Analýza funkční bezpečnosti parních turbín s příslušenstvím

Functional safety analyse of steam turbines with accessories

Bc. Martin Soukeník

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin SOUKENÍK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Automatické řízení a informatika**
Téma práce:	**Analýza funkční bezpečnosti parních turbín s příslušenstvím.**

Zásady pro vypracování:

1. **Rešerše problematiky fází životního cyklu všech částí SIS – tj. snímačů, řídícího systému a koncových prvků.**
2. **Zhodnocení a posouzení nebezpečí a přiřazení bezpečnostních funkcí do kategorií SIL.**
3. **Určování hodnoty HFT (hardwarová poruchová tolerance) a SFF (podíl bezpečných poruch).**
4. **Vlastní výpočet pravděpodobnosti poruch bude proveden metodou FTA (analýzy stromu poruch).**
5. **Prověření plnění požadavků kladených na bezpečnostní funkce.**
6. **Hodnocení na základě hodnot MTBF (střední doba mezi poruchami), popřípadě MCTF (střední počet cyklů mezi poruchami).**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Interní normy společnosti SIEMENS.**
2. **Altmann W. Practical Process Control for Engineers and Technicians. ELSEVIER, 2006, s. 290, ISBN 978-0-7506-6400-4.**
3. **Mikell P. Groover: Automation, Production Systems, and Computer – Integrated Manufacturing (3rd Edition).**
4. **Balatě J. Automatické řízení. BEN, 2004, s.664, ISBN 978-80-7300-148-0.**
5. **HRUŠKA,F.: Projektování systémů integrované automatizace. Učební texty. 2.vyd. Zlín: UTB ve Zlíně, 2002, s. 133. ISBN 80-7318-100-2.**
6. **VDOLEČEK, František; Spolehlivost a technická diagnostika: Text pro podporu výuky v kombinovaném studiu. Brno, 2002. 49 s.**
7. **Soubor ČSN týkající se funkční bezpečností zařízení (např. ČSN EN 61508-*, ČSN EN 61511-*, ČSN EN 62061:2005)**

Vedoucí diplomové práce: **doc. Ing. František Hruška, Ph.D.**
Ústav elektroniky a měření

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá analýzou funkční bezpečnosti ochran parní turbíny. Bezpečnostní funkce jsou zařazeny do příslušného stupně integrity, je proveden výpočet průměrné pravděpodobnosti poruchy metodou analýzy stromu poruch a validace bezpečnosti bezpečnostního přístrojového systému dle ČSN EN 61511 a ČSN EN 61508.

Klíčová slova: Analýza stromu poruch, funkční bezpečnost, průměrná pravděpodobnost poruchy při vyžádání, stupeň integrity bezpečnosti, bezpečnostní přístrojový systém, střední doba mezi poruchami, tolerance hardwaru k poruchám, poruchy se společnou příčinou.

ABSTRACT

This diploma thesis deals by analysis of steam turbine functional safety protections. Safety functions are sorted to the relevant integrity level, is made calculation of average probability of failure by fault tree analysis and validated safety factor of safety instrumented system according to ČSN EN 61511 and ČSN EN 61508.

Keywords: Fault tree analysis, functional safety, probability of failure on demand, safety integrity level, safety instrumented system, mean time between failure, hardware fault tolerance, common case failure.

Děkuji doc. Ing. Františku Hruškovi, Ph.D. za metodické vedení a podmětné připomínky při vypracování závěrečné diplomové práce. Zároveň děkuji firmě Siemens Industrial Turbomachinery s.r.o., zejména Ing. Jiřímu Vašátkovi, CSc za podporu a poskytnuté rady v průběhu tvorby této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Bezpečnost strojních zařízení se v současné době dostává do popředí zájmu techniků. Samozřejmě se již dříve dbalo na bezpečnost, ale spíše na tzv. primární. Normy ISA 84 a IEC 508, které specifikují obecně funkční bezpečnost, byly vydány až po roce 2004. Jejím předchůdcem byla norma DIN 19250 z roku 1989, která specifikovala funkční bezpečnost pouze strojních zařízení. Z hlediska zákonných norem patří tyto normy do skupiny nezávazných.

Novela zákona č.22/1997 Sb. (provedená zákonem č.71/2000 Sb.) o technických požadavcích na výrobky výslovně uvádí, že česká technická norma není obecně závazná. Dle přílohy č.1 nařízení vlády č.176/2008 o technických požadavcích na strojní zařízení článek 1.1.2 Zásady zajišťování bezpečnosti, odstavec b) Při výběru nejvhodnějších řešení výrobce nebo jeho zplnomocněný zástupce uplatňuje níže uvedené zásady v tomto pořadí – vyloučit nebo co nejvíce omezit nebezpečí návrhem a konstrukcí strojního zařízení [1]. V praxi to může znamenat potřebu určení správné míry snížení rizika.

Technické a bezpečnostní požadavky parních turbín jsou dosud specifikovány normou ČSN EN 60045, která však nekvantifikuje vlastní funkční bezpečnost zabezpečovacího systému.

I. TEORETICKÁ ČÁST

1 SPOLEHLIVOST

1.1 Rozdělení spolehlivosti

Spolehlivost je jedna z vlastností jakosti a patří mezi nejdůležitější. Je to schopnost plnit požadované funkce v čase za daných provozních okolností. Spolehlivost lze rozdělit na další části [2]:

- *Bezporuchovost* – schopnost výrobku plnit nepřetržitě požadované funkce po definovanou dobu a za stanovených podmínek
- *Opravitelnost* – způsobilost výrobku ke zjištění příčin vzniku poruch a jejich odstraňování opravou.
- *Pohotovost* – komplexní vlastnost výrobku, skládající se z bezporuchovosti a opravitelnosti.
- *Udržovatelnost* – způsobilost výrobku k předcházení poruch stanovenou údržbou.
- *Životnost* – schopnost výrobku plnit požadované funkce do dosažení mezního stavu daného technickou dokumentací, při dané údržbě, popřípadě opravě.
- *Skladovatelnost* – schopnost výrobku zachovávat nepřetržitě bezvadný stav po dobu skladování a přepravy při daných podmínkách.
- *Bezpečnost* – schopnost výrobku se chránit proti fyzikálním i jiným typům následků poruch, poškození, chyb a jiným událostem. Týká se to zejména ochrany zdraví a ekonomických ztrát [3].

Bezpečnost se dále dělí na [4]:

- *Primární* - bezpečnost, která se zabývá takovými riziky, jako jsou např. požár, výbuch, nebezpečné dotykové napětí.
- *Nepřímá* - bezpečnost, zahrnující nepřímé důsledky nesprávné činnosti systému, jako např. poskytování nesprávných údajů.
- *Funkční* - zahrnuje bezpečnost řízeného zařízení. Úroveň funkční bezpečnosti závisí na opatřeních zavedených s cílem zmenšit riziko, a tudíž záleží i na správné činnosti těchto optření.

1.2 Podmínky pro posuzování spolehlivosti

Abychom mohli definovat stavy funkční bezpečnosti je potřeba definovat podmínky.

- *Závada* (poškození) je jev spočívající v narušení bezvadného stavu, ale výrobek může být nadále provozován.
- *Porucha* je jev jehož následkem ztrácí výrobek schopnost plnit požadovanou funkci.

Z výše uvedených definic vyplývá, že pro posuzování funkční bezpečnosti budeme nadále pracovat pouze s poruchou. Při posuzování se vychází z dvoustavového modelu – výrobek není v poruše nebo je v poruše, přičemž přechod mezi stavy je skokový.

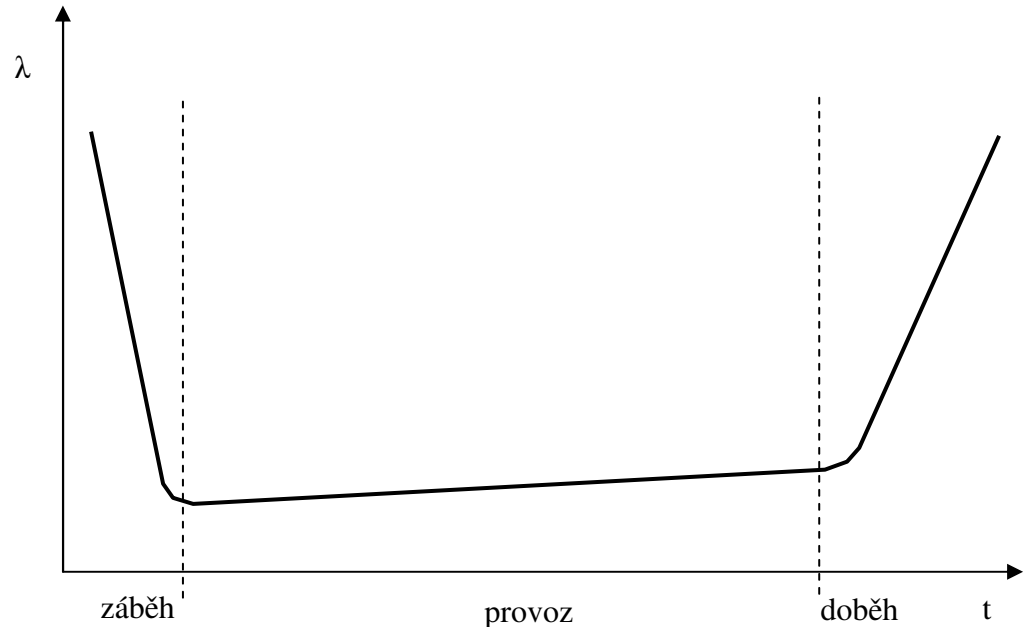
Dalším důležitým kritériem je obnovitelnost systému.

- *Obnovované systémy* – systém je schopen po obnovení plnit požadované funkce. Obnova je řešena výměnou nebo opravou porouchaného dílu. Tyto systémy jsou schopny plnit požadovanou funkci i po poruše.
- *Neobnovované systémy* – v případě poruchy se díl vymění za nový. U těchto dílů je oprava nemožná nebo ekonomicky velmi náročná (elektronické součástky, ložiska, řemeny, atd.).

Normy pro funkční bezpečnost rozlišují tyto systémy. U obnovovaných systémů by se měla hodnota pravděpodobnosti poruchy po opravě snížit. Teorie funkční bezpečnosti však zavádí zjednodušení a předpokládá, že systém je po opravě a následném odzkoušení stejně bezporuchový jako nový.

1.3 Vanová křivka

Předpokládá se, že spolehlivost je náhodný jev, proto se pro výpočty používá teorie pravděpodobnosti a matematická statistika. Volba určitého teoretického modelu vychází z dlouhodobých zkušeností. Na základě nich se předpokládá průběh intenzity poruch, který tvarem připomíná vanu, proto je nazýván *vanovou křivkou* (Obr. 1).



Obr. 1 Charakteristický průběh intenzity poruch

Běžně se pro výpočty uvažuje pouze prostřední část vanové křivky tj. doba provozu. V tomto časovém úseku je pro zjednodušení teoretického modelu uvažováno s konstantní intenzitou poruch λ. Je důležité vymezit tento časový úsek – doba záběhu končí zkušebním provozem a předáním zákazníkovi do užívání. Doba provozu končí předpokládanou dobou životnosti výrobku.

Intenzita poruch je definována

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} \tag{1}$$

Pravděpodobnost bezporuchového provozu

$$R(t) = 1 - F(t) \tag{2}$$

Hustota pravděpodobnosti poruch

$$f(t) = \frac{dF(t)}{dt} = F'(t) \tag{3}$$

1.4 Typy rozdělení pravděpodobnosti

Nejčastěji používaným modelem je *exponenciální rozdělení*. Za podmínek kdy $\lambda(t) = \lambda = konst$, $\lambda > 0$ pravděpodobnost vzniku poruchy nezávisí na době, po kterou je zařízení v bezporuchovém stavu.

Pravděpodobnost poruchy u exponenciálního rozdělení

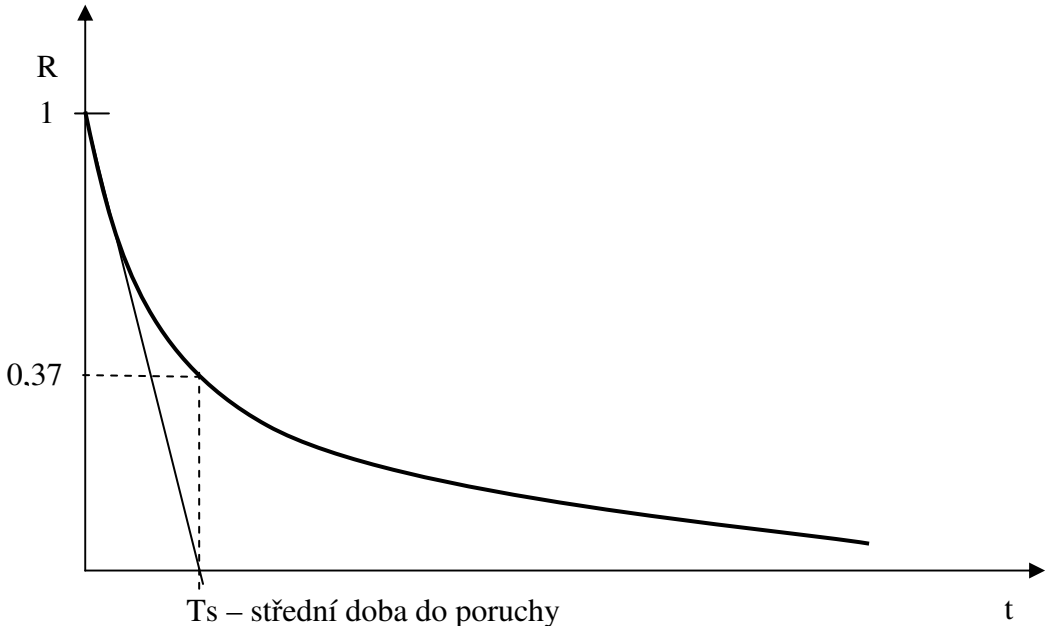
$$F(t) = 1 - e^{-\lambda t} \tag{4}$$

Pravděpodobnost bezporuchového provozu u exponenciálního rozdělení

$$R(t) = 1 - F(t) = e^{-\lambda t} \tag{5}$$

Střední doba bezporuchového provozu u exponenciálního rozdělení

$$T_s = \int_0^{\infty} R(t)dt = \frac{1}{\lambda} \tag{6}$$



Obr. 2 Průběh bezporuchového provozu u exponenciálního rozdělení

Pro strojírenské výrobky je vhodnější použít *Weibullovo rozdělení*.

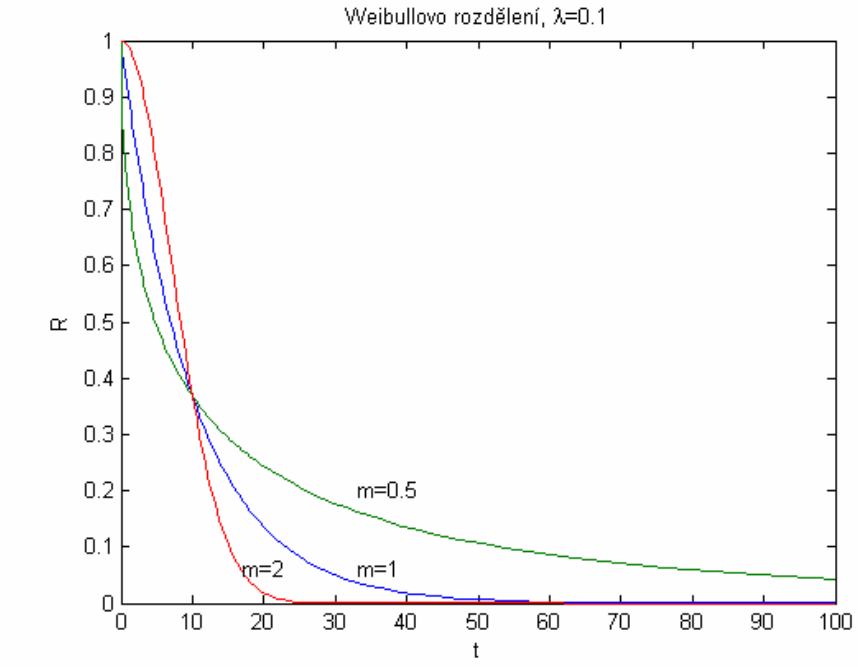
Pravděpodobnost poruchy Weibullova rozdělení

$$F(t) = 1 - e^{-(\lambda t)^m} \tag{7}$$

Pravděpodobnost bezporuchového provozu Weibullova rozdělení

$$R(t) = e^{-(\lambda t)^m} \tag{8}$$

V případě, že $m = 1$ jedná se o zvláštní případ, kdy Weibullovo rozdělení je shodné s exponenciálním. Za podmínek $\lambda > 0$, $m > 0$, $m \neq 1$ dochází k deformaci exponenciály a zohledňuje se nekonstantní intenzita poruch v době provozu výrobku.



Obr. 3 Průběh bezporuchového provozu u Weibullova rozdělení

Z grafu je zřejmé, že pokud je $m < 1$, výrobek má více poruch, když je nový (na počátku užívání rychleji stárne), než v případě exponenciálního rozdělení (Obr. 3). Pro úplnost bych dodal, že výrobky pro energetiku mají plánovanou technickou životnost $t_z = R_{\min} = 0{,}90 \div 0{,}99$.

V praxi se mohou vyskytnout i jiné typy rozdělení, jako např. Gaussovo, Studentovo, Binomické a Poissonovo. Výše uvedená rozdělení se u modelu funkční bezpečnosti nepoužívají a uplatní se v případě výpočtu spolehlivosti.

2 ANALÝZA STROMU PORUCHOVÝCH STAVŮ (FTA)

2.1 Úvod do problematiky

Analýza stromu poruchových stavů se zabývá identifikací a analýzou podmínek, které způsobují nebo přispívají k vrcholové události. Je vhodná pro komplikovanější systémy, kde dochází k větvení a paralelním procesům. Při analýze FTA (Fault Tree Analysis) je touto událostí porucha, vada, zhoršení bezpečnosti nebo zhoršení jiných provozních atributů. Při analýze stromu úspěchů STA (Success Tree Analysis) je vrcholovou událostí úspěch (bezporuchový stav). Metoda se běžně používá při projektování jaderných elektráren, dopravních systémů, komunikačních systémů, chemických průmyslových procesů a zdravotnických systémů. Analýza stromu poruchových stavů se používá při analýze bezpečnosti systémů, ale lze ji také použít pro analýzu pohotovosti a udržovatelnosti systémů.

Existují dva přístupy FTA. První přístup je *kvalitativní* nebo také tradiční, kdy se pravděpodobnost výskytu vstupních událostí nesleduje. Kvalitativní přístup lze použít i tam, kde lze odhadnout pravděpodobnost výskytu události, pak se používá popisný způsob, např. „středně pravděpodobná“. Metoda se používá v případech, kdy se hledají pouze potenciální příčiny poruchových stavů. Druhý přístup je *kvantitativní* při kterém se pomocí analýzy FTA modeluje celý produkt, proces nebo systém. Vstupní události mají známou pravděpodobnost poruchy a tudíž lze spočítat pravděpodobnost výskytu vrcholové události. Při použití ve funkční bezpečnosti, se užívá kvantitativní metody FTA [5].

2.2 Základní pojmy

Metoda FTA je deduktivní metoda analýzy, což znamená, že stav se posuzuje shora dolů. Forma FTA je grafická a symboly jsou definované normou. Norma připouští jistou odchylku grafické formy dle použitého softwarového balíku.

Při popisu FTA se mohou vyskytovat tyto pojmy:

- *Výstup* – výsledek děje či jiného vstupu. Výstupem může být mezilehlá nebo vrcholová událost.
- *Vrcholová událost* – výstup všech vstupních událostí. Je vždy umístěna na vrcholu FTA.

- *Hradlo* – značka která se používá ke stanovení vazby mezi vstupem a výstupem. U *statických* hradel výstup nezávisí na pořadí výskytu vstupů, u *dynamických* výstup závisí na pořadí vstupů.
- *Událost* – výskyt podmínky nebo děje.
- *Základní událost* – událost, kterou nelze dále rozvíjet.
- *Primární událost* – událost nacházející se na základní úrovni. Tato událost může být dále rozvíjena.
- *Mezilehlá událost* – událost, která není vrcholovou ani primární událostí, leží ve střední části FTA.
- *Události se společnou příčinou* – odlišné události v systému, které mají stejnou příčinu svého výskytu.
- *Nerozvíjená událost* – událost, která nemá vstupní události. Událost buď není rozvíjena z důvodu nedostatku informací nebo je rozvíjena v jiné analýze FTA.

Při výpočtech funkční bezpečnosti se používá i metoda analýzy způsobů a důsledků poruch FMEA (Failure Mode Effects Analysis). Je to metoda analýzy zdola nahoru (opačně než FTA) a patří mezi induktivní přístupy. FMEA se používá spíše pro úplnou identifikaci základních událostí, tudíž je vhodná pro modelování jednotlivých komponentů. Jednotlivé metody lze kombinovat a mnohdy se využívají pro kontrolu vzájemného výpočtu, provedeného metodou FTA a FMEA.

2.3 Požadované informace o systému

Analyzovaný systém má být definován popisem funkce a identifikací rozhraní systému. Taková definice má zahrnovat:

- Vymezení, co je podstatou poruchy systému.
- Funkční strukturu systému, reprezentovanou funkčním blokovým diagramem.
- Hranice systému.
- Provozní profil systému.

- Podmínky prostředí systému a příslušná lidská hlediska (výcvik pracovníků obsluhy a údržby).
- Seznam použitých dokumentů, tj. výkresů, specifikací, provozních příruček, ve kterých jsou uvedeny podrobnosti o návrhu a provozu zařízení.
- Doba mezi periodickými zkouškami, doba, která je k dispozici pro zásah údržby při poruše.

