Cybersecurity Requirements for High Performance Computing ECUs in China

Junning Yao
Chief expert of Cybersecurity Standardization and Certification, Huawei IAS BU

October 2026

Advanced Driver Assistance Systems (ADAS)

Definition:

Systems that assist drivers in driving and parking functions

Key Functions:

- Adaptive Cruise Control (ACC) - Maintains safe distance
- Lane Keeping Assist (LKA) - Prevents unintended lane departure
- Automated Parking Assist (APA) - Assists parking maneuvers
- Navigation Cruise Assist (NCA) - Intelligent route guidance

Safety Principle:

Driver remains fully responsible for vehicle operation at all times

Key Components:

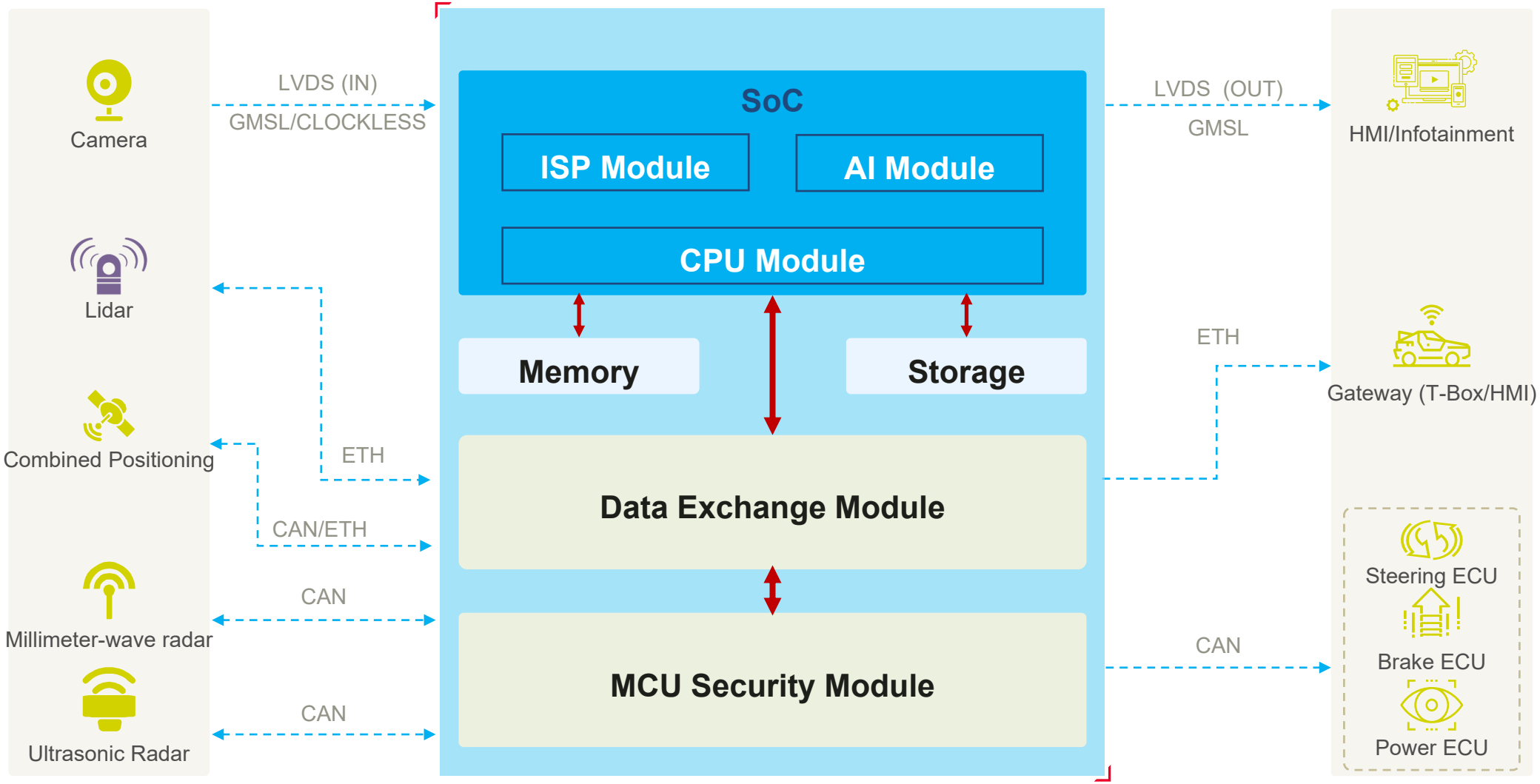
AI Computing Platform

Sensor Fusion Module

Planning & Control Module

Communication Module

High Performance Computing ECUs



GB 44495-2024: Vehicle Cybersecurity Technical Requirements

Technical Requirements for Vehicle Cybersecurity

GB 44495 is not simply a Chinese translation of UN R155. It adapts R155's risk-management principles into vehicle-level technical implementation requirements.

Specifically, Chapter 7 contains 39 technical clauses across four key technical areas.

