

Sicherheitsregelung Fahrzeug (SIRF)

Metodika pro splnění požadavků CSM-RA a EN 50126

Jakub Habásko, Siemens Mobility

Obsah

- Page 3: Důvod vzniku SIRF
- Page 4 - 6: Legislativa a pojmy
- Page 7: Požadavky na organizaci
- Page 8: Důkaz bezpečnosti vozidla
- Page 9: Vztah mezi SIRF a CRM-RA
- Page 10 - 11: Bezpečnostní deník
- Page 12: Klasifikace nebezpečí
- Page 13: Volba způsobu dokazování bezpečnosti
- Page 14: Explicitní posouzení rizik

SIRF - Sicherheitsregelung Fahrzeug – Důvod vzniku

- Reakce na nové technologie a komplexnost technologií
- Cílem bylo vyvinout **praktickou metodiku pro funkčně orientovanou bezpečnost železničních vozidel**
- Metodiky **Sicherheitsregelung Fahrzeug (SIRF)** stanovují pravidla pro proces, rozsah posuzování a prokazování bezpečnosti
- Zohledněné normy: EN 50126, 50128, 50129 und IEC 61508

Legislativa a pojmy – a) Úrovně legislativních požadavků

Legislativa	Nejčastěji aplikované dražní bezpečnostně relevantní dokumenty	Obsah
Národní: DE, UK zákony, ..	Allgemeines Eisenbahngesetz (AEG)	Dražní zákon (DE)
	Sicherheitsrichtlinie Fahrzeug (SIRF)	Směrnice bezpečnosti dražních vozidel (DE)
	Zákon o drahách č. 266/1994 Sb.	Dražní zákon (CZ)
	The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (as amended) (ROGS)	Směrnice drážní bezpečnosti (UK)
Oblastní: EU směrnice,..	Common Safety Methods (CSM) ((EU) Nr. 402/2013 CSM RA)	Proces řízení rizik, společné bezpečnostní metody
	Technical Specifications for Interoperability (TSI)	Technical and operational standards including technical safety requirements
Normy: IEC, EN, UIC, III,...	EN 50126-1:2017+A1:2024 (RAMS)	Bezporuchovost, Spolehlivost, Udržovatelnost a Bezpečnost
	EN 50129:2018+AC:2019	Bezpečnostně relevantní el. systémy pro zabezpečovací zařízení
	EN 50716:2023	Bezpečnostně relevantní SW
Interní procesy organizace (Nařízení a směrnice)	-	-

Legislativa a pojmy – b) Role pro posouzení splnění požadavků 1

Důležité role a jejich označení v EU:

NSA - National Safety Authority
– vnitrostátní bezpečnostní orgán (EBA, DÚ, apod..)

