Zkušenosti s aplikací RAMS podle normy ČSN EN 50126-x

Materiály ze 77. semináře Odborné skupiny pro spolehlivost,
konaného dne 3. 12. 2019 v Praze

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

Obsah

Co nového přináší 2. vydání normy ČSN EN 50126-1 a ČSN EN 50126-2

doc. Ing. Pavel Fuchs, CSc.

Alopex, s.r.o.

e-mail: pavel.fuchs1@gmail.com

1 Úvod

Do soustavy českých technických norem byla překladem převzata EN 50126-1:2017 *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process*. Tato norma nahrazuje EN 50126:1999 (později přeznačená na EN 50126-1:2006), proto je žádoucí přiblížit odborné veřejnosti podstatné změny, ke kterým došlo při revizi normy.

S normou EN 50126-1:2017 souvisí norma a EN 50126-2:2017 *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety*. Jejím předchůdcem byla technická normalizační informace CLC/TR 50126-2:2007, která zastarala. Je tedy třeba se podstatnými informacemi uvedenými v normě seznámit a to i v rámci její vazby na EN 50126-1:2017.

Dalším důvodem, pro seznámení s oběma normami je i vývoj v terminologii a její použití při českém překladu obou norem. Obě normy jsou nyní v soustavě českých technických norem vedeny jako:

- ČSN EN 50126-1 ed. 2:2019 (33 3502) *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Generický proces RAMS*
- ČSN EN 50126-2:2019 (33 3502) *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti*

Příspěvek není určen k výkladu jednotlivých článků normy. Předpokládá alespoň základní obeznámení s problematikou RAMS drážních zařízení, norem RAMS a souvislostí norem RAMS s normami se vztahem ke spolehlivosti a funkční bezpečnosti.

2 Normy RAMS a bezpečnost drážních zařízení

Spolehlivost a bezpečnost dráhy je z vrcholové úrovně (mezinárodní a národní) usměrňována legislativními požadavky a následnými požadavky dozorových orgánů (drážních úřadů). Pro jejich praktickou aplikaci do technického provedení drážních zařízení a procesů jejich životního cyklu se aplikují kodexy správné praxe.

Pro jednotnost, vzájemnou porovnatelnost a uznatelnost drážních zařízení jsou za kodexy správné praxe považovány normy. Příslušné mezinárodní standardy tedy jednotně upravují požadavky na dráhu jako celek a na jednotlivá zařízení dráhy a to v dílčích oblastech, pro kterou jsou normy koncipovány.

Oblast spolehlivosti a bezpečnosti (RAMS) drážních zařízení pokrývají normy EN 50126-1, EN 50126-2, EN 50128 a EN 50129, které vydává Evropský výbor pro normalizaci v elektrotechnice (CENELEC). Tyto normy jsou převzaty do soustavy českých norem, viz [1], [2], [3] a [4]. Přičemž normy [1], [2], [3] jsou převzaty překladem, norma [4] je převzata bez překladu.

Pro oblast bezpečnosti pak dále platí legislativní dokument Směrnice č. 2004/49/ES (směrnice o bezpečnosti železnic) [5] a Prováděcí nařízení Komise (EU) č. 402/2013 (o společné bezpečnostní metodě pro hodnocení a posuzování rizik) [6] a Prováděcí nařízení Komise (EU) č. 2015/1136, kterým se mění nařízení o společné bezpečnostní metodě pro hodnocení a posuzování rizik [7].

Tvorba těchto norem má svoji historii a návaznost na jiné normy a legislativní dokumenty, viz následující přehled v tab. 1.

Tabulka 1: Přehled vydávání normativních a legislativních dokumentů

Rok vydání	**Dokument**
1995	předběžný návrh normy ENV 50126 (RAMS drážních zařízení)
1998	IEC 61508 (funkční bezpečnost – SIL, výrobci a dodavatelé)
1999	EN 50126 (RAMS drážních zařízení)
2001	EN 50128 (SW pro drážní řídicí a ochranné systémy)
2003	IEC 61511(funkční bezpečnost – SIL, LOPA, návrháři, projektanti a uživatelé)
2003	EN 50129 (drážní elektronické zabezpečovací systémy – SIL)
2006	TR 50126-3 (návod pro použití EN 50126-1 pro RAM kolejových vozidel)
2007	TR 50126-2 (návod pro použití EN 50126-1 pro bezpečnost – pro všechna drážní zařízení))
2008	TR 50126-3 (změna)
2009	Nařízení Komise (ES) č. 352/2009 (společná bezpečnostní metoda pro hodnocení a posuzování rizik)
2010	IEC 61508 ed. 2 (funkční bezpečnost – SIL, výrobci a dodavatelé)
2011	EN 50128 ed. 2 (SW pro drážní řídicí a ochranné systémy)
2013	Prováděcí nařízení Komise (EU) č. 402/2013 o společné bezpečnostní metodě pro hodnocení a posuzování rizik
2015	Prováděcí nařízení Komise (EU) č. 2015/1136 o společné bezpečnostní metodě pro hodnocení a posuzování rizik (změna)
2017	EN 50126-1 ed. 2 (RAMS drážních zařízení – generický proces RAMS)
2017	EN 50126-2 (RAMS drážních zařízení – systémový přístup k bezpečnosti)
2017	IEC 61511 ed. 2 (funkční bezpečnost – SIL, LOPA, návrháři, projektanti a uživatelé)
2018	EN 50129 ed. 2 (drážní elektronické zabezpečovací systémy – SIL)

V současnosti je pozornost směřována k tomu, jakým způsobem vyhovět požadavkům společné bezpečnostní metody CSM (Common Safety Method) pomocí implementace norem RAMS pro drážní zařízení.

3 Co nového přináší ČSN EN 50126-1 ed. 2:2019

Původní norma s označením ČSN EN 50126:2001 byla postupně měněna dílčími nepodstatnými doplňky. Proto se při posuzování změn porovnává nejnovější vydání normy s normou původní.

3.1 Zaměření

Základní zaměření normy zůstává stejné. Jedná se o procesní normu, tedy normu, která cílí na řízení procesů za účelem konzistentního přístupu k řízení bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti označované zkratkou RAMS.

Proti předchozímu vydání se uvádí, že norma EN 50126 je součástí uplatnění IEC 61508 v železničním sektoru. Naplnění požadavků této evropské normy společně s požadavky dalších vhodných norem je dostatečné pro to, aby nemusela být prokazováno naplnění požadavků normy IEC 61508.

To je velmi důležitá pasáž s ohledem na návaznost EN 50128 a EN 50129, které se zabývají SW a HW stránkou funkční bezpečnosti. Lze z toho jednoznačně vyvodit, že prokázání SIL podle EN 50129 není bez implementace EN 50126-1 relevantní. Jinými slovy řečeno, není uznatelné ve smyslu prokázání SIL dle IEC 61508.

3.2 Porovnání struktury

Členění normy do kapitol zůstává v zásadě porovnatelné. V novém vydání přibyla kap. 4 (Zkratky) a tak došlo posunu v číslování kapitol proti předchozímu vydání normy. Nově byla přidána kap. 8 věnovaná důkazu bezpečnosti. Dále došlo však k přesunu části textů mezi kapitolami, např. v kapitole 6 (dříve 5) věnované managementu RAMS. Rovněž část informací uváděných v předchozím vydání normy ČSN EN 50126 byla přesunuta do ČSN EN 50126-2 v rámci nového pojetí normy. V obou vydáních normy jsou kapitoly podrobně strukturovány a popsány a to pomocí podkapitol a odstavců s jednoznačnou číselnou identifikací.

Lépe je formulována kap. 5 (v předchozím vydání kap. 4) týkající se RAMS obecně a to zejména v části zabývající se rizikem. Informace týkající se posuzování rizika jsou pojaty obecně a příklady kategorizace a hodnocení rizika jsou přesunuty z normativní části do informativní přílohy.

Následující kap. 6 (dříve 5) se týká managementu RAMS dráhy/železnice založeného na životním cyklu systému. V novém vydání je tato kapitola mnohem propracovanější s důrazem na dokumentování procesů, na jejich verifikaci a validaci a na nezávislé posouzení bezpečnosti. Podstatná změna je v etapách životního cyklu systému, viz tab. 2.

Tabulka 2: Přehled etap životního cyklu systému

Etapy podle ČSN EN 50126:2001	**Etapy podle ČSN EN 50126-1 ed. 2:2019**
1. Koncepce	1. Koncept
2. Definice systému a podmínky použití	2. Definice systému a provozní souvislosti
3. Analýza rizika	3. Analýza rizika a jeho ohodnocení
4. Požadavky na systém	4. Specifikace systémových požadavků
5. Rozdělení požadavků na systém	5. Architektura a rozdělení požadavků na systém
6. Návrh a zavedení	6. Návrh a implementace
7. Výroba	7. Výroba
8. Instalace	8. Integrace
9. Validace systému	9. Validace systému
10. Přejímka systému	10. Přijetí systému
11. Provoz, údržba	11. Provoz, údržba a sledování výkonnosti
12. Sledování výkonnosti	12. Vyřazení z provozu
13. Modifikace a regenerace	
14. Vyřazení z provozu a likvidace	

Kap. 7 (dříve 6) se zabývá životním cyklem RAMS. Zde dochází ke změnám v souladu se změnami v etapách životního cyklu systému.

Kapitola 8 se zabývá problematikou důkazu bezpečnosti. V předchozím vydání normy nebyla tato problematika samostatnou kapitolou řešena.

Původní i nové vydání normy obsahuje informativní přílohy. Došlo ke změně v tématu příloh, případně ke změnám u příloh stejného tematického zaměření. Přehled příloh je uveden v tab. 3.

Tabulka 3: Přehled informativních příloh

Přílohy podle ČSN EN 50126:2001		**Přílohy podle ČSN EN 50126-1 ed. 2:2019**	
A	Stručný nástin specifikace RAMS – příklad	A	Plán RAMS
B	Program RAMS	B	Příklady parametrů pro železnici
C	Příklad parametrů pro dráhy	C	Kalibrace matice rizika a kategorie přijetí rizika
D	Příklady některých principů přijetí rizika	D	Pokyny k definici systému
E	Odpovědnost v rámci procesu RAMS během životního cyklu	ZZ	Vztah mezi touto evropskou normou a základními požadavky směrnice EU 2008/57/EC

3.3 Terminologie

Nové vydání normy přináší podstatně širší rozsah termínů a definic. V předchozím vydání bylo použito 45 definic. Nové vydání obsahuje 83 definic. Je to důsledek vývoje norem souvisejících se spolehlivostí, funkční bezpečností a rizikem. Z těchto norem jsou pak definice přebírány do procesní normy EN 50126-1.

