assets, and service assets, which are the main critical assets related to an AMI system. The main benefits of the OA are its documentation accessibility, its independence from outside specialists, and its simplicity, which make it appropriate for use with the AMI system.
- The operation of an AMI system depends on the three primary security characteristics that are commonly recognized and prioritized in information security—confidentiality, integrity, and availability—and these are already integrated within the OA risk assessment method.
- The OA integrates both qualitative and quantitative risk-analysis approaches, which increases the accuracy of its results and adds value to the risk assessment of an AMI.

6. Conclusions and Future Work

Risk assessment is essential for any critical infrastructure such as an AMI system. It is vital to assess the possible hazards linked to an AMI system because of the enormous amount of data transiting through it and its high level of confidentiality. This task is performed by identifying its existing vulnerabilities, its critical assets, threats, the likelihood of risks occurring, and the consequences of an attack on the AMI system.

There are numerous ISRA approaches that are already in use today. Therefore, this study sought to identify the most appropriate risk assessment method for AMI networks. This article has presented an overview of the characteristics of several ISRA methods and the parameters required to assess the possible risks to an AMI system. Matching between the capabilities of each aforementioned ISRA method and the parameters required to assess an AMI system was performed to determine the most appropriate ISRA method that fully complies with these requirements.

The OA risk assessment approach was identified as the most well-suited method, as it supports audit assets, data assets, information assets, and hardware assets, which are fundamental to the AMI risk assessment requirements. Furthermore, it is a free method, and the easy accessibility of its documentation is an additional advantage. Moreover, the OA method complies with the CIA security attributes, which are essential for assessing the potential risks to an AMI system. It also considers both the tangible and intangible assets of AMI systems.

Future work will focus on applying the OA risk assessment approach to AMI systems, including identifying the crucial resources of an AMI, and its existing vulnerabilities, threats, and threat agents. Later, an assessment of the existing security controls will be performed to choose the most appropriate risk-treatment approach.

