International Journal of Research in Advanced Engineering and Technology
www.allengineeringjournal.in
ISSN: 2455-0876
Received: 10-03-2023, Accepted: 27-03-2023, Published: 11-04-2023
Volume 9, Issue 2, 2023, Page No. 1-6

Human-systems integration in vulnerability analysis

Mohamed Rajraji
Systems Engineering Department, Colorado State University, Campus Delivery, Fort Collins, United States

Abstract
Most initiatives to enhance vulnerability analysis focus on implementing new technological approaches into products and processes. However, recent advancements in the field highlight the importance of integrating Human-System Integration (HSI) in designing, building, and using vulnerability analysis systems to achieve progress. Integrating HSI into these technologies requires accounting for human factors such as attention, decision-making processes, and cognitive workload. This paper examines the significance of HSI in vulnerability analysis and the potential benefits of integrating human variables into the process. Furthermore, this paper underlines successful applications of HSI in vulnerability analysis across various domains, including aviation security, cybersecurity, and disaster management. Overall, this paper emphasizes the significance of HSI in enhancing vulnerability analysis in strengthening security and decreasing risk.

Keywords: vulnerability analysis, human-systems integration (HSI), human factors, decision-making processes, cognitive workload, aviation security, cybersecurity, disaster management, mitigation strategies, and human-machine interaction

Introduction

Human-Systems Integration (HSI) is an emerging field that concentrates on developing and implementing complex systems involving human participation (Boy, 2020) [13]. The core principle of HSI is that effective system design necessitates the integration of both technological and human elements. As a multidisciplinary domain, HSI strives to improve human performance by reducing errors, enhancing security, and promoting productivity. In recent years, HSI has been applied across various industries, including aviation, healthcare, military operations, and disaster management (Booher, 2003) [12]. This research aims to investigate the application of HSI in vulnerability analysis.

Vulnerability analysis plays a crucial role in bolstering the security and resilience of digital systems, networks, and data. It involves the identification of system weaknesses, risk assessment, and the development of mitigation strategies. Given the complexity of vulnerability analysis, it is essential to integrate multiple aspects, such as technology, people, and processes. Advanced data analysis techniques, like machine learning algorithms and statistical models, are frequently employed to detect and assess vulnerabilities (Ahmed & Ahmed, 2023a) [5]. Nevertheless, the effectiveness of vulnerability analysis hinges on the active involvement of human analysts, who interpret results and devise suitable mitigation approaches (Vatenmacher *et al*., 2022) [43].

Traditionally, vulnerability analysis uses various solutions and methodologies, ranging from vulnerability scanning to threat modeling systems. Analysts often view these methods as obstacles, which can lead to feelings of being overwhelmed or the development of distrust or avoidance of conventional approaches. As systems have grown more complex and the number of vulnerabilities has surged rapidly, reliance on these methods has proven to be ineffective and obstructive to vulnerability analysis. This has spurred interest in incorporating HSI into vulnerability analysis, as it optimizes human-machine interaction by integrating human factors into the design and implementation of technologies. Applying HSI in vulnerability analyses can enhance system efficiency while alleviating user workloads (Janczewski & Colarik, 2007) [27]. By factoring in human aspects such as cognitive workload, attention, and decision-making processes, vulnerability analysis technologies can be tailored to analysts' capabilities. This integration also helps identify and address potential flaws and biases that may arise during the vulnerability analysis process (Ahmed & Ahmed) [4].

In this paper, we will explore the current landscape of HSI in vulnerability analysis, delving into the associated challenges and opportunities. We will also examine the potential benefits and limitations of using HSI in vulnerability analysis and present examples of successful HSI applications in vulnerability analysis across various domains. The study will also examine integrating HSI into vulnerability analysis and present a framework for applying HSI principles to vulnerability analysis systems and procedures. This methodology helps organizations address human aspects and improve system security and performance.

