CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

Security Technical Requirements of On-Board Intelligent Terminal

杨正军 Yang Zhengjun
Automotive Security of CTTL-Terminals

OUTLINE

✓ 1.Automotive Cyber threat landscape

2.Security Protection Framework

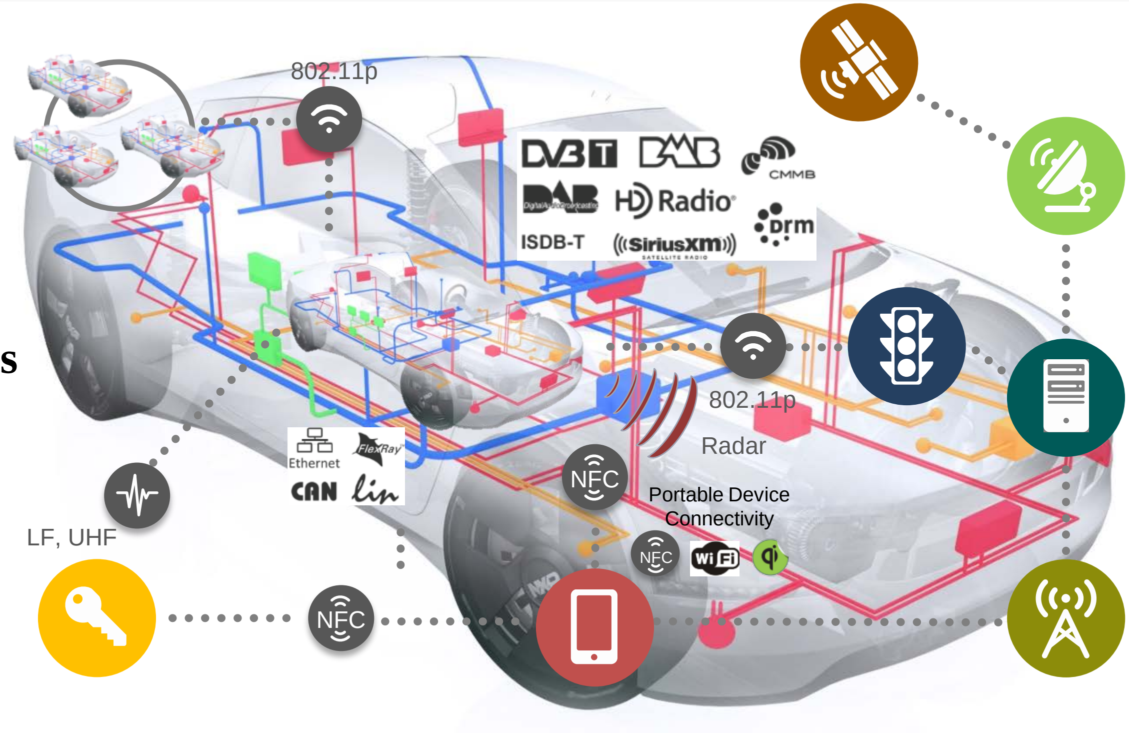
3. International Standardization

4.Security Technical Requirements

THE CONNECTED CAR …

- **A networked computer**
  - up to 100 ECUs per car
  - and many sensors
  - inter-connected by wires
  - more and more software

- **Increasingly connected to its environment**
  - to vehicles & infrastructure
  - to user devices
  - to cloud services

