Design of vehicle traffic information security risk evaluation index system based on grey evaluation method

Bei Xu¹*, Yajun Wang¹, Jinzhan Yang¹
¹Military Transportation Academy, Automotive Command Department, Tian Jin, 300161, China.

*Corresponding author e-mail: huangdandan1@nudt.edu.cn

Abstract: The network security problem of vehicle traffic information system is becoming more and more prominent. In order to effectively defend the system, this paper conducts in-depth research on the network security of vehicle traffic information system and proposes an information security risk assessment system for vehicle traffic control center. Specifically, the vehicle traffic control center is divided into components, and the security attributes of each component of the vehicle traffic control center system are constructed. By studying the information interaction process between the vehicle traffic control center and other subsystems, the security attributes of each component are abstracted; Identify the risk value of the component based on the influence of the component's security attribute on the risk assessment index, aiming to enhance the security defense capability of the vehicle traffic information system.

Keywords: vehicle traffic; information security; risk assessment; index system

1. Introductions
In the vehicle traffic control system, the information system is the nerve center of the entire traffic system, ensuring the safe, orderly and efficient operation of the system. Since the vehicle traffic information system is a complex and safety-critical industrial control system, if the traditional information system security assessment method is mechanically applied, it obviously does not meet the actual requirements of the system. The vehicle traffic information system needs to find a more appropriate information security risk assessment method. In layman's terms, information security risk assessment is to analyze the vulnerability and impact of the organization's information assets facing threats and being threatened, and on this basis, to study the possibility of risk factors and the impact of risk events. The organization selects security control measures to reduce risks, and provides a factual basis for risk decisions [1].
2. PROBLEMS IN CONSTRUCTING VEHICLE TRAFFIC INFORMATION SECURITY RISK ASSESSMENT

2.1. Poor ability to effectively collect, exchange and share information resources

The development of vehicle traffic information application system lacks system planning, single-point applications are common, and the information resource collection, sharing, disclosure, and reporting systems are not perfect. This makes the current vehicle traffic information resources scattered and difficult to integrate. Information resources Low-level repetitive collection, lack of accumulation of historical data, insufficient content, low data quality, many static data, and lack of real-time dynamic information are widespread [2].

2.2. Low level of development and utilization of vehicle traffic information resources

After years of informatization construction, vehicle transportation has accumulated a large amount of information resources, but the level of development and utilization of information resources is still relatively low, and it needs to be integrated and utilized. Information resources are one of the most valuable assets of the industry [3]. Although the integration of provincial-level vehicle traffic information resources has been demonstrated and applied in the transportation informatization demonstration project and promotion and application organized by the Ministry, the integration of provincial-level vehicle traffic information resources has been connected to the Ministry of Vehicle Traffic Management Information System In the work, a pilot project has been carried out to integrate the transportation information resources of various provinces (autonomous regions, municipalities) to the ministerial level. However, in general, the current development of vehicle traffic informatization in various provinces (autonomous regions, municipalities) is still in the information system of different business fields and different regions. It is relatively isolated and scattered, lacks integrated application of information resources, low development and utilization, weak coordination among business systems, and insufficient mining of accumulated massive data, which cannot effectively provide guarantee for high-level decision-making and industry supervision.

![Tree diagram of risk assessment indicators for vehicle traffic information security](image)

3. A RISK ASSESSMENT INDEX SYSTEM FOR VEHICLE TRAFFIC INFORMATION SECURITY

3.1. Principles of setting risk evaluation index

Information security risk assessment is a process of scientifically evaluating the confidentiality, integrity and availability of information systems and the information processed, transmitted and stored by them in accordance with relevant information security technical standards. It evaluates the vulnerability and information of the information system. The threats faced by the system and the negative impacts of vulnerabilities after being exploited, and the security risks of the information system are identified according to the possibility of security incidents and the degree of negative impacts. For organizational information system security risk assessment, before using certain assessment methods and assessment models, an evaluation index that can reasonably reflect information security risks from multiple levels and multiple
angles must be constructed in order to obtain scientific and fair assessment results [4]. In order to comprehensively and objectively assess information system security risks, when constructing and setting up an information security risk assessment index system, the complexity and uncertainty of information security should be fully considered, and the following principles should be followed.

(1) Scientific principles. The entire evaluation index system must be objective and accurate from the composition of the index to its system structure, from the measurement content of the index to the measurement method, and must scientifically and comprehensively reflect the essential characteristics of information system security risks [5].

(2) The principle of comprehensiveness. The information security risk evaluation index system should cover the life cycle and role of information system security, from access control, confidentiality/integrity, emergency planning, auditing, personnel, infrastructure, information systems, management, technology, organization, Legal compliance and other aspects comprehensively evaluate the security risk of information systems, and provide guidance for the organization of information security management [6].

(3) Purpose principle. The composition of the information security risk evaluation indicator system should be closely linked to the organization’s business objectives. The objectives of information security confidentiality, integrity and availability are developed layer by layer. The selected indicators must reflect the information that can reach the target level, so that the final The evaluation results can indeed reflect the true situation of the organization's information security [7].

