Vybrané problémy certifikace bezpečnostního systému

Materiály z 82. semináře Odborného centra Spolehlivost,
konaného dne 13. 9. 2022 v Praze

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

Obsah

Funkční analýza a FMECA ochranného systému

Ing. Jaroslav Zajíček, Ph.D.

TUL, Fakulta mechatroniky, informatiky a mezioborových studií, Studentská 2,

Liberec 461 17

email: jaroslav.zajicek@tul.cz

1. Úvod

Konkurenceschopnost prvků bezpečnostních systémů závisí mimo jiné na dosažené úrovni integrity bezpečnosti (Safety Integrity Level - SIL). Dosaženou úroveň integrity bezpečnosti lze certifikovat inspekčním orgánem, a tím uživatelům bezpečnostních prvků garantovat kvalitativní i kvantitativní parametry požadované normou.

Seminář je zaměřen na vybrané části procesu certifikace SIL ochranného systému turbíny společnosti ZAT a.s., tento příspěvek se věnuje funkční analýze systému a analýze FMECA, na kterou v dalším příspěvku přímo navazuje kvantitativně provedená analýza stromu poruchových stavů (FTA). Certifikace probíhala podle požadavků norem řady ČSN EN 61508 ed.2:2011.

2. Stručný popis systému

Ochranný systém turbíny TPS (Turbine Protection System) vykonává dohled nad provozem funkčního technologického celku – parní turbíny – z pohledu jejího bezpečného provozu. Provádí nepřetržitý sběr a vyhodnocení provozních informací/hodnot. V případě překročení povoleného rozsahu těchto provozních hodnot zabezpečí ochranný systém řízené a bezpečné odstavení technologického funkčního celku z provozu.

Sběrem a vyhodnocením provozních informací/hodnot se rozumí periodické čtení a zpracování signálů ze snímačů v technologii.

Odstavení technologického zařízení z provozu se provádí zavřením uzavíracího ventilu (rychlozávěrný ventil turbíny) na přívodním parovodu. Rychlozávěrný ventil (RZV) je řízen hydraulicky tlakem oleje. Výchozí polohou RZV (bez tlaku RZ oleje) je poloha zavřeno (v této poloze je ventil udržován silou pružiny). Při provozu turbíny je RZV udržován ochranným systémem turbíny v otevřeném stavu. Vazbu mezi elektrickým výstupem ochranného systému a hydraulicky ovládaným RZV zprostředkovává elektro-hydraulický výběrový člen 2oo3. Tento E-H výběrový člen (blok rychlozávěru) je vybaven trojicí solenoidů elektricky ovládaných napájecím napětím +24V. Jsou-li alespoň 2 ze 3 těchto solenoidů sepnuty napětím +24V (log. 1), prochází E-H výběrovým členem RZ olej, který svým tlakem udržuje RZV v otevřené poloze. E-H výběrový člen 2oo3 tak kromě vazby elektro-hydraulické zajišťuje zároveň vazbu trojnásobného výstupního rozhraní ochranného systému na jeden RZV. Akční zásah ochranného systému spočívá v přerušení přívodů napájecího napětí +24V k jednotlivým solenoidům E-H výběrového členu. E-H výběrový člen rychlozávěru (jeho solenoidy) tak tvoří akční člen ochranného systému turbíny. Zásahový signál má charakter negativní logiky (angl. de-energize to trip).

Ochranný systém turbíny zabezpečuje následující funkce:

- Napájí 3 solenoidy/elektromagnetické ventily (3 samostatné kanály) elektro-hydraulického výběrového členu/bloku (2oo3). Tlak oleje na výstupu elektro-hydraulického výběrového bloku přímo působí na rychlozávěrný ventil turbíny (uzavírací ventil vstupní páry na přívodním parovodu).
- Na základě informací ze snímačů monitoruje/vyhodnocuje provozní podmínky technologického zařízení (parní turbíny). Při překročení povolených limitů stanovených pro provoz technologického zařízení aktivuje ochrannou funkci* – uzavření RZV. Ochranný signál (zásah ochranného systému) způsobí přerušení (prostřednictvím výkonových spínačů) napájení každého jednotlivého elektromagnetického ventilu elektro-hydraulického výběrového bloku. To má za následek pokles tlaku oleje (jeho odpuštění) na výstupu výběrového bloku, čímž dojde k uzavření RZV.
- Diagnostiku provozu technologického zařízení – tj. sběr a distribuci technologických signálů důležitých z pohledu funkce ochranného systému
- Vlastní autodiagnostiku** – tj. diagnostiku poruch a provozních stavů týkajících se vlastního zařízení rozvaděče ochranného systému

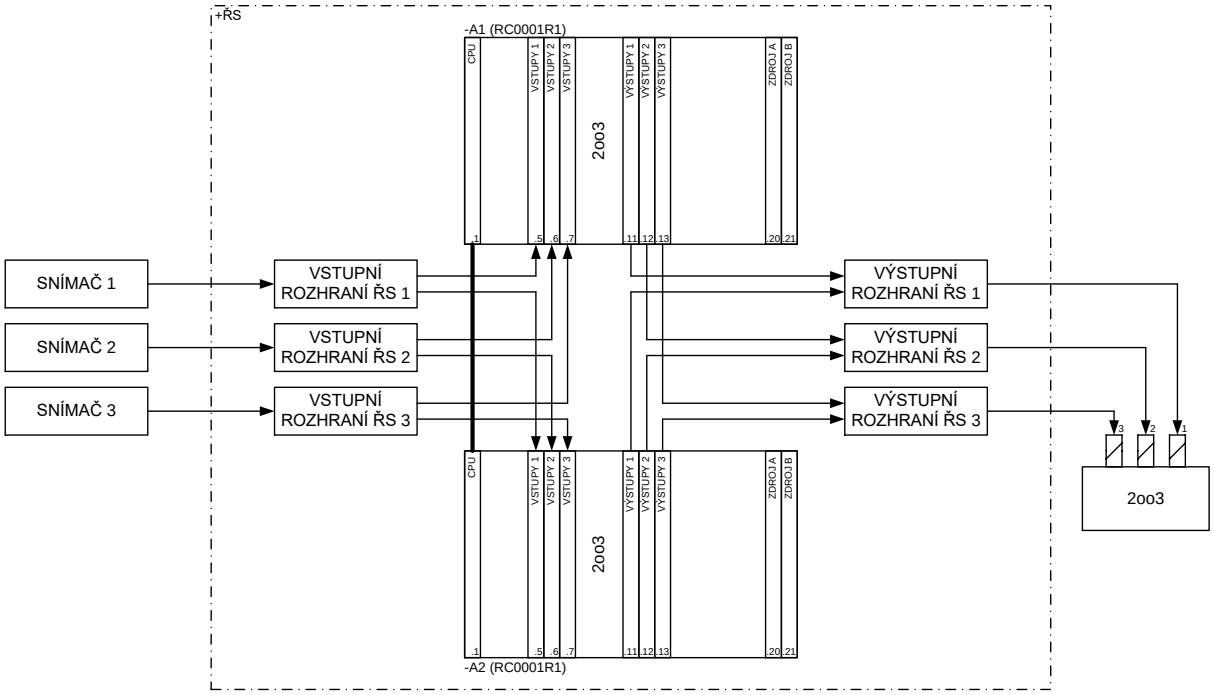
* Ochranný systém zajistí bezpečné vykonání ochranné funkce:

- výběru z analogového signálu 1 z 1
- výběru z analogových signálů 1 ze 2
- výběru z analogových signálů 2 ze 3
- výběru z analogových signálů 1 ze 4 (příp. jiného způsobu zpracování analog. signálů)
- výběru z analogových signálů 2 ze 4 (příp. jiného způsobu zpracování analog. signálů)
- výběru z analogových signálů 1 ze 9 (příp. jiného způsobu zpracování analog. signálů)
- výběru z analogových signálů 1 ze 12 (příp. jiného způsobu zpracování analog. signálů)
- výběru z binárního signálu 1 z 1
- výběru z binárních signálů 1 z 2
- výběru z binárního signálu 2 z 3

** Diagnostika poruch a provozních stavů týkajících se vlastního zařízení rozvaděče ochranného systému zahrnuje:

- diagnostiku napájecích obvodů rozvaděče
- diagnostiku pomocných obvodů rozvaděče
- systémovou diagnostiku

Jádrem ochranného systému turbíny je elektronický programovatelný automatizační systém (PLC) ZAT SandRA Z102. Je umístěn ve skříni rozvaděče ochranného systému KS65. Programovatelná část ochranného systému turbíny je koncipována jako plně redundantní. Sestává ze dvou identických sestav / subsystémů (-A1 a -A2). Každá ze sestav je modulární, tvořená sadou zásuvných elektronických desek. Obě tyto sestavy pak sdílejí společné připojovací rozhraní HW signálů (vstupů/výstupů), viz obr. 1.



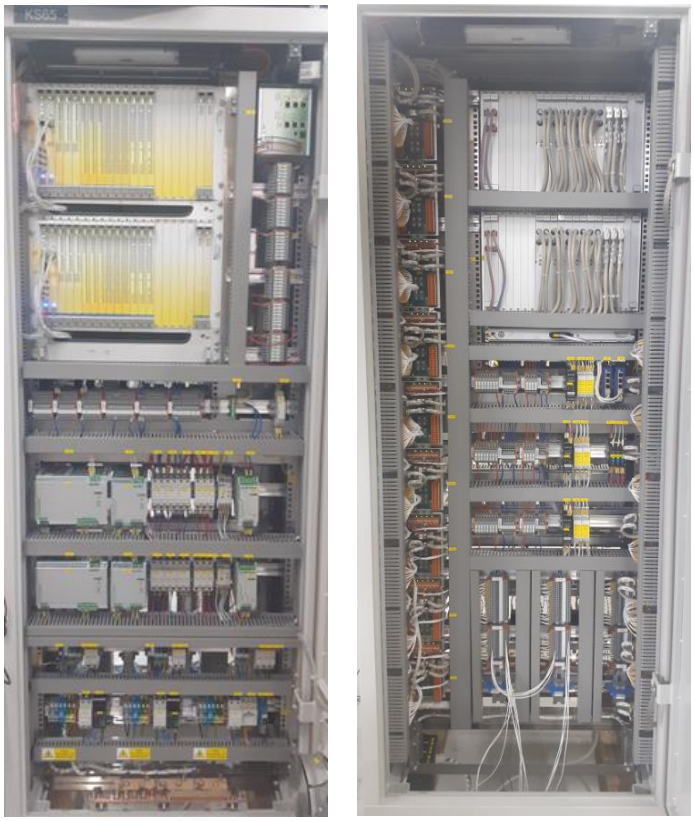
Obr. 1: Koncepce TPS

Vstupní připojovací rozhraní zajišťuje rozbočení každého vstupního signálu do obou sestav ŘS (informace z každého snímače je tak shodně nasdílena do obou subsystémů). Tím je zajištěno, že obě sestavy pracují s identickou množinou vstupních signálů. S touto množinou vstupních signálů je v obou subsystémech prováděno stejné algoritmické zpracování. Je-li tatáž vstupní veličina (informace) snímána vícenásobně (vícenásobnými snímači jedné fyzikální veličiny), je v rámci ochranného systému turbíny zajištěno, že je každý měřící kanál zpracován odděleným/nezávislým měřícím řetězcem (vstupní připojovací svorkovnice -> HW modul připojení vstupního signálu -> propojovací kabel -> adaptér vstupního signálu -> vstupní deska systému). Celý systém je navržen tak, že předpokládá trojnásobné vstupní rozhraní, tj. tři nezávislé kanály HW vstupů.

Každá ze sestav systému (-A1, -A2) generuje na základě algoritmického zpracování vlastní množinu výstupních signálů. Společné výstupní připojovací rozhraní zajišťuje sloučení každého výstupního signálu z obou sestav do výsledného sumárního signálu (realizuje tak pro každý výstupní signál funkci výběru 1oo2). Výstupní rozhraní ochranného systému je rovněž navrženo jako tříkanálové. Každý kanál výstupního rozhraní ovládá jeden solenoid E-H výběrového členu 2oo3. Každý kanál je zpracován rovněž odděleným/nezávislým řetězcem (výstupní deska systému -> propojovací kabel -> HW modul připojení výstupního signálu -> výstupní připojovací svorkovnice). Tato koncepce dvou identických sestav se společným trojnásobným připojovacím rozhraním HW signálů (graficky znázorněná na obrázku 1) výrazně zvyšuje odolnost ochranného systému turbíny vůči jednoduché poruše.

Hlavní/řídicí obvody ochranného systému turbíny jsou napájeny napájecím napětím 230VAC 50Hz ze dvou samostatných přívodů vnějšího napájení. Třetí přívod vnějšího napájecího napětí 230V 50Hz je použit pro napájení pomocných obvodů rozvaděče (servisní zásuvka, dveřní ventilátory, osvětlení). Pro zajištění elektrického napájení všech prvků ochranného systému turbíny je v rámci rozvaděče ochranného systému KS65 vytvořena vnitřní napájecí/zdrojová část. Napájecí/zdrojová část rozvaděče zajišťuje převod napěťové úrovně přívodního napájecího napětí 230V AC 50Hz na napěťové úrovně 48V DC a 24V DC potřebné pro napájení prvků ochranného systému turbíny.

Celá sestava ochranného systému umístěného ve skříni rozvaděče KS65 je zachycena z přední a zadní strany skříně na obr. 2.