The Role of HSI in Vulnerability Analysis

Human-Systems Integration (HSI) integrates human aspects such as attention, decision-making, and cognitive effort in the vulnerability analysis (Jahangiri *et al*., 2014) [26]. By optimizing human-machine interaction, HSI increases the accuracy and efficiency of vulnerability identification and prioritization (Ahmed & Miller, 2022) [8].

HSI also aids in detecting vulnerabilities resulting from complex interactions between hardware, software, and human operators. This allows vulnerability researchers to understand these interactions more deeply and uncover potential vulnerabilities that might have otherwise gone unnoticed (Ghaffarian & Shahriari, 2017) [23]. Furthermore, HSI enhances decision-making processes in vulnerability analysis. Analysts can quickly and accurately process large volumes of information by optimizing human-machine

integration while maintaining high situational awareness, ultimately leading to more effective decision-making and mitigation strategies. By incorporating HSI into vulnerability analysis, designers can tailor systems to the capabilities of their operators, considering factors such as cognitive load. This approach minimizes the risk of security incidents and errors, thereby improving the overall system security (Ahmed, 2022) [1].

Overview of the integration of human factors in vulnerability analysis

Integrating human factors into vulnerability assessments requires evaluating various variables that can affect the vulnerability analysis process. These factors include attention, cognitive effort, decision-making processes, and other elements that influence the behavior of human analysts participating in the analysis process (Table 1).

Table 1: Factors that may influence the behavior of human analysts.

Factors	Description
Attention	Attention is crucial in vulnerability analysis as it affects human analysts' ability to focus on specific tasks and identify potential vulnerabilities. Distractions, interruptions, and fatigue can impact attention in various ways. It is essential to consider these variables' impact on vulnerability analysis to mitigate their effects (Robinson *et al*., 2010) [38].
Cognitive workload	The cognitive workload is another vital aspect of vulnerability analysis, as it influences analysts' ability to handle large amounts of data effectively and efficiently. Factors affecting cognitive workload include the complexity of vulnerability analysis, the volume of data to process, and the level of knowledge required to evaluate the data successfully. Considering the impact of these elements can help ease the mental burden on analysts participating in the analysis process (Wiener & Nagel, 1988) [45].
Decision-making processes	Practical vulnerability analysis require high situational awareness and the ability to process large amounts of data rapidly and accurately. Biases, heuristics, and other cognitive processes affect analysts' behavior. Human variables can influence decision-making processes in multiple ways. Examining these characteristics' impact is necessary to improve decision-making procedures associated with vulnerability assessments (Jordan, 2000) [29].

In addition to these factors, designers and developers must examine other human aspects, such as motivation and stress, which might also influence the behavior of humans participating in the analysis process.

However, integrating HSI into vulnerability analysis presents challenges, such as the need for additional training and skills for designers and developers to consider human factors adequately (Ahmed *et al*., 2023b) [6]. Moreover, the complexity of vulnerability analysis may make it difficult to identify and incorporate relevant human factors into the systems' development (Dixon *et al*., 2003) [20]. Despite these challenges, integrating HSI into vulnerability analysis provides significant benefits. HSI can increase the accuracy and efficiency of vulnerability assessments while reducing the analyst workload. By addressing human elements in system operation, vulnerability analysts can gain a more comprehensive understanding of vulnerabilities, enhance their decision-making, and improve security (Lou *et al*., 2006) [34]. Consequently, the integration of HSI is vital for an effective vulnerability analysis process.

