Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 55-40 (2022) 277–282

A Risk Assessment Framework for Critical Infrastructure Based on the Analytic Hierarchy Process

Fioravanti, C. [*] **Guarino, S.** [*] **Mazzá, B.** [*] **Nobili, M.** [*]
Santucci, F. [*] **Ansaldi, S. M.** [**]

[*] *Unit of Automatic Control, Department of Engineering,*
Universitá Campus Bio-Medico di Roma, via Álvaro del Portillo 21,
00128, Rome, Italy.
(e-mail: {c.fioravanti,s.guarino,bianca.mazza,m.nobili,f.santucci}@unicampus.it).
[**] *Department of Technological Innovation, INAIL Italian National*
Institute for Insurance against Accidents at Work, Via di Fontana
Candida, 1, 00078, Monte Porzio Catone (Rome), Italy.
(e-mail:s.ansaldi@inail.it)

Abstract: Due to their essential role, critical infrastructures (e.g., water, gas, and power distribution systems) are subject to persistent monitoring in order to ensure their operational continuity. Because of this, they constitute appealing targets for malicious attackers who carry out physical or cyber attacks with the aim of compromising such critical systems. In this work, we provide a novel framework for an enhanced risk assessment process for critical infrastructures, which is based on the Analytic Hierarchy Process. Specifically, the proposed solution consists of a quantitative framework for site-specific risk assessment, and follows an approach designed to consider the presence of heterogeneous subsystem characterized by different degree of relevance in the infrastructures. A simulation campaign is carried out in a test-range environment, which emulates the behaviour of a water treatment system, in order to prove the effectiveness of the approach.

Keywords: Critical Infrastructures, Risk Assessment, Cyber Attacks.

1. INTRODUCTION

As it has been dramatically observed in several situations, critical infrastructures (e.g., power, gas or water distribution systems) are often subject to destructive phenomena connected to natural disasters (e.g., the Hurricane Kathrina Knabb et al. (2005), or the meteorite impact in Chelyabinsk Oroian (2010)), to accidental (e.g. the 2003 power outages in the U.S. and in Italy Atputharajah and Saha (2009)), or intentional circumstances (the 2015 and 2016 Ukraine power outages Liang et al. (2016); Setola et al. (2019), or the Colonial Pipeline cyberattack Smith (2022)). Because of this, such systems are at risk of cascading failures that can lead to full or partial disruption of services provided to the population, with dramatic and often life-threatening consequences. To reduce the risk and mitigate the consequences, an effective model of structural and functional interdependencies should be provided (see, Filippini and Silva (2014)). Therefore, effective protection strategies should be developed to prioritize the protection of different sites and components with respect to heterogeneous threats and environments. To this end, it is essential to identify appropriate metrics and indicators by comparatively assessing the criticality and vulnerability of the different elements, especially in heterogeneous contexts.

1.1 Related works

This issue has been recognized by regulators; Khakzad et al. (2017) stressed the need to develop methodologies aimed at assessing the security risk evaluation in critical infrastructures, supporting the scientifically based identification of weak links, and prioritising the risk management resources. Moreover, Kornecki and Zalewski (2010) highlighted the need to address the potential impacts of software within the framework of safety studies.

Nevertheless, general methods for Risk Assessment or Vulnerability Assessment (e.g., VAM-CF (for Chemical Process Safety Staff (2003)), CCPS (Moore (2013)) and API RP 780 Zhu and Liyanage (2021)) provide limited support to the identification and management of cyber-risks. The ISO/IEC 27000, related to security analysis of a computer system and the ISA/IEC 62443, specific for industrial control systems, are not concerned with the distinctive features of the process industry (dynamics of the physical process units, behavior of hazardous materials, etc.). Despite the conspicuous importance of such analyses, some simplified assumptions are frequently adopted (e.g., considering impacts from the safety assessment) leading to incorrect conclusions. As mentioned by Zhu and Liyanage (2021), in the context of cybersecurity of offshore oil&gas production assets, there are many aspects related to organizational issues, human factors, and decision culture,

[*] This work was supported by Italian National Project "DRIVERS: Approccio combinato data-driven ed experience-driven all'analisi del rischio sistemico" funded by INAIL under grant n. BRIC2021-ID03.

