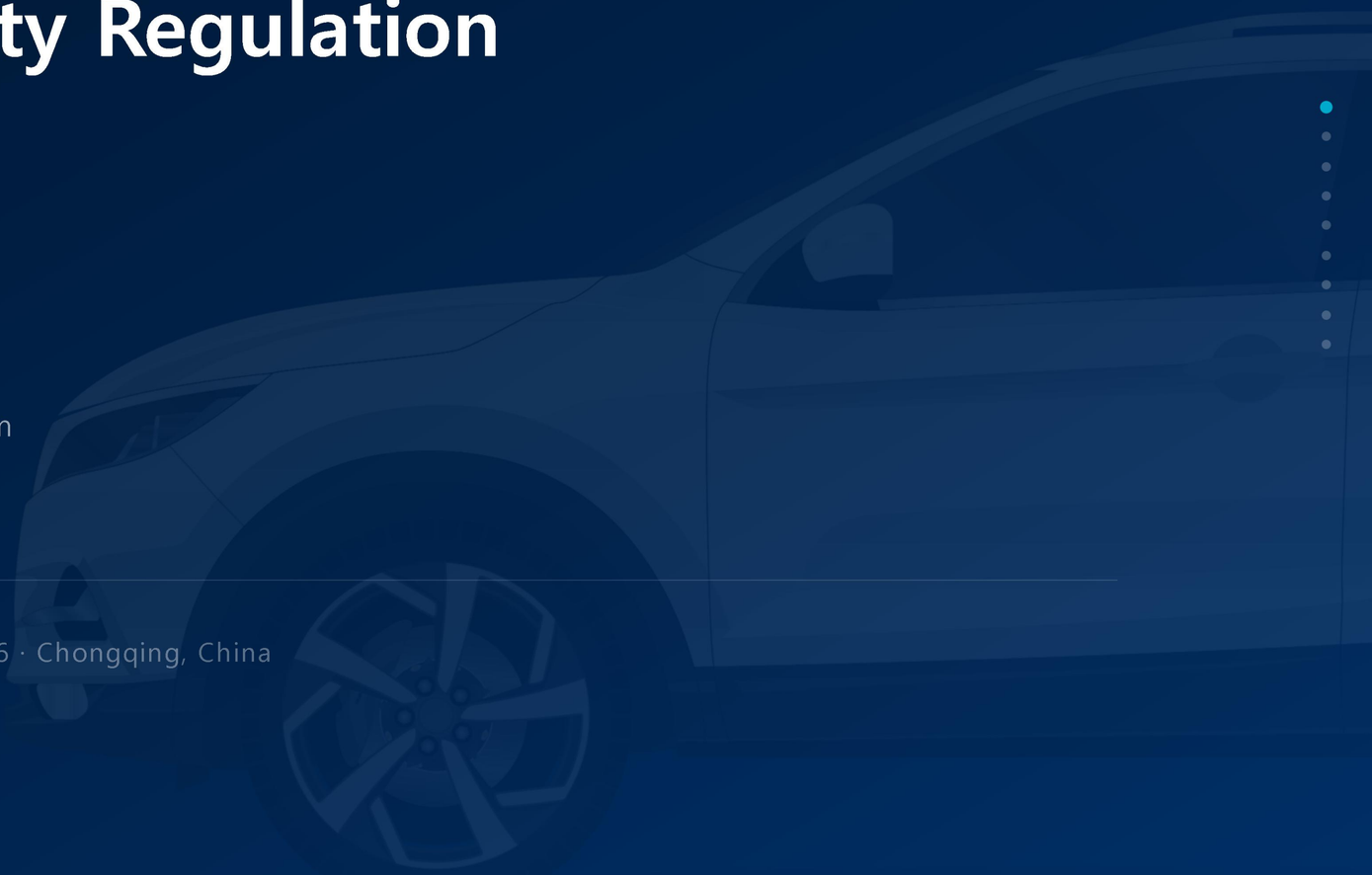
SESSION 1 — REGULATION & STANDARDIZATION

An OEM Perspective on Automotive Cybersecurity Regulation and Standardization

Jiyong Han, Ph.D.

Senior Research Engineer, Vehicle Cybersecurity Development Team
Hyundai Motor Company

ITU-T SG17 Workshop on Security of ITS and CAV · September 7, 2026 · Chongqing, China



1

Global Regulatory Landscape

UN WP.29 adoption cascade — EU, Korea, China, India

2

Multi-Jurisdictional Compliance: An OEM's Reality

One platform, multiple regulatory environments

3

HMC Contributions to ITU-T SG17

From production systems to international standards

4

Looking Ahead — The SDV Era

Emerging technical dimensions worth exploring as vehicles become software-defined

From Voluntary to Mandatory

UN WP.29 CSMS/SUMS is the shared regulatory baseline. Major markets are adopting it in succession.