AsBo - Assessment Body (*Subjekt pro posuzování*)
– posouzení shody s **CSM**

DeBo - Designated Body – posouzení shody se specifickými národními požadavky

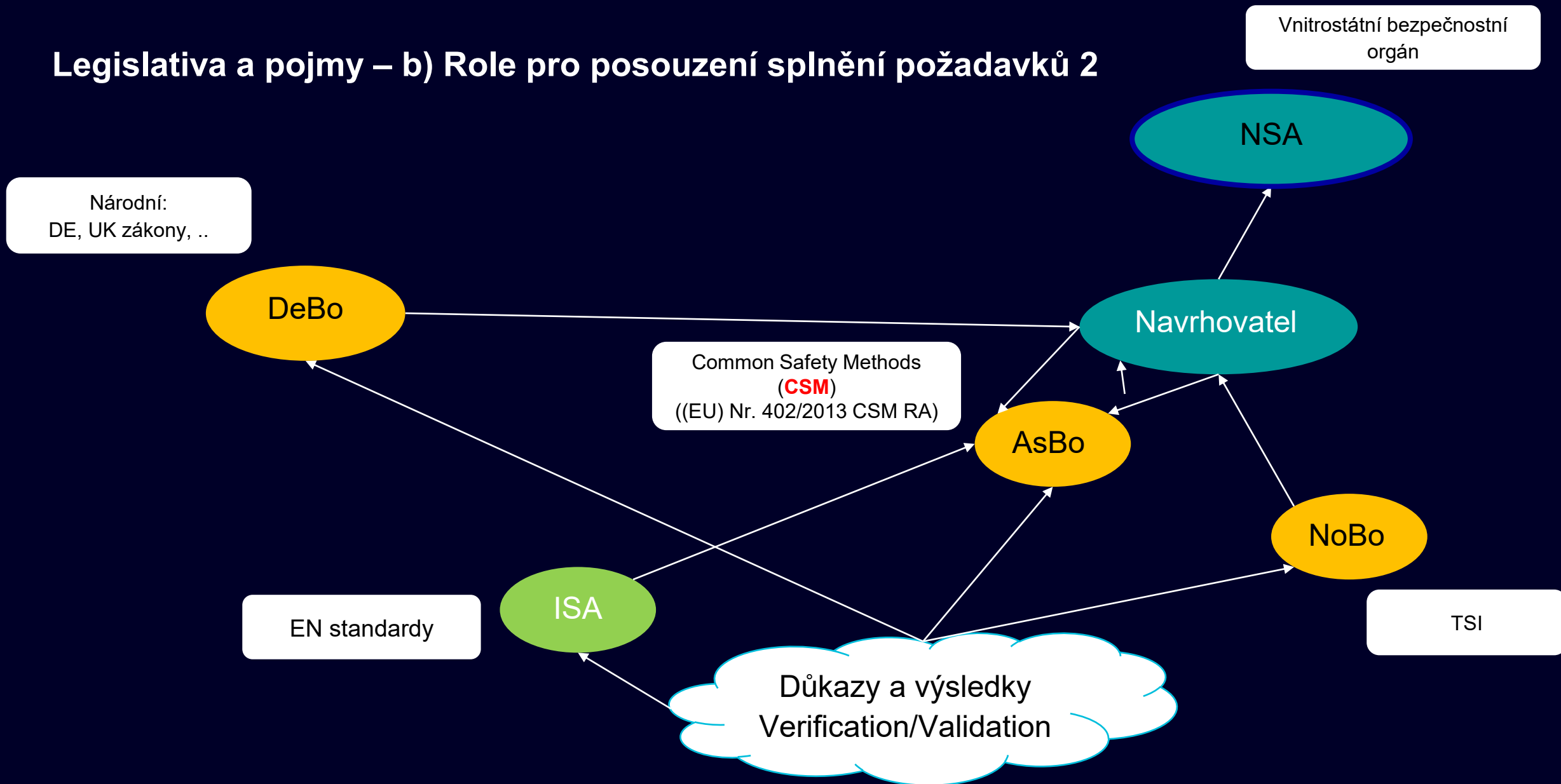
NoBo - Notified Body – posouzení shody s TSI

Navrhovatel (Proposer)

- Navrhuje změnu drážního systému dle CSM (tj. jakákoliv změna včetně zavedení nového vlaku či subsystému, výrobce nebo provozovatel)

ISA - Nezávislý hodnotitel bezpečnosti (v souladu s EN standardy)