Author Contributions: The work presented here was performed in a collaboration involving all the authors. Conceptualization, A.I.A., M.K.A.-E. and A.A.M.K.; Investigation, M.S., A.I.A., M.K.A.-E. and A.A.M.K.; Formal Analysis, M.S.; Writing—Original Draft Preparation, M.S., A.I.A., M.K.A.-E. and A.A.M.K.; Writing—Review and Editing, M.S., A.I.A., M.K.A.-E. and A.A.M.K.; Visualization, M.S.; Research Supervision, A.I.A., M.K.A.-E. and A.A.M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by a joint research grant between United Arab Emirates University and Zayed University (UAEU-ZU). Grant number: 12R141.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Bae, M.; Kim, K.; Kim, H. Preserving privacy and efficiency in data communication and aggregation for AMI network. *J. Netw. Comput. Appl.* **2016**, *59*, 333–344. [[CrossRef](#)]
2. Fenz, S.; Heurix, J.; Neubauer, T.; Pechstein, F. Current challenges in information security risk management. *Inf. Manag. Comput. Secur.* **2014**, *22*, 410–430. [[CrossRef](#)]
3. Barrett, M.P. *Framework for Improving Critical Infrastructure Cybersecurity*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2018. [[CrossRef](#)]
4. Shameli-Sendi, A.; Aghababaei-Barzegar, R.; Cheriet, M. Taxonomy of information security risk assessment (ISRA). *Comput. Secur.* **2016**, *57*, 14–30. [[CrossRef](#)]
5. Nagasree, Y.; Rupa, C.; Akshitha, P.; Srivastava, G.; Gadekallu, T.R.; Lakshmana, K. Preserving Privacy of Classified Authentic Satellite Lane Imagery Using Proxy Re-Encryption and UAV Technologies. *Drones* **2023**, *7*, 53. [[CrossRef](#)]
6. Hansen, A.; Staggs, J.; Sheno, S. Security analysis of an advanced metering infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2017**, *18*, 3–19. [[CrossRef](#)]
7. Sgouras, K.I.; Kyriakidis, A.N.; Labridis, D.P. Short-term risk assessment of botnet attacks on advanced metering infrastructure. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 143–151. [[CrossRef](#)]
8. Yao, J.; Venkatasubramanian, P.; Kishore, S.; Snyder, L.V.; Blum, R.S. Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks. In Proceedings of the 2017 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 22–24 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6. [[CrossRef](#)]
9. Agrawal, V. A Comparative Study on Information Security Risk Analysis Methods. *J. Comput.* **2017**, *12*, 57–67. [[CrossRef](#)]
10. *SP 800-37; Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. National Institute of Standards & Technology (NIST): Gaithersburg, MD, USA, 2018. [[CrossRef](#)]
11. *SP 800-39; Managing Information Security Risk: Organization, Mission, and Information System View*. National Institute of Standards & Technology (NIST): Gaithersburg, MD, USA, 2011. [[CrossRef](#)]
12. *ISO 31000; Risk Management*. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
13. White, G.B.; Sjin, N. The NIST Cybersecurity Framework. In *Research Anthology on Business Aspects of Cybersecurity*; IGI Global: Hershey, PA, USA, 2022; pp. 39–55. [[CrossRef](#)]
14. Smolenski, R.; Szczesniak, P.; Drozd, W.; Kasperski, L. Advanced metering infrastructure and energy storage for location and mitigation of power quality disturbances in the utility grid with high penetration of renewables. *Renew. Sustain. Energy Rev.* **2022**, *157*, 111988. [[CrossRef](#)]
15. Derakhshandeh, S.; Mikaeilvand, N. New Framework for Comparing Information Security Risk Assessment Methodologies. *Aust. J. Basic Appl. Sci.* **2011**, *5*, 160–166.
16. Kuzminykh, I.; Ghita, B.; Sokolov, V.; Bakhshi, T. Information Security Risk Assessment. *Encyclopedia* **2021**, *1*, 602–617. [[CrossRef](#)]
17. Pandey, S.K. A comparative study of risk assessment methodologies for information systems. *Bull. Electr. Eng. Inform.* **2012**, *1*, 111–122. [[CrossRef](#)]
18. Shokry, M.; Awad, A.I.; Abd-Ellah, M.K.; Khalaf, A.A.M. Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Gener. Comput. Syst.* **2022**, *136*, 358–377. [[CrossRef](#)]
19. Shokry, M.; Awad, A.I.; Abd-Ellah, M.K.; Khalaf, A.A.M. CORAS Model for Security Risk Assessment in Advanced Metering Infrastructure Systems. In Proceedings of the 8th International Conference on Advanced Intelligent Systems and Informatics, Cairo, Egypt, 20–22 November 2022; Springer: Cham, Switzerland, 2023; pp. 449–459. [[CrossRef](#)]
20. Borenius, S.; Gopalakrishnan, P.; Bertling Tjernberg, L.; Kantola, R. Expert-Guided Security Risk Assessment of Evolving Power Grids. *Energies* **2022**, *15*, 3237. [[CrossRef](#)]
21. *ISO/IEC 27005:2018; Information Technology-Security Techniques-Information Security Risk Management*. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
22. Baig, Z.; Zeadally, S. Cyber-Security Risk Assessment Framework for Critical Infrastructures. *Intell. Autom. Soft Comput.* **2019**, *25*, 121–129. [[CrossRef](#)]
23. Haider, M.H.; Saleem, S.B.; Rafaqat, J.; Sabahat, N. Threat modeling of wireless attacks on advanced metering infrastructure. In Proceedings of the 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 14–15 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6. [[CrossRef](#)]
24. Ali, B.; Awad, A.I. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817. [[CrossRef](#)] [[PubMed](#)]
25. Line, M.B.; Johansen, G. Assessing information security risks of AMI: What makes it so difficult? In Proceedings of the 2015 International Conference on Information Systems Security and Privacy (ICISSP), Angers, France, 9–11 February 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 56–63. [[CrossRef](#)]
26. Shawly, T.; Liu, J.; Burow, N.; Bagchi, S.; Berthier, R.; Bobba, R.B. A risk assessment tool for advanced metering infrastructures. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 989–994. [[CrossRef](#)]
27. McIlwraith, A. *Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness*; Routledge: Oxford, UK, 2021.

