SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

MATERIÁLOVOTECHNOLOGICKÁ FAKULTA V TRNAVE

ANALÝZA RIZÍK BEZPEČNOSTNÝCH KRITICKÝCH SYSTÉMOV

Dizertačná práca

MTF-3145-2759

Predkladateľ:	Ing. Eduard Nemlaha
Vedúci:	doc. Ing. Pavel Važan, PhD.
Študijný program:	38-01-9 Automatizácia a riadenie
Špecializácia:	Riadenie procesov
Pracovisko:	Ústav aplikovanej informatiky, automatizácie a matematiky

Obsah

Anotácia

Predkladaná dizertačná práca na tému „Analýza rizík bezpečnostných kritických systémov“ je zameraná na analýzu vzniku možných rizík pre bezpečnostne kritické systémy. Cieľom je naznačenie možných metód slúžiacich na analýzu rizika a pomocou nich odhadnúť respektíve vypočítať pravdepodobnosť vzniku poruchy na konkrétnom systéme. Ako príklad bol zvolený systém elektrickej požiarnej signalizácie určitého objektu. Po analýze metód pre výpočet pravdepodobnosti vzniku rizika boli vybrané dve metódy pomocou ktorých bola vypočítaná pravdepodobnosť vzniku poruchy pre daný systém. Tieto metódy tiež pomohli určiť najslabšie články bezpečnostne kritického systému a načrtli jeho možné vylepšenie. Následne bol systém podrobený testovaniu, ktoré umožnilo určiť počet minimálnych testovacích scenárov na otestovanie celého systému.

Prínosom práce je vytvorenie metodiky na určovanie pravdepodobnosti vzniku rizika. Výsledky sa dajú využiť pri odhaľovaní možných porúch nielen pre systémy elektrickej požiarnej signalizácie, ale aj pre ostatné systémy súvisiace s bezpečnosťou budov a osôb (prístupové systémy, elektronické bezpečnostné systémy a podobne).

Annotation

The dissertation thesis with the title “Risk Analysis of Safety Critical Systems“ is orientated on an analysis of possible risks for safety critical systems. The aim is to present the possible methods of risk analysis and estimate or calculate the probability of failure creation of a concrete system. The system of an electric fire signal system of a specific object was selected as an example. Analysis of methods for probability calculation evoked the selection of two methods which supported the calculation of risk probability for the selected system. These methods also helped to determine the weakest components of the safety critical system and possible improvement. The system was tested and a number of minimal testing programmes for a complete system was determined.

The contribution of the thesis is the creation of methodology for determination of risk probability. The results can be used in uncovering possible failures not only for systems of

electric fire signal systems but also other systems connected with buildings and personal safety (Access systems, electronic safety systems and others).

Zoznam použitých symbolov

EPS		Elektrická požiarna signalizácia
EZS		Elektrické signalizačné zariadenie
VZT		Vzduchotechnické zariadenie
MaR		Meranie a regulácia
λ	[1/h]	Intenzita porúch (Failure Rate)
λ_D	[1/h]	Intenzita nebezpečných porúch (Dangerous Failure Rate)
λ_{DD}	[1/h]	Intenzita zistených nebezpečných porúch (Dangerous Detected Failure Rate)
λ_{DU}	[1/h]	Intenzita nezistených nebezpečných porúch (Dangerous Undetected Failure Rate)
λ_{SD}	[1/h]	Intenzita zistených bezpečných porúch (Safe Detected Failure Rate)
λ_{SU}	[1/h]	Intenzita nezistených bezpečných porúch (Safe Undetected Failure Rate)
PFD	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní (Probability of Failure on Demand)
PFH	[h]	Priemerná pravdepodobnosť poruchy za hodinu (Probability of Failure on Hour)
PFD_G	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní pre skupinu kanálov s majoritnou rozhodovacou logikou (Probability of Failure on Demand for group of channels)
PFD_S	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní pre subsystém senzorov (Probability of Failure on Demand for the sensor subsystem)
PFD_L	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní pre subsystém logiky (Probability of Failure on Demand for the logic subsystem)
PFD_{FE}	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní pre subsystém koncových prvkov (Probability of Failure on Demand for the final element subsystem)
PFD_{SS}	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní pre podporný subsystém (Probability of Failure on Demand for support subsystem)
PFD_{SYS}	[h]	Priemerná pravdepodobnosť poruchy pri vyžiadaní bezpečnostnej funkcie pre E/E/PE systém (Probability of Failure on Demand for the E/E/PE safety-related system)
MTBF	[h]	Stredná doba medzi poruchami (Mean Time Between Failure)
MTTF	[h]	Stredná doba do poruchy (Mean Time to Failure)
MCTF	[h]	Stredný počet cyklov do poruchy (Mean Cycles To Failure)
MTTR	[h]	Stredná doba do zotavenia (Mean Time to Repair)
T_1	[h]	Kontrolný interval periodickej skúšky (Test Interval – Mission Time)
t_{CE}	[h]	Ekvivalentná stredná doba prestoja kanálov (Channel Equivalent Mean Down Time)
t_{GE}	[h]	Ekvivalentná stredná doba prestoja rozhodovacej skupiny pre architektúry 1oo2 a 2oo3 (Voted Group Equivalent Mean Down Time for 1oo2 adn 2oo3)
β	[%]	Podiel nezistených porúch, ktoré majú nezistenú príčinu (Common Cause Ratio – undetected failures)
β_D	[%]	Z porúch zistených diagnostickými skúškami podiel tých porúch, ktoré majú spoločnú príčinu (Common Cause Ratio – failures detected by diagnostic test)
DC	[%]	Diagnostické pokrytie (Diagnostic Coverage)
SR	[%]	Podiel bezpečných porúch (safe ratio)
SFF	[%]	Podiel bezpečných výpadkov (Safe Failure Fraction)

MooN	Výber M z N (Voting M out of N)
HFT	Hardwarová poruchová tolerancia (Hardware Fault Tolerance)
SIL	Stupeň integrity bezpečnosti (Safety Integrity Level)
PES/E/E	Elektrické elektronické programovateľné elektronické súčasti (E/E/PES – electrical/electronic/programmable electronic system)
SIS	Bezpečnostný prístrojový systém (safety instrumented system)

1 Úvod

Systémy navrhované pre bezpečnostné účely v dnešnej dobe nie sú žiadnou novinkou. Už dlhšiu dobu sa používajú ako súčasť ochranných systémov, kde existuje nebezpečie ujmy na zdraví či ľudských životoch respektíve ohrozenie životného prostredia. Miera schopnosti odhaliť výskyt poruchy v takýchto systémoch, je závislá aj od konštrukcie daného systému, jeho umiestnenia, spôsobu prevádzky a údržby. Preto sú potrebné opatrenia na minimalizáciu nežiaducich porúch. Vždy existuje určitá miera ohrozenia bezpečnosti systému a preto je potrebné zaistiť aby systém vyhovoval požiadavkám zadaným používateľom. Donedávna sa bezpečnostné systémy navrhovali podľa praxe zavedenej v danej firme. V dnešnej dobe sa situácia rýchlo mení. Jednotný návod, ako navrhovať zariadenia súvisiace s bezpečnosťou, poskytuje výrobcom, ale aj užívateľom všeobecne uznávaná norma IEC EN 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems). Užívateľom prináša mnoho výhod, z ktorých najvýznamnejšia je možnosť pristupovať k bezpečnostným systémom exaktnejšie. Podstatu rizika možno totiž určenými metódami kvantifikovať a navrhnúť zodpovedajúci ochranný systém. Pokiaľ sú ochranné systémy navrhnuté v súlade s uznávanými normami, možno jasne preukázať ich vhodnosť. Zmenší sa počet prípadov, keď je ochranný systém nedostatočný, alebo naopak, predimenzovaný a v mnohých prípadoch sa dosiahne odpovedajúce riešenie s menšími nákladmi.

Analýza úrovne bezpečnostných systémov sa dá zhrnúť do určitých bodov:

- výber funkcií súvisiacich s bezpečnosťou systému
- identifikácia komponentov
- identifikácia nebezpečných stavov
- identifikácia možných príčin porúch
- výpočet intenzity porúch, ktoré majú za následok nebezpečný stav systému

Akým spôsobom možno v praxi použiť normu IEC EN 61508, upravujúcu problematiku funkčnej bezpečnosti elektrických/elektronických a programovateľných elektronických systémov ukazuje dizertačná práca zaoberajúca sa problematikou posudzovania a stanovenia funkčnej bezpečnosti bezpečnostne kritických systémov s následným testovaním navrhnutého systému. Táto problematika je dostatočne prepracovaná a tiež popísaná. Úroveň funkčnej

bezpečnosti závisí na zavedených opatreniach s cieľom zmenšiť riziko, a tiež záleží i na správnej činnosti týchto opatrení.

Cieľom práce je:

- analyzovať jednotlivé metódy a techniky využívané pre posudzovanie rizika.
- Vybrať vhodné metódy na posúdenie rizika a podľa nich navrhnúť metodiku
- Odhadnúť a porovnať bezpečnosť požiarneho, bezpečnostne kritického systému s kontrolou náväznosti na spínacie zariadenia tohto systému
- Navrhnúť testovacie scenáre softvéru pre takýto systém a minimalizovať počet testov pri čo najväčšom otestovaní.

2 Testovanie – základné pojmy a definície

2.1 Pojem testovanie

Ak si chceme byť istý, že softvér je vyvinutý bez chýb, musia sa vykonať potrebné testovania. Ak by sa chcel predať produkt, ktorý by nebol dostatočne odladený a zbavený všetkých chýb a nedostatkov, treba rátať s tým, že takýto predaj viacej uškodí ako pomôže – minimálne v očiach zákazníka, ktorému sa takýto výrobok „pritrafí“. Testovanie však neponúka úplnú istotu, že vyvinutý softvér je korektný. Dáva však možnosť vykonať sériu experimentálnych vyhodnotení produktu.

Priame ciele testovania možno zhrnúť do nasledovných bodov:

1. Testovanie je proces vykonávania (spúšťania) vytvoreného softvéru za účelom odhalenia chyby
2. Dobrý skúšobný prípad je taký, ktorý má vysokú pravdepodobnosť nájdenia doteraz ešte neodhalenej chyby
3. Test je úspešný, ak sa nájde doteraz ešte neodhalená chyba

Ak sa použije systematický prístup, testovaním sa vygenerujú aktivity cez celý životný cyklus softvéru. Celé to začína už pri vytvorení špecifikácie, kedy sa môžu odvodzovať akceptačné testy. Vytvorenie návrhu zasa dáva podklad pre zavedenie integračných a systémových testov. Dokončenie vývoja každého modulu, zasa spustí proces vytvárania a spustenia testov modulov. Navyše, hocijaká aktivita spojená s udržiavaním produktu by mala vyvolať opätovné vykonanie testov a prípadné aktualizovanie výsledkov tak, aby sa dala použiť metóda regresného testovania.

2.1.1 Verifikácia a Validácia

Tieto pojmy úzko súvisia s pojmom kvalita softvéru. Sú to vlastne metódy, príp. postupy, pomocou ktorých sa snažíme odhadnúť kvalitu vyvíjaného softvéru. Ako som už bolo spomínané, kvalitu vyvíjaného softvéru je potrebné zabezpečiť už počas jeho vývoja a nie až kompletným testovaním pred odovzdaním. Na to nám slúžia verifikácia a validácia (V&V).

Softvérová V&V je vlastne nejaká množina aktivít, ktorých cieľom je podporiť kvalitu vyvíjaného softvéru priamo počas vývoja. Je definovaná štandardom IEEE Std. 1012 pre validáciu a verifikáciu softvéru [1]. I napriek tomu, že poznáme viacero spôsobov definície

životného cyklu programu, môžeme s určitosťou vymedziť niekoľko fáz, ktoré sa nachádzajú v každej takejto definícii:

- definícia požiadaviek,
- analýza,
- návrh,
- implementácia,
- testovanie,
- uvedenie do prevádzky,
- dokumentácia

V každej fáze vývoja môžu nastať chyby, ktoré v konečnom dôsledku ovplyvnia kvalitu výsledného produktu, a taktiež aj cenu, či časový plán vývoja. Verifikácia slúži na odhalenie a prípadnú korekciu chýb počas každej fázy vývoja, číže vlastne verifikáciou môžeme zistiť, či daný čiastkový produkt každej fázy spĺňa požiadavky preň vymedzené. Avšak ani takáto verifikácia nezabezpečí, aby výsledný produkt splnil určené požiadavky. Validácia sa väčšinou používa až po ukončení fázy vývoja softvéru, na zisťovanie, do akej miery vytvorený produkt spĺňa potreby pre zamýšľané použitie (teda, či vlastne výsledný produkt robí v skutočnosti to, čo má).

2.1.2 Testovacie metódy

Testovanie je možné rozdeliť podľa spôsobu vykonávania testu na dve hlavné skupiny:

- manuálne,
- automatizované

V súčasnosti je oveľa viacej využívaná manuálna metóda testovania, kedy testovanie vykonáva skupina osôb – testerov priamou interakciou s testovaným produktom najčastejšie podľa dopredu stanoveného testovacieho postupu.

Pod automatizáciou testovania v užšom zmysle slova možno chápať používanie testovacej utility, ktorá zabezpečuje v pravidelných intervaloch (napr. po zostavení novej verzie) spustenie sady vopred definovaných testovacích scenárov. Ich výsledok sa môže ďalej spracovávať ručne i automaticky. Vo všeobecnosti sa dá predpokladať, že automatizovať pri testovaní možno takmer celý proces. V súčasnosti plná automatizácia nedokáže zohľadniť niektoré aspekty ľudskej činnosti akými sú podvedomé konanie či intuícia [2]. Psychologický aspekt sa momentálne darí nahrádzať len technikami umelej inteligencie, ktoré sú však značne

výpočtovo náročné a v konečnom dôsledku vždy len deterministické. Skúseného tvorcu testovacích scenárov nemožno ľahko nahradiť práve pre jeho nadobudnuté intuitívne zručnosti.

Pri samotnom procese testovania sa softvéroví inžinieri sústreďujú na celý životný cyklus testovania, ktorý začína testovaním funkcií a končí preberacím testovaním a podľa [3] zahŕňa:

- Testy funkcií a modulov, vykonávané prevažne softvérovými inžiniermi priamo v etape implementácie.
- Integračné testy, testovanie viacerých modulov súčasne.
- Regresné testovanie – testuje sa, či nenastal vedľajší efekt pridaním nového modulu alebo funkcie (zavlečenie chyby).
- Nezávislé testy - vykonávané nezávislými externými subjektmi.
- Alfa a beta testovanie, testovanie systému v reálnom prostredí. Pri alfa testovaní sa systém testuje bez živých dát. Testuje ho zákazník u vývojára. Beta testovanie používa reálne dáta so sledovaním výsledkov s možnosťou okamžitej nápravy.
- Systémové testovanie, séria rôznych testov, ktorá preveruje celý systém (HW, SW prostredie, databáza, ľudia, ...). Môžeme sem zaradiť aj testovanie obnovy (Recovery), bezpečnostné testovanie, výkonnostné a záťažové testovanie (Stress) a taktiež aj tzv. testovanie citlivosti (Sensititivity testing).
- Inštalačné testy - zahŕňajúce všeobecnú výkonnosť systému, ktorý je prvýkrát nainštalovaný na konkrétnom HW a operačnom systéme.
- Validačné testovanie – overenie, že softvér spĺňa „rozumné očakávania“ zákazníka, ktoré sú definované v špecifikovaných požiadavkách. Validačné testovanie sa vykonáva metódami black-box.
- Preberacie testovanie - je posledné míľnik pri testovaní projektu. V prípade úspešného zvládnutia nastáva oficiálne prevzatie projektu zákazníkom.