Legislativa a pojmy – b) Role pro posouzení splnění požadavků 2



SIRF - Sicherheitsregelung Fahrzeug – Požadavky na organizaci

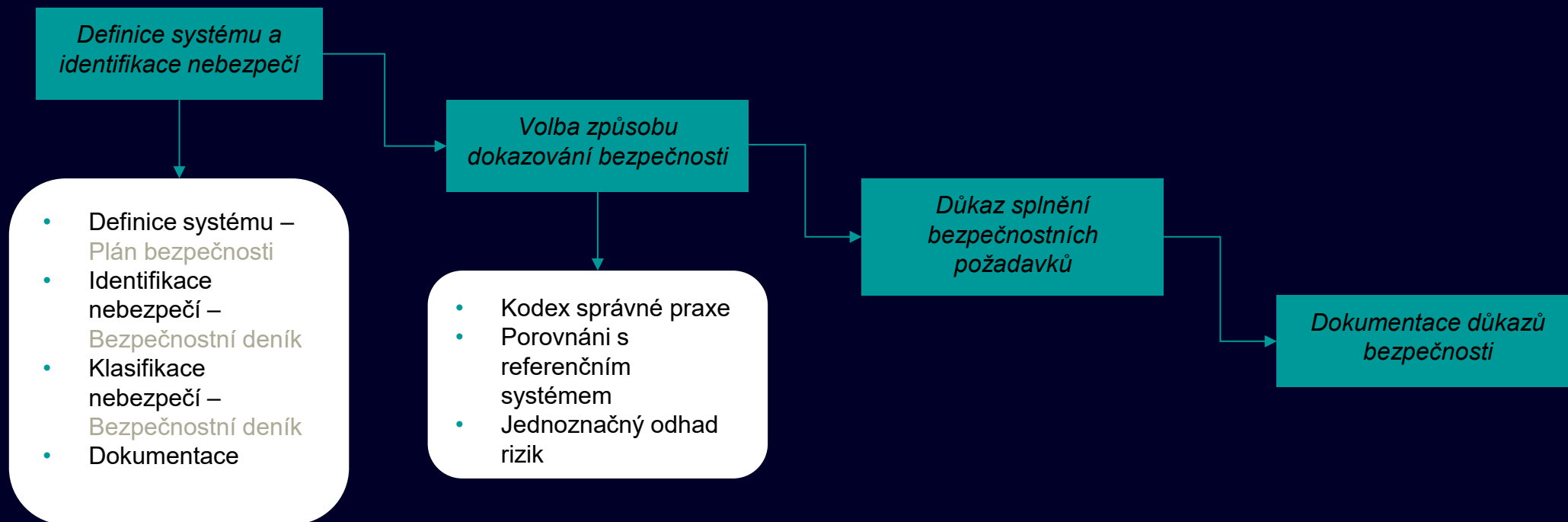
Požadavky na bezpečnostní organizace:

Definice pozic v organizaci (Role členů) – odpovědnosti, jmenování, kompetence, nezávislosti a vztahy v organizaci

Role SAFETY MANAGERA (SM):

- Několikaleté praktické zkušenosti v managementu bezpečnosti;
- Znalost SIRF a CSM-RA
- Znalost norem pro management bezpečnosti