2.4 Použití kvantitativní analýzy FTA

2.4.1 Sériová konfigurace systému

Při sériové konfiguraci systému jakákoliv událost modelované poruchy (bloku v blokovém diagramu bezporuchovosti) způsobí poruchu systému. Pro předpokládanou vzájemnou nezávislost poruch prvků platí, že pravděpodobnost bezporuchového stavu systému sériově seřazených prvků odpovídá součinu dílčích pravděpodobností jednotlivých prvků.

Pravděpodobnost bezporuchového provozu sériového systému

$$R_S(t) = \prod_{i=1}^{n} R_i(t) \tag{9}$$

Pravděpodobnost poruchy sériového systému

$$F_S(t) = 1 - \prod_{i=1}^{n} (1 - F_i(t)) \tag{10}$$

V analýze FTA se používá opačná logika. Poruchový výstup vzniká buď při poruše prvku 1 nebo poruše prvku 2 atd. To je důvod, proč sériová konfigurace systému je reprezentována hradlem OR.

2.4.2 Paralelní konfigurace systému

Jestliže výstupní událost hradla nastala pouze tehdy, jestliže nastaly všechny vstupní události hradla, potom mají být tyto události spojovány pomocí hradla AND. Taková konfigurace systému se nazývá *aktivní záloha*. Předpokládá se, že každý vstup do bloku aktivních záloh je nezávislý.

Pravděpodobnost bezporuchového provozu systému aktivní zálohy

$$R_S(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t)) \tag{11}$$

Pravděpodobnost poruchy systému aktivní zálohy

$$F_S(t) = \prod_{i=1}^{n} F_i(t) \tag{12}$$

Záložní prvky mohou být provozovány v režimu se sdíleným zatížením, potom se pravděpodobnost poruchové události systému může s přibývajícím počtem prvků zvyšovat. Taková konfigurace systému porušuje pravidlo pro systém s konfigurací AND. Pro modelování takového systému je nutné použít majoritního hradla. Podmínkou úspěchu systému je, aby zůstalo *k* z *n* vstupních bloků provozuschopných.

Pravděpodobnost bezporuchového provozu systému s majoritním hradlem

$$R_S(t) = 1 - \sum_{i=0}^{k-1} \frac{n!}{i! \cdot (n-i)!} \cdot (R_0(t))^i \cdot (1 - R_0(t))^{n-i} \tag{13}$$

Pravděpodobnost poruchy systému s majoritním hradlem

$$F_S(t) = \sum_{i=0}^{k-1} \frac{n!}{i! \cdot (n-i)!} \cdot (1 - F_0(t))^i \cdot (F_0(t))^{n-i} \tag{14}$$

Prahová hodnota majoritního hradla *m*, která je uvedená v grafické značce, vyznačuje kolik událostí musí nastat, aby se událost šířila dále ve stromu FTA.

$$m = n - k + 1 \tag{15}$$

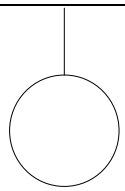
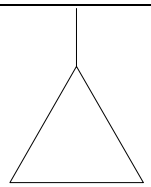
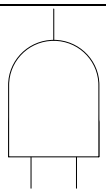
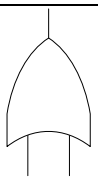
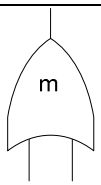
Pasivní zálohování (pohotovostní) je konfigurace systému, kdy je pouze několik prvků aktivních, a v případě poruchy jednoho nebo více těchto prvků se jedna nebo více záložních prvků aktivuje, aby převzaly tyto funkce. Pro posouzení zálohy se uvažuje

- *Studená záloha* – prvky, které nemají sklon k poruše.
- *Teplá záloha* – prvky mají sklon k dílčí poruše, dokud nebyly přivedeny do aktivního provozu.
- *Horká záloha* – prvky mají stejný sklon k poruše, jako když jsou v provozu.

Pasivní zálohy nelze popsat statickými hradly a k analýze tohoto hradla je nutné použít Markovovu analýzu. Tato analýza se musí použít i u podmíněných pravděpodobností.

2.5 Grafická reprezentace

Grafické reprezentace stromů poruchových stavů mohou mít rozmanitou grafiku, záleží na zvyklosti regionů a výrobcích aplikačního softwaru. Je možná reprezentace hradel pomocí obdélníků s vyznačenými funkcemi, potom se kreslí strom poruchových stavů horizontálně a to jak zleva doprava, tak i naopak. Pokud se kreslí strom poruchových stavů vertikálně, používají se odlišné značky pro hradla a vrcholová událost je vždy nahoře (viz. Tab. 1). V praktické části této práce je použit pro výpočet speciální software od firmy Item software. Tento nástroj používá typ značek, které jsou uvedeny v Tab. 1.

Značka	Název	Popis
	Základní událost Basic event	Událost na nejnižší úrovni, pro kterou jsou k dispozici pravděpodobnosti výskytu poruchy.
	Transfer ven / dovnitř Transfer OUT / IN	Hradlo ukazující, že je tato část systému rozvíjena v jiné části nebo na jiné straně diagramu.
	Hradlo AND Gate AND	Sériová konfigurace systému – výstupní událost nastane, jestliže nastane jakákoliv ze vstupních událostí, vzorec (10)
	Hradlo OR Gate OR	Paralelní konfigurace systému typu aktivní záloha - výstupní událost nastane, jestliže nastanou všechny vstupní události, vzorec (12)
	Majoritní hradlo *m* z *n* Majority vote *m* out of *n*	Paralelní konfigurace systému typu majoritní hradlo - výstupní událost nastane, jestliže nastane *m* nebo více událostí z *n* vstupních událostí, vzorce (14), (15)

Tab. 1 Vybrané grafické značky analýzy stromu poruchových stavů

2.6 Sestavení stromu poruchových stavů

Prvním úkolem při sestavování stromu poruchových stavů je jednoznačné vymezení vrcholové události, předmětu, hranic systému nebo objektu analýzy. Ve vymezení vrcholové události musí být popsán problém, který je analyzován, aby se určily příčiny přispívající k poruše systému. Při kvantitativní analýze se určuje pravděpodobnost výskytu vrcholové události a všech nebo většiny vstupů. V předmětu analýzy jsou vymezeny poruchy, které budou začleněny do stromu poruchových stavů.

Dalším krokem je sestavení stromu poruchových stavů a to postupem shora dolů. Vstupy do vrcholové události jsou systematicky rozvíjeny, tak aby vycházely z vlastních vstupních událostí. Každý vstup směřující dolů ve stromu poruchových stavů se rozvíjí samostatně až do okamžiku, kdy dosáhne základních událostí. Musí být definováno do jakých detailů se má systém analyzovat. Systém může být analyzován až po jednotlivé součásti a nebo na úroveň montážních sestav, pokud jsou dostupné jejich hodnoty pravděpodobností poruchy. Na této úrovni se nachází příčiny poruch, které se nazývají základní jednotka. Funkční i fyzické hranice základní jednotky musí být jednoznačné.

Účelem číselné analýzy je poskytnout kvantitativní posouzení pravděpodobnosti výskytu vrcholové události. K provedení této analýzy je nutné mít pravděpodobnostní hodnoty na úrovní součástí (základních jednotek). Tato data lze získat pomocí technik předpovědi bezporuchovosti, data ze skutečných zkoušek nebo z používání v provozu.

Softwarové produkty pro výpočet analýzy stromu poruchových stavů umožňují počítat se vstupními hodnotami zadanými nejen jako pravděpodobnost poruchy, ale dokáží si poradit i s jinými charakteristickými veličinami, jako např. intenzita poruch a MTBF. Pak je nutné zadat i dodatečnou informaci, kterou je časový interval, pro který se pravděpodobnosti poruch uvažují.

3 FUNKČNÍ BEZPEČNOST

3.1 Úvod do problematiky

Funkční bezpečnost zahrnuje identifikovatelné poruchy, které mají za následek vážné důsledky (například úmrtí) a určení maximální přijatelné četnosti pro každý režim poruchy. Zařízení jehož porucha přispívá ke každému z těchto rizik je označované jako „safety related“ (související s bezpečností) [6]. Příkladem jsou systémy řízení průmyslových procesů, systémy nouzového vypnutí procesů, železniční signalizační zařízení, zařízení v automobilovém průmyslu, lékařské vybavení, jaderné elektrárny, atd.

Maximální přijatelná četnost chyb pro každou poruchu bude vést k posouzení každého zařízení v bezpečnostním přístrojovém systému (SIS – Safety Instrumented System) , podle jeho velikosti příspěvku k poruše. Tento ukazatel je nazýván stupeňem integrity bezpečnosti (SIL – Safety Integrity Level) a je obvykle určen jednou ze čtyř úrovní.

- SIL 4 – nejvyšší úroveň, tato úroveň se běžně nepoužívá
- SIL 3 – nižší úroveň než SIL 4, ale vyžaduje použití sofistikované techniky
- SIL 2 – vyžaduje dobrý technický návrh a zkušenosti
- SIL 1 – minimální úroveň, ale používající osvědčená technická řešení (GMP – Good Manufacturer Practice)
- <SIL 1 – zařízení nepatří do skupiny „safety related“, někdy označováno jako SIL 0

Protože každá fyzická část může mít poruchu, každý člověk vytváří chyby a žádný software není navržen pro všechny možné stavy, proto neexistuje nulové nebezpečí [6].

Všechny příčiny (středního věku včetně zdravotních)	$1 \cdot 10^{-3}$ za rok
Všechny nehody (za jedince)	$5 \cdot 10^{-4}$ za rok
Nehoda doma	$4 \cdot 10^{-4}$ za rok
Dopravní nehoda	$6 \cdot 10^{-5}$ za rok
Živelné pohromy (za jedince)	$2 \cdot 10^{-6}$ za rok

Tab. 2 Pravděpodobnost úmrtí podle příčin

Tabulka 2 byla základem pro kvantifikaci ještě tolerovatelného nebezpečí. Riziko nebezpečí je pro běžný život v domácnosti velice vysoké, důvodem je zvýšená frekvence přítomnosti osob v tomto prostoru.

Struktura bezpečnostních norem je následující:

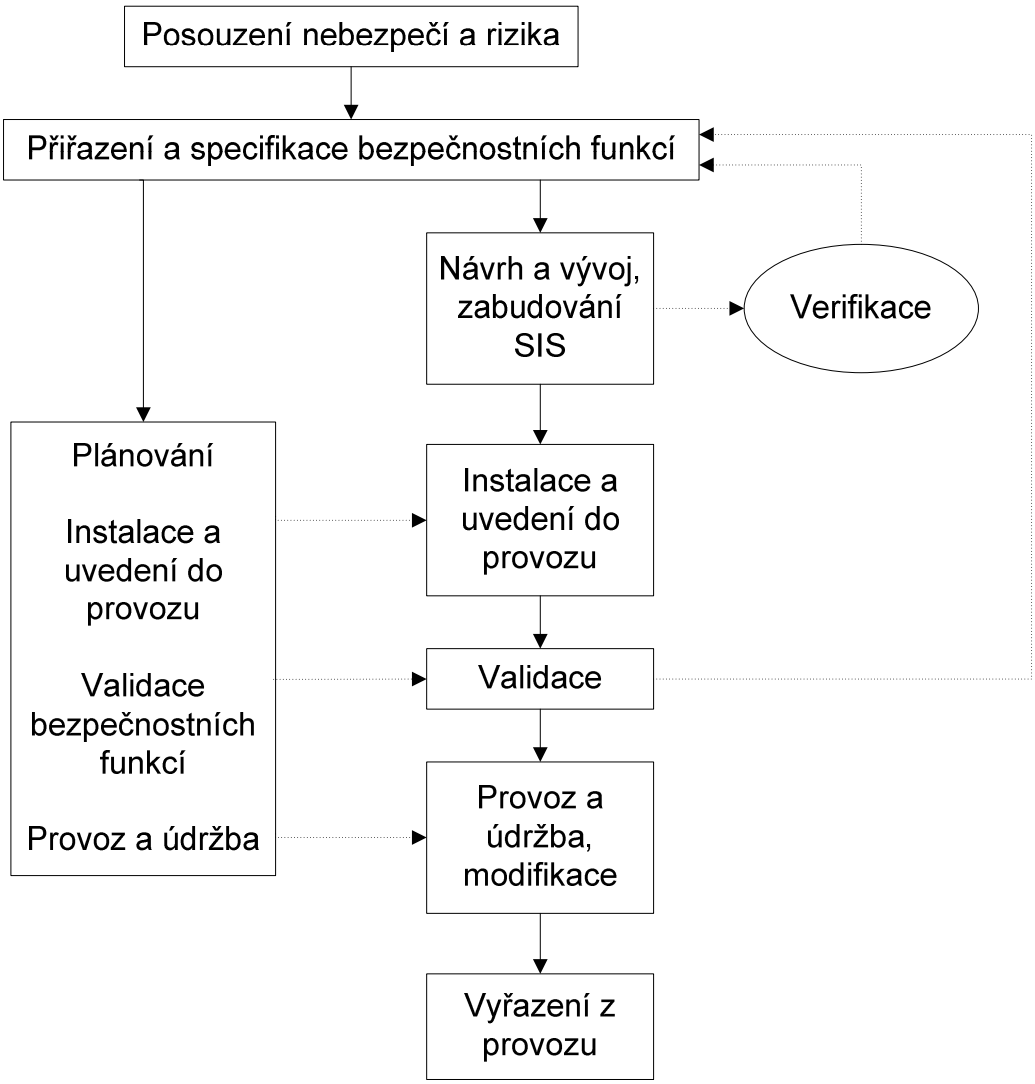
- typu A – základní normy, které uvádějí základní pojmy, zásady pro konstrukci, které mohou být aplikována na všechna strojní zařízení
- typu B – skupinové bezpečnostní normy se zabývají jedním nebo více bezpečnostními hledisky, která mohou být použita pro větší počet strojních zařízení.
- Typu C – bezpečnostní normy pro stroje, určují detailní bezpečnostní požadavky pro jednotlivé stroje.

Normy, které specifikují detailní bezpečnostní požadavky, tj. typu C, mají přednost před normami typu A nebo B. Základní skupinou norem (typu A) zabývající se funkční bezpečnostní je řada norem ČSN EN 61508. Dle těchto norem se budou řídit především výrobci komponentů. Skupina norem ČSN EN 61511 je charakteristická pro průmyslové procesy, patří do skupiny norem typu B. Vzhledem k charakteru dodávek turbosoustrojí bude funkční bezpečnost posuzována podle této skupiny norem. Je to důležitý předpoklad, protože normy typu A a B se liší především v terminologii [7].

3.2 Životní cyklus bezpečnosti SIS

Rozmanitost činností ve fázích životního cyklu SIS snižuje pravděpodobnost systematických chyb. To je nezbytné k dosažení příslušné úrovně funkční bezpečnosti. Normy popisující funkční bezpečnost zavádí komplexní management posuzování jednotlivých fází životního cyklu SIS. Stanovují obecný přístup bezpečnosti systémů obsahujících elektrické a/nebo elektronické a/nebo programovatelné elektronické součásti (E/E/PES systémy) a využívané pro bezpečnostní funkce [8]. Ve většině případů se bezpečnost zajišťuje prostřednictvím kombinací dalších ochranných systémů založených na různých principech – např. mechanických, hydraulických, pneumatických, které dohromady tvoří celistvou sestavu bezpečnostních systémů. I když jsou tyto normy určeny pro E/E/PES systémy, je možné podle nich rámcově posuzovat i systémy založené na

jiných než elektrických principech [9], [10], [11]. Normy se zabývají jak posouzením hardwaru, tak i softwaru a je zde zmínka i o selhání lidského činitele.



Obr. 4 Fáze životního cyklu SIS

Na obr. 4 je zjednodušený model životního cyklu SIS [6]. Z modelu je zřejmé, že jednotlivé fáze se dotýkají nejenom výrobce, ale i provozovatele zařízení. Dle normy ČSN EN 61511-1, odstavce 5.2.6.1.5 musí být i vývojové a výrobní nástroje činnosti životního cyklu bezpečnosti samy předmětem posouzení funkční bezpečnosti [12]. V praxi se to týká především softwaru pro simulaci a modelování, měřících zařízení, zkušebních zařízení a zařízení pro údržbu. Posuzování funkční bezpečnosti nástrojů obsahuje především sledovatelnost až ke kalibračním normám, historii provozu a seznam defektů [13].

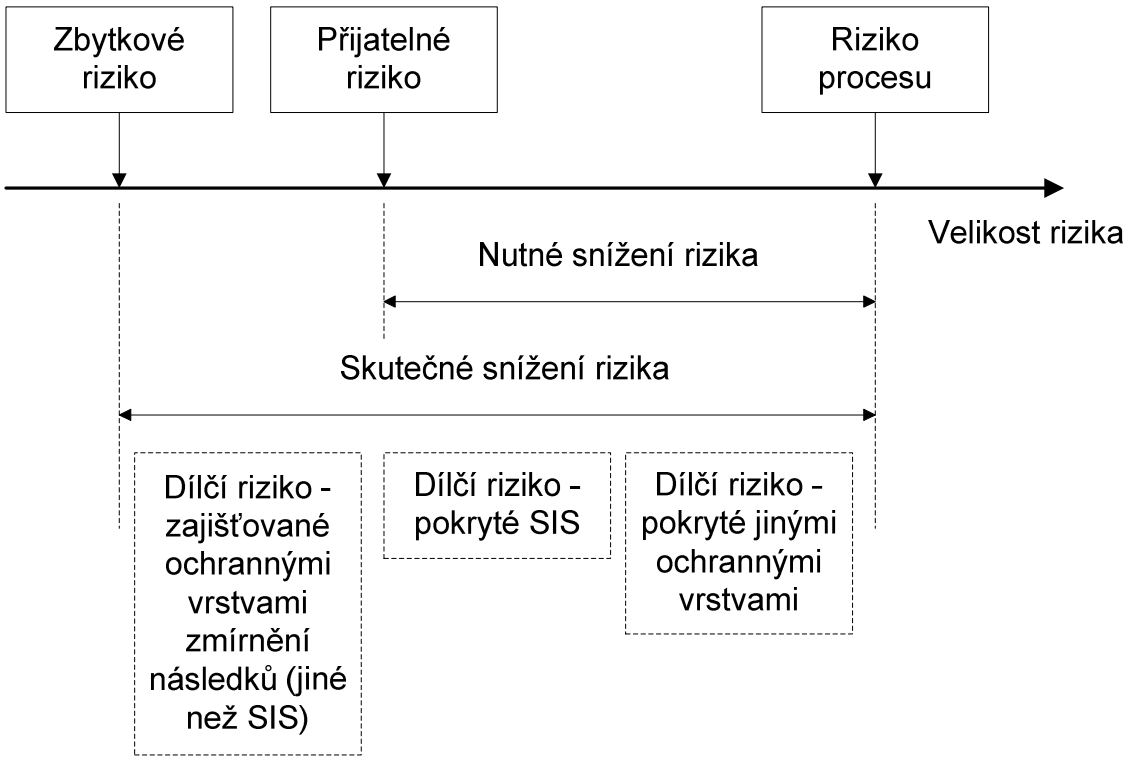
3.3 Posouzení nebezpečí a rizika

Pro posouzení nebezpečí a rizika je normou doporučena komise složená z příslušných expertů. Tato komise pomocí techniky formálního posouzení rizika nebo pomocí studie analýzy nebezpečí a provozuschopnosti (HAZOP - Hazard and Operability study) určí nebezpečné stavy průmyslového procesu. Z nich mohou některé události vést až ke smrti nebo vážnému zranění a tudíž jsou předmětem další studie.

Pomocí studie HAZOP se určí nebezpečí procesu, identifikují se bezpečnostní vrstvy, určí se inicializační události a vytvoří se scénář nebezpečných událostí pro každou iniciační událost. Prakticky se studie HAZOP provádí tak, že vedoucí týmu systematicky vede analyzační tým konstrukcí procesu a používá příslušný soubor „prováděcích“ slov. Studie je podrobně popsána v normě ČSN IEC 61882 Studie nebezpečí a provozuschopnosti (studie HAZOP) - Pokyn k použití.

3.4 Přiřazení bezpečnostních funkcí k ochranným vrstvám

Příklady technik, které se mohou použít pro stanovení SIL bezpečnostních přístrojových systémů uvádí norma ČSN EN 61511-3. K tomu je nutné kvantitativně nebo kvalitativně určit riziko procesu a nutné snížení rizika. Nutné snížení rizika je minimální úroveň snížení rizika, kterého se musí dosáhnout, aby se dosáhlo přijatelného rizika (Obr.5) [14], [15]. Před stanovením potřeby bezpečnostních přístrojových funkcí (SIF – Safety Integrity Function) by se měly vzít v úvahu ochranné vrstvy jiných technologií. Jedná se hlavně o mechanická pojistná zařízení, např. pojišťovací ventil, mechanické dorazy. Ochranné vrstvy zmírnění následků jsou použity s cílem minimalizovat riziko, které již vzniklo. Jsou to např. zdi, náspy.

