Česká společnost pro jakost, Novotného lávka 5, 110 00 Praha 1, www.csq.cz

Příklady postupů prokazování bezpečnosti a spolehlivosti železniční techniky

Materiály z **96. semináře** Odborného centra **Spolehlivost**
konaného dne **10. 2. 2026** v **Praze**

Odborný garant semináře:
Ing. Jan Kamenický, Ph.D. – Technická univerzita v Liberci

Obsah

Dopady a omezení CENELEC architektur na důkaz bezpečnosti

Ing. Luboš Piterka
RAMS Manager (Siemens Mobility, s.r.o.)
lubos.piterka@siemens.com

1 Úvod:

V současné době pozorujeme zvyšující se nároky na jednoduchá řešení komplexních problémů zabezpečovací techniky. Jsou vyžadována řešení použitelná obdobně pro distribuované i centralizované instalace, s velkou mírou škálovatelnosti a modularity. Systémy musí být schopny poskytovat pokročilou diagnostiku s možností vzdáleného přístupu podléhající stále se zvyšujícím nárokům na kybernetickou bezpečnost.

Základní typy CENELEC architektur:

V posledních desetiletích se nejrozšířenější typy použitelných architektur nijak významně nezměnily.

Norma EN50129:2018 v tabulce E.4 připouští pro SIL3/4 následující architektonická řešení:

- jednokanálová struktura s inherentní bezpečností při poruše
- jednokanálová struktura s reaktivní bezpečností při poruše
- vícekanálová struktura s bezpečnou komparací (redundantní nebo diverzní)

Inherentní bezpečnosti lze dosáhnout pouze pro velmi jednoduché části návrhu (typicky zdroje, ochrany, izolační bariéry apod.), přičemž je zde jasné omezení taxativním výčtem komponent v EN50129:2018 příloze C.

2 Aktuální stav problematiky:

Současná řešení vyžadující komplexní elektronické struktury – průmyslová PLC, komunikační procesory, hradlová pole (EN50129:2018 příloha F) však neumožňují prokázání inherentních bezpečných vlastností, a tak dvě aktuálně nejrozšířenější řešení jsou vícekanálové struktury a jednokanálová struktura s nezávislým monitoringem.

Jednokanálová řešení jsou často preferována systémovými architekty z důvodů primárně nesouvisející s funkční bezpečností. Tyto systémy jsou při srovnatelném HW výkonnější než vícekanálové systémy díky absenci výměny vstupních a výstupních dat v rámci pracovního cyklu. Výpočetní jednotka se tak může větší poměrnou částí aplikačního cyklu věnovat sběru dat a jejich zpracování, komunikaci s periferiemi, či nadřazeným systémem.

Vícekanálová řešení jsou naopak preferována RAMS manažery z důvodu absence závislosti důkazu pro SDT (doba detekce + doba negace – EN50126-2:2017) na externích rozhraních a nadřazených systémech. Jelikož reaktivní systémy mohou generovat potenciálně nebezpečný výstup až po dobu SDT, ostatní systémy musí být na takovou situaci připraveny a navrženy.

V případě vícekanálových řešení je obdobný důkaz postaven na výpočtu závisejícím na intenzitách poruch komponent použitých v návrhu v kombinaci s alokovanou TFFR, a tudíž umožňuje týmu vývojářů mít nad ním kompletní kontrolu. Vícekanálové diverzní architektury jsou nákladnější na vývoj,

výrobu i udržování. Tento přístup je obtížně realizovatelný u komplexních výpočetních jednotek, nicméně je naopak velmi efektivní proti poruchám se společnou příčinou, např. u elektrických ochran.

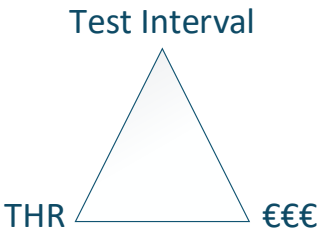
3 Požadavky od zákazníků a regulátorů:

V momentě, kdy má být zařízení použitelné jako generický produkt podle EN50126-1:2017 je nezbytné udržovat jeho provozní rozsah co nejširší s pouze omezenými architektonickými zásahy (rozsah TFFR funkcí, maximální test intervaly). Byť již existuje velká řada zemí používající CENELEC standardy, soulad s nimi nezaručuje automaticky použitelnost zařízení v národních aplikacích.