SIRF - Sicherheitsregelung Fahrzeug – Důkaz bezpečnosti vozidla ve 4 krocích

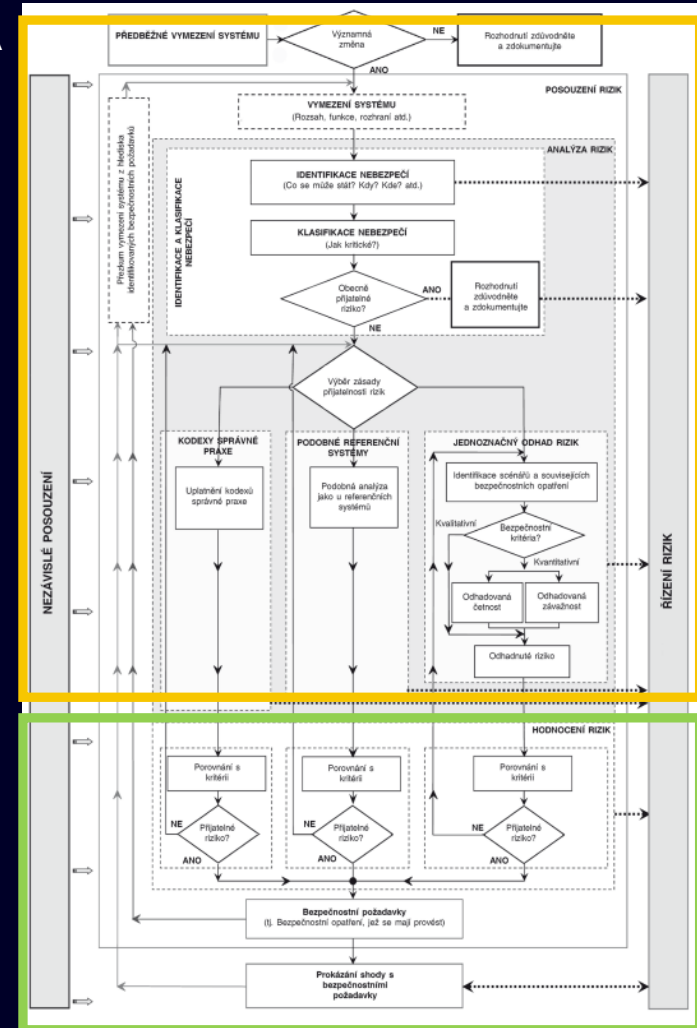


SIRF - Sicherheitsregelung Fahrzeug – Vztah mezi SIRF a CSM-RA

SIRF



CSM-RA



SIRF, CSM-RA a EN 50126 jsou vzájemně harmonizovány.

SIRF - Sicherheitsregelung Fahrzeug – Bezpečnostní deník – Tesip - 1

2	A	B	C	D	E	F	G	H	I	J	K	L
1	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
2	TESIP - Fu											
3	Eisenbahnfahrzeugfunktionen						Gefährdungsermittlung					
4	Hauptfunktion	Teilfunktion	lfd. Nr.	Funktion	Erläuterung der Funktion	Beispiele: Typische Themen / ELEMENTE	Betriebs- und Umgebungsbedingungen (für Hauptfunktion Z: Sicherheitsanforderungen und deren Bedingungen)	Sichere Gewährleistung von...	Gefährdung ist gegeben, wenn....	Nr. Teilgefährdung	Maßgebliche Teilgefährdung	S _A
55	E	B	1	Spurführung gewährleisten	Infrastrukturparametern, unter Ausnutzung aller Bauteil- und Einbautoleranzen sowie im Abnutzungszustand der Bauteile bzw. der Infrastruktur, unter allen zulässigen Betriebsbedingungen, die Spurführung sicher gewährleisten und die beim Betrieb der Fahrzeuge entstehenden Kräfte sicher aufnehmen und übertragen. Die zulässigen Grenzwerte der Infrastruktur sind sicher einzuhalten.	Geometrie, Kräfte, Beschleunigungen		Spurführung innerhalb spezifizierter Grenzen	NICHT-Zusammenwirken der Geometrien von Rad und Schiene	3a	Spurführung versagt, Entgleisung	5,0
56	E	B	2	Spurführung gewährleisten	---	Radsatz, -welle, lager, etc.		---	---	3a	Spurführung versagt, Entgleisung	5,0
57	E	C	1	Laufgüte gewährleisten	---	Laufgüte unter dem Aspekt der Fahrsicherheit, Überwachung der Laufgüte		der Einhaltung der zulässigen Beschleunigungs-Grenzwerte.	NICHT-Einhaltung der zulässigen Beschleunigungs-Grenzwerte.	10I	Gefährdung von Insassen durch zu hohe Beschleunigungen während der Fahrt, (z.B. Rucke, im Innenraum herumfliegende Teile)	5,0
58	E	C	2	Laufgüte gewährleisten	Spurkranzschmierung	Düse dejustiert durch Steinschlag, Ansteuerung, Vorratsbehälter		keine Gefährdung	keine Gefährdung	0	N.A.	0,0
59	F. Fahren											

