Data-driven vulnerability assessment method for industrial

cyber-physical systems

Yimeng Zhaoa, Guohua Chena,\*, Qiming Xua, Yihong Huanga, Honghao Chena

a Institute of Safety Science & Engineering, South China University of Technology, Guangzhou, 510640, Guangdong, China

\**Corresponding author. E-mail: mmghchen@scut.edu.cn*

1. Introduction

Industrial cyber-physical systems (ICPSs), as a key technology of the Industry 4.0 era, have been widely applied across various industrial sectors, including manufacturing, energy, power, chemicals, and transportation. By integrating operational technology (OT) with information technology (IT), ICPSs achieve a high level of interconnectivity and coordination between devices, systems, humans, and data, driving the intelligent transformation of industries. However, despite the immense potential of ICPSs, their implementation also introduces several risks and challenges.Attackers can infiltrate the network, disrupt normal system operations, and even cause severe cyber-physical (C2P) incidents. There were as many as 36 cyber-attacks in the oil, chemical, and energy sectors worldwide between 2006 and 2014 (Iaiani et al., 2021).

ICPSs are composed of multiple components, including sensors, actuators, logic controllers, human-machine Interface, engineering stations, and data servers. This inherently means that ICPSs typically contain numerous vulnerabilities. In practice, however, it is often unrealistic for practitioners to address and patch all vulnerabilities. Furthermore, during the pre-risk assessment phase of a system, considering all possible attack pathways stemming from these vulnerabilities could lead to a combinatorial explosion of accident scenarios. Therefore, conducting vulnerability assessment research and identifying critical vulnerabilities in ICPSs is of paramount importance. Common Weakness Enumeration (CWE), as a collection of Common Vulnerabilities and Exposures (CVE), provides a detailed classification of CVEs. The MITRE CWE database annually lists the top 25 most common CWE types to guide cybersecurity professionals (MITRE CWE database). However, this statistical result is not specific to ICPSs. Currently, the most widely used vulnerability assessment tool is the Common Vulnerability Scoring System (CVSS). However, Nayak et al. demonstrated that the CVSS exploitability and impact scores are only applicable at the software level, failing to account for the subsequent physical consequences in ICPSs. As a result, CVSS scores do not align with the actual exploitation rates of vulnerabilities. Therefore, some researchers have since proposed modifications to the CVSS to address this limitation. Wang et al. (2023) considered the impact of exploited vulnerabilities and enhanced the original CVSS model by incorporating metrics for safety, finance, operations, and privacy. Zhu et al. (2023) optimized the Access Vector (AV) and Access Complexity (AC) parameters by considering factors such as property safety, life safety, functional safety, and privacy safety, addressing some of the limitations within the CVSS framework. However, the effectiveness of most improved CVSS models remains unvalidated by empirical evidence. Falco et al. (2018) analyzed the density of Common Weakness Enumeration (CWE) within ICPS vulnerabilities and examined the real-world exploitation of these vulnerabilities using open-source databases such as CWE, ExploitDB, and CVEDetails. Based on their findings, they proposed a data-driven vulnerability prioritization method to objectively assess systemic risk. Nevertheless, this method has limitations. In practice, incident data is often scarce, and accident reports are typically too brief, making it difficult to map these descriptions effectively to current CWE types.

In summary, this study will improve traditional vulnerability assessment model and, using a data-driven approach, validate the correlation between the vulnerability assessment index system and the actual exploitation frequency of vulnerabilities. Furthermore, the proposed vulnerability prioritization method can significantly simplify the risk assessment process for complex ICPSs while ensuring the objectivity and accuracy of the evaluation results.

1. Methods

**2.1 Research flowchart**

图片1

*Figure 1: Framework of the analysis process in the study.*

As shown in Figure 1, this study consists of three parts: First, a database of vulnerabilities and cyber-attack incidents related to ICPSs is established. Then, based on the CWE groups classification principle, the density of CWE groups and the real-world exploitation density of CWE groups are calculated. An improved CVSS model, which considers the consequences of subsequent incidents, is proposed to compute the average impact and exploitability scores for each CWE group, thus constructing a vulnerability prioritization assessment index system. Finally, multiple linear regression is used to validate the effectiveness of the index parameters, and the method is applied to the tank level control system for risk analysis.

