ISSN 2616-7433 Vol. 4, Issue 7: 47-52, DOI: 10.25236/FSST.2022.040709

On the Methods of Dealing with OTA Compliance under the Policy Environment at Home and Abroad

Yan Li[1,*], Hailong Zhu[1], Hongwei Guo[1], Jindai Qu[1], Yan Ji[1], Yingxuan Tao[1]

[1]China FAW Group Co., Ltd., Changchun, China
**Corresponding author: liyan41@faw.com.cn*

Abstract: *In recent years, with the continuous development of intelligent networked vehicles, there are more and more information exchanges between vehicles and the outside world. Automobile OTA has become one of the important means to ensure automobile competitiveness. The regulatory requirements for OTA at home and abroad are also higher and higher, and the relevant standards are continuously formulated and issued. The part related to information security in OTA test is the focus of the test. Automobile enterprises need to establish relevant capabilities in time and respond effectively.*

Keywords: *OTA, Information Safety, Standard, Test*

1. Introduction

Under the great transformation trend of the intelligent networked automobile industry, the automobile is no longer just a traditional means of transportation, but a new generation of intelligent mobile space with multiple functions such as transportation, entertainment, office, and communication at the same time, as well as the upgrade of application terminals. Driving assistance systems, car networking systems, and related electronic equipment for intelligent cockpit systems that realize intelligent networking functions have gradually become the focus of R&D and application in the automotive electronics industry. Software upgrade OTA has gradually become an important means and method for car companies to improve product competitiveness, but it also brings a series of information security issues.

Compared with the information security issues in the traditional IT field, automotive information security is more complex. The security risks faced by automotive information security are greater, it is more difficult to monitor the electronic status of the vehicle, and network security is more difficult to guarantee. At the same time, the life cycle of the whole vehicle is longer. If there are network security problems in the later stage of R & D, the rectification cost will be higher and the period will be longer.

Table 1: Comparison of automotive network security and traditional IT information security.

	Automotive Cybersecurity	Traditional IT Information Security
hardware	Numerous models, various controller forms, and a high degree of customization	single, standardized
software	The use of embedded systems requires high system real-time performance	Universal operating system (windows, linux, mac)
communications protocol	The functional network is more complex; protocols such as CAN, LIN, Flexray, etc.	internet protocol
attack environment	Park in a parking lot or drive on a public road (close-range attack + long-range attack)	Hidden computer room (remote attack)
attack portal	Network entry + physical entry (USB, OBD, etc.)	web portal
Hazard Dimensions	Personal harm, social harm, national harm, data privacy, property security	Data Privacy, Property Security

The automobile industry chain is long and involves many participants such as OEMs, component suppliers, network operators, content and service providers, and faces greater risks. From the perspective of the automotive industry chain, it currently includes three major parts: cloud, management, and end. The cloud includes software and data providers, service providers, the middle end includes equipment providers and communication service providers, and the bottom end includes automobile manufacturers, automotive electronic system suppliers, component suppliers, and software suppliers.

ISSN 2616-7433 Vol. 4, Issue 7: 47-52, DOI: 10.25236/FSST.2022.040709

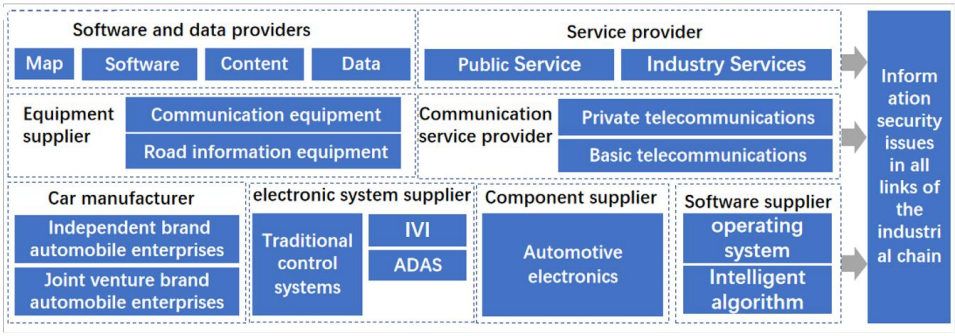

Figure 1: Information security issues in each link of the industrial chain.

To sum up, automotive OTA brings a series of information security issues, and due to the particularity of vehicle products, it poses considerable challenges to how to effectively deal with them.