SIRF - Sicherheitsregelung Fahrzeug – Bezpečnostní deník – Tesip - 2

(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)	(26)	(27)	(28)	(29)
- Funktionsliste																	
Gefährdungseinstufung														Festlegung des Risikoakzeptanzprinzips		Informativ	
S _A	Schaden - Anzahl	S _V	Schaden - Verletzungsgrad	W	Eintrittswahrscheinlichkeit	E	Expositionsdauer	V	Vermeidung	I	Sicherheitsanforderungsstufe (SAS)	für Gefährdungseinstufung relevante Bemerkung	Quellen weiterer Sicherheitsanforderungen aus Regelwerken für die Funktionen	Referenzen zu weiteren Informationen bezgl. der Risikobewertung (z.B. Gefährdungsbäumen, Szenarien)	COP = Anwendung von Regelwerk ERE = explizite Risikoabschätzung SRS = Vergleich mit ähnlichen Systemen (Referenzsystemen) BAR = Broadly Acceptable Risk	Referenzen zur Begründung der Wahl des Risikoakzeptanzprinzips	mögliche Nachweiswege z.B. Gefährdungsbäume
5,0	Mehrere (1 < x ≤ 10 Personen)	9,0	Tote	1,7	Mittel	1,3	Lang	1,0	Nicht möglich	99,45	3	zu W: Funktionsversagen führt nicht zwangsläufig zu Toten			COP		---
5,0	Mehrere (1 < x ≤ 10 Personen)	9,0	Tote	1,7	Mittel	1,3	Lang	1,0	Nicht möglich	99,45	3	zu W: Funktionsversagen führt nicht zwangsläufig zu Toten			COP		---
5,0	Mehrere (1 < x ≤ 10 Personen)	2,0	Leichtverletzte (LV)	1,7	Mittel	1,3	Lang	1,0	Nicht möglich	22,10	1	zu W: Funktionsversagen führt nicht zwangsläufig zu Leichtverletzten		vgl. hierzu Funktionen in Abschnitt Z zu TSI 4.2.3.4.2	COP		---
0,0	---	0,0	---	0,0	---	0,0	---	0,0	---	0,00	0	Funktion ist nicht relevant für den Fahrtechnischennachweis, daher ist diese Funktion nicht eingestuft.			---		---

SIRF - Sicherheitsregelung Fahrzeug – Bezpečnostní deník – Klasifikace nebezpečí

Parametry pro klasifikaci nebezpečí:

- Škoda (S)
- Pravděpodobnost výskytu (W)
- Doba expozice (E)
- Možnost zamezení (V)

Einstufungsindikator I	Sicherheitsanforderungsstufe SAS
$I < 21$	0
$21 \leq I < 36$	1
$36 \leq I < 72$	2
$72 \leq I < 122$	3
$122 \leq I < 281$	4

Schaden (S) = $S_A \times S_V$	
Anzahl S_A	
Einer	1 Person
Mehrere	$1 < x \leq 10$ Personen
Viele	> 10 Personen

Verletzungsgrad S_V	
Leichtverletzte (LV)	Gefährdung führt zu einem Unfall mit leichten Verletzungen (Prellungen, Frakturen) unterhalb von 2 Tagen Krankenhausaufenthalt und ohne irreversible Folgeschäden.
Schwerverletzte (SV)	Gefährdung führt zu einem Unfall mit mindestens 2 Tagen Krankenhausaufenthalt und/oder irreversible Folgeschäden.
Tote	Gefährdung führt zu Unfall mit tödlichen Verletzungen (Tod erfolgt innerhalb von 30 Tagen nach dem Unfall) oder zur sofortigen Todesfolge.

Vermeidung (V)	
Nicht möglich	Die betroffene Person hat durch eigenes Handeln keine Möglichkeit, den Schaden zu vermeiden
Möglich	Die betroffene Person hat durch eigenes Handeln Möglichkeiten, den Schaden zu vermindern oder zu vermeiden.

Eintrittswahrscheinlichkeit (W)	
Niedrig	Die Eintrittswahrscheinlichkeit ist niedrig, wenn das Schadensausmaß nach Versagen der Funktion nahezu ausgeschlossen ist.
Mittel	Die Eintrittswahrscheinlichkeit ist mittel, wenn das Schadensausmaß nach Versagen der Funktion weder nahezu ausgeschlossen ist, noch nahezu zwangsläufig eintritt.
Hoch	Die Eintrittswahrscheinlichkeit ist hoch, wenn das Schadensausmaß nach Versagen der Funktion nahezu zwangsläufig eintritt.

