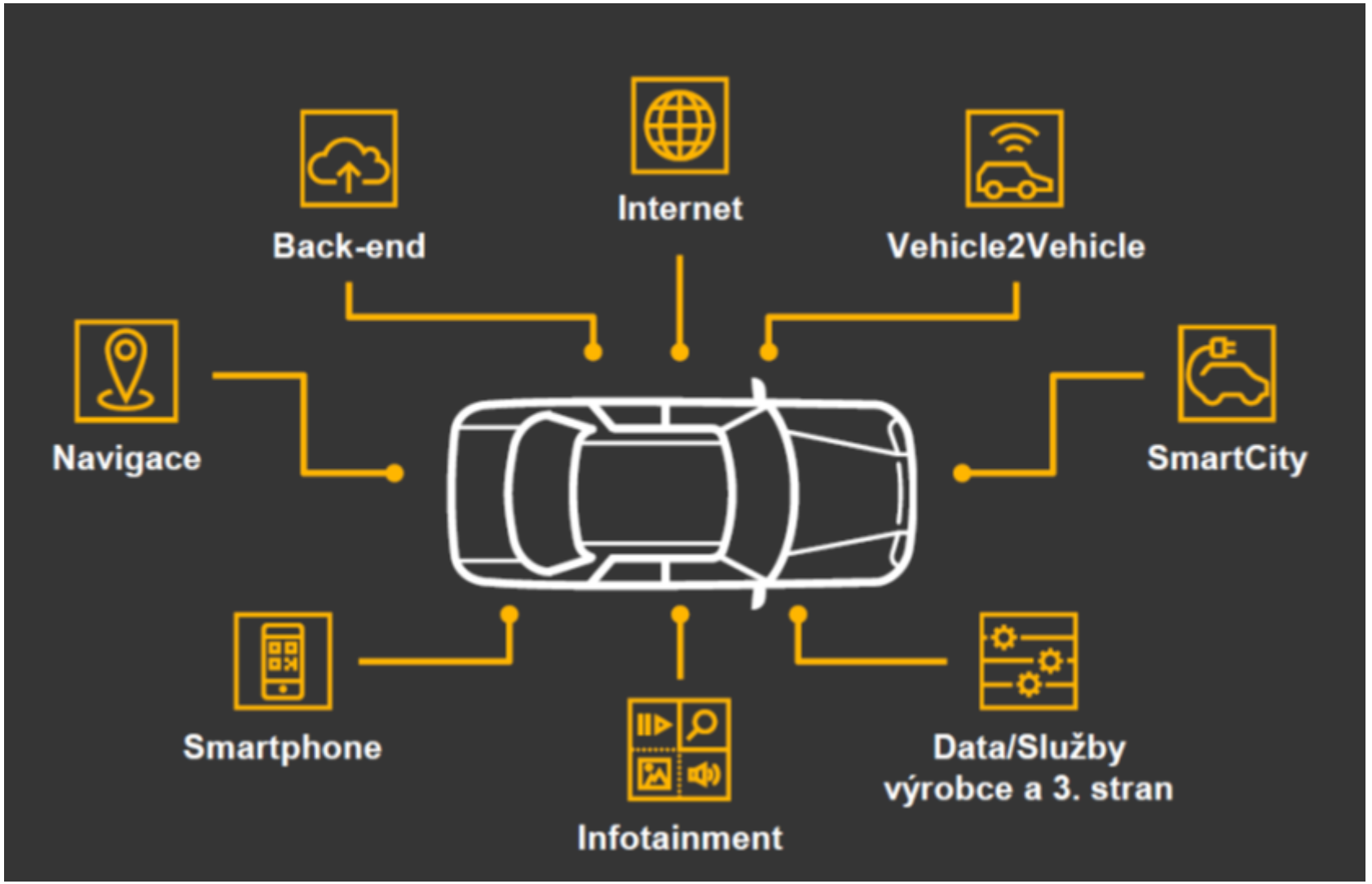
CERTIFICATION NEWS (CSMS, SUMS, ENX - VCSA)

Ing. Martin Drastich Ph.D., MBA

TÜVNORD

NEW STANDARD CSMS + SUMS



TÜVNORD

NEW STANDARD CSMS + SUMS

UNECE

- UNECE WP.29 Regulation on Cybersecurity and **Cyber Security Management Systems (CSMS)**
- UNECE WP.29 Regulation on Software Updates and **Software Updates Management Systems (SUMS)**

ISO

- ISO/SAE 21434 Road vehicles – **Cybersecurity engineering**
- ISO 24089 Road vehicles – **Software Update Engineering**

TÜVNORD

UN Reg. No 155 = CSMS

Only the original UN/ECE texts have legal effect under international public law. The status and date of entry into force of this Regulation should be checked in the latest version of the UN/ECE status document TRANS/WP.29/343, available at:
http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29fdocstts.html

UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387]

Date of entry into force: 22 January 2021

This document is meant purely as documentation tool. The authentic and legally binding texts are:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 and

