88th IFIP WG 10.4 meeting - Cybersecurity of Transportation Systems, 26-29 June, Ischia, Italy

Meeting Organizers: Domenico Cotroneo (University of Naples "Federico II", Luigi Romano (University of Naples "Parthenope")

Workshop Coordinators: Andrea Ceccarelli (University of Florence), Wilfried Steiner (TTTech AG), Marcus Volp (University of Luxemburg)

The relevance of software in transportation systems and related infrastructure is constantly growing. Unavoidably, cybersecurity is an increasing concern. Over two days of technical discussions, the IFIP WG 10.4 members discussed and compared the cybersecurity status and challenges in different transportation industries – automotive, railway, and avionics – also addressing socio-technical aspects and the role of humans in the loop.

Summary of the Automotive Cybersecurity Session

This session explored cybersecurity in connected, software-defined vehicles (SDVs), featuring insights from semiconductor, middleware, and assurance experts. It traced automotive security's history from early immobilizers to today's hardware roots-of-trust and upcoming post-quantum cryptography accelerators.

Key architectural trends include a shift from many decentralized ECUs to a few powerful centralized ones, simplifying hardware security but complicating software due to mixed-criticality and runtime isolation needs. The session highlighted gaps between standards (ISO/SAE 21434, UN R155) and practical assurance, noting that compliance may become a checkbox exercise lacking systemic trust. Supply chain fragmentation – OEMs, Tier 1, Tier 2 – can lead to misaligned security goals, aggravated by poor information sharing.

Discussion underscored that unlike functional safety, cybersecurity must evolve continually to counter intelligent, adaptive threats. Moving forward, the community highlighted benefits shifting from prescriptive compliance to argument-based assurance and improving communication and sharing between the automotive industry chain of supply.

The session was composed of the following talks:

- "The past & future of automotive security – from the perspective of a semiconductor supplier" by Timo van Roermund (NXP),
- "Security in SDVs: Lessons learned from integrating MotionWise Safety Middleware in customer ECUs", by Hector Bravo Amella (TTTECH AUTO), and
- "What the history of Functional Safety can teach us about the future of cybersecurity in automotive", by Robert Stroud and Dimitri Havel (NCC GROUP).

Summary of the Railway Cybersecurity Session

This session provided a critical perspective on how cybersecurity is currently applied in the railway sector, with a specific focus on the practical challenges of adopting the IEC 62443 standard and the CLC/TS 50701 technical specification. Three major implementation gaps affecting today's projects were identified, namely:

i) the tendency to assign flat Security Level Targets per zone, regardless of functional roles and exposure;
ii) the overdesign risks due to lack of guidance on SL-T assignment; and

iii) the incompatibility between generic SL-T targets and railway-specific constraints (e.g., UNISIG protocols).

To address these issues, a context-aware methodology to assign a tailored SL-T value for each node in a zone (based on real exposure and functional impact) was proposed, which applies:

i) node-level threat modeling using STRIDE-LM;
ii) risk estimation through an Attack Feasibility Rating (AFR); and
iii) generation of SL-T vectors per each Foundational Requirement (FR).

The final message delivered was that SL-T must not be treated as a fixed label, but rather as the result of a documented, reasoned, and reproducible process, aligned with both risk and architectural constraints.

Furthermore, this session broadly covered the issues around the digitalization of railway operation, not only from the cybersecurity perspective. In particular, the European EULYNX Initiative, committed to the standardisation of interfaces and elements within railway signaling systems, as well as to enhancing modularity and system longevity, was presented. Another focus was on the ENISA report "Security measures in the Railway Transport Sector", which identifies several cybersecurity challenges, including low cybersecurity awareness in the railway sector and the difficulty in reconciling the safety and cybersecurity worlds. Elaborating on the current trends, the risk has been identified that digitalization may weaken Command, Control, and Signaling (CCS) for railway systems. Needs currently requiring solutions including:

i) to cope with a long system lifetime;
ii) to address attacks that affect innovative technologies as well as publicly available confidential data about the infrastructure;
iii) to make certification processes adaptable and updatable at a low cost;
iv) to trade-off safety and availability;
v) to properly address resiliency.

The final message delivered was that today, the physical security of digital CCS for railways is of much bigger concern than cybersecurity.

The session was composed of the following talks:

- "Current challenges in applying cybersecurity in railway signalling systems according to current available cyber-security standards", by Francesco Brancati (ResilTech) and
- "Digital Railway Operation – Cybersecurity in Critical Infrastructures", by Andreas Polze (Univ. of Potsdam).

Summary of the Aerospace Cybersecurity Session

This session discussed cybersecurity challenges in aerospace systems. Several legacy aerospace subsystems have been presented and practical difficulties in applying existing cybersecurity techniques have been addressed. The long development cycle in aerospace has been identified as key challenge to adequately predicting the security threats several tens of years into the future. Formal methods have been discussed for identification of possible attack propagation.

Furthermore, the benefits and risks associated with the use of Artificial Intelligence in the development and in the operation of aerospace systems have been discussed.

The session was composed of the following talks:

- “Trustworthiness Challenges and needs in modern and future aviation ecosystems”, by Stefano Sebastio (Collins Aerospace) and
- “Current and future challenges in aviation cybersecurity”, by Cora Perner (Airbus).

Summary of the Socio-Economical Aspects Session

This session was comprised of a talk - “The weakest link, and other myths about the human in the loop: a socio-technical understanding of security in critical situations”, by Gabriele Lenzini (University of Luxembourg) – discussing how socio-economical aspects challenged the common perspective of framing humans as the weakest link of securing technical systems. The talk proposed to instead include human weaknesses and strengths in the design of technical systems, discussing as an example, a protocol design that considers typical human behavior.

In addition to the above talks, a panel on the “Future and challenges of cybersecurity of the transportation industry”, moderated by Behrooz Sangchoolie (RISE Research Institutes of Sweden, SE), addressed many aspects of all sessions of the workshop. The need for an economic model for dependability has been stressed to increase impact on decision makers.

Panelists were:

- Saurabh Bagchi (Purdue University, US),
- Cristina Nita-Rotaru (Northeastern University, US),
- Chris Walter (WW Technology Group, US),
- Francesco Brancati (ResilTech, IT).