2022

European Union

WP.29 CSMS/SUMS mandatory for new type approvals

2025

Korea

Full enforcement under Motor Vehicle Safety Act

2026

China

GB 44495-2024 in force (Jan 1) for new approvals

2026+

India

AIS 189 phased rollout; Level 3+ from Oct 2026

COMMON FOUNDATION

UN R155 / R156

Cybersecurity Management System (CSMS) and Software Update Management System (SUMS) — the shared language every jurisdiction adapts to its own market context

KEY OBSERVATION

Coverage expanding

By 2027, mandatory cybersecurity regulation will cover the EU, Korea, China, and India — covering the majority of global new vehicle sales

One Vehicle, Multiple Regulatory Environments

Regulation Divergence

- UN R155 as baseline, but every jurisdiction adds its own layer — no two markets impose the same obligations
- Different approval bodies, testing protocols, and documentation formats across all markets
- Timelines, scope, and enforcement criteria differ entirely — the same vehicle must satisfy completely different rules everywhere it is sold

Supply Chain Burden

- OEM CSMS mandates cybersecurity management across hundreds of suppliers
- Supplier cybersecurity posture directly impacts OEM type approval risk
- Audit and contractual frameworks must span the full supply chain depth

Lifecycle Obligation

- CSMS obligations extend through the full vehicle lifecycle to decommission
- Continuous monitoring, incident response, and periodic re-assessment
- Post-market cybersecurity management obligations extend beyond the scope of any single framework

Bottom line: For a global OEM, regulatory compliance is continuous — not a one-time certification. International standards — developed in bodies like ITU-T SG17 — provide the technical implementation layer that makes regulatory requirements actionable across markets. This is why HMC participates directly in that work alongside WP.29 compliance efforts.

HMC Editorial Contributions to Q13/17

X.1388 — Determined ✓

Feature on Demand Security Guidelines

Authentication, authorization & secure remote feature delivery for vehicle subscriptions

X.1375-rev — Under study

In-Vehicle IDS Guidelines (revised)

CAN & Ethernet detection architecture for heterogeneous in-vehicle networks

X.ivkm-sec — Under study

In-Vehicle Key Management Security

Key lifecycle management across ECUs and HSMs in vehicle architectures

X.aamd-sec — Under study

Advanced Air Mobility Data Security

Security requirements for categorized data in advanced air mobility (AAM) environments

X.abt-sec — Under study

Account-Based Ticketing Security in ITS

Security requirements for account-based ticketing in intelligent transport services

X.cov-sec — Under study

Covert Channel Countermeasures in Connected Vehicles

Security guidelines against covert channel attacks in in-vehicle network communications

X.ota-sec — Under study

Remote SW Update Security Functions

Implementation & evaluation of security functions for remote software update capability

Where ITU-T Standards Meet Industry Practice

X.1388 · DETERMINED ✓

FoD Security Guidelines

Authentication, authorization, and trust model for remote vehicle feature delivery. ITU-T Determined June 2026.

↔

INDUSTRY APPLICATION · 2022–PRESENT

FoD Secure Subscription System

HMC production remote feature subscription system. WP.29 CSMS VTA certified. Provided the technical basis for the standard.

X.1375-REV · UNDER STUDY

In-Vehicle IDS Guidelines (revised)

CAN and Ethernet detection architecture for heterogeneous in-vehicle networks. Existing standard covers CAN only.

↔

INDUSTRY APPLICATION · 2022 & 2025–PRESENT

CAN IDS + Ethernet IDS

Production CAN IDS (2022) and Ethernet IDS (2025) across multiple HMC platforms. WP.29 CSMS VTA certified.

X.IVKM-SEC · UNDER STUDY

In-Vehicle Key Management Security

Vehicle-specific key lifecycle management across ECUs and HSMs — a technical gap in ISO/SAE 21434.

↔

INDUSTRY APPLICATION · 2021–PRESENT

Multi-ECU Key Management at Scale

Cryptographic keys managed across hundreds of ECUs and HSMs in HMC production vehicles across multiple markets.

X.OTA-SEC · UNDER STUDY

Remote SW Update Security Functions

Security functions for integrity verification, authentication, and rollback protection in remote vehicle software update processes.

