Automotive Cybersecurity

Beratung Aufbau und Erfüllung von UN Regulierungen 155/156, ISO/SAE 21434 und verwandten Normen

Im Zuge der Digitalisierung nimmt sowohl der Anteil von Software im Fahrzeug als auch die Vernetzung der Fahrzeuge mit ihrem Umfeld seit Jahren stetig zu. Um die daraus resultierenden Risiken für Cyberattacken geeignet zu adressieren werden durch Regulierung und Standardisierung geeignete Richtlinien und Standards entwickelt.

Welche sind die Cybersecurity-Regulierungen?

Mit den vom UNECE World Forum for Harmonization of Vehicle Regulations verabschiedeten Regelwerke zu Cybersicherheit und Software-Updates für vernetzte Fahrzeuge wurden erstmalig einheitliche und verbindliche Vorgaben in diesem Bereich definiert. Während die UN Regulierung Nr. 155 (kurz UN R155) von Fahrzeugherstellern die Einführung eines zertifizierten Cyber Security Management System (CSMS) verlangt, schreibt die UN Regulierung Nr. 156 den Aufbau und Betrieb eines zertifizierten Software Update Management Systems (SUMS) vor. Mit diesen Regulierungen werden Maßnahmen eingefordert die sich im Wesentlichen auf die Domänen

- Fahrzeugentwicklung (Security-by-Design)
- Feldeinsatz (Monitoring von Cybersicherheitsvorfällen für die Fahrzeugflotte und Sichere Software-Updates Over-the-Air)

konzentrieren und darüber hinaus ein umfassendes Risk-Management (Management von Cyberrisiken über den gesamten Fahrzeuglebenszyklus) erfordern.

Die UN Regulierung Nr. 155 ist seit Januar 2021 in Kraft. Ab Juli 2022 wird diese in der Europäischen Union für alle neuen Typenzulassungen und ab Juli 2024 für alle ab diesem Zeitpunkt hergestellten Neufahrzeuge verpflichtend.

Welche Cybersecurity-relevanten Industry-Standards gibt es?