Obr. 2: Sestava TPS v rozvaděči KS65

3. Použité metody

3.1 PCA

Při aplikaci postupu PCA se vychází z předpokladu, že porucha kteréhokoliv prvku způsobí nefunkčnost celého systému. Tento předpoklad je značně konzervativní, neboť de facto uvažuje celý systém jako složený z prvků v sériovém spolehlivostním uspořádání. Na druhou stranu dává tato metoda výpočtu celkové spolehlivosti systému velmi konzervativní odhad spolehlivosti. Reálný systém tedy bude mít lepší spolehlivostní charakteristiky, než jsou vypočteny pomocí metody počítání z dílů.

Při přijetí předpokladu spolehlivostně sériového uspořádání komponent v systému platí pro pravděpodobnost bezporuchového provozu sytému, složeného z N komponent:

$$R_S = R_1 \cdot R_2 \cdot \cdots \cdot R_N = \prod_{i=1}^{N} R_i$$

kde R je pravděpodobnost bezporuchového provozu.

To lze na základě znalosti vztahu $R = e^{-\lambda \cdot t}$ rozepsat jako:

$$R_S = e^{-\lambda_1 \cdot t} \cdot e^{-\lambda_2 \cdot t} \cdot \ldots \cdot e^{-\lambda_N \cdot t} = e^{-(\lambda_1 + \lambda_2 + \cdots + \lambda_N) \cdot t}$$

kde λ je intenzita poruch [h^{-1}],

t je čas provozu [h].

Důsledkem rozpisu pravděpodobnosti bezporuchového provozu pro systém je možnost vypočítat intenzitu poruch systému pouze ze znalosti intenzit poruch jednotlivých komponent jako jejich prostý součet.

$$\lambda_{sys} = \lambda_1 + \lambda_2 + \cdots + \lambda_N = \sum_{i=1}^{N} \lambda_N$$

Intenzita poruch je snadno převoditelná do ukazatele střední doby mezi poruchami MTBF [h], a to vztahem:

$$MTBF = \frac{1}{\lambda}$$

Výše uvedené vztahy platí za předpokladu exponenciálního rozdělení pravděpodobnosti poruchy. Tento předpoklad je pro elektronické prvky / systémy obecně přijatelný.

3.2 FMEA / FMECA

Analýza FMEA (resp. FMECA) je strukturovaná spolehlivostní analýza, sloužící ke zjištění způsobů poruch systémů, jejich příčin a důsledků. V současnosti je FMEA jednou z nejpoužívanějších metod analýz spolehlivosti a je využívána nejen v technických oborech. Je popsána v normě ČSN EN IEC 60812:2019 Analýza způsobů a důsledků poruch (FMEA a FMECA).

U každého prvku analyzovaného systému jsou vybrány potenciálně možné způsoby poruch, ať už jsou příčiny jejich vzniku jakékoliv, a je určen důsledek na funkci v různých úrovních členění systému. Je využíván induktivní postup řešení problému, tedy postup od nejjednodušších prvků analyzovaného systému směrem k nadřazeným úrovním. Díky identifikaci možných způsobů poruch a jejich příčin je pak snazší hledat účinná opatření, jak těmto poruchovým stavům předcházet nebo je zcela eliminovat.

Celý postup analýzy je možné formalizovat do jednoduchého a srozumitelného pracovního formuláře.

Při analýze jsou všechny prvky systému na zvolené nejnižší úrovni podrobeny systematickému zkoumání. Tuto nejnižší úroveň je třeba nejdříve určit dekompozicí systému (neboli tzv. konstrukčním rozpadem systému), kdy zkoumaný systém postupně členíme na menší celky. Ty jsou pak v poslední fázi rozděleny na nejjednodušší prvky (komponenty). Počet úrovní, na které je systém členěn, je však individuální a záleží na složitosti systému a požadované hloubce analýzy. Důležité je se při konstrukčním členění soustředit na hranice jednotlivých celků, aby byly navzájem disjunktní.

V následujícím kroku je nutné pro všechny prvky na zvolené nejnižší úrovni (tedy komponenty) specifikovat funkci, identifikovat dominantní způsoby (módy) poruch, příčiny, následky a v případě kvantitativní analýzy i pravděpodobnost nastoupení těchto poruch a další požadované údaje.

Následky se mohou určovat v několika úrovních systému, a to v úrovních, které odpovídají vytvořenému konstrukčnímu členění. U poruchového stavu komponenty tedy určujeme nejen selhání funkce samotné komponenty, ale i vliv této poruchy na funkce vyšších úrovní členění. Pouhé přímé určení vlivu na funkce samotného systému může způsobit opomenutí některých funkčních vazeb.

V případě přiřazení kvantitativních ukazatelů spolehlivosti jednotlivým způsobům poruch komponent (obvykle intenzita poruchy, frekvence nebo pravděpodobnost) je možné vyhodnotit souhrnné ukazatele pro systém nebo jeho části.

3.3 Dekompozice systému a Funkční analýza

Prvním krokem je vytvoření stromové struktury členění celého systému, a to až na úroveň elektronických komponent, pro které jsou dostupné (dohledatelné) intenzity poruch prvku, respektive středních dob mezi poruchami MTBF (Mean Time Between Failures).

Rozpad ochranného systému turbíny byl proveden do 5 úrovní:

- Systém (celý ochranný systém turbíny)
- Subsystém (vana)
- Deska (deska, kabel nebo skříň včetně společného napájení)
- Funkční blok (část desky, která je specifická plněním konkrétní funkce v rámci desky)
- Komponenta (elektronické a další součástky, ze kterých jsou jednotlivé funkční bloky sestaveny)

Systém se sestává z téměř 500 různých typů prvků, celkem se jedná o více než 10 tis. fyzických kusů prvků.

Podrobná funkční analýza byla provedena pro úroveň funkčních bloků. Každému funkčnímu bloku (přibližně 300 funkčních bloků v rámci systému) tedy byly specifikovány funkce, které funkční blok plní v rámci celku desky. Jednalo se například o funkce jako:

- Zpracovat vstupní signál
- Validovat vstupní signál
- Zajistit napájení
- Autodiagnostikovat
- Měřit teplotu
- Uchovávat provozní informace
- atd.

Každé funkci byla také přiřazena kategorie funkce, a to z následujících možnosti:

- Bezpečnostní - odstavuje
- Bezpečnostní - odstavuje podmíněně
- Diagnostická - technologie
- Diagnostická - řídicí systém
- Ostatní

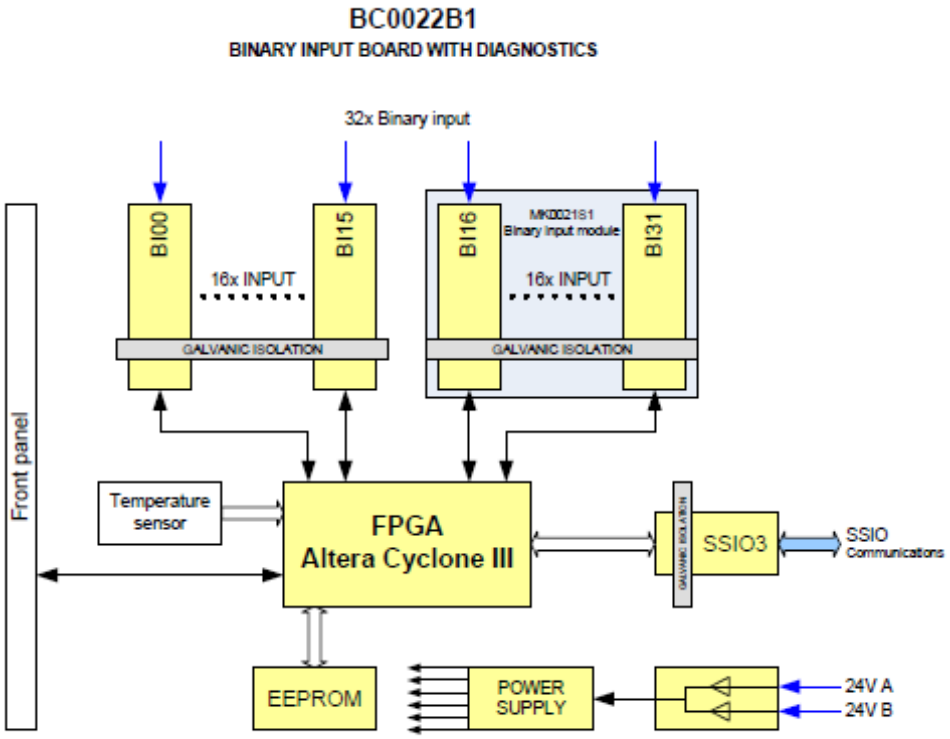
Specifikace funkcí umožnilo přiřadit komponenty (elektronické prvky) jednotlivým funkčním blokům. Vliv poruch na funkce vyšších úrovní členění bylo řešeno až v rámci samotné analýza FMECA.

Během přiřazování komponent jednotlivým funkcím bylo zjištěno, že některé komponenty se podílejí na plnění více funkcí. To způsobuje to, že celková intenzita poruch desky počítaná z funkčních bloků může být vyšší než intenzita poruch desky počítaná přímo z úrovně komponent. Tento nesoulad je na straně konzervativnosti a jeho vliv je poměrně zanedbatelný (týká se pouze menší části desek a zároveň odchylka je v nízkých desítkách procent).

Tab. 1: Příklad vlivu poruchy komponent na funkce desky

Deska	Funkční blok	Označení dle výkresové dokumentace	Funk. 1	Funk. 2	Funk. 3	Funk. 4	Funk. 5	Funk. 6
BC0022B1	BI00	C401	x	x				
BC0022B1	BI00	C402	x	x				
BC0022B1	BI00	C403	x	x		x		x
BC0022B1	BI00	C404	x				x	x
...	...	...						

Uvedený příklad se týká desky s elektronikou BC0022B1, což je deska zpracování binárních vstupů (32 kanálů s diagnostikou) a funkční blok BI00 je určen pro jeden z 32 kanálů pro binární vstup, viz obr. 3.



Obr. 3: Funkční bloky desky BC0022B1

4. Intenzity poruch komponent a vyšších celků

Ke stanovení spolehlivostních ukazatelů systému jako celku a jeho nižších úrovní členění získaných dekompozicí je nutné přiřadit všem komponentám (nejnižší úroveň dekompozice) vhodný ukazatel spolehlivosti. Jedná se konkrétně o intenzitu poruchy λ [h^{-1}] nebo střední dobu provozu mezi poruchami MTBF [h].

Pro tyto dva ukazatele platí, za předpokladu exponenciálního rozdělení doby do poruchy (pro elektronické součástky je tento předpoklad běžný), tento vztah:

$$\lambda = \frac{1}{MTBF}$$

Z toho vyplývá, že pro každou komponentu stačí evidovat jeden ukazatel a druhý lze dopočítat. Toho je využito i v případě, kdy některý výrobce nebo katalog spolehlivosti elektronických součástek udává jako ukazatel intenzitu poruchy a jiný udává střední dobu provozu mezi poruchami.

Ukazatele k jednotlivým typům komponent byly získány z následujících zdrojů:

- Katalogové listy výrobce
- Elektronické databáze konkrétních výrobních typů komponent
- Předchozí analýzy FMEA (dokumentace ÚJV apod.)
- Obecné databáze spolehlivosti elektronických součástek
- Expertní odhad

V procesu získání ukazatelů měly prioritu katalogové listy výrobce. V případě nedostupnosti bylo následně přistoupeno k možnostem v pořadí daném výše uvedeným seznamem.

Elektronické komponenty, které jsou funkčně i konstrukčně obdobné, byly seskupeny a tvoří tzv. typové komponenty, kterým byl následně přiřazen ukazatel spolehlivosti.

Tab. 2: Příklad intenzit poruchy typových komponent je obsahem tabulky níže.

Typ komponenty	**Intenzita poruchy [h^{-1}]**	**Zdroj**	**Výrobce**
Ethernet switch - SPIDER 5TX EEC	9,20E-07	Výrobce	Hirschmann
Filtr - EMI 1206	3,30E-07	Externí dok.	API Delevan
Filtr - FIAM1CF1	3,30E-07	Externí dok.	Vicor
Integrovaný obvod - 74HC1G14GV	6,60E-09	Výrobce	NXP Semiconductors
Integrovaný obvod - AD7980ARMZ	2,20E-09	Výrobce	Analog Device
Integrovaný obvod - ADP2118	1,10E-09	Výrobce	Analog Device
...	...	...	...

Na základě provedené dekompozice systému a stanovení typových komponent včetně přiřazení intenzity poruch je možné vyčíslit souhrnnou intenzitu poruchy pro vyšší celky členění. K tomu je použit standardní předpoklad metody PCA, tzn., že každý z prvků nižší úrovně členění způsobí svojí poruchou poruchu nadřazeného celku.

5. Analýza systému metodou FMECA

Analýza byla provedena dle standardních postupů uvedených v 3.2. Byla využita dekompozice až do detailu úrovně funkčních bloků. Každému způsobu poruchy funkčního bloku odpovídal jeden řádek tabulky s následujícími sloupci, viz tabulka 3.

