88° IFIP WG 10.4 MEETING

Summary for Session 1

Automotive Cybersecurity

Rapporteur: **João R. Campos**
University of Coimbra

29 June 2026

Session overview

- 3 (+1) speakers
- Focus on security challenges in connected, software-defined vehicles (SDVs)
- Explored the intersection of cybersecurity, safety, and assurance
- Insights from semiconductor, middleware, and assurance experts
- Examined gaps between regulations, standards, and practice
- Addressed how to move from compliance checklists to systemic assurance

Timo van Roermund, NXP – Evolution (1/3)

- "The past & future of automotive security – from the perspective of a semiconductor supplier”
- Historical Milestones
  - 1990s: Immobilizers reduced car theft (ID → crypto)
  - 2000s–2010s: Secure Hardware Extensions (SHE), EVITA HSMs
  - 2015: Formation of Auto-ISAC
  - 2018–2024: UWB tech, smart access, ISO/SAE 21434
  - 2024+: Software-defined vehicles, Post-Quantum Crypto (PQC)
- Impact
  - Pressure from external stakeholders, such as insurance companies refusing to insure vehicles without immobilizers
  - European legislation (Directive 95/56/EC) led to drastic car theft reduction
- Trust must be anchored in hardware, chain of thrust from manufacturing to application level

Timo van Roermund - Challenges (2/3)

- **Current Landscape**
  - **Security is now mandatory (UN R155, ISO/SAE 21434)**
  - **Hardware root-of-trust and enclave-based SoC security**
  - **Key provisioning (factory, 3rd party) remains a weak point if not securely managed**
  - **Compliance involves lifecycle-wide validation**

- **Toward the Future**
  - **Post-Quantum Crypto: NIST FIPS 203-205 standards (e.g., Kyber, Dilithium)**
  - **Software-Defined Vehicles need resource isolation, remote attestation**
  - **ECU-to-ECU trust becomes important**

Timo van Roermund - Discussion (3/3)

- Standards vs. Legislation
  - ISO/SAE 21434 vs. legal mandates (EU already has laws)
  - Country-based legislation (EU vs China vs US)
- Implementation & Trust
  - Concern about standalone vs. interconnected systems
  - Standards are essential but insufficient without holistic, practical implementation
  - How to gain confidence in secure complex systems?
- Issues Identified
  - Suppliers often lack context due to data-sharing gaps
  - Checkbox compliance ≠ actual security
  - SESIP and 3rd-party certification are needed for high assurance (unlike self-certification)
  - Need for training and systemic thinking

Hector Bravo Amella, TTTech – Decentralized (1/3)

- "Security in SDVs: Lessons learned from integrating MotionWise Safety Middleware in customer ECUs”
- SDV Redefined
  - Not just software: 4SDV = System + Safety + Security + Software
  - Must be secure and safe by design, not retrofit
- Architecture Shift
  - From ~20+ decentralized ECUs → ~5 high-performance ECUs
  - Centralization reduces hardware attack surface, fewer interfaces
  - Enables simplified key management, unified security policies
- Issues
  - Software complexity increases: shared SoCs, mixed-criticality apps
  - Runtime isolation & freedom from interference are more difficult

Hector Bravo Amella – Supply Chain (2/3)

- **Supply Chain Breakdown**
  - **OEM sets vehicle-level security goals but shares only partial info**
  - **Tier 1 (ECU supplier) must validate based on incomplete assumptions**
  - **Tier 2 (SoC + SW vendors) have even less context → more assumptions → more cost/error**
- **Implications**
  - **Redundant validation, missed threats, or overengineering**
  - **Misaligned controls may lead to system conflicts or vulnerabilities**
  - **Failure to define or propagate goals can halt production**
- **Barriers to Info Sharing**
  - **IP protection, competitive concerns, immaturity of new startups**
  - **OEMs retain full control of security architecture**

Hector Bravo Amella – Discussion (3/3)

- Security Needs Integration
  - Bootloaders: Must be verified early or run-time degraded if tampering
  - Secrets need hardware-isolated storage (MPU/MMU, HSM)
  - Secure Boot + Chain of Trust must survive updates
- Agile & Automotive Industry
  - Various challenges, misalignment between Agile and safety-critical dev
  - Fast SW deployment, slow safe validation – a growing mismatch
  - TTTech sees difficulty in embedding security into fast-moving processes
- Key Issues Raised
  - Centralization simplifies TARA, but impact harder to estimate
  - Good security should not depend on secrecy
  - General agreement: communication across tiers must improve

Robert Stroud, NCC – Functional Safety (1/3)