2405-8963 Copyright © 2022 The Authors. This is an open access article under the CC BY-NC-ND license.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2023.01.085

which play pivotal roles during the planning, implementation, and assurance of cybersecurity. Hashimoto et al. (2013) developed a systematic approach to evaluate the detectability of process plant manipulations, but the identification of the specific set of manipulations is out of the scope of the method. Abdo et al. (2018) proposed an approach that allows the assessment of vulnerabilities and hacking techniques for control systems, but do not contribute to the evaluation of their impact on the process system. Recently, Iaiani et al. (2021) introduced methods, based on a reverse-HazOp concept, for the identification of consequences due to malicious manipulations on the control system of chemical plants. Still, novel strategies based on dynamic process simulation (Fang et al. (2020)), dynamic risk analysis (Hu et al. (2021)) and big data (Pasman et al. (2018)), applied so far only in the domain of process safety, have a promising potential for adaptation in the framework of cybersecurity issues. Other conventional approaches based on (i) reliability analysis (Lees (2012)), (ii) multi criteria-analysis (Faramondi et al. (2020), Bernieri et al. (2016), Oliva et al. (2021), Aminbakhsh et al. (2013)), (iii) optimization problems (Faramondi et al. (2016)), as well as innovative approaches based on (i) Bayesian network analysis (Hu et al. (2021)), (ii) human reliability assessment (Gertman and Blackman (1993)), can be considered to strike a balance between priorities in different domains. Nevertheless, the systematic use of such approaches, in supporting the design of barrier systems, has been limited to some pioneering studies and should be further explored.

1.2 Contribution

In this work, we provide a novel framework for risk assessment based on the Analytic Hierarchy Process (AHP) which is applicable in the context of critical infrastructures. Since the definition of the severity degree associated with each risk item is a critical aspect of risk analysis, the proposed approach is based on the idea of decomposition, thus defining a hierarchical structure as a support for the decision maker. The aim of the hierarchical structure is to consider multiple class of hazards due to several threats, such as physical attacks, cyber attacks, or cyber-physical attacks, i.e., attacks able to compromise the infrastructure from a physical perspective. Specifically, we provide a preliminary analysis focused on categorizing the multiple subsystems that characterize the infrastructure (e.g., the IT subsystem, the OT subsystem, etc). Then, AHP evaluates the extent of the relevance of auxiliary subsystems, to identify which are not essential to the delivery of the critical services. The outline of the paper is as follows: In Section 2 we provide some preliminary definitions about the AHP. In Section 3 we formalize the proposed framework for the estimation of the severity values for each risk item. Simulation and discussions are collected in Section 4 with the aim to validate the proposed framework; finally some conclusive comments are reported in Section 5.

2. PRELIMINARIES

2.1 Notation

We denote vectors by boldface lowercase letters and matrices with uppercase letters and we refer to the (i, j)-th entry of a matrix A by A_{ij}. Let A be an $n \times n$ square matrix, we denote by $\lambda_n\{A\}$ the eigenvalue of A with largest magnitude (e.g., the dominant eigenvalue of a matrix with just positive coefficients).

2.2 The Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP), introduced by Saaty [26], is an effective tool for dealing with complex decisions and supports decision makers in prioritizing decisions among n alternatives. The process is based on the reduction of complex decisions to a series of pairwise comparisons and then synthesising the results, the AHP helps to capture both subjective and objective aspects of a decision. Let us suppose that each alternative i is characterized by an unknown positive value $\mathbf{w}_i > 0$ that represents its utility or relevance. In the context of AHP, decision makers try to identify the unknown values $\mathbf{w}_i$ on the basis of the estimation of the ratios $\mathbf{w}_i/\mathbf{w}_j$ between each pair of alternatives, which are summarised in the $n \times n$ pairwise comparison matrix (PCM) W. Such an approach is typical in contexts involving human decision-makers who usually prefer to make relative comparisons between the utilities of the different alternatives (e.g. "*Alternative A is twice as good as Alternative B* ") rather than directly assessing the utility of each alternative (i.e. "*The utility of Alternative A is x*"). In this paper, we assume that the entries $W_{ij} > 0$ represent an estimate of the ratio $\mathbf{w}_i/\mathbf{w}_j$ and are usually defined according to the well known Saaty's scale (Saaty (1977)) summarized in Table 1. Moreover, for all the entries W_{ij}, it is assumed that $W_{ji} = W_{ij}^{-1}$, i.e., the terms W_{ji} and W_{ij} are *locally consistent* and satisfy $W_{ij}W_{ji} = 1$.

When a decision maker provides his/her relative judgements in a PCM, it is essential to evaluate the inconsistency of the given relative ratios. In particular, according to Saaty (1977), highly inconsistent PCM result in unreliable rankings and should not be considered. Saaty, in the same work, introduces the most used approach for the evaluation of inconsistency degree in PCMs. The *Consistency Index* is based on the dominant eigenvalue of the PCM:

$$CI(W) = \frac{\lambda_n\{W\} - n}{n - 1}, \tag{1}$$

where n is the number of alternatives. Moreover, Saaty proposed to normalize such index with respect to the so-called *Random Index* RI_n which is the average $CI(W)$ computed by considering a large number of random complete pairwise comparison matrices of degree n, thus obtaining the *Consistency Ratio* as:

$$CR(W) = \frac{CI(W)}{RI_n} \tag{2}$$

If the value of Consistency Ratio is smaller or equal to 10%, the inconsistency is deemed acceptable and the absolute utility estimation process is applicable, if instead CR is greater than such threshold, it is suggested to revise the subjective judgment in order to reduce such inconsistency.