Tab. 3: Popis sloupců analýzy FMECA

A	ID	Jednoznačný identifikátor řádku
B	Deska	Označení desky, kabelu, příslušenství; jedná se o 1. úroveň členění systému
C	Funkční blok	Označení funkčního bloku; jedná se o 2. úroveň členění systému
D	Intenzita poruch	Intenzita poruch funkčního bloku; jedná se o hodnotu získanou z provozních dat (pokud byla k dispozici), nebo pomocí predikce metodou PCA
E	Intenzita poruch – Poznámka	Obsahuje informaci o zdroji Intenzity poruchy ve sloupci D
F	Funkce	Popis funkce Funkčního bloku
G	Způsob poruchy	Možné poruchy úrovně Funkční blok; každý funkční blok může mít jeden nebo více způsobů poruch
H	Pravděpodobnost způsobu poruchy	Vyjadřuje pravděpodobnost daného způsobu poruchy za předpokladu, že nastala porucha funkčního bloku; součet pravděpodobností všech způsobů poruch konkrétního funkčního bloku dává zpravidla 100 %, ale mohou nastat situace, že součet je vyšší než 100 %; důvodem je to, že porucha elektronického prvku funkčního bloku může způsobit nastoupení více způsobů poruch; pro funkční bloky, u kterých bylo pravděpodobnost způsobu poruchy obtížné odhadnout, byla zpracována detailní analýza vlivu poruch základních prvků na funkce funkčního bloku
I	Intenzita způsobu poruchy	Intenzita poruchy daného způsobu poruchy funkčního bloku; výpočtová buňka, která je dána součinem Intenzity poruchy (sloupec D) a Pravděpodobnosti způsobu poruchy (sloupec H)
J	Využito v této realizaci	Metoda FMEA byla realizována i na částech, které nejsou součástí analyzovaného systému Z102, z důvodu možného budoucího použití; relevantní řádky pro systém Z102 lze získat filtrem na „Ano“
K	Následek - Deska	Popis projevu poruchy Funkčního bloku na funkci Desky
L	Následek - Subsystém	Popis projevu poruchy Funkčního bloku na funkci Subsystému; v případě, že porucha způsobí pouze snížení redundance (zálohy), je to zaznamenáno v tomto poli
M	Odhalitelnost	Informace o odhalitelnosti poruchového stavu daného Způsobu poruchy

N	Prostředek odhalení	Popis způsobu odhalení poruchového stavu; v analýze byly použity varianty: Nelze odhalit, Offline (kontrola, při použití, tester), Online, Při inicializaci
O	DanDet	Pravděpodobnost, že Způsob poruchy způsobí nebezpečnou detekovatelnou poruchu na úrovni desky; nebezpečná porucha způsobuje neschopnost plnění funkce desky nebo snížení redundance části, která zajišťuje bezpečnostní funkci; detekovatelnost znamená okamžitou informaci o nastoupení Způsobu poruchy – tyto záznamy mají zpravidla Prostředek odhalení „Online“
P	DanUnd	Pravděpodobnost, že Způsob poruchy způsobí nebezpečnou nedetekovatelnou poruchu na úrovni desky; nebezpečná porucha způsobuje neschopnost plnění funkce desky funkce nebo snížení redundance části, která zajišťuje bezpečnostní funkci; nedetekovatelnost znamená, že se o poruše dozvíme až na základě kontroly nebo testu; tyto záznamy mají zpravidla Prostředek odhalení „Offline“
Q	SafeDet	Pravděpodobnost, že Způsob poruchy způsobí bezpečnou detekovatelnou poruchu na úrovni desky; bezpečná porucha způsobuje zpravidla falešnou reakci bezpečnostního systému nebo je zcela bez následku; detekovatelnost znamená okamžitou informaci o nastoupení Způsobu poruchy – tyto záznamy mají zpravidla Prostředek odhalení „Online“
R	SafeUnd	Pravděpodobnost, že Způsob poruchy způsobí bezpečnou nedetekovatelnou poruchu na úrovni desky; bezpečná porucha způsobuje zpravidla falešnou reakci bezpečnostního systému nebo je zcela bez následku; nedetekovatelnost znamená, že se o poruše dozvíme až na základě kontroly nebo testu; tyto záznamy mají zpravidla Prostředek odhalení „Offline“
S	DanDet na úrovni subsystému	viz sloupec „O“; týká se plnění funkce v rámci Subsystému
T	DanUnd na úrovni subsystému	viz sloupec „P“; týká se plnění funkce v rámci Subsystému
U	SadeDet na úrovni subsystému	viz sloupec „Q“; týká se plnění funkce v rámci Subsystému
V	SafeUnd na úrovni subsystému	viz sloupec „R“; týká se plnění funkce v rámci Subsystému
W	MRT	Střední doba do obnovy funkce po identifikaci poruchy; v hodinách
X	Test interval	Testovací interval pro poruchy, které nejsou zjistitelné „Online“; v hodinách
Y	Poznámka Det	Upřesnění způsobu identifikace poruchového stavu
Z	Deska Int DanDet	Intenzita nastoupení nebezpečné detekovatelné poruchy na úrovni Desky
AA	Deska Int DanUnd	Intenzita nastoupení nebezpečné nedetekovatelné poruchy na úrovni Desky
AB	Deska Int SafeDet	Intenzita nastoupení bezpečné detekovatelné poruchy na úrovni Desky

AC	Deska Int SafeUnd	Intenzita nastoupení bezpečné nedetekovatelné poruchy na úrovni Desky
AD	Sub Int DanDet	Intenzita nastoupení nebezpečné detekovatelné poruchy na úrovni Subsystému
AE	Sub Int DanUnd	Intenzita nastoupení nebezpečné nedetekovatelné poruchy na úrovni Subsystému
AF	Sub Int SafeDet	Intenzita nastoupení bezpečné detekovatelné poruchy na úrovni Subsystému
AG	Sub Int SafeUnd	Intenzita nastoupení bezpečné nedetekovatelné poruchy na úrovni Subsystému
AH	Sys Int DanDet	Intenzita nastoupení nebezpečné detekovatelné poruchy na úrovni Systému
AI	Sys Int DanUnd	Intenzita nastoupení nebezpečné nedetekovatelné poruchy na úrovni Systému
AJ	Sys Int SafeDet	Intenzita nastoupení bezpečné detekovatelné poruchy na úrovni Systému
AK	Sys Int SafeUnd	Intenzita nastoupení bezpečné nedetekovatelné poruchy na úrovni Systému
AL	ID lambda	Pomocná identifikace řádků pro analýzu FTA
AM	Způsob vyhodnocení na úrovni subsystému	Požadavek na zpracování v online diagnostice v aplikačním SW
AN	Odkaz na SW	Odkaz na výkres aplikačního SW zpracování požadavku v online diagnostice.

6. Výsledky analýzy

V rámci analýzy ve formuláři v MS Excel, který obsahoval všechna pole uvedená výše, bylo detailně zkoumáno téměř tisíc způsobů poruch. Pro každou desku, subsystém i celý systém byly dopočítány hodnoty intenzit poruch pro kategorie poruch:

- Nebezpečná detekovatelná
- Nebezpečná skrytá
- Bezpečná detekovatelná
- Bezpečná skrytá

Hodnoty vychází z intenzit poruch zaznamenaných ve sloupcích Z až AC.

Další dopočítané ukazatele byly SFF a DC, dále pak MRT a doba latence pro stanovení testovacích intervalů.

Ukazatele SFF a DC

SFF (Safe Failure Fraction) vyjadřuje podíl bezpečných poruch, přičemž do bezpečných poruch jsou zahrnuty i poruchy nebezpečné detekovatelné. Výpočet SFF se provádí dle vztahu:

$$SFF = \frac{DanDet + SafeDet + SafeUndet}{DanDet + DanUndet + SafeDet + SafeUndet}$$

DC (Diagnostic Coverage) vyjadřuje diagnostické pokrytí. Do výpočtu se zahrnují pouze nebezpečné poruchy, a to dle vztahu:

$$DC = \frac{DanDet}{DanDet + DanUndet}$$

U většiny desek byly dosaženy tyto parametry s hodnotou výrazně nad 90 %.

Doba opravy MRT

Ukazatel MRT (Mean Repair Time) udává dobu opravy dané poruchy. Tento čas nezahrnuje dobu latence (skrytosti poruchy) pro nedetekovatelné poruchy, jedná se tedy pouze o čas samotného servisního zásahu.

Bylo zjištění, že více než 70 % oprav je zrealizováno do 2 h, více než 97 % oprav je zrealizováno maximálně do 4 h a téměř 100 % oprav je zrealizováno do 8 h. Pouze jeden způsob poruchy výrazně převyšuje ostatní MRT, a to mechanické a elektrické poškození samotné skříně systému.

Doba latence

Pro stanovení průměrné doby obnovy, která pro nedetekovatelné poruchy obsahuje kromě doby opravy i střední dobu skrytosti poruchy (doba latence), bylo třeba v analýze stanovit testovací interval. Střední doba latence je pak polovinou testovacího intervalu. V analýze byly použity testovací intervaly uvedené v tabulce níže. Je uveden i počet způsobů poruch, kterých se daný testovací interval týká.

Tab. 4: Použité testovací intervaly

Test interval [h]	Počet způsobů poruch	Poznámka
0	733	Poruchy jsou detekovatelné online
720	36	Cca 1 měsíc
8760	52	Cca 1 rok
17520	123	Cca 2 roky
87600	31	Cca 10 let
1E+99	21	Testování se nerealizuje

Deklarované hodnoty střední doby opravy a středního testovacího intervalu pro jednotlivé analyzované způsoby poruch vstupují dále do analýzy FTA. Kromě intenzity poruchy jsou tyto ukazatele nezbytné pro stanovení ukazatelů pohotovosti systému.

7. Závěr

Provedení funkční analýzy a analýzy FMECA na ochranném systému turbíny v takovém rozsahu, aby bylo vyhovující pro následnou certifikaci, vyžadovalo pravidelné setkávání multiprofesního týmu, na kterém byly podrobně diskutovány projektové, funkční i spolehlivostní vlastnosti systému. Následná dokumentace byla pro certifikaci vyhovující a významným vedlejším benefitem celého procesu bylo vědomostní obohacení členů týmu o širší souvislosti řešení spolehlivosti a bezpečnosti díky náhledu do problematiky ostatních profesí.

Výpočet spolehlivostních parametrů pomocí FTA

Ing. Jan Kamenický, Ph.D.
Technická univerzita v Liberci, Oddělení spolehlivosti a rizik
e-mail: jan.kamenicky@tul.cz

1 Úvod

Pro prokazování parametrů spolehlivosti při stanovení úrovně integrity bezpečnosti (SIL) je vhodné použít metodu analýzy spolehlivosti, která uvažuje vnitřní logiku zapojení systému a umí vyhodnotit nejen nepohotovost analyzovaného systému, ale i další jeho spolehlivostní charakteristiky, jako zejm. frekvenci nastoupení poruchy. Tyto parametry jsou stěžejní při prokazování splnění požadavků normy ČSN EN 61508, kde jsou uvedeny požadavky na bezpečnostní systém v režimu nízkého a vysokého vyžádání právě jako určitá hranice PFD (pravděpodobnosti selhání na vyžádání, tedy nepohotovosti) a PFH (pravděpodobnosti selhání za hodinu, tedy přeneseně frekvence poruch).

Jako vstupní informace pro analýzu stromu poruchových stavů je nutné využít logická bloková schémata systému, kde je popsána logika zapojení systému včetně zálohování jednotlivých prvků systému. Dalším zdrojem dat jsou datasheety použitých komponent, obsahující spolehlivostní údaje prvků na nejnižších úrovních členění systému. V našem případě byly spolehlivostní údaje na úrovni karet/subsystémů sjednoceny v analýze FMECA, která předcházela modelování pomocí FTA.

Výstupem analýzy FTA má být prokázání splnění požadavků ČSN EN 61508 na patřičnou úroveň SIL, v prezentovaném případě se jednalo o SIL3. Za tímto účelem byly vypracovány logické modely pro bezpečnou i nebezpečnou poruchu. Složitost řešení spočívala dále v tom, že bezpečnostní systém měl být dle požadavků výrobce certifikován v několika různých způsobech zálohování – 1oo1, 1oo2 a 2oo3, a to jak na úrovni zálohování komponent/karet v subsystémech, tak na úrovni subsystémů. Jelikož se jedná o bezpečnostní systém, je pochopitelně navržen zejména účinně proti nastoupení nebezpečné poruchy. To znamená, že v případě využití zálohování je třeba uvažovat různou logiku systému ze spolehlivostního hlediska při modelování nebezpečné a bezpečné poruchy.

2 Analýza stromu poruchových stavů

V této kapitole bude stručně představena metoda analýzy stromu poruchových stavů.

Teorie spolehlivosti disponuje různými metodami hodnocení spolehlivosti systémů. Pomocí nich se predikují ukazatele bezporuchovosti nebo identifikují kritická místa systému, na která je pak možné aplikovat nápravná nebo ochranná opatření. Obecně lze analýzy spolehlivosti dělit na základě mnoha kritérií. Dělí se dle vhodnosti použití v jednotlivých etapách životního cyklu objektu, podle toho, zda jsou využity pravděpodobnosti nastoupení poruchy nebo je přístup deterministický atd.

Pro kvantifikaci hodnoty nepohotovosti události je vhodná metoda blokových diagramů bezporuchovosti (RBD) a analýza stromu poruchových stavů (FTA). Tyto dvě metody a jejich grafické zobrazení funkčního uspořádání systému jsou navzájem převoditelné, na základě možností použitého softwarového prostředku (RiskSpectrum PSA) byla zvolena metoda FTA.

Jedná se o deduktivní metodu, zaměřenou na zjištění příčin (zpravidla poruch) a jejich kombinací, vedoucích ke vzniku vrcholové události. Z uvedeného vyplývá, že v první fázi je metoda používána ke kvalitativní analýze spolehlivosti systémů a jeho logických vazeb. Pokud je analytik schopen vyčíslit parametry výskytu poruch (MTBF, MTTR, pravděpodobnost, testovací interval apod.), je ve druhé fázi metoda použita pro kvantitativní výpočet nastoupení vrcholového jevu.