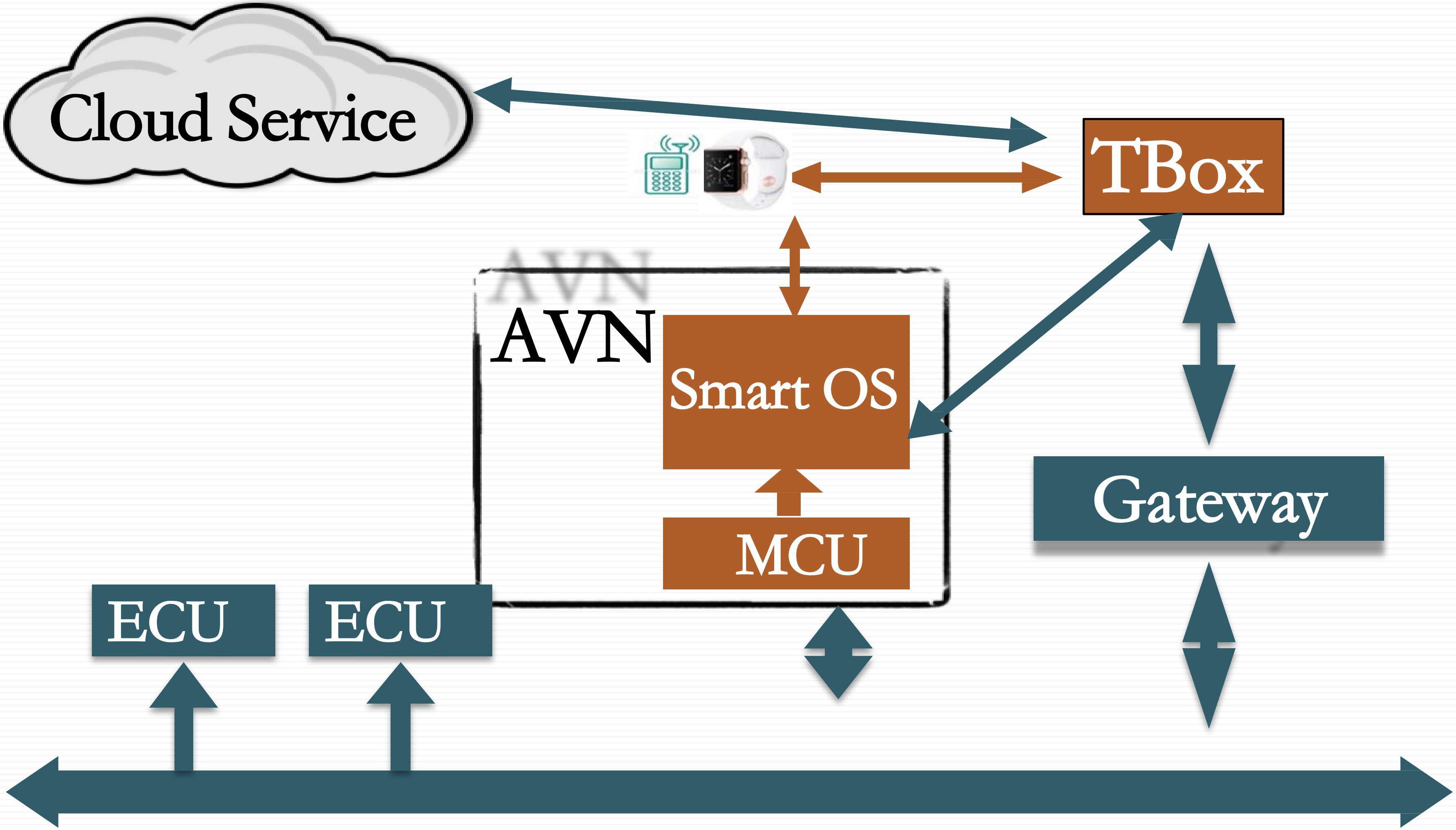


Connected Car = Mobile on the Wheels

1. 78 million new cars sold every year (LMC Automobile)
2. By 2017, 60% new cars will be connected
3. Huge security market for connected cars