In particular, the approach proposed by Saaty relies on the fact that ideally, if W_{ij} is exactly equal to the ratio $\mathbf{w}_i/\mathbf{w}_j$, the dominant eigenvector of W is exactly the vector $\mathbf{w} = [\mathbf{w_1}, \ldots, \mathbf{w_n}]^{\mathbf{T}}$ except for a scaling factor. However, realworld data are usually characterised by inconsistencies; to give an example, Alternative A is three times better than Alternative B, and Alternative B is twice better than Alternative C, but Alternative A is three times better than C, hence the preferences are not transitive. In this case, there is no vector $\mathbf{w}$, such that $W_{ij} = \mathbf{w}_i/\mathbf{w}_j$, and we have to resort to approximate approaches. Among other approaches to solve this problem, one of the most effective method is the Logarithmic Least-Squares approach (LLS), where the aim is the identification of the vector $\mathbf{w}^*$ that solves

$$\mathbf{w}^* = \underset{x \in \mathbb{R}^n_+}{\operatorname{argmin}} \left\{ \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \left(\ln(W_{ij}) - \ln\left(\frac{\mathbf{x}^*_i}{\mathbf{x}^*_j}\right) \right)^2 \right\}. \quad (3)$$

An effective strategy to solve the above problem is to operate the substitution $\mathbf{z} = \ln(\mathbf{x})$, where $\ln(\cdot)$, is the component-wise logarithm, so that Equation (3) can be rearranged as:

$$\mathbf{w}^* = \exp\left(\underset{z \in \mathbb{R}^n_+}{\operatorname{argmin}} \left\{ \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \left(\ln(W_{ij}) - z_i + z_j \right)^2 \right\} \right), \quad (4)$$

where $\exp(\cdot)$ is the component-wise exponential.

3. RISK ASSESSMENT FRAMEWORK

The proposed framework addresses the problem of prioritizing the relevance of heterogeneous risk items by transforming a decision problem into a hierarchy of more easily comprehended sub-problems, each of which can be analyzed independently. A preliminary decomposition of the problem allows to characterize the heterogeneous subsystems of the infrastructure which require an adequate and customized approach for the risk evaluation. We define as

$$\mathbb{S} = \{\mathbb{S}_1, \ldots, \mathbb{S}_{n_s}\}$$

the set of the subsystems $\mathbb{S}_i$ which composes the infrastructure. Furthermore, we consider a second layer of the hierarchical structure in order to take into account the presence of multiple classes of potential hazards

$$\mathcal{H} = \{\mathcal{H}_1, \ldots, \mathcal{H}_{n_h}\};$$

moreover, each class of hazards $\mathcal{H}_i \in \mathcal{H}$ is characterized by a set of compatible attacks (or threats)

$$\mathcal{H}_i = \{\mathcal{A}^i_1, \ldots, \mathcal{A}^i_{n_a}\}.$$

Once the hierarchy structure (see Figure 1) is determined, the experts assign a relative value to each pair of alternatives by defining pairwise comparison with respect to their relevance on the element placed in the higher level in the hierarchy structure. Let S be the $n_s \times n_s$ comparison matrix, where each entry S_{ij} represents the relative relevance of the subsystem $\mathbb{S}_i$ with respect to the subsystem $\mathbb{S}_j$. The goal is to obtain an absolute evaluation of the relevance $\mathbf{s}_i$ of each subsystem $\mathbb{S}_i$ via AHP solving Equation (4). Similarly, let H^z be the $n_h \times n_h$ PCM whose elements $H^z{}_{ij}$ represent the ratio between the relevance of two classes of hazards $\mathcal{H}_i$ and $\mathcal{H}_j$, in the particular subsystem $\mathbb{S}_z \in \mathbb{S}$. Also in this case we apply AHP via Equation (4) in order to obtain an absolute estimation $\mathbf{h}^z_i$ of the hazard $\mathcal{H}_i$ in a specific subsystem $\mathbb{S}_z$. Finally, for each class of hazard $\mathcal{H}_k$ we respectively define the relative relevance of the potential attacks or threats related to the particular hazard in order to better analyze the risks.

