Introduction of IOV Security

Huirong Tian

Security Research Institute,CAICT

2017-11-02

Content:

I. Introduction of IOV

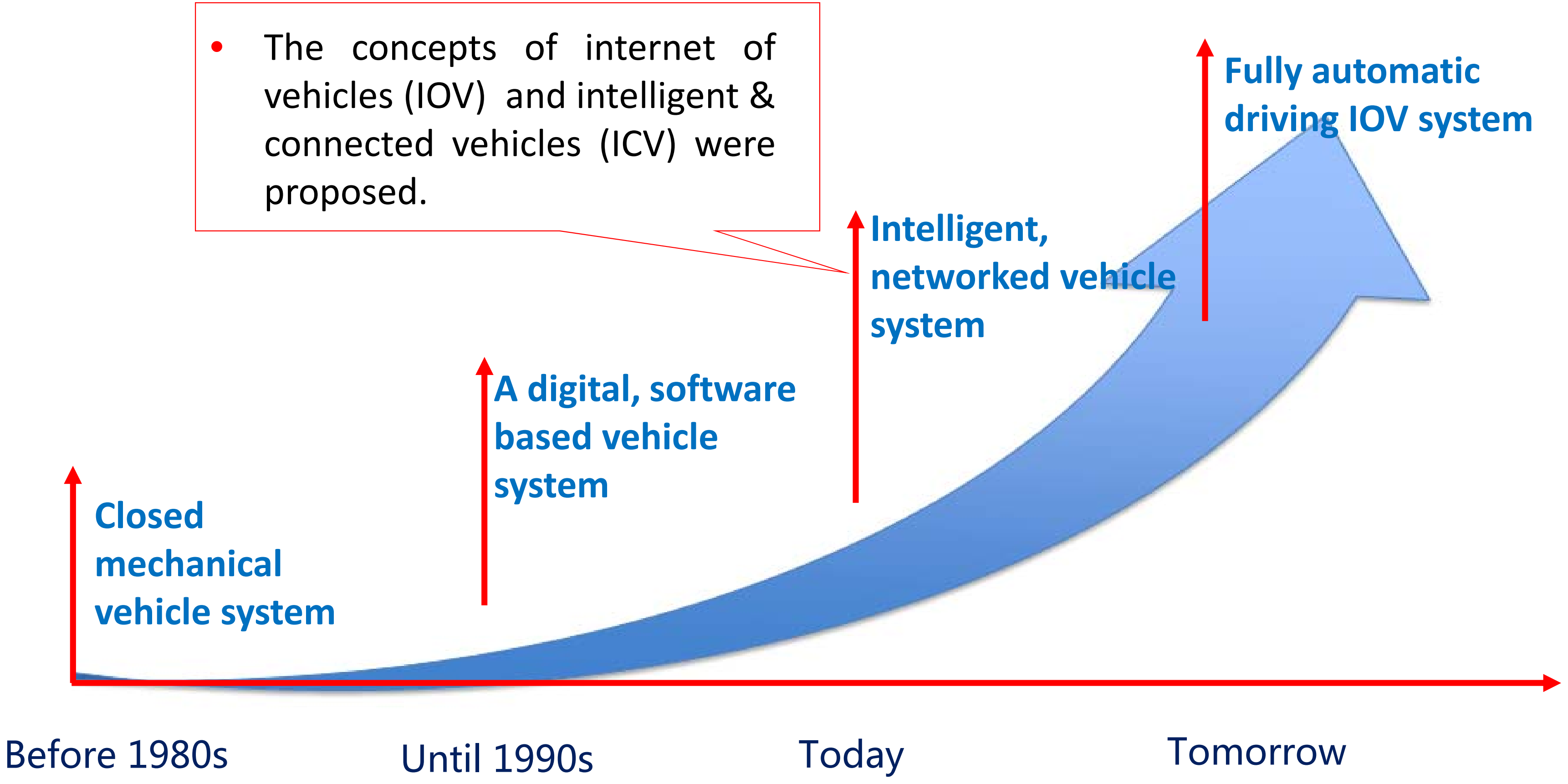
- Definitions of IOV and ICV
- Typical applications of IOV
- Actions and strategies for IOV

II. Analysis of IOV security

III. International trends of IOV security

IV. Suggestions for next step

Development process of vehicles



- The concepts of internet of vehicles (IOV) and intelligent & connected vehicles (ICV) were proposed.

Closed mechanical vehicle system

A digital, software based vehicle system

Intelligent, networked vehicle system

Fully automatic driving IOV system

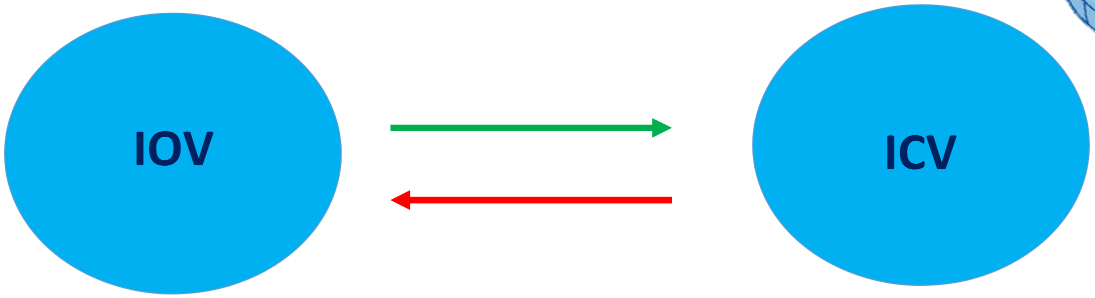
Before 1980s

Until 1990s

Today

Tomorrow

Definitions of IOV and ICV



Internet of vehicles

- Not only **the information and communication networks of V2X**, **but also an integrated service system** to provide the applications for automatic driving, intelligent transport and information service
- A **highly integrated application** of the IOT and intelligent transportation

Intelligent & connected vehicles

- **A new type of vehicle**
- Combine modern information communication technologies
- The ultimate goal is to **achieve automatic driving**

The development of the ICV needs the strong support from IOV,
the applications of IOV become more and more rich with the development of ICV.

Content:

I. Introduction of IOV

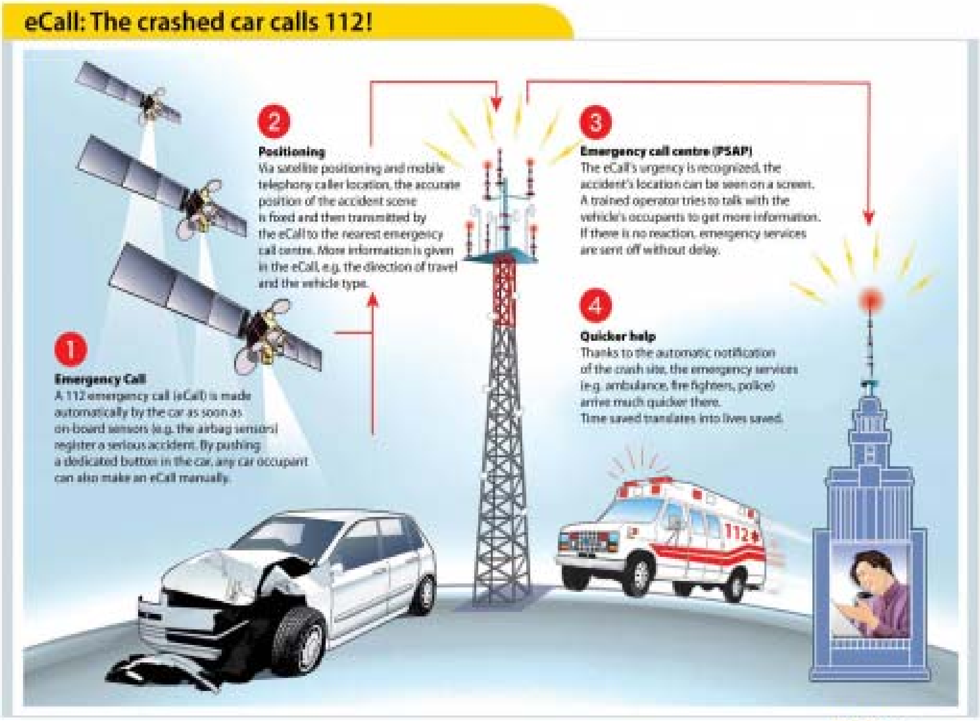
- Definitions of IOV and ICV
- Typical applications of IOV
- Actions and strategies for IOV

II. Analysis of IOV security

III. International trends of IOV security

IV. Suggestions for next step

Typical applications of IOV



eCall: The crashed car calls 112!

