中汽中心 | 数据

中 汽 数 据 有 限 公 司

Development Status of China's Connected Vehicles Cybersecurity Industry

China Automotive Technology and Research Center (CATARC)

2021/01

Introduction of speaker

Ms. Yanan Zhang

- Company: CATARC - Automotive Data Center
- Department: Intelligent Connected Technology Research
- Position: Deputy Director
- Deputy leader of Cybersecurity Working Group of China Intelligent Connected Vehicle Innovation and Development Alliance
- Special review expert of the Cybersecurity Bureau of the Ministry of Industry and Information Technology (MIIT).
- Registered expert of ISO/SAE 21434 and ISO PAS 5112

目录

Contents

01 Background

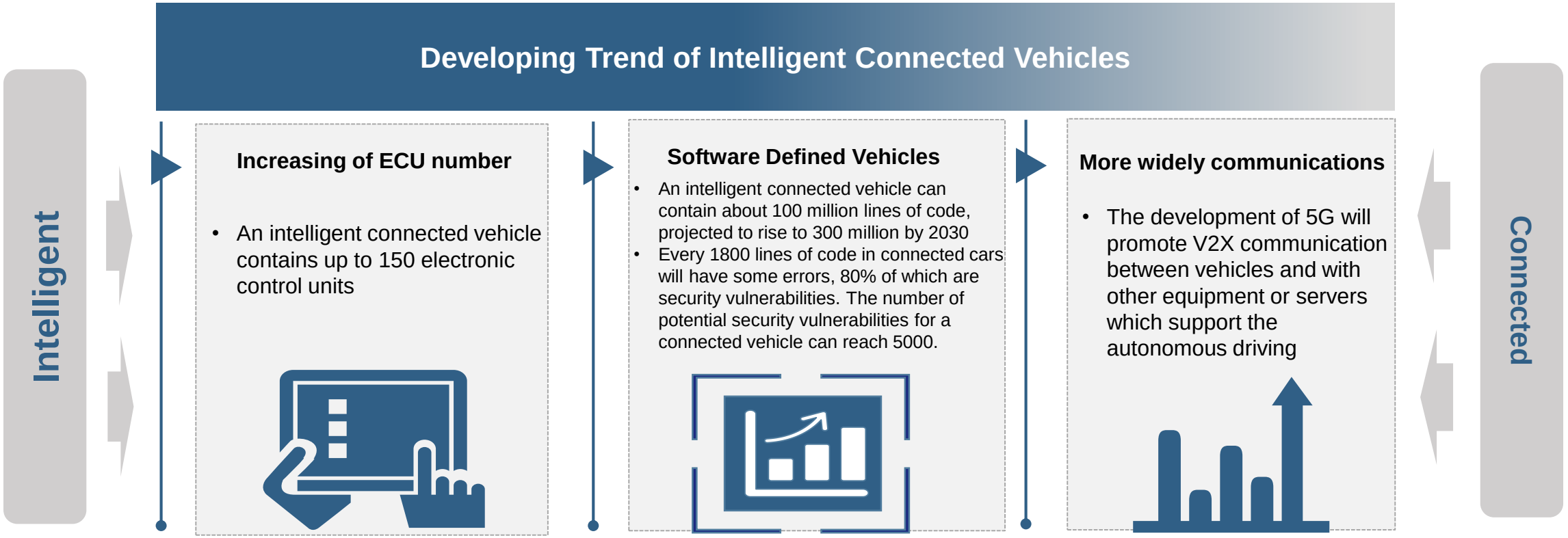
02 Applied Technologies

03 Standard and Regulations

04 Developing Trend

1 Background

- At present, the automotive industry is undergoing profound transition.
- Intelligent connected vehicles provide consumers with better driving feelings, but at the same time facing cybersecurity risks