Nové vydání opustilo pojem program RAMS a nahradilo jej termínem plán RAMS. Projevuje se tendence rozdělovat plánování RAMS na plánování RAM a plánování bezpečnosti. Zřejmě v souvislosti s tím, že ve firemní praxi jsou často management bezpečnosti a management RAM odděleny.

Pokud jde o překlad normy do českého jazyka, lze konstatovat výrazně vyšší odbornou úroveň překladu termínů spojených se spolehlivostí a posuzování rizik.

4 Co nového přináší ČSN EN 50126-2:2019

Prvním předchůdcem této normy byla technická zpráva CLC/TR 50126-2 [8] z roku 2007. Nebyla přejata do ČSN jako technická normalizační informace a tak nemá smysl s ní porovnávat nově vydanou ČSN EN 50126-2:2019. Proto je v následujících provedeno jen základní seznámení s normou.

4.1 Zaměření

Norma ČSN EN 50126-1 se zaměřovala na management RAMS v obecnějším pojetí. Jeho součástí je proces řízení bezpečnosti. Pro podporu procesu řízení bezpečnosti je určena norma ČSN EN 50126-2, která uvádí návody a metody pro bezpečnost.

4.2 Struktura

Tato evropská norma se skládá z hlavní části (1 až 11) a příloh A, B, C, D, E, F, G a ZZ. Požadavky definované v hlavní části normy jsou normativní, zatímco přílohy jsou informativní.

Po úvodních kapitolách normy následuje kap. 5, kde je popsán proces bezpečnosti. Proces je popsán na základě obecných principů, které jsou doplněny upřesňujícím vysvětlením z oblasti drážních zařízení.

V kap. 6 je pojednáno o prokázání bezpečnosti a procesech přijetí důkazu bezpečnosti pro daný systém. Důkaz bezpečnosti je podrobněji specifikován pro generický produkt, pro generickou aplikaci a pro specifickou aplikaci. Je uveden příklad závislosti mezi důkazy bezpečnosti a vztah mezi důkazy bezpečnosti a architekturou systému. Pro důkaz bezpečnosti je stanovena odpovědnost za řízení důkazu bezpečnosti v závislosti na vztahu mezi zúčastněnými stranami.

Důležitá je kap. 7, která se zabývá organizací a nezávislostí roli při řízení bezpečnosti a to v závislosti na etapách životního cyklu systému. Stanovuje míru nezávislosti na projektovém manažerovi pro projektanta, verifikátora, validátora a nezávislého posuzovatele bezpečnosti ISA (Independent Safety Assessor).

Kap. 8 pojednává o posouzení rizik. Je zpracována velmi systematicky a návodně, od analýzy rizik až po přijetí a posouzení rizik. V souladu s CSM za kritéria přijetí rizika uznává:

- použití kodexu praxe CoP (Code of Practice),

- použití referenčního systému,
- použití explicitního odhadu rizika.

Dále jsou zde uváděny pro případ použití explicitního odhadu rizika postupy a příklady pro přípustnou intenzitu rizik THR (Tolerable Hazard Rate).

Specifikace požadavků na bezpečnost systému je metodicky vysvětlena v kap. 9. Přičemž požadavky na bezpečnost jsou kategorizovány jako:

- požadavky na funkční bezpečnost,
- požadavky na technickou bezpečnost,
- požadavky na bezpečnostní souvislost.

Specifikace požadavků je doprovázena vysvětlujícími příklady.

Kap. 10 se zabývá rozdělením požadavků na integritu funkční bezpečnosti pro elektronické a neelektronické architektury. Pro elektronické systémy je dán návod na alokaci funkční bezpečnosti prostřednictvím alokace úroveň integrity bezpečnosti SIL (Safety Integrity Level) a přípustné intenzity nebezpečí TFFR (Tolerable Functional Failure Rate). Integrita bezpečnosti pro neelektronické systémy je řešena prostřednictvím uplatňování kodexu praxe CoP. Oba přístupy jsou vysvětleny na příkladech.

Postupy pro návrh a implementaci uvádí kap. 11a týkají se provedení analýzy nebezpečí, která zahrnuje analýzu příčin, upřesněnou identifikaci nebezpečí a analýzu společných příčin.

Pokud jde o informativní přílohy A, B, C, D, E, F, G a ZZ, jejich stručnou charakteristiku podává následující přehled.

Příloha A – seznamuje se základními kritérii přijatelnosti rizik dle metody ALARP, GAME a MEM.

Příloha B – uvádí postupy odvození hodnoty THR pomocí statistiky poruchy a nehody.

Příloha C – prezentuje návod pro přidělování SIL.

Příloha D – popisuje metody rozdělení bezpečnostních cílů. V rámci těchto metod uvádí příklady výpočtu THR redundantních systémů.

Příloha E – zabývá problematikou společné chyby při kvantifikaci, kdy dochází k nesprávnému kombinování četnosti poruch s pravděpodobností a použití vzorců mimo rozsah jejich použitelnosti.

Příloha F – prezentuje metody pro bezpečnostní analýzu a jejich použitelnost.

Příloha G – specifikuje klíčové role pro systém bezpečnosti a jejich odpovědnost. Specifikace se týká role pro projektanta, verifikátora, validátora, nezávislého posuzovatele bezpečnosti a projektového manažera.

Příloha ZZ – udává vztah mezi touto evropskou normou a základními požadavky směrnice EU 2008/57/EC o interoperabilitě železničního systému ve Společenství.

4.3 Terminologie

V této normě platí termíny a definice uvedené v ČSN EN 50126-1. Pokud jde o překlad normy do českého jazyka, lze konstatovat uspokojivou úroveň překladu termínů spojených se spolehlivostí a posuzování rizik.

5 Závěr

Z uvedeného přehledu je zřejmé, že ČSN EN 50126-1 ed. 2:2019 a ČSN EN 50126-2:2019 jsou v porovnání s jejich předchůdkyněmi vyzrálejší a více konzistentní. Pro odborníky poskytují dobře čitelné a pochopitelné návody, jak nastavit procesy, role, pravomoci a odpovědnosti při řízení RAMS. Značným přínosem je jejich navázání na směrnice EU týkající se CSM a TSI.

Použitá literatura

[1] ČSN EN 50126-1 ed. 2:2019 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Generický proces RAMS.*

[2] ČSN EN 50126-2:2019 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti.*

[3] ČSN EN 50128 ed. 2: 2012 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Software pro drážní řídicí a ochranné systémy.*

[4] ČSN EN 50129 ed. 2:2019 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Elektronické zabezpečovací systémy.*

[5] Směrnice č. 2004/49/ES ze dne 29. 4. 2004 o bezpečnosti železnic Společenství a o změně směrnice Rady 95/18/ES o vydávání licencí železničním podnikům a směrnice 2001/14/ES o přidělování kapacity železniční infrastruktury, zpoplatnění železniční infrastruktury a o vydávání osvědčení o bezpečnosti.

[6] Prováděcí nařízení Komise (EU) č. 402/2013 ze dne 30. dubna 2013 o společné bezpečnostní metodě pro hodnocení a posuzování rizik a o zrušení nařízení (ES) č. 352/2009.

[7] Prováděcí nařízení Komise (EU) 2015/1136 ze dne 13. července 2015, kterým se mění prováděcí nařízení (EU) č. 402/2013 o společné bezpečnostní metodě pro hodnocení a posuzování rizik.

[8] CLC/TR 50126-2:2007 *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety.*

Poznatky z certifikačního procesu drážních zařízení

doc. Ing. Martin Leso, Ph.D.
ČVUT v Praze – Fakulta dopravní.
e-mail: lesomart@fd.cvut.cz

1 Úvod

ČVUT v Praze, Fakulta dopravní prostřednictvím samostatného pracoviště „Certifikační orgán pro výrobky při Fakultě dopravní“[1] se věnuje činnosti posuzování bezpečnosti železničních zabezpečovacích zařízení od roku 1998. Hlavním předmětem posuzování jsou železniční zabezpečovací systémy a v posledních letech rovněž řídicí systémy kolejových vozidel. Za dobu působení v této oblasti se výrazně změnila jak technologie předmětných zařízení (zejména masový přechod k elektronickým systémům s SW programováním), tak se rovněž zpřísňovaly požadavky a kritéria posuzování bezpečnosti. Zásadní zlom přišel po roce 2000, kdy byly aplikovány normy řady ČSN EN 5012x[2]. Zavedení těchto norem vyžadovalo změnu přístupu ke způsobu dokladování bezpečnosti zařízení u výrobců i provozovatelů systémů a zároveň klade nové požadavky na posuzovatele bezpečnosti. Protože v oboru železniční zabezpečovací techniky nebyly principy řízení kvality a řízení bezpečnosti zaváděné normami ČSN EN 5012x dosud systematicky aplikovány, jedná se o zásadně průlomové období v daném oboru. Příspěvek se bude zabývat hlavními aspekty a souvislostmi v procesu posuzování drážních systémů, zejména z pohledu posuzovatele bezpečnosti drážních zabezpečovacích systémů.