1 **Emergency Call**
A 112 emergency call (eCall) is made automatically by the car as soon as on-board sensors (e.g. the airbag sensors) register a serious accident. By pushing a dedicated button in the car, any car occupant can also make an eCall manually.

2 **Positioning**
Via satellite positioning and mobile telephony caller location, the accurate position of the accident scene is fixed and then transmitted by the eCall to the nearest emergency call centre. More information is given in the eCall, e.g. the direction of travel and the vehicle type.

3 **Emergency call centre (PSAP)**
The eCall's urgency is recognized, the accident's location can be seen on a screen. A trained operator tries to talk with the vehicle's occupants to get more information. If there is no reaction, emergency services are sent off without delay.

4 **Quicker help**
Thanks to the automatic notification of the crash site, the emergency services (e.g. ambulance, fire fighters, police) arrive much quicker there. Time saved translates into lives saved.

ADAC Infogramm

Automobile emergency succor

- European union countries are deploying E-call system
- Russia is developing a similar emergency call system according to the E-Call standards, which is called **ERA GLONASS**
- At present, EU and Russia are working together to ensure E-Call and ERA GLONASS be **interoperable**

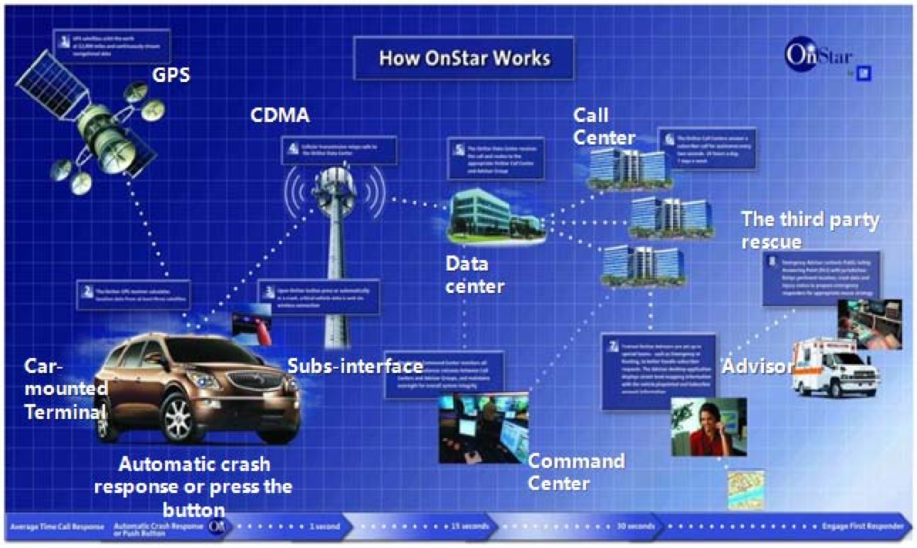
Typical applications of IOV

Security early warning based on 5G and V2X

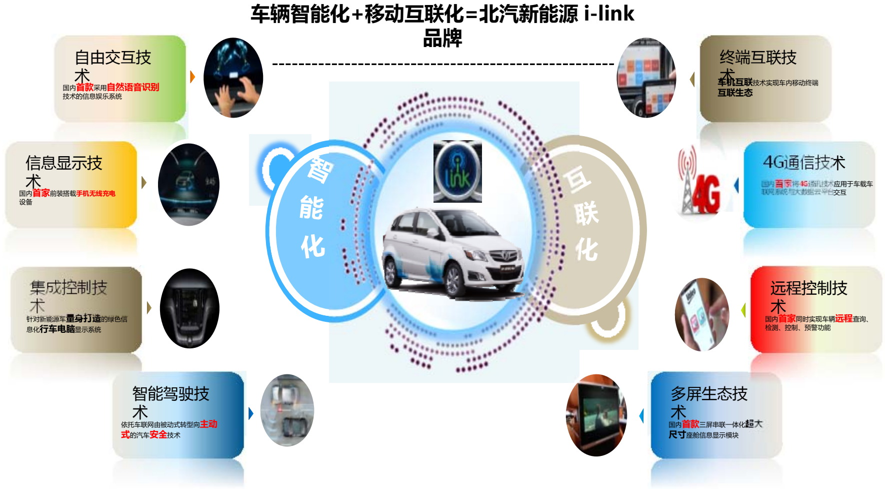
- **To remind drivers in the event of dangerous situations**, for example lane departure, emergency braking of vehicles ahead
- It is **an effective complement** to the vehicle collision warning system and other existing safety devices
- **Based on the real-time sharing information between vehicles**, **the system can respond promptly to reduce the risk of accidents as much as possible.** For example, when the moving forward vehicle has a sudden emergency brake, it will send corresponding signals to inform the surrounding vehicles.
- **Europe and the United States have developed relevant communication standards on security early warning**

Typical applications of IOV

In addition to the above applications, OEMs and service providers also provide call centers, information entertainment and other information services.



- **ON-STAR**: emergency services, information entertainment, security protection, call centers and other services


车辆智能化+移动互联化=北汽新能源 i-link 品牌
自由交互技术
国内首款采用自然语音识别技术的信息娱乐系统
信息显示技术
国内首家前装搭载手机无线充电设备
集成控制技术
针对新能源车量身打造的绿色信息化行车电脑显示系统
智能驾驶技术
依托车联网由被动式转型向主动式的汽车安全技术
终端互联技术
车机互联技术实现车内移动终端互联生态
4G通信技术
国内首家将4G通讯技术应用于车载车联网系统与大数据云平台交互
远程控制技术
国内首家同时实现车辆远程查询、检测、控制、预警功能
多屏生态技术
国内首款三屏串联一体化超大尺寸座舱信息显示模块
智能化
互联化
i-link
4G

- **BAIC MOTOR i-link**： information interaction and display, integrated control, terminal interconnection, remote control and other interconnected functions

Content:

I. Introduction of IOV

- Definitions of IOV and ICV
- Typical applications of IOV
- Actions and strategies for IOV

II. Analysis of IOV security

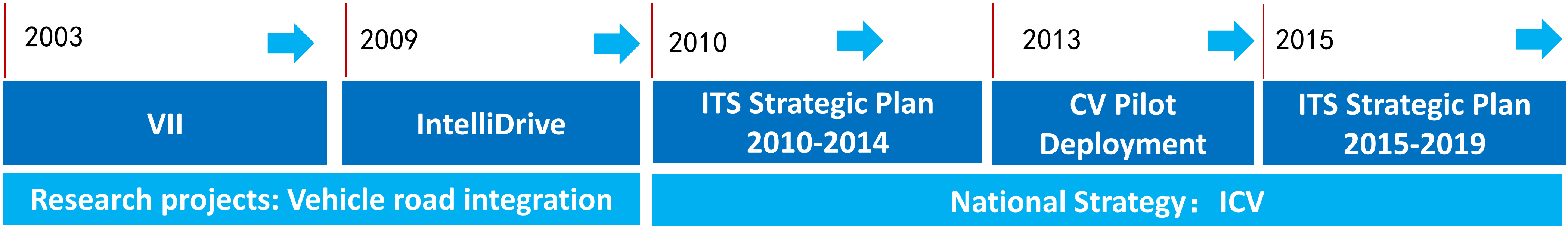
III. International trends of IOV security