Analýzu stromu poruch lze charakterizovat čtyřmi kroky:

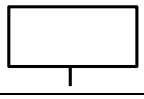
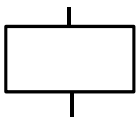
- Definování vrcholové události.
- Zjišťování příčin vzniku události a jejich logických vazeb na nejbližších nižších úrovních systému až do dosažení požadované nejnižší úrovně.
- Grafické zobrazení stromu poruch.
- Kvantitativní ohodnocení systému s možností stanovení minimálních kritických řezů.

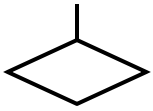
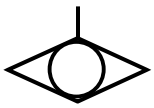
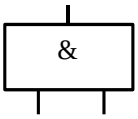
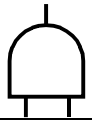
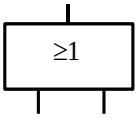
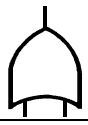
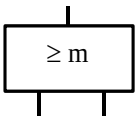
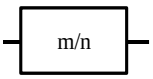
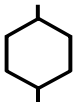
Za vrcholovou událost se zpravidla volí neprovozuschopný stav systému, neboť následná analýza není tolik rozsáhlá a je snáze proveditelná, než kdyby byla vrcholová událost reprezentována provozuschopným stavem.

Řešením analýzy stromu poruchových stavů je názorný a přehledný logický diagram, rozvíjející se shora dolů od vrcholové události k dalším jevům na nižší úrovni systému. Vazby mezi jednotlivými úrovněmi stromu jsou znázorněny normovanými (ČSN EN 61025) značkami, které jsou uvedeny v tabulce 2.1. Soubor těchto značek je dostačující k sestavení úplného stromu poruch. Pro kvantitativní výpočty se používá Booleova algebra a základní matematické operace, případně je vyčíslení možné pomocí příslušného softwarového prostředku. Normalizované značení není v současné době jediným používaným, téměř každá firma používá značení vycházející z její historie.

Pro každý systém je možné definovat celou řadu vrcholových událostí. Metodika analýzy stromu poruch nedovoluje analyzovat najednou více vrcholových událostí, každá vrcholová událost musí být analyzována v samostatném stromu poruch. Mezi možná zjednodušení analýzy patří tzv. transfery, resp. přenosy v rámci stromu poruch. Jev na nejnižší úrovni jednoho stromu poruch, tzv. „listí“ může být zároveň vrcholovou událostí jiného stromu poruch. Pak se jedná o tzv. „událost analyzovanou jinde“. Při používání přenosových bloků je třeba dbát na to, aby byla všechna místa výskytu přenášené události označena stejným symbolem a naopak, aby stejné poruchy různých prvků systému byly označeny různými symboly.

Tabulka 1: Schematické značky používané při grafickém znázornění stromu poruch.

Normovaná značka	**Alternativní značka**	**Název a popis**
		Blok s názvem nebo popisem vrcholové události (TOP jevu).
		Blok s názvem nebo popisem události (jevu), případně s uvedením pravděpodobnosti výskytu (pokud se to požaduje).
		Základní (primární) událost – událost, která se dále nedělí.

Normovaná značka	Alternativní značka	Název a popis
		Nerozvíjená událost – událost, která není dále rozvíjená (zpravidla proto, že se to nepovažuje za nutné).
		Událost analyzovaná jinde – událost dále rozvíjená v jiném stromu poruch.
		Přenos do – událost definovaná kdekoliv jinde ve stromu poruch.
		Přenos ven – opakovaná událost použitá kdekoli jinde ve stromu poruch.
		Hradlo AND (a) – událost nastane pouze tehdy, když současně nastanou všechny vstupní události.
		Hradlo OR (nebo) – událost nastane tehdy, když nastane kterákoliv vstupní událost, nebo jejich libovolná kombinace.
		Zálohovaná struktura – událost nastane tehdy, jestliže nastane minimálně m z n vstupních událostí.
		Hradlo INHIBIT (zdržení) – událost nastane pouze tehdy, když nastane vstupní událost a současně je splněna podmínka vyznačená uvnitř značky.

Takovýmto způsobem rozpadu systému je možné pokračovat až do zvolené nejnižší úrovně systému. Na každé úrovni analýzy musí být vyhledány a uvažovány všechny bezprostřední příčiny vzniku rozebíraného jevu, nelze tedy nějakou úroveň vynechat, vznikly by totiž potíže s logikou stromu poruch a vztahy mezi jednotlivými jevy. Pokud již není možné událost dále rozebírat, jedná se o základní událost. Pokud je ještě možné událost rozdělit na další podřazené události, a přesto to není provedeno, jde o událost nerozvíjenou. Rozhodnutí, zda událost dále analyzovat, je předem určeno hloubkou analýzy. Pokud strom poruch obsahuje na koncích „větví“ pouze události typu „základní událost“ nebo „událost analyzovaná jinde“, je kvalitativní část analýzy ukončena a výsledkem jsou kombinace všech možných poruch systému, vedoucí ke vzniku vrcholové události.

Jelikož cílem analýzy stromu poruch je nalezení všech rozumných kombinací poruch prvků systému, provádí se analýza kritických řezů. Kritickým řezem je konečná množina základních, dále nerozvíjených a jinde analyzovaných událostí, které, nastanou-li současně, vedou ke vzniku vrcholové události. Minimálním kritickým řezem stromu poruchových stavů rozumíme takovou konečnou množinu základních událostí, která je sama kritickým řezem, ale současně žádná její vlastní podmnožina kritickým řezem není.

Detialní informace o analýze stromu poruchových stavů jsou obsahem normy *ČSN EN 61025 – Analýza stromu poruchových stavů*.

3 Popis systému

Popis systému je uveden v přecházejícím příspěvku. Pro účely modelování a výpočty stromů poruchových stavů je nezbytné uvést, že systém byl analyzován ve více konfiguracích a variantách.

Konfigurací je myšleno zapojení řetězce a jeho složení z různých typů komponent, ovšem vždy při zachování logiky *připojovací modul, kabel, adaptér, vstupní karta, sběrnice, procesor, výstupní karta, kabel a připojovací modul*. Tyto konfigurace se lišily „pouze“ v hodnotách parametrů spolehlivosti komponent, které zastávaly svou funkci na patřičné pozici, proto jim dále nebudeme věnovat pozornost.

Variantou zapojení je myšlena vnitřní logika bezpečnostní funkce, tedy zjednodušeně řečeno úroveň zálohování. Ovšem struktura zálohování se měnila pouze u komponent, u kterých to bylo možné, tedy *připojovací modul, kabel, adaptér a vstupní karta*. Zbytek řetězce byl pro všechny varianty zapojení shodný. Přehled o počtu komponent na jednotlivých pozicích podle variant zapojení udává tabulka 2.

Tabulka 2: Počty komponent na pozicích dle varianty zálohování

Var.	Připoj. modul	Kabel	Adaptér	Deska vstupů	Sběrnice 1	Sběrnice 2	CPU	Deska výstupů	Kabel	Připoj. modul
1oo1	1	1	0	1	2	2	1	3	3	3
1oo2	2	2	0	2	2	2	1	3	3	3
2oo3	3	3	0	3	2	2	1	3	3	3

4 Poruchy se společnou příčinou

Pro zlepšení spolehlivostních ukazatelů funkce systému je možné využít zálohování. To může být provedeno na různých úrovních – zálohování komponent ve funkčním bloku, funkčních bloků na kartě, karet v subsystému až po úroveň zálohování subsystémů v rámci finálního dodávaného systému. V případě ochranného systému turbíny jde o zálohování 1oo1 (bez zálohy), 1oo2 (paralelní systém) a 2oo3 (výběrový systém). Při použití zálohování však může dojít ke ztrátě funkce vlivem poruch se společnou příčinou. Proto byly do modelu stromu poruchových stavů přidány primární události, reprezentující CCF na úrovni způsobů poruch a dále CCF subsystémů.

Velikost CCF závisí na mnoha faktorech, ovšem těmi dominantními jsou míra diagnostického pokrytí (DC) a podílu bezpečných poruch (SFF). Oba tyto parametry byly vypočteny na základě provedené analýzy FMECA.

Absolutní hodnoty intenzit poruch CCF byly určeny pomocí β-faktoru jako poměrná část intenzity poruch módu poruchy, ke kterému se CCF vztahuje. Velikost zmíněného poměru byla určena na základě ČSN EN 61508-6 ed. 2 [7] za pomoci tabulky D.1, Zde je uvedeno bodové ohodnocení (skóre) vlastností systému se vztahem k bezpečnosti. Pokud v tomto hodnocení systém určitou vlastnost splňuje, jsou mu přiznány body a na základě finálního bodového hodnocení je možno (podle tab. D.4 z [7]) určit tzv. β-faktor pro logické prvky a pro snímače a koncové prvky

Na základě dosaženého bodového skóre byla pro karty zajišťující logické operace zvolena hodnota β-faktoru na úrovni 2 % a pro senzory a koncové prvky na úrovni 5 %.

Pro názornost příspěvku je v tabulce 3 uvedena část bodovací tabulky D.1 s dosazenými bodovými hodnotami jedné vlastnosti systému.

Tabulka 3: Bodování programovatelné elektroniky nebo senzorů / koncových prvků (vybraná část tabulky D.1)

Položka	Subsystém logiky		Senzory a koncové prvky	
	X	Y	X	Y
Složitost/návrh (konstrukce)/použití/vyzrálost/zkušenost				
Vylučuje vzájemné propojení mezi kanály výměnu všech informací jiných, než jsou informace používané pro diagnostické testování nebo rozhodovací účely (hlasování)?	0,5	0,5	0,5	0,5
Je návrh založen na technikách použitých v zařízeních, které se už v dané oblasti úspěšně používají déle než 5 let?	0,5	1,0	1,0	1,0
Jsou více než pětileté provozní zkušeností se stejným hardwarem používaným v obdobných prostředích?	1,0	1,5	1,5	1,5
Jsou všechny vstupy a výstupy chráněny proti potenciálním úrovním přepětí nebo nadproudu?	1,5	0,5	1,5	0,5

5 Konfigurace a varianty

Jak bylo uvedeno v kapitole 3, systém byl analyzován ve více konfiguracích a variantách. Pro zpracování binárních signálu byly uvažovány čtyři konfigurace a pro zpracování analogových signálů byly uvažovány dvě konfigurace. Celkem tedy bylo uvažováno šest konfigurací (různých komponent na stejných pozicícha tři varianty zálohování (1oo1, 1oo2 a 2oo3). Tyto kombinace systému by znamenaly 3 x 6 = 18 možných zapojení systému. Ovšem výrobce chtěl certifikovat ochranný systém dle ČSN 61508 pro režim vysokého i nízkého vyžádání a kromě toho bylo třeba namodelovat chování systému s ohledem na bezpečné i nebezpečné poruchy. Tím se dostáváme k (18 x 2) +18 = 54 různým modelům stromů poruchových stavů.

Největším myšlenkovým problémem bylo uvědomit si chování systému v různých variantách zálohování při uvažování bezpečné a nebezpečné poruchy. U varianty 1oo1 je vše snadné – pokud dojde k jednoduché poruše, je v poruše celý systém a pouze na jeho nastavení závisí, zda jde o poruchu bezpečnou nebo nebezpečnou.

Nejsložitější variantou bylo překvapivě zálohování 1oo2 (paralelní zálohování). Při modelování nebezpečné poruchy, před kterou má ochranný systém chránit primárně, dojde k zapůsobení ochrany už při signálu z jednoho subsystému (větve), tedy obě větve se vzájemně zálohují a jednoduchá porucha nemá na funkci systému vliv. Oproti tomu při modelování frekvence falešných odstavení (bezpečné poruchy) je situace taková, že systém odstaví už při poruše jediné komponenty, která má za důsledek vydání alarmu. Oba subsystémy se tedy v tomto případě nezálohují. Navíc, čím složitější a více zálohované budou ochrany před nebezpečnou poruchou, tím častější bude i falešné odstavení od poruchy jediného prvku.

Při poslední uvažované variantě zálohování, výběrovém zapojení 2oo3, je již situace příznivější. Hlasovací logika tohoto zapojení eliminuje jednoduchou poruchu v případě modelování nebezpečné poruchy, ale i v případě jednoho falešného signálu je tento „přehlasován“ dvěma zbývajícími správně fungujícími subsystémy.

6 Modelování v RiskSpectrum

Pro účely modelování stromů poruchových stavů, reprezentujících logiku zapojení ochranného systému, byl zvolen SW nástroj RiskSpectrum. Jedná se o světově uznávaný produkt, používaný zejm. v jaderné energetice. Problémem (nikoliv SW, ale metody FTA obecně) je skutečnost, že pro každou vrcholovou událost musí být vytvořen samostatný model stromu poruchových stavů.

RiskSpectrum umožňuje tzv. parametrické zadávání spolehlivostních ukazatelů komponentám na spodní úrovni modelu stromu poruchových stavů. To znamená, že pokud je v modelech vícekrát obsažena typově stejná komponenta, je možné pouze odkazovat na parametr (typicky intenzitu poruch), uložený v databázi. Ovšem musí se zajistit jednoznačná identifikace fyzicky různých kusů komponent jednoho typu.

6.1 Primární události – způsoby poruch

Jako databáze dat pro ohodnocení parametrů spolehlivosti primárních událostí sloužila analýza způsobů, důsledků a kritičnosti poruch (FMECA), viz předchozí příspěvek Vlastní datová základna analýzy FMECA byla pro účely analýzy FTA převzata a doplněna o výběr relevantních způsobů poruch pro jednotlivé modelované situace.