2. Domestic and foreign policy analysis

2.1. Foreign standard situation

The World Forum for Harmonization of Vehicle Regulations (WP.29) under the United Nations Economic Commission for Europe ("UNECE") officially implemented two important regulations on automotive cybersecurity and OTA on January 1 this year, namely "Regulation No. 155 - Cybersecurity and Cybersecurity Management System", "Regulation No. 156 - Software Update and Software Update Management System", applied to the 54 contracting parties of UNECE "1958 Agreement" (China is not among them), has become a new strong inspection item for multinational vehicle access. China is one of the 27 parties to the UNECE "1998 Agreement", and its relevant access regulations are also being formulated.

Table 2: Foreign laws and regulations.

Foreign information security related regulations	Foreign information security related standards
United Nations WP.29/GRVA "Framework document on automated/autonomous vehicles"	ISO/SAE 21434 "Road vehicles – Cybersecurity engineering"
United Nations "Regulation No. 155 - Cybersecurity and Cybersecurity Management System"	ISO PAS 5112 "Road vehicles – Guidelines for auditing cybersecurity engineering"
United Nations "Regulation No. 156 - Software Update and Software Update Management System"	ISO 24089 "Road vehicles – Software Update engineering"
EU GDPR"General Data Protection Regulation"	SAE J3101 "Requirements for Hardware-Protected Security for Ground Vehicle Applications"
"EU Cybersecurity Act"Cybersecurity Act-Data Protection	SAE J3138 "Guidance for Securing the Data Link Connector (DLC)"
EU "General safety regulation"	VDA: Recall Management Using Over-the-Air Updates
EU "Cybersecurity Act"	PAS 1885-2018 The Fundamental principles of automotive Cyber security specification
EU"C-ITS Delegated Act"	2019 "Technical Reference for Automotive Vehicles" (TR68)
Foreign information security related regulations	Foreign information security related standards
United Nations WP.29/GRVA "Framework document on automated/autonomous vehicles"	ISO/SAE 21434 "Road vehicles – Cybersecurity engineering"
United Nations "Regulation No. 155 - Cybersecurity and Cybersecurity Management System"	ISO PAS 5112 "Road vehicles – Guidelines for auditing cybersecurity engineering"
United Nations "Regulation No. 156 - Software Update and Software Update Management System"	ISO 24089 "Road vehicles – Software Update engineering"
EU GDPR "General Data Protection Regulation"	SAE J3101 "Requirements for Hardware-Protected Security for Ground Vehicle Applications"
"EU Cybersecurity Act" Cybersecurity Act-Data Protection	SAE J3138 "Guidance for Securing the Data Link Connector (DLC)"
EU "General safety regulation"	VDA: Recall Management Using Over-the-Air Updates
EU "Cybersecurity Act"	PAS 1885-2018 The Fundamental principles of automotive Cyber security specification
EU"C-ITS Delegated Act"	2019 "Technical Reference for Automotive Vehicles" (TR68)

It can be seen that foreign countries are actively formulating standards related to information security and OTA. It is also necessary to actively carry out standard-setting work in China.

ISSN 2616-7433 Vol. 4, Issue 7: 47-52, DOI: 10.25236/FSST.2022.040709

2.2. Domestic standard situation

"General technical requirements for software update of vehicles", "Technical requirements for vehicle cybersecurity" Referring to foreign R155 and R156 standards, the mandatory conversion is underway. Among them, the final draft of the standard "General technical requirements for software update of vehicles" has been completed.

Table 3: Estimated progress of relevant domestic standards.

first batch	1	"General technical requirements for vehicle cybersecurity"	Submit for approval	2021.9
	2	"Technical requirements and test methods for cybersecurity of remote service and management system for electric vehicles"	Submit for approval	2021.9
	3	"Technical requirements and test methods for cybersecurity of on-board information interactive system"	Submit for approval	2021.9
	4	"Technical requirements and test methods for cybersecurity of vehicle gateway"	Submit for approval	2021.9
	5	"Technical requirements and test methods for cybersecurity of electric vehicle charging system"	Project establishment	2022.3
second batch	6	"General technical requirements for software update of vehicles"	Project establishment	2022.12
	7	"The technical requirement of vehicles diagnostic Interface cybersecurity"	Submit project	2022
	8	"Vehicles Cybersecurity incident response management guideline"	Submit project	2022
	9	"Risk assessment specification for Automotive information Security"	Submit project	2022
The third batch	10	"Technical requirements and test methods of vehicle cybersecurity "	Pre-research	2023
	11	"Road vehicles—Cybersecurity engineering"	Submit project	2022
fourth batch	12	"Technical requirements for commercial password application of intelligent networked vehicles"	Pre-research	2023
	13	"Technical requirements of intelligent networked vehicle digital certificate"	Pre-research	2023

3. Coping means

3.1. Establish a network security testing system

Network security testing is divided into penetration testing and compliance testing, which complement and complement each other.