IV. Suggestions for next step

Actions and strategies for IOV

2015: ITS Strategic Plan (2015-2019)

2016: Federal Automated Vehicles Policy



2003 VII

2009 IntelliDrive

2010 ITS Strategic Plan 2010-2014

2013 CV Pilot Deployment

2015 ITS Strategic Plan 2015-2019

Research projects: Vehicle road integration

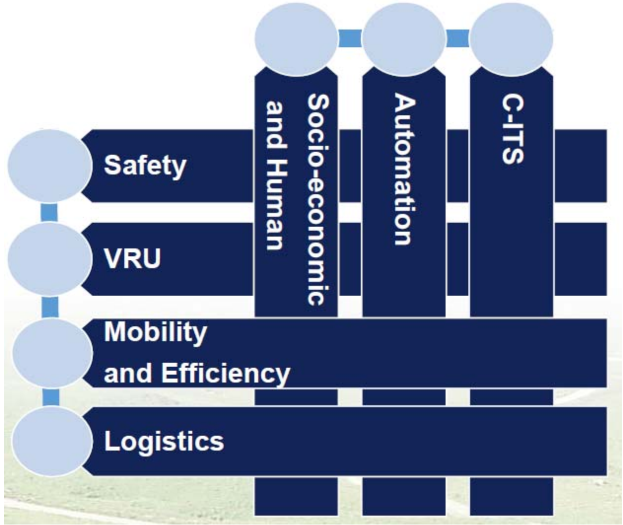
National Strategy： ICV

ITS Strategic Plan（2015-2019）

- **2 Points：** Connected Vehicle, vehicle automation
- **6 categories：** Connected Vehicles, Interoperability, Enterprise Data, Automation, Accelerating Development, Emerging Capabilities

Actions and strategies for IOV

- Focus on top-level design, technology research and development of vehicles
- Take the IOV as a key development area
- Promote IOV development through national projects



EU : conform to "Three Vertical & Four horizontal" strategy

Three vertical ： research contents and directions

Four horizontal ：problems need to be solved

- **2013： HORIZO N2020**
  Propose strategies for developing intelligent and green transportation system, to accelerate the development of connected vehicles
- **Formulate the plan for IOV to realize fully automatic driving in 2030**
- **Up to 2018, all new vehicles must install E-call system**

Actions and strategies for IOV

Construct the committee for IOV industrial development, which is led by MIIT, and jointed with other 20 ministries and departments, to solve major problems faced by the IOV development .

中华人民共和国中央人民政府
The Central People's Government of the People's Republic of China
www.GOV.cn
国务院关于积极推进"互联网+"行动的指导意见
国发〔2015〕40号

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

中华人民共和国中央人民政府
www.gov.cn

2015. 5 — 2015. 7 — 2017. 4 — 2017. 8

□ Made in China 2025

- ➢ Construct the innovation system and industry chain for ICV
- ➢ Construct intelligent transport system
- ➢ Promote the development and industrialization of intelligent transportation tools and products

□ "Internet Plus" action plan

- ➢ Actively promote the application of IOV
- ➢ Speed up the research, development and application of ADAS, and vehicle-intelligent terminals

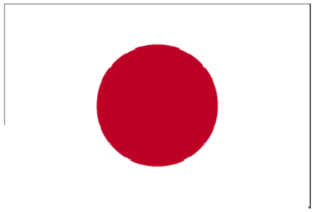
□ The automobile industry medium and long term development plan

- ➢ Take the chance of green-car and ICV development, guide industrial restructuring and upgrading
- ➢ Put forward the ICV promotion project, and define the development goals of each phase of DA, PA and CA

□ Guidance on further expanding and upgrading the potential of information consumption and ……

- ➢ construct the "5+2" demonstration area for ICV
- ➢ Develop ADAS and other equipment related to ICV

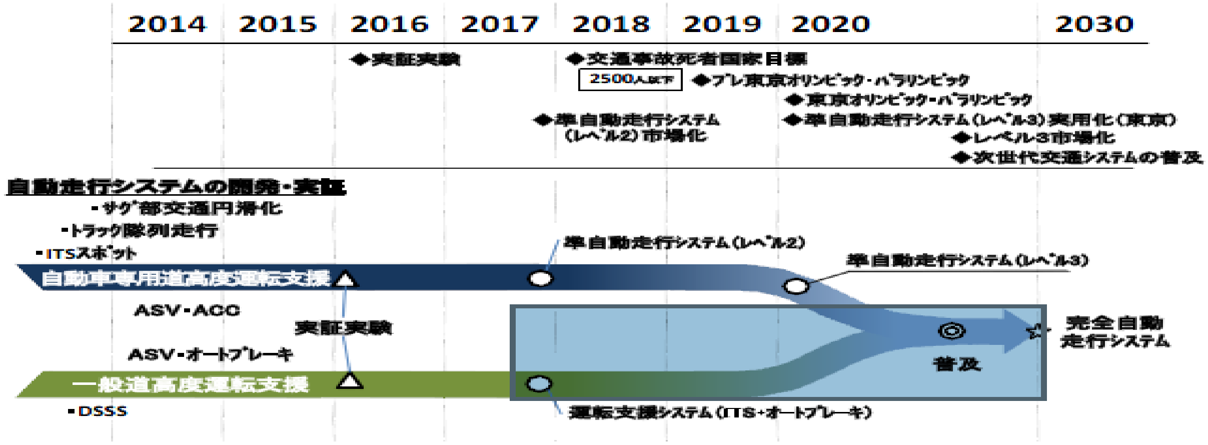
Actions and strategies for IOV



2014 Autonomous-drive plan:

- Includes short-term goal, medium-term goal and long-term goal
- short-term goal (2014-2016): complete the overall deployment
- medium-term goal (2017-2020): accelerate the development of automatic driving vehicles to put into use in 2020 Olympic Games
- long-term goal: up to 2030, fully automatic driving vehicle will be popularized

図表 4. 事故低減のための SIP 自動走行システム　ロードマップ


2014
2015
2016
2017
2018
2019
2020
2030
◆実証実験
◆交通事故死者国家目標
2500人以下
◆プレ東京オリンピック・パラリンピック
◆東京オリンピック・パラリンピック
◆準自動走行システム（レベル2）市場化
◆準自動走行システム（レベル3）実用化（東京）
◆レベル3市場化
◆次世代交通システムの普及
自動走行システムの開発・実証
・サグ部交通円滑化
・トラック隊列走行
・ITSスポット
準自動走行システム（レベル2）
準自動走行システム（レベル3）
自動車専用道高度運転支援
ASV・ACC
実証実験
ASV・オートブレーキ
完全自動走行システム
普及
一般道高度運転支援
・DSSS
運転支援システム（ITS+オートブレーキ）

Content:

I. Introduction of IOV

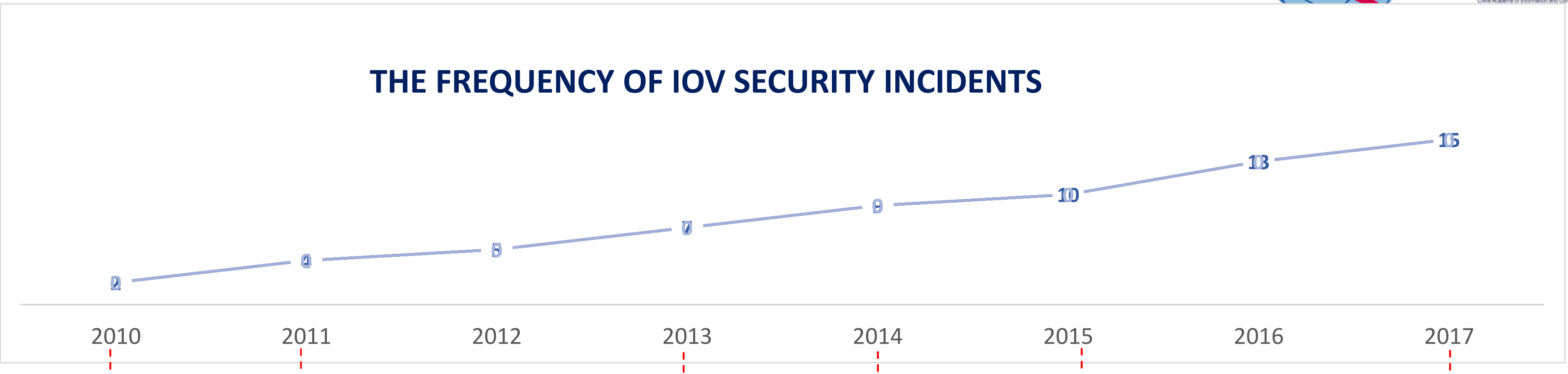
II. Analysis of IOV security

- Architecture of IOV
- Security risks of IOV
- Security solutions of IOV

III. International trends of IOV security

IV. Suggestions for next step

Security incidents



2010: In Texas, more than 100 cars were attacked

2011: Vehicle attack tests began to emerge

2013: In DefCon, vehicles of TOYOTA and Ford were cracked

2014: In GeekPwn, Tesla was invaded

2015: Security vulnerabilities of many major car brands were exposed

2017: American film <The Fate of the Furious>

The number of IOV security incidents has increased rapidly, and IOV security has attracted widespread attention.

Content:

I. Introduction of IOV

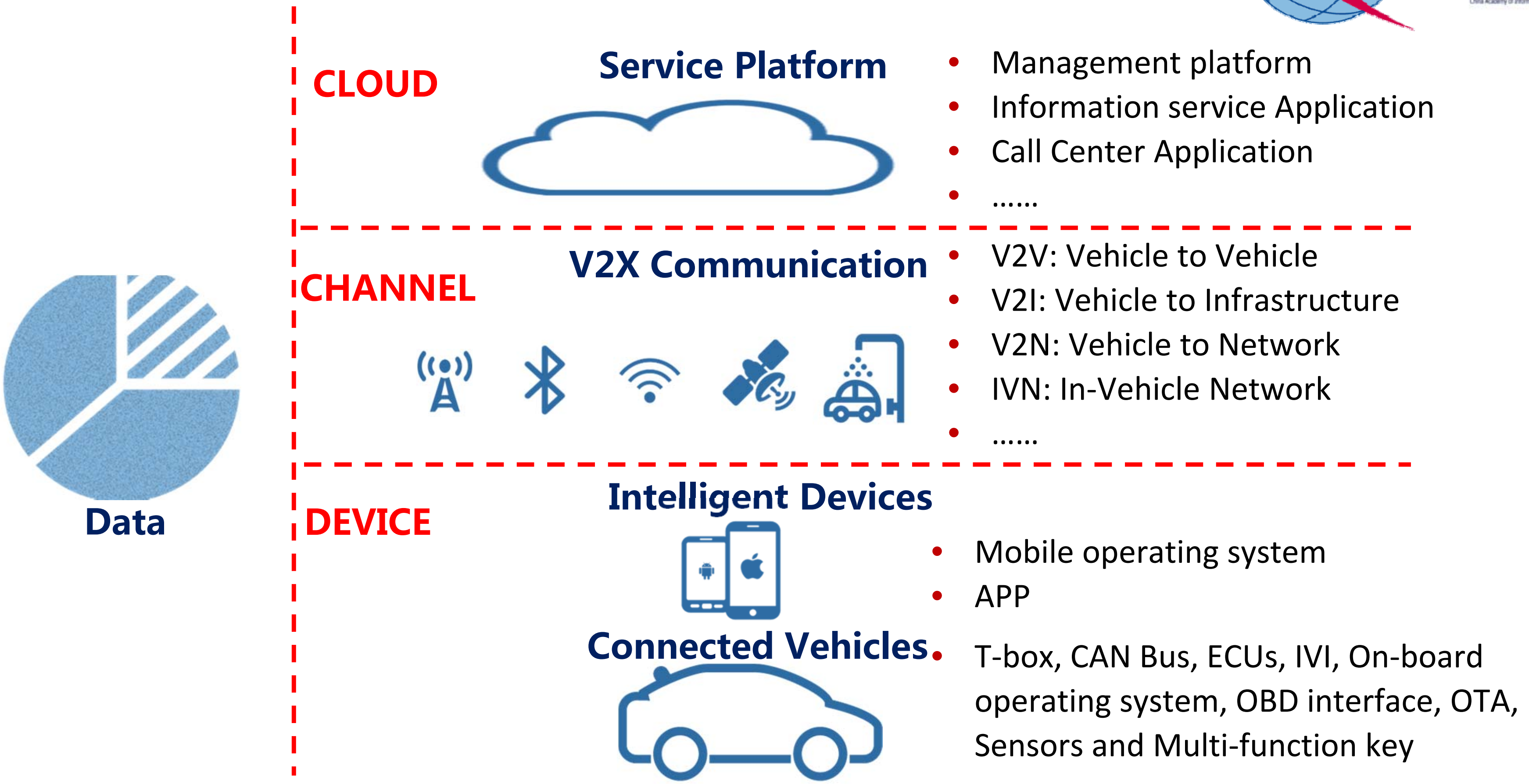
II. **Analysis of IOV security**

- **Architecture of IOV**
- Security risks of IOV
- Security solutions of IOV

III. International trends of IOV security

IV. Suggestions for next step

Architecture of IOV



Service Platform

- Management platform
- Information service Application
- Call Center Application
- ……

V2X Communication

- V2V: Vehicle to Vehicle
- V2I: Vehicle to Infrastructure
- V2N: Vehicle to Network
- IVN: In-Vehicle Network
- ……

Intelligent Devices

- Mobile operating system
- APP

Connected Vehicles

- T-box, CAN Bus, ECUs, IVI, On-board operating system, OBD interface, OTA, Sensors and Multi-function key

Content:

I. Introduction of IOV

II. Analysis of IOV security

- Architecture of IOV
- Security risks of IOV
- Security solutions of IOV

III. International trends of IOV security

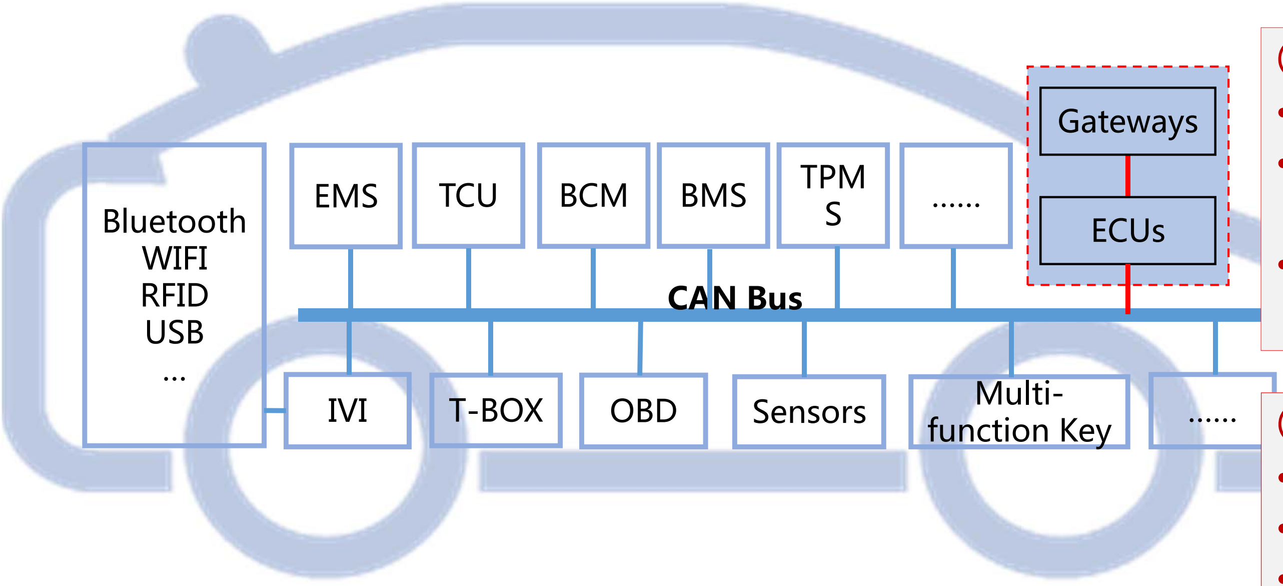
IV. Suggestions for next step

Security risks

The security risks of IOV are mainly on 5 aspects: **connected vehicles, intelligent devices, service platform, V2X communication and data.**

