Research on Risk Analysis and Compliance Solution of Intelligent and Connected Vehicle Data Security

Yuran Li[1*], Hang Sun[2], Hanbing Wu[3] and Baotian Li[4]

liyuran@catarc.ac.cn[1*], sunhang@catarc.ac.cn[2], wuhanbing@catarc.ac.cn[3], libaotian@catarc.ac.cn[4]

China Automotive Technology and Research Centre Co., Ltd., Tianjin, 300300, China

Abstract. With the rapid development of intelligent and connected vehicle technology, all kinds of data security risks and problems of intelligent and connected vehicles are followed. There are a large number of data interaction scenarios in intelligent and connected vehicles. If data security issues such as non-compliant processing or tampering of important data occur, it will seriously affect driving safety, privacy security and personal safety. This paper analysed the data security threats in the entire lifecycle of data processing in intelligent and connected vehicles, summarized the technology standards and regulations in the field of automotive data security formulated by the International Standard Organization, proposed the basic principles and key technologies of data compliance, the process of data security management, the assessment and evaluation methods of data compliance, as well as the standardization recommendations and solutions. This paper is helpful to activate the value of automotive data, guide enterprise application, and ensure the high-quality development of intelligent and connected vehicle industry.

Keywords- Intelligent and connected vehicle, Data compliance, Data security management, Evaluation methods, Standardization

1. Introduction

Intelligent and connected vehicles (ICV) are equipped with advanced on-board sensors, controllers and actuators, and combined with modern communication technology, to realize information exchange and sharing between vehicles, road, pedestrian and cloud, equipped with functions of complex environment perception, intelligent decision-making and collaborative control[1]. Its application scenario is shown in figure 1. The data involved in intelligent and connected vehicles include not only the interconnection data between vehicles, vehicle and road or transportation facilities, but also the personal information of drivers, passengers and pedestrians, as well as the driving trajectory, audio, video, images, geographical information and so on[2-4]. According to statistics, an intelligent and connected vehicle generates about 10TB of data every day. Data is an essential element for enterprises to build an autonomous driving model[5-7], and it is also the core determinant of the commercialization progress of enterprises. The increasing amount of data and the changes in data storage and processing technology have brought great challenges to the industry[8]. Under the background of the close combination of artificial intelligence and big data with modern manufacturing industry, the development speed of intelligent and connected vehicle is much higher than the implementation speed of data security laws and regulations, resulting in the lag of data protection practice. How to ensure the safety of automobile data and promote the full use of data is an urgent problem[9].

ICMEIM 2023, September 08-10, Wuhan, People's Republic of China

DOI 10.4108/eai.8-9-2023.2340108

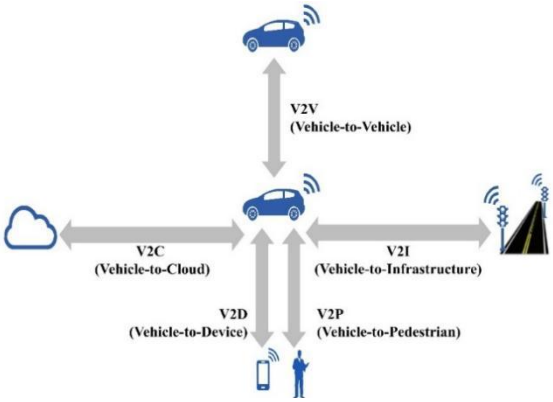

Figure 1. Intelligent and connected vehicles application scenario.

The existing problems of automobile data security include illegal cross-border transmission of important data, insufficient protection of personal information[10], automatic driving technology exacerbating data security risks[11], difficulty in free and safe data flow, nonstandard data format, lack of enforceable data security management and technical standards, and lack of experience in building data security protection capabilities.

At present, the standards of intelligent networked automobile data compliance are still in the exploration stage, The International Standard Organization has issued a series of standards, the relationship with the General Data Protection Regulation (GDPR) is shown in figure 2.