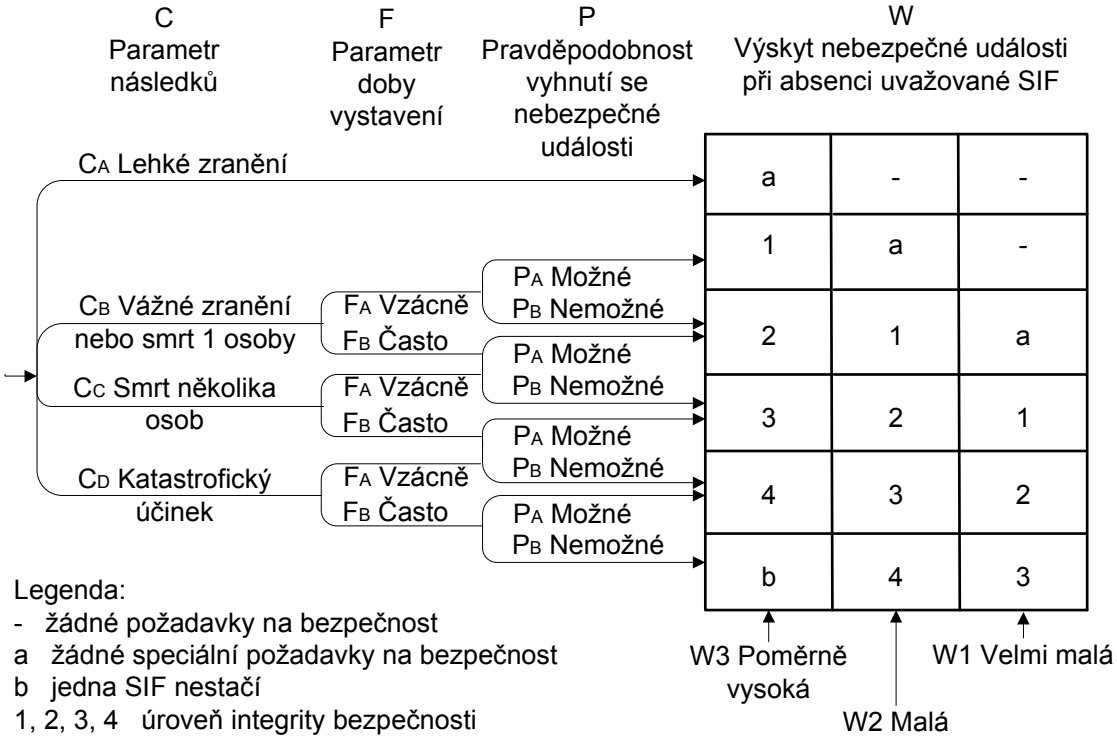


Obr. 5 Obecné zásady snížení rizika

Norma popisuje tyto metody stanovení SIL bezpečnostních přístrojových systémů:

- koncepce nejnižšího rozumně možného a přijatelného rizika (model ALARP)
- semikvantitavní metoda
- metoda matic ochranných vrstev
- analýza vrstvy ochrany (LOPA)
- kvalitativní metoda: diagram rizika
- semikvalitativní metoda: kalibrovaný diagram rizika

Poslední jmenovaná metoda je vhodná pro posouzení úrovně integrity bezpečnosti pro sektor průmyslových procesů při aplikaci rizikových faktorů spojených s procesem a řídícím systémem. Metoda definuje čtyři parametry rizika C, F, P, W (Obr. 6).



Obr. 6 Diagram rizika

Dle EN 61511-3, tabulka D.2 a obrázek D.1 lze bezpečnostní funkce SIF (jednotlivé ochrany) zařadit do příslušných kategorií a přidělit jim nutné minimální snížení rizika. Ve výše jmenované normě je také přesnější popis jednotlivých parametrů. Diagram rizika Obr.6 je obecný a lze ho přizpůsobit konkrétní aplikaci [14].

Normy pro E/E/PES systémy rozdělují bezpečnostní systémy na dva základní typy dle vyžádání:

- *Systémy provozu s velkým nebo trvalým vyžádáním* – jsou to systémy, kde bezpečnostní funkce je jedinou ochranou, pravděpodobnost poruchy je určena hodnotou PFH. Dle normy ČSN IEC 61508 je tento systém definován frekvencí požadavku na SIF a to častěji jak jedenkrát za rok.
- *Systémy provozu s malým vyžádáním* – jsou to systémy, kde bezpečnostní funkci předchází zásah jiného systému, pravděpodobnost poruchy je určena hodnotou PFD. Příkladem z běžného života by mohl být např. airbag v osobním automobilu.

Vzhledem k tomu, že bezpečnostní funkci parních turbín předchází jiné funkce tj. regulační funkce včetně zapůsobení omezovací regulace, výstraha, je tento bezpečnostní systém zařazen do systému provozu s malým vyžádáním.

Systémy zabezpečující bezpečnostní funkci jsou dle normy ČSN EN 61511-1, odstavce 9.2.4 rozděleny do čtyř kategorií SIL (Tab. 3) [12].

SIL Úroveň integrity bezpečnosti	PFD Režim provozu na vyžádání	PFH Průběžný režim provozu (nebezpečné poruchy za hodinu)
4	$\geq 10^{-5}$ až $<10^{-4}$	$\geq 10^{-9}$ až $<10^{-8}$
3	$\geq 10^{-4}$ až $<10^{-3}$	$\geq 10^{-8}$ až $<10^{-7}$
2	$\geq 10^{-3}$ až $<10^{-2}$	$\geq 10^{-7}$ až $<10^{-6}$
1	$\geq 10^{-2}$ až $<10^{-1}$	$\geq 10^{-6}$ až $<10^{-5}$

Tab. 3 Stupně integrity bezpečnosti SIL

Aplikace, které vyžadují v průmyslových procesech použití jedné samotné SIF s úrovní SIL 4 se vyskytují jen zřídka a doporučuje se jim vyhnout.

3.5 Specifikace bezpečnostních požadavků na SIS

Bezpečnostní požadavky na SIS z hlediska návrhu musí zahrnovat zejména:

- Definici bezpečného stavu pro každou SIF
- Požadavky na intervaly kontrolních zkoušek
- Požadavky na dobu odezvy SIF
- Stupeň integrity bezpečnosti SIL a režim vyžádání
- Požadavky na manuální vypínání
- Požadavky na nové nastavení SIS po vypnutí
- Režim poruchy a žádané odezvy v SIS
- Rozhraní mezi SIS a operátorem
- Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS

Je potřeba definovat intervaly kontrolních zkoušek pro jednotlivé komponenty SIS, protože mohou být v rámci jedné SIF rozdílné. Požadavky na dobu odezvy SIF musí vzít v úvahu dynamické chování řízeného procesu.

3.6 Minimální požadavky hardwaru k poruchám

Požadavky na toleranci k náhodným poruchám hardwaru jsou charakterizovány hodnotou HFT (HFT – Hardware Fault Tolerance), která popisuje kvalitu bezpečnostní funkce a znamená schopnost při výskytu poruch dále správně vykonávat funkci. Například při HFT=1 znamená systém s jednoduchou redundancí, kde při výskytu jedné nebezpečné poruchy nedojde k omezení bezpečné činnosti SIS [16].

SIL Úroveň integrity bezpečnosti	HFT Minimální tolerance hardwaru k poruchám		
	SFF < 60%	SFF 60% až 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Zvláštní požadavky		

Tab. 4 Minimální požadavky HFT programovatelných elektronických systémů.

SIL Úroveň integrity bezpečnosti	HFT Minimální tolerance hardwaru k poruchám
1	0
2	1
3	2
4	Zvláštní požadavky

Tab. 5 Minimální požadavky HFT snímačů, koncových členů a neprogramovatelných elektronických členů

Hodnoty HFT v Tab. 5 dle ČSN EN 61511-1 odstavec 11.4.4 mohou být sníženy o jedničku u těch bezpečnostních funkcí, kde je dominantním režimem poruch detekce bezpečného stavu nebo nebezpečných poruch. Další z podmínek je dostupnost dokladů o vhodnosti součástky pro použití v SIS. Doklady mají obsahovat množství provozních zkušeností, zvážení jakosti a managmentu výrobce, předvedení funkčnosti součástek.

Formální posouzení koncového členu pro aplikace SIL3 norma nepředepisuje.V praxi to znamená, že solenoidové ventily jsou při provozu turbíny trvale pod napětím a v případě inicializace bezpečnostní funkce nebo poruchy napájení SIS dojde ke ztrátě napájecího napětí solenoidů a tím i k vypuštění ovládacího oleje rychlozávěrného ventilu a regulačních ventilů turbíny.

3.7 Požadavky na výběr součástek a subsystémů

Při výběru součástek a subsystémů používaných v SIS můžeme postupovat dvěma způsoby. První možností je výběr těch součástek a subsystémů, které splňují požadavky norem ČSN IEC 61508-2 (požadavky na hardware) a ČSN IEC 61508-3 (požadavky na software). Druhou možností je aplikovat součástky a subsystémy, které jsou známy jako spolehlivé (i když nejsou SIL certifikované) a splňují požadavky normy ČSN IEC 61511-2 odstavec 11.5.3. Tato možnost se v praxi bude týkat zejména akčních (koncových) členů, které jsou součástí SIS, ale jsou ovládány pneumatickým nebo hydraulickým systémem. V současné době již existuje dostatečné široká nabídka SIL certifikovaných elektrických, elektronických a programovatelných elektronických systémů.

Součástka nebo subsystém musí splňovat tyto základní požadavky:

- Je natolik spolehlivá, že dosáhne požadované PFD (PFH)
- Splňuje požadavek minimální tolerance hardwaru k poruchám HFT
- Má dostatečně nízkou pravděpodobnost systematických poruch

Při návrhu systému SIS z hlediska projektanta (uživatele) se musí vzít v úvahu:

- Hardwarovou architekturu, HFT
- Dobu odezvy systému SIS
- Požadavky na napájení, včetně monitorování podpětí a přepětí
- Požadavky na vlivy okolního prostředí, indikace poruchy zařízení upravující okolní podmínky
- Požadavky na rozhraní operátora, indikace automatického zásahu SIS, indikace přemostění SIS, indikace výstrah a poruch SIS, ve kterém místě postupu se nachází proces a SIS

- Testování funkčnosti SIS a to jak softwaru nebo hardwaru, pokud to není součástí komponenty
- Požadavky na technické rozhraní pro údržbu a zkoušení

K výše uvedenému je potřeba doplnit, že spínače přemostění (bypass) musí být chráněny heslem nebo zámkem, tak aby se zabránilo neautorizovanému použití. Návrh SIS musí umožnit zkoušení vcelku nebo po částech. Pokud je interval mezi předepsanými prostoji větší než interval mezi kontrolními zkouškami, je nutné použití vybavení pro průběžné zkoušení.

3.8 Výpočet pravděpodobnosti poruch

Pro výpočet pravděpodobnosti poruch na vyžádání bezpečnostní funkce existují níže vyjmenované metody, které obsahují.

- Simulaci
- Analýzu příčin a následků
- Analýzu stromu poruch (FTA – Fault Tree Analysis)
- Markovovy modely
- Blokové diagramy spolehlivosti (RBD – Reliability Block Diagram)
- Bezporuchovostní blokové schémata

Nejjednodušší a zřejmě nejpoužívanější metodou je metoda bezporuchovostních schémat. Tuto metodu nelze plně použít pro systémy, které se asymetricky větví. Další nevýhodou je její nižší přesnost výpočtu, což v praxi nezpůsobuje zásadní problémy, protože je nutné dodržet příslušné číselné intervaly na úrovni řádů. Pro vlastní výpočet v praktické části práce bude použita metoda FTA (popsána v kapitole 2), která nemá nedostatky metody bezporuchovostních schémat. Ve vlastním výpočtu FTA se pracuje s hodnotami pravděpodobnosti poruchy, ale dostupné hodnoty od jednotlivých součástí jsou v jiných charakteristických hodnotách, proto je nutné provést přípravný výpočet.

Vzorce použité pro výpočet pravděpodobnosti poruchy jsou platné za předpokladu, že intenzita poruch λ je konstantní, t.j. SIS systém se nachází v prostřední oblasti vanové křivky a rozdělení pravděpodobnosti je exponenciální. Při hodnotě času MTTF,

vyjádřeného v hodinách, je pravděpodobnost bezporuchové funkce 36,8% [17]. V literatuře se objevuje i označení $MTTF_d$, aby se zdůraznilo, že jde o nebezpečné poruchy.

$$\lambda = \frac{1}{MTTF} \text{ pro obnovitelné zařízení} \tag{16}$$

$$\lambda = \frac{1}{MCTF} \text{ pro neobnovitelné zařízení} \tag{17}$$

Většina výrobců zařízení uvádí hodnotu MTBF a to v hodinách, rocích nebo v jednotkách FIT (1 FIT = 1 porucha /10^9 hodin). MTBF vyjadřuje střední dobu mezi poruchami, která se skládá ze střední doby do poruchy a střední doby do zotavení. Ve většině případů je hodnota MTTR zanedbatelně nízká vůči hodnotě MTBF. Hodnota MTTR je méně než 24 hodin, typicky 8 hodin.

$$MTBF = MTTF + MTTR \tag{18}$$

Pro diskrétní mechanické součásti jako např. relé, tlačítka, ventily se udává hodnota MCTF, která zastupuje hodnotu MTTF. Následné výpočty jsou prováděny stejně jako s hodnotou MTTF. Výrobci často uvádí hodnotu B_{10}, což je statistické 10% rozhraní pro životnost součástí. Potom můžeme tuto hodnotu při znalosti četnosti spínání C přepočítat na hodnotu MCTF. V podstatě se jedná o přibližný převod z Weibullova rozdělení na exponenciální rozdělení.

$$MCTF = \frac{B_{10}}{0{,}1 \cdot C} \tag{19}$$

Intenzita poruch se dělí na nebezpečné a bezpečné.

$$\lambda = \lambda_D + \lambda_S \tag{20}$$

Ta se dále dělí na zjištěné a nezjištěné.

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{21}$$

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \tag{22}$$

Pro další výpočet se předpokládá exponenciální rozdělení intenzity poruch.

$$PFD = 1 - e^{-\lambda_D \cdot t_{CE}} \tag{23}$$

Ekvivalentní střední doba prostoje kanálu, posuzuje kanál tak, jako by byl složen ze dvou sériově uspořádaných částí. Jedna s intenzitou nezjištěných nebezpečných poruch a druhá s intenzitou zjištěných nebezpečných poruch. V literatuře [6] se někdy uvádí jako MDT (Mean Down Time).

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{24}$$

Ve výpočtech se z důvodu zjednodušení vychází z předpokladu, že

$$PFD \approx \lambda_D \cdot t_{CE} \text{ za podmínky } \lambda_D \cdot t_{CE} << 1 \tag{25}$$

Podíl bezpečných poruch uvádí poměr intenzity bezpečných poruch a intenzity poruch. Ze vzorce (26) také vyplývá, že pokud SR=0, pak $\lambda_D = \lambda$.

$$SR = \frac{\lambda_S}{\lambda} \text{ z toho plyne } \lambda_D = \lambda \cdot (1 - SR) \tag{26}$$

Diagnostické pokrytí vyjadřuje poměr intenzity nezjištěných nebezpečných poruch a intenzity nebezpečných poruch. Hodnota DC >0% je u zařízení, která mají diagnostiku hlídající SIS nebo její subsystém. Ve většině případů v elektrotechnice jsou to zařízení, která obsahují procesor, např. PLC systémy a SMART převodníky. U systémů pracujících na jiných principech (mechanickém, hydraulickém, pneumatickém) se hodnota uvádí tam, kde je možno testovat prvek za provozu systému, aniž by to ovlivnilo jeho funkci, např. při částečném posunutí pístu [17]. Ze vzorce (27) také vyplývá, že pokud DC=0, pak $\lambda_{DU} = \lambda_D$.

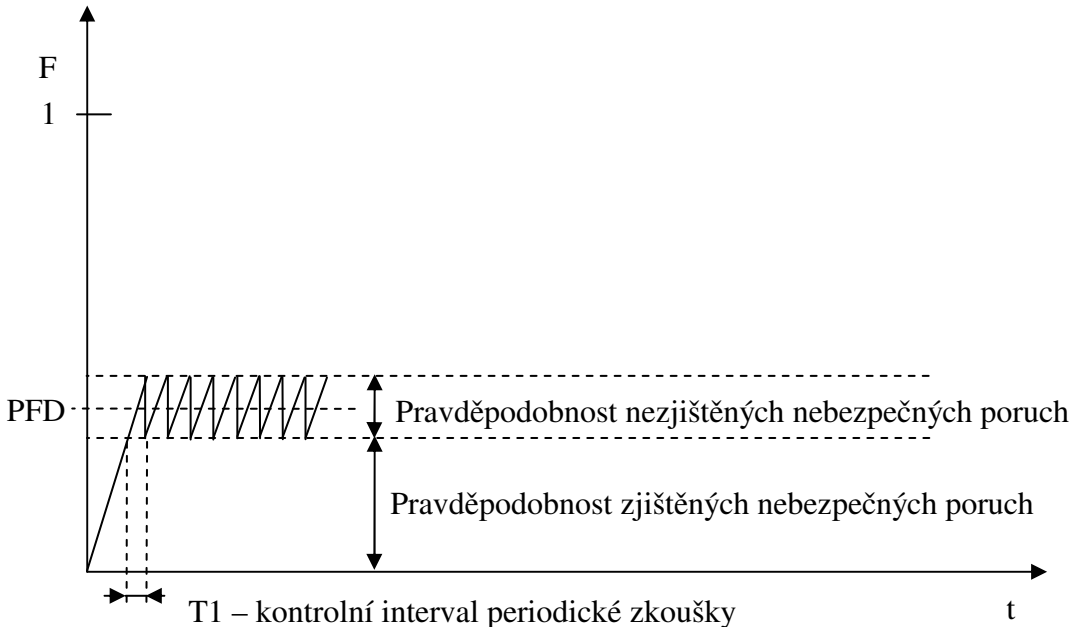
$$DC = \frac{\lambda_{DD}}{\lambda_D} \text{ z toho plyne } \lambda_{DU} = \lambda_D \cdot (1 - DC) \tag{27}$$

Podíl bezpečných výpadků

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \text{ z toho plyne } SFF = 1 - \frac{\lambda_{DU}}{\lambda} \tag{28}$$

Průměrná pravděpodobnost poruchy při vyžádání

$$PFD = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \tag{29}$$



Obr. 7 Průměrná pravděpodobnost poruchy při vyžádání

3.9 Poruchy se společnou příčinou

Výše popsané metody výpočtu vychází z předpokladu, že jednotlivé poruchy jsou náhodné a nezávislé i pro redundantní systém. Při redundanci součástí nebo subsystémů provedené opakovaným použitím stejného typu může dojít k systematické, závislé poruše způsobené společnou příčinou. Porucha se společnou příčinou (CCF – Common Case Failure) je dle normy ČSN IEC 61508-6 příloha D popsána činitelem společných poruch pro nezjistitelné nebezpečné poruchy β a činitelem společných poruch pro zjistitelné nebezpečné poruchy β_D. V literatuře [6] je popsán zjednodušený model beta plus, kde se určuje pouze činitel nebezpečné poruchy β, který je nelineární. Činitelé nabývají hodnot od 0% až po 25 %. Systematické společné poruchy mohou být způsobeny například:

- Chybou návrhu SIS
- Použitím nevhodného hardwaru
- Chyby softwaru
- Chyby člověka
- Chyby návrhu hardwaru
- Chyba úpravy systému

Při určení činitelů nebezpečných poruch β a β_D se berou v úvahu tato kritéria:

- Separace, segregace
- Diversifikace
- Komplexivita, konstrukce, zkušenosti
- Analýza a zpětná vazba dat
- Rozhraní operátora
- Způsobilost, školení, povědomí o bezpečnosti
- Úprava a testování okolních podmínek

Vlastní určení činitelů nebezpečných poruch β a β_D je dáno bodovým ohodnocením parametrů X, Y, Z, s tím, že výsledné parametry S a S_D jsou převedeny tabulkou na hodnotu β a β_D vyjádřenou v procentech [11].

$$S = X + Y \tag{30}$$

$$S_D = X \cdot (Z + 1) + Y \tag{31}$$

Poruchy se společnou příčinou je nutné zohlednit ve výpočtu celkové poruchovosti systému. U metody blokových diagramů spolehlivosti lze hodnotu CCF zařadit za redundantní blok do série. U analýzy stromu poruchových stavů je použito hradlo OR, jehož jedním vstupem je majoritní hradlo a druhým vstupem CCF. Hodnoty λ_{DD}, λ_{DU}, MTTR a T_1 jsou shodné s redundantními součástmi a subsystémy, které posuzujeme z hlediska CCF [6].

$$CCF = \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) \tag{32}$$

3.10 Požadavky na aplikační software

V současné době je mnoho součástek a subsystémů programovatelných (dle normy se jedná o zařízení typu PES). Požadavky na software jsou jednotné pro kategorie SIL 1, 2, 3 [18]. V případě použití v SIS, musí být posuzován i software a ten můžeme rozdělit do těchto kategorií:

- Aplikační software
- Obslužný software, nástroje používané k vývoji a verifikaci aplikačního softwaru
- Vestavěný software, dodávaný jako součást programovatelných elektronických systémů

Druhy vývojových softwarových jazyků:

- Pevný programovací jazyk (FPL – Fixed Program Language)
- Jazyk s omezenou variabilitou (LVL – Limited Variability language)
- Jazyk s plnou variabilitou (FVL – Full Variability language)

FPL je používán v mnoha jednodušších jednoúčelových zařízeních jako jsou např. SMART převodníky, SMART pozicionery, zařízení pro monitorování chodu strojů. Tyto přístroje dovolí uživateli pouze nastavení parametrů souvisejících s provozem jako např. měřící rozsah, tlumení. Přístroj nedovolí změnu funkce uživatelem. Jazyk je na uživatelské úrovni pevný a dodavatel ve své technické dokumentaci popisuje nastavitelné parametry. Tyto přístroje podstoupily typicky rozsáhlé zkoušky a nepředpokládají se u nich systematické poruchy způsobené softwarem.

