講演番号	040

Software Updates as Enabler for Cyber Security in the CV Domain

-From Regulations to Processes to a One-Stop System Solution-

Dr. Alexander Roy [1)] **Gila-Marie Achenbach** [1)]
Dr. Dennis Kengo Oka [2)]

1) IAV GmbH, Rockwellstr. 12, 38518 Gifhorn, Germany
2) IAV Co. Ltd., Uchikanda Chuo Bldg. 3F, 1-18-13 Uchikanda, Chiyoda-ku, Tokyo 101-0047, Japan
(E-mail: dennis.kengo.oka@iav.jp)

KEY WORDS: Software Update Management System, SUMS, OTA, Cyber Security, UN R156, System Solution

The accelerating digitalization of Commercial Vehicles (CV) and the emergence of software-defined vehicle architectures are fundamentally transforming the industry. As software complexity increases, so do the demands for maintaining cybersecurity, ensuring functional integrity, and enabling reliable software updates over the entire vehicle lifecycle. Software Update Management Systems (SUMS) have therefore become a central pillar, integrating regulatory obligations, technical safeguards, and organizational processes into a comprehensive management framework.

From a regulatory perspective, UN R155 (cybersecurity) and UN R156 (software updates) define some mandatory requirements for type approval across most vehicle categories, while standards such as ISO21434 and ISO24089 translate these expectations into detailed technical and process-oriented guidance. The European Cyber Resilience Act (CRA) further expands obligations to products not covered by above mentioned UN ECE regulations, thereby compelling manufacturers to perform systematic regulatory classification and develop sustainable SUMS concepts for virtually all modern vehicles and machines.

SUMS extends far beyond Over-the-Air (OTA) update capabilities. While OTA provides an efficient transmission path, SUMS governs the entire end-to-end process: preparation and protection of update artefacts, variant and configuration management, homologation-relevant documentation, traceability mechanisms, and controlled rollout strategies. A core requirement is the precise knowledge of both current and historical software configurations on every single vehicle, which is essential for compatibility checks, legal compliance, and functional safety.

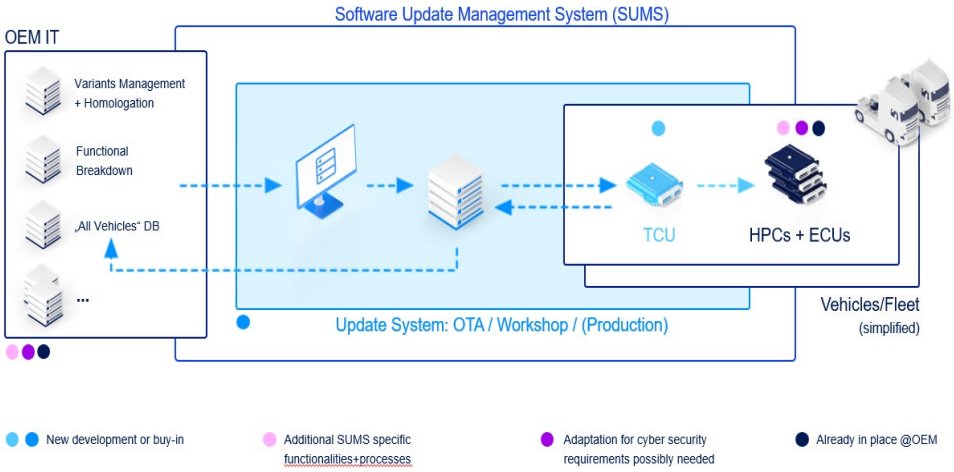

Figure 1 SUMS Functional Blocks (Generalized Concept).

Introducing SUMS affects a wide range of existing processes across development, production, service, IT, and homologation. The primary challenge lies in integrating and harmonizing established systems such as workshop tools, production equipment, configuration and variant databases, Product Livecycle Management (PLM) environments etc. SUMS necessitates clearly defined responsibilities, robust governance structures, and a project-oriented approach to planning, executing, and monitoring each update campaign.

From a technical perspective, SUMS relies on secure vehicle platforms featuring mechanisms such as secure boot chains, redundant memory concepts, integrity validation data (IVD), and resilient recovery procedures. Organizationally, SUMS must be tightly aligned with Cyber Security Management Systems (CSMS), since cybersecurity and software updates are interdependent and must reinforce each other across the entire lifecycle.

For OEMs, a structured implementation approach is recommended: assessing existing capabilities, identifying gaps, addressing strategic make-or-buy decisions, and involving experienced system integrators early in the process. A unified “one-stop solution” approach helps consolidate the diverse regulatory, technical, and organizational requirements into a scalable, auditable, and future-proof SUMS.

A fully integrated SUMS not only ensures compliance with global regulatory frameworks but also enables continuous quality improvements, enhances operational safety and security, and forms the basis for new data- and software-driven business models across the entire fleet lifecycle.