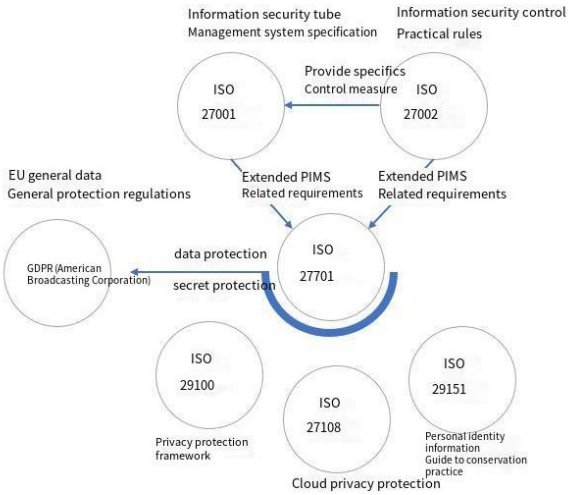

Figure 2. Relationship between ISO standards and GDPR.

The key technical standards of data compliance still exist in the following two types of problems, First, there are more principled standards than practical standards, and there is a lack of implementation guidance for manufacturers. The key technical standards of data compliance need to be based on the premise of data security and personal information security,

combined with the production practice of the industry, taking into account the needs of enterprise competitiveness and security development, and formulate reference technical standards. Second, there are more restrictive standards than fluency standards. With the development of intelligent and connected vehicles, it has become the development trend of the industry to ensure the legal, compliant and orderly flow of intelligent and connected vehicle data. Establishing a credible automotive data supervision centre and standards for the safe circulation of data that can meet the needs of high-quality development of intelligent and connected vehicles, continuously ensure data security and personal information security.

2. Life cycle risk analysis and compliance principle of ICV data processing

2.1. Life cycle risk analysis of ICV data processing

The risks in the whole life cycle of intelligent and connected vehicle data processing include data collection, data storage, data use, data processing, data transmission, data provision, data sharing, and data destruction.

Data collection is the first part of data processing activities, which determines the quality of data life cycle. Confidential collection is based on Intel SGX, AMD SEV, Arm Trust Zone and other confidential computing technology. The Trusted Execution Environment (TEE) created by the hardware builds a remote information service platform to ensure the confidentiality and integrity of the sensitive and private data collected by the vehicle and guarantee the security of the whole chain from the vehicle to the platform. After data collection, cleaning comparison and quality monitoring are carried out. Data storage is connected with the other links of data processing activities and is divided into four aspects, data isolation, database protection, data security audit, and data leakage protection. Data use includes identity authentication, authorisation authentication and access control, and the following risks include the risk of data use beyond boundaries, unclear data responsibility, privacy data leakage, and non-traceability of data. Data processing is the regularisation, transformation, filtering, desensitisation and anonymisation of data to hide sensitive information and prevent illegal use. The security disclosure and sharing of data depends on federated learning, interface security monitoring, data traceability, and data isolation technology. In the cloud computing environment, there are multiple backups of automotive data, and the data destruction operation only destroys the original data without processing the other backup data, which is easy to cause privacy leakage.

2.2. Basic principles of automobile data compliance of ICV

Data compliance management should follow the two basic principles of effective protection and safe sharing, coordinate the relationship between data security and development, and insist on paying equal attention to ensuring data security and promoting data development and utilization.

2.2.1 Principle of effective data protection

In the effective protection of intelligent and connected vehicle data, the principles to be followed include systematization and organization, classification and hierarchical management, minimum necessity and informed consent.

The principle of systematization and organization requires that automobile data processors should establish and improve the management organization system and organizational structure. Establish an automobile data security management system, clarify the responsible department and person, establish a data security emergency response mechanism, and formulate data exit management norms. Instead of formulating a separate and independent response to specific regulation and requirement. The principle of classified management requires that appropriate management requirements should be formulated according to different types of data and automobile data with different safety levels, and important data and sensitive personal information should be stored separately from other data. The principle of minimum necessity requires the automobile data processor to process automobile data legally, justly, concretely and clearly, which is directly related to automobile design, production, sales, use, operation and maintenance. Make clear the source and scope of automobile data collection, the purpose and purpose of data collection, and use the data necessary for business according to the principle of in-vehicle processing, the principle of default non-collection and the principle of application of precision range to ensure the necessity of data use. The principle of notification and consent requires that automobile data processors should inform individuals and obtain personal consent by means of user manual, on-board display panel, voice and relevant procedures for automobile use.