2.1.3 Ďalšie delenie testovania:

Klasifikované podľa cieľov, testovanie softvéru môže byť rozdelené na:

- presné testovanie (correctness testing),
- výkonnostné testovanie (performance testing),

- spoľahlivostné testovanie (reliability testing),
- bezpečnostné testovanie (security testing).

Klasifikované podľa fázy životného cyklu, softvérové testovanie môže byť rozdelené do nasledujúcich kategórií:

- podmienková fáza testovania (requirements phase testing),
- dizajnová fáza testovania (design phase testing),
- programová fáza testovania (program phase testing),
- hodnotenie testovaných výsledkov (evaluating test results),
- inštalačná fáza testovania (installation phase testing),
- akceptančný test a údržba testovanie(acceptance testing and maintenance testing).

Z hľadiska testovanej úrovne SW systému poznáme [4], [5]:

1. Testovanie funkčných blokov (orig. unit testing). Ide o testovanie funkčne ohraničených elementárnych jednotiek programu. Touto jednotkou môže byť napr. funkcia, či procedúra. Tento spôsob testovania testuje SW na najnižšej úrovni. K tomu, aby ho bolo možné vykonať, je potrebné umiestniť danú testovanú jednotku do prostredia, s ktorým je schopná komunikovať. Keďže je len veľmi zriedkavý prípad, že sa všetky vzájomne komunikujúce jednotky testujú súčasne, je potrebné vytvoriť tzv. testovacie drivery, ktoré simulujú očakávanú komunikáciu s testovanou jednotkou.
2. Integračné testovanie (integration testing). Integračné testovanie testuje schopnosť vzájomnej integrácie už otestovaných elementárnych jednotiek. Ide najmä o odhaľovanie chýb v komunikačných rozhraniach medzi jednotlivými jednotkami zúčastnenými v danej integrácii, ako aj medzi samotnými integráciami.
3. Testovanie systému (system testing). Ako už z názvu vyplýva, ide o testovanie na úrovni celého systému. Na tvorbu testovacích scenárov sa tu využívajú skutočné scenáre, ktorých vykonávanie sa od vyvíjaného systému očakáva. Pritom sa zisťuje, či systém spĺňa požiadavky, ktoré sú naňho kladené.
4. Akceptačné testovanie (acceptance testing). Akceptačné testovanie je testovanie, pri ktorom sa s už vyvinutým SW systémom pracuje spôsobom, pre ktorý bol daný systém

vyvinutý. Zisťuje sa, či spĺňa všetky používateľské požiadavky definované v úvodných fázach projektu. Akceptačné testovanie má väčšinou dve etapy. Prvou je akceptačné testovanie u dodávateľa FAT (final acceptance test), ktoré realizujú testeri dodávateľskej firmy. V druhej etape je tento typ testovania realizovaný priamo u zákazníka SAT (site acceptance test).

Napriek tomu, že spoľahlivosť jednotlivých funkčných blokov testovaného programu je základom pre spoľahlivosť celého systému, pri vyhodnocovaní kvality daného systému z pohľadu jeho používateľa je dôležitejšia práve spoľahlivá integrácia jednotlivých blokov a schopnosť ich vzájomnej spolupráce pri zabezpečovaní funkcionality kladenej na celý systém.

Ďalším dôležitým delením testovacích metód je delenie podľa spôsobu prístupu k vytváraniu skúšobných prípadov.

2.1.4 Testovacie prístupy

Existujú dva základné prístupy k testovaniu. V praxi známejší je tzv. testovanie relevantnosti (correctness testing) [6], [3]. Porovnáva skutočný výsledok testu s výsledkom očakávaným. Pri zhodnosti výsledkov, testovanie daným testom bolo úspešné. Ak nie, v programe je chyba. Pre účel porovnávania sa používa súbor očakávaných výsledkov [4]. Pričom tester môže, ale aj nemusí poznať zdrojový kód programu.

- Testovanie formou bielej skrinky (white-box testing)
- Testovanie formou čiernej skrinky (black-box testing)
- Testovanie pomocou šedej skrinky (gray-box testing)
- Výkonnostné testovanie (performance testing)
- Testovanie spoľahlivosti (reliability testing)
- Bezpečnostné testovanie (security testing)

Druhý spôsob je chybovo orientované testovanie (fault based testing). Tu sa skúma, či testovaný program neobsahuje niektorú zo známych chýb, typickú pre konkrétnu programovú sekvenciu.

2.1.5 Testovací prípad

Dobre navrhnutý testovací prípad pozostáva z troch častí [7]:

- Vstupy –môžu prichádzať z iných zdrojov – dáta z paralelných systémov, dáta z paralelných zariadení, dáta čítané zo súborov alebo databáz.
- Výstupy – môžu byť posielané do paralelných systémov a externých zariadení. Dáta môžu byť zapísané do súborov alebo databáz. Stav alebo prostredie môže byť modifikované spustením systému. Všetky tieto podstatné vstupy a výstupy sú dôležité súčasti testovacieho prípadu.
- Poradie vykonávania – existujú dva typy návrhu testovacích prípadov s ohľadom na poradie vykonávania: radenie do kaskády a nezávislé testovacie prípady.

2.1.6 Chyba

Aj keď sú pojmy chyba a porucha v oblasti testovania v úzkom súvise, znamenajú dva úplne rozdielne pojmy [8]. Porucha (failure) je definovaná ako odchýlka skutočnej funkcionality SW systému od funkcionality požadovanej. To znamená, že o výskyte poruchy hovoríme vtedy, ak sa testovaný program správa nesprávne. Chyba (fault) je príčinou poruchy. Ak program pri svojom behu narazí na chybu, jej typickým prejavom je porucha. Príčinou chyby je omyl (error). Podľa [8].je omyl ľudská činnosť, ktorá vedie k vytvoreniu SW systému obsahujúceho chybu. Medzi pojmami omyl, chyba a porucha existuje príčinne – nasledovný vzťah:

$$\text{Omyl} \rightarrow \text{Chyba} \rightarrow \text{Porucha} \qquad \textbf{(2-1)}$$

Základným pravidlom testovania je, že nie je možné dokázať, že systém nie je poruchový. Testovaním je možné zistiť prítomnosť chýb, ale nikdy nie je možné dokázať ich absenciu [4].

Chyby môžu byť do aplikácie vnesené v každom štádiu životného cyklu vývoja aplikácie, vrátane testovania. [9]

2.1.7 Spoľahlivosť a disponibilnosť

K tomu, aby sme mohli definovať spoľahlivosť, je potrebné zadefinovať pojem testovací scenár. Jednu z definícií ponúka napr. [4], kde „Testovací scenár je charakterizovaný počiatočným stavom testovaného objektu, testovacími vstupmi a podmienkami, a predpokladaným výsledkom.“ Jadrom testovacieho scenáru pri špecifikačne orientovanom testovaní je sekvencia akcií, ktoré je potrebné s daným SW vykonať pre otestovanie určitej funkcionality, zatiaľ čo pri implementačne orientovanom testovaní sú jadrom testovacieho scenáru vstupné údaje, ktoré vstupujú do určitej časti kódu za účelom testovania.

Test- naprogramovaný testovací scenár, ktorý je spustiteľný v danom testovacom prostredí. Test je teda spustiteľnou reprezentáciou testovacieho scenára. Test bol úspešný vtedy, ak sa po jeho spustení a vyhodnotení výsledku zhoduje skutočný výsledok s predpokladaným výsledkom definovaným v testovacom scenári.

Spoľahlivosť SW sa dá definovať ako pravdepodobnosť, že daný SW bude správne fungovať v danom prostredí počas daného časového cyklu. Na základe otestovania systému množinou testov sa dá matematicky vyjadriť spoľahlivosť, ktorú je možné od tohto systému očakávať, nasledovne:

$$R = 1 - \frac{f}{n} \qquad \textbf{(2-2)}$$

kde: R predpokladaná spoľahlivosť
n počet spustených testov
f počet neúspešných testov

Cieľom je, aby sa premenná R blížila k hodnote 1. V kategórii systémov, ktoré požadujú extrémne vysokú spoľahlivosť (medicína, letecká doprava a pod.), však nie je možné zabezpečiť dostatočnú spoľahlivosť len jednou testovacou metódou. Tu sa vyžaduje nasadenie viacerých testovacích metód a ich kombinácií [10].

Teoretickou úlohou vývoja SW je vyvinúť taký SW, ktorý neobsahuje žiadnu chybu. Čo je však nedosiahnuteľné [11] a preto sa zavádzajú kvantitatívne ukazovatele chybovosti, resp. bezchybnosti SW. Jedných z najznámejších a v praxi najviac používaných je „Priemerný čas medzi dvoma chybami“ (orig. MTBF – Mean Time Between Failures) [11], [12]. Úlohou vývoja SW je potom tento čas čo najviac predĺžiť.

S hodnotou MTBF úzko súvisí ďalší kvantitatívny znak pre vyjadrenie kvality SW a to je disponibilnosť SW. Výpočet disponibilnosti vychádza z pomeru času opravy a času prevádzky v rámci intervalu MTBF. Disponibilnosť je potom možné vyjadriť ako:

$$V = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF} \qquad \textbf{(2-3)}$$

kde: V disponibilnosť
$MTTR$ Mean Time To Repair (priemerný čas opravy)
$MTTF$ Mean Time To Fail (priemerný čas vzniku chyby – po oprave)
$MTBF$ Mean Time Between Failures (priemerný čas medzi dvoma chybami)

2.1.8 Testovateľnosť softvéru

Testovateľnosť je pravdepodobnosť, že sa v časti programu vyskytne pri jeho najbližšom spustení porucha v prípade, ak sa v tejto časti programu nachádza chyba. Norma IEEE definuje testovateľnosť ako schopnosť systému alebo komponenty umožňovať tvorbu testovacích scenárov a následne určiť, či bolo prevedené testovanie úspešné [13].

Z definícií vyplýva, že testovateľnosť je vlastne schopnosť SW byť testovaný. K tomu musí testovaný SW spĺňať určité podmienky. Prvou je, schopnosť poskytnúť také informácie, na základe ktorých sa dajú generovať potrebné testovacie scenáre. Druhou podmienkou je, že v prípade, že daný SW obsahuje chybu, musí počas testovania vygenerovanými testovacími scenármi reagovať na túto chybu poruchou.

Pri ideálnej testovateľnosti SW by sme mohli zaručiť jeho bezchybnosť v prípade, ak by bola počas testovania vykonaná každá elementárna časť programu aspoň raz, a ak by boli výsledky všetkých testov z testovacej množiny úspešné. V praxi, a to najmä pri nesprávne navrhnutej štruktúre SW systému, sa však vyskytujú chyby, ktoré sú nie vždy zdrojom poruchy, čo výrazne sťažuje proces testovania.

2.1.9 Kritériá adekvátnosti testovania

V ideálnom prípade by mala množina testovacích scenárov testovať daný SW systém s použitím úplnej množiny kombinácií vstupných parametrov, vnútorných premenných a ciest, ktorými môže spracovávanie daného programu prebiehať. Keďže v praxi by bola takáto množina kombinácií prakticky nekonečná (hovoríme, že testovacia množina je absolútna (exhaustive)[3]), bolo potrebné nájsť spôsob, ktorým by sa veľkosť testovacej množiny zredukovala a zároveň by sa docielilo dôveryhodné testovanie SW systému.

Pre tento účel boli zavedené tzv. kritériá adekvátnosti testovania (test adequacy criteria). Niekedy sa týmto kritériám adekvátnosti hovorí aj testovacie kritériá (testing criteria) [14]. Potom hovoríme, že testovacia množina (množina testovacích scenárov a k nim priradených vstupných hodnôt) spĺňa kritérium adekvátnosti vtedy, ak sa pri testovaní SW systému touto množinou dosiahne požadovaná hodnota pokrytia (coverage) [15]. Hodnota pokrytia pritom vyjadruje pomer otestovanej funkcionality vzhľadom na celkovú funkcionalitu testovaného SW systému.

$$pokrytie = \frac{otestovaná\_funkcionalita}{celková\_funkcionalita} * 100\% \qquad \textbf{(2-4)}$$

Ak je hodnota pokrytia 100% znamená to, že po úspešnom prebehnutí všetkých testovacích scenárov, ktoré sa pri určovaní hodnoty pokrytia brali do úvahy, a pri 100% testovateľnosti testovaného SW, je spoľahlivosť tohto SW 100% [16]. Hodnota 100% pre pokrytie a testovateľnosť je však len teoretická a prakticky nedosiahnuteľná.

Testovacie kritérium je možné vyjadriť dvomi definíciami [17]:

$$C(p, f, TS) = b \qquad \textbf{(2-5)}$$

alebo

$$C(p, f, TS) = r \qquad \textbf{(2-6)}$$

kde: p testovaný program
f špecifikácia testovaného programu
TS testovacia množina s použitými testovacími scenármi
B logická premenná nadobúdajúca hodnoty 0 alebo 1
r reálne číslo z intervalu [0,1]

V prvej definícii znamená výsledná hodnota b = 1, že testovacia množina TS je adekvátna pre testovanie programu p na základe jeho špecifikácie f. Analogicky znamená hodnota b = 0, že je množina TS neadekvátna.

Druhá definícia vyjadruje testovacie kritérium ako funkciu, ktorej výsledkom je reálne číslo r vyjadrujúce stupeň adekvátnosti. Čím vyššia je hodnota r, tým adekvátnejšia je testovacia množina TS pre testovanie programu p na základe jeho špecifikácie f.

2.2 Testovanie cesty

2.2.1 Diagram toku riadenia a testovacie kritéria

Pri testovanie cesty (path testing) musí byť splnená podmienka, aby tester poznal zdrojový kód programu. Každý program sa skladá z určitých blokov (podmienky, vetvenie...). Tieto bloky sú pretransformované do vývojového diagramu (flow graph). Tento diagram je orientovaný graf

$$G = (N, A, s, e) \qquad \textbf{(2-7)}$$

kde: N - procesné bloky
A - orientované spojnice blokov N
s,e - vstupy a výstupy programu.

Cieľom je vytvoriť čo najmenšiu množinu testov s čo najväčším pokrytím zdrojového kódu. Generovanie možných ciest je vychádza zo sledovania toku a smeru riadenia vo vývojovom diagrame. Testovanie cesty začína na vstupe programu a končí na výstupe. Takáto cesta je potom označovaná ako kompletná cesta a túto aj testujeme.