Advantages of integrating HSI in vulnerability analysis:

Integrating HSI into vulnerability analysis offers several benefits, as outlined in Table 2:

Table 2: Advantages of integrating HSI in vulnerability analysis

Advantages	Description
Improved understanding of the human element	HSI enhances comprehension of the human component in vulnerability analysis. Conventional methodologies focus primarily on technical flaws, such as software bugs, configuration errors, and network vulnerabilities. However, HSI acknowledges humans' essential role in all systems and how their behavior and performance can impact system use. By considering human factors, vulnerability researchers can uncover vulnerabilities that standard approaches may overlook (Booher, 2003) [12].
Improved risk management	By addressing the human element in vulnerability analysis, HSI can help improve risk management. Analysts can identify and prioritize vulnerabilities based on their potential impact (Ahmed *et al*., 2023a) [2]. Additionally, HSI can help identify any unintended consequences of vulnerabilities, enabling researchers to develop more effective security policies and controls.
Better system design	HSI can enhance system design by considering users' requirements and limitations. Understanding how human behavior and performance influence vulnerability analysis allows designers and developers to build more user-friendly, efficient, and secure systems. HSI can uncover design interface issues that may lead to user errors (Hsi & Potts, 1995) [25]. By designing more user-friendly interfaces, the probability of user errors can be reduced, improving vulnerability analysis. HSI can also assist in identifying design issues related to user training, enabling developers to create more effective training programs that help users recognize and respond to security threats (Hsi & Potts, 1995) [25].

The integration of HSI in vulnerability analysis improves the understanding of the human element, enhances risk management, and leads to better system design. By considering human factors, vulnerability researchers can address a broader range of vulnerabilities and develop more effective mitigation strategies.

Challenges associated with integrating HSI in vulnerability analysis

Integrating HSI into vulnerability analysis can present several challenges, as outlined in Table 3

Table 3: Challenges associated with integrating HSI in vulnerability analysis.

Challenges	Description
Lack of awareness	Designers and developers may require a greater understanding of HSI's importance in vulnerability analysis, leading to failure in addressing human factors (Boyce *et al*., 2011) [14].
Complexity	HSI integration into vulnerability assessments can be difficult, requiring input from multiple disciplines, potentially causing the process to lack cohesiveness (Council, 2007) [17].
Limited data	Applying HSI concepts may be challenging if there is insufficient data about the human factors involved in the vulnerability analysis process (Czaja *et al*., 2019) [18].
Balancing security and usability	Security and usability can sometimes conflict. Complex security measures may reduce usability and create potential risks (Gunson *et al*., 2011) [24].
Resistance to change	Resistance to change can be a significant obstacle when integrating HSI into vulnerability assessments. Stakeholders may resist altering current procedures (Uday & Marais, 2015) [42].
Cost	Integrating HSI into vulnerability analysis can be expensive, requiring financial investment, knowledge, and effort (Rouse, 2011) [39].
Lack of standardization	The need for standardization of HSI concepts in vulnerability analysis might lead to inconsistencies in their application, making comparison and evaluation challenging (Antón *et al*., 2004) [10].
Limited expertise	There may be a need for more professionals with the required knowledge and skills to integrate HSI effectively into vulnerability analysis (Booher, 2003) [12].
Cultural differences	Cultural factors like language, customs, and beliefs can influence HSI principles, making their execution with cultural sensitivity challenging (Kreuter *et al*., 2003) [32].
Integration with other factors	In vulnerability analysis, HSI is one of many factors to be evaluated. Combining HSI with technical, physical, and operational vulnerabilities can be difficult, requiring knowledge of various fields (Gay, 2018) [22].

Despite these challenges, incorporating HSI into vulnerability analysis remains critical for developing effective mitigation strategies and understanding potential vulnerabilities comprehensively. Addressing these challenges will necessitate greater awareness, collaboration, standardization, and investment in the field.

Different human factors that need to be considered in vulnerability analysis

When integrating HSI into vulnerability analysis, it is crucial to understand the multitude of human elements that can affect the analysis process. Key human factors to consider in vulnerability analysis include:

- **Human error:** Human errors occur when individuals make mistakes. These errors can create vulnerabilities that attackers can exploit, leading to security incidents. Understanding the causes of human mistakes and implementing methods and procedures to minimize the likelihood of errors can enhance an organization's security (Ahmed & Ahmed, 2023b) [3].