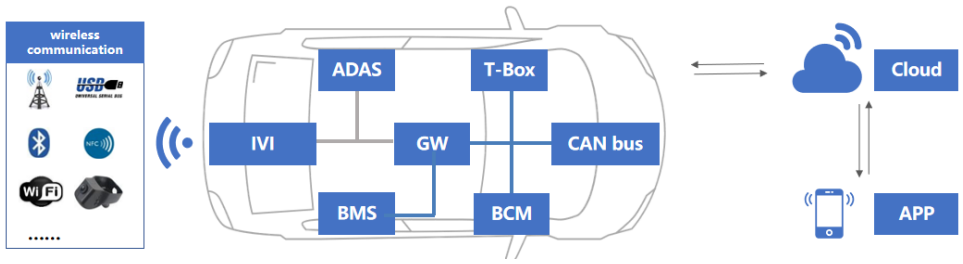

Figure 2: OTA operation system.

OTA needs to guarantee the following security:

(1) Software security: operating system security, application software security, business security, source code security

(2) Hardware security: firmware extraction, chip security, debugging interface, firmware reverse

(3) Communication security: network sniffing, encryption verification, protocol testing, traffic monitoring

(4) Data security: secure storage, secure deletion, permission testing, encryption algorithm cracking

3.1.1. Penetration test

In order to ensure the safety of OTA, it is necessary to conduct thorough tests on the whole vehicle, parts, in-vehicle communication, out-of-vehicle communication, mobile APP, and cloud server, which

ISSN 2616-7433 Vol. 4, Issue 7: 47-52, DOI: 10.25236/FSST.2022.040709

can be roughly divided into the following steps:

Vehicle topology analysis: analyze the bus topology of the vehicle, analyze the interaction function between each ECU, and analyze whether the in-vehicle communication data adopts SecOC communication encryption and other security mechanisms from the perspective of in-vehicle communication;

Radio function analysis of the whole vehicle: analyze the radio functions of the whole vehicle, such as Bluetooth, WiFi, NFC, ble, etc;

Parts function analysis: analyze whether key ECUs such as BCM, SCM, and ALCM run embedded file systems, and whether there are hardware and software interfaces for external communication;

Analysis of off-vehicle communication: analyze whether the off-vehicle communication adopts HTTPS or a common communication protocol or private communication protocol with the same or higher security level for off-vehicle communication. The communication data includes but is not limited to periodic reporting of vehicle data, vehicle status detection, and control commands. upload and download, etc.;

Mobile APP analysis: analyze the communication method (cloud or BLE) between the Android and IOS mobile APPs and the vehicle, and simply analyze whether the APP adopts shelling, obfuscation, etc. to protect the security of the APP itself;

Cloud server analysis: analyze whether the communication between the cloud service and T-BOX and IVI adopts a virtual private network, and analyze whether the cloud server adopts a firewall and other security mechanisms.

Table 4: Component Test Methods.

Test item	Test method
Classic Bluetooth pairing mode test	Analyze the pairing data and whether the connection protocol adopts a qualified encryption algorithm and whether it complies with the Bluetooth pairing security standard.
Classic Bluetooth Protocol Test	For the L2CAP/SDP/RFCOMM/AVRCP/A2DP/HFP-AG/BNEP protocol of the Bluetooth protocol, the protocol robustness test and the fuzzing test of the unknown vulnerability protocol stack and driver are carried out.
Classic Bluetooth Public Vulnerability Test	Open vulnerability scanning for CVE vulnerability Library
Classic Bluetooth Hijacking Test	Perform a Bluetooth man-in-the-middle attack against the car and hijack the intermediate data. Mainly detect whether the Bluetooth communication process is safe and reliable
Bluetooth sniffing	Perform data sniffing from the Bluetooth connection, pairing, authentication, transmission and other processes to detect whether there will be information leakage and key leakage vulnerabilities
BLE Debugging interface security	Disassemble the hardware shell and analyze whether there is a debugging interface
BLE firmware extraction	Use the debugger to extract the firmware of the Bluetooth module
BLE authentication security test	Analyze whether the authentication using the BLE communication protocol has defects such as identity authentication override, password bypass, etc.
BLE encryption algorithm crack	Capture BLE communication key interaction data, whether brute force attack can be performed

3.2. Establish a network security testing system

3.2.1. Standard compliance test

In April 2021, the “General technical requirements for software update of vehicles” was changed from a recommended national standard to a mandatory national standard. It is the first mandatory national standard in the field of domestic automotive software upgrades. The drafting work has been completed. Automotive OTA (Over the Air) software upgrade technology utilizes OTA cloud platform, wireless network, and on-board OTA master node to complete the remote upgrade of vehicle ECUs. The software upgrade manager publishes upgrade tasks on the OTA platform, and the car-end/owner APP compares the previous Notification of upgrade activities and upgrade results.