**2.2 Database construction**

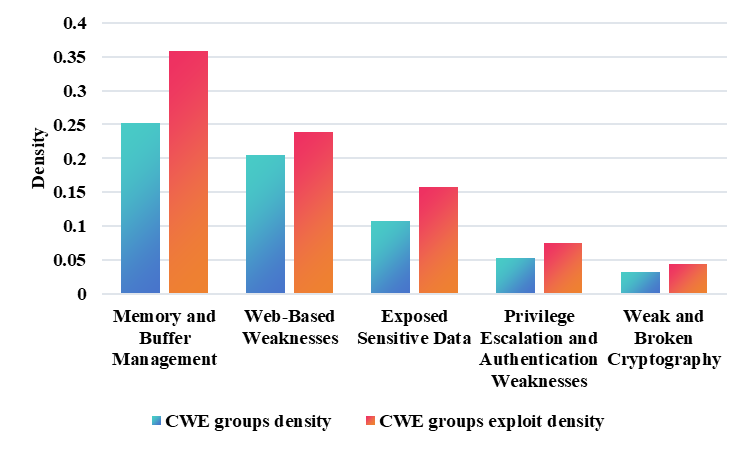
Based on the key devices in ICPSs, a search was conducted in the MITRE CVE database, resulting in the collection of 1,053 vulnerabilities. The corresponding CVE identifiers and base scores were retrieved from the National Vulnerability Database (NVD). Additionally, 19 relevant incident cases were collected from the RISI cybersecurity incident database (RISI database), encompassing various industrial sectors such as chemicals, electricity, manufacturing, and transportation. Furthermore, 48 currently exploited vulnerabilities were obtained from the CVEDetails database. The above data together constitute the ICPS-specific vulnerability and cyber-attack incident database, which provides data support for the vulnerability priority assessment.

**2.3 CWE group classification principle**

Thomas et al. (2020) proposed a novel CWE groups classification approach specifically for ICPSs, which encompass 95% of the vulnerabilities in the database. Unlike previous studies, this classification approach, while still based on CWE, avoids the definitional ambiguity of the traditional CWE classification approach and provides a clearer reflection of how vulnerabilities manifest in ICPS. As mentioned in the introduction, the currently available cybersecurity incident reports for ICPS are often too brief, making it challenging to map incident causes using the conventional CWE classification approach. In this study, the new CWE group classification approach ensures accurate mapping of cybersecurity incident reports to CWE groups, thereby better reflecting the actual exploitation of vulnerabilities. The detailed definitions of each CWE group are outlined below.

1) Web-Based Weaknesses: Attackers exploit vulnerabilities or flaws exposed in web applications to gain unauthorized access. 2)Default Credentials: Attackers use default system passwords or hardcoded sensitive credentials to infiltrate the system. 3)Denial of Service and Resource Exhaustion: Attackers overwhelm the target system with large volumes of requests or data, rendering the system or service unresponsive to legitimate user requests. 4)Exposed Sensitive Data: These vulnerabilities allow unauthorized attackers to access sensitive information, leading to the leakage of user credentials or other sensitive data. 5)Weak and Broken Cryptography: Attackers exploit weak encryption techniques or incorrectly apply strong encryption to gain unauthorized access. 6)Memory and Buffer Management: Attackers input data exceeding the buffer size of a program, causing memory overwrites that can result in the execution of malicious code. 7)Permissions and Resource Access Control: Attackers exploit incorrect privilege allocation or lack of proper access control to perform arbitrary operations on the system. 8)Privilege Escalation and Authentication Weaknesses: Attackers bypass authentication mechanisms by exploiting system vulnerabilities, and gaining elevated privileges to perform unauthorized actions.

Based on the above CWE group classification approach and the data from Section 2.2 on ICPS-specific vulnerabilities and cyber-attack incidents, the CWE group density and actual exploit density for each CWE group are calculated, as shown in Figure 2. It is evident that there is a clear positive linear relationship between the top five CWE group densities and exploit densities. This means that the more frequent occurrence of a particular type of vulnerability increases its exposure rate and makes it more susceptible to exploitation by attackers.



