AUTOMOTIVE CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

0.1 2. Autonomous Driving Governance 1
0.2 3. Cybersecurity 2
0.3 4. Type Approval 2
0.4 5. V2X Communication 2
0.5 6. Quality & Production 3

1 Constraints 3

All vehicle safety functions MUST be classified and governed according to automotive safety integrity levels.

Example: ISO 26262:2018 (Road Vehicles Functional Safety) defines ASIL A through ASIL D based on severity, exposure, and controllability. ASIL D (highest) applies to steering, braking, and airbag systems failures cause life-threatening or fatal injuries with high probability of exposure and difficult controllability. Safety goals derive from hazard analysis and risk assessment (HARA): e.g., Unintended acceleration shall not exceed 0.3g for more than 200ms (ASIL D). Functional safety concept allocates safety requirements to hardware (HW) and software (SW) elements. Hardware metrics: single-point fault metric (SPFM 99% for ASIL D), latent fault metric (LFM 90% for ASIL D), probabilistic metric for random hardware failures (PMHF < 10ˆ-8/h for ASIL D). Software development per Part 6: ASIL D requires formal verification, back-to-back testing, semi-formal notations. MAGIC gate: bitwise AND of required ASIL dimensions before safety-critical ECU command executes.

0.1 2. Autonomous Driving Governance

Autonomous driving functions MUST be governed according to SAE autonomy levels with explicit ODD definition and fallback.

Example: SAE J3016:2021 defines six levels of driving automation: Level 0 (no automation driver performs all DDT), Level 1 (driver assistance single mode: ACC or lane keeping), Level 2 (partial automation combined longitudinal and lateral control, driver must supervise), Level 3 (conditional automation system performs DDT within ODD, driver is fallback-ready within 10s), Level 4 (high automation system handles all DDT and fallback within ODD, no driver needed in ODD), Level 5 (full automation all conditions, no ODD restriction). Operating Design Domain (ODD) defines: road types (highway, urban, rural), speed range, weather (clear, rain,

fog, snow), lighting (day, night, tunnel), geographic boundaries (geofenced areas). Object and Event Detection and Response (OEDR): system must detect and respond to all objects and events within ODD. Fallback: Level 3 = human fallback (transition demand), Level 4-5 = system fallback (minimal risk condition MRC). UNECE WP.29 ALKS regulation (R157): first binding Level 3 regulation max 60 km/h, motorway only, system must achieve MRC within 4s.

0.2 3. Cybersecurity

Vehicle cybersecurity MUST be managed throughout the lifecycle with threat analysis, risk assessment, and continuous monitoring.

Example: ISO/SAE 21434:2021 (Road Vehicles Cybersecurity Engineering) establishes cybersecurity management system (CSMS) across vehicle lifecycle: concept, development, production, operation, maintenance, decommissioning. Threat Analysis and Risk Assessment (TARA): identifies assets (ECU firmware, V2X keys, OTA payloads), threat scenarios (remote code execution, CAN bus injection, GNSS spoofing), attack paths (Bluetooth, Wi-Fi, OBD-II, cellular), and determines cybersecurity assurance levels (CAL 1-4). UNECE WP.29 R155 (Cyber Security Management System): mandates CSMS for type approval 7 categories, 30 specific threats. R156 (Software Update Management System): governs OTA update process integrity verification, rollback capability, update campaign management. Attack surface: CAN/CAN-FD (no authentication by default), Ethernet (SOME/IP, DoIP), V2X (IEEE 1609.2 certificates), telematics (cellular modem), infotainment (USB, Bluetooth, Wi-Fi). Secure boot chain: HSM bootloader OS application, with each stage verifying the next.

0.3 4. Type Approval

Vehicles MUST obtain type approval demonstrating compliance with all applicable safety, emissions, and cybersecurity regulations.