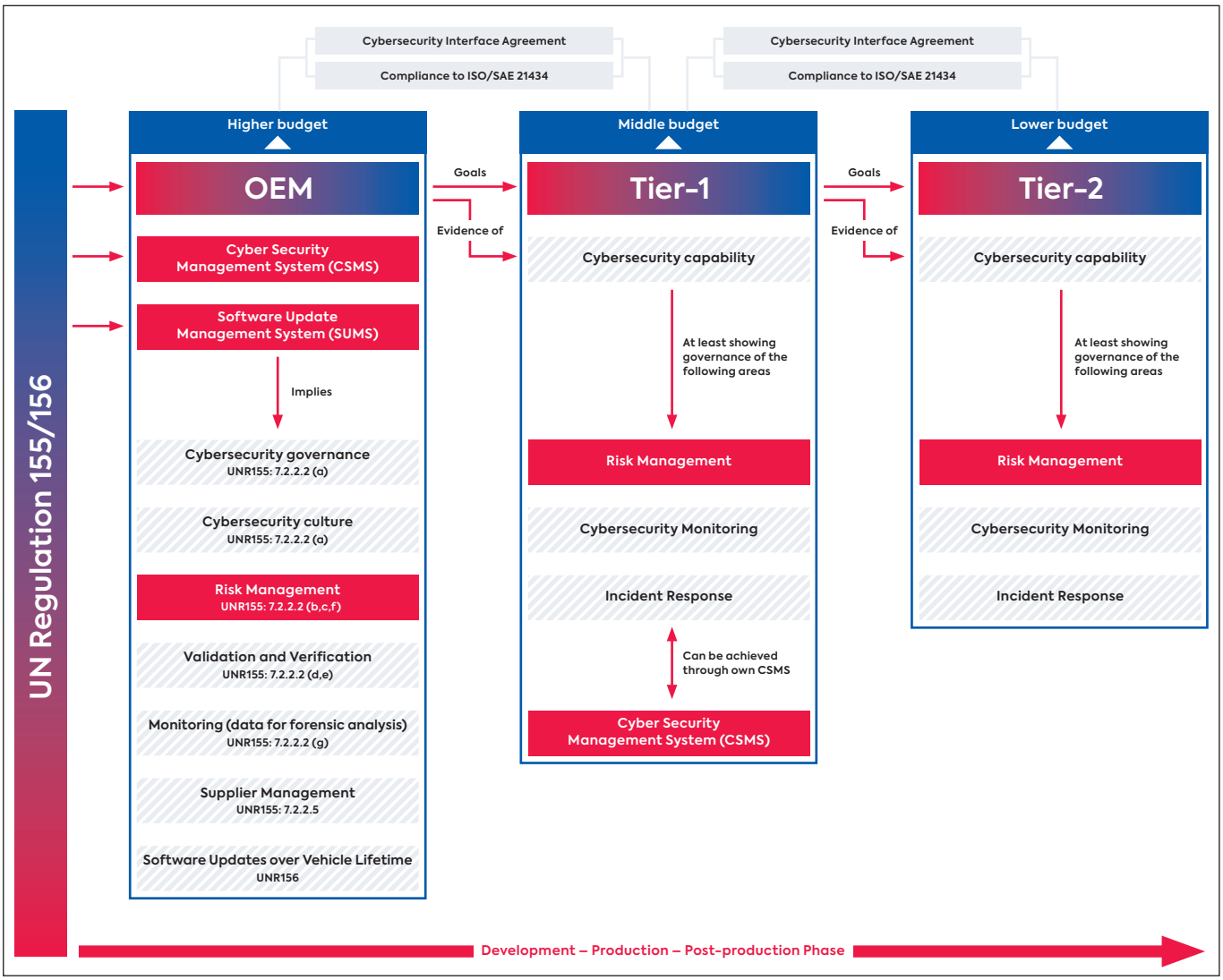
In Anlehnung an die Regulierung beschreibt die internationale Norm ISO/SAE 21434 „Road vehicles – Cybersecurity engineering" Prozesse und Abläufe für ein CSMS in der Automobilindustrie und deckt dabei grundsätzlich die Gebiete des Cybersicherheitsmanagement (z. B. Governance, Toolmanagement, Audits, Projektplanung, Konzeptionierung, Zulieferer, Zuständigkeiten, Monitoring, Produktion, Postproduktion und Decommissioning) und Risikomanagement (z. B. Assetsidentifikation, Bedrohungsanalyse, Risikobewertung und Risikobehebung) ab. Mit den „Road vehicles - Guidelines for auditing cybersecurity engineering" ergänzt die Norm ISO/PAS 5112:2022 die ISO/SAE 21434 hinsichtlich der Anforderungen für Audits. Die aus der Normierung noch zu erwartenden Anforderungen für die Prozesse und Abläufe der Software-Updates sind im Rahmen der ISO 24089 „Road vehicles – Software Update Engineering" definiert.

Wo kann secunet unterstützen?

Mit über 20 Jahren praktischer Erfahrung im Kontext Automotive Security, langjähriger aktiver Mitarbeit in relevanten Gremien und Expertise mit regulierten Märken unterstützt secunet OEMs und Zulieferer bei einer auf die speziellen Gegebenheiten der jeweiligen Unternehmen anpassten Umsetzung der Vorgaben und Normen mit folgenden Leistungen:

- Assessments bzw. Bestandsaufnahme und Gap-Analysen (Konformitätschecks)
- Aufbau Cyber Security Management System (CSMS) und Software Update Management System (SUMS)
- Audits
- Threat Analysis and Risk Assessment (TARA)
- Cybersecurity technische Konzepte (für die Entwicklung/R&D und die Produktion)
- TARA Training

Cybersecurity scope across production chain



Hier Kontakt aufnehmen
info@secunet.com

secunet

Two Pager_secunet_UNECE_DE_05/2023