— ECE/TRANS/WP.29/2020/97

TÜVNORD

UN REG. NO 155 = CSMS = ISO/SAE 21434

INTERNATIONAL STANDARD

ISO/SAE 21434

First edition
2021-08

Road vehicles — Cybersecurity engineering

Véhicules routiers — Ingénierie de la cybersécurité

TÜVNORD

UN REG. NO 155 = CSMS = ISO/SAE 21434

	Kapitola	Název kapitoly	RQ/RC/PM -ID	Požadavek/Doporučení/Povolení (RQ/RC/PM)	Pracovní výstup (WP)	Popis realizace	Odkazující dokumentace
rganizační řízení kybernetické bezpečnosti	5.4.1	Řízení kybernetické bezpečnosti	RQ-05-01	Organizace musí definovat politiku kybernetické bezpečnosti, která zahrnuje: a) uznání rizik kybernetické bezpečnosti silničních vozidel; a b) závazek výkonného vedení řídit odpovídající rizika kybernetické bezpečnosti.	[WP-05-01] Politika, pravidla a procesy kybernetické bezpečnosti vyplývající z požadavků 5.4.1 až 5.4.3		
			RQ-05-02	Organizace musí vytvořit a udržovat pravidla a procesy, aby: a) umožnila implementaci požadavků tohoto dokumentu; a b) podporovat provádění odpovídajících činností.	[WP-05-01] Politika, pravidla a procesy kybernetické bezpečnosti vyplývající z požadavků 5.4.1 až 5.4.3		•
			RQ-05-03	Organizace přidělí a sdělí odpovědnosti a odpovídající organizační pravomoci k dosažení a udržení kybernetické bezpečnosti.	[WP-05-01] Politika, pravidla a procesy kybernetické bezpečnosti vyplývající z požadavků 5.4.1 až 5.4.3		

TÜVNORD

UN REG. NO 155 = CSMS = ISO/SAE 21434

Organizační řízení kybernetické bezpečnosti
Řízení kybernetické bezpečnosti závislé na projektu
Distribuované aktivity v oblasti kybernetické bezpečnosti
Kontinuální aktivity v oblasti kybernetické bezpečnosti
Koncepční fáze
Fáze vývoje produktu
Povývojové fáze
Metody analýzy hrozeb a hodnocení rizik - TARA

TÜVNORD

UN Reg. No 156 = SUMS

Only the original UN/ECE texts have legal effect under international public law. The status and date of entry into force of this Regulation should be checked in the latest version of the UN/ECE status document TRANS/WP.29/343, available at:
http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29fdocstts.html

UN Regulation No 156 – Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]

Date of entry into force: 22 January 2021

This document is meant purely as documentation tool. The authentic and legally binding text is: ECE/TRANS/WP.29/2020/80.