Pokud bychom měly sumarizovat hlavní výzvy vyplývající z návrhu generické platformy pro velké množství rozličných trhů, mohou nás překvapit následující požadavky:

- zvyšující se SIL již zavedených funkcí
- nová, rozmanitější rozhraní vstupující do již jinak identifikovaných hazardů
- tlak na prodlužování testovacích intervalů a preventivní údržby s dopadem na funkční bezpečnost
- vyžadovaná modularita a škálovatelnost (zjednodušení navazujících integrací a projektování)
- snižování nákladů na minimální, příp. typickou instalaci

Jak je zřejmé většina těchto požadavků je vzájemně v rozporu a je tedy třeba vždy najít nějaký kompromis. Tento nekonečný souboj lze reprezentovat „zákaznickým trojúhelníkem“, kdy lze splnit alespoň dva požadavky, ale nikdy všechny tři. Zákazník požaduje nízké THR a dlouhé intervaly mezi testy – řešení bude komplexní a drahé, atd.



4 Závěr:

Návrh architektury, která plní požadavky na funkce s vysokým SIL, neomezuje zákazníka častou preventivní údržbou s dopadem na bezpečnost provozu, není příliš komplikovaná na implementování nových funkcionalit a její použitá technika není extrémně nákladná, je komplexním tématem, které nemá jednoznačné řešení a bude vývojáře a architekty zatěžovat i v nadcházejících letech. Situaci nijak neulehčují mezinárodní rozdíly v analýzách rizik, jež jsou stále často pevně spjaty s historicky používanou technikou a odlišnými přístupy.

Reference:

(1) EN50126-1:2017 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS process;

(2) EN50126-2:2017 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety;

(3) EN50129:2018 Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling; English version

Metodologický přístup k demonstraci funkční bezpečnosti systému CBTC (Communication Based Train Control)

Ing. Luboš Janhuba, Ph.D.
RAMS Manager (Siemens Mobility, s.r.o.)
lubos.janhuba@siemens.com

1 Úvod

Soudobá městská kolejová doprava, zahrnující příměstské železniční linky, metro a tramvajovou dopravu, v posledních dvaceti letech zaznamenává výrazný nárůst počtu cestujících. Tento trend má za přímý důsledek rostoucí nároky na efektivitu, spolehlivost a v neposlední řadě na bezpečnost provozu.

Automatizované železniční zabezpečovací systémy umožňují zkracování rozestupů mezi jednotlivými soupravami prostřednictvím kontinuální detekce polohy vlaku a kontinuální rádiové komunikace s řídicími centry. Systém CBTC (Communication Based Train Control) představuje klíčovou technologii pro moderní vysokokapacitní kolejovou dopravu.

Systém CBTC umožňuje nahrazení signalizačních návěstidel, přímou komunikaci s traťovými komponenty (například čítači náprav nebo přestavníky) a integraci dalších subsystémů, jakým je zabezpečení nástupního prostoru pomocí PSD (Platform Screen Doors), zajišťující kontrolovaný nástup a výstup cestujících.

V závislosti na úrovni automatizace, definované ve standardu EN 62290-1, je palubní subsystém schopen plně vést vlak v rámci zábrzdné dráhy stanovené automatickým řídicím centrem bez přítomnosti řidiče, ovládat dveře souprav, zpracovávat povely drážního dispečinku a řešit nouzové situace na palubě vozidla. Traťový subsystém kontinuálně komunikuje se všemi soupravami na trati, zajišťuje jejich sledování a bezpečnou separaci, ovládá trakční napájení a koordinuje činnost dalších traťových komponent.

2 Metodologie průkazu bezpečnosti a spolehlivosti systému CBTC

Mimořádná komplexita systému CBTC, který se skládá ze dvou oddělených, avšak úzce spolupracujících subsystémů, desítek externích komponent a rozsáhlé sítě komunikačních rozhraní, klade vysoké nároky na ucelený a konzistentní průkaz bezpečnosti a spolehlivosti. Tyto požadavky jsou zároveň závislé plnění kritérií evropských norem EN 50126, EN 50129 a EN 50159, a to pro funkce s nejvyšší úrovní integrity bezpečnosti SIL 4.

Klíčovým prvkem demonstrace bezpečnosti systému CBTC je systematická identifikace nebezpečných stavů (hazardů) a klasifikace jejich důsledků. S rostoucím počtem funkcí a jejich vzájemných vazeb se stává splnění jak kvalitativních, tak kvantitativních bezpečnostních cílů mimořádně náročným úkolem. Příspěvek se proto zaměřuje na popis metodologie definice poruchových stavů na úrovni generického produktu a na jejich následné využití v procesu průkazu bezpečnosti a spolehlivosti.