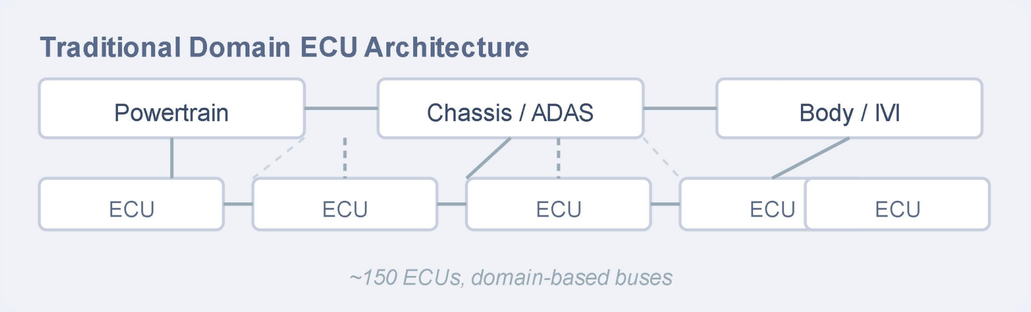
↔

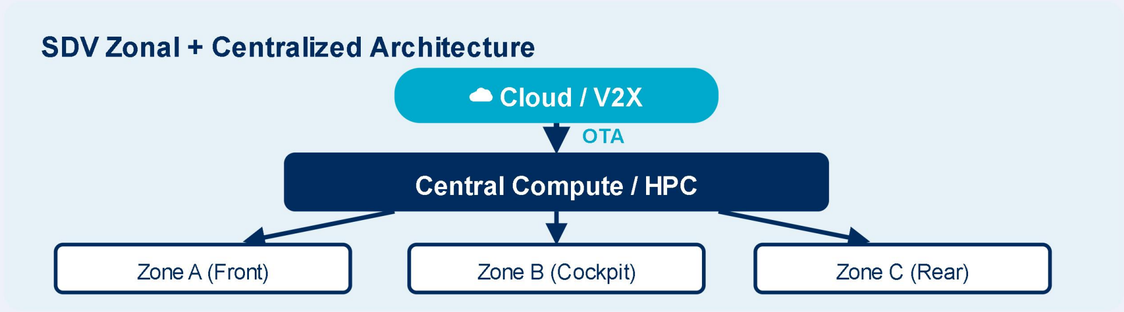
INDUSTRY APPLICATION · 2019–PRESENT

Production Remote SW Update System

HMC production OTA system. WP.29 CSMS VTA certified. Manages secure update delivery and activation across vehicle ECUs at scale.

SDV Introduces Technical Dimensions Worth Addressing Collectively





CONNECTED VEHICLE ERA

- Fixed ECU functions, defined at production
- Periodic, planned software updates
- Known, stable attack surface at time of type approval
- ECU-level TARA methodology sufficient
- Closed, proprietary software supply chain

SOFTWARE-DEFINED VEHICLE ERA

- Software-defined features, updated via remote software updates throughout lifetime
- Continuous, dynamic changes — functions evolve post-market
- Dynamic attack surface; third-party app ecosystem
- Feature-level / platform-level TARA required
- Open ecosystem: SBOM, CBOM management critical

As the Industry Shifts to SDV, These Are Areas Worth Exploring

SDV TECHNICAL DIMENSIONS

01 Cryptographic Bill of Materials (CBOM) for Vehicles

We manage hundreds of cryptographic assets across ECUs today without a common reference framework. As PQC transition approaches, a common CBOM framework will become increasingly valuable across the industry

02 Crypto Agility in the Vehicle Context

Vehicles stay on the road 15+ years. Defining how to safely migrate algorithms via remote update over that lifetime is something the industry will need to handle — and a standard reference would help everyone

03 Feature-Level TARA Methodology

As vehicles become software-defined, threat analysis needs to move from ECU-level to feature and platform level. A common methodology for this would be useful for the whole industry, not just OEMs

WHERE TECHNICAL STANDARDS COMPLEMENT REGULATION

04 Post-Market Remote Updates — Technical Standards Add Precision

Regulations set a clear requirement for CSMS management across the vehicle lifecycle. A technical standard can add the implementation-level precision — specifically, how continuous remote updates interact with that obligation — complementing what regulation defines at a higher level

05 Cross-Jurisdiction Technical Alignment — A Role for Standards

UN R155, GB 44495, and AIS 189 share the same foundational intent. A common ITU-T technical standard could serve as the shared implementation reference that all three frameworks build upon — reducing redundant work for OEMs while reinforcing each framework's objectives

1 Mandatory regulation now covers the majority of global vehicle markets — compliance is no longer optional

2 International standards — ITU-T SG17 in particular — are what makes regulatory requirements implementable in practice

3 SDV is already reshaping what vehicles are — this is the right moment for the standardization community to define what comes next

Thank you