28. Aksu, M.U.; Dilek, M.H.; Tatlı, E.İ.; Bicakci, K.; Dirik, H.I.; Demirezen, M.U.; Aykır, T. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8. [[CrossRef](#)]
29. Mullerova, J.; Nemeč, V. Risk assessment RM/RA CRAMM—quantitative method for environmental, technology and social threats. *Int. Multidiscip. Sci. GeoConf. SGEM* **2019**, *19*, 279–285. [[CrossRef](#)]
30. Faris, S.; Ghazouani, M.; Medromi, H.; Sayouti, A. Information security risk assessment—A practical approach with a mathematical formulation of risk. *Int. J. Comput. Appl.* **2014**, *103*, 36–42. [[CrossRef](#)]
31. *ISO/IEC 27001*; Information Security Management Systems. International Organization for Standardization (ISO): Geneva, Switzerland, 2022.
32. Mullerova, J.; Orincak, M. RM/RA CRAMM-quantitative risk assessment method for prevention of criminality. *Secur. Dimens.* **2017**, *23*, 131–144. [[CrossRef](#)]
33. Csóka, P.; Pintér, M. On the impossibility of FAIR risk allocation. *J. Theor. Econ.* **2016**, *16*, 143–158. [[CrossRef](#)]
34. Zhang, S.; Li, J.; Li, Y.; Zhang, X. Revenue risk allocation mechanism in public-private partnership projects: Swing option approach. *J. Constr. Eng. Manag.* **2021**, *147*, 04020153. [[CrossRef](#)]
35. Gritzalis, D.; Stergiopoulos, G.; Vasilellis, E.; Anagnostopoulou, A. Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud? In *Advances in Core Computer Science-Based Technologies*; Springer: Cham, Switzerland, 2021; pp. 109–128. [[CrossRef](#)]
36. Li, Q.; Yin, X.; Meng, S.; Liu, Y.; Ying, Z. A security event description of intelligent applications in edge-cloud environment. *J. Cloud Comput.* **2020**, *9*, 23. [[CrossRef](#)]
37. Welty, C.J.; Sanford, T.H.; Wright, J.L.; Carroll, P.R.; Cooperberg, M.R.; Meng, M.V.; Porten, S.P. The Cancer of the Bladder Risk Assessment (COBRA) score: Estimating mortality after radical cystectomy. *Cancer* **2017**, *123*, 4574–4582. [[CrossRef](#)] [[PubMed](#)]
38. Mt-Isa, S.; Ouwens, M.; Robert, V.; Gebel, M.; Schacht, A.; Hirsch, I. Structured benefit–risk assessment: A review of key publications and initiatives on frameworks and methodologies. *Pharm. Stat.* **2016**, *15*, 324–332. [[CrossRef](#)]
39. MEHARI 2010: Risk Analysis and Treatment Guide. Club de la Sécurité de l’Information Français (CLUSIF). Available online: <https://clusif.fr/wp-content/uploads/2015/10/mehari-2010-risk-analysis-and-treatment-guide.pdf> (accessed on 9 April 2023).
40. Rivai, M.A.; Suroso, J.S.; Pangemanan, F. Review of the risk analysis using MEHARI model: The guideline to analyze risk for startup educational platform. In Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 13–14 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 577–582. [[CrossRef](#)]
41. Suroso, J.S.; Fakhrozi, M.A. Assessment of information system risk management with octave allegro at education institution. *Procedia Comput. Sci.* **2018**, *135*, 202–213. [[CrossRef](#)]
42. Alfariši, S.; Surantha, N. Risk assessment in fleet management system using OCTAVE Allegro. *Bull. Electr. Eng. Inform.* **2022**, *11*, 530–540.
43. Zia, A.B.; Chauhan, M.K. A research paper on internet of things based upon smart homes with security risk assessment using OCTAVE Allegro. *Int. J. Eng. Res. Technol.* **2020**, *9*, 940–948. [[CrossRef](#)]
44. Suroso, J.S.; Januanto, A.; Retnowardhani, A. Risk Management of Debtor Information System At Bank XYZ Using OCTAVE Allegro Method. In Proceedings of the 2019 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 9–10 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 261–265. [[CrossRef](#)]
45. Ghasempour, A.; Gunther, J.H. Finding the optimal number of aggregators in machine-to-machine advanced metering infrastructure architecture of smart grid based on cost, delay, and energy consumption. In Proceedings of the 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016; pp. 960–963. [[CrossRef](#)]
46. Ghasempour, A. Optimized advanced metering infrastructure architecture of smart grid based on total cost, energy, and delay. In Proceedings of the 2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Las Vegas, NV, USA, 9–12 January 2016; pp. 1–6. [[CrossRef](#)]
47. Hägerling, C.; Kurtz, F.M.; Olsen, R.L.; Wietfeld, C. Communication architecture for monitoring and control of power distribution grids over heterogeneous ICT networks. In Proceedings of the 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, Croatia, 13–16 May 2014; pp. 838–845. [[CrossRef](#)]
48. Alfakeeh, A.S.; Khan, S.; Al-Bayatti, A.H. A Multi-User, Single-Authentication Protocol for Smart Grid Architectures. *Sensors* **2020**, *20*, 1581. [[CrossRef](#)]
49. Díaz Redondo, R.P.; Fernández-Vilas, A.; Fernández dos Reis, G. Security Aspects in Smart Meters: Analysis and Prevention. *Sensors* **2020**, *20*, 3977. [[CrossRef](#)]
50. Pesesky, J.L. The Vulnerabilities of the Advanced Metering Infrastructure in the Smart Grid. Ph.D. Thesis, Utica College, Utica, NY, USA, 2016.

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