CONTENTS

TÜVNORD

UN REG. NO 156 = SUMS = ISO/DIS 24089

DRAFT INTERNATIONAL STANDARD

ISO/DIS 24089

ISO/TC **22**/SC **32**

Secretariat: **JISC**

Voting begins on:
2022-01-11

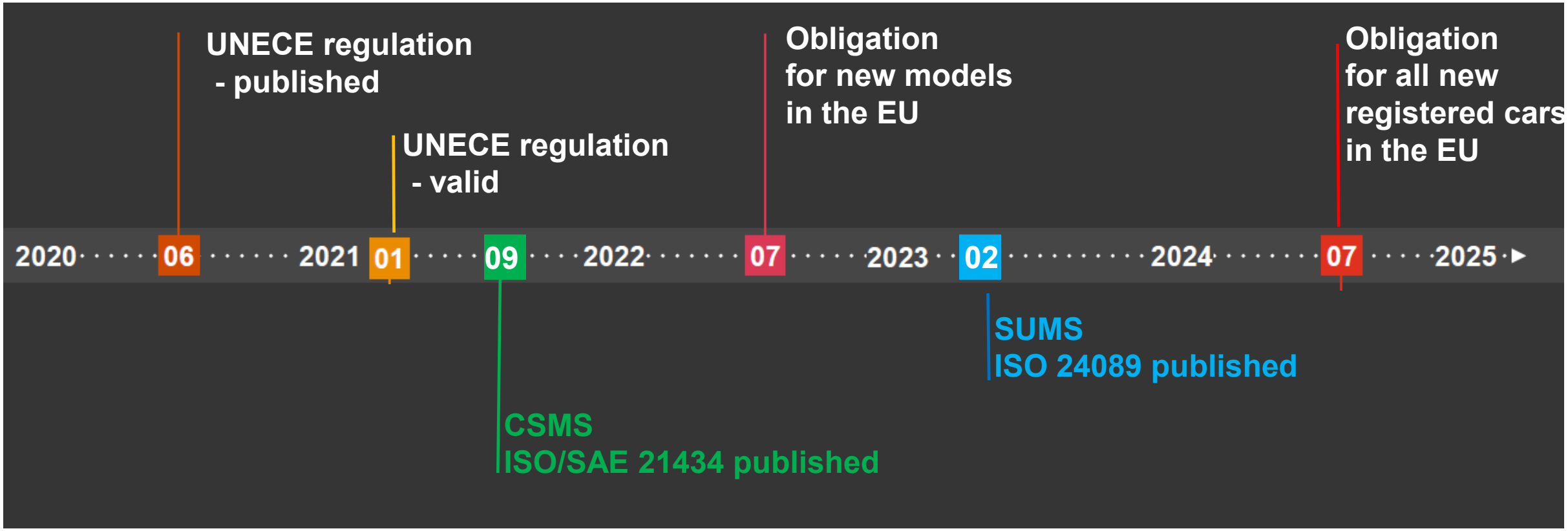
Voting terminates on:
2022-04-05

Road vehicles — Software update engineering

Véhicules routiers — Ingénierie de mise à jour du logiciel

TÜVNORD

TIMELINE OF UNECE REGULATIONS - CSMS + SUMS



TÜVNORD

HOW TO KEEP CAR/VEHICLE SAFE?

1 **Functional safety**

Technical defects in electronics

ISO 26262

2 **Cyber security car and SW update car**

Protection of electronic systems against external attacks.

UNECE – CSMS

ISO/SAE 21434

UNECE – SUMS

ISO 24089

3 **IT security manufacturer**

Protection of systems companies producing cars

ISO 27001, TISAX

TÜVNORD

VCSA - VEHICLE CYBERSECURITY AUDIT

Nr.	Subject	Result
1	Řízení kybernetické bezpečnosti	
2	Lidské zdroje – kultura kybernetické bezpečnosti	
3	Řízení rizik	
4	Interní hodnocení	
5	Fáze vývoje konceptu a produktu	
6	Fáze po vývoji	
7	Bezpečnost provozu	
8	Řízení incidentů	
9	Vztahy v dodavatelském řetězci	

VCSA - VEHICLE CYBERSECURITY AUDIT

Nr.	Subject	Result
1.1	Jsou zásady kybernetické bezpečnosti spravovány?	
1.2	Jsou procesy kybernetické bezpečnosti související s vozidly řízeny v rámci organizace?	
1.3	Jsou zavedeny procesy pro organizaci odpovědností v oblasti kybernetické bezpečnosti?	
1.4	Jsou zavedeny procesy pro řízení kybernetické bezpečnosti závislé na projektu?	
2.1	Je kultura kybernetické bezpečnosti a povědomí o kybernetické bezpečnosti zavedena, implementována a udržována?	
3.1	Jsou zavedeny procesy a metody pro provádění analýzy hrozeb a hodnocení rizik (TARA) k určení rizik kybernetické bezpečnosti pro položku/komponenty v průběhu životního cyklu vozidla?	
3.2	Jsou zavedeny procesy pro řešení rizik kybernetické bezpečnosti u položky v průběhu životního cyklu vozidla?	
3.3	Jsou zavedeny procesy pro transparentní komunikaci rizik kybernetické bezpečnosti?	
4.1	Jsou zavedeny procesy pro kontrolu účinnosti CSMS v rámci organizace?	

TÜVNORD

VCSA - VEHICLE CYBERSECURITY AUDIT

Nr.	Subject	Result
5.1	Jsou zavedeny procesy k definování položky a specifikaci požadavků na kybernetickou bezpečnost?	
5.2	Jsou zavedeny procesy pro ověření plnění požadavků na kybernetickou bezpečnost na komponentách ve fázi vývoje?	
5.3	Jsou zavedeny procesy, které ověřují cíl a požadavky kybernetické bezpečnosti na úrovni položek během vývojové fáze?	
6.1	Jsou zavedeny procesy pro uvolnění položky nebo součásti pro fáze po vývoji?	
6.2	Jsou zavedeny procesy pro uplatňování požadavků na kybernetickou bezpečnost během výrobní fáze?	
7.1	Jsou zavedeny procesy pro sledování informací o kybernetické bezpečnosti a pro identifikaci událostí kybernetické bezpečnosti ze sledovaných informací?	
7.2	Jsou zavedeny procesy pro vyhodnocování událostí kybernetické bezpečnosti?	
7.3	Jsou zavedeny procesy pro identifikaci a analýzu zranitelností?	
7.4	Jsou zavedeny procesy pro správu identifikovaných zranitelností?	
7.5	Jsou zavedeny procesy pro aktualizace položek nebo komponent?	
8.1	Je zaveden proces reakce na kybernetické bezpečnostní incidenty?	
8.2	Je zaveden proces ověřování účinnosti a přiměřenosti reakce na kybernetický bezpečnostní incident?	
9.1	Jsou zavedeny procesy pro řízení závislostí mezi kontrolovanou organizací a jejími relevantními dodavateli VCS?	

TÜVNORD

DĚKUJI ZA POZORNOST!

Ing. Martin Drastich Ph.D., MBA
604 857 854
Drastich@tuev-nord.cz

TÜVNORD