ISSN: 2688-8645

Research on Vehicle Data Safety Activities for Vehicle Development

Junda Li[a], Jue Wang[b], Kexun He[c], Xintian Hou[d], Yueyou Wang[e]

CATARC Automotive Test Center (Tianjin) co., Ltd., Tianjin, 300000, China

[a]lijunda@catarc.ac.cn, [b]wangjue@catarc.ac.cn, [c]hekexun@catarc.ac.cn, [d]houxintian@catarc.ac.cn, [e]wangyueyou@catarc.ac.cn

Abstract

Summarize the exploration experience of data security engineering and privacy engineering at home and abroad, and analyze the applicability of the existing methodology to the automobile industry. Based on the practical experience related to data safety in the automobile industry, the data safety activities in the vehicle development process are analyzed one by one. According to the existing work basis, the future automotive data safety activities based on vehicle development and development are prospected.

Keywords

Automotive Data Safety Engineering; Vehicle Research and Development; Privacy Engineering; Risk Assessment.

1. Introduction

With the rapid development of intelligent and connected vehicles, the types and number of vehicle data processing have increased significantly, and the problems of data security and personal information protection have become increasingly prominent. In recent years, relevant laws and regulations and standards related to data security and privacy protection have been released at home and abroad, providing guidance for the construction of data security in the automobile industry. Among them, both the privacy protection from the design mentioned in the General Data Protection Regulations (GDPR), and the data security protection of vehicle research and development required by domestic data security regulations and standards, all put requirements for the integration of vehicle research and development process and data security.

At present, the field of automotive data safety engineering is still in its infancy, and no automotive data safety engineering methodology or relevant practice guidelines have been formed at home and abroad to guide the implementation of relevant laws, regulations and standards into specific research and development activities. Therefore, this paper studies how to integrate the data safety requirements into each link of the vehicle research and development process, and provides the overall scheme reference covering the objectives, control methods and implementation methods for the relevant practices of the industry.

2. Data Security Engineering Exploration

2.1. International Related Exploration

In the 1990s, Canadian scholar Ann Cavoukian proposed the privacy design theory (PbD) and innovatively proposed the integration of personal information protection into R & D design. In October 2010, the International Data Protection and Privacy Committee adopted a unanimous resolution to make privacy design theory a crucial part of future privacy protection.

ISSN: 2688-8645

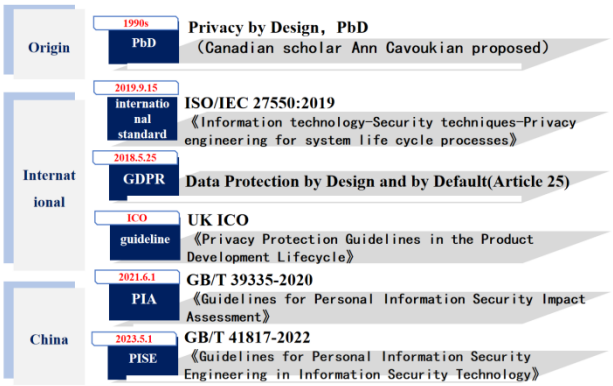

Figure 1. Privacy design developments

The EU GDPR, published in 2018, includes privacy design in Article 25 as a necessary requirement [1]. In 2019, the international standard ISO / IEC 27550:2019 "Privacy Engineering for the Life-Cycle Process of Information Technology Security Technology System" was released, the standard is to increase the activities, output and guidance of privacy engineering on the basis of ISO / IEC / IEEE 15288. Based on GDPR and international standards, the UK has released the ICO Privacy Protection Guidelines in the Product Development Life Cycle to help engineers to understand how to incorporate design and default data protection concepts when developing products or services.

In addition to European countries, other countries continue to explore how to conduct data security engineering practices. In 2012, the Federal Trade Commission (FTC) proposed a new framework for privacy design, with three core principles: privacy protection, simplified selection simplification, and transparency through design [2]. In 2020, the National Institute of Standards and Technology (NIST) released the American Privacy Framework 1.0-A Tool for Improving Privacy through Corporate Risk Management [3]. The purpose of the standard is to guide companies on how to manage the privacy risks caused by their products and services, and to identify data security and privacy protection regulations at home and abroad. At the same time, Brazil, Spain, Japan and other countries, in order to integrate with the EU GDPR and seek the qualification of EU cross-border data whitelist, have carried out legislation on data security and privacy protection, and also mentioned the relevant concepts of privacy design in the regulations, but there is still a certain lag in practice [4]

2.2. Relevant Exploration in China

In 2020, GB / T 35273-2020 "Information Security Technology Personal Information Security Standard" standard was released and implemented. Although the standard does not specify the combination of personal information protection and research and development, it also provides corresponding guidance for enterprises in the research and development and engineering practice related to personal information processing.

