Continental Commercial Vehicle Days

Cybersecurity-Regulierungen

Dr. Markus Tschersich | 8. September 2020

Bevorstehende Vorschriften und Normen

Regulierung soll Verkehrssicherheit gewährleisten

Cybersecurity

Software Update

Gesetzgeber:

UNECE Regulierungen

R.155 - UN Regulierung zur Cybersecurity

Branchenlösungen:

ISO-Normung

ISO/SAE 21434 Road vehicles – Cybersecurity Engineering

Bevorstehende UNECE-Regulierung zu Cybersecurity

Beschleunigung von Automotive-Cybersecurity in der Branche

Fahrzeug-Kategorien

Cybersecurity Management-Systeme

Fahrzeugtyp

Gefahren und Gegenmaß-nahmen

Einführung 06/2020

In Kraft 01/2021

Betroffene Märkte

UN-Regulierung zur Typengenehmigung bzgl. Cybersecurity

Anforderungen an CSMS und Fahrzeugtyp

Ziele

Organisations-struktur und Prozesse

Entwurf der Fahrzeugarchitek-tur und Um-setzung von Abhilfemaß-nahmen

UN-Regulierung zu Cybersecurity

Fahrzeughersteller benötigen ein
Cybersecurity Management-System (CSMS)
COC-Papiere (Certificate of Compliance)

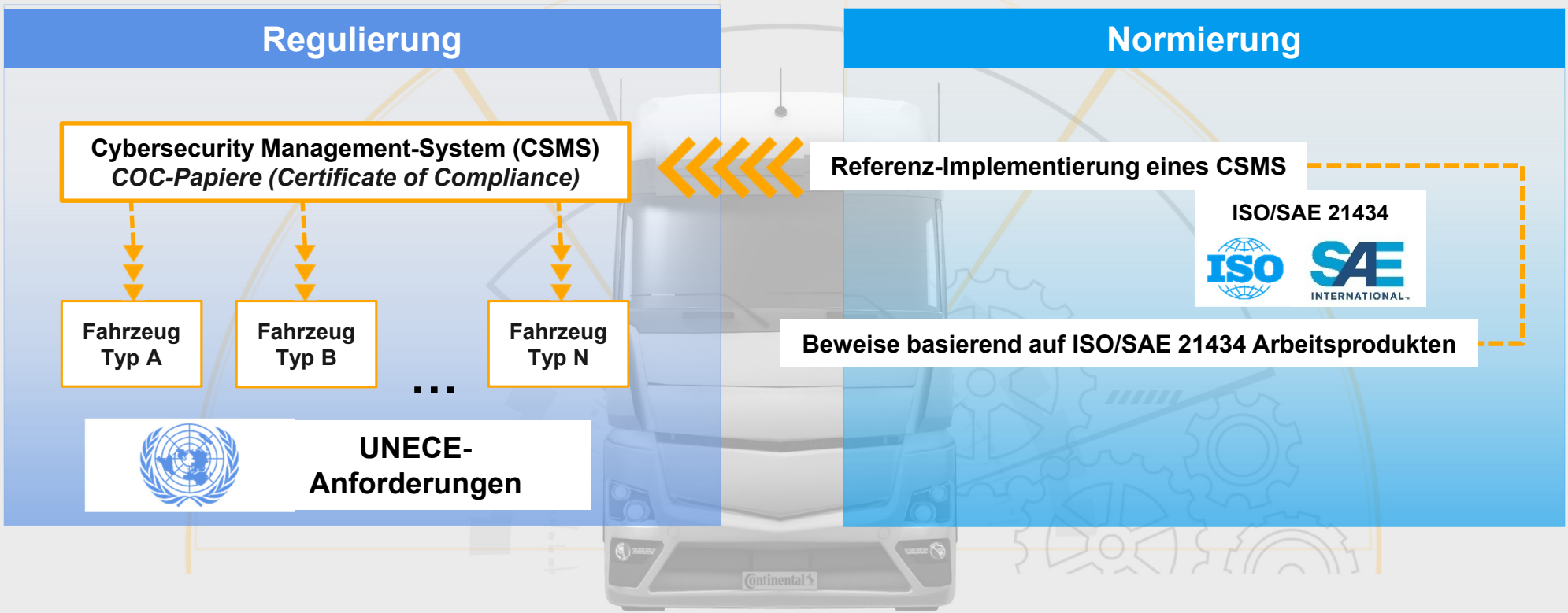
- Prozesse für Entwicklung, Produktion und Betrieb
- Risiko-Management
- Ausreichende Ressourcen und Personal
- ISO/SAE 21434 als CSMS-Referenz-Implementierung

Fahrzeug Typ A | **Fahrzeug Typ B** | ... | **Fahrzeug Typ N**

- Berücksichtigung von Cybersecurity für Fahrzeugtypen
- Umfassende Liste der zur berücksichtigenden Cybersecurity-Bedrohungen und Abhilfemaßnahmen