2.2.2 Principle of data security sharing

In the aspect of safe sharing of intelligent and connected vehicle data, in order to promote the development and utilization of data, the principles that should be followed include the general principle of data grid, the principle of true and complete data, the principle of desensitization and the principle of traceability.

The general principle of data format requires specification of data format and definition. The principle of truthfulness and integrity of data requires data producers to ensure the truthfulness and integrity of data provided when providing or sharing data, to provide basic guarantee for the circulation of data elements and the release of data value, to ensure more application value of data, and to promote the formation of intelligent and connected vehicle industry data ecology. The principle of desensitization requires that when dealing with important data related to national security, public interests, and sensitive data, automobile data processors should be anonymized and de-identified, so as to realize the interaction and sharing of desensitized data. The principle of traceability requires that when providing data, the automobile data processor should record information such as the quantity, time, demand and data receiver, and the approval records involving personal information and important data should meet the requirements of tracking the data flow process and the traceability of the responsible personnel.

3. Life Cycle Data Security Management Process of ICV

As the concrete implementation part of data security governance in the product side, the problems existing in the practices of risk identification, risk management, vulnerability management, and incident response during the whole-life process of vehicle data in conceptual stage, research and development stage, production stage, operation and maintenance stage and end-of-life stage are analysed. A framework of the whole-life-cycle data security management

process is constructed aiming at the problem that there is no enforceable policy or standard at the present time, as shown in table 1.

Table 1. Data security management framework.

process stage	conceptual stage	research and development stage	production stage	operation and maintenance stage	scrap stage
process event	project management	data security and privacy protection design	safety production control	continuous monitoring and emergency response	scrap management
	Requirements summary	development practice	____	data security reporting	used vehicle management
	requirements analysis	Security and privacy test	____	iterative update	____
	security assessment	security assessment and release review	____	security assessment and release review	____

3.1. Conceptual stage

The concept stage includes five steps, project management, requirements summary, requirements analysis, safety assessment and third-party safety management.

As the foundation and key link in the full life cycle of vehicle, enterprises initially need to clarify the market positioning of the product, user groups, and determine the basic product definition, architectural scheme and overall project plan in the conceptual stage. The comprehensiveness of the aggregated information will directly affect the results of the analysis and evaluation, and even the overall data compliance of the enterprise. Requirements summary should specify the specific types of data and field information and related instructions, clear data organisation inside and outside the demand side, the user, the responsible party and other key roles. The data security assessment based on the demand analysis mainly includes: information security threat analysis and risk assessment (TARA) based on automotive data, personal information security impact assessment (PIA) for intelligent networked vehicles, and data exit security assessment. Carrying out data security assessment is conducive to fully identifying the potential security problems faced by current enterprises and model products and formulating automotive data protection programmes, effectively strengthening the protection of important data and the rights of personal information subjects. Data security management work for third parties includes conducting audits of third-party data security qualifications, capabilities and experience, clarifying the data volume, scope, conditions, other rules for third-party data reception or processing, and signing a data processing agreement with a third party to clarify the security terms and conditions, including data lifecycle processing rules, auditing methods, and notification and assistance obligations.

3.2. Research and development stage

The research and development stage includes four steps: security and privacy protection design, development and implementation, security and privacy testing, security assessment and release review.

The cybersecurity and privacy protection around automobile data mainly includes the design of automobile data cybersecurity protection, business platform, APP, privacy protection design of vehicle-side functional services, compilation of user agreements, design review, development of cybersecurity software and hardware and privacy protection. In view of clear regulations, standards or certification requirements, it is necessary to promote relevant compliance testing and certification. In order to further verify the cybersecurity risk of automobile data, it is necessary to carry out the security penetration test of products and services. Before mass production of automobile products, it is still necessary to publish and review the safety design and privacy provisions.

