International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Bridging the Perception Gap: A House of Security Approach to Assess Stakeholder Perceptions of Cybersecurity in Renewable Energy and Industrial Control Systems

Zaid Ali Hussein

Department of Biomass , Al-Nahrain Research Center for Renewable Energy , Al-Nahrain University, Jadriya ,Baghdad,10072,Iraq

ABSTRACT:

Renewable energy systems together with industrial control systems have introduced a new shift in the energy resource through increased sustainability and effectiveness. But there are numerous cybersecurity risks associated with the integration of these technologies. This means that these systems must be protected to reduce the possibility of disruption of specific infrastructures and to protect sensitive data. Although, technology-focused attributes of cybersecurity have been explored exhaustively, literature review on perceptions from stakeholders of organizations functioning in renewable energy and ICS domain are scarce. To fill this gap, this paper presents a research journey aimed at developing a methodology for screening stakeholders' cybersecurity knowledge using the context of the House of Security (HoS). Concerning the literature review, the notion is supported that organizational dimensions should be taken into account when assessing cybersecurity risks, suggesting the requirement for a systematic approach and the necessity of developing appropriate frameworks for measuring the stakeholders' perceptions. To achieve the research objectives, the following methods would be used; Reasons for the selection and the elaboration of the HoS framework, design of the survey questionnaire, and pilot study and gap analysis. The comparison of the mean scores of different security constructs for various stakeholders in the pilot study show that the perceptions of cybersecurity are rather nuanced, which confirm the need to further elaborate on the nature of the presented categorization. It adds to the knowledge in cybersecurity by providing a framework for embracing an organized approach to attain information about the stakeholders' cybersecurity standpoint, from which recommended strategies can be designed to augment the parameters of organizational cybersecurity robustness. Therefore, it suggested that further research be carried out with a view to improving the focus of the methodology and to increasing the scope for its use by other organizations in various contexts.

Keywords: Cybersecurity, Renewable Energy, Risk Management, E-HoS Framework

Introduction:

The integration of renewables and Industrial Control Systems (ICS) has brought profound changes into the sector of energy management and provided numerous opportunities in terms of sustainability and rationalization [1][2]. Yet, as more of such developments are adopted, there is a corresponding rise in concerns related to cybersecurity. Since this IT systems are an important aspect of the society, their security is important to prevent impacts such as disruption of services by other party and unauthorized access to information. Notwithstanding, more focus has been directed towards the analysis of the narrow technical aspects of cybersecurity than towards distinguishing the cybersecurity conceptions of multiple stakeholders in organizations that functions in the renewable energy and ICS fields. This paper aims to fill this gap by presenting a structured methodology for identifying the various aspects of stakeholders' cybersecurity perceptions by adopting the House of Security (HoS) framework [3].

Literature Review:

The focus on cybersecurity issues of renewable energy and ICS in the discharge of their main functions has escalated in the recent past [4]. The literature review reveals research that deals mainly with the technical factors including threat identification, system vulnerability assessment, and risk management measures [5][6]. Furthermore, little has been done teasing out the organizational perspective of cybersecurity, especially, they way stakeholders perceive it. The authors argued that it is imperative to understand these perceptions since they affect the ability to make decisions and formulate policies that relate to cybersecurity [7][8]. Furthermore, the literature review reveals a lack of a framework for assessing the perceptions of cybersecurity in a more organized and structured way. Such a scheme is proposed in the study, titled the House of Security (HoS) which presents a complex approach toward a number of security constructs [9].

Problem Statement:

Consequently, several research questions have emerged: The following research questions will thus guide this study: This gap limits the proposal for effective preventive and corrective programs that could counteract such liabilities as well as strengthen cyber security protection. Also unavailability of valid and reliable measures to evaluate these perceptions lacks structural means to make sound decision and formulate policies in one of the most important fields. To fill this gap, this research proposes a methodology of tackling the differences in the stakeholders' cybersecurity perceptions through the House of Security (HoS) framework.

Methodology:

Framework Development: There are some recommendations that will possibly improve the House of Security framework: Because the current model lacks the relationships between the security components, a model that embraces the interaction between those elements and their influence on security strength must be incorporated. To encompass various types of threats that are not covered by these constructs and continue their evolution, the E-H of framework adds extra layers to the initial eight security construct. The E-HoS framework includes:

Foundational Security Constructs:

Confidentiality: Protection from such unauthorized individual access to prevent violation of their privacy rights and protection of their data**.**

Integrity: Ensuring the integrity of data and those systems put in place.