On August 20,2021, the personal information protection law of the Peoples Republic of China, the upper law in the legal law stipulates the personal information processing in personal information data processing activities should abide by the principles and should be matters, the privacy design principle through the form of specific requirements into the legal requirements, namely the enterprise want to meet the requirements, we must consider the laws and regulations requirements into research and development activities and engineering practice.

In 2022, GB / T 41817-2022 "Information Security Technology Personal Information Security Engineering Guide" was released and implemented. The standard mainly covers the privacy design requirements of the whole life cycle of the ICT system.

ISSN: 2688-8645

On November 17,2023, four ministries jointly issued the implementation of intelligent made car access and road traffic pilot work notice, which clearly put forward to declare pilot automobile enterprises should meet the requirements of product process, in product research and development design and production of all stages of the necessary data security activities, to ensure the whole life cycle of automobile products and automobile data whole life cycle safety. Although the regulation is only for L3 intelligent connected vehicles and above, with the implementation of the pilot, the data safety engineering of the automotive industry has initially defined the direction.

In 2024, GB / T 44464-2024 "General Requirements for Automotive Data" was released and implemented. The standard proposes that automotive data processors should at least formulate a data security process management system for r & D, design and manufacturing links.

2.3. Suitability Analysis of the Auto Industry

First of all, by comparing the definitions of data and personal information in the Data Safety Law of the Peoples Republic of China and the Personal Information Protection Law of the Peoples Republic of China, the data is broader than personal information. Focusing on the automobile industry, the definition of automobile data in China includes at least personal information and important data, as well as the data related to automobile products that are neither personal information nor important data. According to the Civil Code of the Peoples Republic of China and relevant international definitions, privacy is less than personal information. Therefore, the privacy design and personal information security engineering cannot cover the data security engineering in the applicable objects and scope.

Secondly, the existing privacy design framework, product development privacy protection guidelines and personal information security specification are universal requirements for the whole industry, targeted and difficult to meet the needs of the automobile industry; mainly for ICT system, ICT system engineering and automobile research and development, the automotive industry involves a wide range of supply chain, complex operational environment, multi-field crossover and multi-department supervision, and the personal information protection engineering for ICT system cannot solve the practical problem of automobile research and development data security engineering.

In addition, the relevant regulations and standards issued and implemented by the domestic automobile industry have not launched the automobile data safety engineering content in detail, and the industry is still actively exploring in this direction.

Although the existing regulations and standards cannot be directly applied, the framework, structure, process methods and ideas can be fully used for reference.

3. Analysis of Vehicle Data Safety Activities during the Vehicle Development Process

In practice, the main activities of the whole life cycle data safety engineering are summarized. Taking the vehicle development process as an example, the vehicle data safety activities in the vehicle development process are analyzed.

3.1. Clear Data Security Objectives and Scope

This stage defines the overall data safety objectives of the vehicle and the scope of functions related to data safety. By sorting out the automotive data safety regulations, mandatory standards and the non-mandatory requirements expected to be input into the project team, the data safety goal of the vehicle is formed. Transform the input regulations and standard requirements into specific technical and management requirements to form the design baseline

ISSN: 2688-8645

requirements of the vehicle. Secondly, according to the classification and classification of vehicle data, the functions related to vehicle data safety are screened in the function list.

3.2. Combing the Functional Data Processing Situation

The data security team conducts research and interview based on the functional scenarios, or the functional team combs them out by itself to determine the selected vehicle data processing of the functions related to the vehicle data security. When sorting out, the processing activities and protection measures taken by the car terminal, cloud and mobile APP terminal should be differentiated.

By combing the first version of the automotive data asset management ledger or a list of functional data, in order to facilitate the subsequent data assessment, it is suggested to comb the data flow chart is divided into two dimensions, the horizontal dimension is the object of the data or flow, may include vehicle, enterprise cloud, mobile, third party, service providers, etc. The vertical dimension is the whole life cycle of data, namely data collection, storage, transmission, use, processing, providing, and deleting.

3.3. Risk Assessment

Identify the whole data processing activities may involve the data security risk, through the data flow chart auxiliary risk identification, combined with the horizontal and vertical two dimensions (data flow through the object, the whole life cycle of each link) for data flow chart on each path, each object, each stage of analysis, identify the function of data processing activities may exist risks.