ISSN 2616-7433 Vol. 4, Issue 7: 47-52, DOI: 10.25236/FSST.2022.040709

Figure 3: Architecture diagram of automotive software upgrade system.

While the automotive software upgrade brings technological innovation, it also hides certain safety and regulatory risks, which have attracted great attention from the industry, such as the consistency of vehicle software versions before and after the upgrade, malicious tampering of upgrade packages, silent upgrades, and upgrades that affect driving safety, etc. .The “General technical requirements for software update of vehicles(Draft)”standard specifies the general requirements, functional requirements and safety requirements for automotive software upgrades, including the authenticity and integrity of the upgrade package, software identification code update and reading, user notification, user confirmation, etc. 11 Article requires the corresponding test method.

The test for this part requires the use of the following test equipment, including: automotive vulnerability scanning platform, Ethernet application layer test system-bus transceiver, etc.

The test process is roughly as follows: the enterprise needs to issue the update package data through the cloud platform, tamper with the data package through the device, read the version number, and verify the information security; the enterprise needs to provide the necessary documents such as upgrade strategy and security mode, The vehicle is placed on the hub, and the relevant vehicle functional verification tests are carried out.

3.2.2. OTA automated testing

Currently, the number and frequency of upgrades of automotive controllers that support OTA (such as car machines, TBOX, ADAS, etc.) are increasing. However, manual OTA testing is inefficient and has large errors, which lengthens the R&D test cycle for software upgrades. In order to solve the problems in manual OTA testing, it is necessary to adopt an automatic OTA test solution for automobiles, and develop a simulation test module for R&D verification, From the perspective of OTA's full functions, all scenarios and stability, it supports single-component, system bench, and vehicle-level OTA automated testing.

The simulation test module includes the main process simulation subsystem, the master node simulation subsystem, the slave node simulation subsystem, and the abnormal scene simulation subsystem, the self-developed automated test software calls each subsystem in the automated test process to realize test scenarios of upgrade process, functional status, abnormal scenarios, and stability.

OTA automated test system features:

(1) It supports secondary development in multiple scenarios, and can write development scripts to add test cases for new development verification requirements after simple training;

(2) Realize a vehicle-level simulation environment, which can not only meet the simulation test in the real vehicle environment, but also support the system simulation test in different ECU development stages;

(3) Reduce labor time cost, improve test efficiency and test accuracy, shorten R&D cycle and reduce R&D cost.

There are also some problems in the simulation test, such as the adaptability of the simulation test cabinet. At present, the development methods and methods of domestic OTA systems have not been completely unified, resulting in large differences among various car companies. Therefore, how to make one automated cabinet can efficiently adapt to the models of multiple companies is a problem that needs to be solved urgently. The current solution is to ensure the modularization of the underlying code and development logic of the automation cabinet, and to adapt to the upper code layer. Enterprises need to

ISSN 2616-7433 Vol. 4, Issue 7: 47-52, DOI: 10.25236/FSST.2022.040709

provide corresponding documents, so as to ensure that the automation test cabinet can truly be automated.Overall, automated testing has indeed brought a great improvement in test efficiency and test accuracy.

4. Conclusions

The development of OTA for automotive software upgrade is rapid. On April 15, the equipment center also issued an OTA upgrade filing notice, requiring that every upgrade of car companies must be filed in advance, which standardizes the OTA upgrade process and avoids risks and put forward higher requirements. Enterprises need to follow up the progress of domestic and foreign standards and regulations, establish OTA testing-related capabilities as soon as possible, and ensure that each upgrade is efficient and compliant.

References

[1] Maganioti, A.E., Chrissanthi, H.D., Charalabos, P.C., Andreas, R.D., George, P.N. and Christos, C.N. (2010) Cointegration of Event-Related Potential (ERP) Signals in Experiments with Different Electromagnetic Field (EMF) Conditions. Health, 2, 400-406.

[2] Li Baotian. The first ISO international standard in the field of automotive information security was officially released [J]. China automotive, 2021 (09): 2.

[3] Wang Zhao, Li Baotian, Sun hang. Build an information security standard guarantee system for intelligent networked vehicles [J]. China information security, 2021 (07): 45-48.