(4) The principle of operability. The design indicators must have a clear meaning, and strive to be concise and practical. Generally, they should be measurable and quantifiable, and accurate data can be collected in time. For some intangible and indirect benefit indicators that are difficult to measure or difficult to collect data, we should also try to find alternative indicators as much as possible, find ways to investigate and collect indicator data, and determine statistical methods for data estimation [8].

(5) The principle of combining versatility and development. The constructed information security risk evaluation index should be applicable to different assessment scopes, that is, from a single security control system, network to the entire information infrastructure. At the same time, the established risk indicators are developmental and can be adjusted and flexibly applied according to specific organizations.

(6) The principle of consistency with the adopted evaluation method. Different comprehensive evaluation methods may have some differences in the requirements of their evaluation index system, so the constructed evaluation index should be consistent with the model method used in the information security risk assessment.

(7) The principle of meeting the needs of different personnel in the organization. Information security evaluation indicators should meet the different needs of different users in the organization, such as the needs of different levels and roles in finance, technology, law, and senior management.

3.2. Vehicle traffic information security risk assessment indicators

Information security defines that messages have security attributes such as confidentiality, integrity, availability, authentication, and controllability. This article comprehensively considers the requirements of vehicle traffic information systems and information security, and combines the analytic hierarchy process to select integrity, confidentiality and the usability constructs a tree structure of information security risk assessment indicators, and the tree model of vehicle traffic information security risk assessment indicators is shown in Figure 1.

(1) Confidentiality index system. In the vehicle traffic information system, confidentiality means that the party who owns the data or the parties who exchange the data does not want outsiders or opponents to obtain and understand the data. This article defines vehicle traffic confidentiality as: Unable to use and obtain system information normally without authorization from the vehicle traffic control center.

(2) Integrity index system. In the vehicle traffic information system, integrity means that the data is not deleted or modified by unauthorized persons during the exchange and storage, or that the legal receiver can easily determine whether the data has been tampered with. This article defines the completeness of the train control center: without the authorization of the train control center, the data information, infrastructure, services, etc. in the system cannot be modified.

(3) Usability index system. Availability in an information system means that authorized users can effectively use vehicle traffic information resources. Therefore, system reliability is the basis of availability. This article defines the availability of vehicle traffic center: The vehicle traffic center meets the requirements of authorized users to provide normal services, including the right to use software, hardware, and services.
After obtaining the various indicators of the information security risk assessment of the vehicle traffic center, this paper uses the method of expert scoring to score the indicators of the information security risk assessment of the vehicle traffic center. In order to ensure the correctness of the data, this paper selects multiple experts in different fields of vehicle transportation system and information system to score, compare each sub-scheme of the scheme layer pair by pair, and give the importance score table.

3.3. Vehicle traffic information security risk assessment index system

The vehicle traffic information security risk assessment system is divided into 4 parts: assessment preparation stage, element identification stage, risk analysis stage, report and acceptance stage. The information security risk assessment process of the vehicle traffic center is shown in Figure 2.

Different from the traditional IT system risk assessment process, because the vehicle traffic center belongs to the category of industrial control systems, there are many control devices, and the attributes of these devices are quite different. Therefore, it is also necessary to pass the information security risk of the vehicle traffic center based on the component security attributes Evaluate formal modeling and formalize the assets, vulnerabilities, and existing threats of the vehicle traffic center into the security attributes of the components. Information security risk assessment is to evaluate the vulnerability of the system, the threats it faces, and the actual impact of the vulnerability being used, and identify the security risks of the system according to the possibility and impact of security incidents. Considering the particularity of the vehicle traffic center system, in the risk analysis stage, a set of reasonable and clear impact level criteria and possibility level criteria must be formulated according to the actual situation. Therefore, this paper determines the safety attributes and information of the components in the element identification stage. The indicators of security risk assessment use the impact of component security attributes on the information security risk assessment indicators of the vehicle traffic center as risk assessment indicators to simulate the potential impact and probability of occurrence of threat scenarios considered in the risk assessment of information systems. Qualitatively identify the information security risk value of the vehicle traffic center.

Fig 2. Flow chart of vehicle traffic information safety risk assessment

Vehicle traffic information security risk assessment preparation

Asset identification → Vulnerability identification → Threat identification

Determination of risk assessment indicators → Determination of component security attributes

Security risk calculation

Security risk calculation?

Yes → Keep existing safety measures

No → Take appropriate safety measures and assess

Residual risks?

Yes → Implement risk management

No
3.4. Case verification

The vehicle traffic information security risk assessment index system is used to assess the vehicle traffic information of a certain place. In order to meet the needs of applied research, there are four grey classes in evaluation, namely, "excellent", "good", "medium" and "poor". The specific scoring criteria are as follows.

Category 1: "excellent category" with a score of 9 or above; Category 2: "Good" with a score of about 7; Category 3: "Medium class" with a score of about 5 points; Category 4: "Poor category" with a score of 2 or less.