Analýza FMECA obsahuje data, využitelná pro analýzu stromu poruchových stavů, zejména:

- intenzitu poruch způsobu poruchy – λ,
- střední dobu opravy – MRT,
- interval testování – TI.

RiskSpectrum umožňuje zadávat hodnoty těchto ukazatelů jednotlivým primárním událostem a následně z nich vypočte spolehlivostní charakteristiku těchto primárních událostí tak, že v případě poruchy odhalitelné online (nulová doba latence poruchy) je za střední dobu do obnovy (MTTR) považována hodnota MRT a v případě skryté poruchy, odhalitelné pouze pravidelným testováním funkce komponenty, je za hodnotu MTTR považována hodnota MRT + ½ TI. Zadávané vstupní hodnoty MRT a TI v tabulce 4 a tabulce 5.

Tabulka 4: Vstupní hodnoty středních dob opravy MRT (parametrické zadávání)

ID	Popis	Hodnota [h]
2H	2h	2,00E+00
4H	4h	4,00E+00
8H	8h	8,00E+00

Tabulka 5: Vstupní hodnoty intervalů testování TI (parametrické zadávání)

ID	Popis	Hodnota [h]
10 LET	10 let	8,76E+04
2 ROKY	2 roky	1,75E+04
MESIC	mesic	7,20E+02
ONLINE	online	0,00E+00
ROK	rok	8,76E+03
TYDEN	tyden	1,68E+02

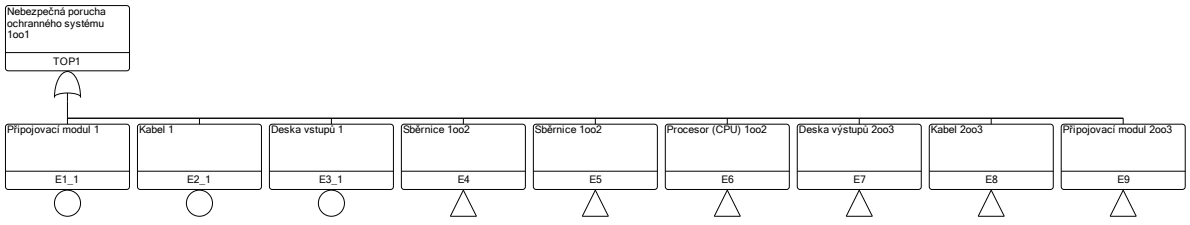
Příklad souboru zadávaných vstupních hodnot intenzit poruch λ je uveden v tabulce 6.

Tabulka 6: Vstupní hodnoty intenzit poruch λ (parametrické zadávání)

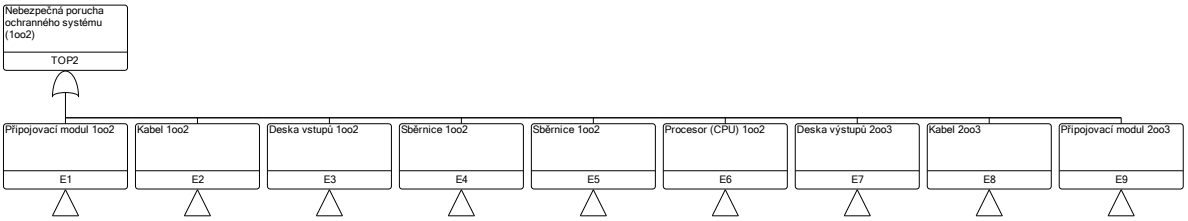
ID	Hodnota [h^{-1}]
108	1,25E-08
116	1,10E-06
12	1,00E-10
123	1,32E-06
137	8,80E-07
14	9,00E-07
156	6,60E-07
157	1,59E-08

6.2 Kvalitativní modely

Kvalitativní modely se liší v závislosti na variantě zálohování a tom, zda modelují bezpečnou nebo nebezpečnou poruchu. Modely FTA korespondují s konfiguracemi zapojení dle tabulky 2. Pro ilustraci zde budou uvedeny pouze 2 varianty zapojení.

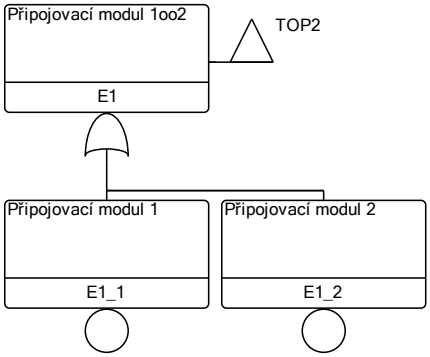


Obrázek 2: Model ochranného systému ve variantě 1oo1



Obrázek 3: Model ochranného systému ve variantě 1oo2

Pod hradlem přenosu je možné si vždy představit podstrom, odpovídající popisu, tedy např. paralelní zálohování v případě připojovacího modulu pro účely modelování nebezpečné poruchy (obrázek 3). Pro účely modelování bezpečné poruchy by bylo vrcholové hradlo tohoto podstromu změněno na AND.



Obrázek 4: Model zapojení dvou připojovacích modulů v logice 1oo2

6.3 Výsledky výpočtů

Pro všechny výše uvedené konfigurace a varianty zapojení ochranného systému byly provedeny výpočty nepohotovostí vrcholových funkcí a zároveň frekvencí nastoupení vrcholových událostí. Jako mezní hranice, určující (ne)splnění požadovaných parametrů, byly uvažovány hodnoty pro SIL3, viz tabulka 7.

Tabulka 7: Úroveň integrity bezpečnosti podle ČSN EN 61508-5

Úroveň integrity bezpečnosti (SIL)	Režim nízkého vyžádání PFDavg [1]	Režim vysokého vyžádání PFH [h^{-1}]
4	≥1E-5 až <1E-4	≥1E-9 až <1E-8
3	**≥1E-4 až <1E-3**	**≥1E-8 až <1E-7**
2	≥1E-3 až <1E-2	≥1E-7 až <1E-6
1	≥1E-2 až <1E-1	≥1E-6 až <1E-5

V režimu vysokého vyžádání byla vypočtena hodnota PFH, což je hodnota frekvence výskytu **nebezpečných** poruch. Tuto hodnotu není možné zaměňovat s hodnotou falešného zapůsobení ochranného systému.

Pro splnění požadavků na SIL3 je třeba dosahovat v režimu nízkého vyžádání hodnoty nepohotovosti nižší, než 10^{-3} [1] a pro režim vysokého vyžádání pak hodnot frekvence poruch

nižší než 10^{-7} [h^{-1}]. Výrobce se interně rozhodl deklarovat a splňovat tvrdší podmínky pro své ochranné systémy. Tyto hodnoty byly stanoveny na PFDavg = < 5.10^{-4} a PFH < 5.10^{-8} [h^{-1}].

Po dosazení všech hodnot do modelů stromů poruchových stavů byla v RiskSpectrum vypočtena hodnota nepohotovosti a frekvence pro každou vrcholovou událost. Výsledky jsou uvedeny v tabulce 8 a tabulce 9 za celý systém pro jednotlivé konfigurace zapojení.

Tabulka 8: Výsledky výpočtů nepohotovostí U (koresponduje s PFDavg)

Konfigurace	**Druh vstupního signálu**	**Varianta zapojení vstupního signálu**		
		1oo1	1oo2	2oo3
1	binární	2,89E-05	4,99E-06	5,04E-06
2	binární	2,89E-05	5,01E-06	5,05E-06
3	binární	3,83E-06	3,79E-06	3,79E-06
4	binární	6,66E-05	6,16E-06	6,18E-06
5	analogový	6,71E-05	6,39E-06	6,52E-06
6	analogový	6,70E-05	6,39E-06	6,52E-06

Z tabulky 8 je zřejmé, že systém s vysokou rezervou dosahuje hodnot požadovaných pro SIL3. Je to dáno vysokým diagnostickým pokrytím poruch a potlačením latence skrytých poruch. Numericky je systém schopen dosahovat SIL4. Avšak pro SIL4 je požadováno diverzní řešení systému. Zálohování formou redundance není pro SIL4 akceptovatelné.

V tabulce 9 jsou barevně zvýrazněny varianty a konfigurace zapojení ochranného systému, které nesplňují toto přísnější kritérium. Je třeba zmínit, že požadavky na SIL3 v režimu vysokého vyžádání jsou splněny i pro konfigurace 1 a 2 při zálohování 1oo1. Výrobce si však zadal přísnější numerické cíle, a proto jsou i tyto varianty zapojení hodnoceny jako nevyhovující. Pro všechny ostatní (barvou nezvýrazněné) varianty zálohování a konfigurace ochranný systém na hodnoty PFDavg a PFH specifikované výrobcem pro dosažení SIL3 a dané normou ČSN EN 61508-1 [2].

Tabulka 9: Výsledky výpočtů frekvencí výskytu nebezpečných poruch (koresponduje s PFH)

Konfigurace	**Druh vstupního signálu**	**Varianta zapojení vstupního signálu**		
		1oo1	1oo2	2oo3
1	binární	6,90E-08	2,39E-08	2,41E-08
2	binární	6,97E-08	2,45E-08	2,47E-08
3	binární	3,54E-08	2,29E-08	2,29E-08
4	binární	1,21E-07	2,50E-08	2,50E-08
5	analogový	4,13E-07	3,63E-08	3,65E-08
6	analogový	4,14E-07	3,71E-08	3,72E-08

Kromě požadavků, daných normou ČSN EN 61508 na funkční bezpečnost a její numerické hodnoty, byly pro analyzovaný systém specifikovány další spolehlivostní parametry:

systém musí vykonávat bezpečnostní funkce tak, aby střední doba provozu mezi bezpečnými poruchami (MTBF) byla pro každou bezpečnostní funkci větší než 5,00E+5 h,

systém musí dosahovat hodnotu ustálené (asymptotické) nepohotovosti (U) ze všech funkčních poruch (bezpečných i nebezpečných) menší než 5,00E-3,

systém musí u jednotek vyměnitelných na místě (LRU) dosahovat hodnoty střední doby opravy (MRT) menší než 4 h.

Pro účely tohoto článku je zajímavý požadavek v první odrážce, který de facto specifikuje povolenou frekvenci bezpečných poruch. I tento spolehlivostní ukazatel byl modelován a dokladován, viz výsledky uvedené v tabulce 10. Ve variantě zálohování 1oo2 je možné modelovat pouze frekvenci falešného zásahu pro jeden subsystém a tu dále násobit dvěma, protože falešné odstavení nastane při zapůsobení jediného subsystému.

Tabulka 10: Výsledky výpočtů frekvencí nastoupení bezpečné poruchy (falešného odstavení) pro jeden subsystém [h^{-1}])

Konfigurace	**Druh vstupního signálu**	**Varianta zapojení vstupního signálu**		
		1oo1	1oo2	2oo3
1	binární	2,64E-06	3,88E-06	1,45E-06
2	binární	2,64E-06	3,88E-06	1,46E-06
3	binární	1,40E-06	1,41E-06	1,39E-06
4	binární	3,08E-06	4,77E-06	1,47E-06
5	analogový	3,19E-06	4,55E-06	1,46E-06
6	analogový	3,19E-06	4,55E-06	1,46E-06

Podle požadavku má být MTBF bezpečných poruch vyšší, než 5E+5 [h]. Pokud vypočteme převrácenou hodnotu tohoto požadavku, dostaneme požadovanou maximální frekvenci nastoupení nežádoucí události – falešného odstavení. Přípustná hodnota frekvence je v tomto případě tedy < 2E-6 [h^{-1}]. Z porovnání hodnot vypočtených a hodnot požadovaných vyplývá, že požadavek na minimální MTBF bezpečných poruch celého systému **není splněn**. Při zapojení systému se vstupními signály v zálohování 2oo3 by frekvence bezpečných poruch dosahovala od obou subsystémů hodnoty cca 3E-6 [h^{-1}] (dvojnásobek hodnoty pro jeden subsystém), což odpovídá MTBF = 3,33E+5 h. Jedná se tedy o mírné neplnění specifikovaného spolehlivostního parametru.

7 Závěr

Účelem tohoto textu nebylo seznámit čtenáře s principy analýzy stromu poruchových stavů, ale ukázat možné nástrahy, které na tvůrce modelu strmou poruchových stavů čekají, pokud bude modelovat více variant jednoho systému, případně určí více vrcholových událostí téhož systému. Příspěvek shrnuje zkušenosti z reálného případu, který skončil udělením certifikátu SIL3 analyzovanému systému.

Použitá literatura

[1] ČSN IEC 60050-192: Mezinárodní elektrotechnický slovník - Část 192: Spolehlivost

[2] ČSN EN 61508-1 ed. 2: Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky

[3] ČSN EN 61508-2 ed. 2: Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností

[4] ČSN EN 61508-3 ed. 2: Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 3: Požadavky na software

[5] ČSN EN 61508-4 ed. 2: Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 4: Definice a zkratky

[6] ČSN EN 61508-5 ed. 2: Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 5: Příklady metod určování úrovní integrity bezpečnosti

[7] ČSN EN 61508-6 ed. 2: Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3

[8] ČSN EN 61025: Analýza stromu poruchových stavů (FTA)

Řízení procesů a dokumentace při certifikaci SIL

Ing. Miroslav Vaněček

ZAT a.s.

e-mail: miroslav.vanecek@zat.cz

doc. Ing. Pavel Fuchs, CSc.