Základné testovacie kritéria stanovujúce hodnotu pokrytia kódu:

1. Všetky cesty (all path). Vykonávajú sa všetky existujúce cesty medzi vstupom a výstupom programu.
2. Všetky výrazy (all statements). Hlavným účelom je, aby každý výraz bol testovaný aspoň raz.
3. Všetky vetvy (all branches). Každá vetva každého rozhodovania musí byť vykonaná aspoň raz.

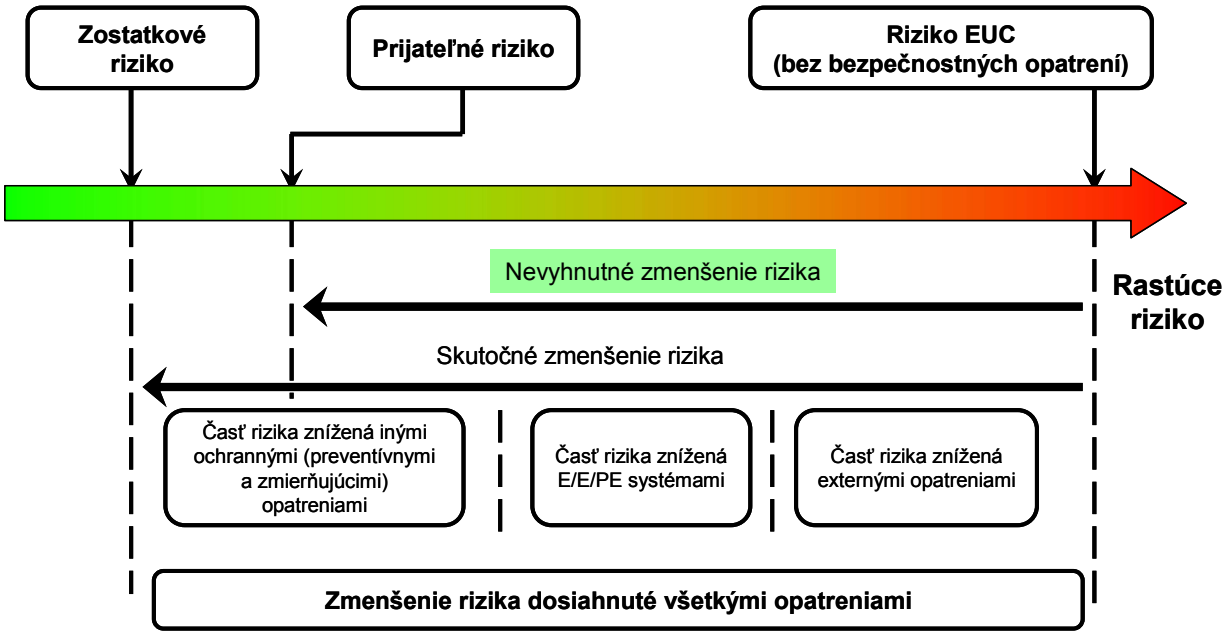
2.2.2 Etapy testovacieho procesu

Celý testovací proces možno rozdeliť do niekoľko fáz [18]:

- plánovanie testov – v tejto etape je nutné sa zamerať na správu incidentov, požiadaviek a konfigurácií a taktiež na plán zaistenia kvality.
- špecifikácia testov – definuje vlastne čo sa má testovať. Špecifikácia je súčasťou testovacích prípadov, skriptov a dát
- vykonávanie testov – manuálne, alebo automatizované, pričom sa používajú rôzne testovacie sekvencie, prostredia ale aj dáta
- záznam testov a vyhodnocovanie – aktuálne výstupy sa zaznamenávajú a porovnávajú s očakávanými výstupmi, pričom je zaznamenávaná aj správa o pokrytí cesty, o incidentoch...
- ukončovacie kritéria – musia byť špecifikované už v úvode testovacieho procesu

3 Bezpečnosť

Bezpečnosť vo význame anglického pojmu Safety je v technickej praxi chápaná ako jeden z atribútov komplexného ukazovateľa spoľahlivosti (Dependability), ktorý vyjadruje mieru, do akej sa môže používateľ spoľahnúť, že systém funguje tak, ako fungovať má, že je v daných podmienkach a v danom časom úseku použiteľný a že je bezpečný. Takto ponímaná spoľahlivosť predstavuje kombináciu atribútov bezporuchovosti, pohotovosti, udržiavateľnosti a bezpečnosti, známu pod anglickou skratkou RAMS (Reliability, Availability, Maintainability, Safety). Komplexný pohľad na taxonómiu spoľahlivosti a jej jednotlivých atribútov je k dispozícii napr. v [19].



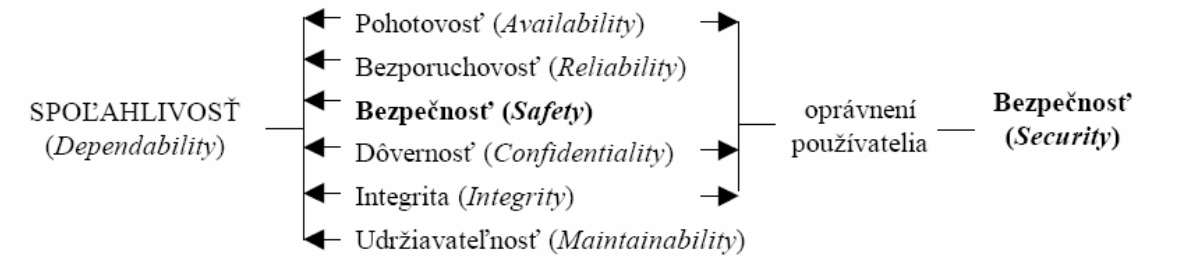
Obr. 3-1 Znižovanie rizika

Bezpečnosť sa používa na označenie neprítomnosti neprijateľných úrovní rizika fyzického zranenia alebo poškodenia zdravia osôb, priamo alebo nepriamo v dôsledku poškodenia majetku alebo životného prostredia. Odráža tak schopnosť systému fungovať s prijateľnou úrovňou rizika pre okolie systému i pre systém samotný. Od bezpečnostne kritických systémov sa očakáva realizácia špecifickej funkcie alebo funkcií zaisťujúcich udržanie rizík na prijateľnej úrovni. Tieto funkcie sú označované ako bezpečnostné funkcie. Na dosiahnutie funkčnej bezpečnosti sú potrebné dva typy požiadaviek:

- požiadavky na bezpečnostné funkcie (t.j. čo má daný systém robiť, aby fungoval bezpečným spôsobom), ktoré sú výsledkom analýzy nebezpečenstiev (Hazard Analysis);
- požiadavky na integritu bezpečnosti (t.j. s akou mierou istoty bude bezpečná funkcia vykonaná uspokojivým spôsobom), ktoré sú výsledkom procesu posúdenia rizík (Risk Assessment).

Pokiaľ by boli bezpečnostné funkcie systému nedostatočné z pohľadu požadovaného zníženia rizika, nezáležalo by na tom, aká bude bezporuchovosť systému, pretože takýto systém by nebol bezpečný. Bezpečnostné funkcie sú v čoraz väčšej miere vykonávané E/E/PES systémami, ktoré sú zložité a je prakticky nemožné určiť všetky druhy ich porúch alebo otestovať všetky ich možné správania Obr. 3-1.

Treba pripomenúť, že slovenský i český jazyk používajú ten istý výraz „bezpečnosť“ na označenie anglických pojmov Safety aj Security. Vzťah medzi spoľahlivosťou a bezpečnosťou (v obidvoch významoch) ukazuje (Obr. 3-2) [20]



Obr. 3-2 spoľahlivosť a bezpečnosť

Nebezpečenstvo - vlastnosť objektu spôsobiť neočakávaný negatívnu jav (latentná vlastnosť objektu). Systém je nebezpečný vtedy, keď počas jeho prevádzky môže vzniknúť negatívny jav.

Ohrozenie - stav keď môže byť aktivované nebezpečenstvo (aktívna vlastnosť objektu).

Riziko predstavuje vzájomný vzťah medzi pravdepodobnosťou vzniku negatívneho javu a jeho dôsledkom. Dôsledky ohrozenia sú priamo závislé na tom, aká je pravdepodobnosť, že sa nežiaduca udalosť stane, a čo môže spôsobiť ohrozenie.

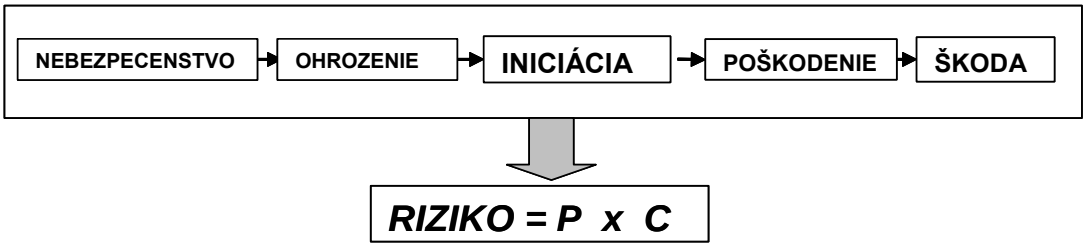
Matematické vyjadrenie rizika:

$$R = P.C \qquad \textbf{(3-1)}$$

kde: R – stupeň rizika

P – pravdepodobnosť výskytu danej udalosti

C – dôsledok sledovanej udalosti.



Obr. 3-3 Kauzálna závislosť

Rozšírená definícia rizika zahŕňa v sebe aj hodnoty ako E a hodnotu O

$$R = P.C.E.O \qquad \textbf{(3-2)}$$

kde: E – časová expozícia t.j. doba trvania podmienok pre vznik negatívneho javu

O – možnosť využitia ochranných opatrení v etape ohrozenia

Pri analýze rizika treba zistiť, o aké riziká sa ide a rozdeliť ich do skupín na riziká akceptovateľné a riziká, ktoré treba redukovať. Akceptovateľné riziká sú také, ktoré neprekračujú prijateľné riziko. Prijateľné riziko je najväčšie ešte možné riziko určitého technického procesu alebo stavu. Riziko, ktoré túto hranicu prekračuje treba redukovať, preto musíme použiť ochranné opatrenia (viackanálová štruktúra, technika reakčnej bezpečnosti, normy, atď.) na jeho zníženie. Po použití týchto opatrení sa nám zníži akceptovateľné riziko na zostatkové. Zvyšné riziko je riziko redukované, ktoré už redukujeme pomocou ochranných zariadení alebo bez ochranných zariadení.

Vo všeobecnosti sa nedá prijateľné riziko kvantitatívne vyjadriť. Prijateľné riziko je určované subjektívnymi aj objektívnymi vplyvmi a je pre rôzne použitia značne rozdielne. Subjektívne vplyvy sú napr.:

- osobné, pocity ohrozenia vyjadrené skutočnosťou, že určité nebezpečenstvá sú viditeľné, iné nie, alebo či za istých okolnosti ohrozené osoby sami neovplyvňujú priebeh procesu;
- spoločenská akceptácia nebezpečenstva;
- postihnutý okruh osôb, napr. potreba ochrany detí a chorých.

Ochrana obecne znamená zníženie rizika pomocou opatrení, ktoré obmedzia buď početnosť výskytov alebo rozsah škôd alebo oboje. Často sa dá bezpečnosť dosiahnuť spolupôsobením viacerých týchto opatrení. [21]

3.1.1 Metódy analýzy rizík

Prejavom rizika je vždy počet obetí, počet zranení, materiálne straty alebo škody na životnom prostredí. Riziko je preto orientované na hodnotenie havárii. Havária môže byť dôsledkom veľkého množstva iných udalostí, preto je kladený väčší dôraz na štatisticko-analytický prístup. Taký prístup je dobrým základom, ak sa zameriame na riziko ako veličinu ktorá je jasne definovaná a merateľná, metódami hodnotenia rizika a dokážeme ju modelovať.

Hodnotenie bezpečnosti systému je závislé od časového horizontu na ktorý vytvorený model orientujeme. Toto kritérium závisí od oblasti použitia systému. Ak sa hovorí o štatisticko-analitickom hodnotení, ide o skúmanie kauzálnej súvislosti javov v zmysle „možnosti očakávaného a nie predpovedi istého“. Odhad rizika má tri zásadné zložky: zistenie rizika (t.j. identifikáciu a kvantifikáciu rizika), ocenenie rizika (t.j. porovnávanie a váženie rôznych aspektov bezpečnosti v priebehu času) a riadenie rizika, (t.j. formulácia a implementácia riziku zodpovedajúcej bezpečnostnej politiky).

Pri vyhodnocovaní rizika sú známe metódy predikujúce možné cesty ku katastrofickému správaniu sa systému (ex ante) alebo metódy založené na analýze podobných havarijných udalostí, ku ktorým došlo v minulosti (ex post).

Na vytváranie modelov je dôležitý matematický opis dynamického systému. Najvhodnejším nástrojom sa zdá byť teória diskrétneho stavového priestoru. Jej výhodou je formalizmus vhodný na riešenie počítačom, ako aj jej použiteľnosť na riešenie zložitejších úloh, čím prekonáva teóriu založenú na frekvenčnej analýze, kompenzácii nulových bodov a pólov a použití transformácií.

Nevýhoda vyplývajúca zo zložitosti maticového počtu sa kompenzuje, ak sa modeluje systém Petriho sieťou. Tak sa dajú zistiť všetky možné prechody systému do stavov, kedy už nie je možné žiadne východisko (blokovanie Petriho siete) alebo okolnosti vedúce do stavov, ktoré nie sú z hľadiska bezpečnosti povolené.

Na modelovanie stochastického správania sa sústavy sa dá použiť štatistická neurónová sieť. Deterministické zobrazenie vykonávané systémom najlepšie aproximujúcim požadovanú funkci (ak je známa množina vstupov z p rozmerného, a im zodpovedajúce výstupy z r

rozmerného priestoru) môže byť vykonávané doprednou neurónovou sieťou. Tá je vhodná pri časovo invariantnom správaní sa systému. Niekedy je však dôležitý časový kontext predkladaných vstupov. Vtedy je použiteľná rekurentná neurónová sieť.

Uznávaným štandardom je metóda HAZOP (HAZard and OPerability systém). Každý subsystém sa skúma a definujú sa možné odchýlky od základnej funkcie, kľúčovými výrazmi: NO, NOT, MORE, LESS, AS WELL AS, PART OF, SONNER, LATER, REVERSE, OTHER THAN. Systematickým kombinovaním týchto slov sa dajú postihnúť všetky možné cesty od normálnej funkcie k odchýlke. Ak nie sú dôsledky významné alebo udalosti vedúce k nim sú veľmi nepravdepodobné, nemusia byť brané do úvahy. [22]

Tradičné metódy sú založené na analytickom prístupe. V niektorých metódach je dôležitý brainstorming- kladenie otázok, vyslovovanie námietok skupinami expertov.