Example: UNECE regulations provide harmonized type approval framework: R13 (braking heavy vehicles), R13-H (braking passenger), R79 (steering), R94 (frontal impact), R95 (side impact), R137 (frontal impact updated), R127 (pedestrian safety). US Federal Motor Vehicle Safety Standards (FMVSS): FMVSS 108 (lighting), FMVSS 208 (occupant crash protection frontal), FMVSS 214 (side impact), FMVSS 301 (fuel system integrity), FMVSS 305 (EV electrolyte spillage). EU General Safety Regulation (EU 2019/2144 GSR): mandates intelligent speed assistance (ISA), alcohol interlock installation facilitation, drowsiness/attention warning, advanced emergency braking (AEB), emergency lane-keeping (ELKS), event data recorder (EDR), tire pressure monitoring (TPMS) effective July 2022 for new types, July 2024 for all new vehicles. Homologation process: manufacturer submits technical documentation, test reports from accredited labs (e.g., Euro NCAP, TUV, DEKRA), authority issues type approval certificate with approval number.

0.4 5. V2X Communication

Vehicle-to-everything communication MUST be governed with authenticated messages, bounded latency, and privacy preservation.

Example: IEEE 802.11p (WAVE Wireless Access in Vehicular Environments): 5.9 GHz band, 10 MHz channels, range 300-1000m, latency <100ms. C-V2X (Cellular Vehicle-to-Everything): 3GPP Release 14+ PC5 sidelink direct communication without cellular infrastructure, latency <20ms for Mode 4. V2V (Vehicle-to-Vehicle): Basic Safety Message (BSM) per SAE J2735 broadcasts position, speed, heading, acceleration, brake status at 10 Hz. V2I (Vehicle-to-Infrastructure): Signal Phase and Timing

(SPaT), MAP (intersection geometry), Traveler Information Message (TIM). V2P (Vehicle-to-Pedestrian): vulnerable road user awareness. DSRC (Dedicated Short-Range Communications): IEEE 1609 family 1609.2 (security services, PKI certificates), 1609.3 (networking), 1609.4 (multi-channel operation). Security: SCMS (Security Credential Management System) provides pseudonym certificates (rotating every 5 minutes for privacy), misbehavior detection, certificate revocation lists (CRL). Latency requirements: pre-crash warning <100ms, intersection collision <200ms, cooperative adaptive cruise control <50ms.

0.5 6. Quality & Production

Automotive quality management MUST follow IATF 16949 with core tools ensuring defect prevention and continuous improvement.

Example: IATF 16949:2016 (Quality Management System Automotive) builds on ISO 9001 with automotive-specific requirements: customer-specific requirements (CSR), production part approval process (PPAP), control plans, MSA, SPC. PPAP (Production Part Approval Process) 18 elements: design records, engineering change documents, DFMEA, process flow diagram, PFMEA, control plan, MSA studies, dimensional results, material/performance test results, initial process studies, qualified laboratory documentation, appearance approval report, sample parts, master sample, checking aids, customer-specific requirements, Part Submission Warrant (PSW), bulk material requirements. FMEA (Failure Mode and Effects Analysis): AIAG & VDA FMEA Handbook (2019) 7-step process: planning and preparation, structure analysis, function analysis, failure analysis, risk analysis (AP Action Priority instead of RPN), optimization, results documentation. SPC (Statistical Process Control): Cpk 1.33 for stable processes, Ppk 1.67 for new processes. MSA (Measurement Systems Analysis): Gage R&R %GRR < 10% acceptable, 10-30% conditionally acceptable, >30% unacceptable. 8D problem-solving methodology for customer complaints.

---

1. Constraints

```
MUST:     Cite ISO 26262, SAE J3016, or domain-specifi
MUST:     Map ASIL level to MAGIC checkset governance
MUST:     Distinguish between SAE Levels 0-5 with expl
MUST NOT: Present Level 2 (partial automation) as auto
```

AUTOMOTIVE | CANON | VERTICALS