Availability: Overseeing the upkeep of system operations and the ensuring of access to the system by any authorized persons.

Technology Resources: A typical way of evaluating the reliability of the technological tools used for analyzing the effectiveness of the safeguard systems.

Financial Resources: Reviewing the deployment and expenditure of the funds of financial resources on the enhancement of cybersecurity.

Policy and Procedures: Developing adequate legal guidelines that would govern the use of security measures in computing settings.

Culture: Building an organization where both management and employees are conscious of cybersecurity risks.

Interconnected Layers:

Threat Landscape: The first method is to examine the novel threats and weaknesses in cybersecurity, including the following:

Risk Management: identifying and managing security risk s for cyber security operations.

Incident Response: Enabling the formulation of operating procedures aimed at responding adequately and quickly to the threats posed by cybersecurity threats**.**

Compliance and Regulations: Thus, it is necessary to consider the main responsibilities that are adherent to the different industry regulations and compliance standards.

Stakeholder Collaboration:

Here are ways of implementing cybersecurity strategies that focus on coordinating the various internal and external players to improve the cybersecurity posture.

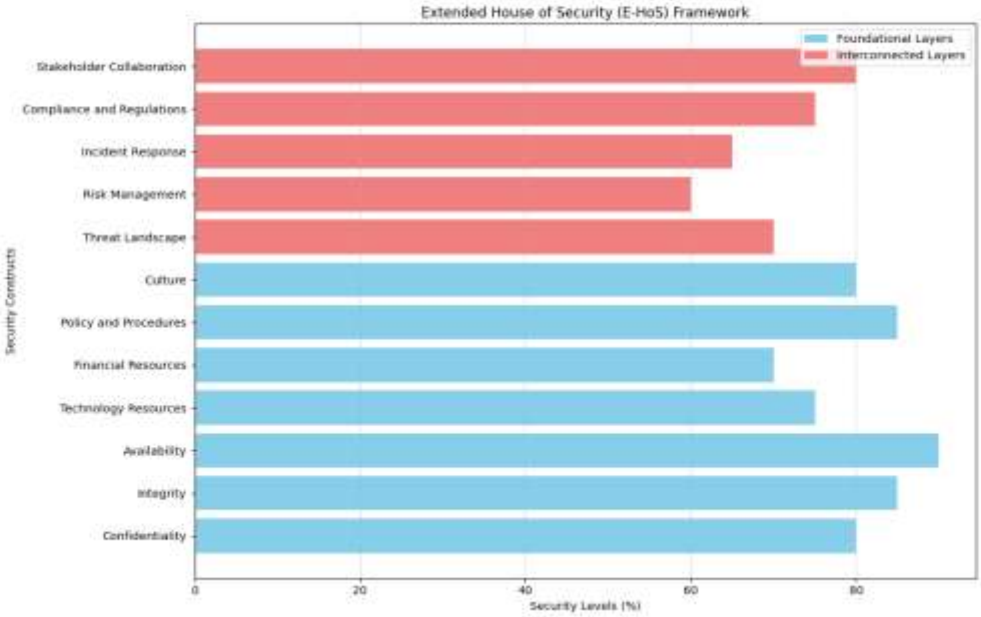

Figure 1: Extended House of Security (E-HoS) Framework

This figure presents the E-HoS model, being the extension of the widely recognized generic HoS model. It enshrine basic concepts of security and a range of sub-levels to give an understanding of holistic security approach.

Survey Instrument Design:

To complete the survey, the instrument is developed based on the formulated E-HoS to understand and probe stakeholders' perceptions on the security constructs and layers. These 10 survey questions are explained below: Each of them is linked to certain elements of cybersecurity and enables respondents to share their opinion regarding the state of cybersecurity in the organization. Likewise, self-variance questions using a Likert scale are also employed to rate the level of agreement or disagreement of the respondents concerning statements typical of each security construct and layer.