In the risk assessment of vehicle traffic information security, 9 experts from road transport management departments, road transport information centers, road transport enterprises and universities were selected and divided into four assessment groups. There are 2 people in group 1, 2 and 4 and 3 people in group 3. The grey assessment coefficient and assessment weight obtained by the four assessment teams after assessment of each assessment index are shown in Tab.1.

| Evaluation indicators | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
|-----------------------|-------|-------|-------|-------|
| $V_1$                 | 7.3   | 7.8   | 3.4   | 0.00  |
| $V_2$                 | 7.7   | 8.1   | 3.3   | 0.00  |
| $V_3$                 | 7.4   | 7.8   | 4.1   | 0.00  |
| $V_4$                 | 7.2   | 7.9   | 5.9   | 0.00  |
| $V_5$                 | 7.5   | 7.6   | 4.8   | 0.00  |
| $V_6$                 | 7.4   | 7.5   | 3.8   | 0.00  |
| $V_7$                 | 7.4   | 7.7   | 4.7   | 0.00  |
| $V_8$                 | 7.2   | 7.8   | 4.9   | 0.00  |
| $V_9$                 | 7.6   | 8.2   | 4.3   | 0.00  |

According to Tab.1, the grey assessment weight matrix of vehicle traffic information assessment in this area can be constructed:

$$R_1 = \begin{bmatrix} 7.3 & 7.8 & 3.4 & 0.00 \\ 7.7 & 8.1 & 3.3 & 0.00 \\ 7.4 & 7.8 & 4.1 & 0.00 \\ 7.2 & 7.9 & 5.9 & 0.00 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 7.7 & 8.1 & 3.3 & 0.00 \\ 7.4 & 7.8 & 4.1 & 0.00 \\ 7.2 & 7.9 & 5.9 & 0.00 \\ 7.5 & 7.6 & 4.8 & 0.00 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 7.4 & 7.8 & 4.1 & 0.00 \\ 7.2 & 7.9 & 5.9 & 0.00 \\ 7.5 & 7.6 & 4.8 & 0.00 \\ 7.4 & 7.5 & 3.8 & 0.00 \end{bmatrix}$$

$$R_4 = \begin{bmatrix} 7.4 & 7.7 & 4.7 & 0.00 \end{bmatrix}$$
However, according to the following formula, the above two levels of evaluation indicators can be comprehensive evaluation.

\[ B_i = A_i \cdot R_i = \left( b_{i1}, b_{i2}, \ldots, b_{ig} \right) \]

where, \( A_i \) is the corresponding weight vector.

Judging from the assessment results, the vehicle traffic information security risk assessment result value in this area is 7.325. Judging from the assessment grey standard determined above, its information level is in the "good" category, indicating that the overall situation of vehicle traffic information security risk construction and development in this area is good. The evaluation results were exchanged with the four evaluation teams. The evaluation team agreed with the evaluation process and the evaluation results, accepted the judgment of vehicle traffic information security risk assessment in this area, and believed that the evaluation results were in line with the actual situation of vehicle traffic information security risk construction and development in this area.

4. Conclusions

The purpose of risk assessment is for better risk management. However, due to the complex associations between the various risk factors of vehicles and roads, this article starts from the information security criteria of confidentiality, integrity and availability, and proposes a vehicle traffic information security risk. The method of evaluation index system construction. This method can quantitatively reflect the relative size of the information security risk of each unit of the vehicle traffic system, and provide a quantitative reference for risk managers to identify unit risks and carry out effective risk management.

References

[1] Mirtsch M, Kinne J, Blind K. Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis [J]. IEEE Transactions on Engineering Management, 2020, 6(99): 1-14.

[2] Chettupuzha A J A, Haas C T. Algorithm for Determining the Criticality of Documents within a Construction Information System [J]. Journal of Computing in Civil Engineering, 2016, 30(3): 040150399.

[3] Fu C, Wang X, Zhang W, et al. A Component Security Attribute Model Driven Information Security Risk Assessment Approach for Train Control Center [J]. Tiedao Xuebao/Journal of the China Railway Society, 2017, 39(8): 77-847.

[4] Qing H, Qingsheng X, Shaobo L. The model of information security risk assessment based on advanced evidence theory[J]. International Journal of System Assurance Engineering & Management, 2017, 8(nov.suppl.3): 2030- 20353.

[5] Kumah P, Yaokumah W, Okai E S A. A Conceptual Model and Empirical Assessment of HR Security Risk Management [J]. Information and Computer Security, 2019, 27(3): 411-433.

[6] Kumah P, Yaokumah W, Okai E S A. A Conceptual Model and Empirical Assessment of HR Security Risk Management [J]. Information and Computer Security, 2019, 27(3): 411-433.

[7] Sylvester Hatsu, Martin B. Ujapka, Enoch D. Mpimwood. An examination of the extent of implementation of the information security system and IT audit system in Ghanaian Banks [J]. Journal of Mass Spectrometry, 2015, 11(11): 375-382.

[8] Chensi W U, Wen T, Zhang Y. A revised CVSS-based system to improve the dispersion of
vulnerability risk scores [J].  ece China. Information ences, 2019, 62(03): 193-195.