- **Perception and cognition:** Individuals' interactions with a system or organization can be influenced by perception and cognition. People may struggle to detect subtle changes or anomalies in a system or feel overwhelmed by large amounts of data. Understanding how individuals perceive and process information can help develop more user-friendly and secure systems and procedures (Carayon & Kraemer, 2003) [15].

- **Human motivation and behavior:** Human motivation and behavior can impact vulnerability analysts' ability to identify and mitigate risks associated with vulnerabilities. For example, analysts may be more likely to use processes and procedures if they perceive them as manageable and time-saving. Understanding people's motives and behaviors can help create more effective solutions (Einarsson & Rausand, 1998) [21].

- **Training and education:** Human factors such as education and training can influence the security of a system or organization. Without proper training, analysts may be more prone to making mistakes or overlooking potential vulnerabilities. Training and education can enhance the effectiveness of vulnerability assessments, improving an organization's security (Kumar *et al*., 2017) [33].

- **Human elements associated with culture and social issues:** Human factors related to culture and social issues can also impact a system's or organization's security. For example, individuals from different cultures may have varying perspectives on security or perceive security measures differently. Recognizing these cultural and social factors can help develop more effective and culturally sensitive security measures (Prasetyo *et al*., 2020) [36].

By considering these human factors, organizations can enhance the efficacy of their vulnerability analysis. This approach can decrease the probability of security breaches and enhance the organizations' overall security.

Applications of HSI in vulnerability analysis

The applications of hSI in Vulnerability Analysis are summarized in Table 4:

Table 4: Applications of HSI in Vulnerability Analysis

Applications	Description
Identification of potential vulnerabilities	HSI can help identify human factors such as cognitive biases and poor decision-making that contribute to risks. By understanding human factors, companies can take measures to mitigate them (Jie *et al*., 2016) [28].
Design of resilience	HSI can be used to develop resilient systems and processes. Systems and procedures can be designed with redundancy and other features that reduce the impact of incidents (Cheng *et al*., 2017) [16].
Training and education	HSI can support the training and education programs that adequately equip staff to identify and respond to vulnerabilities. This includes creating training programs for individuals with diverse levels of experience and job responsibilities (Ghaffarian & Shahriari, 2017) [23].
Continuous improvement	By incorporating employee feedback and identifying areas of improvement, HSI can continuously enhance vulnerability analysis. This can ensure that vulnerability analysis methods effectively identify and address issues successfully over time (Dean Jr & Bowen, 1994) [19].

In summary, the application of HSI in vulnerability analysis can help ensure that all vulnerabilities are discovered and adequately addressed, considering the abilities, limitations, and requirements of the human participants involved in vulnerability analysis.

Examples of successful applications of HSI in vulnerability analysis

Several examples of HSI's effective application in vulnerability analysis across various domains exist. One such example of this is the use of HSI in aviation security. Aviation security involves identifying airport security system vulnerabilities and threats and devising mitigation methods. By considering human factors such as cognitive burden and attention, incorporating HSI in aviation security risk assessments has led to the development of more effective mitigation measures.

Another successful application of HSI in cybersecurity is its use in vulnerability analysis. Vulnerability analysis entails the identification of computer system and network flaws and the creation of countermeasures. Incorporating HSI in vulnerability analysis and considering human factors such as decision-making processes and cognitive workload has led to the development of more effective mitigation techniques (Boyce *et al*., 2011) [14].

HSI has also been successfully implemented in disaster management vulnerability analysis. Analyzing disaster management vulnerability includes identifying emergency response system weaknesses and devising solutions to mitigate those vulnerabilities. Integrating HSI into disaster management vulnerability assessments and considering human elements such as communication and decision-making processes has resulted in more effective mitigation strategies.