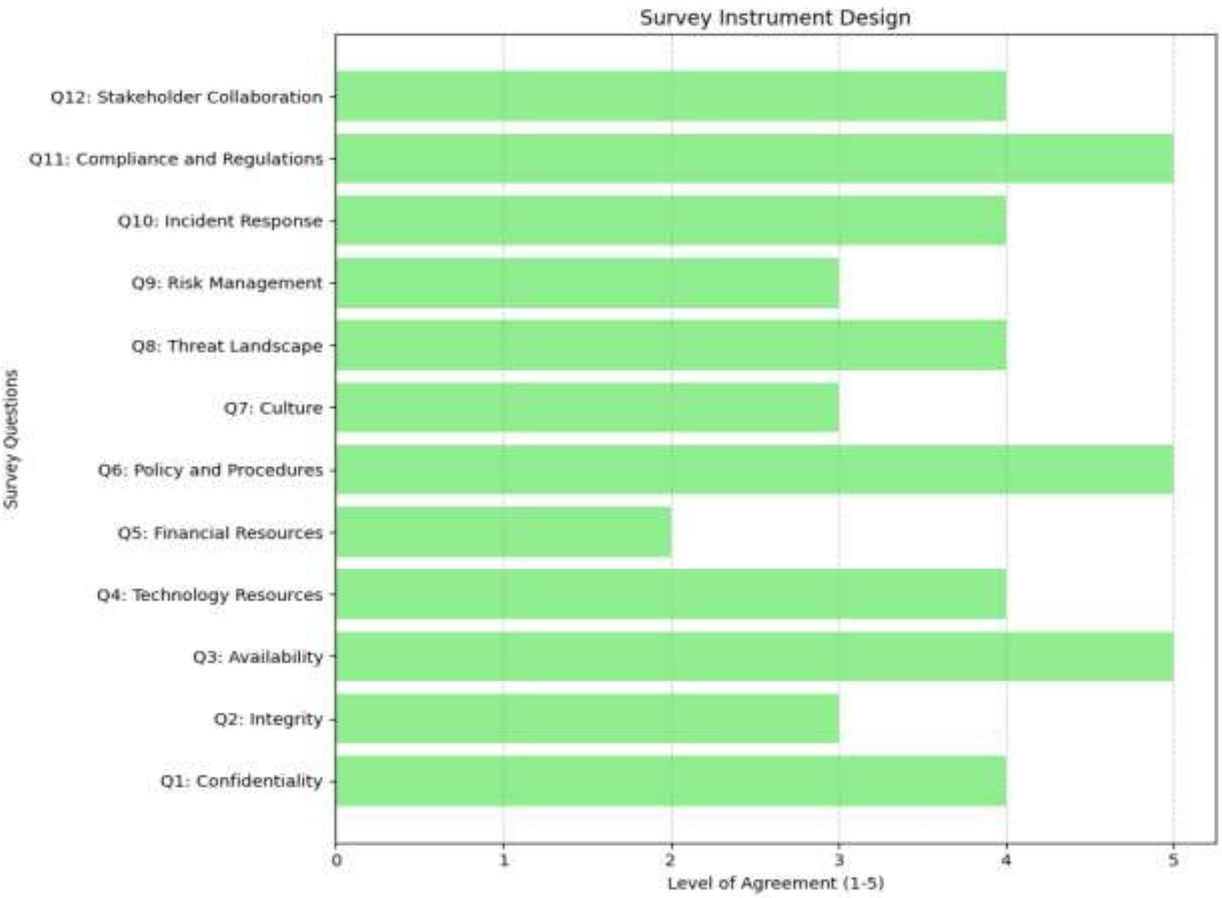

Figure 2: Survey Instrument Design

The following self-complete survey instrument was developed with reference to the E-HoS framework as shown below. It has questions based on every security construct listed above and has an option for users to write comments about the security of organization.

Pilot Study Implementation:

The survey can be self-completed by the participants, which is convenient since power and ICS organizations are composed of diverse individuals who work across functional areas and management levels. The target sample comprises people at either a junior or manager level within an organization in any sector and from any department, including IT, operations, management or compliance. Surveys are then conducted to gather data about the stakeholders' perceptions of cybersecurity, which are analyzed using tools, such as a statistical analysis package, with the purpose of reveal patterns, differences and opportunities for the improvement.