- “Automotive Systems Engineering – Standards and Regulations”
- Historical Context & Key Standards
  - ISO 26262 (2011): Functional safety (based on IEC 61508)
  - Introduced “Safety Element Out of Context” (SEooC)
  - ISO/SAE 21434 (2021): Cybersecurity engineering across the lifecycle
  - ISO 21448 (SOTIF): Risks from functional insufficiencies, not “failures”
  - Complements ISO 26262, especially relevant for AI-driven systems
  - PD ISO/TR 4804: Merging safety + cybersecurity for automated driving
- System-level cybersecurity for automotive is recent

Robert Stroud – Regulation (2/3)

- UN Regulation No. 155 (2021) (WORLD FORUM FOR HARMONIZATION OF VEHICLE REGULATIONS):
  - Requires Cybersecurity Management System (CSMS)
  - Type-approval basis in many countries (mainly EU-centric)
- U.S. Model: Self-certification, not approval
  - Manufacturer claims compliance (no pre-market regulatory check)
- Cybersecurity lacks an equivalent to SEooC – makes reusing validated components harder
- International inconsistency leads to complex compliance challenges

Robert Stroud – Compliance (3/3)

- Compliance vs. Assurance
  - Compliance = checkbox; Assurance = confidence
  - Standards (e.g., ISO/SAE 21434) describe what, not how
- Questions Raised in Discussion
  - What/how should evidences be presented?
  - How are hazards defined in the context of insufficiencies (SOTIF)?
  - Level of evidence needed is still evolving – industry is “learning by doing”
  - What is “enough” assurance? Who decides?
- Key Paradigm Shift
  - From prescriptive compliance → to argument-based assurance
  - Not just “follow the rule”, but “demonstrate it’s safe and secure”

Dimitri Havel, NCC – FuSA (1/3)

- “What the history of Functional Safety can teach us about the future of cybersecurity in automotive”
- Several FuSa and Cybersecurity Parallels:
  - Both follow the V-model lifecycle.
  - Both involve systematic risk identification, classification, and treatment.
  - Structured standards exist:
    - FuSa: ISO 26262 (~1000 pages)
    - Cybersecurity: ISO/SAE 21434 (~100 pages)
- Organizational & Process Similarities:
  - Both rely on formal management systems (FSMS/CSMS).
  - Increasing need for tailored tooling (moving away from Excel to integrated platforms).
  - Shared needs in reuse, out-of-context development, and COTS integration.

Dimitri Havel – Why not FuSA (2/3)

- **Failure Distribution:**
  - **FuSA: Uniform (static over time)**
  - **Cybersecurity: Cumulative (gets riskier with time if unmanaged)**
- **Root of Threat:**
  - **Safety = random/systematic faults**
  - **Security = intelligent threat actors with intent**
- **Incentives:**
  - **FuSA = best practice**
  - **CS = legal compliance and homologation (you *must comply to sell)**
- **Challenges in Practice:**
  - **Cybersecurity is a moving target**
  - **Requires continual improvement & lifecycle integration**
  - **Current efforts often rely on implicit security cases (expectation is to shift to explicit)**

Dimitri Havel – Discussion (3/3)

- Cybersecurity ROI is hard to quantify — seen as bottom priority
- Industry tends to avoid action unless incentivized
- Might be cheaper to pay lawsuit costs than do cybersecurity right
- Cybersecurity is evolving – regulatory pressure will escalate expectations
  - CRA and similar initiatives might extend pressure across the supply chain, although automotive industry already has legislation
- Security is “a moving target,” unlike safety
- FuSA practices and knowledge should be leveraged for cybersecurity maturity
- Legal liability is growing — failure might require demonstrating due diligence in court

Session Summary & Key Takeaways

- **Technical & Architectural Trends**
  - **Transition to centralized, high-performance ECUs in SDVs**
  - **Increased complexity in securing mixed-criticality systems**
  - **Security needs to be rooted in hardware and extend throughout the lifecycle**
- **Cybersecurity Evolution**
  - **Cybersecurity is no longer optional — enforced by UN R155, ISO/SAE 21434, and national laws (e.g., EU, China)**
  - **Requires continuous risk management, not one-time compliance**
  - **PQC, secure enclaves, and ECU-to-ECU monitoring emerging as new frontiers**

Open Challenges & Future Directions

- **Key Issues Identified**
  - **Lack of transparency across OEM–Tier 1–Tier 2 supply chain leads to misaligned security goals**
  - **Standards are necessary but insufficient without assurance and system-level context**
  - **Security by design is hindered by speed-focused development, immature tooling, and organizational silos**

- **Where We Go Next**
  - **Shift from checklist compliance to explicit assurance arguments**
  - **Develop shared tooling, threat models, and certification strategies across the supply chain**
  - **Promote cross-disciplinary collaboration between cybersecurity, safety, and systems engineering teams**

88° IFIP WG 10.4 MEETING

Summary for Session 1

Automotive Cybersecurity

Rapporteur: **João R. Campos**
University of Coimbra

29 June 2026