3.3. Production and operation and maintenance stage

In the production stage of vehicles, production control activities such as key and certificate management involved in automobile data security protection are mainly considered. The maintenance operation stage includes four steps: continuous monitoring and emergency response, data security reporting, user exercise processing, security assessment and distribution review.

By establishing a continuous risk monitoring mechanism, we can effectively prevent improper data access and operation, and reduce security risks such as unauthorized access, data abuse and data leakage in the whole life cycle of data. Establish data security emergency response system to respond and deal with all kinds of data security incidents in a timely manner. Monitoring and emergency response include collecting security vulnerabilities, monitoring vehicle safety and privacy status and security emergency response. After the data security incident occurs, communicate and report it in time according to the relevant regulations of the state and industry. The report includes the type, quantity, content and nature of data involving vehicles and owners, the possible impact of the incident, and the disposal measures taken. Enterprises should establish a supporting management mechanism to deal with the rights and interests of customers on their personal information.

In the operation and maintenance stage, when the vehicle function is upgraded or changed, there should be a review and test mechanism for data collection and usage scenario changes. At the same time, vehicle enterprises should formulate data usage specifications, clarify the data usage scope and authority, compliance requirements, safety protection requirements, data usage restrictions. For the new demand of automobile data in the operation and maintenance stage, release and review activities before sharing and disclosure should be added.

3.4. Scrap stage

The scrapping stage includes vehicle scrapping data processing and vehicle used car transfer data processing. In the scrapping stage of vehicles, users should be provided with a perfect data clearing function, and a data deleting mechanism should be established within the enterprise to manage the deleting process of scrapped data and establish a corresponding evaluation mechanism to ensure the effectiveness of the mechanism. When the vehicle is transferred, it should provide users with a perfect data clearing function, so that user can confirm that their relevant personal data can not be recovered at the vehicle.

4. Key technologies and assessment methods of data compliance

4.1. Research on key technologies of data compliance

The basic supporting technology of data compliance is data format standardisation, which is divided into static data and dynamic data according to whether it comes from or flows into big data environment, defining the standard format of the data respectively, and clarifying the scope of data that needs to be standardized. The first and foremost part of data processing activities is data acquisition, which can directly read the data from the in-vehicle bus and each sensing module, or through the interface of the operating system. Data needs to be re-examined, calibrated and quality monitored. Access control, physical environment isolation, and encryption are used to ensure the confidentiality, integrity and availability of data storage. Data processing includes anomalous behaviour identification, data anonymisation, and data desensitisation to prevent improper use of data, which is important guarantee for data compliance.

4.2. Data compliance assessment methods

The data compliance assessment process includes the licence application of automotive data processors, the initial assessment by assessment agency, the assessment of data change, the data security test and supervisory inspection. As shown in figure 3, the data of security compliance assessment is divided into basic vehicle data, perception data, decision-making data, operation data and user data. Two aspects of assessment are carried out for these five types of data, namely, data security management system audit and data security technology assessment.

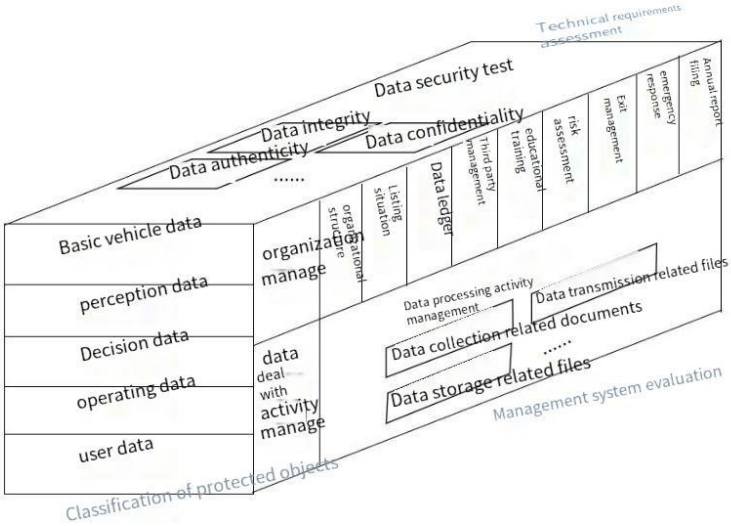

Figure 3. Data Security Compliance Assessment.