- **Connected vehicle security**
- **Intelligent device security**
- **Service platform security**
- **V2X Communication security**
- **Data security**

Security risks – connected vehicle



① T-BOX

- Firmware analysis (reverse analysis firmware)
- Internal information leakage

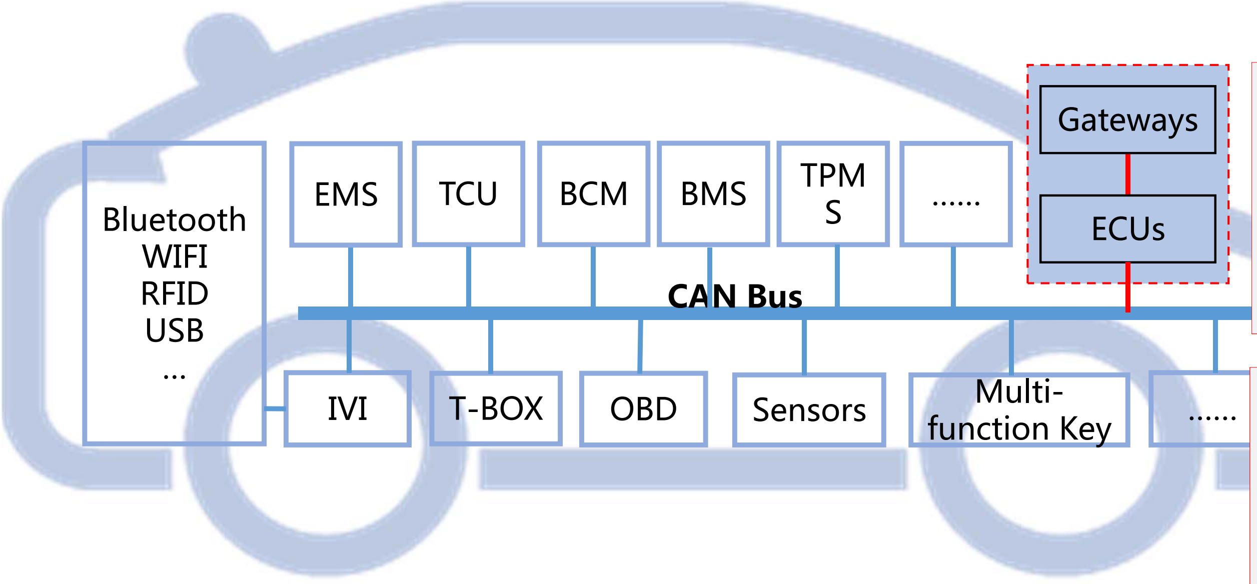
② CAN bus

- Lack of security isolation
- Lack of encryption and access control mechanisms
- Lack of authentication and message authentication mechanism

③ OBD Interface

- Break through the OBD bus protocol
- External devices bring attack codes
- Lack of authentication, unable to identify malicious code

Security risks – connected vehicle



④ ECU

- ECU chip security vulnerabilities
- ECU firmware security vulnerabilities
- The update program lacks signature verification

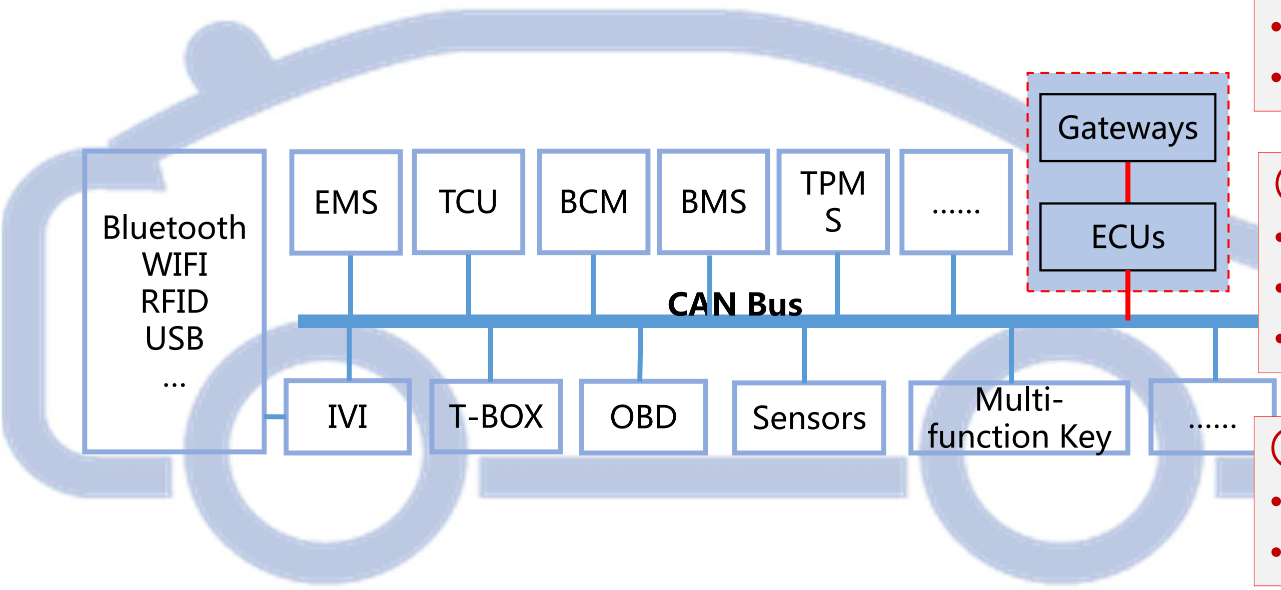
⑤ On-borad operating system

- Operating system vulnerabilities
- Malicious applications installed
- Security vulnerabilities of system components and third-party applications

⑥ IVI system

- Attackers can gain access to the target system during software upgrades
- Disassembling hardware for eavesdropping or reverse

Security risks – connected vehicle



⑦ OTA

- Upgrade lacks verification and signature
- Remote update is blocked

⑧ Sensor

- Ultrasonic radar: acoustic interference
- Millimeter wave radar: noise attack
- HD camera: blinding glare