- Kontrolné záznamy (angl. Check list analysis, CLA): pre každý podsystém sa určí tabuľka jednotlivých udalostí, ktoré majú výstupné atribúty ÁNO-NIE-NIE JE VHODNÉ. Takto je možné riešiť nielen očakávané kritické udalosti, ale aj neskôr analyzovať stav, ku ktorému došlo.
- Rutinné testy (angl. Routine tests, RT): zisťovanie, či sú zabezpečené všetky údaje o nebezpečenstve v danom procese a o jeho možných následkoch. Požadujú sa údaje získané simuláciou tohto procesu.
- Bezpečnostný audit (angl. Safety audit, SA) :Vzťahuje sa na kritické posúdenie všetkých aspektov prevádzky systému, na inšpekčné pochôdzky neformálneho charakteru alebo dlhodobé posudzovanie tímom odborníkov rôznych profesií.
- Čo sa stane ak... (angl. What if analysis, WFA): kladením otázok sa zisťujú možné medzery v bezpečnosti a navrhujú sa vhodné opatrenia.
- Použitie ukazovateľov bezpečnosti (angl. Hazard Indices, HI): sústava sa rozdelí na časti, ktoré sa ohodnotia podľa dohodnutej stupnice stupňa nebezpečenstva v rozmedzí NÍZKE-KATASTROFÁLNE. Ak sú analyzované bezpečnostné mechanizmy systému je možné zmierniť tieto hodnotenia.
- Predbežná analýza nebezpečenstva (angl. Preliminary Hazard Analysis, PHA) obsahuje prehľad nebezpečenstiev vhodných pre neskoršiu detailnú analýzu. Základom metódy je identifikovať predmet štúdia a definovať problémy, ktoré môžu vzniknúť.

Iné metódy hodnotenia

- Analýza vplyvov porúch a ich následkov (angl. Failure Modes, Efects and Criticaly Analysis, FMECA)
- Analýza stromu porúch (angl. Fail Tree Analysis, FTA)
- Analýza nebezpečenstva (angl. Hazard Analysis, HAZAN)
- Analýza stromom nebezpečenstva (angl. Hazard Tree Analysis, HTA)
- Analýza príčin následkov (angl. Cause Consequence Analysis, CCA)
- Analýza spoľahlivosti človeka (angl. Human Reliability Analysis, HRA)

Identifikácia nebezpečenstva zahŕňa systematické preskúmanie skúmaného systému s cieľom identifikovať druh prítomných obsiahnutých nebezpečenstiev spolu so spôsobmi, ako by mohli vzniknúť. Užitočný vstup do procesu identifikácie nebezpečenstva môžu poskytnúť záznamy o predchádzajúcich haváriách a skúsenosť z predchádzajúcich analýz rizika. Pri posudzovaní nebezpečenstiev je prítomný prvok subjektivity a že identifikované nebezpečenstvá nemusia vždy práve ohrozovať systém [23]. Dôležité je, aby sa identifikované nebezpečenstvá preskúmali vo všetkých súvisiacich nových údajov.

Metódy identifikácie nebezpečenstva sa dajú zhruba rozdeliť do troch kategórií: [22]

- porovnávacie metódy (kontrolné zoznamy, indexy nebezpečenstva, preskúmania predchádzajúcich údajov)
- základné metódy (štúdie nebezpečenstva a prevádzkyschopnosti, analýza spôsobov a následkov poruchových stavov)
- techniky induktívnych úvah (logický diagram stromu udalostí)

Bez ohľadu na skutočne použitú techniku je dôležité, aby sa v celom procese identifikácie nebezpečenstva venovala primeraná pozornosť. Preto sa do procesu identifikácie nebezpečenstva zahŕňa aj havarijný scenár zahrňujúci ľudské a organizačné chyby.

Odhad rizika je ďalším krokom analýzy rizika. V praxi môže identifikácia nebezpečenstva konkrétneho systému, zariadenia alebo činnosti poskytnúť značné množstvo potencionálnych havarijných scenárov. Nemusí sa vždy pokladať za reálne podrobiť každý z nich podrobnej kvantitatívnej analýze početnosti a následkov. V takýchto prípadoch môže byť vhodné usporiadať havarijné scenáre kvalitatívne a umiestniť ich do matice rizika v závislosti od

rozličných úrovní rizika. Kvantifikácia sa potom sústredí na tie scenáre, ktorým prisudzujeme vyššie úrovne rizika. Jestvuje veľa matíc rizík. Najvhodnejšia z nich pre danú analýzu závisí od konkrétnej aplikácie. Dôležité je, aby sa tvar akejkoľvek použitej matice zaznamenal spolu s odhadnutými pozíciami všetkých predpokladaných havarijných scenárov bez ohľadu na to, či sa ďalej podrobujú kvantitatívnej analýze.

Kvantitatívna analýza zvyčajne vyžaduje odhady početnosti (alebo pravdepodobnosti) výskytu nežiaducej udalosti a súvisiaceho následku (alebo závažnosti), aby poskytla ukazovateľ rizika.

Cieľom analýzy početnosti (pravdepodobnosti) výskytu je určiť početnosť výskytu každej nežiaducej udalosti alebo havarijného scenára opísaného v etape identifikácie nebezpečenstva. Zvyčajne sa používajú tri postupy:

1. Vychádza sa z príslušných predchádzajúcich údajov na určenie početnosti s akou sa tieto udalosti nastali v minulosti. Potom sa posúdi ich početnosť výskytu v budúcnosti. Použité údaje majú zodpovedať danému druhu systému i prevádzkovým normám danej organizácie.

2. Predpovedá sa početnosť výskytov pomocou techník ako je analýza stromu udalostí a analýza stromu poruchových stavov. Ak údaje z minulosti sú nedostupné alebo nevhodné, je nevyhnutné odvodiť frekvencie udalostí analýzou systému a jeho súvisiacich spôsobov poruchových stavov. Číselné údaje o všetkých príslušných udalostiach sa potom kombinujú tak, aby poskytli odhad početnosti výskytu nežiaducich udalostí. Pri používaní techniky predpovedí je dôležité zabezpečiť, aby sa v analýze nechal primeraný priestor možnosti vzniku porúch rovnakého typu, ktorý zahŕňa náhodné poruchy viacerých rozličných častí v rámci systému.

3. Využije sa úsudok expertov. Jestvuje veľa formálnych metód na získanie transparentných a explicitných úsudkov expertov, ktoré poskytujú pomoc pri formovaní vhodných otázok. Úsudky expertov sa majú zakladať na všetkých dostupných informáciách.

Analýza následkov (angl. Cause-Consequence Diagrams, CCD) je kombináciou metód ETA a FTA, pričom príčiny inicializačných udalostí stromu udalostí ETA sú analyzované pomocou stromu porúch FTA. Metóda zahŕňa odhad účinku na osoby, majetok alebo životné prostredie ak nastane nežiaduca udalosť. Z dôvodu priamej súvislosti metódy CCD s ETA a FTA nie je CCD štandardizovaná.

Najčastejšie používané metódy z hľadiska vhodnosti uplatnenia danej metódy sú:
Markovove modely sú mimoriadne často používanou metódou na modelovanie a analýzu

širokého spektra spoľahlivostných úloh a sú štandardizované. Metóda na rozdiel od FTA dovoľuje modelovať časovú i sekvenčnú závislosť stavov systému. Určitou modifikáciou Markovových modelov sú Petriho siete, ktoré sú tiež veľmi prehľadným a výkonným nástrojom na grafickú interpretáciu modelu.

Analýza stromu udalostí (angl. Event Tree Analysis, ETA) je technikou analýzy nebezpečenstva a početnosti výskytu, ktoré využívajú induktívne zdôvodnenia na prenos rozličných inicializačných udalostí do možných výstupov. Metóda sleduje priebeh procesu od danej iniciačnej udalosti cez konštruované udalosti vždy na základe dvoch možností – priaznivej a nepriaznivej. Táto technika môže byť kvalitatívna alebo kvantitatívna. ETA sa široko požíva na zariadenia s inžinierskymi vlastnosťami zabraňujúcimi haváriám. Treba poznamenať, že pravdepodobnosti v strome udalostí sú podmienené pravdepodobnosti., čo znamená, že vlastne vzniknú na základe nejakej inej okolnosti ktorá danú pravdepodobnosť vyvolá. ETA je induktívny druh analýzy, ktorom základnou otázkou je čo sa stane, ak.... Poskytuje zreteľný vzťah medzi činnosťou alebo poruchou rozličných zmierňujúcich systémov a výslednou nebezpečnou udalosťou, ktorá nastane po výskyte jednej iniciačnej udalosti. Je veľmi užitočná pri identifikácii udalostí, ktoré vyžadujú ďalšiu analýzu pomocou FTA.

Analýza príčin a následkov porúch (angl. Fault Modes and Effects Analysis, FMEA) je základná technika identifikácie nebezpečenstva a analýzy početnosti výskytu, ktoré analyzujú všetky príčiny poruchových stavov daného zariadenia a ich účinky na ďalšie časti. Tieto hľadá na základe systematicky a štruktúrovane vymedzených porúch zariadenia. Táto technika je pôvodne kvalitatívna, hoci ju možno kvantifikovať. Je to induktívna technika, ktorá vychádza zo sekvencie otázok typu ”čo sa stane, ak....?“ Analýza sa zvyčajne znázorňuje vo vytvorenej tabuľke alebo na pracovnom hárku. FMEA je prístup typu odspodu hore a rozoberá vždy iba jeden následok vybraných druhov poruchových stavov súčastí. Hlavnými nevýhodami tejto techniky sú ťažkosti pri rezervovaní a pri zohľadňovaní opravárenských činností, ako aj jej koncentrácia na poruchy jedného prvku, modulu.

Analýza stromu poruchových stavov (angl. Fault Tree Analysis, FTA) je technika identifikácie nebezpečenstva a analýzy početnosti výskytu, ktorá začína od nežiaducej udalosti a určuje všetky spôsoby, akými by mohla nastať. Postupy sa znázorňujú graficky. Táto metóda môže byť buď kvalitatívna alebo kvantitatívna. Poruchové stavy identifikované v strome môžu byť udalosti súvisiace s poruchami hardvérových súčastí, s ľudskými chybami alebo inými dôležitými udalosťami, ktoré vedú k nežiaducej udalosti. FTA ponúka usporiadaný prístup,

ktorý je vysoko systematický súčasne však dostatočne pružný, aby umožňoval analýzu množstva faktorov vrátane ľudských interakcií s fyzikálnymi javmi. Aplikáciu prístupu zhora – dolu, ktorá je vlastná tejto technike, sústreďuje pozornosť na tie účinky porúch, ktoré priamo súvisia so špičkovou udalosťou.

Štúdia nebezpečenstiev a prevádzkyschopnosti (angl. Hazard and Operability, HAZOP) je základná technika identifikácie nebezpečenstva pomocou systému kľúčových slov, ktorá systematicky vyhodnocuje každú časť systému s cieľom odhaliť, ako môžu nastať odchýlky od konštrukčného zámeru a či môžu spôsobiť problémy. Zároveň sú navrhované alebo overované opatrenia, ktoré zabránia nežiaducemu rozvoju udalosti alebo zmiernia nežiaduce dôsledky. Osobitne užitočná je pri identifikácii nepredvídaných nebezpečenstiev zabudovaných do zariadení vďaka nedostatku informácií alebo vyvolaných na jestvujúcich zariadeniach zmenami podmienok procesu alebo prevádzkových postupov.

Analýza spoľahlivosti človeka (angl. Human Reliability Assessment, HRA) je technika analýzy početnosti výskytu, ktorá sa zaoberá účinkom osôb na činnosť a výkon systému a vyhodnocuje vplyv chýb človeka na jeho bezporuchovosť. Vychádza sa z predpokladu, že rozhodovanie operátorov prebieha v krízových situáciách a za stresových podmienok.

Predbežná analýza nebezpečenstva (angl. Preliminary Hazard Analysis, PHA) je technikou identifikácie nebezpečenstva a analýzy početnosti výskytu, ktorú možno využiť v rannej etape návrhu na identifikáciu nebezpečenstiev a posúdenie ich kritickosti. Spravidla sa používa ako prostriedok na výber inej, podrobnejšej metódy. Môže byť taktiež užitočná pri analýze jestvujúcich systémov alebo pri priraďovaní priorít nebezpečenstvám, keď okolnosti bránia použiť dokonalejšiu techniku. Stanovuje zoznam nebezpečenstiev a všeobecných nebezpečných situácií na základe rôznych charakteristík (použité materiály, zariadenia, prevádzkové prostredie, umiestnenie, atď). Použitie končí identifikáciou možností, že nastane úraz a kvalitatívnym vyhodnotením rozsahu možného úrazu alebo poškodenia, ktoré ďalej môže vyústiť do identifikácie možných nápravných opatrení.

Blokový diagram bezporuchovosti (angl. Reliability Block Diagram, RBD) je technika analýzy početnosti výskytu udalostí, ktorá vytvára model systému a jeho rezerv na vyhodnotenie bezporuchovosti celého systému. Ide o grafickú reprezentáciu logickej štruktúry systému, pozostávajúcej so subsystémov a prvkov.

Zatrieďovanie do kategórií je prostriedkom zatrieďovania rizík do príslušných a vhodne

definovaných kategórií s cieľom vytvoriť príslušné skupiny rizík.

Kontrolné zoznamy je technika identifikácie nebezpečenstva, ktorá poskytuje zoznam typických nebezpečných materiálov a potencionálnych zdrojov havárií, ktoré treba brať do úvahy. Môže vyhodnotiť zhodu s kódmi a normami. Je to veľmi jednoduchá metóda pre rýchlu prevádzkovú kontrolu.

Analýza spoločnej príčiny porúch (angl. Common Cause Failure Analysis, CCF) je metóda posudzovania, či je možný výskyt náhodnej poruchy viacerých častí alebo prvkov systému a jej pravdepodobný celkový účinok na systém. Ak je pravdepodobnosť výskytu poruchy vplyvom spoločnej príčiny významne väčšia ako dvoch alebo viacerých samostatných udalostí, potom je spoločná príčina poruchy dôležitým rizikovým činiteľom.

Modely následkov znamenajú odhad účinku udalostí na ľudí, majetok alebo na prostredie. Sú dostupné zjednodušené analytické postupy a zložité počítačové modely.

Delfská technika je prostriedok na kombinovanie názorov expertov, ktoré môžu podporiť analýzu početností výskytu, modelovanie následkov a odhad rizika. Táto metóda je výhodná najmä pri riešení krízových situácií v rozsiahlych systémoch, ktoré sú už v prevádzke.

Indexy nebezpečenstva je technika identifikácie a vyhodnocovania nebezpečenstva, ktorú možno použiť na klasifikáciu rozličných voliteľných možností systému a identifikáciu menej nebezpečných voliteľných možností.

Simulácia metódou Monte-Carlo a ďalšie simulačné techniky, sú technikami analýzy početnosti výskytu, ktoré využívajú model systému na vyhodnocovanie variácií vstupných podmienok a predpokladov.

Metóda anketovej analýzy je hlavne zameraná na hľadanie možných následkov vybraných porúch zariadenia. Kladením vhodných otázok možno získať množstvo kvalitných informácií využiteľných v metóde matíc a v metóde podpory rozhodovania.

Metóda matíc je výhodnou z hľadiska schopnosti podchytiť veľké množstvo vzájomných vzťahov medzi hmotnými a nehmotnými aktívami, hrozbami a slabinami.