2 Historie schvalování železničních zabezpečovacích zařízení

Schvalování železničních zabezpečovacích zařízení je prováděno již od samotného počátku vzniku železničních zabezpečovacích systémů. Počátky nezávislého hodnocení a posuzování bezpečnosti železničních zabezpečovacích systémů je možné spatřovat již při masovém nasazování mechanických a elektromechanických zabezpečovacích zařízení na přelomu 19. a 20. století. Počátkem 50. let 20. století se započaly masově nasazovat reléové systémy. Pro tyto systémy nebyly z počátku definovány jednoznačné postupy pro posuzování a hodnocení. Protože složitost a rozsah těchto systémů výrazně narůstaly, záhy se ukázalo, že samotná zkouška zařízení při jeho aktivaci je nedostačující. Hlavním důvodem je skutečnost, že i reléové zařízení je již složeno z velkého množství součástek na bázi relé, případně elementárních elektrotechnických prvků, později také polovodičových prvků, u kterých je nutné uvažovat rovněž poruchové stavy jednotlivých komponent. Proto počátkem 70. let minulého století byla ve VÚŽ zpracována interní směrnice, která podrobně definovala postup schvalování těchto technologií. Tato směrnice byla výchozím dokumentem pro oborovou normu ON 34 2606, která po roce 1989 byla převedena na TNŽ 34 2606. Norma zavedla

[1] Pro subjekt ČVUT v Praze - Certifikační orgán pro výrobky při Fakultě dopravní bude dále používána zkratka COV FD.
[2] Pro zjednodušení textu bude dále používáno označení ČSN EN 50 12x pro soubor norem ČSN EN 50 126, ČSN EN 50 129 a ČSN EN 50 128.

detailní postup, tzv. „Rozbor bezpečnosti funkce“, který sloužil k doložení toho, že navržený systém nezahrnuje předpokládaná bezpečnostní rizika. Postup byl založen na základních předpokladech jednonásobných poruch, zapojení obvodů na stálý proud, katalog poruch součástek – definování seznamu prvků a definování jejich uvažovaných poruch, které musely být v rámci „Rozboru bezpečnosti funkce“ uvažovány, tj. předpokládají se pouze poruchy z tohoto katalogu. Na základě tohoto postupu musel výrobce předložit výsledek rozboru funkce nezávislému schvalovateli, kterým bylo pracoviště VÚŽ, od roku 1998 rovněž pracoviště Fakulty dopravní ČVUT v Praze. Technické schválení probíhalo na základě pověření Ministerstva dopravy k provádění prohlídky a zkoušky dle §47 Zákona o drahách. Provádění „Technického schválení“ bylo ve smyslu výnosu „Schvalování železničních zabezpečovacích systémů pro ČD“, zveřejněném ve Věstníku ČD č. 4. ze dne 28. 2 1997. Postup umožňoval doložení analýzou, že systém je schopen za definovaných podmínek vykonávat bezpečnou funkci. Mylně se však předpokládalo, že dodržením tohoto postupu podle výše uvedené normy je prokázáno, že zařízení je absolutně bezpečné, neboli že nemůže selhat. Některé případy nehodových událostí však také toto tvrzení vyvracely, což potvrdil např. v roce 1974 Ing. Karel Kulle ve své disertační práci zabývající se „Analýzou bezpečnosti a spolehlivosti železničních zabezpečovacích zařízení“. Na základě vyhodnocení nehod na železničních zabezpečovacích zařízeních počínaje rokem 1953 až 1974 bylo zjištěno, že jednou za cca 1 100 000 hodin došlo k fatálnímu selhání zabezpečovacího zařízení.

První elektronické zabezpečovací zařízení bylo uvedeno do provozu v roce 1978 v železničním uzlu Göteborg ve Švédsku. Později se počaly masově nasazovat systémy na bázi mikroprocesorů s SW vybavením. Současně se změnou technologie musel být změněn přístup k dokládání a posuzování těchto systémů, neboť dosavadní přístup založený na „Rozboru bezpečnosti funkce“ nelze z důvodu odlišné technologie a koncepce systémů aplikovat. Nový přístup vychází z pravděpodobnostního přístupu založeného na modelech spolehlivosti, aplikací procesů řízení kvality a procesu řízení bezpečnosti zahrnující analýzu rizik.

Zásadní změnou vyplývající z aplikace nových přístupů v souvislosti se zavedením požadavků dle normativů ČSN EN 5012x je pro vývojáře skutečnost, že kromě popisu konečného návrhu řešení zařízení (jak bylo obvyklé u reléových systémů), je nutné dokladovat veškeré činnosti a postupy prováděné během vývoje a návrhu. Zároveň musí být aplikován účinný systém řízení jakosti zaručující jednotný a definovaný přístup k návrhu a vývoji systémů. Proces hodnocení se díky tomuto přístupu nyní již **nemůže zabývat pouze konkrétním výsledným technickým řešením daného zařízení**, ale musí se zabývat rovněž **posouzením všech procesů, které byly použity pro výsledné řešení**. To klade nároky také na management výrobců, kteří musí implementovat požadavky do interních postupů návrhu a vývoje. Rovněž kvalifikace hodnotitelů bezpečnosti již musí mimo odbornou kvalifikaci v oboru také zahrnovat schopnost hodnotit systémy kvality a procesy řízení návrhu a vývoje. Je však nutné konstatovat, že železniční zabezpečovací technika není v tomto přístupu ojedinělou oblastí, postupně ke stejnému procesu návrhu i hodnocení dospěly všechny průmyslové obory, u kterých je nutné dokládat úroveň bezpečnosti. Mimo jiné to dokládá skutečnost, že soubor norem pro drážní zařízení ČSN EN 5012x vychází z normativů řady ČSN EN 61508 pro Funkční bezpečnost elektrických /elektronických / programovatelných elektronických systémů souvisejících s bezpečností, které jsou používány v dalších průmyslových oblastech.

3 LEGISLATIVNÍ RÁMEC HODNOCENÍ BEZPEČNOST

Aplikace norem řady ČSN EN 5012x vyžaduje zcela jiný přístup z pohledu legislativy, která má zajistit jednotné a jednoznačné prostředí definující požadavky pro všechny zainteresované strany. Navíc se výrazně začal uplatňovat vliv Evropského společenství prosazující zařízení spadající pod tzv. „Součásti evropského železničního systému“, tedy v případě zabezpečovacích zařízení zejména systémy ERTMS/ETCS.

V současné době je legislativa pro schvalování železničních zabezpečovacích zařízení a jejich uvádění do provozu ošetřena Zákonem o drahách č. 266/1994 Sb., kde je obsažen §47 pro určená technická zařízení (UTZ) a §49b pro systémy, které jsou součástí evropského železničního systému.

Technická způsobilost posuzovaná dle §47 je řešena v odstavci 2), který je naplněn Vyhláškou MD č. 177/1995 Sb. V této vyhlášce je v 3. odstavci stanovena povinnost, aby před uvedením UTZ do provozu, aby byla schválena jeho způsobilost k provozu, kterou „schvaluje drážní správní úřad vydáním průkazu způsobilosti“. Ve 4. odstavci je definováno, že „…drážní správní úřad vydá průkaz způsobilosti určeného technického zařízení na základě technické prohlídky a zkoušky…“, která je řešena Vyhláškou MD č. 100/1995 Sb. Ta však definuje obecné požadavky na provádění prohlídky, zkoušky a pravidelné revize, technickou dokumentaci, stanovuje časové lhůty pro provedení revizí apod., nově je v reakci na Nařízení Komise (ES) č. 352/2009 doplněn požadavek na hodnocení rizik. Vyhláška se však nezabývá doložením nezávislého hodnocení bezpečnosti v souladu s normami ČSN EN 5012x.

Podmínky pro konstrukci, výrobu a provoz určených technických zařízení a jejich konkretizaci stanovuje prováděcí předpis. V případě systémů, které nejsou součástí evropského železničního systému je platná zejména vyhláška MD č. 177/1995 Sb., kde v části §23, odst. 2) stanovuje povinnost, aby „byly navrženy, dimenzovány, provedeny a jištěny tak, aby tuto svoji funkci plnily spolehlivě při všech provozních stavech zařízení i při všech poruchových stavech způsobených uvažovanými poruchami“. To musí být provedeno definovanými normami, mezi kterými jsou mimo jiné rovněž uvedeny normativy ČSN EN 5012x.

Vliv Evropského společenství na tuto oblast není pouze v zavádění jednotných systémů řízení a zabezpečení (ERTMS/ETCS) ale má dopad rovněž na úroveň zavedení jednotné metodiky pro posuzování rizik na železnici vyplývající ze směrnice Evropského parlamentu a rady č. 2004/49/ES a následně Nařízení Komise (ES) č. 402/2013, je zavedena tato problematika do procesu uznávání způsobilosti zařízení formou „Zprávy o posouzení bezpečnosti“. Tato zpráva požadovaná dle metodického pokynu DÚČR[3] je však zprávou posuzující rizika, zejména v souvislosti uváděním systémů do provozu, nikoliv komplexním hodnocením bezpečnosti zařízení v rozsahu, v jakém je předpokládají normativy ČSN EN 5012x. Proto tato legislativní úprava řeší pouze jistý segment nasazení systémů do provozu a do jisté míry může způsobit zásadní nedorozumění, že bezpečnost zařízení je schválena „pouze“ posouzením rizik. Skutečnost je však opačná, posouzení rizik je nutnou podmínkou k definování bezpečnostních požadavků zařízení, jejichž naplnění musí být potvrzeno komplexním hodnocením bezpečnosti v souladu s normativy ČSN EN 5012x.

Jednoznačný požadavek na provedení posouzení bezpečnosti nezávislým hodnotitelem bezpečnosti definuje pouze SŽDC, s.o., ve své Směrnici č. 34 z roku 1997. Jedná se

[3] DÚ = Drážní úřad České republiky

o směrnici, která definuje podmínky, za jakých může být nové zařízení uvedeno do provozu na železniční dopravní cestě ve vlastnictví státu. Tato směrnice kromě definovaného procesu zavádění nových výrobků v oblasti zabezpečovacích zařízení a detailních požadavků na doložení dokumentace definuje v Článku 12. Požadavky na „Zprávu o hodnocení bezpečnosti výrobku“. Směrnice se zabývá zejména doložením požadavků podle normy ČSN EN 50129, přičemž neřeší úroveň doložení kritérií podle normy ČSN EN 50126. S ohledem na požadavek ČSN EN 50129, kap. 5.2, kde je jednoznačná souvislost s nutností vyhovění procesu řízení kvality v souladu s požadavky ČSN EN 50126-1, zdá se působnost požadavků této normy být jednoznačně zahrnuta. V praxi tomu však nebývá a řada výrobců se snaží tuto normu obejít pouze plněním požadavků ČSN EN 50129.