LVL jsou více flexibilní než FPL. Tyto jazyky se skládají z předdefinovaných a testovaných funkcí. Jsou to typicky jazyky definované normou ČSN IEC 61131 pro použití v PLC systémech. Jedná se o jazyk kontaktních schémat (LD - Ladder Diagram), jazyk logických schémat (FBD – Function Block Diagram), jazyk sekvenčního programování (SFC – Sequential Function Chart), jazyk mnemokódů (IL – Instruction List) a strukturovaný textový jazyk (ST – Structured Text). Tyto jazyky dovolí uživateli měnit konfiguraci funkcí nebo programu. Výrobce dodává s programovacím nástrojem knihovnu funkcí, která je použita do aplikačního programu.

FVL představiteli jsou programovací jazyky, jako např. C++ nebo Pascal. Tento typ jazyka využívá operační systém, který poskytuje systémové přidělení zdrojů a real time prostředí.

Použití těchto jazyků je omezené na počítačové odborníky, kteří programují software na zakázku. U programovatelných elektronických zařízení je možné tento software nalézt jako zabudovaný (embedded) v zařízení, někdy je nazýván firmware [19].

Protože norma ČSN EN 61511 je určena pro projektanty průmyslových procesů a ne pro výrobce jednotlivých součástek a subsystémů, určuje požadavky pouze na přístroje se softwarem typu FPL a LVL. Přístroje se softwarem typu FVL jsou řešeny normou ČSN EN 61508.

Aplikační program je složen s použitím softwarových nástrojů a knihovny funkcí. Pokud má být software bezchybný je potřeba, aby výrobce LVL software měl plně testované výše uvedené části aplikačního programu a to nezávislou osobou nebo organizací. Pro usnadnění testování aplikace obsahuje obslužný software nástroje, které pomáhají verifikovat funkčnost a integritu. Standardním kontrolním modelem na kontrolu aplikace je „V“ model, kde na jedné straně jsou návrhové kroky a na straně druhé jejich jednotlivá zkoušení a verifikace.

Při vytváření aplikačního programu je nutné vzít v úvahu:

- Vytvoření slovního popisu funkce aplikačního programu
- Splnění požadavků na časovou odezvu řídícího systému
- Funkčnost bezpečnostní logiky obslužného softwaru (priority I/O, komunikace, diagnostika systému)
- Nebezpečí, která mohou vzniknout při přechodných dějích (zapnutí, vypnutí napájení)
- Separace SIF od ostatních funkcí, separace jednotlivých SIF vzájemně a vyznačení SIF
- Pořízení druhé nezávislé analýzy, verifikace a validace jinou osobou
- Ochrana programu proti neautorizovanému zásahu heslem
- Architekturu hardwaru (redundanci snímačů, I/O, komunikace, akčních členů)
- Diagnostiku vstupů (překročení, podkročení měřícího rozsahu, drift)
- Automatické zkoušení SIS, přemostění SIS při údržbě
- Uvádět revizi programu – managament změn

Testování aplikačního programu se musí provádět na skutečně použitém hardware a to jak použitím simulátorů, tak emulátorů. Je nutné odzkoušet všechny odezvy SIF a poruchy

obvodu SIS, jako jsou např. poruchy procesoru, porucha vstupní a výstupní karty, porucha komunikace. Současně se testuje i výstražné hlášení a rozhraní pro operátora. Uvedené požadavky jsou důležité, protože na rozdíl od hardwaru s náhodnými poruchami, zde se bude jednat o závislé chyby způsobené programátorem a obslužným softwarem, u kterých nelze určit intenzitu poruch [13].

3.11 Požadavky na další fáze životního cyklu

Po ukončení výroby SIS následuje tovární přejímací zkouška (FAT – Factory Acceptance Test), jejímž cílem je vyzkoušet logický automat a k němu přiřazený software. Pro tyto účely je zapotřebí specifikovat druhy potřebných zkoušek a zkušební kritéria. Výsledek FAT má být zadokumentován i s provedenými modifikacemi SIS, aby se určil vliv na dosažení příslušné integrity bezpečnosti SIL.

Při instalaci SIS je nutné zkontrolovat, zda montáž a umístění jsou provedeny dle návrhu a instalačních plánů. Kontrola zahrnuje uzemnění, napájení, fyzickou neporušenost, zda jsou přístroje kalibrovány a funkčnost systému včetně návazností.

Validace bezpečnosti SIS se provádí při místní přejímací zkoušce (SAT – Site Acceptance Test). Cílem je validovat, že SIS odpovídá stanoveným požadavkům určeným na začátku životního cyklu. Při validaci se zjišťuje funkčnost snímačů, logického automatu, akčních členů, rozhraní operátora, a to při různých režimech procesu. Jedná se o poslední krok kontroly před spuštěním technologického procesu, proto jsou požadavky na testy a dokumentaci rozsáhlé - jsou popsány v ČSN IEC 61511-1 odstavec 15.2.4.

Provoz a údržba SIS, při této fázi životního cyklu se předpokládá, že SIS dosahuje po zbytek svého provozu stanovené úrovně integrity bezpečnosti. Faktorem, který ovlivňuje kvalitu funkce, je testování v pravidelných intervalech. Aby se minimalizovala cena údržby a ztráty při odstávce technologie, je vhodné, aby se už při návrhu uvažovalo s jednotným intervalem testování pro všechny SIF [12].

II. PRAKTICKÁ ČÁST

4 FUNKČNÍ BEZPEČNOST V PRAXI

4.1 Popis technologie

Praktická část práce se bude zabývat výpočtem funkční bezpečnosti systému ochran parní turbíny. Parní turbíny v Siemens Industrial turbomachinery Brno s.r.o. (bývalá První brněnská strojírna) jsou vyráběny v rozsahu výkonu 2,5 až 150 MW. Převážná část aplikací je průmyslová, tj. jejich účelem není vyrábět pouze elektrickou energii, ale i redukovat parametry páry pro další využití v průmyslové výrobě nebo za účelem vytápění. V současné době se používá nová koncepce dodávek turbosoustrojí pro výkony do cca 45 MW, kde turbína, převodovka a generátor jsou umístěny na kovovém rámu. Na rámu jsou umístěna i další pomocná zařízení, mezi něž patří systém dodávky mazacího a regulačního oleje, olejový systém zabezpečení turbíny, olejový systém regulace turbíny a elektronický systém pro sběr dat. Na takovém „turbínovém balíčku“ jsou osazeny i snímače pro zabezpečení, regulaci a monitorování turbosoustrojí. Informace z těchto snímačů mohou být použity i pro vibrační diagnostiku a pro automatické najíždění a zatěžování turbíny. Kompletace „turbínového balíčku“ je prováděna přímo ve výrobním podniku.

Řídící systém turbosoustrojí s označením TORLOOP S7 byl navržen tak, aby splňoval funkční, bezpečnostní a topologické požadavky. Snímače umístěné na „turbínovém balíčku“ jsou prokabelovány do elektronického systému pro sběr dat tj. do místního rozvaděče řídícího systému turbíny. Tento panel obsahuje kromě pomocných obvodů i inteligentní vstupně/výstupní moduly od fy Siemens ET200M a vyhodnocovací aparaturu pro měření vibrací turbosoustrojí od fy Bently Nevada typové řady 3500. Architektura modulů ET200M je tvořena třemi nezávisle a paralelně pracujícími kanály, včetně ztrojení funkčně důležitých snímačů. Komunikace se vzdáleným rozvaděčem umístěným v místnosti rozvaděčů je optickými kabely pomocí protokolu Profibus DP a je rovněž ztrojená. V tomto rozvaděči jsou umístěny dva rámy programovatelných automatů (PLC) od fy Siemens SIMATIC S7-400 a aparatura pro vyhodnocení otáček od fy Epro s označením DOPS. Jeden systém PLC je určen pro funkci regulace turbíny a druhý pro zabezpečení a sekvenční řízení pomocných zařízení turbosoustrojí. Systémy PLC jsou vzájemně propojeny sériovou komunikací Profibus DP, která zajišťuje výměnu potřebných informací. Pro styk systému s obsluhou je na velínu umístěno operátorské pracoviště obsahující průmyslové PC s příslušenstvím a s vizualizačním SW od fy Siemens WinCC.

Komunikace mezi operátorským pracovištěm a rozvaděčem řídícího systému na velínu je pomocí sériové komunikace Industrial Ethernet. Podrobný výkres konfigurace řídícího systému je uveden v příloze P I [21].

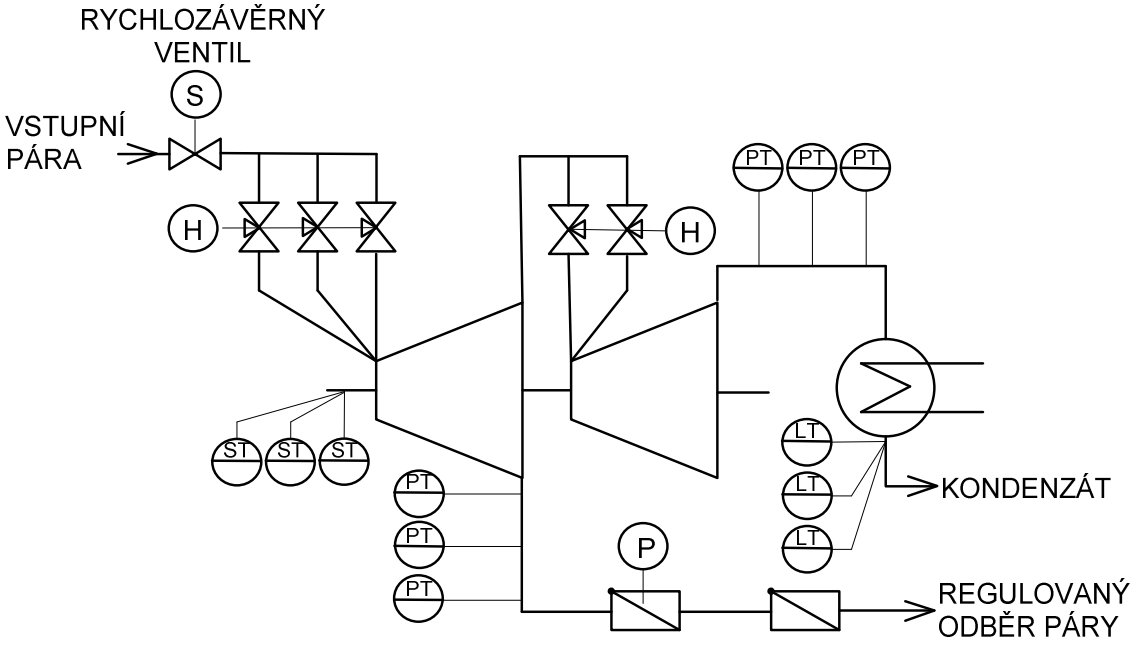
Mechanické prvky zabezpečení turbíny tvoří rychlozávěrný ventil a regulační ventily. Ventily jsou ovládány hydraulickými servomotory, které jsou napájeny olejem z hydraulického regulačního a zabezpečovacího systému turbíny. Ventily jsou zapojeny v sérii na přívodu vstupní páry do turbíny. Oba servomotory jsou jednočinné s poruchovou funkcí „failure close“.

Je potřeba se zmínit, že turbína má i další zabezpečovací orgány, které jsou použity v závislosti na konstrukci turbíny. Mezi ně patří zpětné odběrové klapky s i bez pneumatického servomotoru a standardní uzavírací ventily s pneumatickými servomotory na odběru páry. Tyto orgány mají také bezprostřední vliv na bezpečnost turbíny.

Médiem (parou) poháněný servomotor rychlozávěrného ventilu dosahuje poloh otevřeno, zavřeno a je ovládám blokem hydraulického olejového vypínače. Tento hydraulický olejový vypínač obsahuje tři solenoidové ventily a diferenciální píst, který provádí hydraulicky výběr 2 ze 3. Jsou zde také osazeny tři převodníky tlaku, které monitorují stav solenoidových ventilů a jeden převodník umístěný na výstupu z hydraulického vypínače.

Servomotor regulačních ventilů je plynule nastavitelný pomocí elektro-hydraulického převodníku od fy VOITH typu E360. Žádaná hodnota otevření ve formě 4-20mA je přiváděna z regulačního systému turbíny a v převodníku převedena na hodnotu 2 – 4 bar g [18]. V případě zapůsobení bloku olejového vypínače, je pomocí hydraulického rozvaděče vypouštěn pracovní olej i ze servomotoru regulačních ventilů.

Předpokládám, že praktická část této práce bude sloužit spíše jako příklad k určení příslušných SIF, protože technologie parních turbosoustrojí je různorodá a pro závazné určení skutečného nebezpečí je nutné ustanovit komisi z odborníků různých profesí. Pro základní přehled problému je na obr. 8 zjednodušené procesní schéma kondenzační parní turbíny s jedním regulovaným odběrem. Na tomto schématu jsou zobrazeny pouze ty prvky, které mají souvislost s funkční bezpečností.



Obr. 8 Zjednodušené procesní schéma

4.2 Posouzení nebezpečí a rizika

Vzhledem k velikosti tabulky je posouzení nebezpečí a rizika uvedeno v příloze P II. Jsou zde uvedeny pouze ty ochranné funkce turbosoustrojí, které jsou „safety related“, tj. jsou zařazeny do některého stupně integrity bezpečnosti. Avšak i toto zařazení je podmíněno splněním určitých podmínek. Tyto podmínky souvisí s dispozicí turbíny a příslušenství, s konstrukcí lopatek posledních stupňů turbíny, použitím obtokové stanice a s případným použitím pojistných ventilů na 100% průtoku páry.

4.3 Přiřazení bezpečnostních funkcí k ochranným vrstvám

Přiřazení bezpečnostních funkcí k ochranným vrstvám je provedeno na základě tabulky posouzení nebezpečí a rizika uvedené v příloze P II. Číslo řádku v Tab. 6 odpovídá číslu řádku uvedené v tabulce přílohy P II.

P. č.	Č. ř. přílohy P II	Bezpečnostní funkce SIS	Parametry diagramu rizika				Stupeň integrity bezpečnosti SIL
			C	F	P	W	
1	1, 2	Vysoké otáčky.	C_C	F_B	P_B	W_2	3
2	3, 4	Vysoký tlak páry na výstupu.	C_B	F_A	P_B	W_2	1 (*
3	5	Vysoká hladina v kondenzátoru.	C_B	F_A	P_B	W_2	1 (*
4	6	Vysoký tlak páry v regulovaném odběru.	C_B	F_A	P_B	W_2	1 (*
5	7	Signál externí požadavek na odstavení.	C_B	F_A	P_B	W_2	1
6	8	Tlačítko nebezpečí pro turbínu	C_B	F_A	P_B	W_2	1

(* pouze za určitých podmínek uvedených v tabulce přílohy P II

Tab. 6 Přiřazení bezpečnostních funkcí

4.4 Specifikace bezpečnostních požadavků na SIS

Název SIF: *Vysoké otáčky.*

Funkce SIF: Při otáčkách $>n_{vyp}$ systém ochran odstaví turbínu uzavřením rychlozávěrného ventilu a regulačních ventilů. Jedna ze dvou zpětných odběrových klapek je vybavena servomotorem pro překonání pasivních odporů klapky. Tento servomotor pomocí elektrického signálu pomůže uvolnit klapku.

Bezpečný stav SIF: Uzavření přívodu páry. Zastavení rotorové soustavy, popřípadě protáčení pomocí otáčecího zařízení turbíny. Nebo při plánovaném testu otáčky turbosoustrojí nižší než jmenovité.

Kontrolní interval T_1 SIF: Vzhledem k provozu turbosoustrojí je nutné minimálně každý rok provést odstavení turbíny zkouškou skutečným převýšením otáček.

Doba odezvy SIF: Turbosoustrojí nesmí dosáhnout vyšších otáček než předepsaných. Jedná se o dynamický děj, při kterém se vychází z doby rozběhu rotorové soustavy a z vlivu sekundární expanze páry po uzavření akčních orgánů. Dále je nutné

uvažovat zpoždění ve vyhodnocování otáček, zpoždění v hydraulickém systému olejového vypínače a zpoždění akčních orgánů.

Režim vyžádání a stupeň SIL: Jedná se o systém provozu s malým vyžádáním, protože zásahu systému ochran předchází regulační funkce. Stupeň integrity bezpečnosti je SIL 3.

Nové nastavení SIS po vypnutí: Systém ochran má paměť, která vyžaduje potvrzení operátora pro nové nastavení. Systém ochran nastaví regulátor turbíny do výchozího stavu.

Požadavky na manuální vypínání: Nejsou žádné zvláštní požadavky.

Režim poruchy a žádané odezvy v SIS: V případě detekce poruchy na jednom měřícím kanále ze tří nedojde k odstavení turbíny. Operátor obdrží výstrahu přes operátorskou stanici. Porucha musí být odstraněna do doby dalšího testu převýšení otáček simulací (zkušební interval 1 měsíc). Turbína nesmí být spuštěna s touto poruchou. Při poruše dvou kanálů ze tří bude turbína odstavena systémem ochran automaticky. V případě nebezpečné poruchy regulátoru dojde k odstavení turbíny systémem ochran.

Rozhraní mezi SIS a operátorem: Veškeré provozní a diagnostické informace jsou zobrazovány na operátorské stanici. Při dosažení hodnoty ochrany nebo výstrahy se spustí zvuková signalizace.

Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS: V případě selhání SIS (systému ochran turbíny) dojde k uzavření regulačních ventilů regulátorem turbíny. Je nutné uzavřít oddělovací armatury, tj. hlavní uzavírací armaturu a armaturu regulovaného odběru. V případě selhání nebo netěsnosti rychlozávěrného ventilu a regulačních ventilů turbíny nebo zpětných odběrových klapek nedojde k dosažení motorického chodu generátoru. Zpětná wattová ochrana generátoru neodpojí generátorový vypínač a turbosoustrojí bude udržováno na provozních otáčkách generátorem a sítí.

Název SIF: *Vysoký tlak páry na výstupu.*

Funkce SIF: Při tlaku páry na výstupu z turbíny $>p_{vyp}$ systém ochran odstaví turbínu. Při určení hodnoty $>p_{vyp}$ se musí vycházet z konstrukčních kritérií kondenzátoru a turbíny. Ve speciálních případech je nutné hodnotu $>p_{vyp}$ přestavovat v závislosti na průtoku páry výstupu z turbíny.

Bezpečný stav SIF: Uzavření přívodu páry. Zastavení rotorové soustavy, popřípadě protáčení pomocí otáčecího zařízení turbíny.

Kontrolní interval T_1 SIF: Vzhledem k intervalům generálních oprav turbosoustrojí je nutné každých 5 let provést odstavení turbíny simulací tlaků na procesním přípoji převodníků tlaku.

Doba odezvy SIF: Při poruše na kondenzátním nebo evakuačním systému nemůže dojít ke skokové změně průtoku páry a to z důvodu velkých parních objemů výstupního hrdla a kondenzátoru. Nejsou zde kladeny speciální podmínky na dobu odezvy SIF. Doba odezvy bude menší než 2 sekundy.

Režim vyžádání a stupeň SIL: Jedná se o systém provozu s malým vyžádáním, protože zásahu systému ochran předchází regulační funkce. Stupeň integrity bezpečnosti je SIL 1.

Nové nastavení SIS po vypnutí: Systém ochran má paměť, která vyžaduje potvrzení operátora pro nové nastavení. Systém ochran nastaví regulátor turbíny do výchozího stavu.

Požadavky na manuální vypínání: Nejsou žádné zvláštní požadavky.

Režim poruchy a žádané odezvy v SIS: V případě detekce poruchy na jednom měřícím kanále ze tří nedojde k odstavení turbíny. Operátor obdrží výstrahu přes operátorskou stanici. Porucha musí být odstraněna v průběhu nejbližší odstávky turbosoustrojí. Při poruše dvou kanálů ze tří bude turbína odstavena systémem ochran automaticky. V případě nebezpečné poruchy regulátoru dojde k odstavení turbíny systémem ochran. V případě poruchy měření průtoku páry výstupu z turbíny (pokud je požadováno) se přestaví vypínací hodnota $>p_{vyp}$ na přísnější hodnotu.

Rozhraní mezi SIS a operátorem: Veškeré provozní a diagnostické informace jsou zobrazovány na operátorské stanici. Při dosažení hodnoty ochrany nebo výstrahy se spustí zvuková signalizace.

Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS: V případě selhání SIS (PLC systému ochran turbíny) je možné odstavit turbínu tlačítkem nebezpečí pro turbínu, protože tato SIF je hardwarově nezávislá na PLC. V případě selhání SIS (systému ochran turbíny) dojde k uzavření regulačních ventilů regulátorem turbíny. V případě selhání SIS (převodníků tlaku) bude turbína odstavena ochranou od vysokých vibrací turbíny až po vzniku události (není součástí SIS). Je nutné uzavřít oddělovací armatury, tj. hlavní uzavírací armaturu a armaturu regulovaného odběru. V případě selhání nebo netěsnosti rychlozávěrného ventilu a regulačních ventilů turbíny nebo zpětných odběrových klapek dojde k roztržení pojistné membrány.

Název SIF: *Vysoká hladina v kondenzátoru.*

Funkce SIF: Při výšce hladiny kondenzátu v kondenzátoru $>h_{vyp}$ systém ochran odstaví turbínu. Při určení hodnoty $>h_{vyp}$ se musí vycházet z dispozičního uspořádání kondenzátoru, odvodnění a turbíny. Pokud nehrozí zaplavení turbíny kondenzátem, tato SIF není aplikována.

Bezpečný stav SIF: Uzavření přívodu páry. Zastavení rotorové soustavy, popřípadě protáčení pomocí otáčecího zařízení turbíny.

Kontrolní interval T_1 SIF: Vzhledem k intervalům generálních oprav turbosoustrojí je nutné každých 5 let provést odstavení turbíny simulací hladin na procesním přípoji převodníků.

Doba odezvy SIF: Při aktivaci bezpečnostní funkce je objem kondenzátního systému dostatečně velký, aby pojal kondenzát z parních prostorů. Nejsou zde kladeny speciální podmínky na dobu odezvy SIF. Doba odezvy bude menší než 2 sekundy.