Analýza skrytých ciest je metóda identifikácie skrytých ciest, ktoré by mohli spôsobiť výskyt nepredvídaných udalostí.

3.1.2 Úrovne integrity bezpečnosti (SIL)

Pravdepodobnosť, že systém bude za všetkých stanovených podmienok a v stanovenom časovom období uspokojivo vykonávať bezpečnostné funkcie, označujeme pojmom integrita bezpečnosti (Safety Integrity). Úroveň (hladina) integrity bezpečnosti (Safety Integrity Level, SIL) sa vyjadruje číslom 1 až 4, pričom SIL 4 označuje najvyššiu možnú úroveň a používa sa pre najnebezpečnejšie dôsledky zlyhania bezpečnostných funkcií.

Úroveň integrity bezpečnosti SIL je typicky vyjadrovaná pojmami, ktoré súvisia s bezporuchovosťou alebo pohotovosťou. Konkrétne hodnoty jednotlivých SIL definuje generický štandard IEC 61508 v závislosti od režimu prevádzky, v akom sa daný systém nachádza. Bezpečnostne kritické systémy môžu vo všeobecnosti fungovať:

- v režime nepravidelnej prevádzky (Low Demand Mode);
- v režime nepretržitej prevádzky (High Demand Mode / Continuous Mode)

Tabuľka 1 Úrovne integrity bezpečnosti podľa IEC 61508

SIL	Low Demand Mode		High Demand / Continuous Mode	
	Faktor redukcie rizika	Priemerná pravdepodobnosť nebezpečnej poruchy pri požiadaní o bezpečnostnú funkciu	Faktor redukcie rizika	Intenzita
SIL 4	100000 - 10000	$\geq 10^{-5}$ - $< 10^{-4}$	100000000 - 10000000	$\geq 10^{-9}$ - $< 10^{-8}$
SIL 3	10000 - 1000	$\geq 10^{-4}$ - $< 10^{-3}$	10000000 - 1000000	$\geq 10^{-8}$ - $< 10^{-7}$
SIL 2	1000 - 100	$\geq 10^{-3}$ - $< 10^{-2}$	1000000 - 100000	$\geq 10^{-7}$ - $< 10^{-6}$
SIL 1	100 - 10	$\geq 10^{-2}$ - $< 10^{-1}$	100000 - 10000	$\geq 10^{-6}$ - $< 10^{-5}$

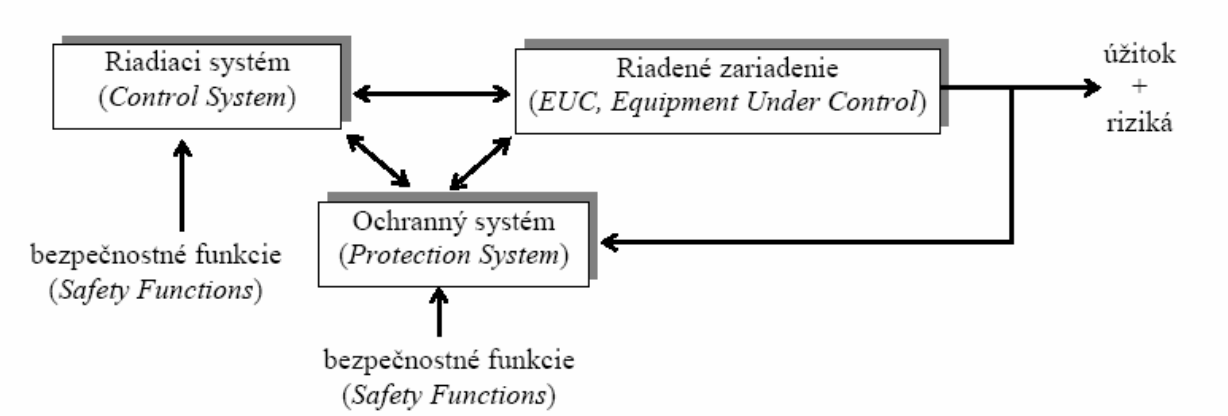
Úroveň integrity bezpečnosti v prípade nepravidelnej prevádzky sa udáva ako priemerná pravdepodobnosť poruchy, v dôsledku ktorej nemožno na požiadanie vykonať bezpečnú funkciu.

V prípade nepretržitej prevádzky ide o pravdepodobnosť poruchy za jednotku času alebo intenzitu porúch, typicky počet porúch za rok (Tabuľka 1). Dôležité je podotknúť, že SIL je navrhovaná pre bezpečnostnú funkciu, nie pre zariadenie či systém.

3.1.3 Štandardizačný rámec pre bezpečnostne - kritické systémy

Medzinárodný štandardizačný proces pre oblasť bezpečných riadiacich systémov je primárne vedený generickou normou IEC 61508 [24], ktorá vychádza z pojmu celkový životný cyklus bezpečnosti. Používa tento cyklus ako pracovný rámec pre činnosti nevyhnutné na zaistenie funkčnej bezpečnosti E/E/PE bezpečnostne kritických systémov. Pokrýva tak všetky činnosti od počiatočného konceptu, cez analýzu nebezpečenstiev a posúdenie rizík, vývoj bezpečnostných požiadaviek, špecifikáciu, návrh a implementáciu, prevádzku a údržbu, modifikáciu, finálne uvedenie do prevádzky až po vyradenie z nej. Technické požiadavky sa stanovujú v poradí určenom jednotlivými fázami celkového životného cyklu bezpečnosti systému. Štandard tiež špecifikuje techniky a opatrenia na dosiahnutie požadovanej integrity bezpečnosti. Vychádza z modelu ukázaného na (Obr. 3-4), v ktorom sú uvažované dve skupiny, resp. dva typy systémov:

- riadené zariadenie (Equipment Under Control, EUC), ktoré realizuje daný proces; môže ísť o kompletný proces alebo výrobné zariadenie, môže sa však jednať aj o relatívne malé zariadenie ako napr. domáci spotrebič alebo automobilovú súčiastku;
- riadiace systémy (Control Systems) a ochranné systémy (Protection Systems), ktoré implementujú bezpečnostné funkcie potrebné na zaistenie toho, že riadené zariadenie je primerane bezpečné, s EUC komunikujú pomocou snímačov a akčných členov používaných na monitorovanie a na riadenie určitých parametrov/nastavení.



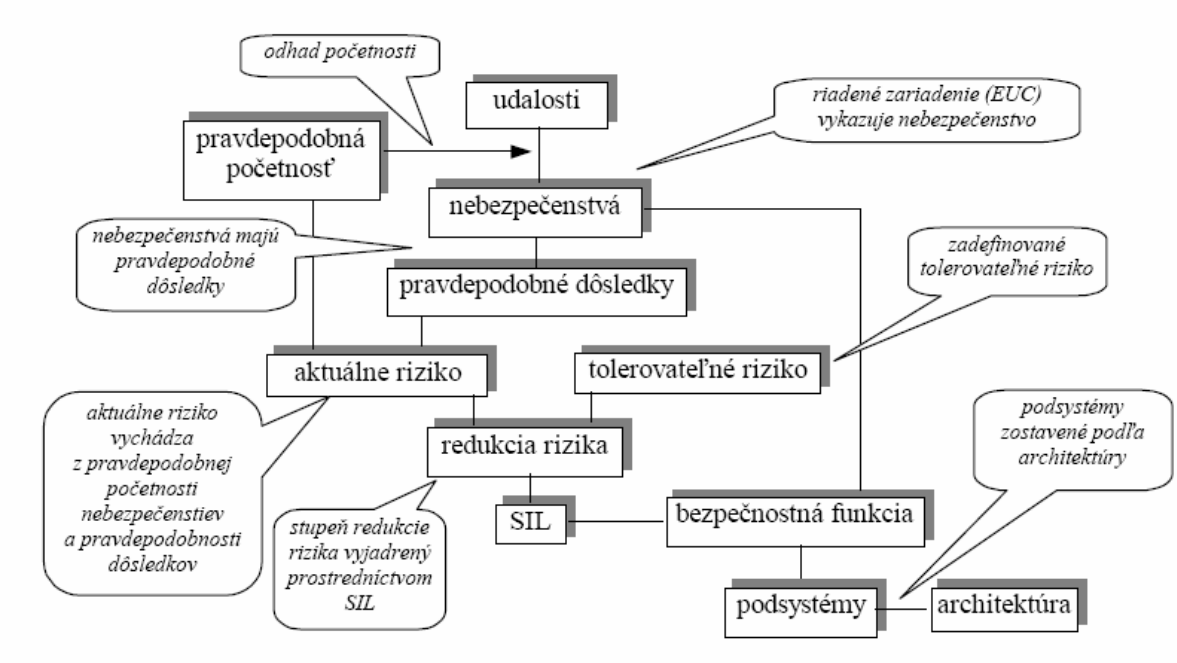
Obr. 3-4 Riadiaci a ochranný systém a riadené zariadenie

Základným cieľom je dosiahnutie a udržanie bezpečného stavu riadeného zariadenia. V tomto kontexte môžeme na riadiaci systém nazerať ako na systém, ktorý „spôsobuje“ požadovanú činnosť riadeného zariadenia. Ochranný systém je naopak systém, ktorý reaguje na nežiadúcu

situáciu, keď sa fungovanie riadeného zariadenia dostane do rozporu s požadovaným správaním. V mnohých prípadoch má akcia ochranného systému podobu vypnutia/odstavenia riadeného zariadenia. V norme IEC 61511 sa ochranný systém objavuje pod názvom Safety Instrumented System, SIS (v literatúre tiež ako Shutdown Systems, Interlock Systems, Permissive System a pod.). Bezpečnostná funkcia (Safety Instrumented Function, SIF) je potom definovaná ako funkcia realizovaná systémom SIS, ktorý má dosiahnuť alebo udržať bezpečný stav procesu so zreteľom na konkrétnu nebezpečnú udalosť.

Myšlienkový model normy [24] je naznačený na Obr. 3-5.

Vo vzťahu k bezpečnosti možno taktiež spomenúť normu EN 61511 [25], ktorá sa zaoberá funkčnou bezpečnosťou spojitých technologických procesov, normu EN 62061 [26] určenú pre oblasť strojov a mnohé ďalšie aplikačné normy odvodené od pôvodného generického štandardu IEC 61508 (napr. STN IEC 61513 pre oblasť jadrových elektrární, STN EN 50129 pre aplikácie v doprave a pod.).



Obr. 3-5 Myšlienkový model IEC 61508

V iných riadiacich systémoch sa prihliada na vývojové smernice pre softvér, ktoré sledujú obdobný prístup ako IEC 61508 v tom, že používajú koncept bezpečného životného cyklu, úrovne integrity bezpečnosti a pod. Sú zamerané predovšetkým na automobilový priemysel, v ktorom výrazným spôsobom narastá zastúpenie E/E/PE systémov, pričom sa očakáva, že

automobily budú bezpečné a elektronika v nich nepredstavuje nejaké riziko. Technika na výber SIL bola prebratá z projektu DRIVE venovaného dopravným telematickým systémom.

Tabuľka 2 kategorizácia podľa [27]

Kategória riaditeľnosti	Prijateľná intenzita porúch	Úroveň integrity
Uncontrollable	Extrémne nepravdepodobná	4
Difficult to control	Veľmi nepatrná	3
Debilitating	Nepatrná	2
Distracting	Nepravdepodobná	1
Nuisance only	Dosť nemožná	0

Každé nebezpečenstvo je posúdené z hľadiska stupňa zvládnutia bezpečnosti situácie, ktorá nastane po výskyte poruchy – vyberie sa jedna z kategórií riaditeľnosti (Tab. 2), čo definuje SIL spolu s prijateľnou intenzitou porúch: SIL 4 sa dotýka porúch, ktorých účinky nie sú posádkou vozidla zvládnuteľné a ktorých následky budú s vysokou pravdepodobnosťou extrémne závažné a reakcia ľudí im nedokáže zabrániť; SIL 3 sa dotýka porúch, ktorých účinky normálne nie sú posádkou vozidla zvládnuteľné, za priaznivých okolností a vďaka správnej reakcii ľudí by však mohli byť, zväčša však vedú k závažným dôsledkom; SIL 2 sa dotýka porúch, ktorých účinky sú zvyčajne zvládnuteľné rozumnou reakciou ľudí a ktoré (napriek zníženej miere bezpečnosti) možno očakávať, že v najhoršom prípade skončia vážne; SIL 1 sa dotýka porúch, ktoré vedú k prevádzkovým obmedzeniam, avšak správna reakcia ľudí obmedzí ich dopad na nepatrné dôsledky. Na rozdiel od IEC 61508, smernica udáva aj SIL 0, ktorá sa vzťahuje na poruchy, ktoré normálne neovplyvňujú bezpečnosť a kde spokojnosť zákazníka stojí v centre záujmu. Pri výbere vhodnej kategórie sa zvažujú rôzne faktory – všeobecné aj veľmi špecifické (stabilita vozidla, riaditeľnosť zrýchlenia, brzdenie, zníženie viditeľnosti atď.).

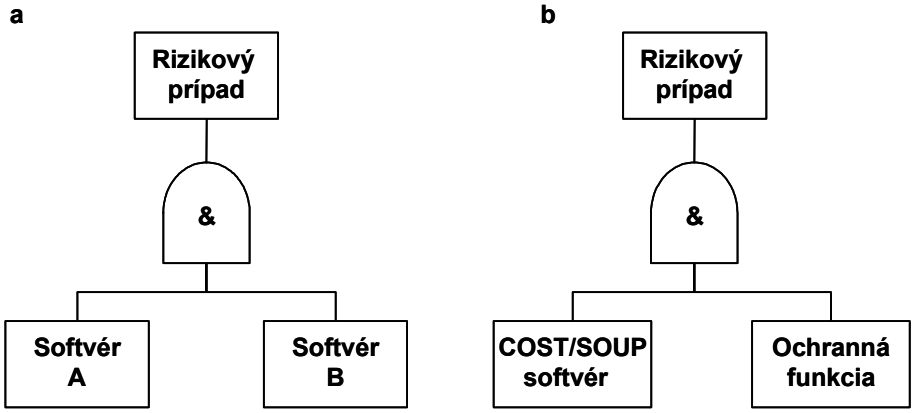
V bezpečnostne kritických systémoch je požadovaná vysoká kvalita. Výnimočnosť bezpečnostne kritických systémov je v tom, že návrh obyčajne zahŕňa hardwarovú redundanciu, niektoré druhy softvérovej redundancie, softvérová odolnosť proti poruchám a kvalitný, samostatne riadený, diagnostický softvér. Systém musí byť analyzovaný jedným, alebo viacerými všeobecne uznávanými rizikovo analytickými metódami, aby sme preverili dostatočnosť redundancie a diagnostiky. Jednou z metód na získanie určitých bezpečnostne kritických funkcií je monitorovací systém [28].

Je rozdiel medzi bezpečnostnými systémami, ktoré majú bezpečný stav, napr. automobilový priemysel kde proces môže byť zastavený resp. spomalený a medzi bezpečnostnými systémami s nulovým bezpečným stavom, napr. letectvo.