V článku 13 směrnice SŽDC č. 34 jsou definovány požadavky na samotné hodnotitele bezpečnosti výrobku. Jako hlavní požadavek je uvedeno, že „SŽDC uzná za hodnotitele bezpečnosti výrobku jen takové subjekty, které jsou:“

a) právnickou osobou pro provádění technických prohlídek a zkoušek UTZ dle §47 odst. 4 zákona č. 266/1994 Sb., o dráhách, nebo

b) autorizovanou osobou pro systém řízení a zabezpečení dle nařízení vlády č. 133/2005 Sb, nebo

c) certifikačním orgánem splňujícím požadavky ČSN EN 45011(nově ČSN EN 17065 a ČSN EN 17021) pro výrobky železniční zabezpečovací a sdělovací zařízení; Evropský železniční systém, subsystém řízení a zabezpečení (kód SKP 31.62.11).

Kvalifikace dle a) je dostačující pouze pro posuzování jednodušších systémů, reléových a elektronických (nikoliv ucelených rozsáhlých systémů, jako je např. elektronické stavědlo, elektronické přejezdové zabezpečovací zařízení, apod.)

Kvalifikace dle b) a c) umožňuje plné provádění posuzování shody s požadavky norem ČSN EN 5012x a dalšími normativy a předpisy související se všemi zabezpečovacími systémy. Prakticky této podmínce vyhovují hodnotitelé VUŽ – Notifikovaná osoba a COV FD.

Výhodu takto definovaného požadavku na kvalifikaci Hodnotitele bezpečnosti je možné spatřovat především v tom, že činnost hodnotitelů je přímo kontrolovatelná zavedeným a osvědčeným procesem Certifikačních orgánů, jejichž postupy a výkon činnosti jsou pod přímou kontrolou Českého institutu pro akreditaci o.p.s. (ČIA). Tímto je zajištěno, že je využíván stejný proces posuzování a hodnocení, který je obvyklý v západních evropských zemích a je v současné době obvyklý také v případě interoperabilních systémů.

Bohužel současný stav ustrnul na poloviční cestě tím, že Směrnice č. 34 vyžaduje pouze předložení ***„Zprávy o hodnocení bezpečnosti výrobku“,*** nikoliv ***„Certifikát shody výrobku“***. Zásadní problémem pro Certifikační orgány je v tom, že činnosti prováděné pod akreditací ČIA lze provádět pouze postupem, který je ukončen vydáním ***„Certifikátu shody výrobku“***, nikoliv pouze ***„Zprávou o hodnocení bezpečnosti“***. To by však znamenalo, že žadatel (výrobce) by musel požádat o Certifikaci výrobku, včetně plnění dalších kritérií související s Certifikací výrobků dle obecně platných postupů certifikace, což je v současné době bez přesné legislativy nařizující výrobcům dodržení tohoto postupu prakticky nemožné. Lze však doložit (zkušenostmi na pracovišti COV FD), že v případě hodnocení výrobků, není tento proces výrazně složitější ani nákladnější oproti dosavadnímu smluvnímu vztahu na vypracování Zprávy o hodnocení bezpečnosti.

Přes veškeré snahy našeho pracoviště u všech zainteresovaných stran (SŽDC, ACRI, MD ČR) se dosud nepodařilo sjednat pokrok v tom, aby byl povinný standardní proces Certifikace výrobků, jehož nedílnou součástí je rovněž Zpráva o hodnocení bezpečnosti.

Tento stav bohužel neumožňuje využití všech kladných přínosů, které dle mého názoru proces Certifikace výrobků přináší. Jako hlavní výhody lze uvést následující:

- Jednotnost postupů, kritérií a požadavků všech Hodnotitelů bezpečnosti – to má výrazný přínos pro všechny zainteresované strany jak po stránce věcné, tak i ekonomické.
- Uznatelnost Certifikátů shody mezi jednotlivými Certifikačními orgány – výrazný prvek zabraňující monopolu „jediného“ hodnotitele v daném státě. Umožňuje rovněž snazší přístup na zahraniční trhy pro výrobce, neboť proces uznávání Certifikátu je celoevropsky uznávaným procesem.
- Pravidelné dozory Certifikačním orgánem u všech vydaných Certifikátů – v rámci ročních auditů systému jakosti daného výrobku umožňuje trvale sledovat a prokazovat shodu výrobků, případně jeho vhodnost k použití, což má výrazný dopad na funkčnost a použitelnost výrobků především pro provozovatele, ale má sloužit i výrobcům ke zlepšení kvality stávajících i nových výrobků.

Argumentem výrobců zabezpečovacích zařízení proti procesu Certifikace většinou bývá obava z vyšší ceny, složitosti a náročnosti tohoto procesu. Lze však konstatovat, že tyto obavy nejsou z pohledu COV FD opodstatněné. Stávající procesy hodnocení bezpečnosti na našem pracovišti probíhají přesně podle postupů, které by byly aplikovány i v případě Certifikace výrobků. Hodnotící zpráva bezpečnosti je vždy nutným mezistupněm k udělení Certifikátu shody. Odlišnost v případě Certifikace je dána spíše formálními a procesními záležitostmi spočívajícími ve vydání Certifikátu a posléze dozoru (pravidelný roční audit systému kvality) nad vydaným Certifikátem. Navýšení náročnosti prací a tedy časové i finanční stránky takového posuzování jsou dle mého názoru minimální. Přínosy takového procesu jsou však zřejmé i pro výrobce, chápe-li tento proces jako pozitivní podnět ke zlepšení vlastního procesu a svých výrobků.

Kritéria na posuzovatele bezpečnosti jsou definovány jednoznačně především ve vztahu k posuzování interoperabilních systémů, kterých je dosud ale v rozsahu posuzování systémů na železnici výrazné minimum. Zde musí být splněny požadavky na tzv. Autorizovanou / Notifikovanou osobu, jejichž posuzování způsobilosti spadá pod kompetenci úřadu UNMZ[4]. Pro systémy, které patří mezi součásti evropského železničního systému, jsou závazné postupy definované v TSI[5] pro CCS[6]. Zavedený proces je řešen jako posouzení shody definovanými moduly (certifikačními postupy) na základě požadavků, mezi kterými jsou mimo technických specifikací všechny normativy ČSN EN 5012x. V českém legislativním prostředí jsou požadavky na posuzování shody řešeny Vyhláškou č. 352/2004 Sb., o provozní a technické propojenosti evropského železničního systému. Proces posuzováni shody je zajišťován autorizovanými/notifikovanými osobami ve smyslu zákona č. 22/1997 Sb. V současné době dochází v této oblasti k zásadní změně díky novým požadavkům

[4] UNMZ = Úřad pro technickou normalizaci, metrologii, a státní zkušebnictví
[5] TSI = Technická specifikace pro interoperabilitu
[6] CCS = Control command systém, který je tvořen částí traťovou (umístěnou v infrastruktuře) a mobilní (umístěnou na vozidle)

přicházejícím z Evropského společenství a bude od 6/2020 aplikován nový systematický přístup definovaný EURA[7]

Lze konstatovat, že proces hodnocení bezpečnosti, který by zajišťoval kompletní naplnění normativu ČSN EN 5012x není v ČR dostatečně legislativně ošetřen. Navzdory tomu procesy hodnocení bezpečnosti ve smyslu ČSN EN 50129 jsou zajišťovány za účelem naplnění požadavků SŽDC, s.o., avšak pouze formou **„Zprávy o hodnocení bezpečnosti“** jejíž vydání však nespadá do působnosti akreditace Certifikačních orgánů pro výrobky. Zavedením obdobného procesu Certifikace výrobků i na zařízení UTZ – elektronické systémy, které musí plnit požadavky norem ČSN EN 5012x by bylo prospěšné všem zainteresovaným stranám a vedlo by ke zvýšení úrovně prokázání parametrů železničních zabezpečovacích zařízení a tím také ke zvýšení jejich úrovně bezpečnosti.

4 Problematické body při posuzování shody – kritéria hodnocení

Aplikace norem ČSN EN 5012x přinesla zásadní změnu ve způsobu dokládání výrobku ze strany výrobců i způsobu posuzování jednotlivých kritérií hodnotiteli bezpečnosti.

Z pohledu výrobců musí být podle požadavků norem dokládán celý proces návrhu a vývoje, tedy nepostačuje již pouze deklarace výsledného řešení a obhájení jeho funkčnosti. Stěžejní pro doložení bezpečnosti zařízení jsou ustanovení ČSN EN 50129 kap. 5 tzv. ***„Důkazu bezpečnosti“***, který tvoří požadavky v kap. 5.2 – Doklady o řízení jakosti, kap. 5.3 – Doklady o řízení bezpečnosti a kap. 5.4 – Doklady o funkční a technické bezpečnosti. Z těchto kapitol je dále odkazováno na plnění požadavků podle normativů ČSN EN 50126-1 a ČSN EN 50128.

4.1 Problematika přístupu k návrhu a vývoji

Zásadním problémem se jeví jistá změna ve filozofii pojetí vývoje a návrhu, kde návrh a vývoj musí postupovat podle požadavků životního cyklu definovaného v ČSN EN 50126-1. Proces vývoje podle norem ČSN EN 5012x striktně postupuje od návrhu koncepce, definice systému a jeho použití ke stanovení jednotlivých odůvodněných požadavků. Až následně se vývojář dostává k řešení samotného technického problému tj. navrhnout HW a SW řešení. Tento přístup byl a stále je pro řadu technických pracovníků velmi velkým zvratem v jejich myšlení (zejména pro ty zkušenější, kteří již tvořili reálné návrhy před platností těchto normativů), protože dosavadní přístup spočíval spíše v navržení řešení a v případě jeho uspokojivého funkčního výsledku jeho následné zdokumentování.

4.2 Problematika řízení bezpečnosti a analýzy rizik

Po celou dobu životního cyklu musí být aplikován také cyklus řízení bezpečnosti. Ten po věcné stránce především spočívá v ***průběžném hodnocení možných nebezpečí*** a z nich vyplývajících rizik. V této fázi se řada technických pracovníků dokáže orientovat již lépe, protože dokáží již praktičtěji vymýšlet různé scénáře možných příčin selhání a navrhovat jistá opatření k jejich zamezení. Normy však požadují, aby tento proces byl formalizován tzv. procesem analýzy rizika, používali se strukturované záznamy jako např. ***„záznam o nebezpečí“*** který musí mít doloženy výpočty a analýzami. Naštěstí již v dnešní době je tato oblast pokryta řadou pomocných nástrojů pro řešení FTA či FMEA analýz a situace se po

[7] EURA = European Union Agency for Railways (Evropský drážní úřad)

věcné stránce zlepšuje. Převládá však nadále nepochopení v rozsahu uvažovaných rizik, která norma ČSN EN 50126-1 uvádí jako příklady včetně dalších obecných rizik přímo nesouvisejících s konkrétním výrobkem. Zároveň tato oblast může být výrazně komplikována skutečností, že jsou v posledních letech řešeny tzv. generické systémy, jejichž konkrétní účel nasazení a sním spojených nebezpečí a z nich vyplývajících rizik dopředu obtížně analyzovatelná.