Režim vyžádání a stupeň SIL: Jedná se o systém provozu s malým vyžádáním, protože zásahu systému ochran předchází regulační funkce nebo záskok (teplá záloha) kondenzátního čerpadla. Stupeň integrity bezpečnosti je SIL 1.

Nové nastavení SIS po vypnutí: Systém ochran má paměť, která vyžaduje potvrzení operátora pro nové nastavení. Systém ochran nastaví regulátor turbíny do výchozího stavu.

Požadavky na manuální vypínání: V případě doplňování kondenzátu do kondenzátoru, uzavření systému pro doplňování kondenzátu.

Režim poruchy a žádané odezvy v SIS: V případě detekce poruchy na jednom měřícím kanále ze tří nedojde k odstavení turbíny. Operátor obdrží výstrahu přes operátorskou stanici. Porucha musí být odstraněna v průběhu nejbližší odstávky turbosoustrojí. Při poruše dvou kanálů ze tří bude turbína odstavena systémem ochran automaticky.

Rozhraní mezi SIS a operátorem: Veškeré provozní a diagnostické informace jsou zobrazovány na operátorské stanici. Při dosažení hodnoty ochrany nebo výstrahy se spustí zvuková signalizace.

Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS: V případě selhání SIS (PLC systému ochran turbíny) je možné odstavit turbínu tlačítkem nebezpečí pro turbínu, protože tato SIF je hardwarově nezávislá na PLC. V případě selhání SIS (převodníků hladiny) bude turbína odstavena ochranou od vysokých vibrací turbíny až po vzniku události (není součástí SIS). Je nutné uzavřít oddělovací armatury, tj. hlavní uzavírací armaturu a armaturu regulovaného odběru.

Název SIF: *Vysoký tlak páry v regulovaném odběru.*

Funkce SIF: Při tlaku páry v regulovaném odběru turbíny $>p_{vyp}$ systém ochran odstaví turbínu. Při určení hodnoty $>p_{vyp}$ se musí vycházet z konstrukčních kritérií potrubí, popřípadě turbíny.

Bezpečný stav SIF: Uzavření přívodu páry. Zastavení rotorové soustavy, popřípadě protáčení pomocí otáčecího zařízení turbíny.

Kontrolní interval T_1 SIF: Vzhledem k intervalům generálních oprav turbosoustrojí je nutné každých 5 let provést odstavení turbíny simulací tlaků na procesním přípoji převodníků tlaku.

Doba odezvy SIF: Při poruše regulačních ventilů regulovaného odběru turbíny (ve smyslu uzavření) může dojít ke skokové změně průtoku do nízkotlaké části turbíny a tím ke zvýšení (vzdutí) tlaku v regulovaném odběru. Na tento podnět musí reagovat regulační ventily vstupní páry zavíráním. Pokud zavření těchto ventilů není

dostatečně rychlé, dojde ke zvýšení tlaku na hodnotu $>p_{vyp}$. Jedná se o dynamický děj, při kterém se vychází z doby uzavření regulačních ventilů vstupní páry, rychlosti zavírání regulačních ventilů regulovaného odběru (na mechanický doraz) a z vlivu sekundární expanze páry po uzavření akčních orgánů. Dále je nutné uvažovat zpoždění ve vyhodnocení (snímač tlaku a systém ochran), zpoždění v hydraulickém systému olejového vypínače a zpoždění akčních orgánů na přívodu páry. Vzhledem k množství faktorů, které ovlivňují dynamiku soustavy, mohou být kladeny speciální podmínky na dobu odezvy SIF. Typická doba odezvy bude menší než 1 sekunda.

Režim vyžádání a stupeň SIL: Jedná se o systém provozu s malým vyžádáním, protože zásahu systému ochran předchází regulační funkce. Stupeň integrity bezpečnosti je SIL 1.

Nové nastavení SIS po vypnutí: Systém ochran má paměť, která vyžaduje potvrzení operátora pro nové nastavení. Systém ochran nastaví regulátor turbíny do výchozího stavu.

Požadavky na manuální vypínání: Nejsou žádné zvláštní požadavky.

Režim poruchy a žádané odezvy v SIS: V případě detekce poruchy na jednom měřícím kanále ze tří nedojde k odstavení turbíny. Operátor obdrží výstrahu přes operátorskou stanici. Porucha musí být odstraněna v průběhu nejbližší odstávky turbosoustrojí. Při poruše dvou kanálů ze tří bude turbína odstavena systémem ochran automaticky. V případě nebezpečné poruchy regulátoru dojde k odstavení turbíny systémem ochran.

Rozhraní mezi SIS a operátorem: Veškeré provozní a diagnostické informace jsou zobrazovány na operátorské stanici. Při dosažení hodnoty ochrany nebo výstrahy se spustí zvuková signalizace.

Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS: V případě selhání SIS (PLC systému ochran turbíny) je možné odstavit turbínu tlačítkem nebezpečí pro turbínu, protože tato SIF je hardwarově nezávislá na PLC. V případě selhání SIS (systému ochran turbíny) dojde k uzavření regulačních ventilů regulátorem turbíny. Je nutné uzavřít oddělovací armatury, tj. hlavní uzavírací armaturu a armaturu regulovaného odběru. V případě selhání nebo

netěsnosti rychlozávěrného ventilu a regulačních ventilů turbíny nebo zpětných odběrových klapek dojde k otevření pojistného ventilu (pouze na 10% průtoku páry).

Název SIF: *Signál externí požadavek na odstavení.*

Funkce SIF: Při ztrátě signálu dojde k odstavení turbíny.

Bezpečný stav SIF: Uzavření přívodu páry. Zastavení rotorové soustavy, popřípadě protáčení pomocí otáčecího zařízení turbíny.

Kontrolní interval T_1 SIF: Vzhledem k intervalům generálních oprav turbosoustrojí je nutné každých 5 let provést odstavení turbíny simulací ztráty signálu.

Doba odezvy SIF: Nejsou kladeny speciální podmínky na dobu odezvy SIF. Typická doba odezvy bude menší než 1 sekunda.

Režim vyžádání a stupeň SIL: Jedná se o systém provozu s malým vyžádáním. Stupeň integrity bezpečnosti je SIL 1.

Nové nastavení SIS po vypnutí: Systém ochran má paměť, která vyžaduje potvrzení operátora pro nové nastavení. Systém ochran nastaví regulátor turbíny do výchozího stavu.

Požadavky na manuální vypínání: Nejsou žádné zvláštní požadavky.

Režim poruchy a žádané odezvy v SIS: V případě detekce poruchy na jednom měřícím kanále ze tří nedojde k odstavení turbíny. Operátor obdrží výstrahu přes operátorskou stanici. Porucha musí být odstraněna v průběhu nejbližší odstávky turbosoustrojí. Při poruše dvou kanálů ze tří bude turbína odstavena systémem ochran automaticky.

Rozhraní mezi SIS a operátorem: Veškeré provozní a diagnostické informace jsou zobrazovány na operátorské stanici. Při dosažení hodnoty ochrany se spustí zvuková signalizace.

Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS: V případě selhání SIS (PLC systému ochran turbíny) je možné odstavit turbínu tlačítkem nebezpečí pro turbínu, protože tato SIF je hardwarově nezávislá na PLC.

Je nutné uzavřít oddělovací armatury, tj. hlavní uzavírací armaturu a armaturu regulovaného odběru.

Název SIF: *Tlačítko nebezpečí pro turbínu.*

Funkce SIF: Při stisku tlačítka nouzového zastavení se samočinnou aretací dojde k odstavení turbíny.

Bezpečný stav SIF: Uzavření přívodu páry. Zastavení rotorové soustavy, popřípadě protáčení pomocí otáčecího zařízení turbíny.

Kontrolní interval T_1 SIF: Vzhledem k intervalům generálních oprav turbosoustrojí je nutné každých 5 let provést odstavení turbíny simulací.

Doba odezvy SIF: Nejsou kladeny speciální podmínky na dobu odezvy SIF. Typická doba odezvy bude menší než 1 sekunda.

Režim vyžádání a stupeň SIL: Jedná se o systém provozu s malým vyžádáním. Stupeň integrity bezpečnosti je SIL 1.

Nové nastavení SIS po vypnutí: Systém ochran má paměť, která vyžaduje potvrzení operátora pro nové nastavení. Systém ochran nastaví regulátor turbíny do výchozího stavu.

Požadavky na manuální vypínání: Nejsou žádné zvláštní požadavky.

Režim poruchy a žádané odezvy v SIS: V případě detekce poruchy na jedné smyčce vypínacího obvodu ze tří nedojde k odstavení turbíny. Operátor obdrží výstrahu přes operátorskou stanici. Porucha musí být odstraněna v průběhu nejbližší odstávky turbosoustrojí. Při poruše dvou kanálů ze tří bude turbína odstavena systémem ochran automaticky.

Rozhraní mezi SIS a operátorem: Veškeré provozní a diagnostické informace jsou zobrazovány na operátorské stanici. Při dosažení hodnoty ochrany se spustí zvuková signalizace.

Specifikace požadavků na udržení bezpečného stavu řízeného procesu při výpadku SIS: V případě selhání SIS tlačítko nebezpečí pro turbínu je možné odstavit turbínu přes PLC systému ochran turbíny (přes obrazovku operátora), protože tato cesta je

hardwarově nezávislá. Je nutné uzavřít oddělovací armatury, tj. hlavní uzavírací armaturu a armaturu regulovaného odběru.

4.5 Minimální požadavky hardwaru k poruchám

P. č.	Bezpečnostní funkce SIS	SIL	Hardwarová poruchová tolerance HFT						
			Subsystém senzorů		Subsystém logiky			Subsystém koncových prvků	
			Aplikováno	Min.	Aplikováno	Min.	SFF	Aplikováno	Min.
1	Vysoké otáčky.	3	2	2	-	3	< 60%	1	1 (*
					-	2	60% až 90%		
					2	1	> 90%		
2	Vysoký tlak páry na výstupu.	1	2	0	-	1	< 60%	1	0
					2/0	0	≥60%		
3	Vysoká hladina v kondenzátoru.	1	2	0	-	1	< 60%	1	0
					2/0	0	≥60%		
4	Vysoký tlak páry v regulovaném odběru.	1	2	0	-	1	< 60%	1	0
					2/0	0	≥60%		
5	Signál externí požadavek na odstavení.	1	2	0	-	1	< 60%	1	0
					2	0	≥60%		
6	Tlačítko nebezpečí pro turbínu	1	2	0	-	1	< 60%	1	0
					2	0	≥60%		

(* dle normy lze snížit o 1 stupeň, viz. kapitola 3.6

Tab. 7 Požadavky hardwaru k poruchám

4.6 Výpočet pravděpodobnosti poruch

Aby byl výpočet pravděpodobnosti poruch jednoznačně popsán je nutné jednotlivé komponenty SIF funkčně popsat, např. blokovým uspořádáním. Bylo by vhodné uvést i procesní schéma, ale v této práci nelze uvádět interní firemní dokumentaci. Procesní schéma může být natolik složité, že z něj nemusí být patrna vlastní funkce SIF.

Komponenty mohou být použity i v redundantní konfiguraci s příslušným výběrem z hlediska funkčnosti. Pak je nezbytné popsat architekturu SIF, která je odlišná od analýzy

stromu poruch. Na tomto diagramu se opět objeví veškeré komponenty, které jsou součástí SIF.

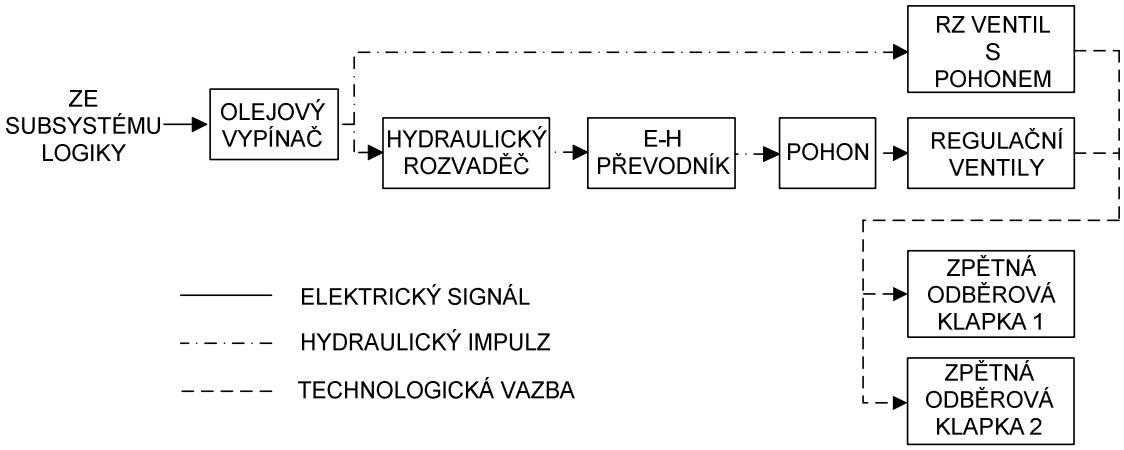
Komponenty SIF musí být jednoznačně určeny, což je provedeno tabulkou. Každá komponenta má příslušnou hodnotu pravděpodobnosti poruchy. Zdrojem pro tyto informace je příslušný certifikát nebo typická hodnota z katalogu. Aby byl dohledatelný zdroj informací je v tabulce uveden krátký popis dokumentu. Protože informace od dodavatelů komponent jsou udávány v různých parametrech, provádí se přepočet na hodnotu PFD, popřípadě CCF a to tabulkovým procesorem. Hodnoty PFD a CCF jsou bezrozměrné, ale je nutné zadat do výpočtu vstupní hodnoty v hodinách. Pro výpočet PFD jsou použity vzorce (16) – (22), (24), (26), (27), (29) v závislosti na typu vstupního parametru. Výpočet CCF je realizován za pomocí vzorců (30) – (33). Bodovým ohodnocením parametrů X, Y, Z (viz. kapitola 3.9) a převodní tabulkou byly určeny hodnoty $\beta = 5\,\%$ a $\beta_D = 2\,\%$, které jednotně vstupují do výpočtu CCF veškerých redundantních komponentů. Kontrolní interval $T_1 = 1\,\text{rok}$ je uvažován pro SIF vysoké otáčky v souladu s doporučením VGB-R 103. Pro ostatní SIF je hodnota $T_1 = 5\,\text{roků}$, což odpovídá intervalu pravidelných generálních oprav turbosoustrojí.

Vlastní analýza poruchových stromů je provedena diagramem, kde vrcholovou událostí je porucha příslušného SIF. Při sestavování stromu se zohledňuje architektura SIF z hlediska poruchy. Na nejnižších úrovních jsou uvedeny základní události, nebo-li pravděpodobnosti poruch na vyžádání PFD příslušných komponentů. Strom poruch se sestavuje seshora dolů, ale výpočet je prováděn opačným směrem. Grafické provedení je dáno softwarovým programem FTA od fy Item software [20]. Výpočet provádí výše zmíněný software na základě vzorců uvedených v kapitole 2.4. Výsledkem analýzy je hodnota uvedená ve vrcholové události.

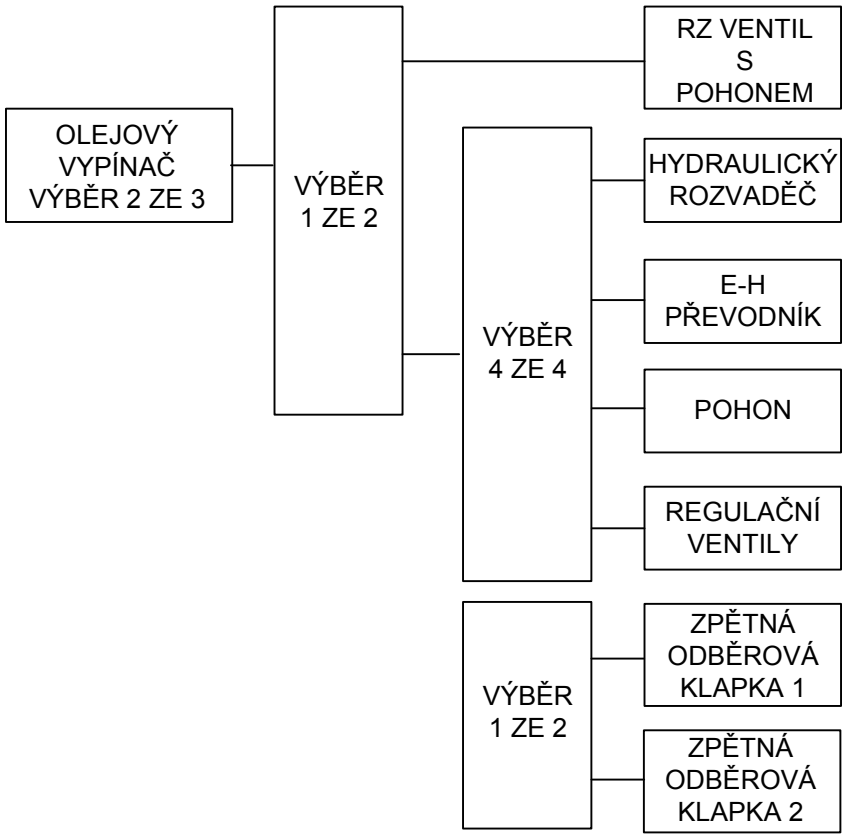
Příslušná SIF splní předpokládaný stupeň integrity bezpečnosti pokud plní požadavky na hodnoty PFD, HFT a SFF současně. Vyhodnocení těchto hodnot je přehledně uvedeno v tabulce za každým konečným výpočtem FTA.

Protože, skladba komponentů jednotlivých SIF je rozsáhlá, byl výpočet rozdělen dle subsystémů a to tak, aby se zamezilo opakování již jednou vypočtených hodnot. Subsystém koncových prvků se objevuje ve výpočtech FTA všech SIF. Subsystém Fail Safe PLC se vyskytuje pouze tam, kde je v obvodu skutečně zapojen.

4.6.1 Subsystém koncových prvků



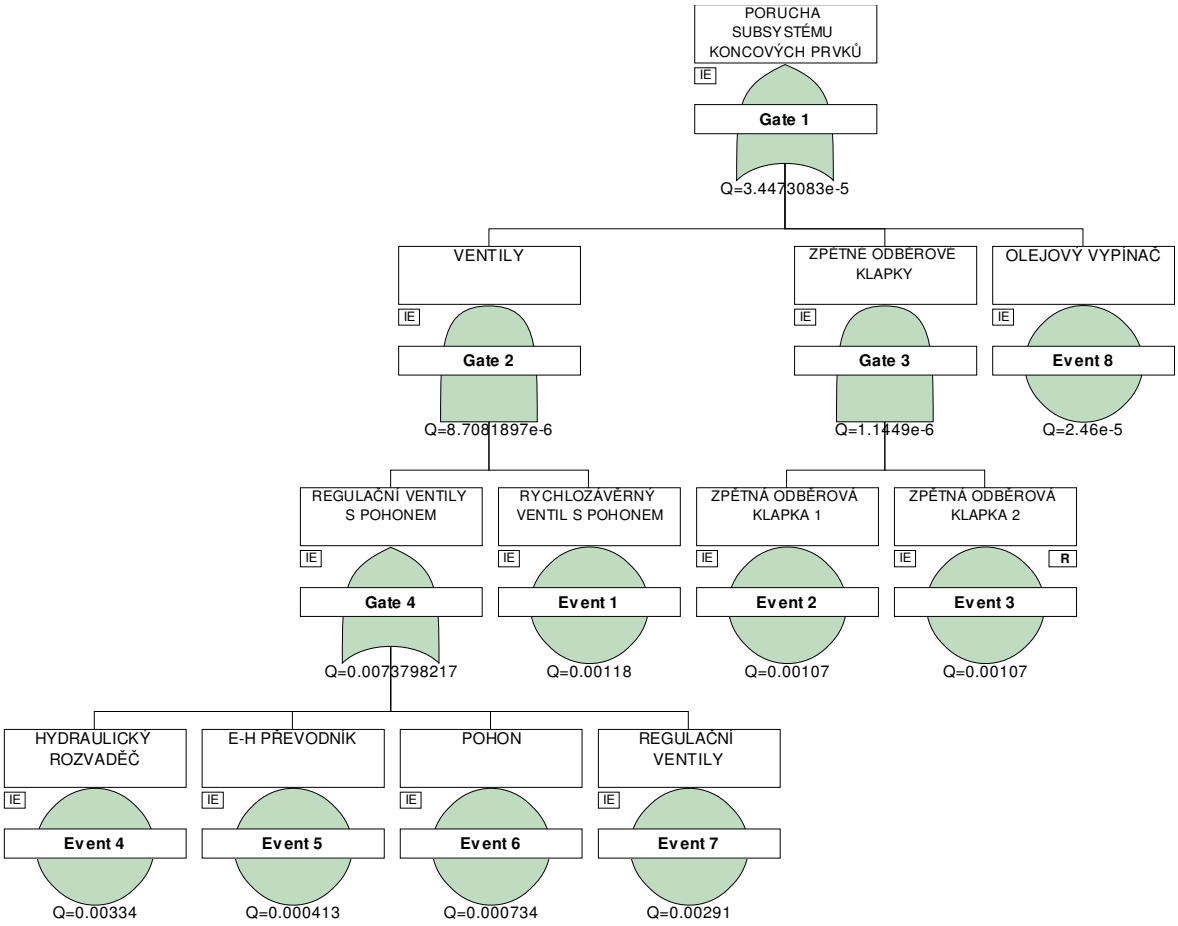
Obr. 9 Blokové uspořádání SIF



Obr. 10 Architektura SIF

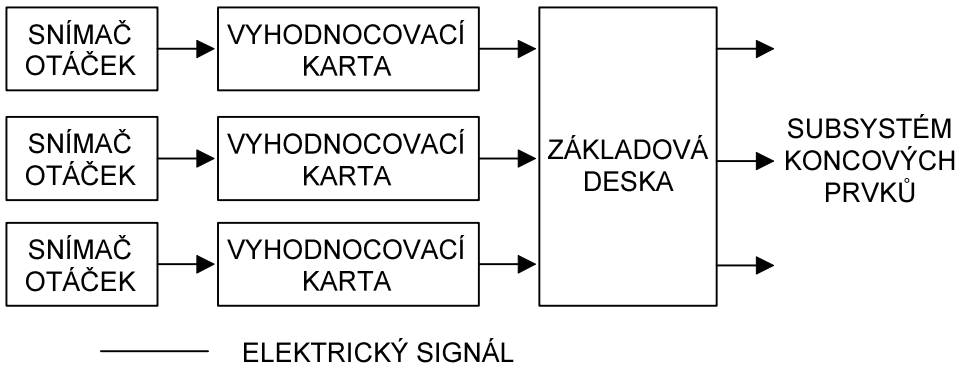
Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Olejový vypínač	Siemens TB SST300	Ingenieurburo Urban, protokol z 30.9.2009	$T_1 = 1\,\text{rok}$ $PFD = 2{,}46 \cdot 10^{-5}$	$PFD = 2{,}46 \cdot 10^{-5}$
RZ ventil s pohonem	Siemens ESV DN300 PN160	Ingenieurburo Urban, protokol z 20.3.2010	$T_1 = 1\,\text{rok}$ $PFD = 1{,}18 \cdot 10^{-3}$	$PFD = 1{,}18 \cdot 10^{-3}$
Hydraulický rozvaděč	Rexroth LC16B00E7	Bosh Rexroth AG, dokument RD08012/03.10	$T_1 = 1\,\text{rok}$ $MTTF_d = 150\,\text{roků}$ $SR = 0\,\%$	$PFD = 3{,}34 \cdot 10^{-3}$
E-H převodník	Voith E360	Voith Turbo, prezentace ze 14.6.2009	$T_1 = 1\,\text{rok}$ $\lambda = 94{,}2\,\text{FIT}$ $SR = 0\,\%$	$PFD = 4{,}13 \cdot 10^{-4}$
Hydraulický pohon	Siemens RD200KSCH FK H.70	Ingenieurburo Urban, protokol z 20.3.2010	$T_1 = 1\,\text{rok}$ $PFD = 7{,}34 \cdot 10^{-4}$	$PFD = 7{,}34 \cdot 10^{-4}$
Regulační ventily	Siemens AUM DN250 PN160	Ingenieurburo Urban, protokol z 20.3.2010	$T_1 = 1\,\text{rok}$ $PFD = 2{,}91 \cdot 10^{-3}$	$PFD = 2{,}91 \cdot 10^{-3}$
Zpětná odběrová klapka	Typický představitel	VGB, dokument ZEDB z 12/2007	$T_1 = 1\,\text{rok}$ $\lambda_D = 2{,}43 \cdot 10^{-7}\,\text{h}$	$PFD = 1{,}07 \cdot 10^{-3}$