*Figure 2: The CWE groups density and exploit density of top 5 CWE groups.*

**2.4 Improved CVSS model**

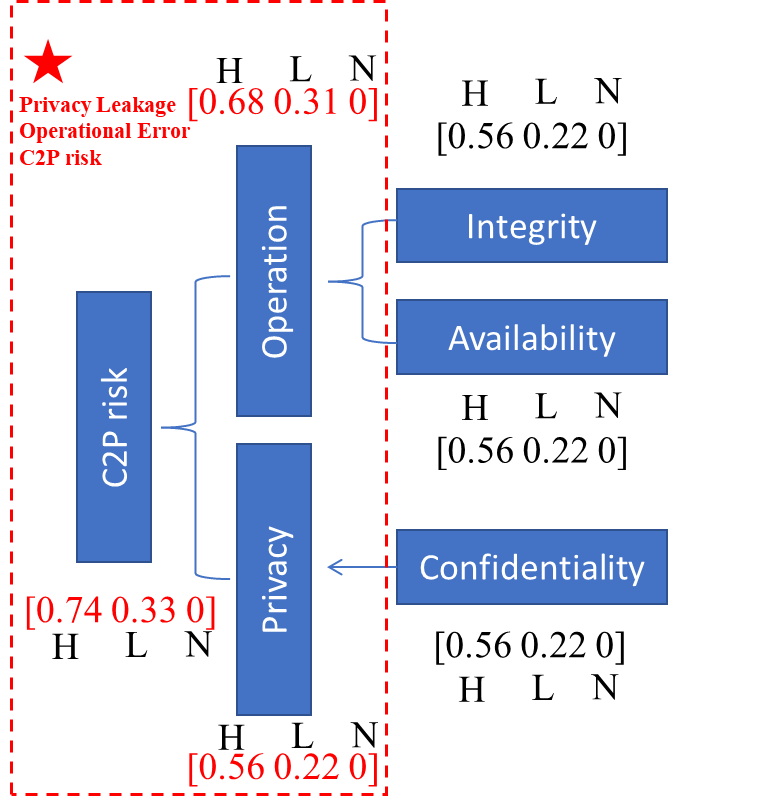
To more objectively quantify the prioritization of vulnerability importance, this section takes into account the impact of subsequent incidents on the significance of vulnerabilities. Therefore, on the basis of the CVSS 3.1 framework, additional nodes have been introduced, including operational error, privacy leakage, and C2P Risk. The operation node is determined by the Integrity and Availability scores of the vulnerability, while the C2P risk level is influenced by both the operation and privacy nodes. These nodes are connected through OR gates, and the H, L, and N thresholds for each node are calculated separately. The improved CVSS model is illustrated in Figure 3, and using Eq. (1-4), the impact score, exploitability score, the condition probability of successful attacks, and risk level of the vulnerability are calculated (Zhang et al. 2017).







 (4)



*Figure 3: Improved CVSS model*

**2.5 Index system verification**

In this section, the MATLAB multiple linear regression tool is used to calculate the standard error, and R² of the regression parameters between CWE group density, average impact score, average exploitability score, and CWE group exploit density, in order to verify the effectiveness of the index system. As shown in Table 1, there is a significant correlation between CWE group density and exploit density. Moreover, after applying the improved CVSS model, the R² value increased from 0.955 to 0.994, demonstrating the effectiveness of the vulnerability assessment index system.