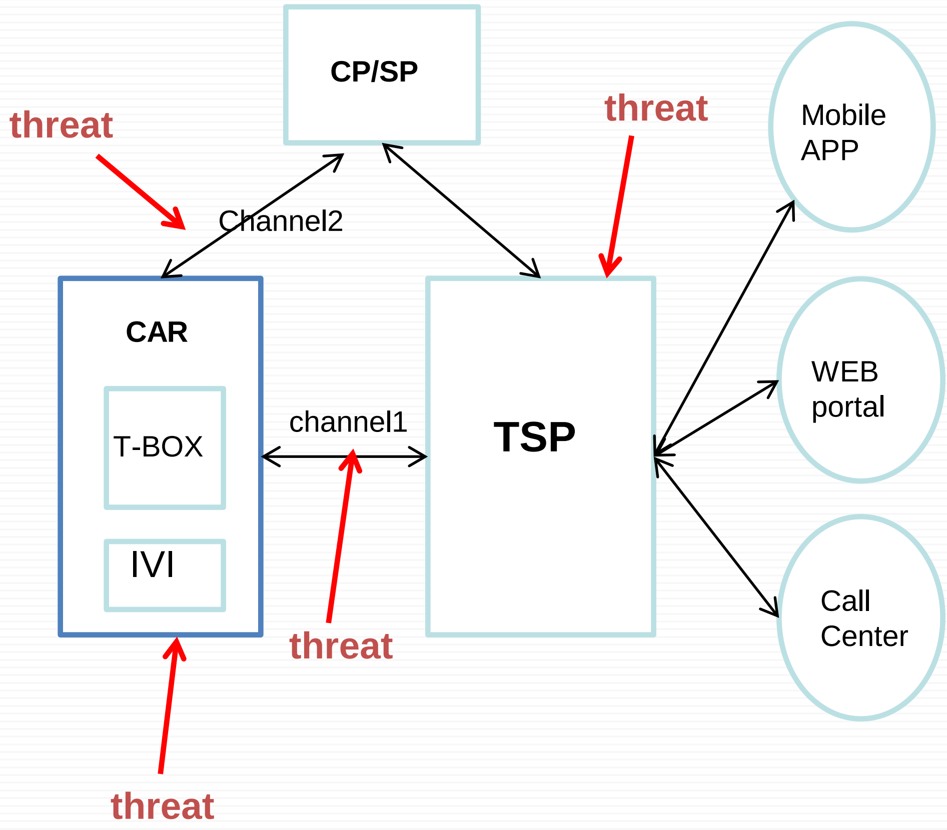
Mobile: 40+ various security vendors
Car: <span style="color:red">sparse</span>

Internet Vehicle Architecture



Automotive Cyber Threat Points

□ Architecture



□ Threats

- **CP/SP Connection threat**

Once CP/SP is hacked, the connection between CP/SP and car becomes dangerous.

- **TSP background connection threat**

No-authorized access expose risk to TSP.

- **Remote update（ firmware，application）threat**

Uncontrolled(unencrypted or no-authorized) update expose risk to T-BOX and IVI.

- Car data upload threat

Unknown layer（not only TLS）could upload sensitive data.

- **Remote Configuration/Control threat**

No check of connection request source.

OUTLINE

1.Automotive Cyber threat landscape

✓ 2.Security Protection Framework

3. International Standardization

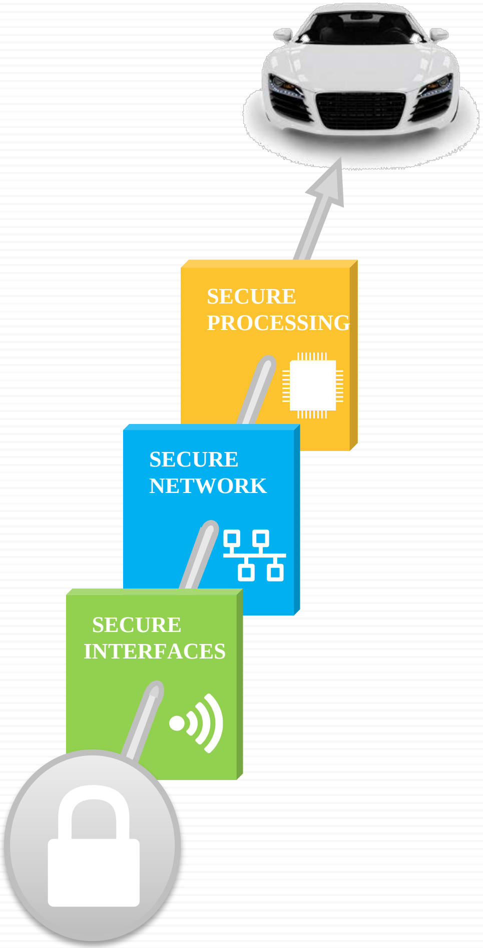
4.Security Technical Requirements

Security Protection Framework

- Multiple security techniques, at different levels in the architecture
- To mitigate the risk of one component of the defense being compromised or circumvented