External interface Security	**Communication** Security	**Software Update** Security	**Data** Protection & Privacy

Communication Security Requirements

External Interface: Clauses 7.1.1–7.1.4 address externally accessible physical and wireless interfaces, such as cellular, USB, OBD diagnostics and connected mobile devices.

Remote Control:

- Remote Control Command Authenticity and Integrity
- Secure Log
- Remote Control Procedure Integrity

Diagnostic:

- UDS security access
- Role-based access control
- Session timeout

Third-party Application:

- Vulnerability Scanning
- Authenticity and Integrity
- Resource Access Control

Communications security: Clauses 7.2.1–7.2.12 cover in-vehicle networks (CAN/CAN-FD and automotive Ethernet), vehicle-to-cloud links, V2V/V2I communications, and V2X certificate systems.

Cloud Communication:

- TLS secure channels
- Mutual authentication
- Session management

CAN/Ethernet:

- anti-DOS
- VLAN segmentation

V2X Communication:

- Message authentication
- Certificate check

Software Update &Data Protection

Software Updates: Clauses 7.3.1–7.3.3 address package integrity, source authenticity, and verification for general, online, and offline update scenarios.

- Update package integrity verification
- Source authentication (signature)
- Safe update process (atomic updates)
- Vulnerability Scanning

Data Protection: Clauses 7.4.1–7.4.7 address data (PII, VIN, cryptography key, critical data etc.) protection and cross-border transmission.

- Personal data classification (PII)
- VIN and Cryptography Key
- Cross-border Transmission

TARA Analysis - Key Security Goals

Critical Assets Identified:

- AI models and algorithms
- Control commands
- Certificates and cryptographic keys
- ADAS software packages
- Sensor data (Camera, LiDAR, Radar)
- Personal data (location, video)

Top Threats (by Risk Level):

SEVERE:	Unauthorized vehicle control
SEVERE:	Software tampering/malicious injection
MAJOR:	Data interception & privacy breach
MAJOR:	Certificate/key compromise
MAJOR:	Sensor data spoofing

Major Security objective

O.SECURE_INITIALIZATION — Secure Initialization of the Platform
O.EXECUTION_ISOLATION — Isolation of Execution Environments
O.ACCESS_PROTECTION — Protection Against Unauthorized Access
O.SECURE_UPDATE — Secure Platform Update
O.SECURE_KEY_MANAGEMENT — Protection of Cryptographic Keys
O.SECURE_DEBUG — Controlled Debug and Privileged Access
O.SECURE_COMPOSITION — Preservation of Security Properties During Integration

Security requirements | Interfaces and Communications

ID	Capability	Product-level requirement (shall)	Traceability
01	Non-essential ports	Disable network ports that are not required for intended vehicle functions.	GB 44495
02	Remote-control commands	Where remote-control functions exist, authenticate and integrity-protect commands; enforce access control and required security logging.	GB 44495
03	Remote-control system integrity	Where applicable, verify the integrity of systems implementing remote-control functions.	GB 44495
04	Third-party applications	Where supported, verify authorized third-party app authenticity/integrity and control unauthorized installation and resource access.	GB 44495
05	External interfaces	Protect external interfaces from unauthorized access; apply prescribed controls to applicable USB, SD-card and diagnostic interfaces.	GB 44495
06	Communication identity	Where applicable, authenticate peers for vehicle-to-cloud communication and validate certificates for relevant V2X direct communication.	GB 44495
07	Wireless integrity	Apply integrity protection to applicable external wireless communication channels.	GB 44495
08	External data commands	Control external data-operation commands and validate applicable external critical command data.	GB 44495
09	Sensitive data in transit	Protect sensitive personal information against disclosure when transmitted outside the vehicle.	GB 44495
10	Network segmentation	Where MDC performs cross-domain/gateway functions, enforce zone boundaries and access control using default-deny and least privilege.	GB 44495; R155 risk mapping
11	DoS and malicious data	Where responsible for relevant channels, detect/respond to DoS attacks and identify malicious V2X or diagnostic data.	GB 44495; R155 risk mapping