Tab. 8 Tabulka hodnot

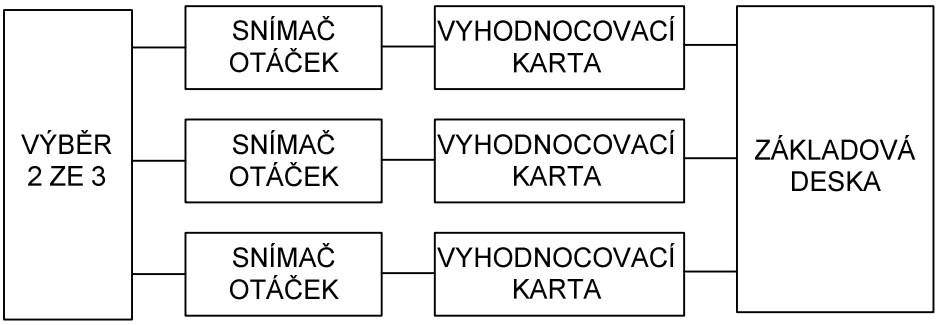


Obr. 11 Strom poruchových stavů

4.6.2 Vysoké otáčky



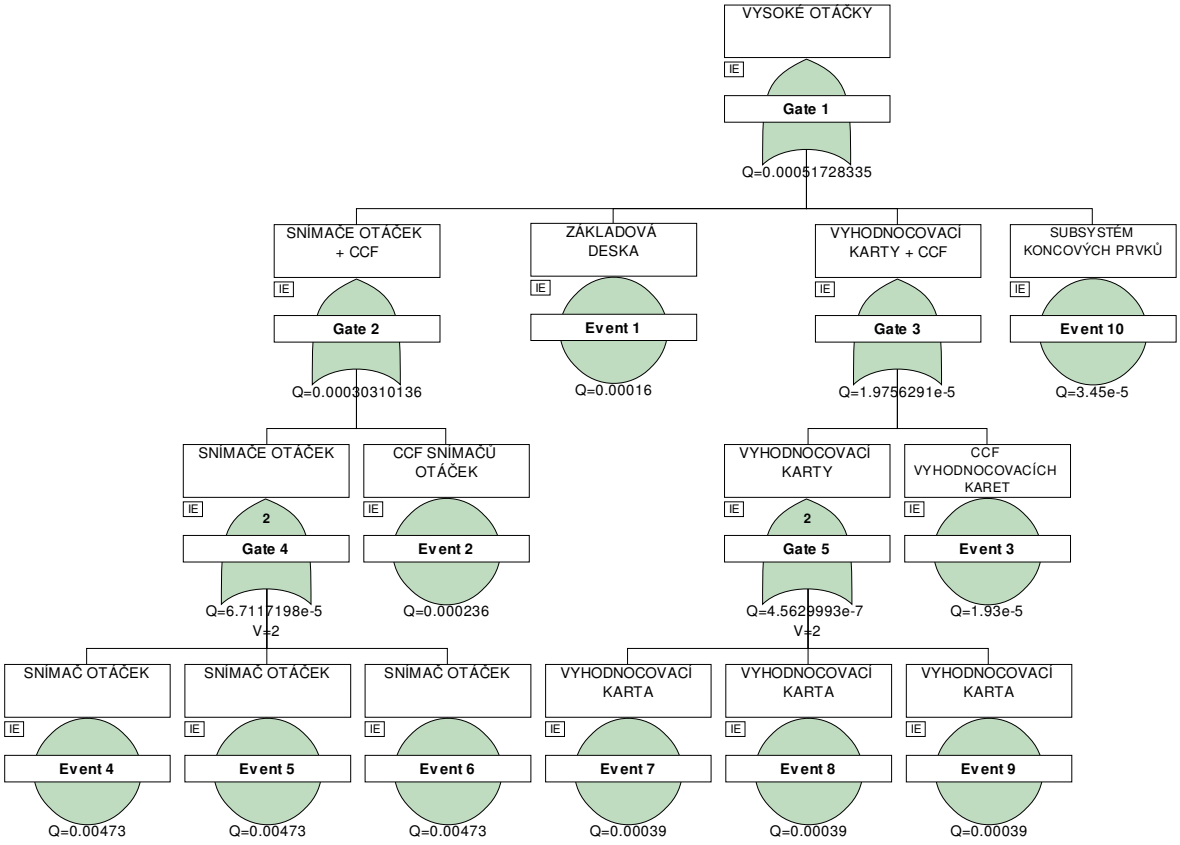
Obr. 12 Blokové uspořádání SIF



Obr. 13 Architektura SIF

Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Snímač otáček	Epro MMG1070	TUV Rheinland, protokol z 25.3.2004	$T_1 = 1\,\text{rok}$ $MTBF = 10{,}6\,\text{roků}$ $SR = 90\%$ $DC = 0\,\%$ $\beta = 5\,\%$	$PFD = 4{,}73 \cdot 10^{-3}$ $CCF = 2{,}36 \cdot 10^{-4}$
Vyhodnocovací karta	Epro MMS6350	TUV Rheinland, protokol z 25.3.2004	$T_1 = 1\,\text{rok}$ $MTBF = 13{,}06\,\text{roků}$ $SR = 90\%$ $DC = 90\,\%$ $\beta = 5\,\%$ $\beta_D = 2\,\%$	$PFD = 3{,}9 \cdot 10^{-4}$ $CCF = 1{,}93 \cdot 10^{-5}$
Základová deska	Epro MMS6351/10	TUV Rheinland, protokol z 25.3.2004	$T_1 = 1\,\text{rok}$ $MTBF = 31{,}24\,\text{roků}$ $SR = 99\,\%$ $DC = 0\,\%$	$PFD = 1{,}6 \cdot 10^{-4}$
Subsystém koncových prvků	-	Viz. kapitola 4.5.1	-	$PFD = 3{,}45 \cdot 10^{-5}$

Tab. 9 Tabulka hodnot



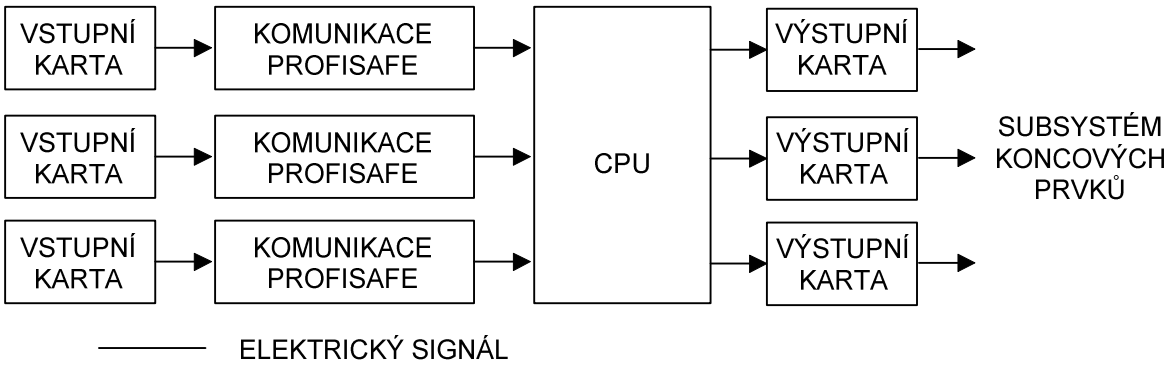
Obr. 14 Strom poruchových stavů

	Požadavek normy	Výsledek výpočtu	Závěr
PFD	$<10^{-3}$	$5{,}17 \cdot 10^{-4}$	Splněno
HFT	≥ 1 (*	1	Splněno
SFF subsystému logiky	> 90%	99%	Splněno
Závěr	Splněn požadavek na SIL3 za podmínky $T_1 = 1\,\text{rok}$		

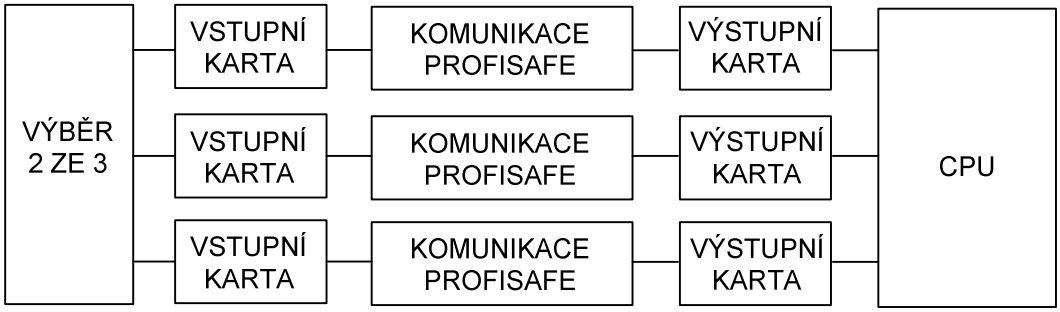
(* dle normy lze snížit o 1 stupeň, viz. kapitola 3.6

Tab. 10 Tabulka výsledku

4.6.3 Subsystém logiky– Fail Safe PLC



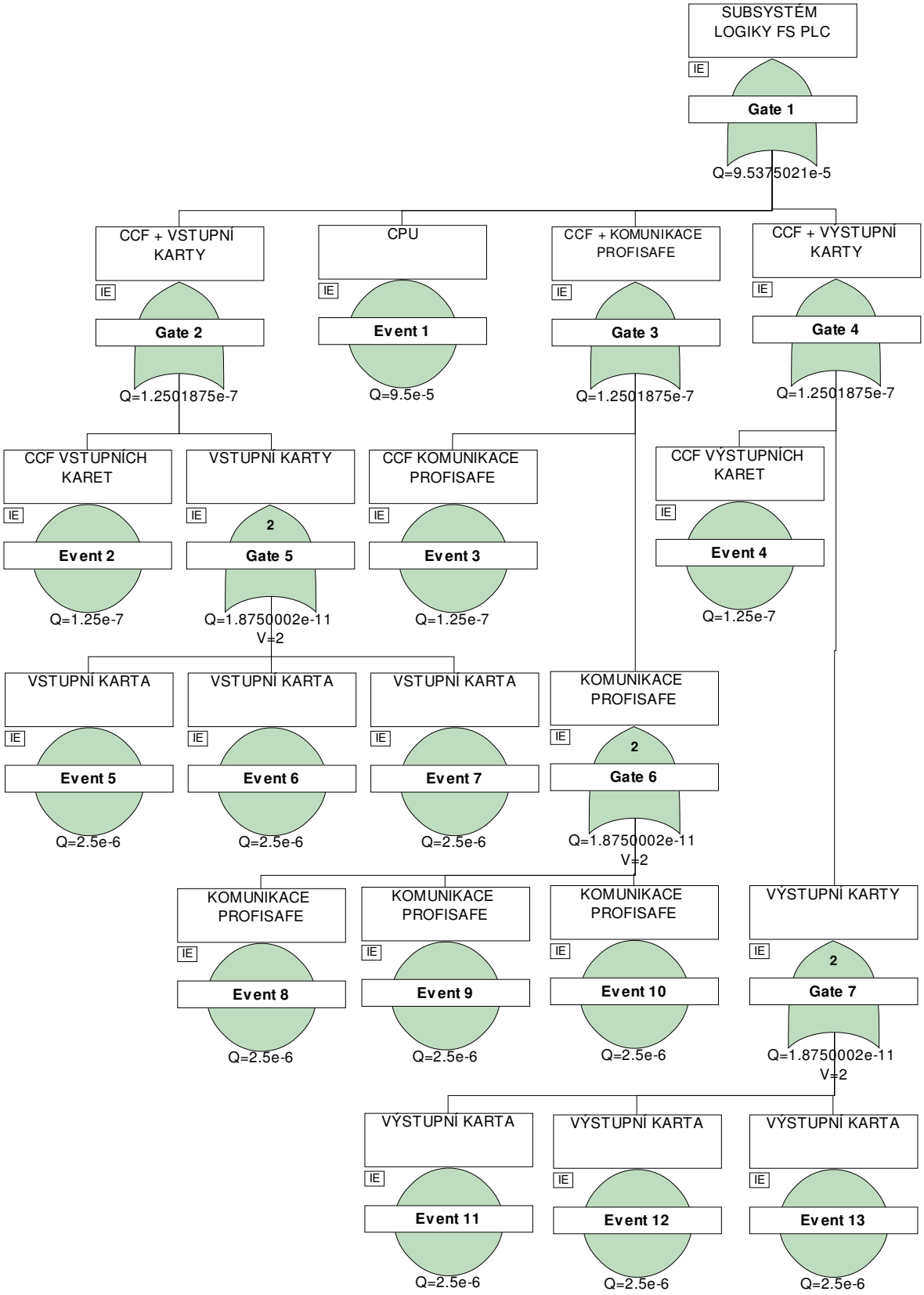
Obr. 15 Blokové uspořádání SIF



Obr. 16 Architektura SIF

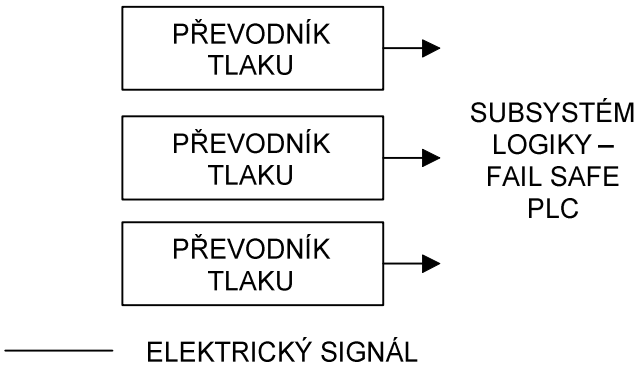
Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Vstupní karta	Siemens SM336	Siemens, dokument Safety engineering z 9.2.2009	$T_1 = 5$ roků $PFD = 2{,}5 \cdot 10^{-6}$ $\beta = 5\,\%$	$PFD = 2{,}5 \cdot 10^{-6}$ $CCF = 1{,}25 \cdot 10^{-7}$
Komunikace PROFIsafe	Siemens	Siemens, dokument Safety engineering z 9.2.2009	$T_1 = 5$ roků $PFD = 2{,}5 \cdot 10^{-6}$ $\beta = 5\,\%$	$PFD = 2{,}5 \cdot 10^{-6}$ $CCF = 1{,}25 \cdot 10^{-7}$
CPU	Siemens CPU 417-4H	Siemens, dokument Safety engineering z 9.2.2009	$T_1 = 5$ roků $PFD = 9{,}5 \cdot 10^{-5}$	$PFD = 9{,}5 \cdot 10^{-5}$
Výstupní karta	Siemens SM326	Siemens, dokument Safety engineering z 9.2.2009	$T_1 = 5$ roků $PFD = 2{,}5 \cdot 10^{-6}$ $\beta = 5\,\%$	$PFD = 2{,}5 \cdot 10^{-6}$ $CCF = 1{,}25 \cdot 10^{-7}$

Tab. 11 Tabulka hodnot

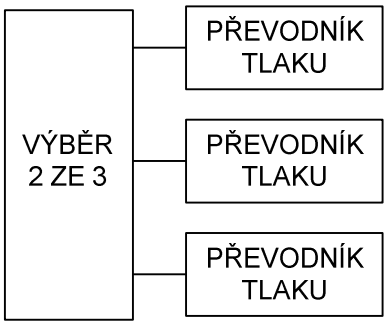


Obr. 17 Strom poruchových stavů

4.6.4 Vysoký tlak páry na výstupu, vysoký tlak páry v regulovaném odběru



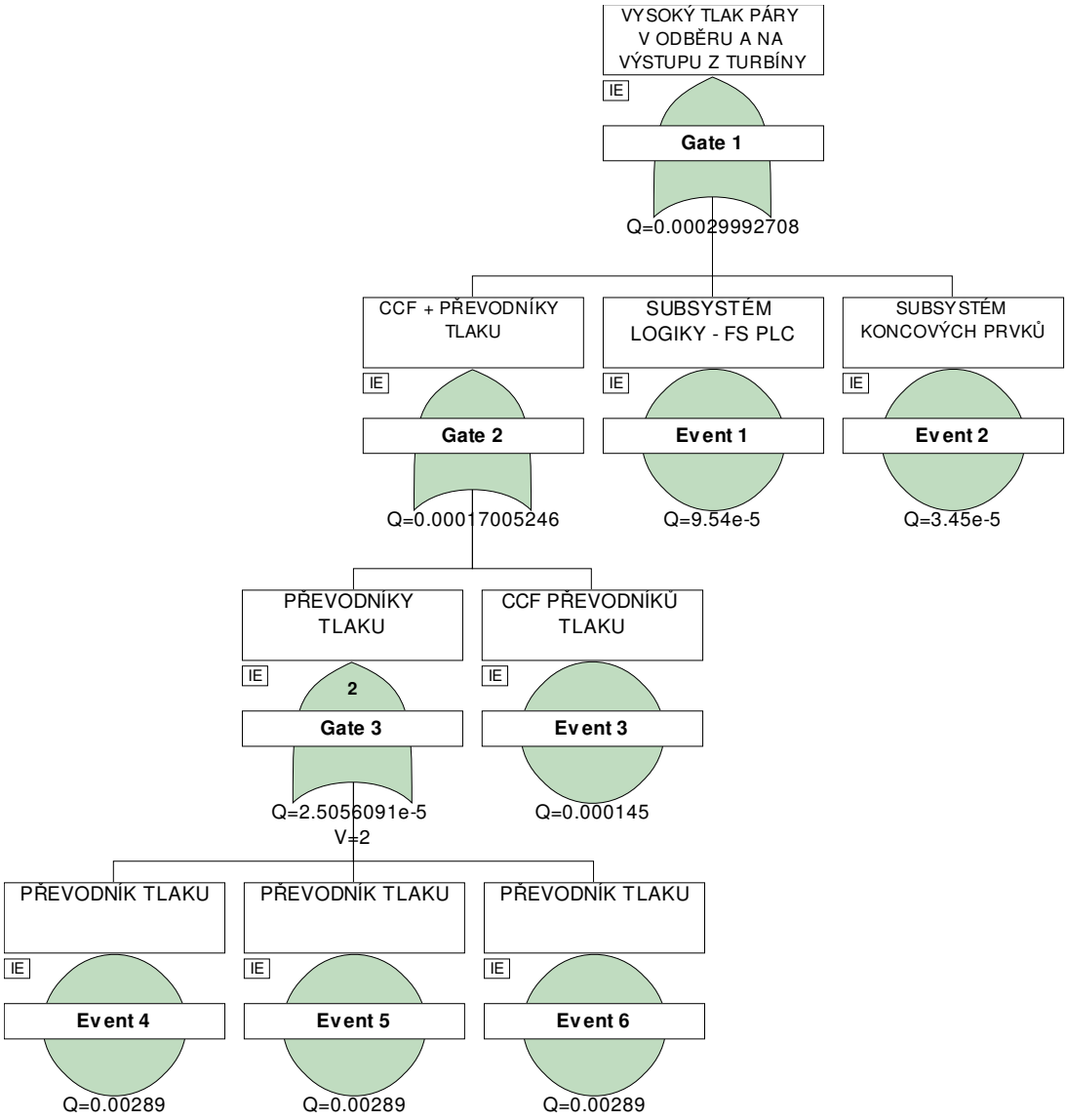
Obr. 18 Blokové uspořádání SIF



Obr. 19 Architektura SIF

Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Převodník tlaku	Siemens SITRANS DSIII	Siemens, protokol z 29.9.2006	$T_1 = 5$ roků $\lambda_{SD} = 0$ FIT $\lambda_{SU} = 151$ FIT $\lambda_{DD} = 381$ FIT $\lambda_{DU} = 132$ FIT $\beta = 5\,\%$ $\beta_D = 2\,\%$	$PFD = 2{,}89 \cdot 10^{-3}$ $CCF = 1{,}45 \cdot 10^{-4}$
Subsystém logiky – Fail Safe PLC	-	Viz. kapitola 4.5.3	-	$PFD = 9{,}54 \cdot 10^{-5}$
Subsystém koncových prvků	-	Viz. kapitola 4.5.1	-	$PFD = 3{,}45 \cdot 10^{-5}$