Bezpečnosť systému závisí od spoľahlivosti a funkčnosti, pričom sa zabezpečuje, že systém nevstupuje do nebezpečného stavu. Hodnoty systému sa musia nastaviť tak, aby v krízových situáciách, kde je ohrozený život, prostredie alebo zariadenie, nedošlo k poškodeniu resp. ohrozeniu.

Jedným z dôležitých spôsobov ako zvýšiť spoľahlivosť, je redundancia. Toto je tradičný spôsob ako zvýšiť spoľahlivosť hardvéru.

Požiadavka na bezpečnostne kritický systém často zahŕňa rôznorodosť funkcií. Môže to byť vo forme odlišného kódu realizácie alebo vo forme manipulácie s COTS (štandardný softvér Commercial Of The Shelf), SOUP (pochybný softvér Software Of Uncertain Pedigree) s ochrannou funkciou ako je zakreslené v strome chýb na obrázku (Obr. 3-6).



Obr. 3-6 Požiadavky odlišných štruktúr v bezpečnostne kritických systémoch, a) úplný redundantný systém, b) s ochrannou funkciou na funkčný kód, eventuálne typ COTS.

Hlavnou požiadavkou systému je v skutočnosti funkčnosť softvérovej verzie uvedenej na obrázku 4-6 (a) alebo funkčnosť COTS na obrázku 4-6 (b) [29]

3.1.4 Celkový životný cyklus bezpečnosti

Súčasné riadiace systémy sú spravidla budované ako distribuované riadiace systémy s niekoľkoúrovňovou hierarchickou štruktúrou. Najnižšia, prevádzková úroveň zabezpečuje priame napojenie riadiaceho systému na technologický proces. Ako technické prostriedky sa používajú programovateľné elektronické zariadenia - priemyselné regulátory a programovateľné automaty (PLC). V niektorých úlohách sa vyžaduje, aby okrem štandardných

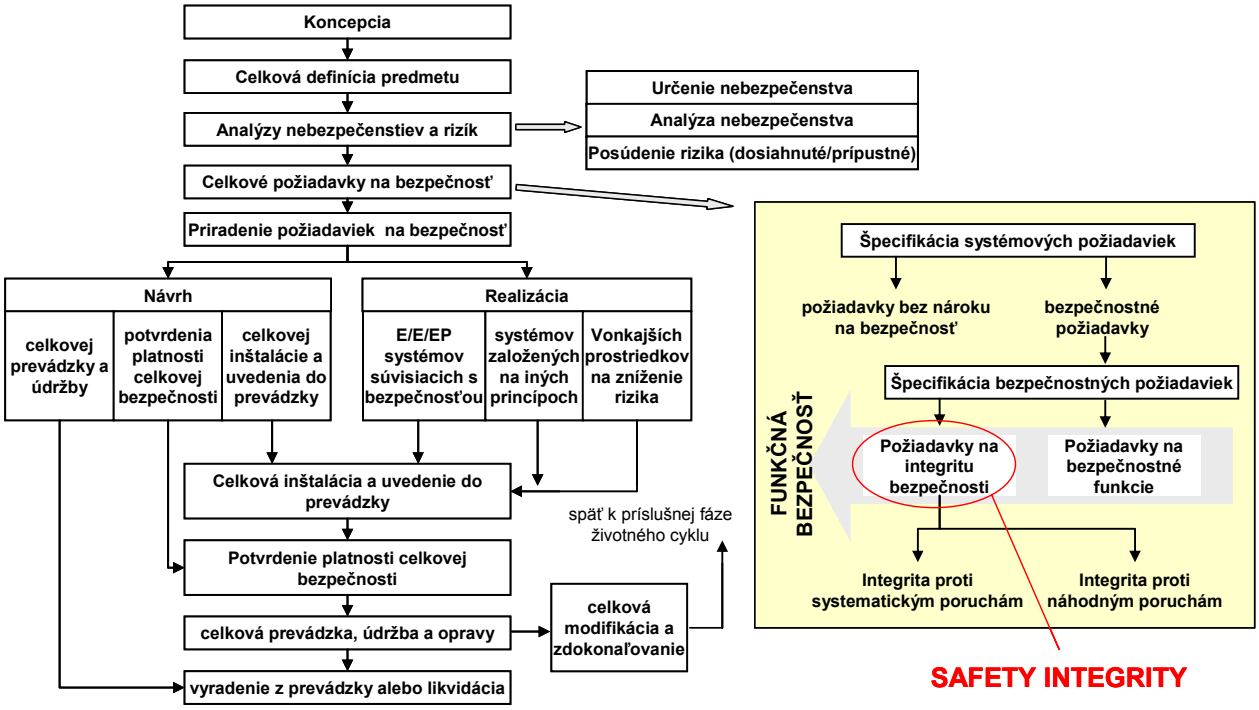
funkcií riadiaceho systému, ako sú napr. zber a prvotné spracovanie údajov, monitorovanie riadeného procesu, spracovanie alarmov, výpočet a vykonávanie akčných zásahov atd., systém poskytoval dostatočnú úroveň komplexnej bezpečnosti. V takom prípade sa hovorí o funkčnej bezpečnosti riadiaceho systému.

Medzinárodná norma IEC 61508 [24]

Funkčná bezpečnosť elektrických/elektronických/programovateľných elektronických bezpečnostných systémov podrobne stanovuje obecný prístup pre celý životný cyklus bezpečnosti systémov, ktoré obsahujú elektrické, elektronické a programovateľné elektronické (E/E/PES) časti využívané na zabezpečenie bezpečnostných funkcií riadiaceho systému. Norma obsahuje tieto časti:

- Všeobecné požiadavky,
- Požiadavky na E/E/PES systémy súvisiace s bezpečnosťou,
- Požiadavky na softvér,
- Definície a skratky,
- Príklady metód určovania úrovní integrity bezpečnosti (SIL),
- Metodické pokyny pre použitie IEC 61508-2 a IEC 61508-3,
- Prehľad postupov a opatrení.

Norma IEC 61508 uvažuje všetky dôležité fázy životného cyklu celkovej bezpečnosti, bezpečnosti E/E/PES a bezpečnosti softvéru (počínajúc koncepciou, cez návrh, realizáciu, prevádzku a údržbu až po vyradenie z prevádzky) pri používaní E/E/PES pre plnenie bezpečnostných funkcií. Poskytuje metodiku pre vypracovanie špecifikácie bezpečnostných požiadaviek potrebných pre dosiahnutie funkčnej bezpečnosti E/E/PES súvisiacich s bezpečnosťou a pre stanovenie celkovej úrovne integrity bezpečnosti pre bezpečnostné funkcie realizované E/E/PES súvisiace s bezpečnosťou používanou na úrovni bezpečnostnej integrity. Pre stanovenie úrovne komplexnej bezpečnosti používa metódy založené na analýze rizika. Norma ďalej stanovuje číselné hodnoty výslednej miery porúch pre E/E/PES súvisiace s bezpečnosťou, viazané na jednotlivé úrovne bezpečnostnej integrity. Používa model životného cyklu celkovej bezpečnosti pre systematické vykonávanie všetkých činností, ktoré sú potrebné pre zaistenie funkčnej bezpečnosti E/E/PES súvisiacich s bezpečnosťou.



Obr. 3-7 Celkový životný cyklus bezpečnosti.

Celkový životný cyklus bezpečnosti E/E//PES je prehľadne znázornený na Obr. 3-7. Uvedený životný cyklus funkčnej bezpečnosti sa odporúča používať ako základ pri uplatňovaní zhody s touto normou. Naproti tomu však, za predpokladu splnenia cieľov a požiadaviek všetkých častí tejto normy, sa môže použiť aj iný životný cyklus, ako je na Obr. 3-7. Organizácie alebo jednotlivci, ktorí majú celkovú zodpovednosť za jednu alebo niekoľko fáz životného cyklu celkovej bezpečnosti, bezpečnosti E/E/PES alebo bezpečnosti softvéru, stanovujú, pokiaľ ide o tieto fázy, za ktoré majú celkovú zodpovednosť, všetky činnosti manažmentu a technické činnosti nutné k tomu, aby E/E/PES súvisiace s bezpečnosťou dosiahli a udržali svoju požadovanú funkčnú bezpečnosť.

IEC 61511 – stručný prehľad

Norma IEC 61511 [25] Funkčná bezpečnosť. Bezpečnostné riadiace systémy spojitých technologických procesov je zameraná na implementáciu životného cyklu bezpečnosti procesných riadiacich systémov, kde technologické veličiny majú prevažne spojitý charakter a aj riadenie je spojitého charakteru (nie logické riadenie). Má tieto časti:

- Požiadavky na systémy hardvéru a softvéru, štruktúra, definície,
- Metodický pokyn pre používanie IEC 61511-1,

- Pokyny pre stanovenie požadovanej celkovej úrovne bezpečnosti.

Norma prezentuje systematickú metódu na vypracovanie všetkých postupov týkajúcich sa rizika. Špeciálny dôraz kladie na dizajn a potvrdenie platnosti systémov týkajúcich sa bezpečnosti. Základom normy je riadenie a funkčná bezpečnosť. Stratégia na dosiahnutie bezpečnosti by mala byť opodstatnená a mali by byť stanovené všetky činnosti, vrátane spôsobu hodnotenia ich dosiahnutia. Toto by malo byť časťou manažmentu funkčnej bezpečnosti.

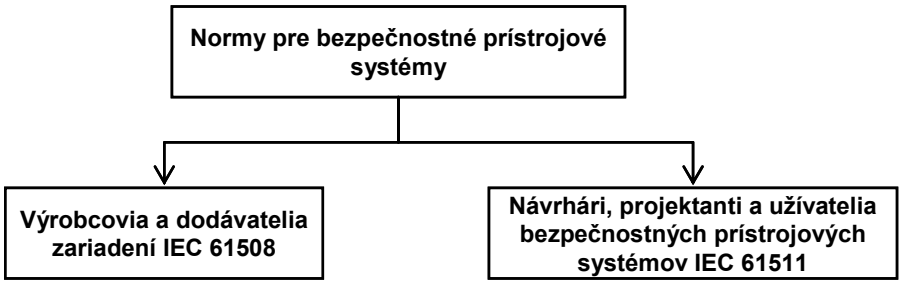
Z tohto dôvodu norma určuje bezpečnostný životný cyklus, ktorý istí všetky fázy životného cyklu samotného systému. Životný cyklus bezpečnosti zahrnuje činnosti súvisiace s prístrojovou bezpečnosťou, ktoré sú riadené všetkými zúčastnenými, ako sú inžinierski pracovníci, dodávatelia, integrátori a koneční užívatelia. Všetci musia zavádzať manažérsky systém funkčnej bezpečnosti v časti životného cyklu systému, ktorá spadá do ich kompetencie, a musia medzi sebou úzko spolupracovať, aby dosiahli očakávanú úroveň celkovej bezpečnosti počas jeho životnosti. Norma platí pre bezpečnostné prístrojové systémy založené na E/E/PES. Základné princípy tejto normy, ktorá bola vytvorená aj v nadväznosti na IEC 61508 do oblasti priemyselných procesov, sa však môžu použiť taktiež pre senzory, snímače a koncové členy bezpečnostných prístrojových systémov bez ohľadu na použitú techniku.

Norma vyžaduje zistenie všetkých bezpečnostných požiadaviek, aby boli posúdené nebezpečenstvá a riziká, vyžaduje, aby k bezpečnostným prístrojovým systémom boli pridelené bezpečnostné požiadavky, podrobne uvádza použitie niektorých činností v rámci manažmentu bezpečnosti, ktoré sa môžu použiť u všetkých metód funkčnej bezpečnosti, stanovuje požiadavky na architektúru systémov a konfiguráciu hardvéru, na aplikačný softvér a na integráciu systémov, na aplikačný softvér pre užívateľov a tvorcov softvérových bezpečnostných prístrojových systémov a obzvlášť špecifikuje:

- požiadavky na fázy životného cyklu bezpečnosti a činnosti, ktoré sa uplatňujú po čas návrhu a vývoja aplikačného softvéru obsahujú požiadavky na použitie opatrení a techník dovoľujúcich zabrániť chybám a kontrolovať vznik možných porúch,
- informácie o validácii bezpečnosti softvéru,
- informácie potrebné pre používateľa počas prevádzky a údržby.

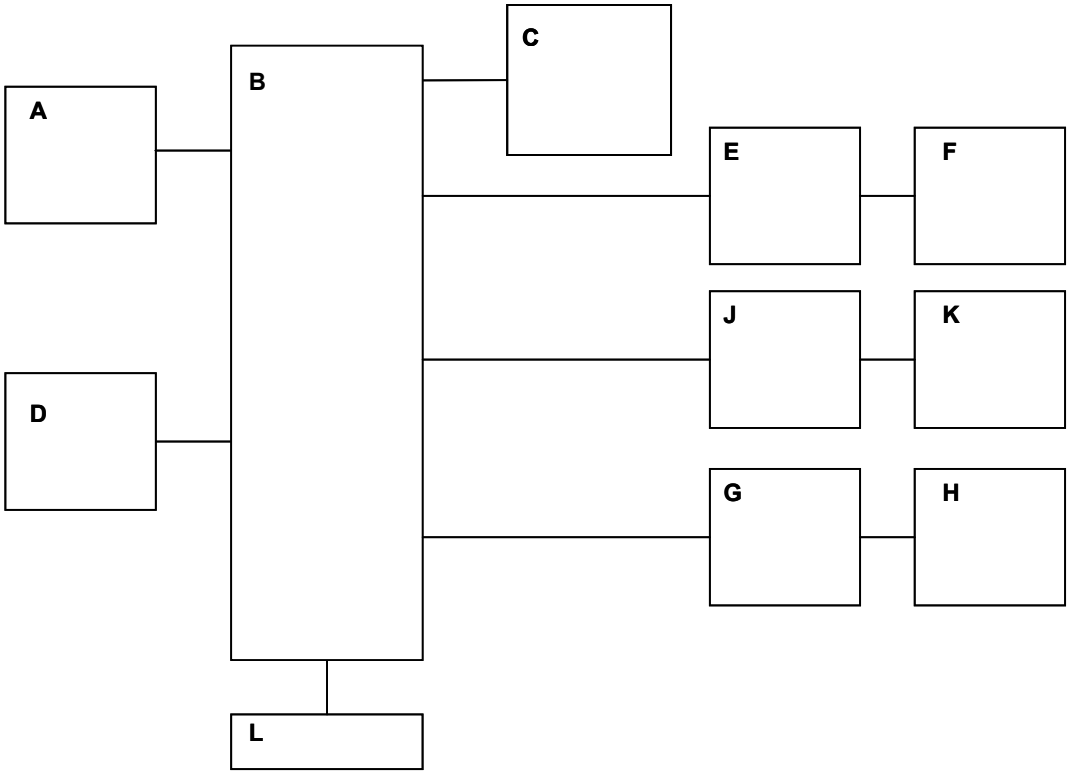
Ďalej norma uvádza zoznam činností potrebných pre stanovenie funkčných požiadaviek a požiadaviek na integritu bezpečnosti pre bezpečnostné prístrojové systémy. Platí pre všetky fázy životného cyklu bezpečnosti, od začiatočného návrhu, cez implementáciu, prevádzku a údržbu až po vyradenie z prevádzky. Norma tiež stanovuje vzťah medzi IEC 61508 a IEC 61511.