Rovněž velmi problematickou kapitolou se jeví proces přiřazení a stanovení úrovně SIL[8]. V tomto norma ČSN EN 50126-1 dává příklad možného přiřazení kritéria akceptovatelnosti rizik. Není však jednoznačně definován vztah mezi identifikovanými riziky, jejich ohodnocení (je možné používat kvalitativní i kvantitativní modely stanovení odhadu rizik) a jejich mírou přijatelnosti pro konkrétní případ výrobku a jeho použití.

Jako největší úskalí v naplnění požadavků norem ČSN EN 5012x je možné v této souvislosti považovat legislativní nestanovení *„Orgánu pro otázky bezpečnosti"*. Tento orgán je uváděn v normách ČSN EN 5012x jako stěžejní subjekt, který definuje a vymáhá naplňování zejména bezpečnostních požadavků. Mimo jiné definuje a odsouhlasuje bezpečnostní cíle, bez kterých jakákoliv analýza rizik a rozhodnutí týkající se požadované úrovně bezpečnosti prakticky pozbývají smysl. Dle zvyklostí to bývá instituce na úrovni Drážního úřadu, nicméně současné pojetí řízení bezpečnosti toto zcela nenaplňuje. Chybí tedy podle mého názoru aktivně prováděný proces řízení bezpečnosti na úrovni uživatele daného výrobku (např. SŽDC) a dozorujících orgánů stanovujících bezpečnostní standarty (DÚ ČR), které by měly poskytnout a aktivně řídit všechna relevantní rizika a spolupracovat na přijetí rizik nových technologií.

Neexistence jednoznačných kritérií pro přijetí rizik poté bohužel vede k ryze účelovému (marketingově) stanovení požadavků na bezpečnost a to SIL=4, jakožto nejvyšší míry bezpečnosti definovaná normativy. Částečně totiž přežívá dojem tzv. ***„Absolutní bezpečnosti"***, přestože současný přístup definovaný normativy ČSN EN 5012x zavádí pravděpodobnostní přístup stanovení a prokázání bezpečnosti. V praxi bývá většinou použit argument, že ***„více bezpečné to již udělat nejde, proto jsme nemohli dělat víc a jinak"***. Bohužel s tím je částečně eliminován řádný proces stanovování rizik. Tento fakt je však irelevantní s ohledem na to, že analýza rizika má odhalit potenciální zdroje nebezpečí a z nich vyplývající rizika, která ve svém důsledku mohou znamenat zásadní změnu v definování bezpečné funkce a případně její realizace. Bohužel marketingově se požaduje dané číslo SIL, čím vyšší tím lepší pro prodej. Výrobce poté přenáší na sebe větší zodpovědnost, než mu přísluší a provozovatel „slepě" důvěřuje, že systém se ve všech situacích zachová, jak očekává.

4.3 Problematika nezávislého posuzování bezpečnosti

Z pohledu posuzovatele bezpečnosti je hlavním cílem a předmětem provedení na výrobci, provozovateli i dodavateli nezávislého posouzení naplnění požadavků jak norem ČSN EN 5012x, tak dalších normativů a předpisů provozovatele, legislativy apod. Tato činnost, ačkoliv by se zdála nadbytečnou a zbytečně komplikující a prodražující vývoj zařízení, je ve skutečnosti dalším kontrolním mechanismem, který má minimalizovat pravděpodobnost selhání systému nebo jeho nevyhovující chování. Řada zkušeností pramenící i z jiných oborů, např. letectví nebo vesmírného programu, ukazuje, že pro zamezení zejména systematických chyb (tedy chyb zapříčiněných zejména lidskou chybou při

[8] SIL = Safety Integrity Level (úroveň bezpečnosti definovaná jako tolerovatelná míra selhání bezpečnostní funkce systému za 1hodinu provozu)

vývoji, návrhu či výrobě systému) je jedním z velmi účinných mechanismů nezávislého (na vývojovém týmu i samotném vývojovém procesu) posouzení. Nejedná se přitom o standardní verifikační nebo validační procesy, které mají svoje definované postupy a jsou začleněny do procesu vývoje.

Při aplikaci normativů ČSN EN 5012x vyvstává velká otázka způsobu hodnocení návrhu bezpečných systémů.

Postup a předmět činnosti hodnotitele bezpečnosti je definován v předmětných normách ČSN EN 5012x. Výchozí normou pro všechny elektronické zabezpečovací systémy je ČSN EN 50129. Tato norma v kapitole 5. definuje „Podmínky pro uznání a schválení bezpečnosti“, které musí být doloženy definovanou formou jako tzv. „Důkaz bezpečnosti“.

Zásadní otázkou je metodický způsob posuzování jednotlivých kritérii požadavků norem či dalších zásad technického návrhu. Dlouhodobě spatřuji v oboru dva různé přístupy zavedených posuzovatelů bezpečnosti v ČR.

První, dá se říci tradiční, vychází z historického přístupu, kde se zejména posuzovatel zaměřuje na technické zajištění bezpečnosti návrhu a velmi detailně posuzuje technické aspekty návrhu a odhalování možných bezpečnostních rizik. Mnohdy jsou kladeny návrháři požadavky na doložení rozboru bezpečnosti funkce tak, že musí doložit, že daná hypotetická (posuzovatelem bezpečnosti nadefinovaná) nebezpečná situace v návrhu ***“nikdy nemůže nastat***“. Takový přístup sice umožňuje posuzovateli hluboce proniknout do velké úrovně návrhu, avšak je otázkou, jaké „pokrytí“ všech možných chyb v návrhu lze tímto detailním pohledem odhalit a vyřešit. Přístup tolik nedává aspekty na dodržování formálních požadavků norem. Aspekty životního cyklu jsou prověřovány posouzením systému kvality výrobce, ve kterém by měl být zahrnut rovněž proces řízení bezpečnosti. Vývojářům tento přístup do jisté míry vyhovuje, protože jsou tzv. ve svém oboru a zabývají se výhradně technickými důkazy, které jsou schopni řešit a ovlivňovat.

Druhý přístup, který aplikuje COV FD, vychází z kritérií požadavků na certifikační orgány podle normativu ČSN EN 17065. Požadavkem na hodnocení je jednoznačné stanoven kritérií hodnocení, které musí být všem žadatelům o certifikaci dopředu a jednoznačně známy a musí být aplikovány nediskriminačním způsobem. Proto při posuzování bezpečnosti výrobku jsou jednotlivé požadavky definovány na základě normativů anebo legislativou definovaných dokumentů a proces posuzování bezpečnosti je veden s cílem prokázat shodu se všemi relevantními kritérii podle normativů. Při posuzování bezpečnosti je snaha dodržet formálně jednotlivé požadavky, vůči kterým musí být prokázána shoda naplnění všech relevantních požadavků.

Bohužel současné normy, zejména ČSN EN 50126-1 trpí poměrně vysokou neurčitostí až nesrozumitelností jednotlivých požadavků. Je to danou částečně značnou obecností pro použití na všechny drážní systémy. Výrobce mají zejména potíže s naplněním požadavků v případě malých jednoúčelových a specifických prvků v systémech. Požadavky norem se jeví jako obtížně škálovatelné podle rozsahu projektu. Navíc k nepochopení jednotlivých ustanovení a požadavků přispívá fakt, že kritéria přirozeně zahrnují celý životní cyklus výrobku, který je u žadatele řešen na mnoha úrovních struktury firmy. Bohužel zodpovědnost za „zajištění schválení“ má většinou návrhář, v lepším případě projektový manažer. COV FD se proto snaží většinu systémových otázek týkající se nastavení procesů návrhu a vývoje řešit systematicky v rámci auditů systému kvality výrobce. Stěžejní je identifikovat procesy návrhu a vývoje, které jsou zavedeny u výrobce a jsou ve shodě s požadavky ČSN EN 5012x a zároveň jsou implementovány do jeho funkčního systému řízení kvality dle

ČSN EN ISO 9001:2016. Tento přístup činnost výrobce i posuzovatele výrazně zjednodušuje, pokud je však podle těchto směrnic a postupů skutečně postupováno. Bohužel často je sledován tlak managementu firmy na urychlení vývoje a je snaha tyto procesy „obcházet“ tím, že se daný výrobek vyrábí pro trh či aplikaci, kde není potřeba doložení bezpečnosti (nižší úroveň SIL, nebo východní trhy). Problém nastane ale v okamžiku, kdy výrobek, případně jeho část, se aplikuje pro použití, kde je vyžadována posouzení bezpečnosti výrobku podle ČSN EN 5012x normativů. Z tohoto přístupu neblahým následkům plynoucím lze účinně předejít respektováním jak požadavku norem ČSN EN ISO 9001:2016 a ČSN EN 50126-1, že management je součástí procesu řízení kvality a bezpečnosti a musí plnit svoje rozhodující řídící funkce. Osobní zkušeností je, že toto je možné dodržovat ve společnostech o cca. max. 200 zaměstnancích. V případě velkých korporátních firem s více jak 1000 zaměstnanci bývá řízení projektů již často velmi těžkopádné a systémy řízení kvality a bezpečnosti nemusí být zcela funkční. Podle několika reálných případů však evidentně záleží i na konkrétní zemi, firemní kultuře a tradici realizace bezpečných systémů.