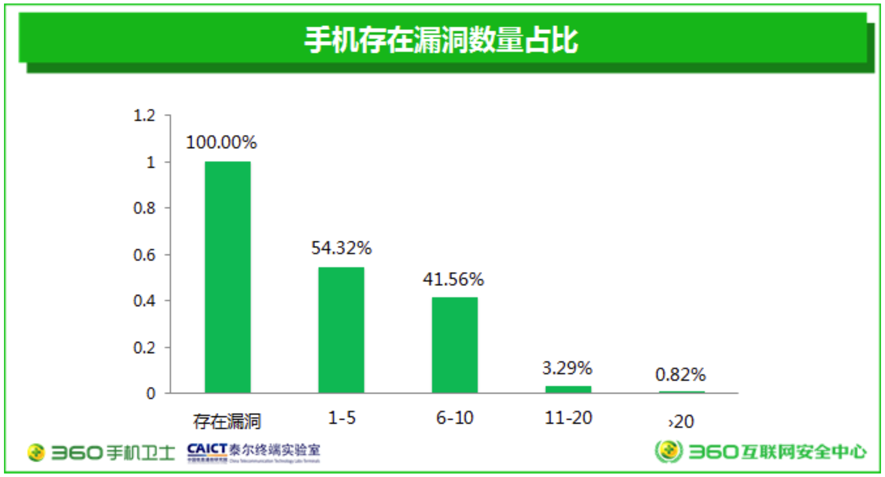
⑨ Multifunctional car key

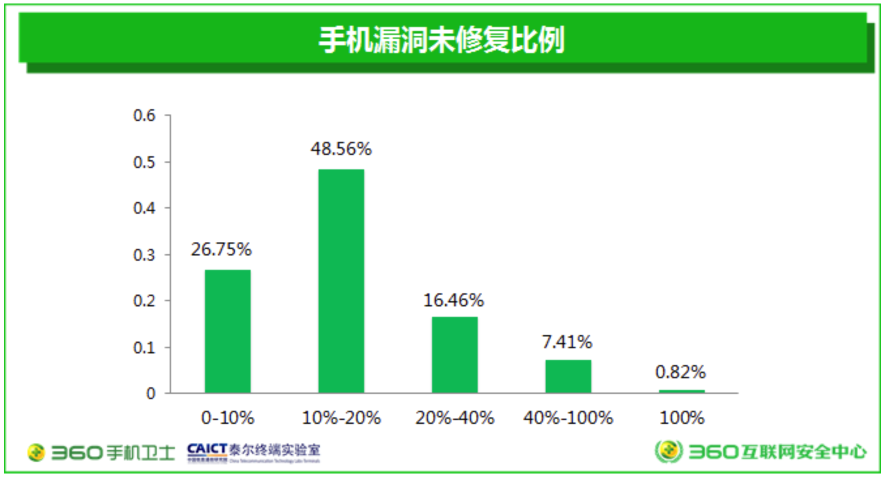
- Signal relay or signal replay
- Security vulnerabilities in chip solutions

Security risks – intelligent devices

◆ **Application crack has become a major threat**

- **Mobile APP is gradually becoming an essential part for IOV. For attackers, it is a hot spot of crack.**
- More and more attackers choose to debug or decompile applications to obtain communication keys and analyze communication protocols. And combined with the remote control function of connected vehicles, attackers can interfere with the state of vehicles, such as remote lock or open window and so on.





Security risks – intelligent devices

◆ **Operation system security of intelligent devices is an important factor**

- In the case of connecting with vehicles, the intelligent devices can be used as a springboard for further attacks on IVI or on-board operating system, to penetrate into the internal network of connected vehicle, and further threat the safety of vehicle
- If the accounts, passwords of cloud platform and other information existed in mobile App is accessed by attackers, the safety of vehicles will be threatened through remote control functions of service platforms

Security risks – service platform

The service platform faces the traditional cloud platform security problem

- **Platform layer:** there are problems of traditional operating system vulnerabilities and threats, and virtual resource scheduling
- **Application level:** service platform is also facing SQL injection and cross site scripting attacks
- **Access control**: faced with user authentication, password security and other issues
- **others**：denial of service attacks

The management platform of IOV is exposed to attackers and faces cyber attacks

- At present, the access control policies of management platforms are based on vehicle code or fixed certificate authentication, which are too weak to meet the strong access control requirements. Attackers can access the management platform by falsifying credentials to launch an attack.

Security risks - V2X communication

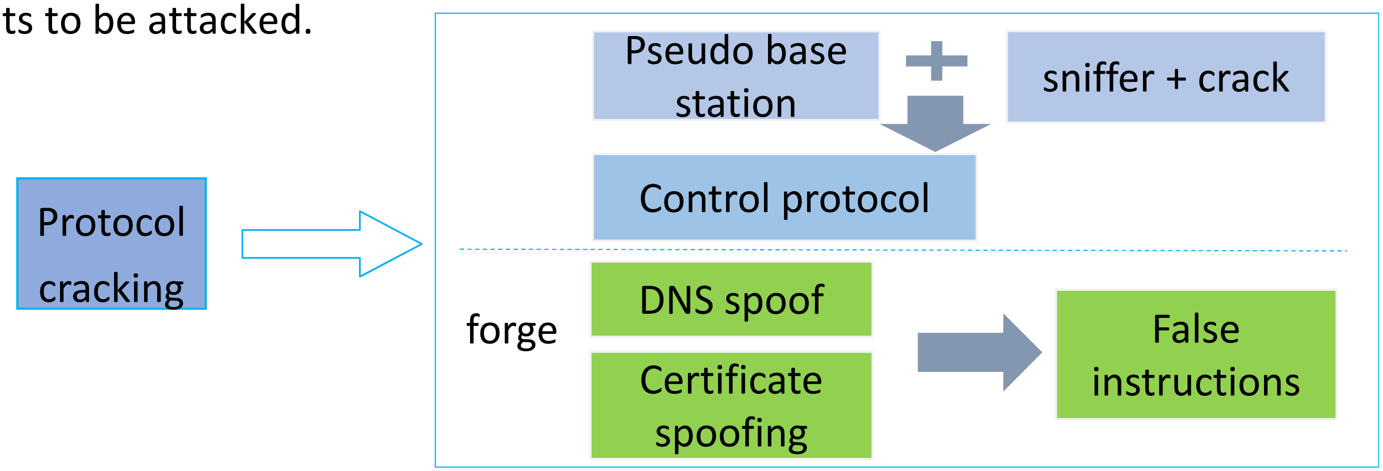
- **V2N communication is the main target of IOV attack**
  - Communication protocol cracking and man-in-the-middle attack are the two main threats of V2N Comm., such as **wireless communication hijacking** based on pseudo base station, **intermediate attack based on DNS spoofing** is the main attack mode of V2N communications

- **The malicious nodes is the main threat of V2V Comm.**
  - V2V trusted communication environment is the key for communication between vehicles.
  - As **lack of isolation and punishment mechanism** to the untrusted nodes, there could be many malicious nodes in V2V communications.
  - Once malicious nodes invade, the V2V communications will face **a variety of attacks**, such as eavesdropping, blocking, forging, tampering with communications, replay attacks and other communication attacks

Security risks - V2X communication

◆ **A variety of communication technologies and interfaces are the main risk resources for short distance communications**

- Protocol cracking and lack of authentication are the main threats
- For WIFI and Bluetooth communication, **the protocol key** is very vulnerable to be attacked, **and the passwords of WIFI hotspot authentication and PIN codes of Bluetooth** are the main targets to be attacked.



Security risks - data

Why is data security the major issue of IOV?

I. **The consequence of data security indecent is serious**

- **IOV involves a variety of data,** such as traffic management data, or data related to automobile operation, for example brake data, speed, tire pressure, fuel consumption, etc.. **If the data is falsified or tampered, it will threat the safety of vehicle or affect road management.**

II. **The risk of individual privacy exposure will become more and more serious**

- **An individual can be figured out based on** driver‘s license, vehicle identification number, the user’s trajectory, and other business application data. Once the data is disclosed, **individual privacy will be revealed almost without reservation.**

Security risks - data

Why is data security the major issue of IOV?

III. The impact of data security issues is gradually expanding to other areas

- Vehicle application data is being applied gradually in other industries, such as vehicle insurance and vehicle loan, and the impact of security issues is gradually expanding to other areas.