■ Refer to NXP solution

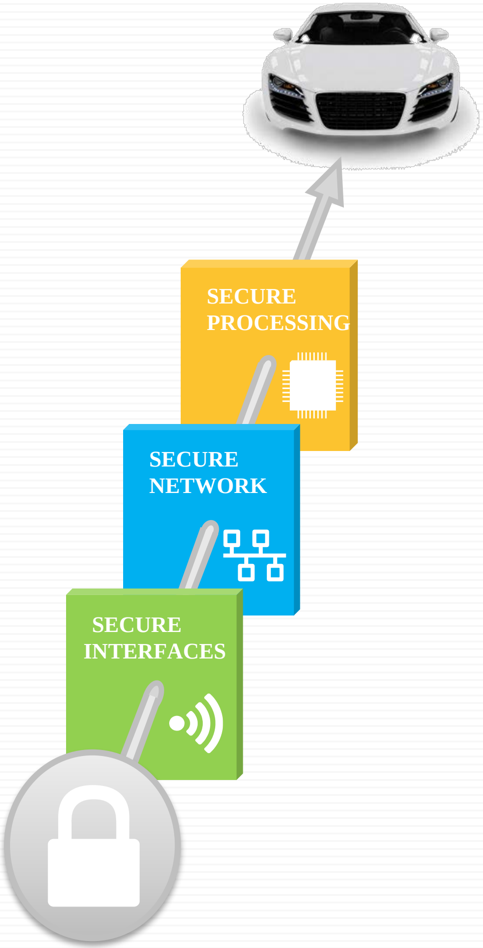
Prevent access	Detect attacks	Reduce impact	Fix vulnerabilities
Authenticate code (secure boot)	Run-Time Integrity Protection	Resource control (virtualization)	Secure OTA firmware updates
Firewalls (context-aware message filtering) Secure messaging	Intrusion detection systems (IDS)	Separate / isolated domains within network	Secure OTA policy updates (firewall, IDS)
M2M authentication Firewalls (isolate access points)			



Security Protection Framework

HARDWARE SECURITY

1. Crypto accelerators,
   to guarantee strict performance requirements
   - E.g. V2X message authentication, CAN authentication, secure boot, …
2. Hardware-enforced isolation,
   to protect against software attacks
   - E.g. system vs. user mode, TrustZone, SHE/HSM, …
3. Tamper-resistant hardware,
   to protect against advanced, physical attacks
   - E.g. Secure Elements



OUTLINE

1.Automotive Cyber threat landscape

2.Security Protection Framework

✓ 3. International Standardization

4.Security Technical Requirements

International Standards for Automotive Cyber Security

ISO

SC27 Security Techniques

- ISO/IEC 15408 ISO/IEC 15443 ISO/IEC218279 ISO/IEC 27000

IETF

- BTNS、DKIM、EMU、HONKEY、ISMS、 KEYPROV、KITTEN、KRB-WG、LTANS、MSEC、 NEA、OPENPGP、PKIX、SASL、SMIME、 SYSLOG、TLS ,and son ,17working groups, over 270 RFCs.