Protože normy ČSN EN 5012x jsou definovány jako procesní a požadavkové normy, které neřeší konkrétní požadavky na zařízení, tak se ve fázi návrhu a vývoje se postupuje podle jasně definovaných požadavků na systém (s identifikovanými požadavky na bezpečnost) a sleduje se jejich rozpad na architekturu systému a jejich realizaci jak HW, tak SW částmi. Je kladen důraz na provázanost mezi jednotlivými požadavky a jejich realizací, případně následnou integrací HW a SW s výsledným testováním, verifikací a validací systému. Ve fázi posuzování konkrétního technického návrhu jsou posuzovány důkazy podle ČSN EN 50129, kap. 5.4. Důkaz bezpečnosti systému, kde jednotlivé kapitoly vyžadují detailní doložení bezpečnosti návrhu jak při řádném, tak poruchovém stavu systému. Zde posuzovatel musí proniknout do dostatečné úrovně návrhu tak, aby pochopil zvolné principy a předpoklady zajištění bezpečné funkce systému. Část SW se posuzuje podle kritérií normy ČSN EN 50128 obdobným způsobem (formální dodržování hodnotících kritérií) s tím, že bývá detailní posouzení zaměřeno také na analýzu zdrojových kódu SW. Zde se liší přístup výrobců, zda předloží zdrojové kódy k provedení nezávislých statických testů a analýzám u posuzovatele bezpečnosti anebo musí být tyto činnosti prováděny u výrobce.

4.4 Systém řízení kvality

Způsob nastavení systému řízení kvality výrobce je stěžejním předpokladem úspěšného posouzení bezpečnosti jak z pohledu řízení jakosti, tak řízení bezpečnosti. Drtivá většina firem vlastní certifikát na systém kvality podle ČSN EN ISO 9001:2016. Certifikace je prováděna certifikačními orgány pro systémy kvality, avšak při jejich posuzování nebývají hodnocena kritéria norem ČSN EN 5012x. Proto COV FD vždy provádí nezávislé posouzení systému kvality výrobce s tím, že se zaměřuje na způsob aplikace požadavků na systém řízení kvality a řízení bezpečnosti s ohledem na daný předmětný výrobek. Jedná se tedy o jiný pohled než v případě certifikace systému kvality, který je zaměřen na obecné systematické požadavky a výrobek je vybrán jeden jako vzorek (náhodný příklad) k ověření.

V systému kvality je stěžejní, aby vedení firmy bylo zahrnuto do rozhodování v rámci životního cyklu výrobku. Zejména se to týká stanovení projektového týmu, harmonogramu, který by měl být realistický a nevytvářející nepřijatelný tlak na neadekvátní urychlování vývoje, dostatek finančních prostředků a vyjednávání akceptovatelných technických podmínek se zákazníkem. Bohužel často se setkávám s managementem firmy, který je dost často věcně oddělen od procesu rozhodování výrobku a klade nesplnitelné cíle a požadavky. Tyto požadavky jsou velmi vysokým rizikem pro funkčnost a bezpečnost výrobku.

4.5 Zainteresované strany

Nutnou podmínkou úspěšného naplnění všech podmínek a předpokladů, které v zařízení musí být naplněny, je aktivní účast všech zainteresovaných subjektů. Informativní přehled všech zainteresovaných subjektů a doporučené role v rámci celého životního cyklu uvádí příloha E normy ČSN EN 50126. Tento přehled je nutné vykládat pouze jako příklad, konkrétní přiřazení zodpovědnosti jednotlivým subjektům je věcí národní legislativy a zvyklostí. Každopádně musí být vždy tyto role jednoznačně definovány.

Norma ČSN EN 50126-1 do značné míry předpokládá, že zejména na úvodních čtyřech etapách životního cyklu pracuje anebo se aktivně spolupodílí budoucí uživatel/provozovatel systému. V životním cyklu v úvodních etapách jsou definovány otázky směřující k podmínkám širšího zapojení navrhovaného systému či komponenty do celkového systému. Bohužel skutečné případy ukazují, že zákazník či provozovatel nemá procesy podle normativů ČSN EN 5012x osvojeny a zahrnuty do vlastních procesů (otázka aplikace ISO 9001:2016 u SŽDC, s.o.) a není tedy ve většině případů vůbec schopen aktivně na definování požadavků na koncepci, definice a požadavků včetně analýzy rizika na systém spolupracovat. Výrobce, konkrétně technik zodpovědný za návrh systému, je přitom postaven před velmi problematickou úlohu řešení a souvislostí, na které nemůže téměř prakticky pojmout.

Další velmi neopominutelnou rolí provozovatele drážního systému jsou záležitosti týkající se instalace, validace a přejímky systému. Vychází se z historicky zavedených procesů, které minimálně po formální stránce nebývají v souladu s předpoklady a požadavky norem. Zejména co se týče oblastí plánování a stanovování požadavků a generování a udržování odpovídajících záznamů.

Stěžejní fází v životním cyklu každého drážního systému je fáze provozování systému, kdy musí být umožněn výrobci, který zodpovídá (minimálně morálně) za bezpečný a spolehlivý provoz systému, přístup k diagnostickým informacím a identifikací vzniklých nebo i potenciálních poruch. Aby totiž bylo možné udržovat parametry RAMS systému, musí mít výrobce přístup k reálným parametrům a chování systému. Tento vztah se velmi obtížně nastavuje a vyžaduje vysoké uvědomění si zodpovědnosti za bezpečnost, spolehlivost a dostupnost zabezpečovacích zařízení na železnici.

Odběratel by měl rovněž respektovat požadavky norem z pohledu stanovení parametrů a metodiky stanovení parametrů RAMS. S ohledem na historické souvislosti je vyžadováno od dodavatele stanovení parametrů spolehlivosti a bezpečnosti, není však propracována metodika sledování a vyhodnocování těchto parametrů. Důsledky jsou poté v řešení nedostupnosti systému a řešení sporu o uznávání / neuznávání reklamací či systematických chyb.

5 Závěr

Příspěvek se mohl z důvodu omezeného rozsahu dotknout pouze části hlavních poznatků z více jak 20 let zkušeností posuzovatelů bezpečnosti železničních zabezpečovacích zařízení. Je evidentní, že vývoj zabezpečovacích zařízení, který by měl vyhovovat plně požadavkům předmětných normativů ČSN EN 5012x, je velmi náročným procesem. Tento proces může být úspěšně zvládnut, ale vyžaduje plné pochopení a zapojení všech zainteresovaných stran. Není to tedy pouze záležitostí výrobce, ale i provozovatele drážního systému, legislativních dozorujících a schvalujících institucí. V současné době platné nové revize souboru norem

ČSN EN 5012x dávají jistou naději k preciznějšímu vyjasnění a konkretizaci jednotlivých požadavků. Do jaké míry budou tyto požadavky bez problému naplnitelné, se musí prokázat až v následujícím období.

Použitá literatura

[1] ČSN EN 50126-1:2001 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS).*

[2] ČSN EN 50128:2003 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Software pro drážní řídicí a ochranné systémy.*

[3] ČSN EN 50129:2003 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Elektronické zabezpečovací systémy.*

Specifikace zákazníka a požadavky na bezpečnost drážního zařízení

Ing. Martin Tomášek

Elektroline a.s., Praha

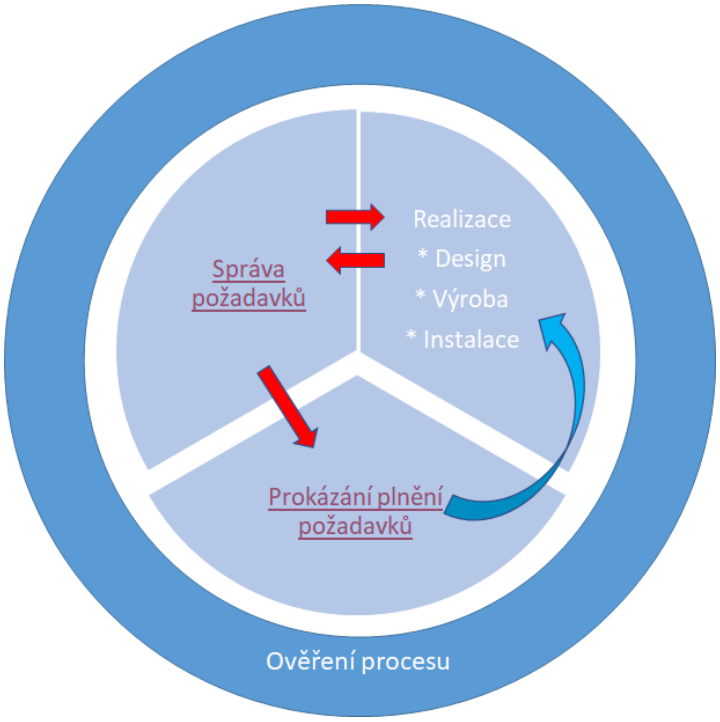
e-mail: tomasek@elektroline.cz; www.elektroline.cz

1 Úvod

Společnost Elektroline a.s. se zabývá projektováním, výrobou, dodávkou a montáží celého sortimentu armatur, tramvajových přestavníků, trolejbusových výhybek a také elektrických či elektronických zařízení. Dodává systémy trakčního vedení a systémy řízení a signalizace pro tramvaje a trolejbusy.

Při řešení zakázek se společnost stále častěji setkává s požadavky zákazníků na plnění norem EN 50126-1 [1] a EN 50126-2 [2]. Z toho důvodu se musí zabývat implementací postupů RAMS do svých procesů. To klade značné nároky na odbornou kvalifikaci pracovníků a nastavení příslušných procesních postupů (organizační směrnice, pracovní instrukce, vzory dokumentů, příklady analýz z řešených projektů).

V tomto příspěvku je popsána významná část aktivit spojených procesem vytvoření požadavků na systém a prokázání splnění požadavků na systém. Ten je nedílnou součástí procesu realizace systému, viz obr. 1.



Obr. 1: Schéma procesu realizace systému

Při realizaci systému je uskutečňována řada aktivit, včetně aktivit RAMS. S ohledem na rozsah a důvěrnost informací, nejsou v tomto příspěvku výsledky aktivit prezentovány.

2 Projekt Ost002

V roce 2017 získala společnost Elektroline kontrakt na dodávku zabezpečovacího systému tramvajového provozu v dopravním uzlu vlakového nádraží v belgickém přístavním městě Ostende. Lokalita dodávky je uvedena na obr. 2.

Obr. 2: Lokalita tramvajového terminálu Ostende

Naplnění kontraktu je řešeno projektem s interním označením Ost002. Předmětem dodávky jsou níže uvedené celky.

Základní charakteristiky systému jsou uvedeny v následujícím přehledu.