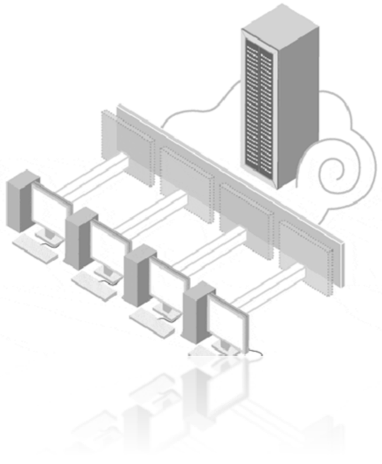
IV. Lack of mature and referenced standards and solutions on data security

- Compared with connected vehicles security and V2X communication security, there is lack of the referenced standards for IOV data security protection. And there is also no mature and referenced solution. **IOV data security protection is still in a gradually advancing stage.**

Security risks - data

Data security problems are mainly reflected in the following:

- Which types of data can be collected?
- How to ensure the security of data in transmission, access, sharing and other processes?
- What data is trustworthy in the data sharing?
- How to protect the privacy data in collection and sharing?
- How data be shared with third parties?
- ……



Content:

I. Introduction of IOV

II. Analysis of IOV security

- Architecture of IOV
- Security risks of IOV
- Security solutions of IOV

III. International trends of IOV security

IV. Suggestions for next step

Security solutions for IOV

Corresponding to the IOV security risks analysis, and the security solutions are also mainly on 5 aspects: **connected vehicles, intelligent devices, service platform, V2X communication and data.**

- **Connected vehicle security**
- **Intelligent device security**
- **Service platform security**
- **V2X Communication security**
- **Data security**

Security solutions – connected vehicles

① Use private solution and hidden technical details to increase the difficulty of attack

- Private solution
- Hide technical details without open to the outside
- Hide or close the debug interfaces, such as OBD/UDS interface

② Establish overall life-cycle security management system

- Based on standards: ISO 26262/SAE J3061
- Overall life-cycle management: includes the stages of planning, design, research, development, testing, release

Security solutions – connected vehicles

③ Hardware security protection is one of the important means

- Embed security functions into vehicle systems with hardware security module (HSM) to enhance the security of ECUs
- The security functions as follows: encryption algorithm, access control and integrity check, etc.

④ Take software security services as a supplement

- Build independent, mature OTA services
- Adopt software firewall and access control functions
- Application signature authentication for IVI system
- Encryption for firmware, data, and communications
- Adopt vehicle safety protection program
- Take sensor robustness algorithm

Security solutions – intelligent devices

Carry out overall life-cycle security protection

Mobile App: Overall life-cycle security protection

Protection measures

- **Design and development** → **Secure design and development**
- **Release** → **Security inspection and reinforcement**
- **Operation and maintenance** → **Security response**

Industrial protection status

At present, security enterprises begin to cooperate with OEMs, to provide security reinforcement, penetration testing and other security services, to improve mobile App security.

Security solutions – service platform

I. **Using mature cloud platform security technology**

- The existing network security technologies and products are used for security reinforcement, such as deploy network firewall, intrusion detection system, intrusion prevention system, web firewall and other security devices.

II. **Deploy centralized security capabilities base on cloud platform to strengthen the security of intelligent connected vehicles**

➢ Security capabilities are integrated into IOV service platform

- **Set up security detection service for connected vehicles**
- **Perfect remote OTA update function**
- **Establish the certificate management mechanism of IOV**
- **Share security information among OEMs, service providers and government agencies**

Security solutions – V2X communication

At present, the security protection for V2X communications is **mainly related to V2N and IVN scenarios**, and **authentication, access control and abnormal flow monitoring** are the mainly security technologies adopted.

1 Enhance access control and sub-domain management

- **Network isolation** between the control network and information entertainment network
- **System isolation** between vehicle systems
- **Separate data** between sub-domain systems

2 Protect V2N Comm. based on PKI and encryption

- Use the certificates based identity authentication
- Transmission encryption with certificate , and use negotiation key
- **Application layer encryption** with HTTPS encryption, or **transport layer encryption** with SSL and TLS
- **Private communication encryption**, such as VPN

3 Monitor abnormal flow

- **Monitoring and warning**
- **Network control**: define the protected IP address / range, block abnormal IP communication with firewall and intrusion detection system

Security solutions – data protection

◆ Formulate data classification standards

✓ Data classified protection

- Define different security mechanisms based on data types
- Take a higher level of management requirements for the privacy data, such as driver information, driving habits, vehicle information, location information and other privacy data, and only the applications approved by OEMs can read the relevant sensitive data
- The applications without signature authentication, only can read the non-sensitive data

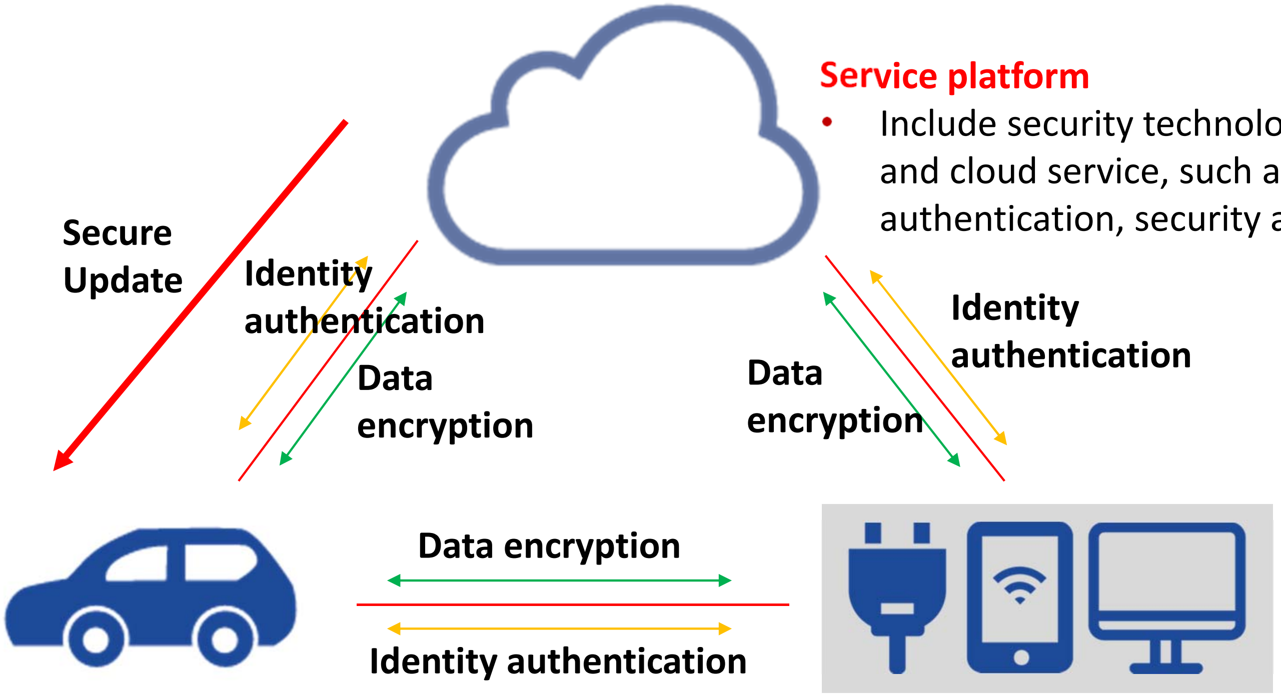
Security solutions – data protection

◆ **Strengthen the data security management to avoid data leakage**

✓ **Ensure the security of data**

- Transmit sensitive data in APN1
- Encrypt the sensitive transmission data with VPN, TLS/SSL, etc.
- Restrict the open and sharing of sensitive data

Security solutions for IOV



Service platform

- Include security technologies of platform and cloud service, such as access control, authentication, security audit, etc.

Connected vehicles

- Lightweight firewall
- Hardware encryption
- Trusted execution environment

Intelligent devices

- Secure application reinforcement
- Secure code check
- Secure application signature

Content:

I. Introduction of IOV

II. Analysis of IOV security

III. International trends of IOV security

- Government activities
- Standard
- Industry

IV. Suggestions for next step

International trends of IOV security - government activities

◆ **Automotive security research and regulatory agencies are actively developing IOV security guidelines and corresponding policies.**

UN/WP29

- To formulate the international regulations and standards
- ToR: network security, data protection and OTA security
- Plan to issue UN auto cybersecurity regulations or guidelines (2018)

- Focus on rules and guidelines
- Issued Cybersecurity Best Practices for Modern Vehicles (2016), mainly focus on personal information protection, life cycle security management, etc.