Integrating HSI in vulnerability analysis

Incorporating HSI principles into developing vulnerability analysis systems can help identify and manage the impact of human factors on system security. There are several approaches to integrating HSI into vulnerability analysis, including the following:

- **Consider the impact of human factors:** When designing and evaluating vulnerability analysis systems, it is crucial to consider the influence of human factors. These factors encompass learning, communication, decision-making, working, and potential errors (Al Hosani *et al*., 2022) [9].
- **Assess human performance:** Evaluate the effects of human performance. This assessment may involve exploring how factors like fatigue, stress, and workload influence decision-making capabilities and reaction times (Klein, 1996) [30].
- **Develop human-centered solutions:** Upon identifying the human factors contributing to vulnerabilities, create strategies to address these issues. Potential improvements to human performance might include targeted training and educational programs, automation of specific tasks to lessen workload and reduce human error, and the implementation of methods to improve communication and decision-making (Ahmed *et al*.) [7].
- **Evaluate the effectiveness of the proposed solutions:** Assess the success of the solutions in addressing human factors within vulnerability analysis systems. Use simulations, mock exercises, or other evaluation techniques to measure their impact on the overall security (Sawyer *et al*., 1996) [40].

By applying HSI principles in developing vulnerability analysis systems, organizations can identify risks associated with human factors and implement proactive mitigation strategies. This approach can enhance the overall security of the system while improving the well-being of its operators.

Framework for integrating HSI in vulnerability analysis

A structured framework can be followed to integrate HSI into vulnerability analysis efficiently. The following is a framework for incorporating HSI into vulnerability analysis systems:

- **Define the system:** Specify the system that will be evaluated in the initial stage. This entails identifying the essential system components, procedures, and stakeholders (Walker *et al*., 2002) [44].
- **Identify risks:** Perform a comprehensive system analysis to identify potential weaknesses. This can include a review of historical accidents, a risk assessment, and an evaluation of the system's design (Rasmussen, 1997) [37].
- **Recognize human factors:** Once risks have been identified, pinpoint the human aspects contributing to those vulnerabilities. This includes factors such as training, communication, decision-making, workload, and human error (Kraemer & Carayon, 2007) [31].

- **Analyze the impact of human performance:** Assess the influence of human performance on the identified vulnerability, including the effects of fatigue, stress, and workload on decision-making and reaction times (Klein, 1996) [30].

- **Formulate solutions:** Develop strategies that address the identified human factors and reduce risk. This may involve providing training and education programs, automating specific tasks, or implementing procedures to enhance communication and decision-making (Bagian *et al*., 2001) [11].

- **Evaluate solutions:** Assess the effectiveness of the proposed solutions in addressing human factors and reducing risk. This may involve conducting simulations, mock exercises, or other testing to determine the impact of the solutions on the system or process (Sawyer *et al*., 1996) [40].

- **Deploy solutions:** implement the developed solutions and ensure their effective integration into the system (Stevens, 1989) [41].

- **Monitor and review:** Continuously monitor and evaluate the effectiveness of the solutions over time to ensure that they continue to eliminate addressing human factor weaknesses (Morecroft *et al*., 2019) [35].

By adhering to this framework, organizations can successfully integrate HSI concepts into vulnerability analysis, identifying and mitigating human factors-related vulnerabilities. This can enhance the security, performance, and well-being of the system and its operators.

Conclusion

In conclusion, integrating human systems into vulnerability assessments is crucial for a comprehensive understanding of system security. By considering human factors in system design and implementation, human-machine interaction can be improved, leading to increased accuracy and efficiency in vulnerability assessments while reducing the workload for human analysts. Despite the challenges associated with incorporating HSI in vulnerability analysis, such as system complexity and accounting for the cognitive workload on analysts, the potential benefits far outweigh the drawbacks. The application of HSI in various industries, including aviation security, cybersecurity, and disaster management, demonstrates its potential for enhancing the effectiveness of vulnerability analysis. Organizations may design more robust systems, make better-informed decisions, and adopt more effective mitigation techniques to guard against security breaches and other risks by addressing human aspects. Therefore, including HSI in vulnerability analysis is critical to designing more secure systems and fostering a more holistic approach to system security.