UNECE-Anforderungen an ein Cybersecurity Management-System

ISO/SAE 21434 kann Wertschöpfungskette für die Einhaltung vorbereiten

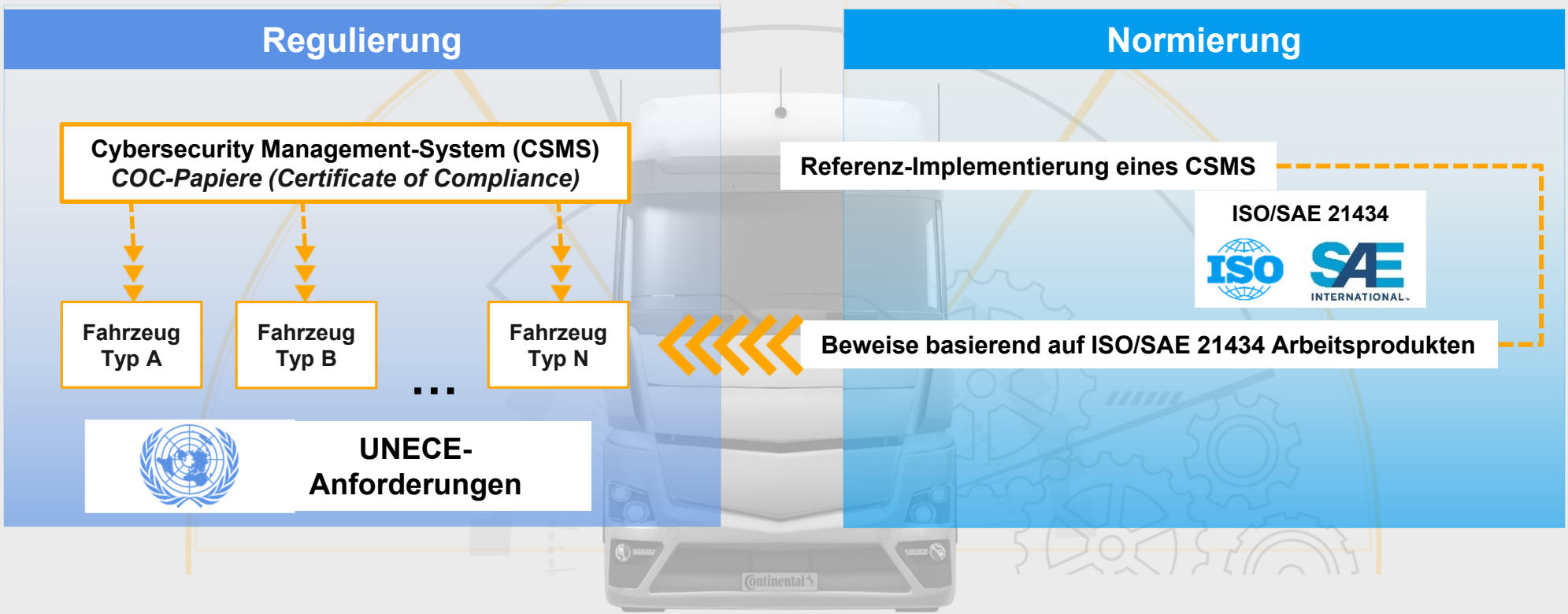


ISO/SAE 21434 Straßenfahrzeuge – Cybersecurity-Technik

Branchenlösungen für Cybersecurity-Herausforderungen

UNECE-Anforderungen an Cybersecurity für Typengenehmigung

ISO/SAE 21434 kann den Austausch der Dokumentation unterstützen



UNECE-Anforderungen an Cybersecurity für Typengenehmigung

Minimal erforderliche Gegenmaßnahmen für potenzielle Bedrohungen

Quellen

- ENISA Bericht „Cyber-security und Wider-standsfähigkeit von Smart Cars“
- UK DfT Cybersecurity-Prinzipien
- NHTSA Cybersecurity Richtlinie
- IPA „Ansätze für Fahrzeug-Informations-sicherheit“
- UNECE Cybersecurity Richtlinie (ITS/AD)

Bedrohungen

- Beschreibung der Bedrohungen
- Bsp. für Schwachstellen u. Angriffsmethode

Beispiel

Mann in der Mitte Angriff/Session Hijacking

entsprechend

Abhilfe für Bedrohungen (im Fzg)

- Fahrzeug-Kommunikationskanäle
- Update-Prozess
- Unbeabsichtigte menschliche Handlungen
- Externe Vernetzung
- Ziele/Motivation des Angriffs
- Datenverlust
- Physische Manipulation

Beispiel

Fahrzeug muss die **Authentizität einer Nachricht prüfen**, die es erhält.

Abhilfe für Bedrohungen (außerhalb Fzg)

- Back-End-Server
- Unbeabsichtigte menschliche Handlungen
- Physischer Verlust

Beispiel

Server muss **Nachrichten signieren,** die an Fahrzeuge gesendet werden.

Bevorstehende Vorschriften und Normierungen für Cybersecurity

Zeitstrahl

Continental
The Future in Motion