Alopex, s.r.o.

e-mail: pavel.fuchs1@gmail.com

1 Úvod

Pokud chce výrobce řídicích systémů být konkurenceschopný, musí systematicky aplikovat procesy zajišťující dosažení vysoké úrovně spolehlivosti jeho výrobků. Jen tak může následně prokazovat splnění hodnot příslušných ukazatelů spolehlivosti.

Společnost ZAT, jakožto dodavatel řídicích systémů pro jadernou i klasickou energetiku a další průmyslová odvětví, se ve výběrových řízeních běžně setkává s tím, aby dokladovala spolehlivostní parametry bezpečnostních aplikací nejen podle standardů jaderné bezpečnosti, ale i podle standardů pro funkční bezpečnost (soubor norem ČSN EN 61508-x). Proto vedení společnosti přijalo rozhodnutí získat pro bezpečnostní funkce elektronického programovatelného automatizačního systému (PLC) založeného na platformě SandRA Z102 certifikaci pro úroveň bezpečnosti označovanou jako SIL3.

Analýzy spolehlivosti (nejen FMECA a FTA) a jejich doložení věrohodnými údaji jsou jen dílčí, byť nezbytnou, podmínkou certifikace SIL. Jsou důkazem, že jsou potlačeny náhodné poruchy bezpečnostního systému na přijatelnou úroveň. Pro potlačení systematických (nenáhodných) poruch je třeba dokladovat, že jsou dodrženy postupy pro jejich eliminaci v procesech jednotlivých etap životního cyklu bezpečnostního systému.

V následujících částech příspěvku je stručnou formou popsán přístup společnosti ZAT při řízení procesů a dokumentace při certifikaci SIL pro TPS.

2 Základní úvahy a rozvržení prací

V prvé řadě bylo třeba zvážit, zda úsilí pro SIL3 vynaložit na komerčním projektu (zakázce) ZAT, nebo na interním projektu zaměřeném na budoucí zakázky ZAT. Po zvážení rozsahu požadavků ČSN EN 61508-x se vedení společnosti se rozhodlo o zahájení vývojového projektu, na kterém by aplikovalo procesy řízení bezpečnosti a vypracovalo příslušnou dokumentaci pro hardwarové a softwarové řešení podle ČSN EN 61508-x. Výsledkem vývojového projektu měl být certifikát SIL3 pro funkční vzorek ochranného systému turbíny – TPS (Turbine Protection System) a získání zkušeností s aplikací funkční bezpečnosti.

Průběh prací na vývojovém projektu TPS potvrdil správnost tohoto rozhodnutí. A to zejména s ohledem na časovou náročnost procesů řízení bezpečnosti a vypracování příslušné dokumentace podle požadavků ČSN EN 61508-x.

Práce na projektu byly rozvrženy do dvou etap. První etapa (E1) měla za cíl zmapovat základní požadavky ČSN EN 61508-x [1 – 7] a z nich plynoucí nároky na řešení projektu. Druhá etapa (E2) byla zaměřena na realizaci hardwarové a softwarové části TPS a příslušné dokumentace potřebné k certifikaci SIL3.

3 Přípravná fáze – etapa E1

V rámci této etapy bylo třeba jednoznačně vymezit pojmy týkající se bezpečnosti a úlohy TPS v rámci řízeného zařízení. Dále bylo třeba stanovit rámcové požadavky na funkcionalitu a koncepci TPS z pohledu dosažitelnosti SIL3. A specifikovat základní požadavky na procesy a dokumentaci pro etapu E2.

3.1 Vymezení pojmů týkající se bezpečnosti a role TPS

Pojem „funkční bezpečnost“ je definován v ČSN EN 61508 jako *část celkové bezpečnosti týkající se řízeného zařízení, která závisí na správném fungování systémů E/E/PE souvisejících s bezpečností a na jiných opatřeních pro snížení rizika.*

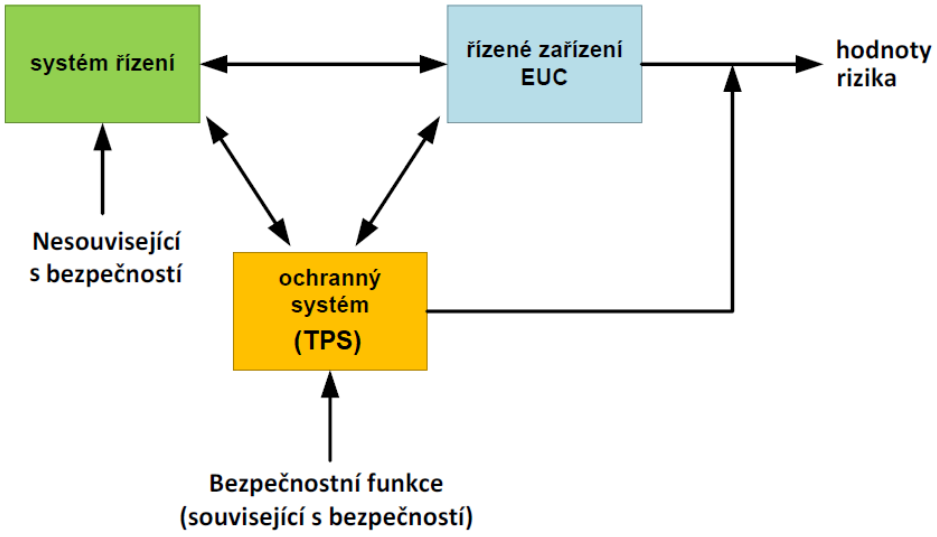
Vztahuje se k zajištění nebo udržení bezpečného stavu **řízeného zařízení** (EUC) prostřednictvím E/E/PE systémů. Z uvedené definice je zřejmé, že funkční bezpečnost se aplikuje **jen na systém související s bezpečností**.

Funkční bezpečnost se **nesmí zaměňovat s celkovou bezpečností.** Funkční bezpečnost je podmnožinou celkové bezpečnosti a technické bezpečnosti EUC. Funkční bezpečnost se vztahuje k bezpečnostní funkci (jedné či více), kterou vykonává E/E/PE systém související s bezpečností (SRS). Úroveň („kvalita“) funkční bezpečnosti je vyjádřena úrovněmi integrity bezpečnosti (SIL). Vztahuje se k zajištění nebo udržení bezpečného stavu **řízeného zařízení** (EUC) prostřednictvím E/E/PE systémů.

Pro pochopení souvislostí je třeba uvést některé základní pojmy a definice z ČSN EN 61508.

- Řízené zařízení (Equipment Under Control – EUC) – zařízení, stroj, přístroj nebo instance použité pro spojité i nespojité výrobní, dopravní, lékařské nebo jiné činnosti.
- Systém řízení EUC (EUC Control System) – systém reagující na signály z procesu anebo od operátora a vytvářející výstupní signály způsobující, že EUC pracuje požadovaným způsobem.
- Systém související s bezpečností (Safety-Related System – SRS) – navržený systém, který současně provádí požadované bezpečnostní funkce nezbytné pro dosažení nebo udržení bezpečného stavu v EUC.

Základní vazby mezi systémem řízení, řízeným zařízením (EUC) a ochranným systémem uvádí obrázek 1. Cílem celého uspořádání je dosáhnout předepsané (přijatelné) hodnoty rizika. Účinnost ochranného systému, která vede ke snížení rizika je číselnými vyjádřena hodnotami parametrů spolehlivosti v jednotlivých pásmech SIL. Aplikace SIL3 znamená, že ochranný systém snižuje riziko 1 000krát až 10 000krát, a to podle dosažených hodnot spolehlivosti.



Obrázek 5: Role TPS v rámci EUC

Systém řízení EUC je koncipován tak, že není systémem souvisejícím s bezpečností (SRS). Tolerovatelné/přijatelné hodnoty rizika EUC je dosaženo použitím ochranného systému. Ochranný/bezpečnostní systém je koncipován jako SRS.

Při tomto řešení nemusí být systém řízení EUC podroben požadavkům normy ČSN EN 61508, což vede k tomu, že základní řídicí funkce jsou realizovány levnějšími (necertifikovanými) řídicími prostředky. Bezpečnostní funkce jsou pak realizovány ochranným systémem se zaručenou úrovní spolehlivosti dokladovanou certifikáty SIL. Uspořádání podle obrázku 1 je charakteristické pro ochranné systémy používané v jaderné a klasické energetice a v petrochemických provozech. Tím je i vymezena role TPS jakožto ochranného systému.

3.2 Funkcionalita a koncepce TPS pro SIL3

Pro základní stanovení požadovaných bezpečnostních funkci TPS využil ZAT předchozí obchodní případy. Tyto specifikace zahrnovaly požadavky na různé typy vstupních signálů a způsoby jejich vyhodnocování (výběrové konfigurace) pro vydání povelů k akčnímu zásahu k odstavení EUC.

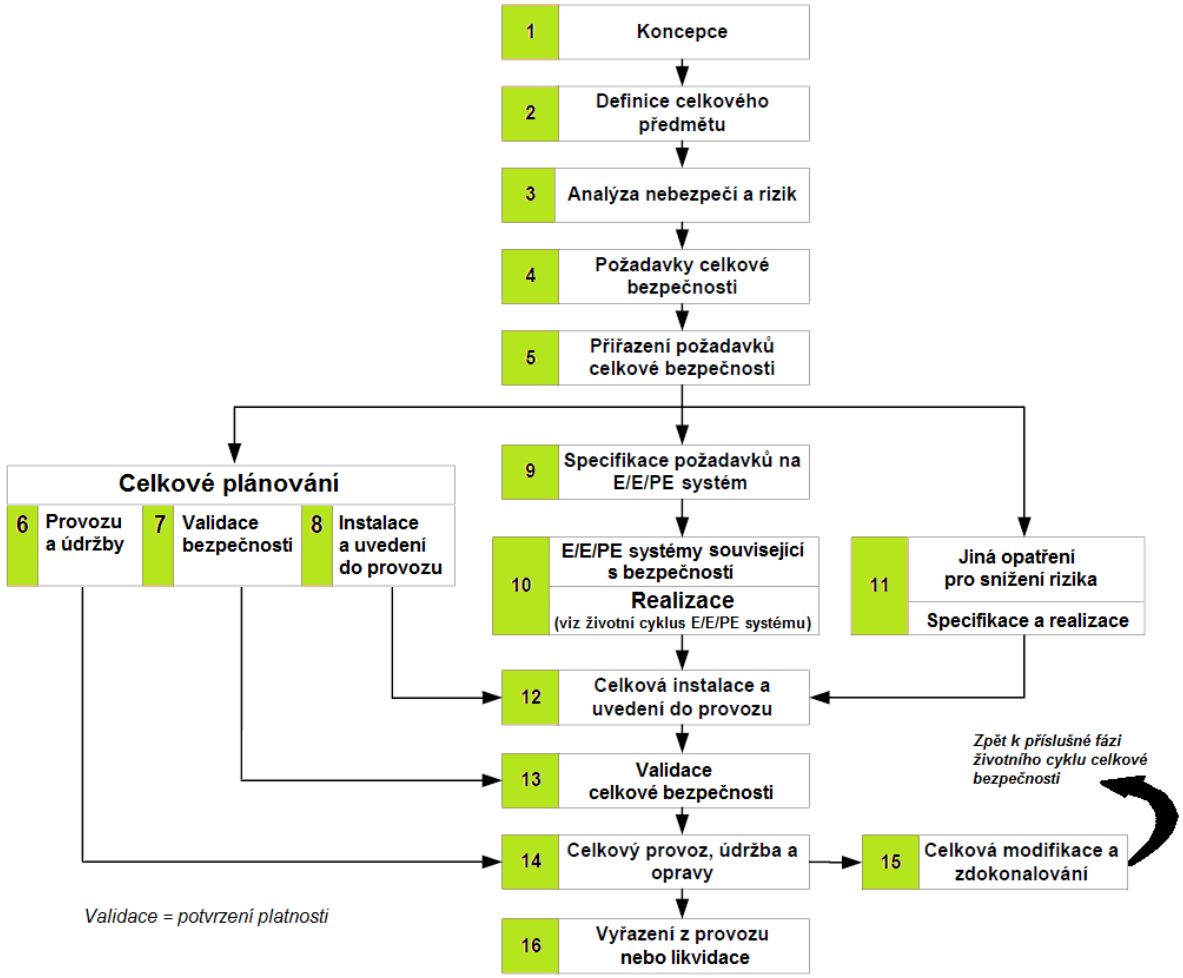
Pro realizace těchto bezpečnostních funkcí TPS bylo třeba zvážit, zda pro úroveň SIL3 budou postačovat dva identické vzájemně se zálohující subsystémy (vany s PLC) nebo bude třeba použít tři subsystémy. Na základě rámcového odhadu spolehlivosti bylo zvoleno řešení dvou vzájemně se zálohujících subsystémů. K tomuto odhadu posloužily dříve zpracované analýzy spolehlivosti základních modulů platformy SandRA Z102.

3.3 Aplikovatelné fáze životního cyklu bezpečnosti pro TPS

Při určování požadavků na funkční bezpečnost E/EPE systémů je třeba vycházet z celkové bezpečnosti EUC. Celková bezpečnost EUC se zabezpečuje řízením (managementem) procesů prostřednictvím životního cyklu celkové bezpečnosti, viz obrázek 2. Pro výrobce E/E/PE systémů souvisejících s bezpečností jsou podstatné fáze (etapy) 10 a 12. Je však třeba chápat souvislosti. Proto je vhodné chápat cíle fáze 9 a fází 12 až 16.