- Pay attention to the implementation of security technologies, driven by government project plans, such as PRESERVE, EVITA, SeVeCom, PRECIOSA

International trends of IOV security - government activities

◆ **Automotive security research and regulatory agencies are actively developing IOV security guidelines and corresponding policies.**

- Issued the Key Principles of Cyber Security for Connected and Automated Vehicles(2017)

- launched ITS-Safety Project to implement collaborative driving safety support systems based on V2I and V2V (2014)

- Build a large-scale test space for the development and safety of autopilot vehicles (2016)

International trends of IOV security
- government activities

- Pay attention to the **high level design and the overall plan for IOV security**
- The IOV security supervision is **in charge of** MIIT (Ministry of Industry and Information Technology), Ministry of Public Security, Ministry of Transport, and other ministries
- **A coordination mechanism between ministries is being established**
- **Formulate national standard structure for IOV security**, involving information and communication security , intelligent vehicles security and transport security, etc.
- **To promote the development of protection techniques for IOV** from developing key security technologies and products, training of security technicians, and increasing security investment

International trends of IOV security - government activities

◆ Cooperation between governments and enterprises

- **A security agreement has been reached between the department of transportation of United States, and 18 global car manufacturers**, such as GM, Ford
- The agreement is to **strengthen the cooperation** on the analysis of the information from early warring report, on the data sharing and solving the security issues.

- **EU ENISA set up the automotive and road safety working group**
- The group includes the expects in many fields, in order to discuss the solution of vehicle and road security protection, and strengthen communication and put forward relevant regulatory proposals

Content:

I. Introduction of IOV

II. Analysis of IOV security

III. International trends of IOV security

- Government activities
- Standard
- Industry

IV. Suggestions for next step

International trends of IOV security - standard

◆ **International standards organizations are actively promoting the vehicle network security standards research and development work.**

- **SAE J3061**: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)
- Mainly pay attention to the cyber security in all life cycle of vehicles

ISO/TC22

- Released security architecture of ITS system, privacy protection, legal monitoring and other security-related research reports
- Plan to issue international auto cybersecurity standard (2019)

- Issued the standard of DSRC (Special Short Range Communication Technology) vehicle communication security (1609.2-2013)
- Focus on communications security and privacy protection

International trends of IOV security - standard

◆ **International standards organizations are actively promoting the vehicle network security standards research and development work.**

- Established FG CarCOM (Focus Group on Car Communication) (2009)
- Established the ITS security question
- Mainly work on the communication security outside the vehicles

- ITS WG5 Security Working Group issued ITS Communications Security (TS 102 940 V1.2.1)
- Other related standards: Privacy and Trust Management (TS 102 941 V2.1.1), Security Threat Assessment Criteria (TR 102 893 V1.2.1)

International trends of IOV security - standard

➢ **Chinese relevant institutions are developing the IOV security standards**

- Chinese relevant standard organizations are developing the security standards based on national IOV standard structure, such as data protection
- Up to now, NTCAS, CCSA, NIST and other organizations have made some progress

International trends of IOV security - standard

◆ **Active cooperation between the international standardization organizations**

ISO/TC22

- **ISO and SAE: set up a joint working group**, mainly work on the cybersecurity for vehicle systems, in order to formulate the international standards

- **ETSI, CEN and ISO**: **have cooperated the standards of EU ITS system (Version 2)**, which involves the ITS cybersecurity, such as security architecture, secure management, HSM, etc.

- ITU, ISO, ETSI, CCSA, SAE and other agencies are actively cooperating on the international standards of IOV security

Content:

I. Introduction of IOV

II. Analysis of IOV security

III. International trends of IOV security

- Government activities
- Standard
- Industry

IV. Suggestions for next step

International trends of IOV security
- industry

◆ **Major auto OEMs begin to pay attention to IOV security, and increase IOV security investment.**

BMW
mazda
GM
Ford
CHRYSLER

The above 7 enterprises issued joint statements:

- **Place the vehicle security in the first place**
- Carry out the security protection from **hardware configuration and software development control**
- Conduct **continuous security testi**ng

International trends of IOV security - industry

◆ **Active cooperation is being carried out for the major vehicle OEMs.**

16 major auto OEMS, represented by GM, NXP, have set up the Auto-ISAC.

Auto-ISAC (Information Sharing and Analysis Center)

- Designed to **build a security platform** to share, track and analyze the information of the security risks and security incidents, and other related vehicle information
- Auto-ISAC, Alliance of Automobile Manufacturers, and OICA (Organisation Internationale des Constructeurs d'Automobiles), have actively cooperated. They **have jointly issued the best practices in American Automotive Network security**
- In this best practices, there is a **guidance for the enterprise to improve the security capabilities** on secure management, risk management, detection, incident response, training, cooperation with the third parties, and other aspects

International trends of IOV security - industry

◆ Chinese relevant enterprises have made a certain progress on IOV security

CAICT

- Based on “Industrial Internet security technology test and evaluation laboratory of MIIT”, build IOV security testing environment
- Mainly focus on IOV security detection and evaluation
- issued ‘**IOV Cybersecurity white paper (2017)**’

Neusoft

- Neusoft has taken part in the development of international car networking security standards in UN/WP29
- Played an active role in the development of vehicle security

360 company

- 360 car network security center works on car life cycle security protection
- Mainly focus on researching and promoting the vehicle security technologies

Bang Bang Security Company

- Issued the '**Intelligent Network Automotive Information Security White Paper**' with China Society of Automotive Engineers and Beijing University of Aeronautics and Astronautics

International trends of IOV security - industry

◆ China Automobile industry

China automobile industry are strengthening cooperation between enterprises based on industry alliances, in order to jointly promote the IOV development and explore the IOV security problems.

In terms of IOV security, CAICV and TIAA have made some progress.

- **CAICV:** China industry innovation alliance for the intelligent and connected vehicles, sets up a information security working group, development vehicle related automotive information security requirements and test methods

- **TIAA:** telematics industry application alliance, sets up a information security working group, issued the guidelines for security protection of IOV

Content:

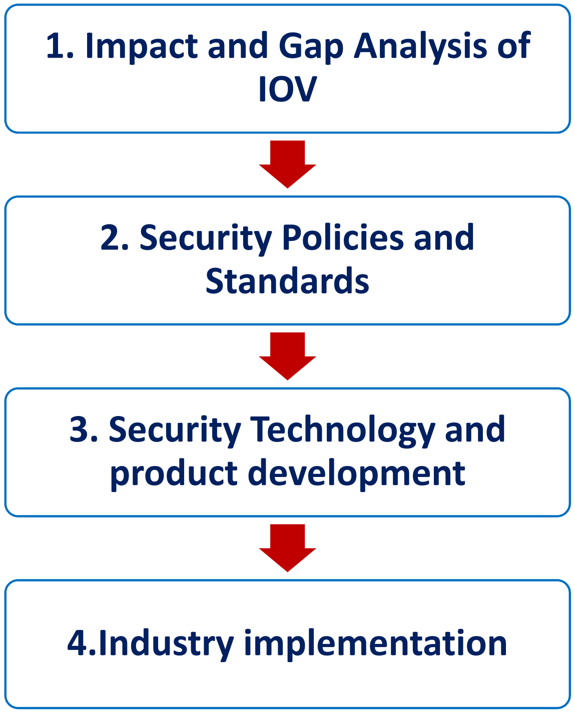
I. Introduction of IOV

II. Analysis of IOV security

III. International trends of IOV security

IV. Suggestions for next step

Suggestions for next step



1. Impact and Gap Analysis of IOV

2. Security Policies and Standards

3. Security Technology and product development

4.Industry implementation

- Launch overall impact and gap analysis of IOV, mainly on current regulations, standards, industry readiness, etc.
- Based on responsibilities, revise, complement or development security policies, mechanisms and standards, to adapt to the development of IOV
- Support security technologies research, security tests, security product development, and build IOV security verity and assessment environment to help reinforce the security abilities
- Strengthen industrial cooperation, move forward the implementation of IOV security solutions

Trainer: Huirong Tian

E-mail: tianhuirong@caict.ac.cn

Department: Institute of Security Research

Address: Building A, No.52 Huayuan Bei Road, Haidian District,
Beijing, China 100191

Photo：

Thanks!

China Academy of Information and Communication Technology

http://www.caict.ac.cn