Oblasť použitia IEC 61508 a IEC 61511 v rámci noriem pre bezpečnostné prístrojové systémy je uvedená na Obr. 3-8



Obr. 3-8 Oblasť použitia noriem.

4 Technické prostriedky požiarnych systémov



Obr. 4-1 Príklad znázorňujúci dielce a časti tvoriace zariadenie elektrickej požiarnej signalizácie.

Hlásič požiaru A dielec zariadenia elektrickej požiarnej signalizácie, ktorý obsahuje najmenej jeden snímač monitorujúci trvalo, alebo v časových intervaloch aspoň jeden fyzikálny alebo chemický jav súvisiaci s požiarom. Pritom zabezpečuje do ústredne elektrickej požiarnej signalizácie aspoň jeden zodpovedajúci signál (B).

Hlásiče požiaru možno rozlišovať rôznymi spôsobmi.

tepelný hlásič	hlásič reagujúci na zvýšenie teploty	
dymový hlásič	hlásič citlivý na častícové produkty horenia a/alebo pyrolýzy, ktoré sú rozptýlené v atmosfére (aerosóly)	
	ionizačný dymový hlásič	hlásič citlivý na produkty horenia, ktoré ovplyvňujú ionizačné prúdy vnútri hlásiča
	optický dymový hlásič	hlásič citlivý na produkty horenia, ktoré ovplyvňujú absorbovanie alebo rozptyľovanie vyžarovania v infračervenej, viditeľnej alebo ultrafialovej oblasti elektromagnetického spektra
	plynový hlásič	hlásič citlivý na plynné produkty horenia a/alebo tepelného rozkladu
	plameňový hlásič	hlásič reagujúci na vyžarovanie z plameňa pri požiari

	hlásič s viacerými snímačmi	hlásič reagujúci na viac ako jeden jav požiaru	
	statický hlásič	hlásič reagujúci, na prekročenie hodnoty meraného javu, stanovenej v dostatočne dlhom trvaní	
	diferenčný hlásič	hlásič reagujúci, keď rozdiel (spravidla malý) hodnôt meraného javu na dvoch alebo viacerých miestach prekračuje stanovenú hodnotu v dostatočne dlhom trvaní	
	dynamický hlásič	hlásič reagujúci, keď rýchlosť zmeny meraného javu prekračuje stanovenú hodnotu v dostatočne dlhom trvaní	
	bodový hlásič	hlásič reagujúci na jav snímaný v blízkosti jedného pevného bodu	
	viacbodový hlásič	hlásič reagujúci na jav snímaný v blízkosti viacerých pevných bodov	
	líniový hlásič	hlásič reagujúci na jav snímaný v blízkosti jednej spojitej rovnej čiary	
	nulovateľný (resetovateľný) hlásič	hlásič, ktorý po reagovaní možno uviesť zo stavu signalizovania do základného stavu, v ktorom je pripravený reagovať, ak už netrvajú podmienky, ktoré spôsobili reakciu bez výmeny akejkoľvek súčiastky	
		samočinne nulovateľný hlásič	nulovateľný (resetovateľný) hlásič, ktorý sa automaticky uvedie do základného stavu pohotovosti snímania
		diaľkovo nulovateľný hlásič	nulovateľný (resetovateľný) hlásič, ktorý možno uviesť do základného stavu pohotovosti snímania operáciou vykonávanou vzdialene od hlásiča
		miestne nulovateľný hlásič	nulovateľný (resetovateľný) hlásič, ktorý možno uviesť do základného stavu pohotovosti snímania ručnou operáciou vykonávanou na hlásiči
		nenulovateľný hlásič (s vymeniteľnými súčiastkami)	hlásič, ktorý po reagovaní vyžaduje výmenu súčiastky alebo súčiastok na uvedenie do základného stavu pohotovosti snímania
		nenulovateľný hlásič (bez vymeniteľných súčiastok)	hlásič, ktorý po reagovaní nemožno uviesť zo stavu poplachového signalizovania do základného stavu pohotovosti snímania
		odnímateľný hlásič	hlásič skonštruovaný tak. aby ho bolo možné ľahko odstrániť zo zvyčajnej prevádzkovej polohy na účely údržby a opravy
		neodnímateľný hlásič	hlásič s takým montážnym usporiadaním, že nie je možné jeho ľahké odstránenie na účely údržby a opravy
		dvojstavový hlásič	hlásič poskytujúci jeden z dvoch výstupných stavov vzťahujúcich sa buď

			na základný stav. alebo na stav signalizovania požiaru
		viacstavový hlásič	hlásič poskytujúci jeden z obmedzeného počtu (väčšieho ako 2) výstupných stavov vzťahujúcich sa na základný stav, stav signalizovania požiaru a na iné špecifické podmienky
		analógový hlásič	hlásič poskytujúci výstupný signál, ktorý' predstavuje hodnotu snímaného javu

Ústredňa elektrickej požiarnej signalizácie (písmeno B na Obr. 4-1): časť zariadenia elektrickej požiarnej signalizácie, cez ktorú možno napájať ostatné časti a ktorá:

a) sa používa na:

- príjem signálov z pripojených hlásičov;
- určovanie, či tieto signály zodpovedajú stavu signalizovania požiaru;
- akustické a optické indikovanie každého takého stavu signalizovania požiaru:
  - indikovanie nebezpečného miesta;
  - možné zaznamenanie každej takej informácie:

b) sa používa na sledovanie správnej funkčnosti zariadenia a poskytovanie akustického a optického signalizovania každej poruchy (napríklad skrat, prerušenie vedenia alebo porucha dodávky energie):

c) ak sa to požaduje, umožní vyslanie signálu požiarnej signalizácie, napríklad:

- do zariadení akustického alebo optického signalizovania požiaru:
- cez zariadenie prenosu požiarnej signalizácie na jednotku požiarnej ochrany;
- cez ovládanie automatických zariadení požiarnej ochrany na automatické hasiace zariadenia.

Zariadenie požiarnej poplachovej signalizácie (písmeno C na Obr. 4-1): dielec zariadenia signalizácie požiaru, ktorý nie je súčasťou ústredne elektrickej požiarnej signalizácie. Používa sa na výstražné signalizovanie požiaru, napríklad akustické alebo optické signalizačné zariadenie

Tlačidlový hlásič požiaru (písmeno D na Obr. 4-1): dielec zariadenia elektrickej požiarnej signalizácie, ktorý sa používa na ručné signalizovanie požiaru

Zariadenie na prenos požiarnej signalizácie (písmeno E na Obr. 4-1): zariadenie, ktoré prenáša signál požiarnej signalizácie z ústredne elektrickej požiarnej signalizácie do ohlasovne požiaru.

Ohlasovňa požiaru (písmeno F na Obr. 4-1): centrála, z ktorej možno trvalo iniciovať potrebné opatrenia požiarnej ochrany a hasenia požiarov

Ovládanie automatického zariadenia požiarnej ochrany (písmeno G na Obr. 4-1): automatické zariadenie používané na spustenie automatického zariadenia požiarnej ochrany po prijatí signálu z ústredne elektrickej požiarnej signalizácie.

Automatické zariadenie požiarnej ochrany (písmeno H na Obr. 4-1): automatické zariadenie zabraňujúce šíreniu požiaru, alebo automatické hasiace zariadenie, napríklad stabilné hasiace zariadenie.

Zariadenie na prenos signalizácie poruchy (písmeno J na Obr. 4-1): zariadenie, ktoré prenáša výstražný signál poruchy z ústredne požiarnej signalizácie do príjmovej stanice hlásenia poruchy.

Príjmová stanica hlásenia poruchy (písmeno K na Obr. 4-1): ústredňa, z ktorej možno iniciovať opatrenia potrebné na odstránenie poruchy.

Zariadenie napájacieho zdroja (písmeno L na Obr. 4-1): časť zariadenia elektrickej požiarnej signalizácie, ktorá napája ústredňu elektrickej požiarnej signalizácie a tie časti, ktoré sú napájané z ústredne požiarnej signalizácie. Zariadenie napájacieho zdroja môže obsahovať viaceré zdroje energie (napríklad elektrická energia zo siete a z náhradných pohotovostných zdrojov).

Spájacie prvky: všetky prvky, ktoré tvoria spoje medzi rôznymi časťami zariadenia elektrickej požiarnej signalizácie.

Autonómna poplachová signalizácia dymu: jediná skrinka obsahujúca dymový hlásič, zdroj energie a prvky poplachovej signalizácie ktorá je určená na poplachové signalizovanie požiaru v bytových priestoroch. [30]

4.1 Náväznosť ovládacích zariadení

Systém EPS prostredníctvom vstupno-výstupných zariadení môže ovládať nasledovné systémy a zariadenia.

- systém požiarneho evakuačného rozhlasu (spúšťanie evakuačných a poplachových hlásení).
- systém odvodu tepla a splodín horenia, systém EPS vysiela informácie o požiarnom poplach,. zároveň ovláda otvorenie dverí slúžiacich na privetrávanie vzduchu.
- ovládanie blokovania chodu vzduchotechnických zariadení, prostredníctvom systému merania a regulácie, prípadne aj priamym ovládaním.
- vypínanie vybraných elektrických rozvodov s výnimkou rozvodov slúžiacich pre napájanie požiarnotechnických zariadení.
- blokovanie zvukových signalizačných zariadení systému EZS (ak sa v objekte nachádzajú).
- odblokovanie elektrických zámkov v prípade ich inštalácie.
- blokovanie chodu výťahov, resp. riadenie ich funkcie pri požiari.
- blokovanie prívodu plynu do budovy, privedením 24V DC do ventilu v regulačnej stanici plynu.

Zároveň môže systém EPS pre komplexnosť vyhodnotenia požiarnej situácie preberať prostredníctvom vstupno-výstupných modulov signály od iných zariadení:

- signály o činnosti a prevádzkovom stave systému stabilného hasiaceho zariadenia.
- signály o aktivácií zariadení pre odvod tepla a splodín horenia.
- signály o stave požiarnych klapiek systému VZT.

Technické prostriedky systémov protipožiarnej ochrany možno rozdeliť do dvoch základných skupín:

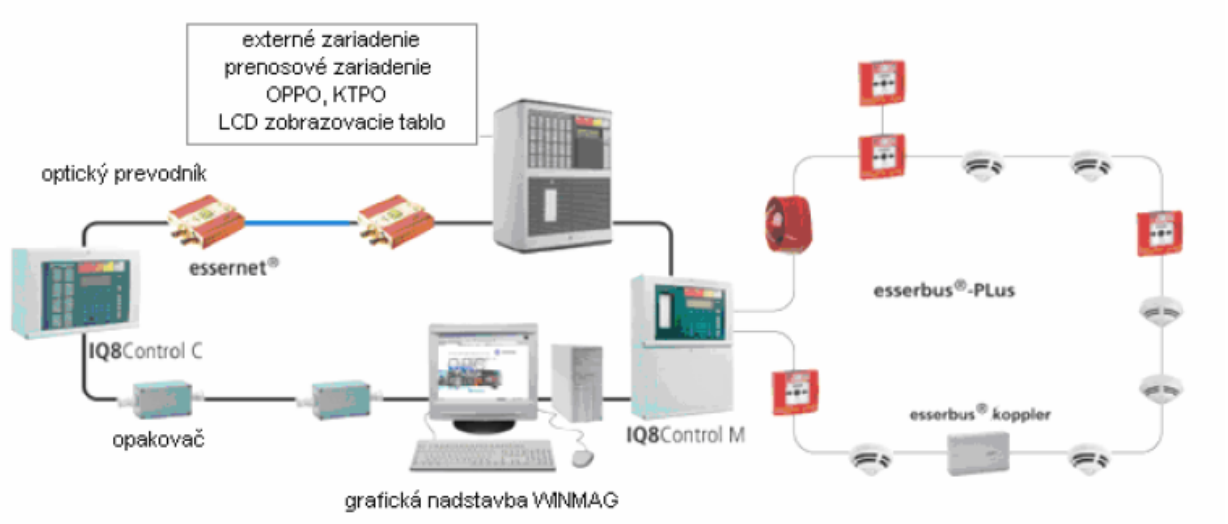
- Systémy ochrany a v časnej detekcie, kde patrí elektrická požiarna signalizácia a prípadne na ňu pripojené snímače ako periférna zariadenia,

- Systémy na hasenie a elimináciu rozsahu požiaru, kde patrí stabilné hasiace zariadenie, zariadenie na hasenie iskier v uzavretom priestore, zariadenie na hasenie požiaru, zariadenie na odvod tepla a dymu.

Ďalej sa v práci budem podrobnejšie zaoberať elektrickou požiarnou signalizáciu, kde som si vybral zariadenie od výrobcu Esser, ktoré z hľadiska štatistiky majú u nás najväčšie zastúpenie na trhu.

4.2 Elektrická požiarna signalizácia

Systém elektrickej požiarnej signalizácie je flexibilný požiarny systém zložený z jedného, alebo dvoch procesorov požiarnych ústrední. Počet a typ ústrední je možné zvoliť podľa veľkosti objektu a v prípade potreby jednotlivé ústredne prepojiť do siete, čo umožňuje jednoduché rozširovanie existujúcich inštalácií, ale tiež inštalovanie zložitých systémov pri zachovaní jednoduchého a prehľadného ovládania. K ústredniam možno pomocou vedenia pripojiť hlásiče a vstupno-výstupné prvky tzv. kopplery. Pomocou kopplerov je možné monitorovať a riadiť špeciálne hlásiče alebo ostatné zariadenia budovy. [31] Hlavnou funkciou požiarneho systému je včasná detekcia požiaru a riadení náväzných zariadení, tak aby bola zabezpečená ochrana zdravia, života osôb a minimalizácia škôd na majetku.



Obr. 4-2 Príklad zapojenia elektrickej požiarnej signalizácie

Systém elektrickej požiarnej signalizácie má všeobecne stále väčšiu dôležitosť. Preto je voľba správneho typu systému rozhodujúca pre minimalizáciu škôd pri prípadnom požiaru.

4.2.1 Ústredňa elektrickej požiarnej signalizácie

Obr. 4-3 Ústredňa elektrickej požiarnej signalizácie.

Hlavné časti ústredne:

a) základná doska,

b) zdrojová doska,

c) toroidný transformátor,

d) skrinka.

Ďalšia výbava:

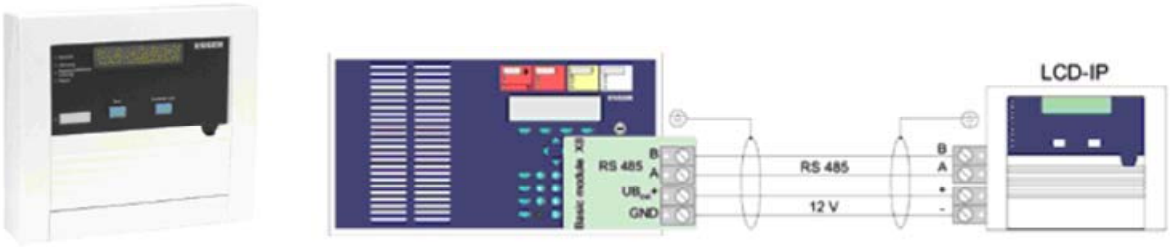
a) periférna karta,

b) Karta pre 3 mikromoduly

c) čelný ovládací panel v niekoľkými rôznymi prevedeniami (1/4 VGA, tlačiareň, GEA panel),

d) mikromoduly (IQ8control C max. 2 ks, IQ8control M max 7 ks).