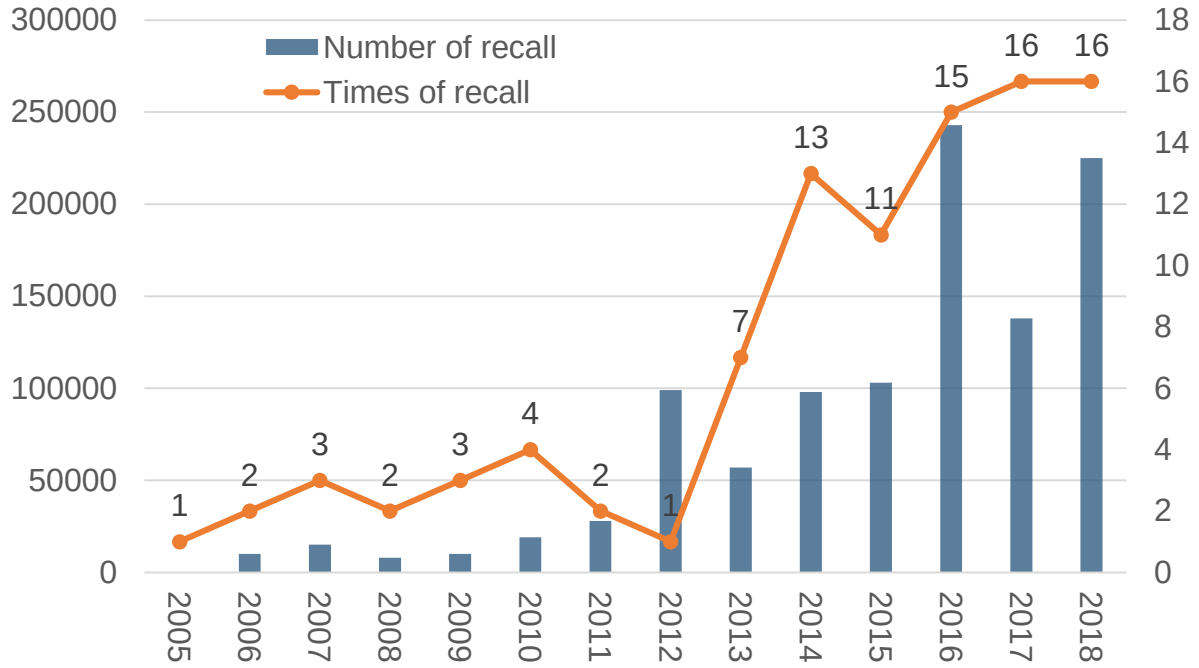


1 Background

- In recent years, cybersecurity incidents occurred frequently, OEMs began to realize the importance of cybersecurity.

- According to statistics from Upstream, the number of publicly reported cybersecurity attacks on connected vehicles increased from 80 in 2018 to 155 in 2019.
- In 2020, there are about 2.8 million malicious attacks on related companies and platforms

- 2019.3, the server of Toyota was hacked, resulting in leakage of the privacy of about 3.1 million individuals
- 2019.4, Car2Go of Daimler announced over 100 vehicles stolen due to the cracked mobile APP
- 2019.6, BMW suffered an APT attack. The attacker could penetrate into the company's network system, remotely monitor and control the computer, and remain active



Vehicle recall due to program or software

Importance of cybersecurity to automotive industry in China

- As the largest automotive market in the world, there are over 20 million vehicles produced and sold in China
- Due to the high population density in Chinese cities and the complicated road traffic conditions, Chinese government and enterprises along the automotive value chain are attaching great importance to automotive cybersecurity.

目录 Contents

01 Background

02 Applied Technologies

03 Standard and Regulations

04 Developing Trend

2.1 Vehicle cybersecurity protection technology

- By security analysis of key components and systems, formulating targeted security protection strategies and design developing design scheme

ECU

T-BOX | IVI | Gateway | ADAS | …

Threats of key ECUs

- Operation system
- Interface
- Communication
- Update
- Sensitive data
- 3rd party application
- External devices
- Authentication
- Key management

Protection Strategies


Key management

Coding protection


Authentication


Secure transmissio


Security storage


Access control

Security update


Security kernel


Firmware protection

In-Vehicle Network

Bus

Type
- CAN
- CANFD
- Ethernet

Strategies
- Encryption
- Message authentication
- OBD packet isolation
- Message monitoring
- Fresh Value Management

Diagnose

Assessment
- Policy security
- Key security
- Logical security

Strategies
- Service order restrictions
- Limitation of service order opening
- Key storage security

2.1 Vehicle cybersecurity protection technology

- By security analysis of key components and systems, formulating targeted security protection strategies and design developing design scheme

Cloud platform

Assessment

- Security Threats to Virtualized Environments
- Cloud platform data privacy
- Cloud platform system security
- Cloud platform network theft
- Attack the cloud platform itself
- Shared technology & shared risk

Strategies

- Security agreement between cloud and device
- Cloud host security protection platform
- Cloud Security Resource Pool
- Cloud security situational awareness platform
- Cloud Security Management Platform

APP

Assessment

- Communication security risks
- Data security risks
- Encryption algorithm risk
- Business security risks
- Code security risk
- Terminal Client risk

Strategies

- White box key
- Application reinforcement
- Safe operating environment
- Security Protocol
- Certificate validity
- Data encrypted transmission
- Data encryption storage
- Strong encryption algorithm
- Verification coding security
- Payment security