System audit is to check the compliance of the data security management system of automobile data processors, that is, whether the data processing activities of automobile data

processors comply with relevant data security laws and regulations, including the inspection of system documents and implementation. Evaluate the documents and implementation of 12 parts, including organizational structure, external partner management, data ledger, risk assessment, safety annual report, emergency response, education and training, data collection, data transmission, data storage, data processing and data deletion. Data security testing is an inspection of data compliance, integrity and authenticity in the form of field tests.

Data security protection in the process of vehicle data collection and transmission to vehicle data processor, including data capture, fixed-point transmission confirmation, data storage verification and data verification, involving package capture analysis, penetration test, interface scanning, storage verification and other testing means, covering all data life cycle processing activities such as data collection, storage, use, processing, transmission, provision and disclosure, mainly including in-vehicle data security, out-of-vehicle environment security, personal information security and data exit.

Data security oversight inspections include annual reviews and routine oversight inspections. The way is on-site data verification. Operation process is as follows, First, through vehicle data capture, the consistency between the collected data and the vehicle state and the consistency between the data uploaded by the vehicle and the number and format definition of the application fields of the vehicle data processor are detected. Secondly, the authenticity of vehicle data fixed-point transmission is detected and the data compliance and integrity are confirmed. Finally, check the correspondence between the plaintext standardized data stored by the regulatory agency and the original data obtained by the platform side of the automobile data processor.

Data security compliance evaluation can adopt item-by-item evaluation scoring system, and evaluate the overall data compliance based on system audit and data security test results. It can be examined and tested by means of document review, personnel interview, on-site inspection and real vehicle test. The results of each evaluation item of system audit are divided into conformity, basic conformity and non-conformity, and the results of each test item of data security test are divided into passing and failing.

The principle of system audit and evaluation is to establish and improve the system involved in the corresponding evaluation items according to the requirements of laws and regulations. The relevant system documents are complete and effective, and it is judged to be in compliance when the implementation is completed. The evaluation principle of test results is to design test cases according to laws and regulations to carry out real vehicle tests, and it is judged as passing if no defects or loopholes involved in the corresponding test items are detected. The principle of data security compliance evaluation is that there are no nonconformities in the data security system audit of the evaluated automobile data processor, and all the data security test items have passed, which is considered as excellent data security, and the basic conformity items in the evaluation items can be rectified in combination with suggestions.

5. Solution suggestions

In order to ensure the effective protection of data, it is necessary to establish a data security guarantee system from decision-making level to technical level, from management system to the support of tools. Data security governance consists of four levels: governance level, management level, execution level and supervision level, and its important links include data classification, data security risk management, and data security incident response.

In terms of data security governance, it is recommended to standardize data classification principle, catalogues and management requirements. Combined with the characteristics of automotive data, a data security governance system framework is established. Formulate automotive data security risk classification, data security risk assessment specifications, vulnerability classification and grading guidelines, and emergency management guidelines. Build an automotive data security capability maturity model to guide enterprises in four dimensions: organisational construction, institutional process, personnel capability and technical tools.

In terms of automotive data security risk management, the relationship between the various elements of automotive data risk should be determined. In the process of assessment and implementation, data assets, data application scenarios, compliance, data threats, vulnerability, risk analysis and evaluation need to be determined. The risk level, risk description, risk value, risk treatment steps and responsible person need to be determined in risk treatment measures.

In terms of data classification, a dynamic balance between data security and industrial innovation should be maintained, exploring the method of automotive data classification in cross-fields, providing practical guidance on data security management for the whole industry, and coordinate with the top-level design of laws and regulations. In data security assessment, the scope of assessment, the conditions of the assessment, the categories of the assessment and the assignment of weights should be confirmed.