At present, the risk is divided into two levels. The first level is the compliance risk, that is, the risk arising from the failure to meet the compliance requirements, and the second level is the security risk, that is, the security risk that may occur in terms of resources, operations and related parties after the compliance requirements are met.

3.4. Requirements Design and Risk Disposal

For the data security risk assessment results, the risk management recommendations are given based on the design baseline requirements. Combined with the risk disposal suggestions, a product demand document involving the security function of automobile data is formed. Each function may involve the segmentation of multiple scenarios and involve multiple data processing activities.

3.5. Requirements Design Review and Function Development

After the functional product requirements document is formed, the corresponding review should also be conducted to avoid the unrecognized risks. After passing the review, the function will be developed, and the design scheme will be formed and implemented according to the requirements.

3.6. The Risk Assessment is Continuously Updated

Since the function definition in the early concept stage may change in the subsequent R & D design and even production process, when the functional data processing activities change may introduce new risks, the risk assessment should be carried out for the function, and the disposal plan should be proposed for the identified risks to complete the risk disposal.

3.7. Test and Verification

In this stage, after the implementation of the design scheme, test cases and execution tests can be prepared for the platform or vehicle, and system level and vehicle level test cases and corresponding test reports can be formed [5]. According to the problems and risks found in the test, put forward the corresponding rectification plan and disposal measures.

ISSN: 2688-8645

The rectification effect is verified by means of test and verification, confirming that all the identified risks have been closed, and the product achieves the expected data security goal, forming a closed loop of overall automotive data security.

3.8. Form the Vehicle Development Data Safety Process Through Practice

Through specific engineering practice, the division of responsibilities, input and output, specific requirements are defined, and the data safety process of vehicle development is finally improved and formed.

The above is the main content of the data safety engineering practice in the stage of vehicle research and development. The main purpose of this practice is to form a vehicle data safety management system oriented by vehicle data safety, and guide enterprises to implement vehicle data safety through effective organizing activities and matching corresponding resources.

4. Outlook of Vehicle Data Safety Activities based on Vehicle Development

Compared with other industries, the data security of the automobile industry is characterized by the automobile has a long life cycle, integrates a variety of systems and functions, continuous operation and maintenance involves many relevant parties, and may affect the safety of customers life and property, social and public environment, and even national security[6]. Vehicle once shape the design rolled off the production line, then the data safety rectification, not only high cost and low income, and the rectification dead Angle, so the automotive data safety engineering, through engineering practice, ensure that the vehicle after the offline can achieve data security, and continue in a state of data security, from the perspective of positive data security has become an inevitable choice.

In the future, we will work with the industry to carry out automotive data safety engineering research, form specific methodology and operational guidelines, and clarify the specific data security activities, nodes, input and output of each stage of the research and development process. After achieving this goal, the idea of risk management will be further integrated into the automotive data safety engineering, forming the automotive data safety risk assessment methodology juxtaposed with functional safety HARA and information security TARA.

5. Conclusion

At present, different enterprises have different r & d process methodology, different internal structure and division of labor. In practice, the vehicle data security activities carried out in each link of the vehicle development process are also different, and the level is uneven. Therefore, it is necessary for the industry to build consensus, standardize the automotive data safety engineering through developing standards, and guide enterprises to integrate the regulations and standards issued by different competent departments into the research and development process, so as to effectively realize the safety and compliance of the whole life cycle of products and data.

References

[1] Shah A .HOW GDPR IMPACTS ENGINEERING[J].Mechanical Engineering,2018,140(10):24-24.

[2] Hiller S J ,Russell S R .Privacy in Crises: The NIST Privacy Framework[J].Journal of Contingencies and Crisis Management,2017,25(1):31-38.

[3] Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents[J].Berkeley Technology Law Journal,2013,28(2):1333-1413.

ISSN: 2688-8645

[4] Brancher M P ,Thomaz C A .Brazilian Data Protection Law – A New Scenario For Business In Brazil Compared To Eu-Gdpr[J].Computer Law Review International,2018,19(4):130-132.

[5] Li Y ,Xia X ,Wu H , et al. Research on the requirement decomposition and test verification for vehicle data security[J].Journal of Electronics and Information Science,2023,8(6).

[6] S. L ,T. M .DATA SECURITY CHALLENGES IN SELF-DRIVING CAR[J].The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,2022, XLVIII-4/ W3-202261-66.