3 Výstupy

Cílem je představení specifik spojených s demonstrací bezpečnosti a spolehlivosti komplexního systému CBTC, který prochází kontinuálním vývojem v průběhu celého životního cyklu. Pozornost je soustředěna především na metodologické aspekty prokazovaní bezpečnosti, nikoli na prezentaci konkrétního architektonického řešení nebo principů železniční dopravy.

Doprovodným přínosem je stručné porovnání přístupů ke klasifikaci poruchových stavů a k následnému přiřazování kvantitativních bezpečnostních cílů v letecké a železniční dopravě. V oblasti letectví je ilustrativně uveden příklad certifikační kategorie EASA CS-23, zatímco v železniční dopravě jsou analyzovány postupy vycházející z evropských norem EN 50126, EN 50129 a EN 50159.

Reference

[1] EN62290-1 Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts
[2] EN50126-1:2017 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS process;
[3] EN50126-2:2017 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety;
[4] EN50129:2018 Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling; English version

Metodika Sicherheitsregelung Fahrzeug (SIRF) pro efektivní prokazování bezpečnosti kolejových vozidel

Ing. et Ing. Jakub Habásko
Safety Manager (Siemens Mobility, s.r.o.)
jakub.habasko@siemens.com

1 Úvod

S rostoucí komplexností železničních systémů a zaváděním nových technologií, zejména v oblasti software a hardware, se zvyšují nároky na prokazování jejich bezpečnosti. V reakci na tuto potřebu vznikla metodika *Sicherheitsregelung Fahrzeug* (SIRF), která představuje praktický a propracovaný přístup k zajištění funkční bezpečnosti kolejových vozidel. Cílem této prezentace je představit metodiku SIRF jako efektivní nástroj pro splnění legislativních požadavků a normativních standardů v železničním sektoru.

2 Metodika SIRF

Metodika SIRF, vyvinutá s ohledem na aktuální legislativní rámec (např. CSM-RA – Nařízení Komise (EU) č. 402/2013) a harmonizovaná s klíčovými evropskými normami (EN 50126, EN 50128, EN 50129 a IEC 61508), stanovuje jasná pravidla pro proces, rozsah posuzování a prokazování bezpečnosti. Její vývoj byl motivován snahou o vytvoření srozumitelného a použitelného rámce, který by umožnil holistický přístup k bezpečnosti železničních vozidel s ohledem na všechny provozní podmínky.

3 Klíčové aspekty a přínosy

SIRF definuje proces o čtyřech krocích pro prokazování bezpečnosti vozidla, který zahrnuje definici systému a identifikaci nebezpečí, volbu způsobu dokazování bezpečnosti, důkaz splnění bezpečnostních požadavků a dokumentaci důkazu bezpečnosti. Metodika klade důraz na systematickou identifikaci a klasifikaci nebezpečí prostřednictvím bezpečnostního deníku a umožňuje jednoznačný odhad rizik, například s využitím stromu nebezpečí (Gefährdungsbaum). Dále specifikuje požadavky na hardware a software a definuje roli Safety Managera v rámci bezpečnostní organizace.

4 Závěr

Metodika SIRF nabízí ucelený, a přitom poměrně jednoduchý rámec pro prokazování bezpečnosti železničních vozidel, který je plně v souladu s mezinárodními standardy a legislativou. Její propracovanost spočívá v detailním vedení celým procesem řízení rizik, od počáteční definice až po finální dokumentaci, čímž přispívá k vyšší úrovni bezpečnosti v železniční dopravě a zjednodušuje komplexní proces certifikace a schvalování vozidel.

Reference

[1] EISENBAHN-BUNDESAMT: *Sicherheitsregelung Fahrzeug Überarbeitete Fassung 2019.* PDF. Online. Dostupné z: https://www.eba.bund.de/SharedDocs/Downloads/DE/Fahrzeuge/Fahrzeugtechnik/Funktionale_Sicherheit/31_SIRF_Sicherheitsregelgung_Fahrzeuge.pdf?__blob=publicationFile&v=2 [citováno 2026-01-20]

[2] *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]

Příklady postupů prokazování bezpečnosti a spolehlivosti železniční techniky

Sborník přednášek

kolektiv autorů

1. vydání

rok vydání 2026, Česká společnost pro jakost

vazba brožovaná, 8 stran