In terms of sensitive information and important data, according to the desensitisation needs of human face and license plate, the standards related to desensitization technology are formulated, including which feature information needs to be desensitised, the degree of desensitisation, how to verify the effect of desensitisation, and dynamically adjust the scope of important data[12], set up an important data management department, and regularly update and maintain the important data of intelligent and connected vehicle. Enterprises should establish standardised data security management process, regular self-inspection and optimisation, deal with security risks such as network attacks and network intrusions in a timely manner, reduce data security threats, and enhance the ability of emergency response to security incidents.

6. Conclusion

With the increasing production and sales volume of intelligent and connected vehicles, data security continues to attract attention and gradually becomes the focus of the industry. Previously, a lot of research work has been carried out by scholars on the functional safety of intelligent and connected vehicle. However, the research on data security is still in a blank stage. This paper analysed the data security threats in the whole life cycle of intelligent and

connected vehicle data processing, summarized the technology standards and regulations in the field of automotive data security formulated by the International Standard Organization, as well as the key technologies of data compliance, specified the basic principles of data compliance, proposed the process framework of the data security management in the whole life cycle of intelligent and connected vehicle, data compliance assessment and evaluation method. Solutions and standardisation recommendations are given. In this paper, the in-depth research on data security of intelligent and connected vehicle is helpful to accelerate the application of intelligent and connected vehicles, reduce the data security risk, protect the privacy and security of drivers and passengers, and has certain reference value for the research and development stage of enterprises, promote the healthy and orderly development of the intelligent and connected vehicle industry.

References

[1] Ministry of Industry and Information Technology of the P.R.C., 2023. Guide for National IoV Industrial Standard System Building (Intelligent and Connected Vehicle).

[2] Chen L, Liu K, Zhou B and Li Q. (2021) Key technologies of multi-agent collaborative high definition map construction. *Acta Geodaetica et Cartographica Sinica*, **50(11)**:1447-1456.

[3] Qin Z, Li Y and Liu Y. (2020) Discussion on compliance of crowdsourcing update of high-precision maps. *Automobile & Parts*, **16**: 62-64.

[4] Liu J, Dong Y, Zhan J and Gao K. (2019) Thoughts and Suggestions on Autonomous Driving Map Policy. *Engineering Science*, **21(3)**: 92-97.

[5] Pang Z, Tang C and Li G. (2022) A Complexity Quantification Method for Safety of the Intended Functionality Scenario Library. *Chinese Journal of Automotive Engineering*，**12(1)**:12-17.

[6] Li P F, Wang M and Che Y. (2022) Risk Assessment Method of Road Test Scenario Based on Vehicle- to-Vehicle Crashes. *Journal of Transportation Engineering*, **22(03)**: 88-96.

[7] Wang R, Sun Y and Song J. (2021) Evaluation Method and Test Verification of Road Test Scenes for Autonomous Vehicles. *Automotive Engineering*, **43(04)**: 620-628.

[8] Harn, L., Hsu, C.F., Xia, Z. (2022) General logic-operation-based lightweight group-key distribution schemes for Internet of Vehicles. *Vehicular Communications, 34: prepublish.* doi:10.1016/J.VEHCOM.2022.100457.

[9] Zheng Z. (2019) Privacy protection in the era of artificial intelligence. *Science of Law - Northwest University of Political & Law*, **37(2)**: 51-60.

[10] Cheng X. (2018) Personal Data Rights in the Age of Big Data. *Social Sciences in China*, **3**: 102-122+208.

[11] Bayat, M., Barmshoory, M., Rahimi, M. (2015) A secure authentication scheme for VANETs with batch verification. *Wireless Networks*, **21(5)**: 1733-1743.

[12] Yuan K and Yan H. (2022) The Logic Elucidation and System Construction of Categorical and Hierarchical Data Protection ——Centering on the Recognition and Protection of Important Data. *Forum on Science and Technology in China*, **7**: 167-177.