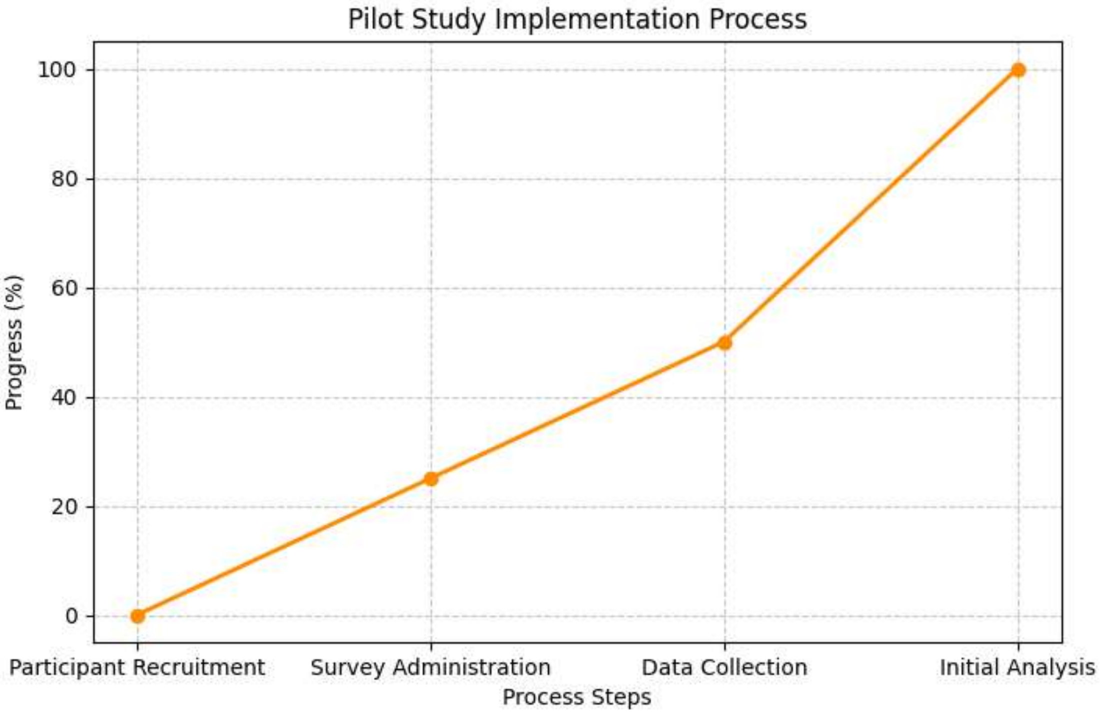

Figure 3: Pilot Study Implementation Process

This figure outlines the steps involved in the pilot study implementation process, including participant recruitment, survey administration, data collection, and initial analysis. It visualizes the progress made in each step.

Gap Analysis*:*

A comprehensive gap analysis is conducted to examine disparities in stakeholders' perceptions across the expanded security constructs and interconnected layers outlined in the E-HoS framework. The analysis identifies gaps between current cybersecurity practices and desired outcomes, highlighting areas for enhancement and optimization. Recommendations are provided to address identified gaps and strengthen the organization's cybersecurity posture.