Tab. 12 Tabulka hodnot

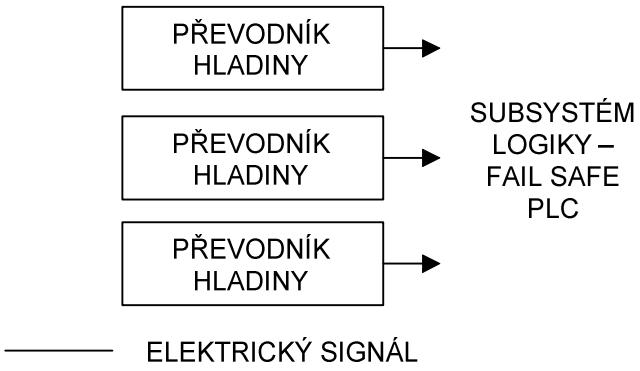


Obr. 20 Strom poruchových stavů

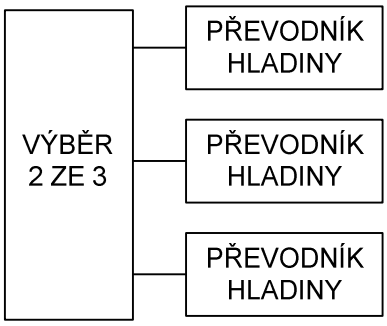
	Požadavek normy	Výsledek výpočtu	Závěr
PFD	$<10^{-1}$	$PFD = 3{,}00 \cdot 10^{-4}$	Splněno
HFT	≥ 0	1	Splněno
SFF subsystému logiky	>0%	>90%	Splněno
Závěr	Splněn požadavek na SIL1 za podmínky $T_1 = 5$ roků		

Tab. 13 Tabulka výsledku

4.6.5 Vysoká hladina v kondenzátoru



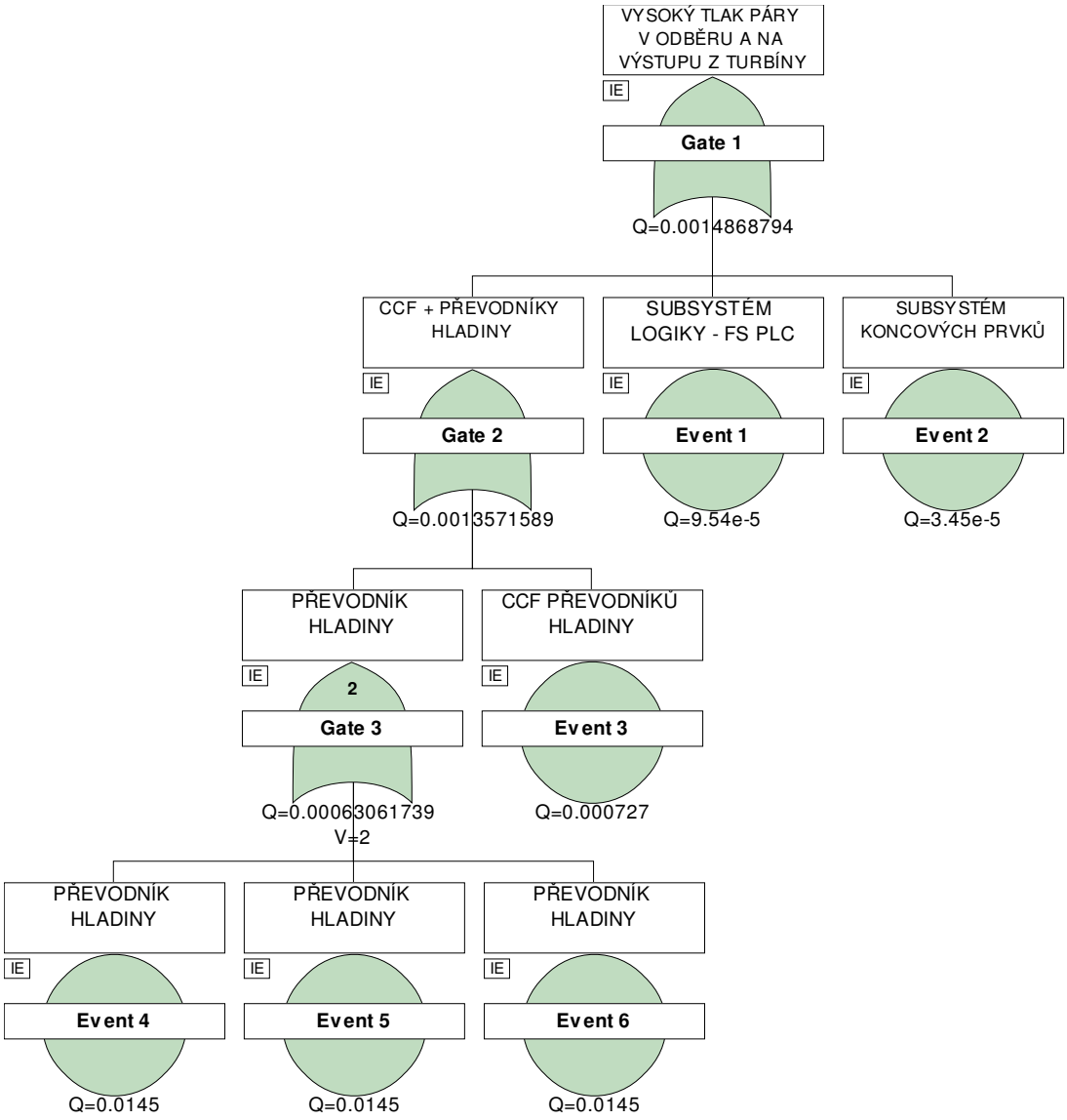
Obr. 21 Blokové uspořádání SIF



Obr. 22 Architektura SIF

Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Převodník hladiny	KSR Kuebler AUVK	KSR Kuebler, dokument z 2003	$T_1 = 5$ roků $MTBF = 172$ roků $SR = 0\,\%$ $\beta = 5\,\%$	$PFD = 1{,}45 \cdot 10^{-2}$ $CCF = 7{,}27 \cdot 10^{-4}$
Subsystém logiky – Fail Safe PLC	-	Viz. kapitola 4.5.3	-	$PFD = 9{,}54 \cdot 10^{-5}$
Subsystém koncových prvků	-	Viz. kapitola 4.5.1	-	$PFD = 3{,}45 \cdot 10^{-5}$

Tab. 14 Tabulka hodnot

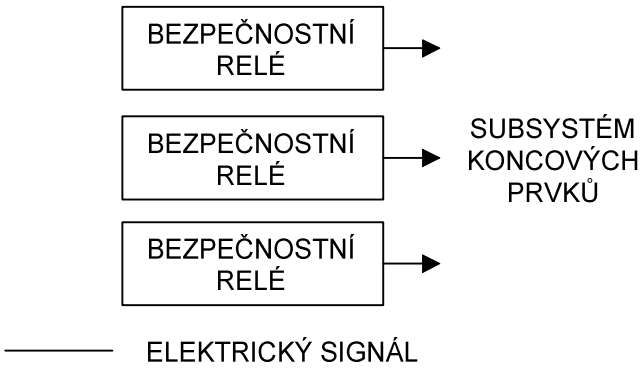


Obr. 23 Strom poruchových stavů

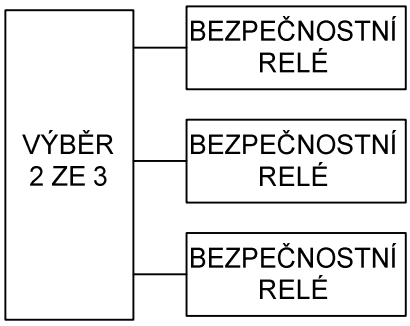
	Požadavek normy	Výsledek výpočtu	Závěr
PFD	$<10^{-1}$	$PFD = 1{,}49 \cdot 10^{-3}$	Splněno
HFT	≥ 0	1	Splněno
SFF subsystému logiky	>0%	>90%	Splněno
Závěr	Splněn požadavek na SIL1 za podmínky $T_1 = 5$ roků		

Tab. 15 Tabulka výsledku

4.6.6 Signál externí požadavek na odstavení



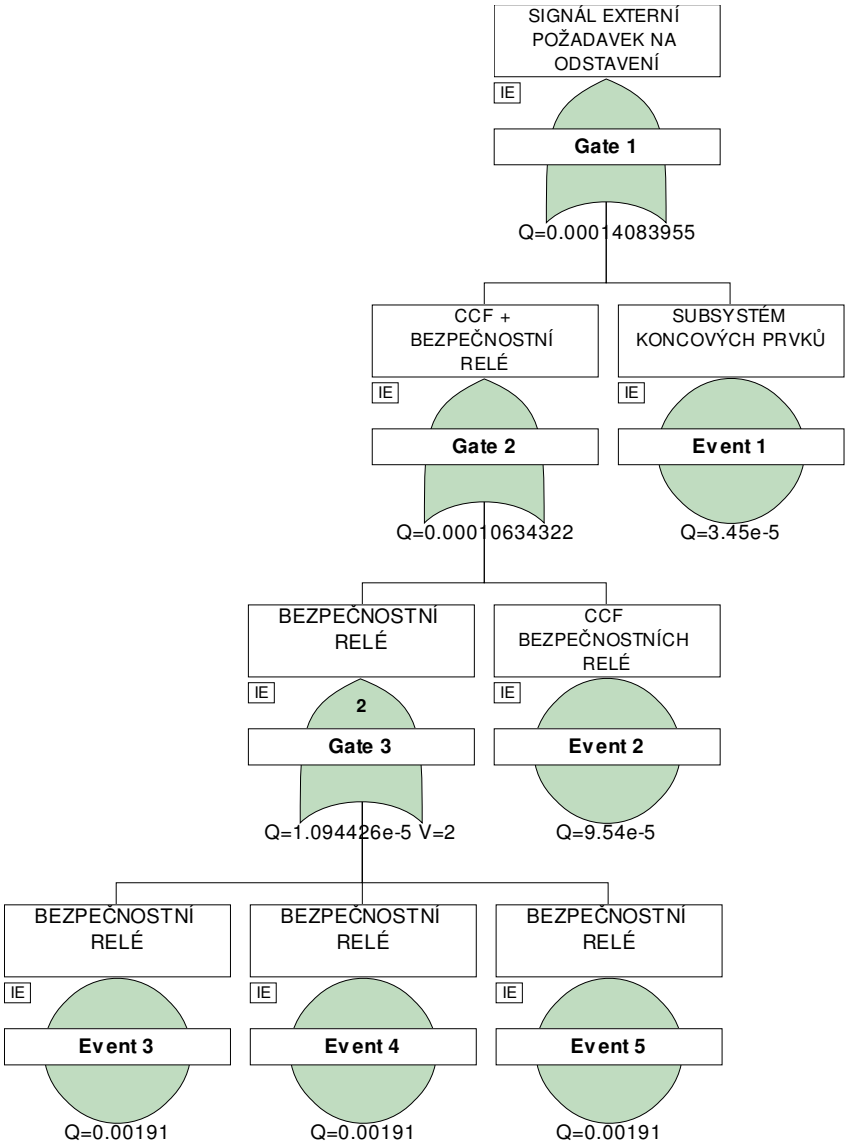
Obr. 24 Blokové uspořádání SIF



Obr. 25 Architektura SIF

Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Bezpečnostní relé	Phoenix Contact PSR-SCP	TUV Rheinland, protokol z 26.6.2008	$T_1 = 5$ roků $B_{10d} = 2{,}3 \cdot 10^5$ h $C = 2$ sepnutí/h $DC = 90\,\%$ $\beta = 5\,\%$ $\beta_D = 2\,\%$	$PFD = 1{,}91 \cdot 10^{-3}$ $CCF = 9{,}54 \cdot 10^{-5}$
Subsystém koncových prvků	-	Viz. kapitola 4.5.1	-	$PFD = 3{,}45 \cdot 10^{-5}$

Tab. 16 Tabulka hodnot

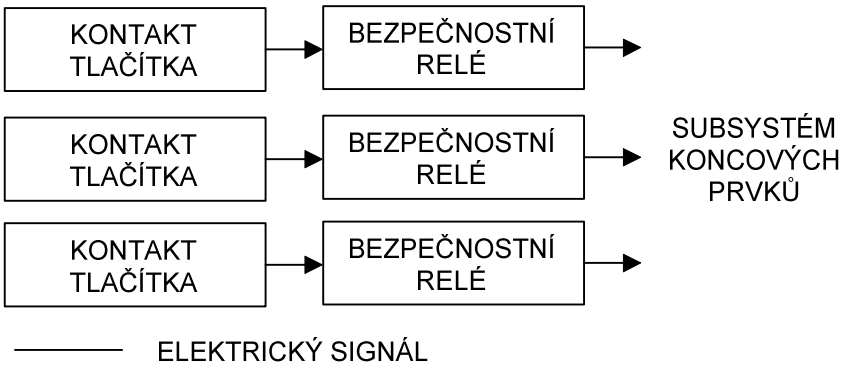


Obr. 26 Strom poruchových stavů

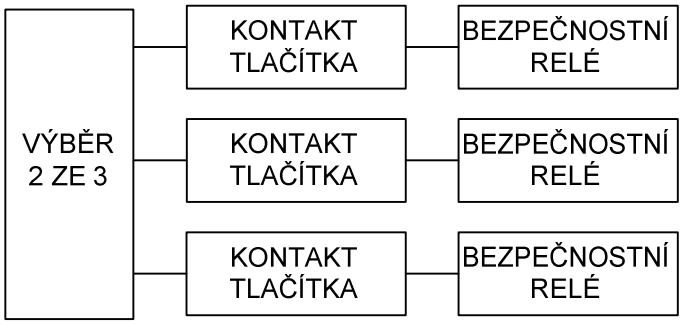
	Požadavek normy	Výsledek výpočtu	Závěr
PFD	$<10^{-1}$	$PFD = 1{,}41 \cdot 10^{-4}$	Splněno
HFT	≥ 0	1	Splněno
SFF subsystému logiky	>0%	>90%	Splněno
Závěr	Splněn požadavek na SIL1 za podmínky $T_1 = 5$ roků		

Tab. 17 Tabulka výsledku

4.6.7 Tlačítko nebezpečí pro turbínu



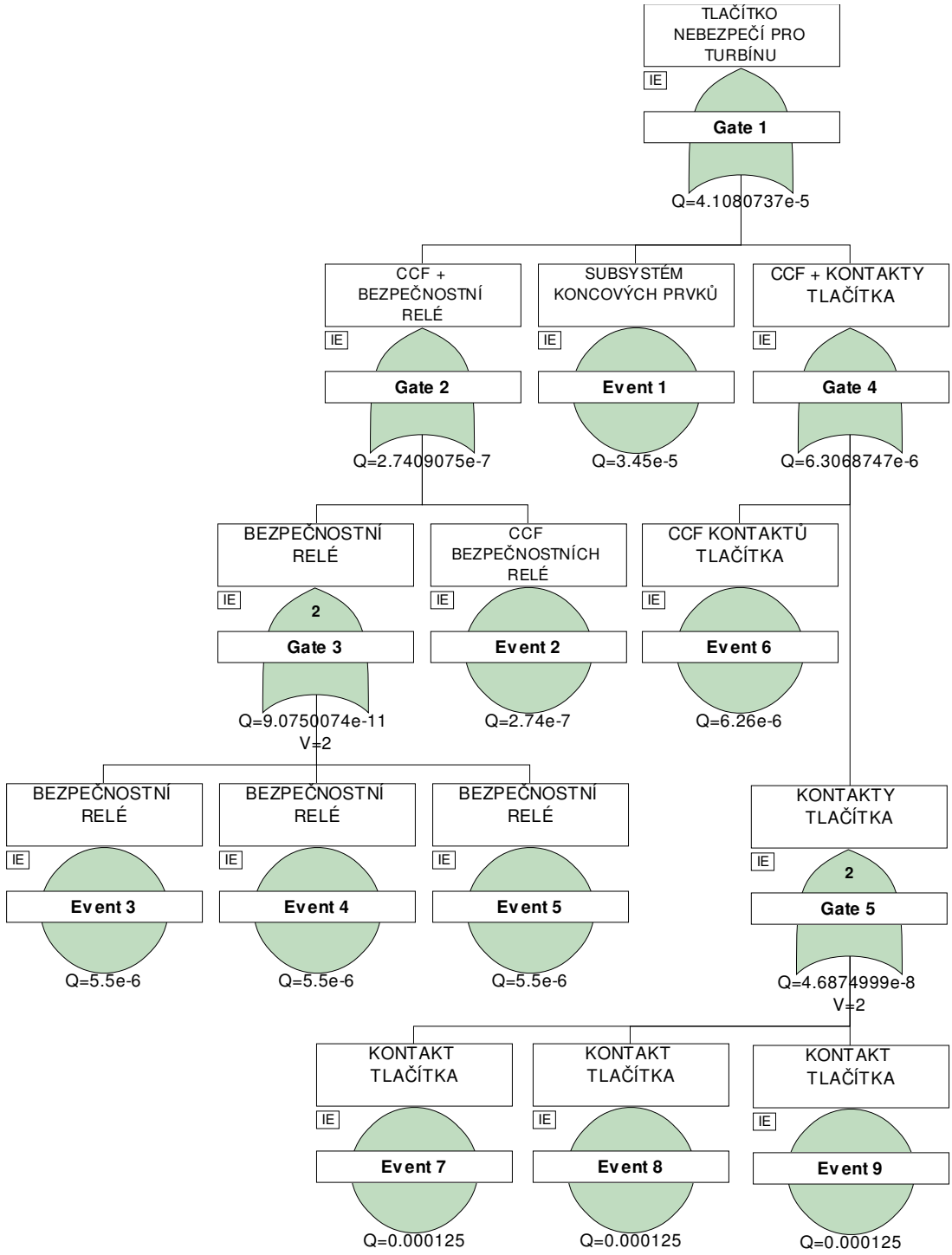
Obr. 27 Blokové uspořádání SIF



Obr. 28 Architektura SIF

Komponenta	**Výrobce a specifikace**	**Zdroj informací**	**Zadaná data**	**Data vstupující do FTA**
Kontakt tlačítka	Typický představitel	TUV Nord, dokument z 2008	$T_1 = 5$ roků $B_{10d} = 1 \cdot 10^5$ h $C = 50$ sepnutí/rok $\beta = 5\,\%$	$PFD = 1{,}25 \cdot 10^{-4}$ $CCF = 6{,}26 \cdot 10^{-6}$
Bezpečnostní relé	Phoenix Contact PSR-SCP	TUV Rheinland, protokol z 26.6.2008	$T_1 = 5$ roků $B_{10d} = 2{,}3 \cdot 10^5$ h $C = 50$ sepnutí/rok $DC = 90\,\%$ $\beta = 5\,\%$ $\beta_D = 2\,\%$	$PFD = 5{,}5 \cdot 10^{-6}$ $CCF = 2{,}74 \cdot 10^{-7}$
Subsystém koncových prvků	-	Viz. kapitola 4.5.1	-	$PFD = 3{,}45 \cdot 10^{-5}$

Tab. 18 Tabulka hodnot



Obr. 29 Strom poruchových stavů

	Požadavek normy	Výsledek výpočtu	Závěr
PFD	$<10^{-1}$	$PFD = 4{,}11 \cdot 10^{-5}$	Splněno
HFT	≥ 0	1	Splněno
SFF subsystému logiky	>0%	>90%	Splněno
Závěr	Splněn požadavek na SIL1 za podmínky $T_1 = 5$ roků		

Tab. 19 Tabulka výsledku

ZÁVĚR

Analýzou a výpočtem bylo zjištěno, že navržené provedení ochran (bezpečnostních funkcí) parních turbín splňuje požadavky na funkční bezpečnost dle norem ČSN EN 61508 a ČSN EN 61511 a to pro navrhovaný případ. Pro jiné případy, kde je např. více regulovaných odběrů páry, neregulované odběry páry, jiná další rizika z navazující technologie, jsou použity jiné komponenty než uvažované ve výpočtu, je nutné výpočet provést pro konkrétní případ.

V praxi se vyskytují dva způsoby realizace SIS pro subsystém logiky. Při použití SIL certifikovaných relé zapojených paralelně ke standardnímu PLC, může dojít ke zhoršení provozuschopnosti a identifikaci poruchy zařízení. Jako technicky výhodnější, ale cenově dražší řešení, je možno použít řešení, kde jsou současně v jednom systému integrovány „běžné“ a „safety related“ úlohy. Toto řešení je použito v praktické části této práce.