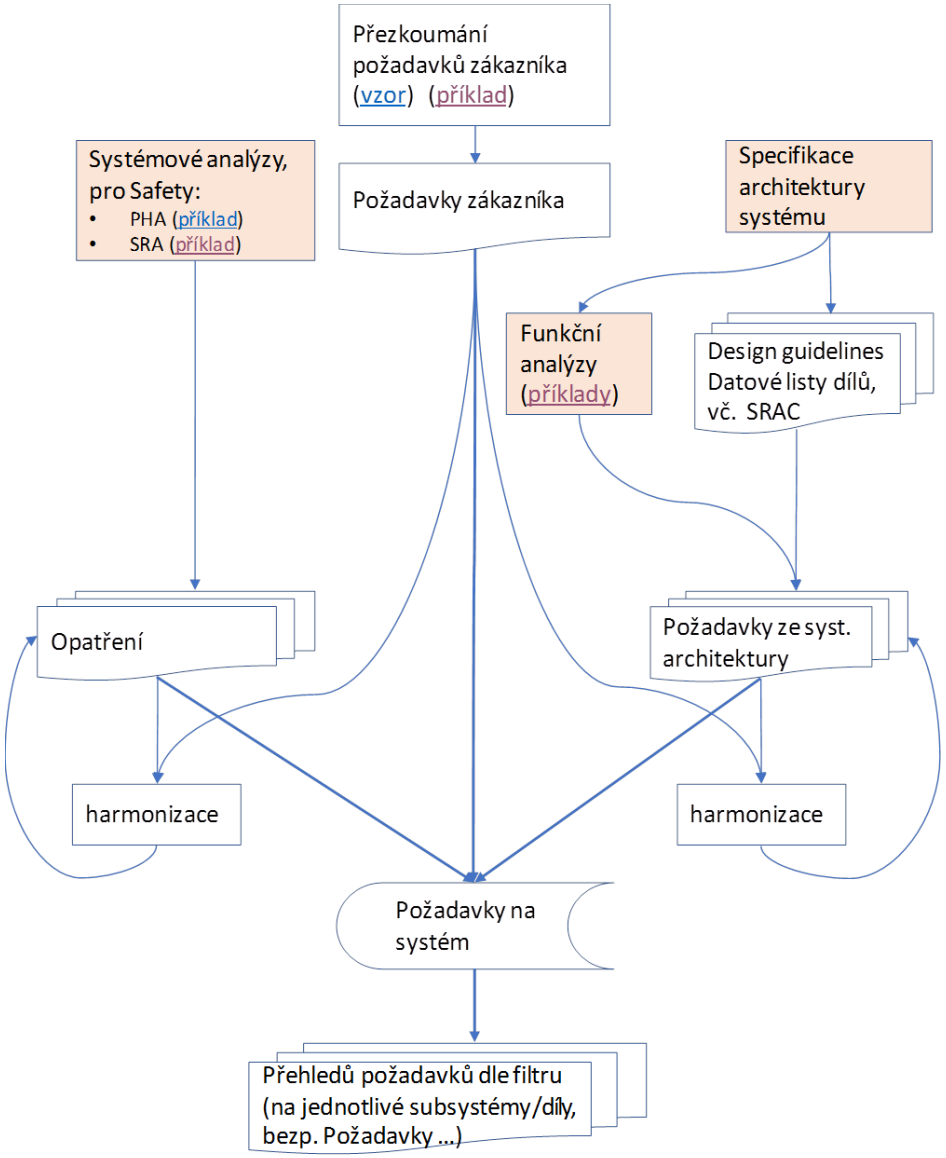
- Dopravní uzel:
  - přestup z vlakového nádraží na MHD,
  - 4 tramvajová nástupiště,
  - 5 křížení s ostatními účastníky silničního provozu,
  - příjezd ze 2 směrů,
  - bypass.
- Požadované vlastnosti:
  - zajištění automatického průjezdu uzlem,
  - postupné uvolňování sekcí,
  - jízda v obou směrech po všech kolejích,
  - couvání,
  - varování ostatních účastníků silničního provozu,
  - funkční bezpečnost na úrovni SIL3,
  - vzdálená správa z dispečinku vzdáleného cca 80 km
  - náhradní trasy v případě odstavené sekce,
  - doplňkové funkce (vyhřívání výhybek, kamerový dohledový systém).
- Rozsah systému:
  - 11 vstupních bran,
  - 19 výhybek,
  - 80 kolejových obvodů,
  - 35+8 sekcí.

Technická specifikace zákazníka (technická příloha dokumentace výběrového řízení) je zpracována:

- jako ucelená a komplexní (cca 80 stran včetně obrázků),
- požadavky sepsány jako běžný text strukturovaný do kapitol a odstavců, ve kterém je řada požadavků formulována implicitně a je třeba pochopit a převést do explicitní podoby,
- v jazyce vlámském (nizozemsky).

3 Požadavky na systém

První z klíčových podmínek úspěchu při realizaci projektu je zvládnutá správa požadavků na dodávaný systém. Správa požadavků zajišťuje, aby mezi všemi v projektu zúčastněnými stranami panovala shoda na všech charakteristikách dodávaného systému. Mapu procesu správy požadavků na systém, který je aplikován na Ost002 znázorňuje obr. 3. Proces pracuje se třemi hlavními zdroji požadavků na systém, které jsou popsány v odstavcích 3.1 – 3.3.



Obr. 3: Mapa procesu/dokumentace pro správu požadavků

3.1 Analýza požadavků zákazníka

Postup přezkoumání požadavků zákazníka je realizován v několika postupných krocích, viz přehled.

- Překlad technické specifikace zákazníka.
- Rozdělení komplexních požadavků na dílčí požadavky a jednoznačná identifikace (označení) všech požadavků pro další zpracování.
- Třídění požadavků na základě čeho se požadavek týká (např. bezpečnosti), přičemž zjištěno:
  - 860 požadavků zákazníka,
  - z toho 95 požadavků se vztahem k bezpečnosti.
- Hodnocení splnitelnosti požadavků.

Výstupy z přezkoumání požadavků zákazníka slouží společnosti Elektroline jako:

- podklady pro jednání se zákazníkem (vyjasnění/upřesnění požadavku),
- podklady pro potvrzení (např. odsouhlasení bezpečnostních požadavků mezi dodavatelem, zákazníkem a ISA),
- vstup do databáze požadavků na systém.

3.2 Požadavky vyplývající z analýz systému

Analýza rizik dopravního systému zákazníka, nebyla Elektroline předána. Nicméně její výstupy se promítly do formulace bezpečnostních požadavků v technické specifikaci zákazníka. Společnost Elektroline provedla vlastní analýzu rizik, jejímž výstupem je soubor opatření, která tvoří další část požadavků na systém.

Aby v požadavcích na systém nedocházelo k duplicitám, je potřeba harmonizovat požadavky z analýz se stávajícími požadavky zákazníka. Tak byl celkový počet 81 bezpečnostních požadavků vyplývající z analýzy rizik redukován na 48 požadavků.

3.3 Požadavky vyplývající z architektury systému

Předmětem dodávky celku (dále jen systému) je soubor dílčích subsystémů včetně příslušných stavebních částí. Architektura systému popisuje koncepci řešení, tedy rozčlenění systému do subsystémů a klíčových komponent, jejich rozhraní, výběr technologie.

Výběr technologie automaticky generuje soubor požadavků vyplývající z charakteristiky vybrané technologie. Řada z nich jsou požadavky na ostatní komponenty systému, ale jsou zde i požadavky směřující na celkový systém. V oblasti bezpečnosti jsou to podmínky použití se vztahem k bezpečnosti SRAC (Safety-Related Application Conditions). Tyto požadavky je potřeba vytřídit podle konkrétního způsobu použití technologie v systému. Při identifikaci těchto požadavků se s velkou výhodou můžeme opřít o „architektonický“ dokument Konstrukční rozpad.

Další požadavky na systém jsou výstupy (stanovená opatření) funkčních analýz. Nezbytným „architektonickým“ dokumentem pro provedení funkčních analýz je Funkční model systému (funkční rozpad), který stanoví identifikaci funkcí systému, včetně jejich vztahů a základních charakteristik.

Při doplňování požadavků na systém o požadavky ze systémové architektury je opět potřeba předejít duplicitám a to harmonizací, viz odstavec 3.2.

3.4 Databáze požadavků na systém

Databáze požadavků na systém sdružuje všechny požadavky na systém, včetně jejich kategorizace a je zdrojem podkladů pro další činnosti plnění projektu. Databáze požadavků slouží:

- k potvrzení všech bezpečnostních požadavků s nezávislým posuzovatelem bezpečnosti ISA (Independent Safety Assessor),
- pro formulaci vstupních požadavků při specifikaci požadavků na komponenty systému,
- jako podklad pro plán verifikace a validace systému.

4 Prokázání plnění požadavků na systém

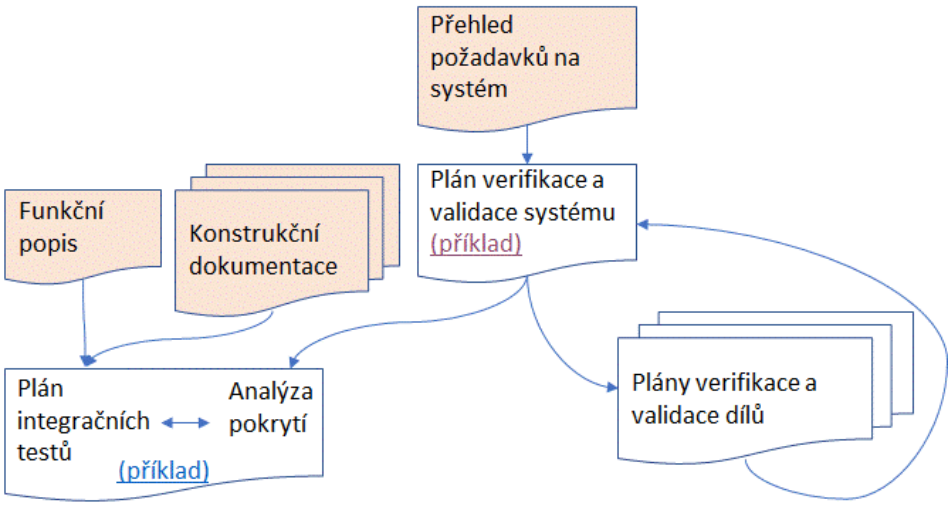
Prokázání plnění požadavků na systém probíhá ve 3 krocích:

- plánování,
- prokazování,
- validace.