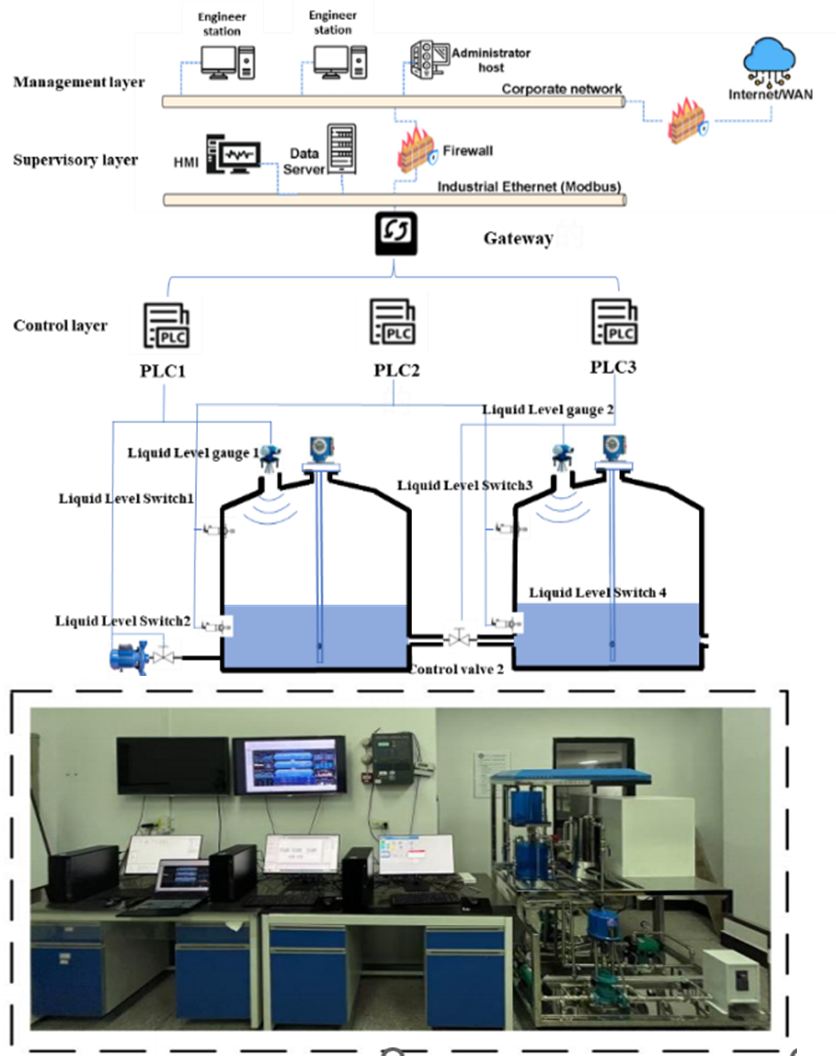
*Table 1：Results of Multiple Linear Regression*

|  |  |  |
| --- | --- | --- |
| **Traditional CVSS model** | **Estimate** | **Standard error** |
| Intercept | -0.119 | 0.283 |
| CWE group density | 1.004 | 0.734 |
| average impact score | 0.021 | 0.029 |
| average exploitability score | 0.021 | 0.095 |
| **R2** | 0.955 |  |
| **Improved CVSS model** | **Estimate** | **Standard error** |
| Intercept | -0.634 | 0.257 |
| CWE group density | 0.167 | 0.013 |
| average impact score | 0.185 | 0.067 |
| average exploitability score | 0.044 | 0.034 |
| **R2** | 0.992 |  |

**3. Case study: an application to tank level control system**

**3.1 Construction of tank level control system**

This section takes the real tank level control system as an example to conduct vulnerability prioritization and risk level analysis. As shown in Figure 4, the tank level control system is composed of the management layer, monitoring layer, and control layer. Key equipment includes the Administrator host, HMI, Data server, and PLC. In the control layer, three PLCs are responsible for controlling the level gauge, pump, level interlock device, and control valve



*Figure 4: The tank level control system*

**3.2 Risk analysis**

Based on the methods outlined in Section 2, an attack graph was established for vulnerabilities in the top 5 CWE groups with an average impact score and exploitability score sum greater than 7. The results of the high-risk vulnerability screening are shown in Table 2, which displays the CVE ID, corresponding device name, the sum of the average impact score and exploitability score, and the associated probability of the successful attack.

*Table 2：Result of high-risk vulnerability screening*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CWE group | CVE number | NO. | Equipment | ES+IS | Pattack success |
| Memory and Buffer Management | CVE-2022-47393 | V1 | HMI | 9.1 | 0.727 |
| CVE-2022-4046 | V2 | HMI | 12.2 | 0.727 |
| Web-Based Weaknesses | CVE-2016-8673 | V3 | PLC | 12.1 | 0.727 |
| CVE-2018-8997 | V4 | PLC | 12.2 | 0.345 |
| CVE-2017-1498 | V5 | AH | 7.2 | 0.531 |
| Exposed Sensitive Data | CVE-2018-1994 | V6 | DS | 8.5 | 0.727 |
| Privilege Escalation and Authentication Weaknesses | CVE-2017-0283 | V7 | ES | 12.2 | 0.727 |
| CVE-2017-8692 | V8 | AH | 12.1 | 0.416 |
| Weak and Broken Cryptography | CVE-2018-6618 | V9 | DS | 12.2 | 0.471 |

Using the GeNle software, the attack graph is converted into a Bayesian Network (BN), quantifying the probability of successful attack and risk level for each device node, as shown in Figure 5. In this representation, circles denote vulnerability nodes, while squares represent device nodes. The attack success probabilities for the Administrator host, HMI, Data server, and PLC are 0.73, 0.67, 0.62, 0.53, and 0.59, respectively, and the risk level increases with the penetration of attack levels.