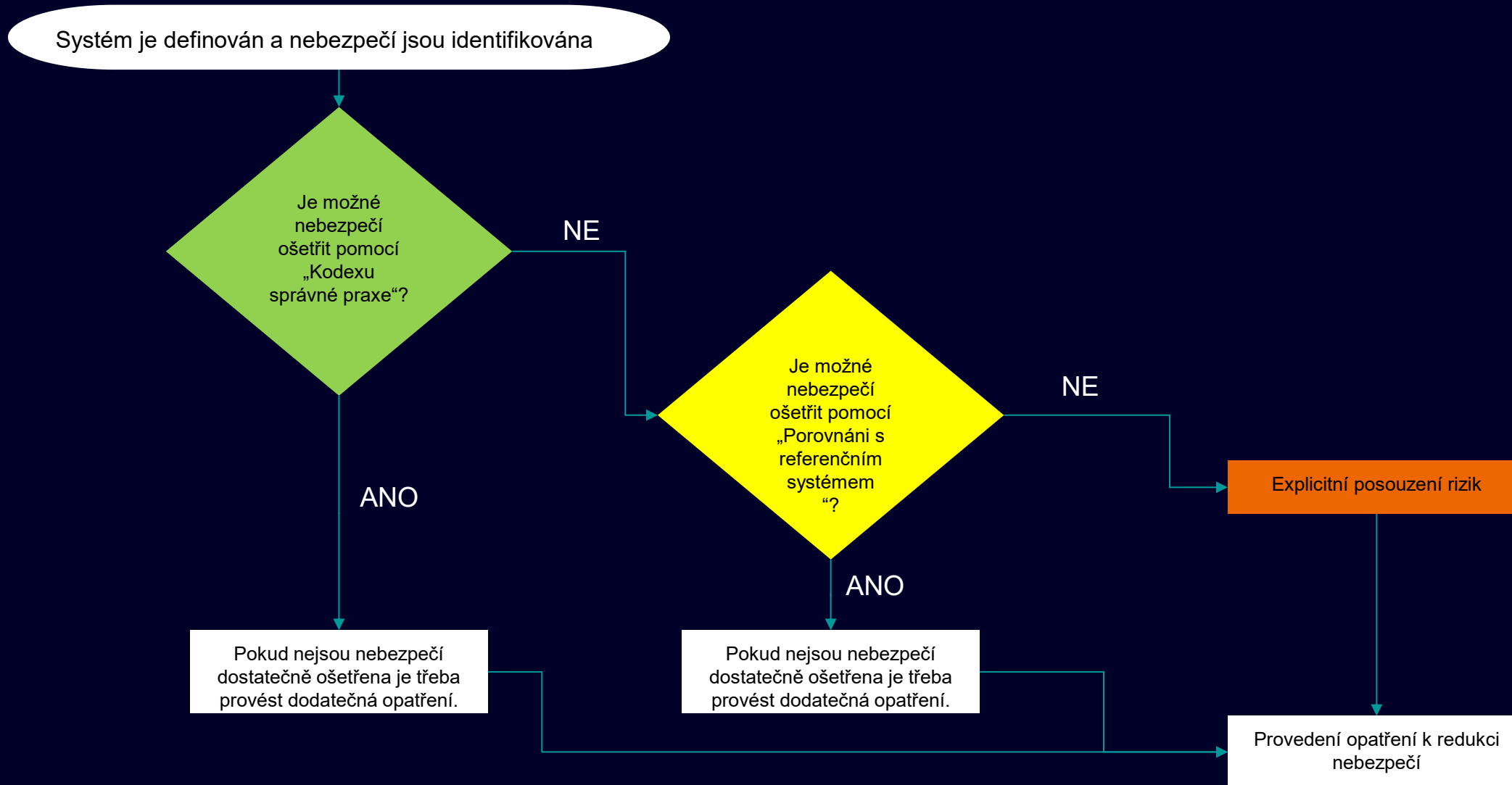
Expositionsdauer (E)	
Kurz	Die Expositionsdauer ist kurz, wenn diese klein im Vergleich zur gesamten Aufenthaltszeitdauer im Gefahrenbereich ist. $t_{exp} \ll t_{auf}$
Lang	Die Expositionsdauer ist lang, wenn die betroffene Person während der überwiegenden Aufenthaltsdauer im Gefahrenbereich der möglichen Gefährdung ausgesetzt ist. $t_{exp} \approx t_{auf}$