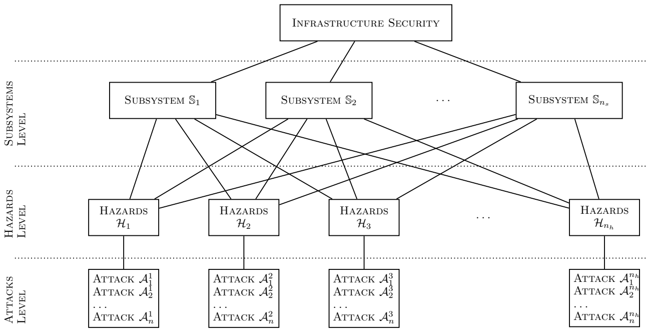
INFRASTRUCTURE SECURITY
SUBSYSTEMS LEVEL
SUBSYSTEM $\mathbb{S}_1$
SUBSYSTEM $\mathbb{S}_2$
...
SUBSYSTEM $\mathbb{S}_{n_s}$
HAZARDS LEVEL
HAZARDS $\mathcal{H}_1$
HAZARDS $\mathcal{H}_2$
HAZARDS $\mathcal{H}_3$
...
HAZARDS $\mathcal{H}_{n_h}$
ATTACKS LEVEL
ATTACK $\mathcal{A}^1_1$ ATTACK $\mathcal{A}^1_2$ ... ATTACK $\mathcal{A}^1_n$
ATTACK $\mathcal{A}^2_1$ ATTACK $\mathcal{A}^2_2$ ... ATTACK $\mathcal{A}^2_n$
ATTACK $\mathcal{A}^3_1$ ATTACK $\mathcal{A}^3_2$ ... ATTACK $\mathcal{A}^3_n$
ATTACK $\mathcal{A}^{n_h}_1$ ATTACK $\mathcal{A}^{n_h}_2$ ... ATTACK $\mathcal{A}^{n_h}_n$

Fig. 1. Proposed hierarchical structure for problem decomposition

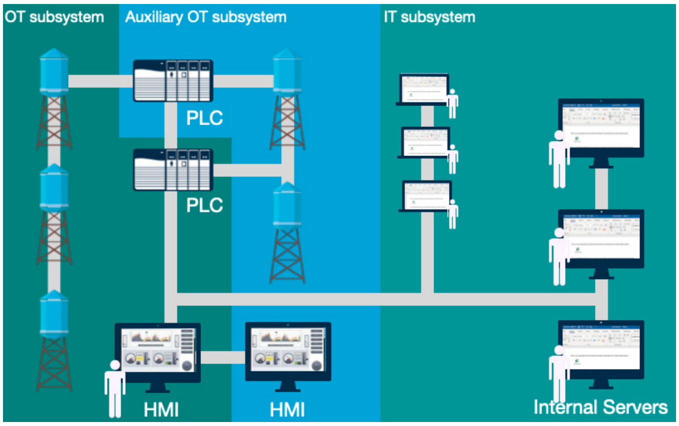

Fig. 2. Water treatment test-range

Let us define $A^{(k)}$ as the comparison matrix whose elements $A^k{}_{ij}$ represent the ratio between the relevance of the attacks $\mathcal{A}^k_i$ and $\mathcal{A}^k_j$; in relation to this, we have that the absolute relevance vector $\mathbf{a}^{(k)}$ is obtained by applying the same procedure. Furthermore, the severity of a particular attack $\mathcal{A}^k_i$ which belong to the hazard class $\mathcal{H}_k$, identified in the subsystem $\mathbb{S}_z$, is computed according to the following equation:

$$\mathcal{I}(i,z) = \frac{1}{n_h} \mathbf{a}^k_i \mathbf{h}^z_k \mathbf{s}_z, \quad (5)$$

where n_h represents the number of classes of hazards considered in the framework. Finally, we are able to normalize by linear interpolation the severities according to the classic evaluation adopted in the risk analysis, where the severity is often ranked on a five point scale as follows: (1) negligible, (2) minor, (3) major, (4) critical, and (5) catastrophic.

4. SIMULATION

In this simulation campaign we consider the critical infrastructure performed by the test-range depicted in Figure 2, which represents a water treatment critical infrastructure. The test-range is composed by the three following subsystems:

OT Subsystem ($\mathbb{S}_1$): the physical industrial plant composed of machines, electromechanical devices, indus-

W_{ij}	**Definition**	**Explanation**
1	Equal importance	Alternative i and Alternative j are considered equally important
3	Moderate importance of one over another	Alternative i moderately more important than Alternative j
5	Essential or strong importance	Alternative i is strongly favored with respect to Alternative j
7	Very strong importance	Alternative i is strongly favored with respect to Alternative j, and its dominance is demonstrated in practice
9	Extreme importance	The evidence favoring Alternative i over Alternative j is of the highest possible order of affirmation
2, 4, 6, 8	Intermediate values between the two adjacent judgements	When compromise is needed

Table 1. The Saaty's scale for AHP.