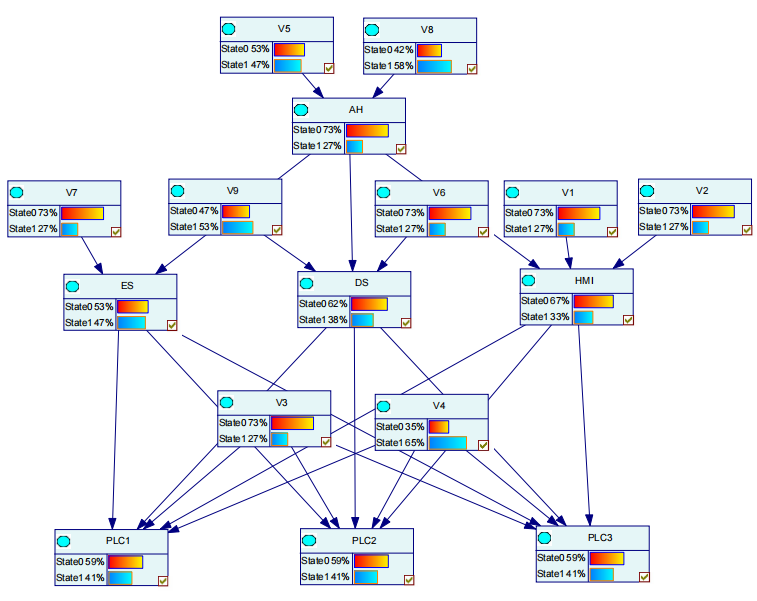


Figure 5: The risk calculation result based Bayesian Network

4. Conclusions

This study developed a vulnerability prioritization assessment method tailored for ICPSs based on an improved CVSS model and a novel CWE) groups classification approach and verified the effectiveness of the assessment index system by applying the incident case-driven. Finally, a case study on a tank level control system was conducted to quantify attack paths and risk levels. The application of this vulnerability assessment method can significantly reduce the complexity of security assessments in ICPSs while ensuring the objectivity of the assessment results to some extent.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (22478128), and the China Scholarship Council (202406150078).

References

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021, Analysis of Cybersecurity-related Incidents in the Process Industry. Reliability Engineering & System Safety. 209, 107485.

Wang, Y., Yu, B., Yu, H., Xiao, L., Ji, H., Zhao, Y., 2023, Automotive Cybersecurity Vulnerability Assessment Using the Common Vulnerability Scoring System and Bayesian Network Model. IEEE Systems Journal. 17(2), 2880-2891.

Zhu, Q., 2023, Enhancing vulnerability scoring for information security in intelligent computers. International Journal of Intelligent Networks. 4, 253-260.

Falco, G., et al. 2018, CALDERA C, SHROBE H. IIoT Cybersecurity Risk Modeling for SCADA Systems. IEEE Internet of Things Journal. 5(6), 4486–4495.

Thomas, R.J., Chothia, T., 2020, Learning from vulnerabilities - categorising, understanding and detecting weaknesses in industrial control systems. In: Computer Security. Springer International Publishing, Cham.

Nayak, K., Marino, D., Efstathopoulos, P., Dumitras, T., 2014, Some vulnerabilities are different than others. In: Research in Attacks, Intrusions and Defenses. Springer International Publishing, Cham.

RISI - The Repository of Industrial Security Incidents. https://www.risidata.com/. [dataset].

Common vulnerability enumeration (CVE). MITRE, https://www.cve.org/. [dataset].

Zhang, H., Lou, F., Fu, Y., Tian, Z., 2017, A conditional probability computation method for vulnerability exploitation based on CVSS. 2017 IEEE 2nd International Conference on Data Science in Cyberspace, 238–241.