U komunikačního protokolu PROFIBUS DP je možno použít modulu PROFIsafe pro bezpečnostně orientovanou komunikaci. To umožňuje přenos „safety related“ informací spolu s „běžnou“ výměnou dat, kde není nutná samostatná komunikační linka. Podobně lze kombinovat i v/v karty, které jsou zařazeny v obvodech SIS a které nejsou „safety related“ ve společném rámu PLC nebo distribuovaných v/v jednotek. Pak se pro tyto systémy užívá výraz „distribuovaná bezpečnost“. Samozřejmě i CPU systému PLC musí být certifikován pro použití v SIS. Programovací software STEP 7 umožňuje rozšíření o nástroj na programování „safety related“ funkcí.

Při realizaci SIS je potřeba přihlédnout i k teplotě okolí, protože hodnoty MTBF jsou udávány výrobci v rozmezí 25°C až 40°C, ale maximální teplota zařízení udávaná výrobcem může být až 65°C. Zařízení obsahující mikroprocesor může mít až dvojnásobně vyšší pravděpodobnost vzniku poruchy při zvýšení teploty o 10 K oproti předpokládané teplotě.

Oblast funkční bezpečnosti se stále vyvíjí. Lze očekávat, že komponentů certifikovaných pro SIS bude stále více a to nejen elektronických. Výrobci poskytující tyto výrobky mají konkurenční výhodu před ostatními.

ZÁVĚR V ANGLIČTINĚ

It was proven by analysis and calculation, that the proposed design of steam turbines protections (safety functions) meets the requirements on functional safety according to standards CSN EN 61508 and CSN EN 61511 namely for the suggested case. For other cases, in which, for example, there's a lot of steam extractions, bleeds, other additional hazards resulting from related technology, other components than those taken in consideration in the calculation have been used, calculation for the specific case shall be performed.

Practically there are two ways of implementation of SIS for subsystem logic. On using SIL certified relays connected in parallel to standard PLC, downgrading of the availability and identification of equipment failure can occur. The solution, where „regular" and „safety-related" tasks are simultaneously integrated in one system can be used as technically preferable, but more expensive. This solution has been used in practical part of this thesis.

Module PROFIsafe for safety-oriented communication can be used in the case of the communications protocol PROFIBUS DP. It enables transmission of the „safety-related" information together with the „regular" data exchange, where a separate communication line isn't necessary. Similarly it is possible to combine also I/O cards, connected in SIS loops and not „safety-related" in a common rack of PLC, or distributed I/O modules. Then the term „distributed safety" is used for these systems. Of course also CPU of PLC system has to be certified for the use in SIS. Programming software STEP 7 allows extension with the tool for programming of „safety-related" functions.

On implementation of SIS also ambient temperature shall be taken in consideration because the values of MTBF are indicated by manufacturers from 25°C to 40°C but the maximum temperature of the equipment indicated by its manufacturer can be as high as 65°C. The equipment containing a microprocessor can have nearly a double probability of failure at the temperature rise by 10 K compared with the supposed temperature.

The development of the section of functional safety is still going on. It can be expected that the quantity of the components certified for SIS will be increasing and that these won't be only electronic ones. Manufacturers providing these products have competitive advantage over the others.

SEZNAM POUŽITÉ LITERATURY

[1] Česko. Nařízení vlády č. 176/2008 Sb. : o technických požadavcích na strojní zařízení. In *č. 176/2008 Sbírky zákonů*. 2008, 56, s. 62. Dostupný také z WWW: <http://docs.google.com/viewer?url=http://www.tzb-info.cz/docu/predpisy/download/NV176-2008.pdf>.

[2] VDOLEČEK, František; *Spolehlivost a technická diagnostika: Text pro podporu výuky v kombinovaném studiu.* Brno, 2002. 49 s

[3] Safety In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 12:59, 8 November 2007 , 13:35, 15 February 2010 [cit. 2010-03-27]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Safety>.

[4] UHER, Jaromír. Úvod do funkční bezpečnosti I: norma ČSN EN 61508 . *Automa* [online]. 2004, 2004, 08, [cit. 2010-03-27]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=32520>.

[5] ČSN EN 61025. *Analýza stromu poruchových stavů (FTA)*. Praha : ČNI, 2007. 48 s.

[6] SMITH, David J; SIMPSON, Kenneth G L. *Functional Safety : A straightforward Guide to applying IEC 61508 and Related Standards*. 2nd edition. Oxford (GB) : Elsevier, 2004. 263 s. ISBN 0-7506-6269-7.

[7] ČSN EN ISO 13849-1. *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů. : Část 1: Všeobecné zásady pro konstrukci.* Praha : ČNI, 2008. 84 s.

[8] ČSN EN 61508-4. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. : Část 4: Definice a zkratky.* Praha : ČNI, 2002. 32 s.

[9] ČSN EN 61508-1. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností : Část 1:Všeobecné požadavky*. Praha : ČNI, 2002. 60 s.

[10] ČSN EN 61508-2. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. : Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností.* Praha : ČNI, 2002. 76 s.

[11] ČSN EN 61508-6. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. : Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3.* Praha : ČNI, 2002. 72 s.

[12] ČSN EN 61511-1. *Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů. : Část 1: Požadavky na systémy hardwaru a softwaru, struktura, definice.* Praha : ČNI, 2004. 88 s.

[13] ČSN EN 61511-2. *Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů. : Část 2: Pokyny pro použití normy IEC 61511-1.* Praha : ČNI, 2004. 48 s.

[14] ČSN EN 61511-3. *Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů. : Část 3: Pokyn pro stanovení požadované úrovně integrity bezpečnosti.* Praha : ČNI, 2004. 48 s.

[15] ČSN EN 61508-5. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. : Část 5: Příklady metod určování úrovní integrity bezpečnosti.* Praha : ČNI, 2002. 32 s.

[16] KNICK GmbH. Funkční bezpečnost podle IEC / EN 61508: : Normy – fakta – pozadí. *Profess - info* [online]. 2006, 1, [cit. 2010-03-27]. Dostupný z WWW: <http://www.profess.sk/pdf_pci_info/INFO-SIL.pdf>.

[17] SOUKENÍK, Martin. *Analýza spolehlivosti parních turbín s příslušenstvím*. Brno, 2008. 43 s. Bakalářská práce. Vysoké učení technické, Fakulta strojního inženýrství, Ústav automatizace a informatiky. Dostupné z WWW: <http://autnt.fme.vutbr.cz/szz/2008/BP_Soukenik.pdf>.

[18] ČSN EN 61508-3. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. : Část 3: Požadavky na software.* Praha *:* ČNI, 2002. 52 s.

[19] SUMMERS, Angela E. Software - implemented safety logic. *Process Safety Progress* [online]. June 2002., 1, [cit. 2010-03-27]. Dostupný z WWW: <http://www.sis-tech.com/downloads/Software%20Implemented%20Safety%20Logic.pdf>.

[20] *Item ToolKit Fault Tree* [program na CD-ROM]. Ver. 7.08.7.2. Whiteley (Hampshire, UK): Item software, 2010. Full version pro komerční použití, vlastník licence Siemens Industrial Turbomachinery s.r.o., Brno

[21] Siemens. Turloop S7 Standard: Overview digram I&C. Siemens Industrial Turbomachinery s.r.o., Brno, 2010, 1s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

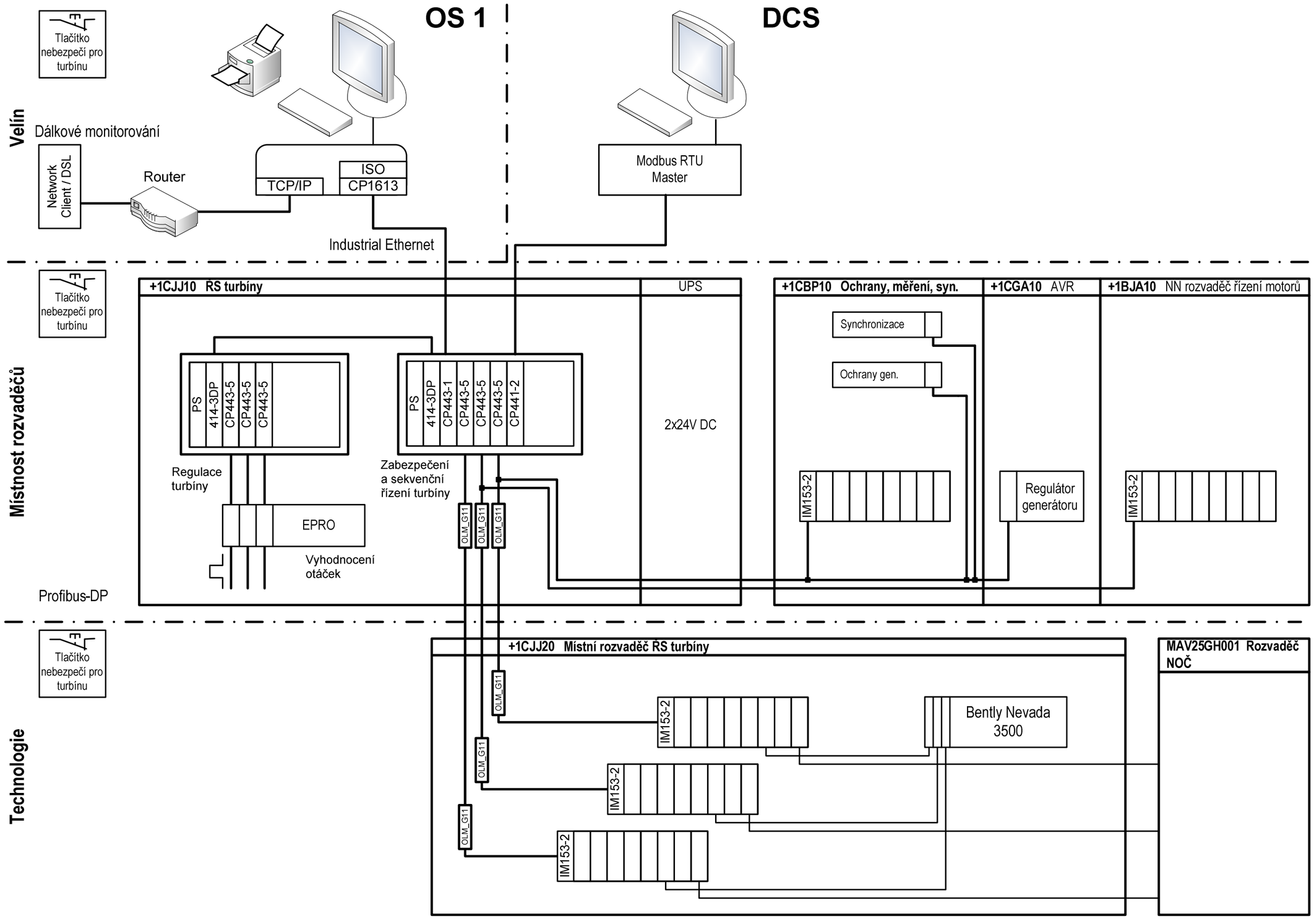
λ	Intenzita poruch (Failure Rate)
λ_D	Intenzita nebezpečných poruch (Dangerous Failure Rate)
λ_{DD}	Intenzita zjištěných nebezpečných poruch (Dangerous Detected Failure Rate)
λ_{DU}	Intenzita nezjištěných nebezpečných poruch (Dangerous Undetected Failure Rate)
λ_{SD}	Intenzita zjištěných bezpečných poruch (Safe Detected Failure Rate)
λ_{SU}	Intenzita nezjištěných bezpečných poruch (Safe Undetected Failure Rate)
PFD	Průměrná pravděpodobnost poruchy při vyžádání (Probability of Failure on Demand)
PFH	Průměrná pravděpodobnost poruchy za hodinu (Probability of Failure on Hour)
MTBF	Střední doba mezi poruchami (Mean Time Between Failure)
MTTF	Střední doba do poruchy (Mean Time to Failure)
MCTF	Střední počet cyklů do poruchy (Mean Cycles To Failure)
MTTR	Střední doba do zotavení (Mean Time to Repair)
T_1	Kontrolní interval periodické zkoušky (Test Interval – Mission Time)
t_{CE}	Ekvivalentní střední doba prostoje kanálů (Channel Equivalent Mean Down Time)
β	Podíl nezjištěných poruch, které mají nezjištěnou příčinu (Common Cause Ratio – undetected failures)
β_D	Z poruch zjištěných diagnostickými zkouškami podíl těch poruch, které mají společnou příčinu (Common Cause Ratio – failures detected by diagnostic test)
DC	Diagnostické pokrytí (Diagnostic Coverage)
SR	Podíl bezpečných poruch (Safe Ratio)

SFF	Podíl bezpečných výpadků (Safe Failure Fraction)
HFT	Hardwarová poruchová tolerance (Hardware Fault Tolerance)
SIL	Stupeň integrity bezpečnosti (Safety Integrity Level)
E / *E* / *PES*	Elektrické a/nebo elektronické a/nebo programovatelné elektronické součásti (Electrical/electronic/programmable electronic system)
SIS	Bezpečnostní přístrojový systém (Safety Instrumented System)
SIF	Bezpečnostní přístrojová funkce (Safety Instrumented Function)
MooN	Výběr M z N (Voting M out of N)
CCF	Porucha se společnou příčinou (Common Case Failure)
FAT	Tovární přejímací zkouška (FAT – Factory Acceptance Test)
SAT	Místní přejímací zkouška (SAT – Site Acceptance Test)
B_{10d}	Počet cyklů do 10% nebezpečných selhání součástí (number of cycles until 10% of the components fails dangerously)
C	Počet cyklů (number of cycles)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH


OS 1
DCS
Velín
Dálkové monitorování
Tlačítko nebezpečí pro turbínu
Network Client / DSL
Router
TCP/IP
ISO
CP1613
Modbus RTU Master
Industrial Ethernet
Místnost rozvaděčů
+1CJJ10 RS turbíny
UPS
PS
414-3DP
CP443-5
CP443-5
CP443-5
PS
414-3DP
CP443-1
CP443-5
CP443-5
CP443-5
CP441-2
2x24V DC
Regulace turbíny
EPRO
Vyhodnocení otáček
Zabezpečení a sekvenční řízení turbíny
OLM_G11
OLM_G11
OLM_G11
+1CBP10 Ochrany, měření, syn.
+1CGA10 AVR
+1BJA10 NN rozvaděč řízení motorů
Synchronizace
Ochrany gen.
IM153-2
Regulátor generátoru
IM153-2
Profibus-DP
Technologie
+1CJJ20 Místní rozvaděč RS turbíny
MAV25GH001 Rozvaděč NOČ
OLM_G11
OLM_G11
OLM_G11
IM153-2
IM153-2
IM153-2
Bently Nevada 3500

Příloha P II: Tabulka posouzení nebezpečí a rizika

Č.:	Zdroj nebezpečí	Příčina nebezpečí	Důvod nebezpečí	Následky v případě selhání SIS	Použité ochranné vrstvy
1	Zvýšené otáčky.	Převýšení otáček.	1. Náhlé odlehčení zátěže turbíny a porucha regulačního systému. 2. Porucha regulačního systému v průběhu najíždění turbíny. 3. Porucha regulace otáček při provozu turbosoustrojí v ostrovním režimu. 4. Porucha buzení generátoru. 5. Zničení spojky rotorů turbosoustrojí. 6. Pomalá reakce regulačního systému při překonávání pasivních odporů rotoru turbosoustrojí z nulových otáček. 7. Porucha regulačního systému při zkoušce skutečným převýšením otáček turbíny.	1. Poškození rotoru turbíny nebo zničení spojky rotorů. 2. Vytržení lopatek z rotoru. 3. Utržení ze základu a vymrštění turbíny. 4. Požár a další vážné následky.	1. Systém ochran odstaví turbínu - uzavře rychlozávěrný ventil turbíny při otáčkách turbíny >n_{vyp}. 2. Systém ochran odstaví turbínu -uzavře regulační ventily turbíny při otáčkách turbíny >n_{vyp}. 3. ad 5. Konstrukcí spojky rotorů turbosoustrojí 4. ad 6, 7 Monitorováním funkce regulačního systému.
2	Zpětné proudění páry do turbíny z odběru páry.	Převýšení otáček.	1. Netěsnost zpětné odběrové klapky v potrubí odběru páry.	1. Poškození rotoru turbíny nebo zničení spojky rotorů. 2. Vytržení lopatek z rotoru. 3. Utržení ze základu a vymrštění turbíny. 4. Požár a další vážné následky.	1. Použití dvou zpětných odběrových klapek, zapojených v sérii. 2. Nebo předpokládat uzavření regulačních ventilů turbíny na dostatečnou úroveň, tak aby nedošlo k převýšení otáček.

Č.:	Zdroj nebezpečí	Příčina nebezpečí	Důvod nebezpečí	Následky v případě selhání SIS	Použité ochranné vrstvy
3	Vysoký tlak páry na výstupu z turbíny (v kondenzá-toru).	Zvýšení tlaku páry na výstupu z turbíny	1. Porucha čerpadel chladícího okruhu kondenzátoru. 2. Porucha evakuačního systému. 3. Roztržení pojistné membrány. 4. Zanesení chladících trubek kondenzátoru.	1. Ulomení lopatek z důvodu mechanického namáhání. 2. Poškození lopatek posledních stupňů vlivem vlastních rezonancí. 3. Nevývaha rotujících hmot a těžké poškození radiálních ložisek. 4. Utržení ze základu.	1. Systém ochran odstaví turbínu při tlaku páry $>p_{vyp}$. 2. Hodnota odstavení turbíny p_{vyp} je závislá na průtoku páry na výstupu z turbíny, tak aby nedošlo k buzení vlastních rezonancí lopatek. 3. Použití záložního čerpadla chladícího okruhu. 4. Použití záložní vývěvy.
4	Vysoký tlak páry v konden-zátoru (na výstupu z turbíny).	Zvýšení tlaku páry v kondenzá-toru.	1. Porucha čerpadel chladícího okruhu kondenzátoru. 2. Porucha evakuačního systému. 3. Roztržení pojistné membrány. 4. Zanesení chladících trubek kondenzátoru. 5. Pojistná membrána je dimenzována pouze na 10% průtoku páry z důvodu netěsnosti uzavíracích orgánů při odstavení turbíny.	1. Roztržení pláště konenzátoru. 2. Roztržení výstupního hrdla turbíny.	1. Systém ochran odstaví turbínu při tlaku páry $>p_{vyp}$. 2. Použití záložního čerpadla chladícího okruhu. 3. Použití záložní vývěvy.

Č.:	Zdroj nebezpečí	Příčina nebezpečí	Důvod nebezpečí	Následky v případě selhání SIS	Použité ochranné vrstvy
5	Vysoká hladina kondenzátu v kondenzá-toru.	Ulomení lopatek posledních stupňů při zaplavení kondenzá-tem.	1. Pouze v případě, že dispoziční uspořádání kondenzátoru, odvodnění a turbíny umožňuje zaplavení kondenzátem. 1.1 Porucha regulátoru výšky hladiny kondenzátu v kondenzátoru. 1.2 Porucha kondenzátních čerpadel. 1.3 Přeplnění kondenzátoru systémem pro doplňování kondenzátu.	1. Ulomení lopatek z důvodu mechanického namáhání. 2. Nevývaha rotujících hmot a těžké poškození radiálních ložisek. 3. Utržení ze základu.	1. Systém ochran odstaví turbínu při výšce hladiny v kondenzátoru >h_{vyp}. 2. Použití záložního kondenzátního čerpadla. 3. Doplňování kondenzátu napojit na sběrnou nádrž kondenzátu.
6	Vysoký tlak páry v regulova-ném odběru páry.	Zvýšení tlaku páry v regulova-ném odběru páry	1. Zařazení regulovaného odběru páry do uzavřeného parního systému 2. Porucha způsobená uzavřením uzavíracího ventilu reg. odběru při zařazeném reg. odběru. 3. Porucha způsobená uzavřením regulačních ventilů regulovaného odběru při uzavřeném uzavíracím ventilu reg. odběru. 4. Pojistný ventil je dimenzován pouze na 10% průtoku páry z důvodu netěsnosti uzavíracích orgánů při odstavení turbíny.	1. Únik páry způsobený vytlačením těsnění na přírubových spojích. 2. V extrémním případě roztržení potrubí.	1. Systém ochran odstaví turbínu při tlaku páry v regulovaném odběru >p_{vyp}.

Č.:	Zdroj nebezpečí	Příčina nebezpečí	Důvod nebezpečí	Následky v případě selhání SIS	Použité ochranné vrstvy
7	Vysoký tlak vstupní páry.	Zvýšení tlaku vstupní páry.	1. Porucha parního kotle, napájecích čerpadel.	1. Únik páry způsobený vytlačením těsnění na přírubových spojích. 2. V extrémním případě roztržení potrubí. 3. V extrémním případě roztržení ventilové komory turbíny.	1. Ochranná funkce musí být realizována v systému ochran kotle. 2. Systém ochran odstaví turbínu při požadavku na odstavení z ochranného systému kotle.
8	Jiné nebezpečí, kterému může zabránit reakce operátora	Např. vysoká teplota páry na výstupu z turbíny, únik vody z chladiče generátoru, vysoká teplota ložisek turbosoustrojí, větší únik oleje	Např. příliš dlouhý chod turbíny bez zatížení, poškození chladiče generátoru, nedostatečný průtok oleje do ložiska, únik oleje na teplé části turbíny.	Např. poškození posledních stupňů lopatek, snížení izolačního stavu statorového vinutí generátoru, vytečení kompozice ložiska, požár.	1. Kontrola příslušných parametrů operátorem. 2. V případě požadavku operátora, odstavení turbíny bezpečnostním tlačítkem.