$\mathcal{A}_i^k$	**Hazard class**	**Attack definition**
$\mathcal{A}_1^1$	Cyber Hazards	Port Scan
$\mathcal{A}_2^1$	Cyber Hazards	Passive MITM
$\mathcal{A}_3^1$	Cyber Hazards	Phishing Campaign
$\mathcal{A}_4^1$	Cyber Hazards	Cross-Site Scripting
$\mathcal{A}_1^2$	Cyber Hazards	Code Injection
$\mathcal{A}_2^2$	Physical Hazards	Vandalism
$\mathcal{A}_3^2$	Physical Hazards	Explosion
$\mathcal{A}_4^2$	Physical Hazards	Hardware Failures
$\mathcal{A}_5^2$	Physical Hazards	Sabotage
$\mathcal{A}_1^3$	Cyber-Physical Hazards	Active MITM
$\mathcal{A}_2^3$	Cyber-Physical Hazards	DoS
$\mathcal{A}_3^3$	Cyber-Physical Hazards	DDoS

Table 2. Attack types considered in the simulation campaign

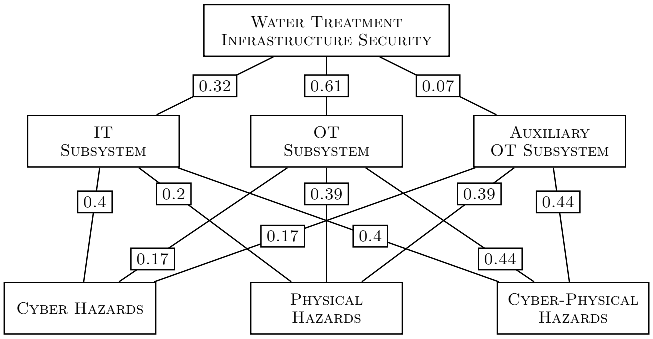

Fig. 3. Decomposition of the problem *Water Treatment Infrastructure Security* into hierarchy

trial controllers such as PLCs (programmable logic controllers), sensors, actuators (such as pumps and valves), HMIs (human machine interfaces), and other industrial equipment.

IT Subsystem ($\mathbb{S}_2$): the classic enterprise layer composed of servers, storage, networking and other devices used to run applications, process data, and support management activities.

Auxiliary OT Subsystems ($\mathbb{S}_3$): the physical replication of some fundamental OT subsystems. We recall that redundant architectures are essential to prevent the system from stopping. Auxiliary (or redundant) subsystems refer to the presence of components in the infrastructure that can compensate for the failing components and ensure a continuous functionality of the infrastructure.

Additional details about the test-range are described in Faramondi et al. (2021).

In the risk assessment analysis we consider the three following classes of hazards: *cyber hazards ($\mathcal{H}_1$)* such as hijacked accounts, frauds or identity thefts; *physical hazards ($\mathcal{H}_2$)* such as plant stop, infrastructure functionality reduction, actuators or sensors breakdown, etc. Moreover, we consider the presence of hybrid hazards, such as the *cyber-physical hazards ($\mathcal{H}_3$)*, that pose severe potential consequences to the IT or OT physical elements of the infrastructure. Finally, for each class of hazards we define the compatible attacks as in Table 2.

After defining the levels of the hierarchical structure, as shown in Figure 3, the expert provides the PCMs about the comparisons between the relative relevance of the subsystems S, and the comparison matrix used in order to compare the relevance of each hazard class for each subsystem of the infrastructure H^1, H^2, and H^3.

$$\mathrm{S} = \begin{array}{c} \\ \mathbb{S}_1 \\ \mathbb{S}_2 \\ \mathbb{S}_3 \end{array} \!\!\begin{array}{c} \begin{array}{ccc} \mathbb{S}_1 & \mathbb{S}_2 & \mathbb{S}_3 \end{array} \\ \begin{pmatrix} 1 & 1/2 & 5 \\ 2 & 1 & 9 \\ 1/5 & 1/9 & 1 \end{pmatrix} \end{array} \qquad \mathrm{H}^1 = \begin{array}{c} \\ \mathcal{H}_1^1 \\ \mathcal{H}_2^1 \\ \mathcal{H}_3^1 \end{array} \!\!\begin{array}{c} \begin{array}{ccc} \mathcal{H}_1^1 & \mathcal{H}_2^1 & \mathcal{H}_3^1 \end{array} \\ \begin{pmatrix} 1 & 2 & 1 \\ 1/2 & 1 & 1/2 \\ 1 & 2 & 1 \end{pmatrix} \end{array}$$

$$\mathrm{H}^2 = \begin{array}{c} \\ \mathcal{H}_1^2 \\ \mathcal{H}_2^2 \\ \mathcal{H}_3^2 \end{array} \!\!\begin{array}{c} \begin{array}{ccc} \mathcal{H}_1^2 & \mathcal{H}_2^2 & \mathcal{H}_3^2 \end{array} \\ \begin{pmatrix} 1 & 1/2 & 1/3 \\ 2 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix} \end{array} \qquad \mathrm{H}^3 = \begin{array}{c} \\ \mathcal{H}_1^2 \\ \mathcal{H}_2^2 \\ \mathcal{H}_3^2 \end{array} \!\!\begin{array}{c} \begin{array}{ccc} \mathcal{H}_1^2 & \mathcal{H}_2^2 & \mathcal{H}_3^2 \end{array} \\ \begin{pmatrix} 1 & 1/2 & 1/3 \\ 2 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix} \end{array}$$