Radio

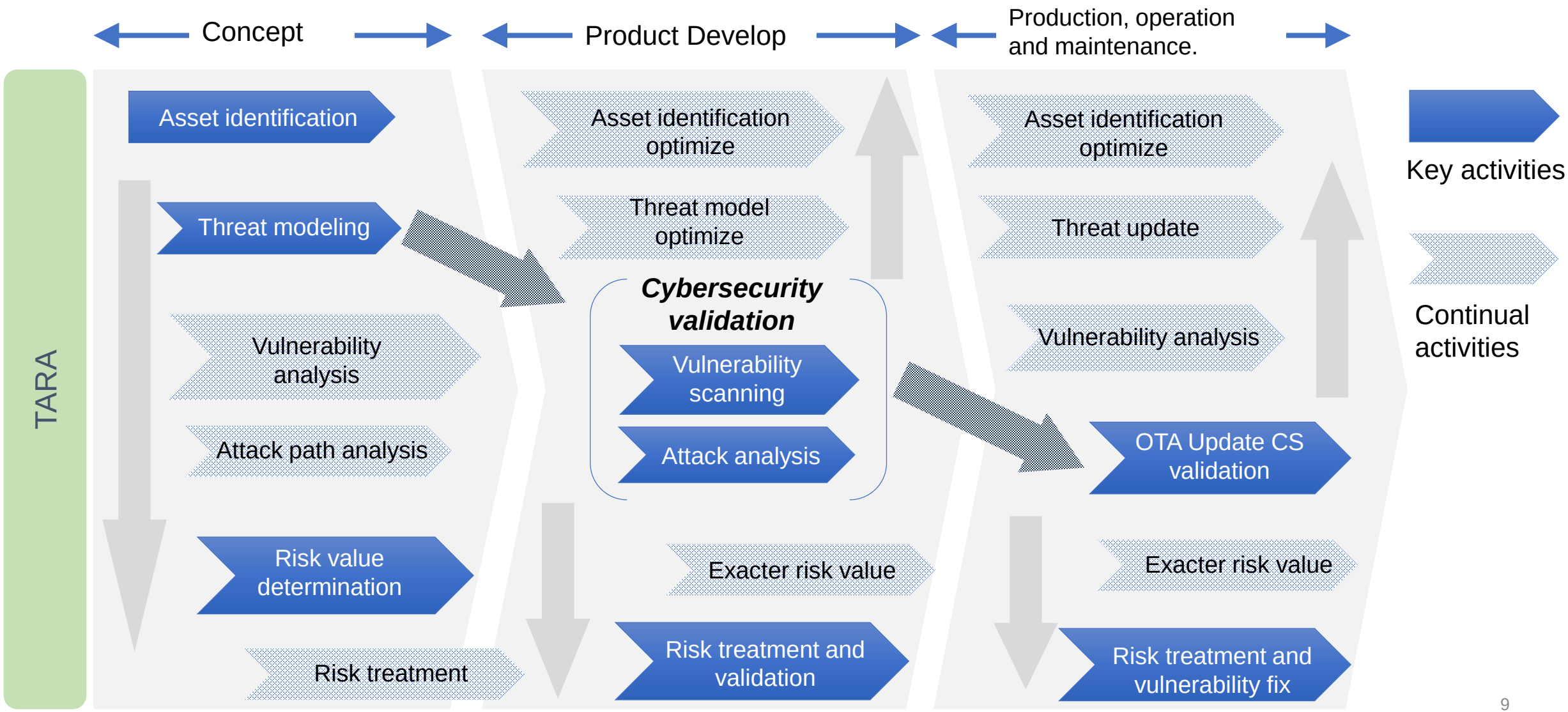
Type

- Bluetooth
- 2G/4G/5G
- GPS
- Smart key
- TPMS
- WIFI

Strategies

- Strong password detection
- Protocol information protection
- Communication data encryption
- Multiple location evaluation
- Pseudo AP recognition
- Data validation
- Condition recognition
- Two-way verification

2.2 Threat Analysis And Risk Assessment (TARA)



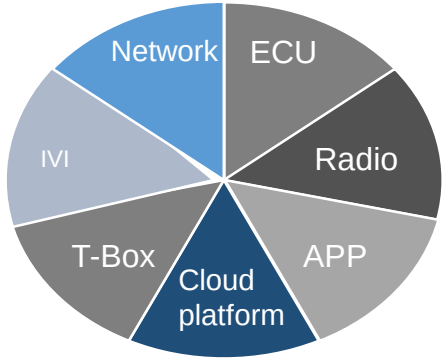
2.3 Vehicle Cyberecurity Testing

- Cybersecurity testing for vehicles in seven aspects: Network architecture, ECU, T-Box, IVI, cloud platform, APP and radio.