TPS se zcela týká fáze životního cyklu bezpečnosti 10 „Realizace E/E/PE systémů souvisejících s bezpečností“. V rámci této fáze také vznikají dokumenty potřebné pro fáze 12 až 16. Proto je třeba částečně aplikovat i fáze 12 až 16, které specifikují požadavky pro fázi 10. Dále pro fázi 10

je třeba specifikovat požadavky na TPS, které mají vznikat ve fázi 9. Proto se pro TPS částečně aplikují i požadavky z fáze 9.



Obrázek 6: Životní cyklus celkové bezpečnosti

3.4 Další uvažované aspekty

Při rozhodování o rozsahu prací a kapacit, které bude třeba použít pro etapu E2 bylo třeba dále zvážit následující aspekty.

- Interpretace norem funkční bezpečnosti. Zde se jednalo četné rozpory mezi originálním standardem IEC 61508-x a jeho harmonizovanou českou verzí ČSN EN 61508-x. V mnoha případech bylo třeba českou verzi upravit, aby formulace v ní použité dávaly smysl.
- Základní požadavky na procesy a dokumentaci pro etapu E2. K tomu byl vypracován seznam požadavků uvedených v ČSN EN 61508-1, 2 a 3. Protože že ZAT dodává své systémy do jaderné energetiky, kdy aplikuje vysoké nároky na procesy a dokumentaci, se usoudilo, že je možné převzetí či přizpůsobení stávající dokumentace ZAT a.s. pro účely funkční bezpečnosti dle požadavků ČSN EN 61508-x.
- Norma ČSN EN 61508-1 specifikuje pro různé úrovně funkční bezpečnosti míru nezávislosti. Pro bezpečnostní aplikace na úrovni SIL3 je třeba aplikovat princip "dvoje oči" a role pro verifikaci, validaci a nezávislé posouzení bezpečnosti. S ohledem na tuto skutečnost bylo rozhodnuto pro etapu E2 angažovat specialisty z Technické univerzity

v Liberci a společnosti Alopex, s.r.o., znalé analýz spolehlivosti a problematiky funkční bezpečnosti.

4 Realizační fáze – etapa E2

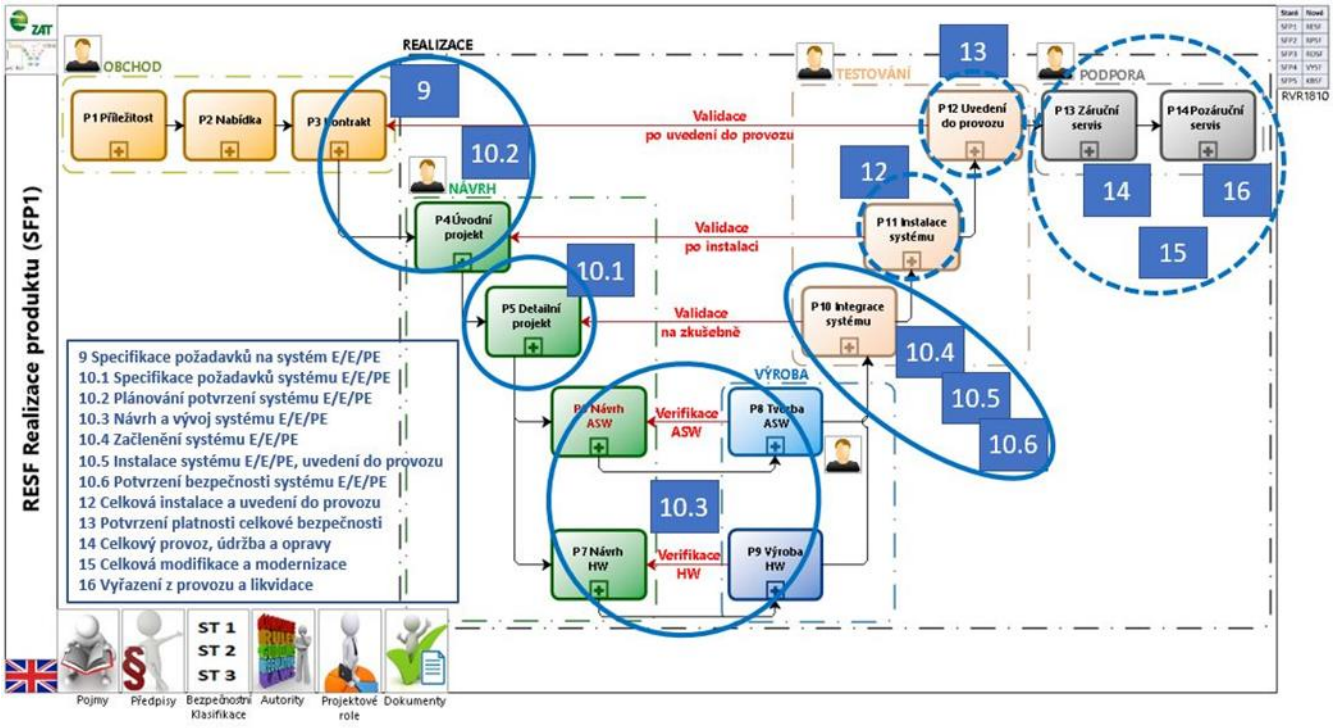
V rámci této etapy bylo třeba vypracovat dokumentaci dokladující plánování a řízení projektu a technickou dokumentaci hardwarové a softwarové části TPS. Dále bylo třeba vyrobit a odzkoušet TPS, provést posouzení funkční bezpečnosti a úspěšně absolvovat certifikační audit TÜV. To vše v podmínkách omezení způsobených COVID-19.

4.1 Zpracování dokumentace

V rámci etapy E2 bylo vypracováno téměř 70 dokumentů pokrývajících procesy plánování a řízení projektu a týkajících se návrhu a výroby TPS včetně dokumentů pro instalaci, provoz a údržbu TPS.

4.1.1 Plánovací a řídicí dokumentace

Účelem plánovací a řídicí dokumentace byla eliminace příčin systematických poruch TPS. Proto v rámci integrovaného managementu procesů ZAT bylo realizováno plánování a řízení projektu ve smyslu požadavků na řízení bezpečnosti dle ČSN EN 61508-1. Naprosto zásadní byl důraz kladený na procesy verifikace a validace (VaV) uplatňované pro TPS s ohledem na fáze životního cyklu 9 až 16 celkové bezpečnosti EUC. Začlenění těchto fází do procesního „V diagramu“ znázorňuje obrázek 3.

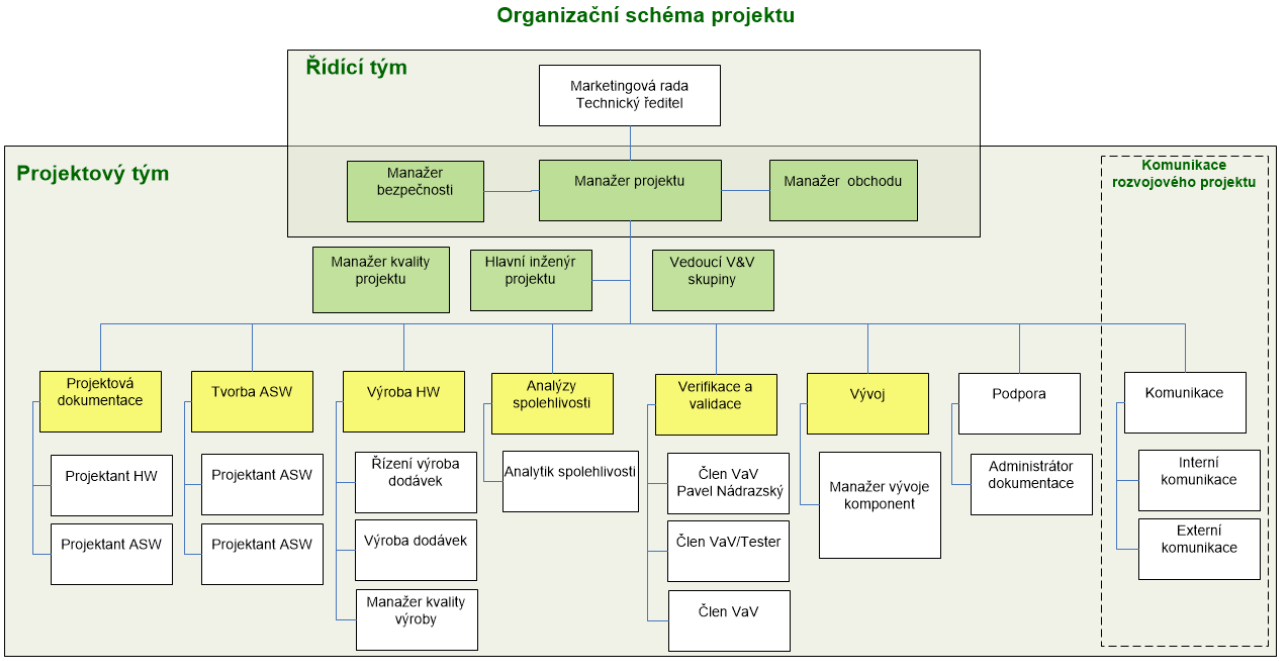


Obrázek 7: Diagram procesu se zakreslením vazeb na životní cyklus celkové bezpečnosti

Fáze životního cyklu 12-16 jsou v obrázku 3 uvedeny čárkovaně, protože nejsou součástí interního vývojového projektu. V konkrétních projektech ochranných systémů pro zákazníky budou ale tyto etapy standardní součástí projektů.

Pro věrohodnou verifikaci a validaci procesů a jejich výstupů je třeba respektovat požadavky na rozdělení rolí pro VaV a nezávislé posouzení funkční bezpečnosti FSA (Functional Safety Assessment) podle ČSN EN 61508-1. Pro E/E/PE systém související s bezpečností navržený na SIL3 se požaduje, aby posouzení bylo provedeno nezávislým oddělením nebo nezávislou organizací.

V rámci interního projektu TPS byl tento požadavek naplněn nezávislým oddělením), jehož členem je manažer bezpečnosti, který je posuzovatelem funkční bezpečnosti. Nezávislé oddělení bylo ze strany ZAT a.s. reprezentováno řídicím týmen projektu, viz organizační schéma projektu na obrázku 4.



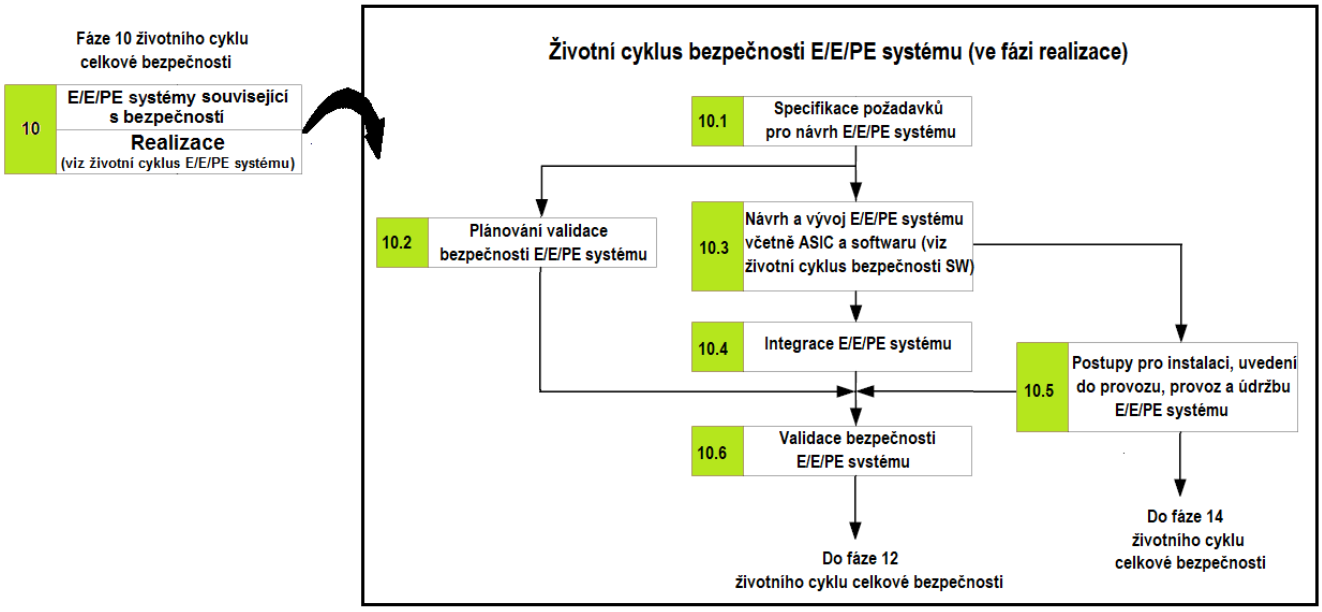
Obrázek 8: Organizační schéma projektu s rozdělením rolí

V rámci integrovaného managementu procesů ZAT byl vytvořen soubor plánovacích a řídicích dokumentů, přičemž na vrcholové úrovni plánování se jednalo o tyto dokumenty:

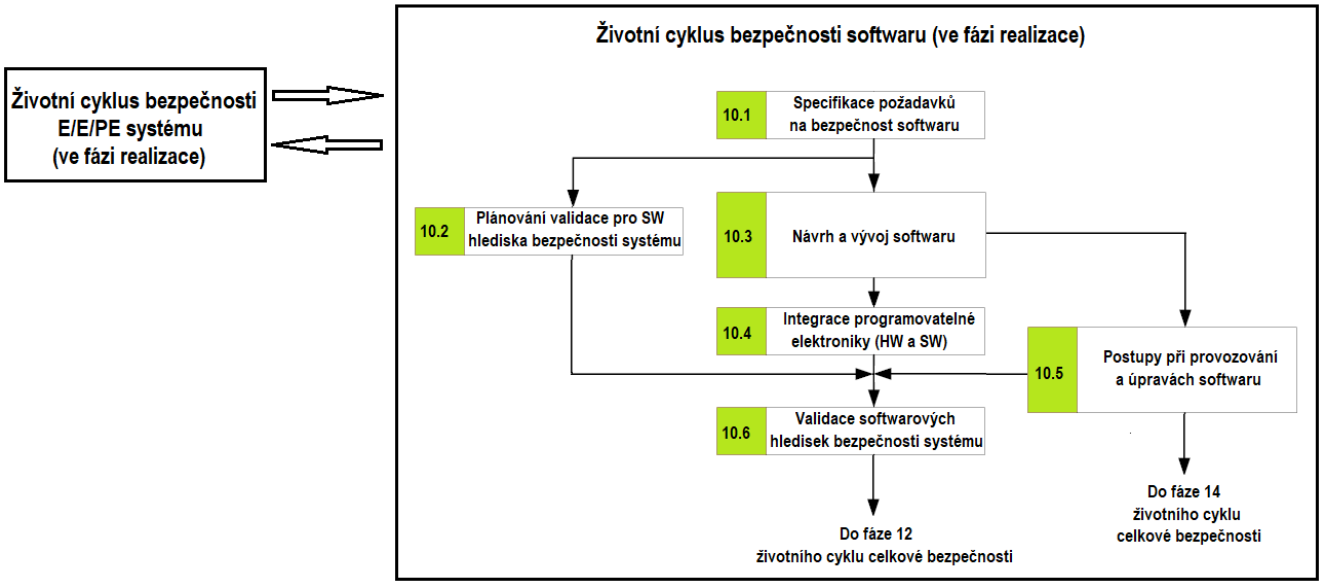
- plán bezpečnosti SW,
- plán kontrol a zkoušek,
- plán posouzení funkční bezpečnosti,
- plán realizace produktu,
- plán řízení konfigurace,
- plán řízení kvality,
- plán řízení projektu,
- plán řízení verifikace a validace.

4.1.2 Technická dokumentace

Účelem technické dokumentace je popis řešení a výrobního provedení TPS. Při zpracování této dokumentace je rozhodující fáze 10 životního cyklu celkové bezpečnosti, která charakterizuje realizaci E/E/PE systému souvisejícího s bezpečností, tedy se vztahuje na TPS. Členění fáze 10 pro popis životního cyklu bezpečnosti TPS a implementovaného softwaru je uvedeno na obrázcích 5 a 6.



Obrázek 9: Životní cyklus bezpečnosti TPS



Obrázek 10: Životní cyklus bezpečnosti softwaru TPS

Tato dokumentace je založena na **detailní specifikaci požadavků na TPS**. Tato detailní specifikace pak umožňuje formulovat níže uvedené třídy požadavků.

- Základní požadavky pro hardware (s přihlédnutím k software) dle ČSN EN 61508-2 pro eliminaci příčin náhodných poruch hardware, kterými jsou:
  - specifikace HW a SW požadavků na TPS,
  - dokumentace technického řešení a zkoušek TPS,
  - dokumentace analýz spolehlivosti a bezpečnosti TPS (funkční analýza, FMEA/FMECA, FTA).
- Základní požadavky pro software dle ČSN EN 61508-3, kterými jsou:
  - specifikace požadavků na softwarové provedení TPS,

- dokumentace architektury software a programování (kódu) algoritmů pro eliminaci příčin chyb software.

Při naplňování těchto požadavků byly s porozuměním uplatněny návody a postupy uvedené v ČSN EN 61508-6 a ČSN EN 61508-7.

Z uvedeného je zřejmé, že naprosto zásadním krokem při návrhu ochranného systému je **sestavení podrobné specifikace požadavků**, které musí splňovat. Tyto požadavky ZAT pro TPS odvodil z předchozích obchodních případů a vytvořil systém sledování požadavků. Zmíněný systém sledování požadavků pro TPS obsahuje celkem126 jednoznačně popsaných požadavků s kritérii jejich splnění. Tyto požadavky jsou členěny do následujících oddílů:

- požadavky na projekt (1 položka - získání certifikátu SIL3 pro TPS),
- požadavky na TPS (13 položek),
- požadavky na koncepci TPS (27 položek),
- detailní požadavky na provedení TPS (85 položek).

Předchozí požadavky na TPS jsou v systému sledování požadavků dedikovány a dále rozšířeny do specifikace požadavků na software. Nedílnou součástí specifikace požadavků na software jsou požadavky, které vyplývají z výsledků analýzy FMEA. Výsledná specifikace požadavků na software TPS obsahuje celkem 78 položek.

4.2 Posouzení funkční bezpečnosti

Nezávislé posouzení funkční bezpečnosti je založeno na provedení interních auditů ZAT. Interní audity byly prováděny formou kontrolních seznamů (check list) podle:

- jednotlivých článků ČSN EN 61508-1 (posouzení procesů ZAT),
- jednotlivých článků ČSN EN 61508-2 (posouzení hardwarového řešení TPS),
- jednotlivých článků ČSN EN 61508-3 (posouzení softwarového řešení TPS).

Splnění požadavků uváděných v článcích norem bylo vyhodnocováno a bylo podkladem pro vypracování zprávy o posouzení funkční bezpečnosti včetně uvedení odkazů na důkazy bezpečnosti.

4.3 Certifikační audit

Po předání relevantních podkladů ZAT certifikační autoritě (TÜV SÜD Czech s.r.o.) proběhl 5. ledna 2022 v prostorách společnosti ZAT certifikační audit zaměřený jak na procesní a technickou dokumentaci, tak na funkční zkoušky TPS. Při funkčních zkouškách byly prověřeny bezpečností funkce (simulovány vstupní signály a sledováno působení výstupů na akční členy) a jejich chování při poruše jednotlivých částí TPS (tam, kde bylo možné provést simulaci poruch).

Připomínky a požadavky certifikační autority na vysvětlení některých postupů analýz spolehlivosti a k technické dokumentaci byly vyřešeny. Následně byl pro TPS vydán příslušný certifikát SIL3, viz obrázek 7.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Czech

INSPEKČNÍ CERTIFIKÁT

evidenční číslo 14.375.401

vydaný inspekčním orgánem č. 4002 akreditovaným ČIA dle ČSN EN ISO/IEC 17020:2012

ZAT a.s.
K Podlesí 541
261 80 Příbram VI

Na základě výsledků provedených kontrolou, zkouškami a hodnocením, které jsou uvedeny v Inspekční zprávě TÜV SÜD Czech evidenční číslo 14.375.400 potvrzujeme shodu níže uvedeného zařízení:

Název: **E/E/PE systémy související s bezpečností ochranného systému turbíny s koncepcí PLC systému platformy ZAT SandRa Z100**
Typ: **TPS – KS65**
Výrobní číslo: E6114/3063338 (E6114-KS65)

s požadavky **ČSN EN 61508-1 ed.2:2011 (idt EN 61508-1:2010),**
ČSN EN 61508-2 ed.2:2011 (idt EN 61508-2:2010),
ČSN EN 61508-3 ed.2:2011 (idt EN 61508-3:2010),
ČSN EN 61508-6 ed.2:2011 (idt EN 61508-6:2010).

Systém související s bezpečností ochranného systému turbíny TPS – KS65 splňuje podle řady norem ČSN EN 61508 ed. 2 požadavky úrovně integrity bezpečnosti až do úrovně SIL3:
a) v režimu provozu s nízkým vyžádáním a varianty zálohování 1oo1, 1oo2 a 2oo3,
b) v režimu provozu s vysokým vyžádáním a varianty zálohování 1oo2 a 2oo3.

Podmínky platnosti:

- uvedeny v Inspekční zprávě TÜV SÜD Czech s.r.o., evidenční číslo 14.375.400 ze dne 2022-03-16:
  a) budou dodrženy pokyny pro užití zařízení za podmínek SIL3,
  b) budou dodrženy požadavky výše uvedených norem,
  c) bude akceptován rozsah a četnost pravidelných kontrol a revizí.

Podrobné technické údaje uvedeny na straně 2.

v Ostravě, dne 2022-03-16

TÜV SÜD Czech s.r.o. - 34 -

Za TÜV SÜD Czech s.r.o. : Ing. Petr Navrátil

TÜV SÜD Czech s.r.o. ● Novodvorská 994 ● 142 21 Prague 4 ● Czech Republic ● certification@tuv-sud.cz

F 540-003-0 (2016-02-16) (IC14.375.401_ZAT_TPS_20220316.doc)

TÜV®

Obrázek 11: Certifikát SIL3 pro TPS

V rámci etapy E2 bylo vypracováno více jak 70 dokumentů pokrývajících procesy plánování a řízení projektu a týkajících se návrhu, výroby HW a SW TPS včetně dokumentů zkoušek, dokumentů pro instalaci, provoz a údržbu TPS. Dále bylo třeba vyrobit a odzkoušet TPS, provést posouzení funkční bezpečnosti a úspěšně absolvovat certifikační audit TÜV. To vše v podmínkách omezení způsobených COVID-19.

5 Poznatky z projektu

Zvolený přístup, kdy činnosti vedoucí SIL3 byly uskutečněny na interním vývojovém projektu TPS se ukázal jako optimální z pohledu pružného využití kapacit pracovníků ZAT a externích pracovníků. To bylo důležité s ohledem na COVID-19, kdy kvůli onemocnění pracovníků ZAT bylo třeba soustředit kapacity na řešení komerčních zakázek. To na druhou stranu vedlo ke zpoždění řešení projektu TPS. Doba řešení jednotlivých etap projektu je uvedená v tabulce 1.

Tabulka 11: Doba řešení projektu TPS

Etapa	**Plán**	**Skutečnost**	**Poznámka**
E1	05/2020 – 06/2020	05/2020 – 06/2020	Plánovaný termín 2 měsíce dodržen.
E2	11/2020 – 05/2021	11/2020 – 03/2022	Plánovaná 7 měsíců, skutečná 17 měsíců (včetně udělení certifikátu).

Naprosto podstatná byla týmová spolupráce při řešení analýz spolehlivosti a jejich aspektů týkajících se funkční bezpečnosti. Situace spojená s COVID-19 si vyžádala tuto týmovou činnost vykonávat distančně. To bylo řešeno formou 32 schůzek týmu prostřednictvím aplikace MS Teams.

Peněžní náklady vynaložené na řešení projektu TPS, jsou interní informací společnosti ZAT. Pro informaci lze však uvést jejich procentuální rozložení, viz tabulka 2.

Tabulka 12: Nákladová náročnost řešení projektu TPS

Nákladová náročnost	**V procentech**
Celkem E1 a E2	100
Vlastní náklady ZAT	71
Náklady na externí pracovníky	21
Náklady na certifikaci	8

Časová náročnost řešení projektu TPS na kapacity ZAT (pracnost) je uvedena v tabulce 3 a tabulce 4.

Tabulka 13: Hodinová náročnost řešení projektu TPS podle etap

Náročnost dle pracovních hodin ZAT	V hodinách	V procentech
Celkem E1 a E2	3 368	100
E1	440	13
E2	2 928	87

Tabulka 4: Hodinová náročnost řešení etapy E2 projektu TPS podle činností

Náročnost E2 dle pracovních hodin ZAT	V hodinách	V procentech
Celkem E2	2 928	100
Analýzy – PCA, FMEA, FTA	528	18
Zpracování SW	360	12
Vytvoření dokumentace vč. verifikace	1 440	49
Validace produktu (zkoušky)	600	21

6 Závěr

Udržení certifikátu a aplikace získaných zkušeností pro komerční projekty vyžaduje udržovat a rozvíjet procesy funkční bezpečnosti, a to zejména v níže uvedených oblastech.

- Udržování a zdokonalování zpětné vazby z provozu, kde jsou podstatnými faktory:
  - sběr a vyhodnocování provozních informací pro získání specifických dat o spolehlivosti vlastních produktů,
  - komunikace se zákazníkem.
- Včasné reakce na změny při uvědomění, že změna ve výrobci či dodavateli základních komponent může mít za následek změny hodnot jejich spolehlivosti, a tudíž i změny v hodnotách spolehlivosti funkcí bezpečnostního systému.
- Udržování a prohlubování znalostí o funkční bezpečnosti a spolehlivosti, které vyžaduje:
  - školení zaměstnanců s ohledem na jejich funkční zařazení,
  - sledování vývoje v oboru a jeho dopady na aktualizaci norem funkční bezpečnosti,
  - komunikací s projektanty EUC pro optimální návrh a začlenění PE systému do EUC.

Udělením certifikátu SIL3 pro TPS proto práce na poli funkční bezpečnosti nekončí. Je nedílnou součástí naplňování vize společnosti ZAT.

Použitá literatura

[1] ČSN EN 61508-1 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky*

[2] ČSN EN 61508-2 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností*

[3] ČSN EN 61508-3 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 3: Požadavky na software*

[4] ČSN EN 61508-4 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systému souvisejících s bezpečností – Část 4: Definice a zkratky*

[5] ČSN EN 61508-5 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovní integrity bezpečnosti*

[6] ČSN EN 61508-6 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3*

[7] ČSN EN 61508-7 ed. 2:2011 *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 7: Přehled technik a opatření*

ISBN 978-80-02-02988-5
Vybrané problémy certifikace bezpečnostního systému
Sborník přednášek
kolektiv autorů
1. vydání
rok vydání 2022, Česká společnost pro jakost
vazba brožovaná, 38 stran