Parameter für den Schaden (S) = S _A x S _V			
Anzahl S _A		Verletzungsgrad S _V	
einer	3	LV	2
mehrere	5	SV	4
viele	8	Tote	9
Parameter für die Eintrittswahrscheinlichkeit (W)			
niedrig	1		
mittel	1,7		
hoch	3		
Parameter für die Expositionsdauer (E)			
kurz	1		
lang	1,3		
Parameter für die Vermeidung (V)			
nicht möglich	1		
möglich	1,7		

Ermittlung der Sicherheitsanforderungsstufe (SAS)
Die Sicherheitsanforderungsstufe (SAS) wird mit nachfolgender Berechnungsmethode ermittelt.
Aus den o. a. Parametern berechnet sich der Einstufungsindikator I anhand folgender Formel:

$$I = \frac{(S * W * E)}{V}$$

SIRF - Sicherheitsregelung Fahrzeug – Volba způsobu dokazování bezpečnosti



SIRF - Sicherheitsregelung Fahrzeug – Jednoznačný odhad rizik

- **Strom nebezpečí** (Gefährdungsbaum) jako metoda pro znázornění rozdělení architektury a rozdělení bezpečnostně-technické odpovědnosti
- SIRF definuje metodiky pro vytváření stromu nebezpečí např.

	Kombination nicht zulässig, da (a) oder (b) nicht erfüllt ist.
	Kombination zulässig, da (a), (b), (c) und (d) erfüllt sind.
	Kombination zulässig, sofern (e) beachtet wird.
Erläuterung eines Zahlenbeispiels	
2 2	2 2 steht für die SAS-Einstufung der jeweiligen kombinierten Elemente. Hier 2 Elemente mit der jeweiligen SAS-Einstufung 2

Tabelle 15: Kombinationsmöglichkeiten bei UND-Verknüpfung von 2 Elementen

SAS=		SAS=	
1		2	
0 0	0 1	0 0	0 1
1 0	1 1	1 0	1 1
		2 0	2 1

- Dále definuje požadavky na Hardware a Software např.

Tabelle 8: Übertragung der SAS in Kategorie Software Normen für Fahrzeuge

SIRF		DIN EN 50657	DIN EN 50128
SAS 0	→	BI	SSAS 0
SAS 1	→	SIL 1	SSAS 1
SAS 2	→	SIL 2	SSAS 2
SAS 3	→	SIL 3	SSAS 3
SAS 4	→	SIL 4	SSAS 4

SIRF - Sicherheitsregelung Fahrzeug – Zdroje

- EISENBAHN-BUNDESAMT: *Sicherheitsregelung Fahrzeug Überarbeitete Fassung 2019*. PDF. Online. Dostupné z: https://www.eba.bund.de/SharedDocs/Downloads/DE/Fahrzeuge/Fahrzeugtechnik/Funktionale_Sicherheit/3_1_SIRF_Sicherheitsregelung_Fahrzeuge.pdf?__blob=publicationFile&v=2 [citováno 2026-01-20]
- EUROPEAN UNION - AGENCY FOR RAILWAYS: *Common Safety Method for Risk Evaluation & Assessment* PDF. Online. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32013R0402> [citováno 2026-01-20]

Děkuji za pozornost

Contact

Published by Siemens Mobility s.r.o.

Jakub Habásko

Safety manager

SMO RS EEC EN EH CZ PRO ASR

Siemensova 2715/1

155 00 Praha

Czech republic

E-mail Jakub.Habasko@siemens.com