Test methods

Test tools

Test procedures



☑ Guidelines handbook for cybersecurity test on vehicle level

☑ Covering seven major vehicle cybersecurity attack path

☑ Complete tests on nearly 80 vehicle models

Accumulated results

Test case database

- Support automation testing of cybersecurity;
- Standardize the testing process;
- Conduct comprehensive cybersecurity testing of vehicles to prevent the test from falling;
- Integration common test cases used for the development of automated testing tools

Vulnerability database

- The vulnerability database is the vulnerability sharing platform for the automotive industry;
- Sharing automobile vulnerabilities, in order to save investment cost of OEMs and suppliers in cybersecurity vulnerability exploration;
- Applied for scientific classification and management of vulnerabilities in automotive industry;
- Automobile enterprises SRC data support;

Protection strategy database

Test process database

Test tool library
(including independent research and development tools)

2.4 CAVD and C-Auto-ISAC

CAVD

Platform name

- China Automobile Vulnerability Database (CAVD)
- Platform address: https://cavd.org.cn

Platform purpose

- Information exchange of automotive and internet industry, including terminal users, white hats and security organizations.
- Collecting and verifying vulnerabilities to construct emergent incident response center of automotive industry.
- Establish a systematic database by statistical analysis, big data and other technical means.

Based on CAVD, a new cybersecurity related information sharing mechanism and analysis center is established: C-Auto-ISAC

Data Share | **Compliance** | **Current Situation** | **Technology** | **Product** | **Ability**

Members

BAIC BJEV 北汽新能源 · 长城汽车 Greatwall · DFM 东风汽车 · 东风柳汽 · 北汽集团 BAIC Group · NISSAN 东风日产 · MITSUBISHI MOTORS 广汽三菱 · RENAULT NISSAN MITSUBISHI

LEAPMOTOR · HYUNDAI · 德赛西威 DESAY SV AUTOMOTIVE · JTEKT JTEKT CORPORATION · VOLVO · 华人运通 HUMAN HORIZONS

目录

Contents

01 Background

02 Applied Technologies

03 Standard and Regulations

04 Developing Trend

3.1 China’s contribution to cybersecurity related international regulations and standards

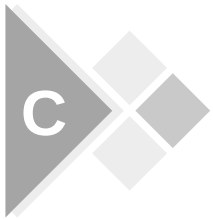
- Chinses experts have participated in drawing up cybersecurity international standards and regulations

ISO/SAE 21434: Road vehicles - Cybersecurity engineering

- Discussion in PG meetings
- Discussion in JWG meetings
- Comments to drafts

ISO PAS 5112: Road vehicles - Guidelines for auditing cybersecurity engineering

- Discussion in TG meetings
- Discussion in JWG meetings
- Compile content for sub-chapters
- Comments to drafts
- Co-leader of 2 TGs



ISO 24089: Road vehicles – Software Update Engineering

- Discussion in JWG meetings
- Comments to drafts
- Proposals to drafting

UN/WP29 regulation No.155

- Participate in regulation creation

3.2 Chinese local cybersecurity related standards

全国汽车标准化技术委员会
National Technical Committee of Auto Standardization

	Standard	Status
1	General technical requirements for vehicle cyber security	Approved
2	Technical requirements for cybersecurity of vehicle gateway	Approved
3	Technical Requirements for Cybersecurity of On-board Interactive System	Approved
4	Cybersecurity technical requirements for EV remote Service and Management system	Approved
5	Technical requirements for cybersecurity of EV charging system	Draft
6	Cybersecurity Risk Assessment Specification of vehicle	Project in discussion
7	Technical requirements for vehicle software update	Project in discussion
8	OBD interface cybersecurity technical requirements	Project in discussion
9	Cybersecurity emergency response management guide of vehicle	Project in discussion
10	Vehicle cybersecurity test method	Project in discussion
11	Road vehicles -Cybersecurity engineering (ISO/SAE21434 transform)	Project in discussion

- Recommended national standards
- Assist companies to produce cybersecurity ensured products
- References of mandatory type approval in the future
- Drafts of standard 1-5 are open on the Internet (Chinese version only)
- The approved standards will be released in 2nd quarter of 2021

目录

Contents

01 Background

02 Applied Technologies

03 Standard and Regulations

04 Developing Trend

4 Developing trend of China's automotive cybersecurity industry

01

Accelerate the establishment and implementation of cybersecurity related standards

02

Improve the approval management of cybersecurity related products, including vehicles and components

03

Improve the testing system and risk assessment system for intelligent connected vehicles

04

Establish national pilot areas for intelligent connected vehicles and smart traffic system

05

Improve the information sharing mechanism for the automotive industry

06

Accelerate the construction of testing and certification system for intelligent and connected vehicles

Thank you for your attention!