Security requirements | Data, cryptography and Software updates

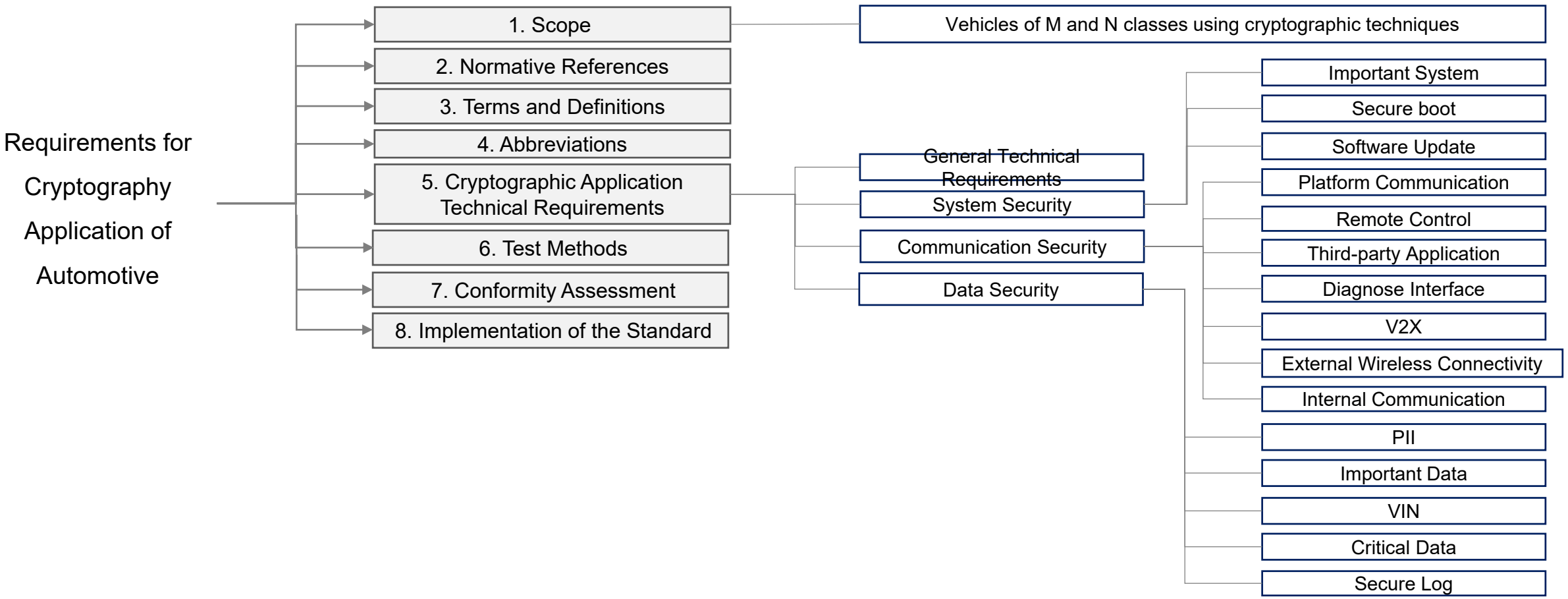
ID	Capability	Product-level requirement (shall)	Traceability
12	Security-event logs	Record applicable key communication security events and protect stored security logs from unauthorized modification/deletion.	GB 44495
13	Cryptographic key protection	Protect stored symmetric keys and private keys using secure access and/or secure storage mechanisms.	GB 44495; R155 mapping
14	Sensitive-data storage	Protect stored sensitive personal information from unauthorized access or acquisition.	GB 44495
15	Vehicle identity / critical data	Protect VIN and applicable vehicle identity, critical operating and configuration data from unauthorized deletion or modification.	GB 44495
16	Personal-data deletion	Where implemented, delete in-scope vehicle personal information, except data required to be retained by law.	GB 44495
17	Cryptographic mechanisms	Use public, effective cryptographic algorithms and compliant cryptographic modules, subject to provisions in the applicable text.	GB 44495; R155 mapping
18	Secure defaults	Use default security settings that avoid introducing unnecessary security risks through product configuration.	GB 44495; R155 risk mapping
19	Update-system integrity	Where HPC includes the vehicle update system, protect its trust anchor, bootloader and system firmware against tampering, or prevent normal startup if tampered.	GB 44495
20	Update verification	For supported update paths, authenticate relevant endpoints and verify update-package authenticity/integrity; apply prescribed controls to offline flashing.	GB 44495

Standard under developing

Requirements for vehicle data security

- 1. Scope
  - Data security requirements for M and N class vehicles
- 2. Normative References
- 3. Terms and Definitions
- 4. Security Assurance Requirements
- 5. Security Basic Requirements
- 6. Security Technical Requirements
  - General requirements for vehicle data processing
  - Requirements for individual consent
    - General requirements for individual consent
    - Exceptions to individual consent
    - Options for individual consent and refusal
    - Re-obtain individual consent
    - Withdrawal of individual consent
  - Requirements for vehicle data collection
  - Requirements for vehicle data storage
  - Requirements for vehicle data usage
  - Requirements for vehicle data transmission
    - Requirements for external vehicle transmission
    - Anonymization requirements
  - Requirements for vehicle data deletion
  - Requirements for vehicle data cross-border transfer
- 7. Test method for Security Assurance Requirements
- 8. Test method for Security Basic Requirements
- 9. Test method for Security Technical Requirements
- 10. Determination of Identical Type
- 11. Implementation of the Standard
- Annex A：Table of Vehicle Important Data Identification
- Annex B：Table of Personal Information Classification
- Annex C：Necessary Personal Information for Common Vehicle Functions
- Annex D：List of Vehicle Data Processing Activities based on Vehicle Functions
- Annex E：Parameters of Vehicle Data Collection Devices
- Annex F：Exceptions to Individual Consent

Standard under developing



Thank You

Questions & Discussion

For more information:

yaojunning@huawei.com