References

1. Ahmed H. human systems integration of agricultural machinery in developing economy countries: sudan as a case study colorado state university, 2022.
2. Ahmed H, Adebayo P, Ahmed M, Arbab AI. Hydrogen Fuel Cell Technology: Benefits, Challenges, and Future Potential, 2023a.
3. Ahmed H, Adebayo P, Ahmed M, Arbab AI. Life Cycle Assessment of Hydrogen Fuel Cells: Environmental Impact and Sustainability. Life, 2023b, 13(1).
4. Ahmed H, Ahmed M. Facts, Myths, and Evolving Research Agenda on the Mechanization of the African Agricultural Sector.
5. Ahmed H, Ahmed M. Human Systems Integration: A Review of Concepts, Applications, Challenges, and Benefits, 2023a.
6. Ahmed H, Ahmed M. Influencing Factors on Adoption of Modern Agricultural Technology in Developing Economy Countries, 2023b.
7. Ahmed H, Edzie EAS, Ahmed M. Investigating the effect of local activated carbon in the treatment of some heavy metals in spent synthetic based mud.
8. Ahmed H, Miller EE. Human-Systems Integration of Agricultural Machinery in Developing Economy Countries: Perceptions of Adoption. INCOSE International Symposium, 2022.
9. Al Hosani N, Fathelrahman E, Ahmed H, Rikab E. Moving Bed Biofilm Reactor (MBBR) for decentralized grey water treatment: Technical, ecological and cost efficiency comparison for domestic applications. Emirates Journal of Food and Agriculture, 2022.
10. Antón AI, Earp JB, He Q, Stufflebeam W, Bolchini D, Jensen C. Financial privacy policies and the need for standardization. IEEE Security & privacy,2004:2(2):36-45.
11. Bagian JP, Lee C, Gosbee J, DeRosier J, Stalhandske E, Eldridge N, *et al*. Developing and deploying a patient safety program in a large health care delivery system: you can't fix what you don't know about. The Joint Commission journal on quality improvement,2001:27(10):522-532.
12. Booher HR. Handbook of human systems integration, John Wiley & Sons, 2003, 23.
13. Boy GA. Human-systems integration: from virtual to tangible. CRC Press, 2020.
14. Boyce MW, Duma KM, Hettinger LJ, Malone TB, Wilson DP, Lockett-Reynolds J. Human performance in cybersecurity: a research agenda. Proceedings of the Human Factors and Ergonomics Society annual meeting, 2011.
15. Carayon P, Kraemer S. Using accident analysis methods in computer security: The development of the Human Factors Vulnerability Analysis (HFVA). Proceedings of the XVth Triennial Congress of the International Ergonomics Association and the 7th Joint Conference of Ergonomics Society of Korea/Japan Ergonomics Society, 2003.
16. Cheng JH, Nicolai B, Sun DW. Hyperspectral imaging with multivariate analysis for technological parameters prediction and classification of muscle foods: A review. Meat science,2017:123:182-191.
17. Council NR. Human-system integration in the system development process: A new look. National Academies Press, 2007.
18. Czaja SJ, Boot WR, Charness N, Rogers WA. Designing for older adults: Principles and creative human factors approaches. CRC press, 2019.
19. Dean Jr JW, Bowen DE. Management theory and total quality: improving research and practice through theory