Finally it is required to provide comparison matrices A^1, A^2, and A^3 in order to compare the severity of each attack:

$$\mathrm{A}^1 = \begin{array}{c} \\ \mathcal{A}_1^1 \\ \mathcal{A}_2^1 \\ \mathcal{A}_3^1 \\ \mathcal{A}_4^1 \\ \mathcal{A}_5^1 \end{array} \!\!\begin{array}{c} \begin{array}{ccccc} \mathcal{A}_1^1 & \mathcal{A}_2^1 & \mathcal{A}_3^1 & \mathcal{A}_4^1 & \mathcal{A}_5^1 \end{array} \\ \begin{pmatrix} 1 & 1/2 & 2 & 1/2 & 1/3 \\ 2 & 1 & 3 & 1/2 & 1/2 \\ 1/2 & 1/3 & 1 & 1/4 & 1/5 \\ 2 & 2 & 4 & 1 & 1 \\ 3 & 2 & 5 & 1 & 1 \end{pmatrix} \end{array},$$

$$\mathrm{A}^2 = \begin{array}{c} \\ \mathcal{A}_1^2 \\ \mathcal{A}_2^2 \\ \mathcal{A}_3^2 \\ \mathcal{A}_4^2 \end{array} \!\!\begin{array}{c} \begin{array}{cccc} \mathcal{A}_1^2 & \mathcal{A}_2^2 & \mathcal{A}_3^2 & \mathcal{A}_4^2 \end{array} \\ \begin{pmatrix} 1 & 1/4 & 1/3 & 1/4 \\ 4 & 1 & 2 & 1 \\ 3 & 1/2 & 1 & 1 \\ 4 & 1 & 1 & 1 \end{pmatrix} \end{array}, \qquad \mathrm{A}^3 = \begin{array}{c} \\ \mathcal{A}_1^3 \\ \mathcal{A}_2^3 \\ \mathcal{A}_3^3 \end{array} \!\!\begin{array}{c} \begin{array}{ccc} \mathcal{A}_1^3 & \mathcal{A}_2^3 & \mathcal{A}_3^3 \end{array} \\ \begin{pmatrix} 1 & 1/2 & 1/3 \\ 2 & 1 & 1/2 \\ 3 & 2 & 1 \end{pmatrix} \end{array}.$$

Notice that all the PCMs defined by the expert are consistent, hence the CR for each matrix is less then 10%. Finally, the problem in Equation (3) is solved for each given comparison matrix, thus we obtain:

$$\mathbf{s} = \begin{bmatrix}0.32\\0.61\\0.07\end{bmatrix}, \quad \mathbf{h}^1 = \begin{bmatrix}0.40\\0.20\\0.40\end{bmatrix}, \quad \mathbf{h}^2 = \mathbf{h}^3 = \begin{bmatrix}0.17\\0.39\\0.44\end{bmatrix},$$

$$\mathbf{a}^1 = \begin{bmatrix}0.12\\0.18\\0.07\\0.30\\0.33\end{bmatrix}, \quad \mathbf{a}^2 = \begin{bmatrix}0.09\\0.33\\0.25\\0.33\end{bmatrix}, \quad \mathbf{a}^3 = \begin{bmatrix}0.16\\0.30\\0.54\end{bmatrix}.$$

For each risk item, which is characterized by an attack $\mathcal{A}_i^k$ and a subsystem $\mathbb{S}_z$, its severity is computed according to Equation (5) and it is normalized in the range $[1, \dots, 5]$ using linear interpolation.

As shown in Table 3, the most severe attack in terms of normalized $\mathcal{I}$ is represented by the Dos and DDoS attacks targeting the OT subsystem, respectively associated to the values 3.2 and 5.0. As a matter of fact, such attacks are able to overwhelm an online device (such a computer, sensor, actuator, or a PLC) and render it unusable. Moreover, the results in Table 3 show that in general the highest average severity value is associated to the OT subsystem $\mathbb{S}_2$, which represents the physical core of the infrastructure. Conversely, a limited average severity value characterizes the auxiliary OT system, thus reflecting the fact that it is not essential for the infrastructure operation. Moreover, estimated frequency of occurrence has been associated to each risk item, according to the classic 5-point scale as follows: (1) low, (2) medium low, (3) medium, (4) medium high, and (5) high, while the magnitude of the risk is reported in the last column of Table 3. We can observe that the magnitude of the risk is computed as the product between the severity and the frequency for each risk item. Although the frequency of attacks targeting the OT subsystem ($\mathbb{S}_2$) is lower than the frequency of attacks targeting the IT subsystem ($\mathbb{S}_1$), we have that the average risk magnitude in the OT subsystem is greater than the average risk magnitude in the IT subsystem. Lastly, despite the frequency of DDoS attacks in the OT subsystem is low (2), this cyber threat represents the higher risk item for the security of the water treatment test range.

