講演番号	160

Cybersecurity for Euro 7

Requirements, Risks and Technical Solutions for Next-Generation Vehicles

Dr. Claude-Pascal Stöber-Schmidt [1)] Richard Lange [1)] Steve Peters [2)] Dr. Dennis Kengo Oka [2)] Dr. Philipp Jungklass [1)]

1)IAV GmbH Ingenieurgesellschaft Auto und Verkehr, Carnotstraße 1, 10587 Berlin, Germany
2) IAV Japan Co., Ltd., Uchikanda Chuo Bldg. 3F, 1-18-13 Uchikanda, Chiyodaku, Tokyo, 101-0047, Japan

KEY WORDS: **heat engine, post treatment system,** measurement/diagnosis/evaluations (A1), **Software and its underlying technologies, cyber attack methods,** cybersecurity (E3), **regulations/engineering ethics**, standard/regulation (F2)

This paper analyzes the cybersecurity and anti-tampering requirements introduced by the Euro 7 regulation and highlights their implications for the design and operation of next-generation vehicle electronics. Euro 7 significantly expands the regulatory scope by introducing stricter emission limits, durability requirements, and comprehensive cybersecurity obligations for all emission-relevant systems. Annex XIV places particular emphasis on preventing unauthorized modifications, mandating the integration of Threat Analysis and Risk Assessment (TARA), continuous vulnerability management, and manipulation-resistant system design. The paper shows that cybersecurity and emissions compliance are fundamentally interdependent, especially as Euro 7 requires secure handling of diagnostic data, on-board monitoring (OBM) outputs, and software updates.

A major focus of the paper lies on the OBM system, which acts as a central element for detecting manipulation of emission-relevant components. The authors describe how OBM uses a digital twin composed of steady-state NOx models, transient neural network models, and high-fidelity catalyst simulations to estimate real-time emissions. These model predictions are compared to sensor data under varying driving conditions, supported by validity checks to prevent false positives. The paper demonstrates that OBM—when combined with intrusion-detection capabilities—classifies tampering through a three-level status system (0–2), with Level 2 triggering an inducement mechanism that can restrict vehicle operation.

Two detailed attack scenarios illustrate practical vulnerabilities: removal of the three-way catalyst combined with a man-in-the-middle manipulation of NOx sensor signals, and odometer manipulation intended to exploit Euro 7 durability factors. These examples reveal that OBM alone cannot provide complete protection, as sensor authenticity must be ensured through lightweight cryptographic key management systems and secure ECU architectures. The authors conclude that only the combined use of hardware-based safeguards—such as Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs)—and software-based protections—such as secure boot, authenticated flash, secure onboard communication, and runtime integrity validation—can achieve the level of cybersecurity resilience demanded by Euro 7.

Overall, the paper makes clear that future emissions legislation cannot be met without cybersecurity. It argues that Euro 7 fundamentally transforms emissions control into a cybersecurity-dependent discipline and calls for a holistic, multilayered defense strategy across all emission-relevant vehicle components.

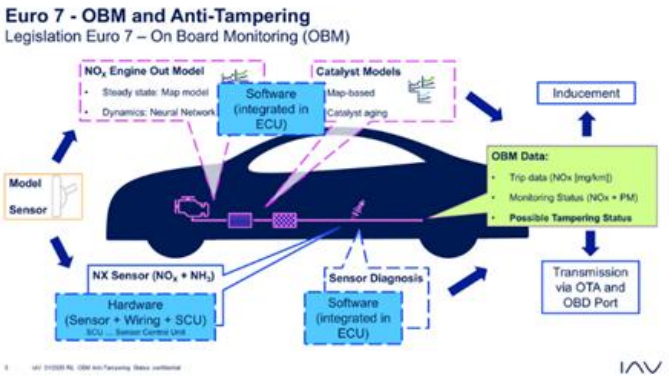

Fig. 1: Overview of OBM System