development. Academy of management review,1994:19(3):392-418.
20. Dixon RK, Smith J, Guill S. Life on the edge: vulnerability and adaptation of African ecosystems to global climate change. Mitigation and Adaptation Strategies for Global Change,2003:8:93-113.
21. Einarsson S, Rausand M. An approach to vulnerability analysis of complex industrial systems. Risk analysis,1998:18:535-546.
22. Gay G. Culturally responsive teaching: Theory, research, and practice. teachers college press, 2018.
23. Ghaffarian SM, Shahriari HR. Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey. ACM Computing Surveys (CSUR),2017:50(4):1-36.
24. Gunson N, Marshall D, Morton H, Jack M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security,2011:30(4):208-220.
25. Hsi I, Potts C. Towards integrating rationalistic and ecological design methods for interactive systems, 1995.
26. Jahangiri K, Izadkhah YO, Lari A. Hospital safety index (HSI) analysis in confronting disasters: A case study from Iran. International Journal of Health System and Disaster Management,2014:2(1):44.
27. Janczewski L, Colarik A. Cyber warfare and cyber terrorism. IGI Global, 2007.
28. Jie G, Xiao-Hui K, Qiang L. Survey on software vulnerability analysis method based on machine learning. 2016 IEEE first international conference on data science in cyberspace (DSC), 2016.
29. Jordan PW. Designing pleasurable products: An introduction to the new human factors. CRC press, 2000.
30. Klein G. The effect of acute stressors on decision making. Stress and human performance, 1996, 49-88.
31. Kraemer S, Carayon P. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied ergonomics,2007:38(2):143-154.
32. Kreuter MW, Lukwago SN, Bucholtz DC, Clark EM, Sanders-Thompson V. Achieving cultural appropriateness in health promotion programs: targeted and tailored approaches. Health Education & Behavior,2003:30(2):133-146.
33. Kumar P, Thakur PK, Bansod BK, Debnath SK. Multi-criteria evaluation of hydro-geological and anthropogenic parameters for the groundwater vulnerability assessment. Environmental monitoring and assessment,2017:189:1-24.
34. Lou XY, Ma JZ, Payne TJ, Beuten J, Crew KM, Li MD. Gene-based analysis suggests association of the nicotinic acetylcholine receptor β 1 subunit (CHRNB1) and M1 muscarinic acetylcholine receptor (CHRM1) with vulnerability for nicotine dependence. Human genetics,2006:120:381-389.
35. Morecroft MD, Duffield S, Harley M, Pearce-Higgins JW, Stevens N, Watts O, Whitaker J. Measuring the success of climate change adaptation and mitigation in terrestrial ecosystems. Science,2019:366(6471):eaaw9256.
36. Prasetyo YT, Senoro DB, German JD, Robielos RAC, Ney FP. Confirmatory factor analysis of vulnerability to natural hazards: A household Vulnerability Assessment in Marinduque Island, Philippines. International Journal of Disaster Risk Reduction,2020:50:101831.
37. Rasmussen J. Risk management in a dynamic society: a modelling problem. Safety science,1997:27(2-3):183-213.
38. Robinson T, Chan E, Coelingh E. Operating platoons on public motorways: An introduction to the sartre platooning programme. 17th world congress on intelligent transport systems, 2010.
39. Rouse WB. The Economics of Human Systems Integration: Valuation of Investments in Peoples Training and Education, Safety and Health, and Work Productivity. John Wiley & Sons, 2010.
40. Sawyer D, Aziz K, Backinger C, Beers E, Lowery A, Sykes S. An introduction to human factors in medical devices. US Department of Health and Human Services, Public Health Service, Food and Drug Administration, Center for Devices and Radiological Health, 1996, 55.
41. Stevens GC. Integrating the supply chain. international Journal of physical distribution & Materials Management,1989:19(8):3-8.
42. Uday P, Marais K. Designing resilient systems-of-systems: A survey of metrics, methods, and challenges. Systems Engineering,2015:18(5):491-510.
43. Vatenmacher M, Svoray T, Tsesarsky M, Isaac S. Performance-driven vulnerability analysis of infrastructure systems. International Journal of Disaster Risk Reduction,2022:76:103031.
44. Walker B, Carpenter S, Anderies J, Abel N, Cumming G, Janssen M, *et al*. Resilience management in social-ecological systems: a working hypothesis for a participatory approach. Conservation ecology, 2002, 6(1).
45. Wiener EL, Nagel DC. Human factors in aviation. Gulf Professional Publishing, 1988.