5. CONCLUSION

With respect to the problem of designing a risk assessment framework for critical infrastructures, the study proposes an approach to breakdown the decision-making process; specifically, the protocol first classifies the relevance of several risk items by considering multiple sub-problems based on pairwise comparison and then it is able to properly define the severity of multiple risk items. This methodology, based on the AHP or the LLS approach, can assist decision-makers in allocating adequate budgets for risk item prevention.

REFERENCES

Abdo, H., Kaouk, M., Flaus, J.M., and Masse, F. (2018). A safety/security risk analysis approach of industrial control systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Computers & security*, 72, 175–195.

Aminbakhsh, S., Gunduz, M., and Sonmez, R. (2013). Safety risk assessment using analytic hierarchy process (ahp) during planning and budgeting of construction projects. *Journal of safety research*, 46, 99–105.

Atputharajah, A. and Saha, T.K. (2009). Power system blackouts-literature review. In *2009 International Conference on Industrial and Information Systems (ICIIS)*, 460–465. IEEE.

Bernieri, G., Damiani, S., Del Moro, F., Faramondi, L., Pascucci, F., and Tambone, F. (2016). A multiple-criteria decision making method as support for critical infrastructure protection and intrusion detection system. In *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*, 4871–4876. IEEE.

Fang, Y., Rasel, M., and Richmond, P.C. (2020). Consequence risk analysis using operating procedure event trees and dynamic simulation. *Journal of Loss Prevention in the Process Industries*, 67, 104235.

Faramondi, L., Flammini, F., Guarino, S., and Setola, R. (2021). A hardware-in-the-loop water distribution testbed dataset for cyber-physical security testing. *IEEE Access*, 9, 122385–122396.

Faramondi, L., Oliva, G., Pascucci, F., Panzieri, S., and Setola, R. (2016). Critical node detection based on attacker preferences. In *2016 24th Mediterranean Conference on Control and Automation (MED)*, 773–778. IEEE.

Faramondi, L., Oliva, G., and Setola, R. (2020). Multi-criteria node criticality assessment framework for critical infrastructure networks. *International Journal of Critical Infrastructure Protection*, 28, 100338.

Filippini, R. and Silva, A. (2014). Irml: An infrastructure resilience-oriented modeling language. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(1), 157–169.

for Chemical Process Safety Staff, C. (2003). *Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites.* American Institute of Chemical Engineers.

Gertman, D.I. and Blackman, H.S. (1993). *Human reliability and safety analysis data handbook.* John Wiley & Sons.

Hashimoto, Y., Toyoshima, T., Yogo, S., Koike, M., Hamaguchi, T., Jing, S., and Koshijima, I. (2013). Safety securing approach against cyber-attacks for process control system. *Computers & Chemical Engineering*, 57, 181–186.

Hu, J., Khan, F., and Zhang, L. (2021). Dynamic resilience assessment of the marine lng offloading system. *Reliability Engineering & System Safety*, 208, 107368.

Iaiani, M., Tugnoli, A., Bonvicini, S., and Cozzani, V. (2021). Major accidents triggered by malicious manipulations of the control system in process facilities. *Safety science*, 134, 105043.

Khakzad, N., Landucci, G., and Reniers, G. (2017). Application of dynamic bayesian network to performance assessment of fire protection systems during domino effects. *Reliability Engineering & System Safety*, 167, 232–247.

Knabb, R.D., Rhome, J.R., and Brown, D.P. (2005). *Tropical cyclone report: Hurricane katrina, 23-30 august 2005.* National Hurricane Center.

Kornecki, A.J. and Zalewski, J. (2010). Safety and security in industrial control. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1–4.

