

ASSOCIATION STANDARD

T/CSAE 101-2018

**Intelligent and Connected Vehicles On-Board Terminal Cyber
Security Technical Requirements
(English Translation)**

Issued on: June 19, 2018

Implemented on: January 1, 1970

Issued by: China Society of Automotive Engineers

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms, definitions and abbreviations	
3.1 Terms and definitions	
3.2 Abbreviations	
4 Vehicle-side security architecture and goals	
4.1 Vehicle-side security architecture	
4.2 Overall safety objectives	
4.3 Hardware Security Objectives	
4.4 Operating System Security Objectives	
4.5 Application Security Objectives	
4.6 Intranet communication security objectives	
4.7 External communication security objectives	
4.8 User Data Security Objectives	
5 Vehicle-side safety technical requirements	
5.1 Overall security	
5.2 Hardware Security	
5.3 Operating System Security	
5.4 Application Software Security	

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

1 Scope

This standard stipulates the technical requirements for information security of intelligent networked vehicles. The overall information security technology of intelligent networked vehicles and vehicles it is not within the scope of this standard to obtain cloud-related information security technical requirements related to vehicle networking and information security technical requirements for communication protocols.

This standard is only applicable to the vehicle-mounted terminal with networking function. The networking category includes mobile internet, car network and in-vehicle network.

This standard applies but is not limited to vehicle T-BOX, in-vehicle infotainment system In-Vehicle Infotainment (IVI) and other vehicle end Information system.

2 Normative references

The provisions contained in the following standards constitute provisions of this standard by reference in the standard. At the time of publication of this standard, the versions shown are to be effective. All standards will be revised and parties using this standard should explore the possibility of using the latest version of the following standards.

GB/T 5271 data processing vocabulary GB 17859-1999 Computer Information System Security Protection Level Division Guidelines GB/T 19596-2017 electric vehicle terminology

3.3.1 Intelligent Network Connected Vehicles Intelligent and Connected Vehicles (ICV)

Intelligent networked vehicles are equipped with advanced in-vehicle sensors, controllers, actuators, etc., and incorporate modern communications and networks.

Technology, realize intelligent information exchange and sharing between vehicles and X (car, road, people, cloud, etc.), with complex environment awareness, intelligent decision-making, Collaborative control and other functions can achieve "safe, efficient, comfortable, energy-saving" driving, and finally can achieve a new one to replace people to operate Generation of cars.

3.3.2 Intelligent network car car terminal ICV On-Board Terminal

The intelligent networked car vehicle end is a subsystem of the intelligent networked car, with data input and output, calculation processing, storage, and communication.

Letter and other functions, can collect relevant ECU data in the car and send instructions to control the ECU, and can also integrate positioning, navigation, entertainment and other functions.

It is a functional unit for car networking, access to the mobile Internet and the inter-vehicle network.

3.3.3 User User

Use the body of the car-side resource.

2T/CSAE 101 -.2018

3.3.4 User Data User Data

Vehicle-side collection, processing, generation, and storage of user personal information and information about the user's use of the vehicle, including but not limited to vehicles Asset data (vehicle identification, etc.), user identification information, application data (locally generated data, externally after user permission) Enter data in the user data area, etc.).

3.3.5 Authorization Authorization

After the user identity is authenticated, the user is granted the corresponding permission according to the preset security policy.

3.3.6 Digital Signature Digital Signature

A numeric string appended to the data generated by the sender of the information or operated by a password conversion method. number the recipient of the data can verify the source and integrity of the data by verifying the digital signature, and the digital signature can also protect the data from tampering.

Forgery, to ensure the non-repudiation of data.

3.3.7 Code Signing Code Signature

A mechanism for signing all or part of a code by an entity with signature authority using a digital signature mechanism.

3.2 Abbreviations

ICV Intelligent and Connected Vehicle BGA Ball Grid Array Solder Ball Array Package LGA Land Grid Array Grid Array Package SPA Simple Power Analysis Simple Power Analysis DPA Differential Power Analysis Differential Power Analysis CPA Correlation Power Analysis related power analysis SE Secure Element security unit ECU Electronic Control Unit Electronic Control Unit CAN Controller Area Network TLS Transportation Layer Security Secure Transport Layer Protocol CD Compact Disc DVD Digital Video Disk Digital Video Disc SD Secure Digital Secure Digital USB Universal Serial Bus Universal Serial Bus

4.1 Vehicle-side security architecture

One of the new business requirements of intelligent networked vehicles is that the vehicle-mounted terminal with network connection function communicates externally through cellular network and short-distance communication.

Letters, as well as vehicle/vehicle communication, establish connections with the Internet and the inter-vehicle network for data exchange; internal and automotive bus and electronic

and electrical 3T/CSAE 101 -.2018 the system collects information and issues instructions. As an important node of the intelligent network connection inside and outside the vehicle, the vehicle end should adopt technical measures.

Prevent, detect and block security attacks implemented through multiple network interfaces, ensuring that important subsystems in the vehicle do not have network connectivity and increase security risks.

The intelligent network connection vehicle information security system and the vehicle-side security architecture are shown in Figure 1. The overall security system is secure by the cloud.

The letter security and vehicle safety are composed of multiple parts. The vehicle end is an important part of the intelligent networked car, and its information security architecture is the vehicle.

An important part of information security, covering the hardware level of the vehicle end itself, the operating system level, the application level security, Security of external and inbound communications, as well as data security.

4.2 Overall safety objectives

The overall safety goal of the vehicle-mounted terminal is to avoid the security problems caused by information security problems through various measures at all levels of the vehicle-mounted end.

Damage to drivers and traffic participants, and the resulting public safety issues; while preventing personal information from leaking and due to information Property damage caused by security incidents.

4.3 Hardware Security Objectives

The vehicle-side hardware security goal is to ensure that the circuits and chips used by the vehicle-side system implement data calculation and data storage functions.

Security, the ability to use hardware-related technologies to combat multiple attacks at the physical level for encryption and decryption operations, such as cryptanalysis attacks, Side channel attacks, fault injection attacks, etc.

4.4 Operating System Security Objectives

The operating system security goal is that the operating system is correct by the identity rights management and access control mechanism that conforms to the vehicle-side application scenario.

Respond to authorized operations and handle abnormal behavior against overflow attacks, brute force attacks, man-in-the-middle attacks, replays, Tampering, forgery and other