IEC

- JTC1 、 TC5 、TC74 、TC77 TC108…

IEEE

- WLAN Security、WiMAX Security 、 Institue of Electrical and Electronics Engineers…

ITU

SG17

- Q2：Security architecture and framework Q4：Cybersecurity Q7：Telecommunications information security management Q8：Telebiometrics

Other

- 3GPP TSG-S WG4
- ATIS IDSC
- OASIS E-commerce Security、Web Application Security

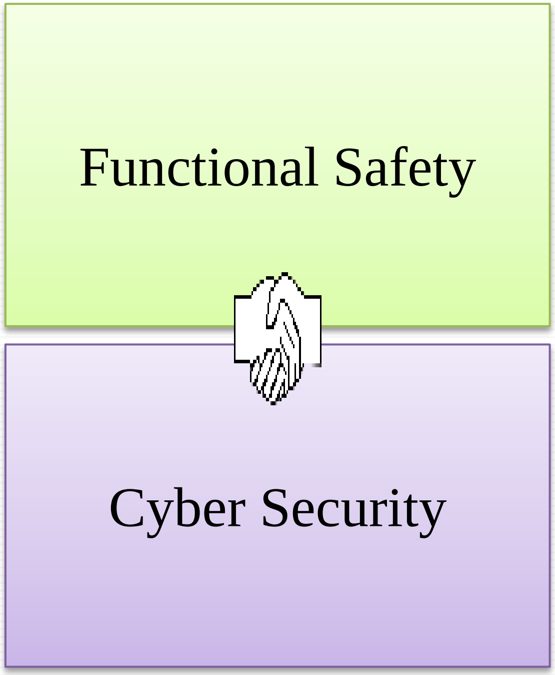
International Standards for Automotive Cyber Security

1. **Standards & Best Practice**

   - ISO 26262 “Road vehicles – Functional safety” is an international standard for functional safety of electronic systems in vehicles
   - General IT security standards ISO 15408, ISO 27001
   - SAE J3061 is under development Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

2. **Processes**

   - Aligned development processes for Functional Safety and Cyber Security including
     - Risk management and requirements management
     - System design based on defence-in-depth strategy
     - Comprehensive verification and validation