Attack $\mathcal{A}_i^k$	Attack Description	Subsystem $\mathbb{S}_z$	$\mathcal{I}(i,z)$	Normalized $\mathcal{I}(i,z)$	Frequency	Risk Magnitude
$\mathcal{A}_1^1$	Port Scan	$\mathbb{S}_1$	0.01	1.46	3	4.37
$\mathcal{A}_2^1$	Passive MITM	$\mathbb{S}_1$	0.02	1.71	1	1.71
$\mathcal{A}_3^1$	Phishing Campaign	$\mathbb{S}_1$	0.01	1.25	5	6.25
$\mathcal{A}_4^1$	Cross-Site Scripting	$\mathbb{S}_1$	0.03	2.14	3	6.41
$\mathcal{A}_5^1$	Code Injection	$\mathbb{S}_1$	0.04	2.29	2	4.58
$\mathcal{A}_1^2$	Vandalism	$\mathbb{S}_1$	0.01	1.32	2	2.64
$\mathcal{A}_2^2$	Explosion	$\mathbb{S}_1$	0.04	2.41	2	4.82
$\mathcal{A}_3^2$	Hardware Failures	$\mathbb{S}_1$	0.03	1.93	3	5.78
$\mathcal{A}_4^2$	Sabotage	$\mathbb{S}_1$	0.03	2.18	2	4.37
$\mathcal{A}_1^3$	Active MITM	$\mathbb{S}_1$	0.02	1.63	3	4.88
$\mathcal{A}_2^3$	DoS	$\mathbb{S}_1$	0.03	2.14	3	6.42
$\mathcal{A}_1^3$	DDoS	$\mathbb{S}_1$	0.06	3.07	3	9.21
$\mathcal{A}_1^1$	Port Scan	$\mathbb{S}_2$	0.02	1.88	2	3.76
$\mathcal{A}_2^1$	Passive MITM	$\mathbb{S}_2$	0.04	2.37	1	2.37
$\mathcal{A}_3^1$	Phishing Campaign	$\mathbb{S}_2$	0.01	1.48	2	2.97
$\mathcal{A}_4^1$	Cross-Site Scripting	$\mathbb{S}_2$	0.06	3.19	1	3.19
$\mathcal{A}_5^1$	Code Injection	$\mathbb{S}_2$	0.07	3.49	2	6.98
$\mathcal{A}_1^2$	Vandalism	$\mathbb{S}_2$	0.02	1.61	2	3.23
$\mathcal{A}_2^2$	Explosion	$\mathbb{S}_2$	0.08	3.72	2	7.44
$\mathcal{A}_3^2$	Hardware Failures	$\mathbb{S}_2$	0.05	2.79	2	5.58
$\mathcal{A}_4^2$	Sabotage	$\mathbb{S}_2$	0.06	3.29	1	3.29
$\mathcal{A}_1^3$	Active MITM	$\mathbb{S}_2$	0.03	2.21	2	4.42
$\mathcal{A}_2^3$	DoS	$\mathbb{S}_2$	0.06	3.20	2	6.40
$\mathcal{A}_1^3$	DDoS	$\mathbb{S}_2$	0.11	5.00	2	10.00
$\mathcal{A}_1^1$	Port Scan	$\mathbb{S}_3$	0.00	1.09	2	2.19
$\mathcal{A}_2^1$	Passive MITM	$\mathbb{S}_3$	0.00	1.15	1	1.15
$\mathcal{A}_3^1$	Phishing Campaign	$\mathbb{S}_3$	0.00	1.05	2	2.10
$\mathcal{A}_4^1$	Cross-Site Scripting	$\mathbb{S}_3$	0.01	1.24	1	1.24
$\mathcal{A}_5^1$	Code Injection	$\mathbb{S}_3$	0.01	1.27	1	1.27
$\mathcal{A}_1^2$	Vandalism	$\mathbb{S}_3$	0.00	1.07	1	1.07
$\mathcal{A}_2^2$	Explosion	$\mathbb{S}_3$	0.01	1.29	1	1.29
$\mathcal{A}_3^2$	Hardware Failures	$\mathbb{S}_3$	0.01	1.19	1	1.19
$\mathcal{A}_4^2$	Sabotage	$\mathbb{S}_3$	0.01	1.25	1	1.25
$\mathcal{A}_1^3$	Active MITM	$\mathbb{S}_3$	0.00	1.13	1	1.13
$\mathcal{A}_2^3$	DoS	$\mathbb{S}_3$	0.01	1.24	2	2.47
$\mathcal{A}_1^3$	DDoS	$\mathbb{S}_3$	0.01	1.43	2	2.86

Table 3. Risk analysis result

Lees, F. (2012). *Lees' Loss prevention in the process industries: Hazard identification, assessment and control*. Butterworth-Heinemann.

Liang, G., Weller, S.R., Zhao, J., Luo, F., and Dong, Z.Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4), 3317–3318.

Moore, D.A. (2013). Security risk assessment methodology for the petroleum and petrochemical industries. *Journal of Loss Prevention in the Process Industries*, 26(6), 1685–1689.

Oliva, G., Faramondi, L., Setola, R., Tesei, M., and Zio, E. (2021). A multi-criteria model for the security assessment of large-infrastructure construction sites. *International Journal of Critical Infrastructure Protection*, 35, 100460.

Oroian, I. (2010). Eyjafjallajökull volcano eruption–a brief approach. *ProEnvironment Promediu*, 3(5).

Pasman, H.J., Rogers, W.J., and Mannan, M.S. (2018). How can we improve process hazard identification? what can accident investigation methods contribute and what other recent developments? a brief historical survey and a sketch of how to advance. *Journal of loss prevention in the process industries*, 55, 80–106.

Saaty, T.L. (1977). A scaling method for priorities in hierarchical structures. *Journal of mathematical psychology*, 15(3), 234–281.

Setola, R., Faramondi, L., Salzano, E., and Cozzani, V. (2019). An overview of cyber attack to industrial control system. *Chemical Engineering Transactions*, 77, 907–912.

Smith, S. (2022). Out of gas: A deep dive into the colonial pipeline cyberattack. In *SAGE Business Cases*. SAGE Publications: SAGE Business Cases Originals.

Zhu, P. and Liyanage, J.P. (2021). Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: A specific review of issues and challenges in safety instrumented systems. *European Journal for Security Research*, 1–25.