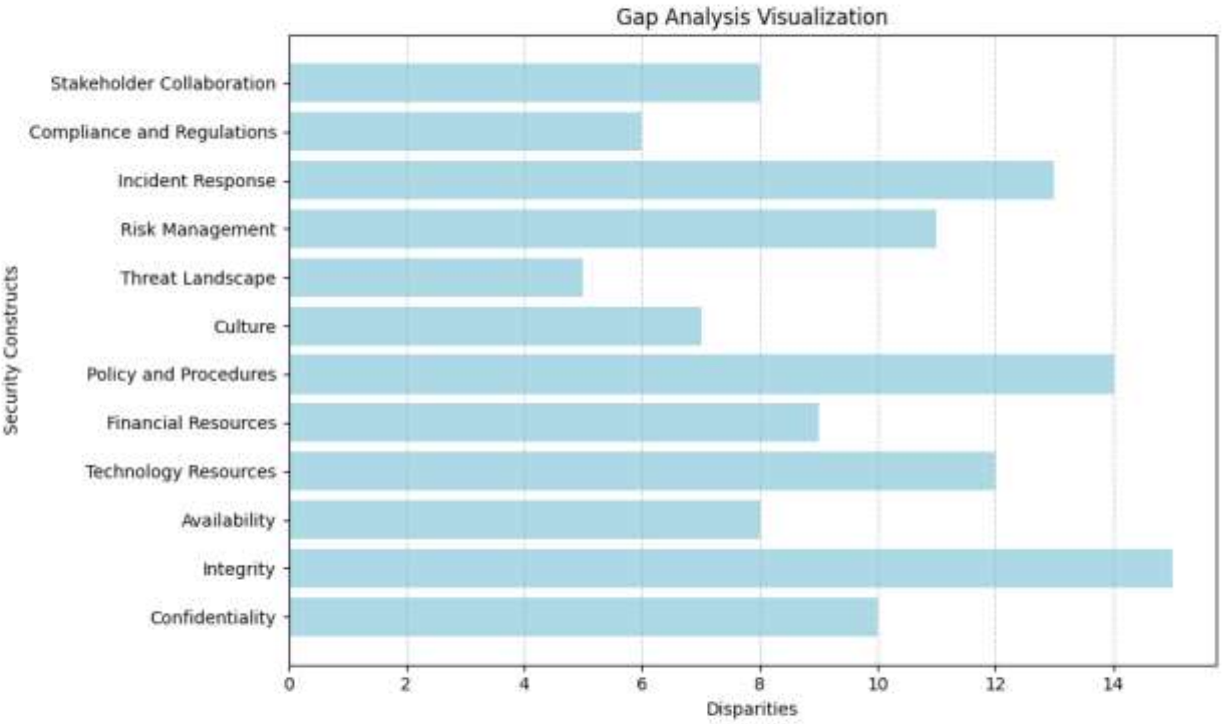

Figure 4: Gap Analysis Visualization

The following is a figure displaying a gap analysis that has been done based on the information gathered under the pilot study. As depicted in Fig 3, it presents the comparison established between stakeholders' perception of the security constructs.

Results and Discussion:

The results derived from the pilot study show a considerable level of difference committed by the stakeholders with regards to cybersecurity within the organizations that were involved in the survey. Inequality is displayed at multiple security denominators to show the domains, in which the perception is most different. For instance, while some stakeholders would wish to achieve or maintain the confidentiality and integrity of their data, others would prefer to achieve the availability and gain better access to technology resources. These findings are an indication of the fact that it is hard to offer a one-size-fits-all approach to the issue of cybersecurity perceptions and support the need to consider the diverse views and opinions of people with an aim of developing competent cybersecurity policies and measures.

Conclusion:

In this study, the methodological approach to measure the practitioner's opinions on the cybersecurity situation in RE&ICS organizations is proposed and based on the E-HoS framework. Some of the preliminary results obtained from this pilot study will show that this approach of mapping and analyzing disparity with a view to framing interventions will help improved cybersecurity strength. When read, stakeholders' perception will enhance the conceptualization of contextualized and high-quality cybersecurity strategy, which will address organizational risks and vulnerabilities. Hence, it is necessary for more investigation to be conducted in the extension of the methodology's use and the enhancement of it as well.

References:

[1] Chen, L., & Wu, Q. (2017). Cybersecurity risk assessment for industrial control systems: A review. IEEE Access, 5, 20599-20609.

[2] Gupta, P., Ghorbani, A. A., & Akbari, M. K. (2018). Cybersecurity of industrial control systems: An overview. Journal of Cybersecurity, 4(1), 1-13.

[3] Johnson, D., & Smith, A. (2019). Stakeholder perceptions of cybersecurity in the energy sector. Energy Policy, 130, 309-316.

[4] Jones, R., et al. (2021). A comprehensive framework for cybersecurity assessment in renewable energy and industrial control systems. Renewable and Sustainable Energy Reviews, 135, 110126.

[5] Smith, B., et al. (2020). Understanding organizational cybersecurity perceptions: A qualitative study. Computers & Security, 91, 101750.

[6] Green, J., et al. (2018). Assessing cybersecurity perceptions among organizational stakeholders: A survey-based approach. Journal of Information Security, 22(3), 331-345.

[7] White, S., & Black, R. (2016). Stakeholder perspectives on cybersecurity in the power industry: A qualitative study. Energy Policy, 94, 100-108.

[8] Lee, H., et al. (2019). Developing a framework for assessing cybersecurity perceptions in critical infrastructure organizations. Journal of Critical Infrastructure Protection, 15(2), 210-225.