Functional Safety

Cyber Security

OUTLINE

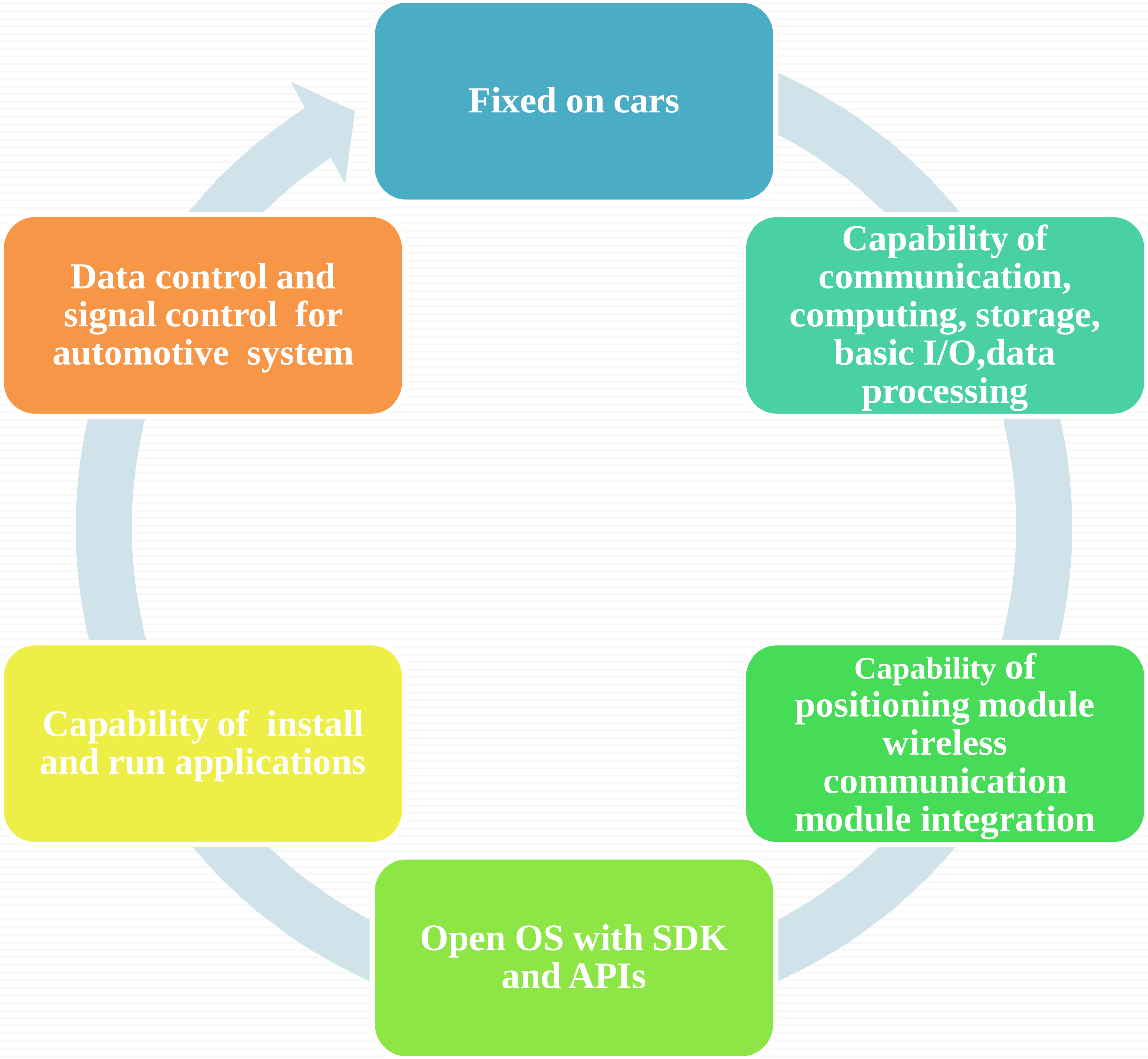
1.Automotive Cyber threat landscape

2.Security Protection Framework

3. International Standardization

✓ 4.Security Technical Requirements

On-board Intelligent Terminal



Fixed on cars

Capability of communication, computing, storage, basic I/O,data processing

Capability of positioning module wireless communication module integration

Open OS with SDK and APIs

Capability of install and run applications

Data control and signal control for automotive system

Research Report of On-Board Intelligent Terminal

Contents

- □ Developing status and trends
- □Threat status
- □Security Technical Requirements and security mechanism
- □Standardization system

Security Technical Requirements and Security Mechanism

Security Technical Requirements and security mechanism of Cloud-Side

- Identification and Authentication requirements
- Web page requirements
- Remote control requirements of devices
- resource control requirements
- Tolerant requirements of applications

Security Technical Requirements and security mechanism of external communication

- Communication network access authentication requirements
- Channel isolation requirements
- Certificate Authority requirements of key operations
- Service level differentiation requirements

Security Technical Requirements and security mechanism of Terminal-Side

- OS security requirements
- Secure Boot
- integrity check
- Mandatory Access Control
- App Sandbox
- data encryption
- Privacy Management
- Anti-reverse engineering
- Authentication and Authorization
- ……

Security Technical Requirements and security mechanism of internal communication

- Isolation requirements between terminal and ECU
- Isolation requirements of secure domain
- Authentication and auditing requirements
- limitation of delivery requirements
- remote refresh requirements of ECU

References

1. Remote Exploitation of an Unaltered Passenger Vehicle, IOActive 2015 .
2. YD/T 2407-2013 Technical requirements for security capability of smart mobile terminal（TC11/WG3 CCSA CHINA）
3. http://www.autosec.org/pubs/cars-oakland2010.pdf
4. http://www.consumerreports.org/cro/news/2015/05/keeping-your-car-safe-from-hacking/index.htm

- We focus on standards and technics of automotive Cyber security.
- For a better and secure environment of automotive cars.

Yang Zhengjun
CTTL Terminals of CATR
Tel: +86-10-62300475
Mobile: +86-13811733249
E-mail: yangzhengjun@catr.cn