Základní popis jednotlivých kroků a vzájemných souvislostí je uveden v následujících odstavcích.

4.1 Plánování

K plánování prokázání plnění požadavků na systém slouží Plán verifikace a validace systému. Zkoušky prováděné simulací na integračním vzorku FAT (Factory Acceptance Test) a zkoušky prováděné formou testu finálního systému SAT (Site Acceptance Test) jsou pak naplánovány v Plánu integračních testů. Vztahy mezi jednotlivými dokumenty při plánování znázorňuje obr. 4.



Obr.4: Dokumentace plánování

Plán verifikace a validace systému

Plán verifikace a validace systému přiřazuje každému požadavku na systém způsob prokázání plnění, milník projektu, kdy musí k prokázání dojít, předmět, na kterém k prokázání dojde, akceptační kritérium, v jakém dokladu bude výsledek zaznamenán a odpovědnost za

prokázání plnění požadavku. Výtah ze záhlaví plánu verifikace a validace systému je na obr. 5.

Column explanation		
Verification/Validation plan	Item	Requirement number derived from requirement source: CR... customer requirement SRA ... risk analysis ER ... requirements comming from the next project development PME ... point machine SRAC
	Requirement	Requirement description
	V/V	primary selection Verification or Validation
	Method	Method of verification/validation document review - review of Ost002 design document check - review of external document check tech. - investigation of real solution, mostly on site inspection - complex investigation of real solution on site examination - test on final sample simulation - test on the sample, where are certain parts of the tested function implemented by simulation V/V of child requ. - too complex requirements cannot be verified/validated individually, they are verified/validated by verification/validation of all they child requirements For more detail explanation please refer to chapter 4.6. and 4.7. in the Safety plan Ost002 SP EID00000400
	Milestone	Project milestone, when the requirement shall be verified/validated
	Object	Object of verification/validation
	Criterion	Acceptance criterion(s)
	Evidence	Document(s) where evidence of verification/validation result shall be registered
	Responsibility	A project role responsible for verification/validation activity for role description refer to Ost002_project team or Ost002 Safety plan

Obr.5: Dokumentace plánování

Plán integračních testů

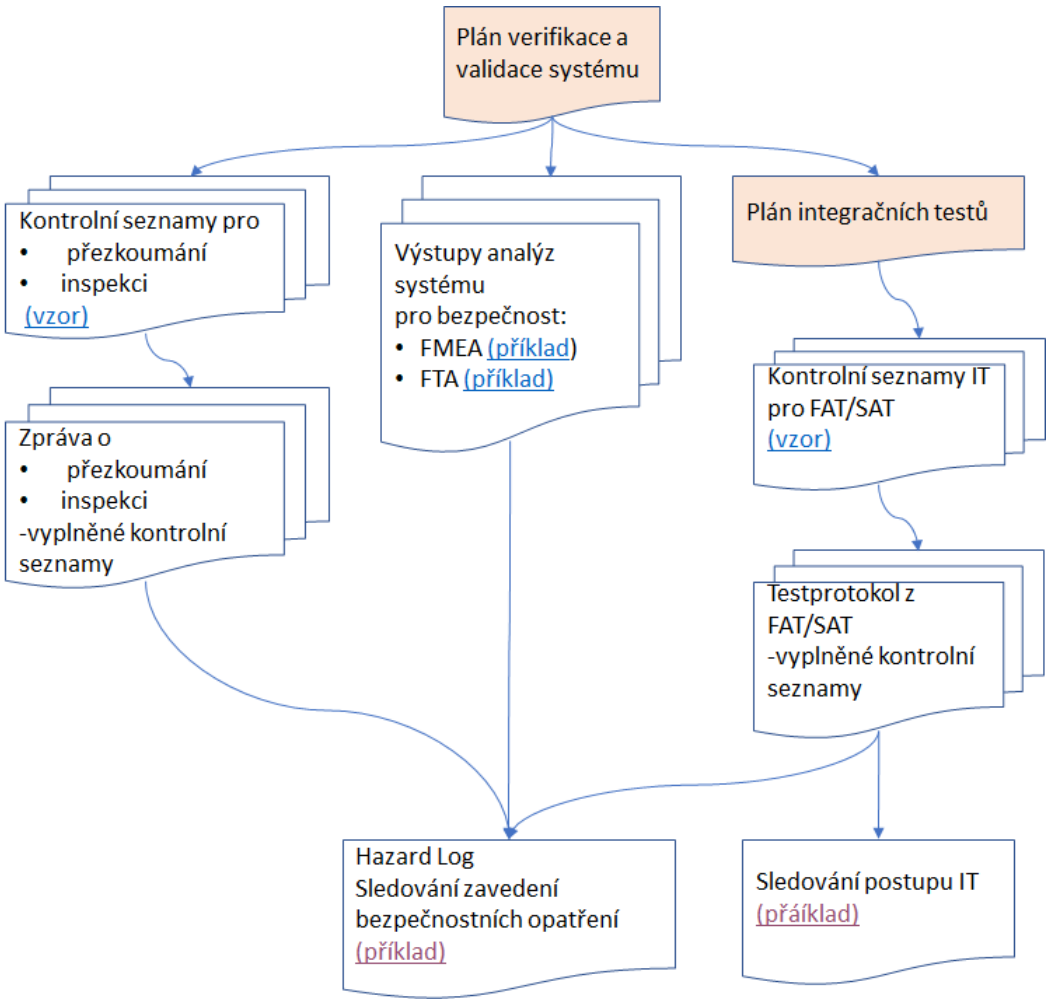
Plán integračních testů specifikuje zkoušky prováděné simulací na integračním vzorku FAT a zkoušky prováděné formou testu finálního systému SAT. Kromě postupu a akceptačních kritérií specifikuje „prostředí testů“ použitá zařízení, simulátory, změny vzorku oproti realitě a další. Podkladem pro sestavení Plánu integračních testů je Funkční popis systému a jeho konstrukční dokumentace.

Pro validaci Plánu integračních testů slouží analýza pokrytí. Podkladem pro analýzu pokrytí je seznam všech požadavků na systém, jejichž plnění je prokazováno simulací, nebo testem finálního systému.

4.2 Prokazování

Prokazování plnění požadavků na systém se provádí řadou způsobů, viz, řádek *Method* na obr. 5. Pro různé typy přezkoumání a inspekcí slouží kontrolní seznamy. Prokazování plnění funkčních požadavků probíhá při integračních testech, které se řídí Plánem integračních testů. Prokazování plnění bezpečnostních požadavků je založeno na analýzách způsobů a důsledků poruch FMEA (Failure Mode and Effect Analysis) a analýzách stromu poruchových

stavů FTA (Fault Tree Analysis). Pro přehled o postupu prací při prokazování plnění požadavků je praktické jej zaznamenávat. K tomu slouží záznam nebezpečí Hazard Log (pouze plnění požadavků na bezpečnost) a Sledování postupu integračních testů (pouze ověření funkčních požadavků). Vztahy mezi jednotlivými dokumenty při prokazování znázorňuje obr. 6.



Obr.6: Dokumentace prokazování

Prokazování plnění požadavků na úroveň integrity bezpečnosti SIL bezpečnostních funkcí systému a funkcí souvisejících s bezpečností je založeno na výpočtu přípustné intenzity nebezpečí THR (Tolerable Hazard Rate). To je prokázáno analýzami FMEA a FTA.

Pro každou bezpečnostní funkci systému je provedena analýza FMEA, která má za cíl určit, jaké módy poruch vedou k nebezpečnému nedetekovatelnému selhání funkce. Analýza FMEA je přizpůsobena účelu prokazování, tj. je vykonána na vhodné úrovni funkčního rozčlenění systému, kdy k příslušné funkci se přiřazují jednoznačně specifikovaná zařízení (fyzické objekty vedené jako položky).

Ke každé položce analýzy FMEA bezpečnostní funkce systému je uvedeno:

- identifikace a specifikace položky,
- funkce položky,
- způsob (mód) poruchy,
- příčina poruchy,

- důsledek poruchy,
- kategorie poruchy (bezpečná, nebezpečná),
- detekovatelnost poruchy (detekovatelná, nedetekovatelná),
- prostředek pro detekování poruchy,
- výsledná kategorizace poruchy položky (bezpečná detekovatelná, bezpečná nedetekovatelná, nebezpečná detekovatelná, nebezpečná nedetekovatelná),

Poznatky z FMEA vstupují do následné analýzy FTA, ve které se nejprve vytvoří logický model selhávání příslušné bezpečnostní funkce v podobě stromu poruchových stavů. Vrcholovou událostí je nebezpečné nedetekovatelné selhání bezpečnostní funkce. Pro výpočet THR se do modelu bezpečnostní funkce zadávají hodnoty intenzity nebezpečných nedetekovatelných poruch (λ_{DU}). Zdrojem dat jsou jednak vlastní sběr a vyhodnocení dat o provozu a poruchách Elektroline a dále údaje z katalogových listů či certifikátů výrobců.

4.3 Validace

Validace plnění požadavků je souhrnná zpráva, jak proběhly dílčí úkony v rámci prokázání plnění požadavků. Vhodným podkladem dokumentování průběhu validace jsou statistiky postupu prací, např. Sledování postupu integračních test a přehledy schválených dokumentů.

Ohledně validace plnění požadavků na bezpečnost je souhrnnou zprávou důkaz bezpečnosti v normativní struktuře dle ČSN EN 50129 [3].

5 Závěr

Ke konci září 2019 byla výroba systému Ost002 dokončena, proběhly integrační testy na úrovni FAT, systém byl nainstalován, a začaly integrační testy na úrovni finálního systému (SAT). Díky důkladné přípravě očekáváme plánované ukončení zkušebního provozu systému a jeho předání do plného provozu začátkem roku 2020.

Použitá literatura

[1] ČSN EN 50126-1 ed. 2:2019 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Generický proces RAMS.*

[2] ČSN EN 50126-2:2019 *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti.*

[3] ČSN EN 50129:2003 *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy pro zpracování dat – Elektronické zabezpečovací systémy.*

ISBN xxxxxxxxxxxxx
Zkušenosti s aplikací RAMS podle normy ČSN EN 50126-x
Sborník přednášek
kolektiv autorů
1. vydání
rok vydání 2019, Česká společnost pro jakost
vazba brožovaná, 29 stran