4.2.2 Paralelné tablo

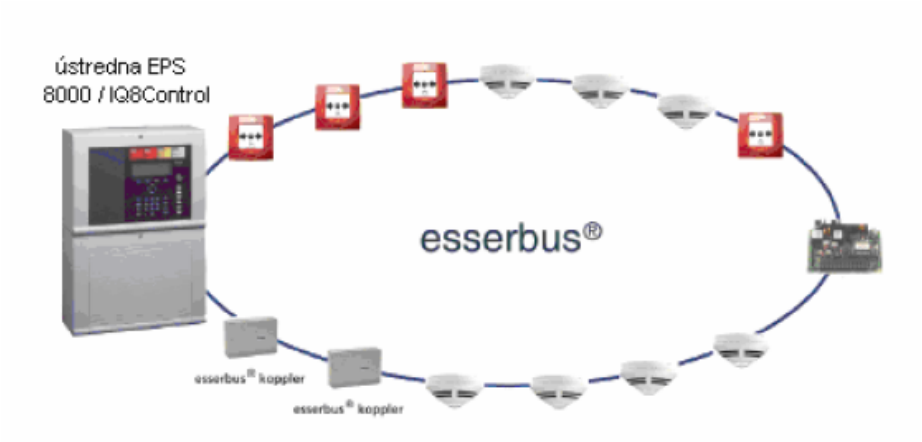


Obr. 4-4 Paralelné tablo elektrickej požiarnej signalizácie a jeho zapojenie.

K ústredniam možno pripojiť pomocou rozhrania RS485 do vzdialenosti až 1200m maximálne 31 zobrazovacích LCD tabiel. Každá ústredňa pripojená do siete Essernet môže byť pre ostatné ústredne v sieti ovládacím a zobrazovacím panelom.

4.2.3 Prvky pre zbernicu Esserbus a EsserbusPLus

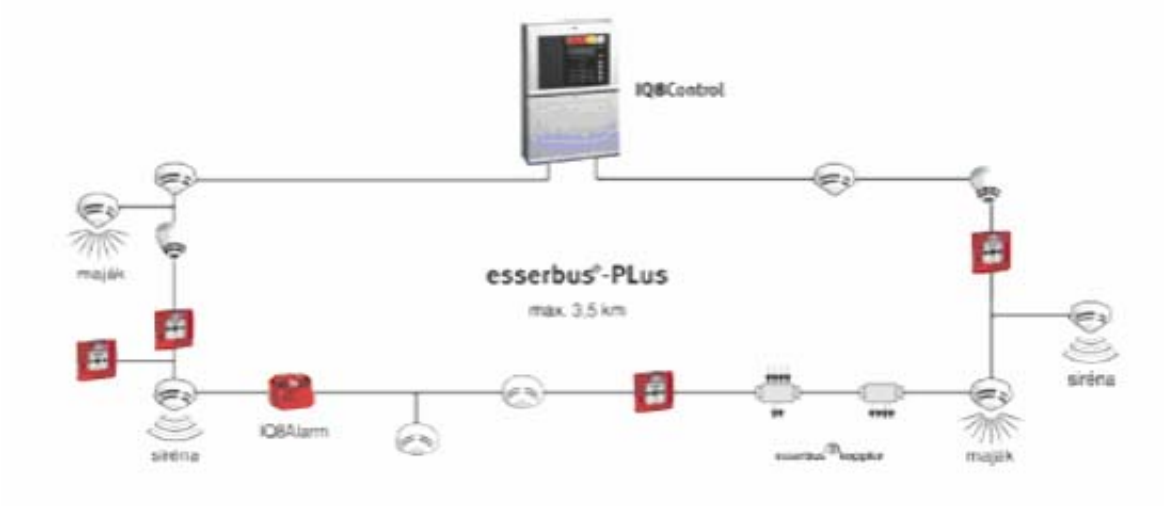
Pomocou mikromodulu Esserbus a EsserbusPLus sa k ústredne pripájajú hlásiče a ďalšie inteligentní prvky. Topológia dvoj-vodičového vedenia esserbus je kruhová s možností odbočiek bez použitia ďalšej elektroniky. Vedenie esserbus je odolné na skrat či prerušenie s celkovou dĺžkou 3.500 metrov. Počet účastníkov na tomto vedení je 127 individuálne adresných prvkov.



Obr. 4-5 Kruhová topológia vedenia Esserbus.

4.3 Hlásiče

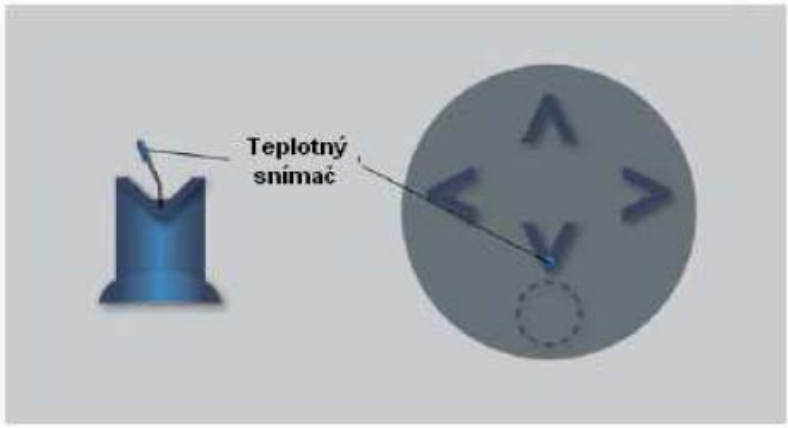
Hlásiče série 9200 boli v súčasnosti nahradené novou radou hlásičov IQ8Quad. Hlásiče ESSER série IQ8Quad sú 100 % kompatibilné s existujúcou radou 9200. Na jednom kruhovom vedení esserbus možno súčasne nainštalovať sériu 9200 aj hlásiče novej série IQ8Quad. Nové hlásiče majú moderný atraktívny design, používajú nový veľmi výkonný mikroprocesor a obsahujú štandardne oddeľovače. Použitím oddeľovačov v každom hlásiče so spojením s kruhovou topológiou vedenia Esserbus a EsserbusPLus, bolo dosiahnuté úplná odolnosť systému na skrat a prerušenie vedenia.



Obr. 4-6 Zapojenie hlásičov na kruhovú topológiu vedenia Esserbus.

Fyzikálne princípy zariadení na detekciu

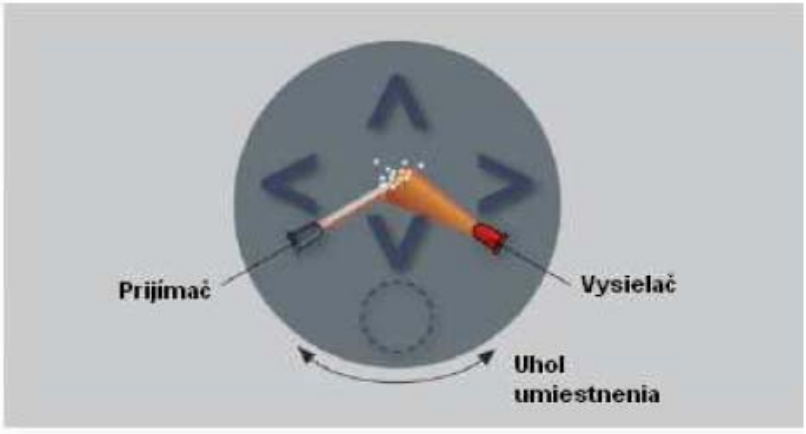
Princíp detekcie rozdielu teplôt a maximálnej teploty [31]



Obr. 4-7 Schéma tepelného snímača

Tepelné hlásiče sledujú zvýšenú teplotu, ktorá vzniká pri horení a zareagujú, keď teplota priestoru prekročí určitú medznú hodnotu (spravidla približne 60 °C), ale bo keď teplota okolitého prostredia počas určitého časového intervalu narastie nadpriemerné rýchle (vyhodnocovanie rozdielu teploty). Maximálna teplota detekcie hlásiča a teplota pri normálnom použití je určená podľa triedy tepelných hlásičov normy EN 54-5.

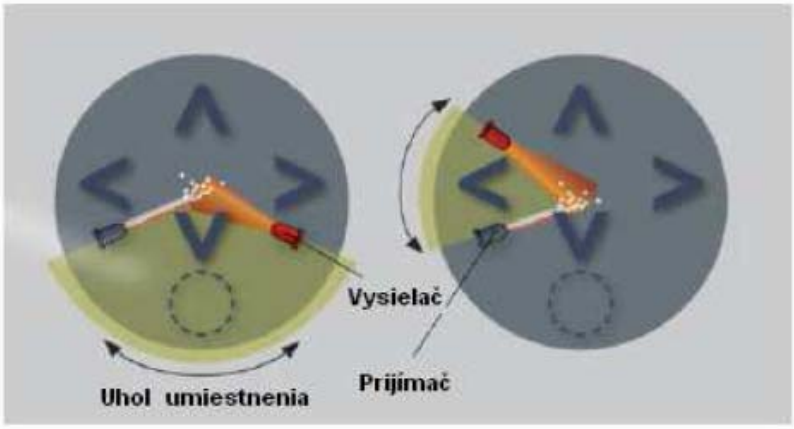
Optický princíp s infračerveným svetlom



Obr. 4-8 Schéma detekcie požiaru s infračerveným svetlom

Optické hlásiče dymu využívajú metódy rozptýleného svetla: LED dióda vysielača a foto-dióda prijímača sú navzájom umiestnené v určitom uhly. Pokiaľ viditeľné častice aerosoly požiaru preniknú do meracej komory, dôjde k rozptýlení časti svetelného lúču LED diódy vysielača a zvýšený signál je vyhodnocovaný v prijímači.

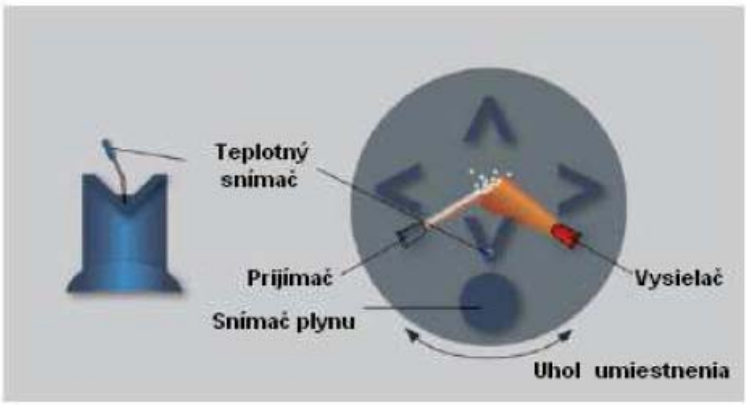
Optický princíp s dvomi uhlami



Obr. 4-9 Schéma detekcie požiaru s infračerveným svetlom pomocou dvoch uhlov

V porovnaní s tradičným hlásičom s metódou rozptyle svetla, hlásič O2T pracuje s metódou dvoch uhlov. Na základe toho je hlásič schopný odlíšiť rôzne častice dymu v meracej komore. Týmto spôsobom sú klamné veličiny spoľahlivo odlíšený od charakteristických veličín požiaru a v určitých medziach možno rozlišovať rôzne typy dymu.

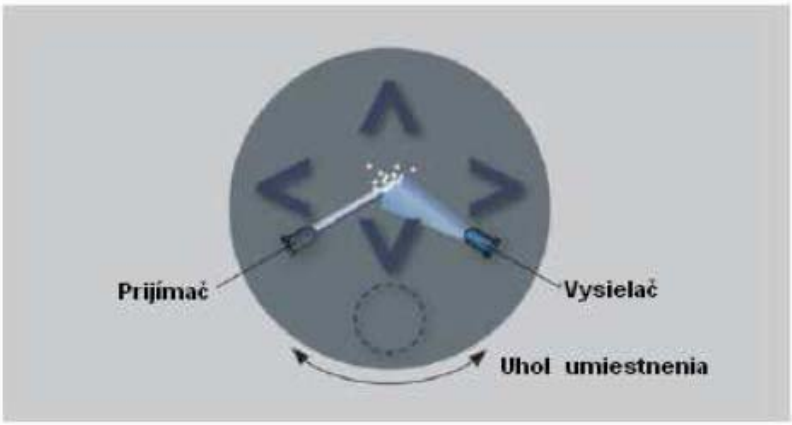
Detekcia plynu s detektorom CO



Obr. 4-10 Schéma detekcie požiaru s kombinovanou metódou a detektorom CO

Hlásič plynných splodín horenia detekuje požiar, keď koncentrácia (napr. CO) v priestore prekročí určitú hodnotu. U snímacích detektorov na tomto princípu sú plyny zo vzduchu okolitého prostredia chemicky viazaný na povrchovou plochu snímače. Pritom molekuly plynu odovzdávajú elektrické náboje, ktoré zvyšujú hodnotu vodivosti polovodiče. Pre spoľahlivú detekciu požiaru sa v jednom hlásiči kombinuje viac optimalizovaných snímacích detektorov.

Optický princíp s modrým svetlom

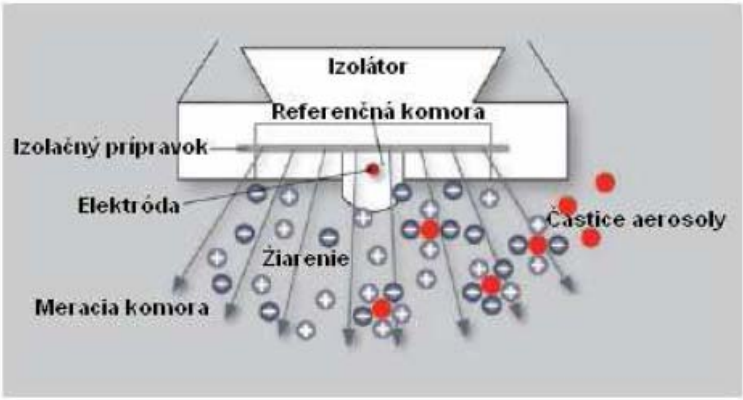


Obr. 4-11 Schéma detekcie požiaru s modrým svetlom

Miesto infračerveného svetla využíva hlásič s modrým svetlom modrou LED diódu. Krátka vlnová dĺžka svetla umožňuje detekciu tých najmenších častíc, ktoré až doposiaľ dokázali rozpoznať len ionizační hlásiče. Vďaka vyššej citlivosti prebieha detekcia celého spektra dymu: od neviditeľných až po veľké aerosoly. Hlásiče s modrým svetlom dnes nahradzujú väčšinou ionizačné hlásiče, pretože v porovnaní s ionizačnými hlásičmi pracujú bez rádioaktívneho zdroje.

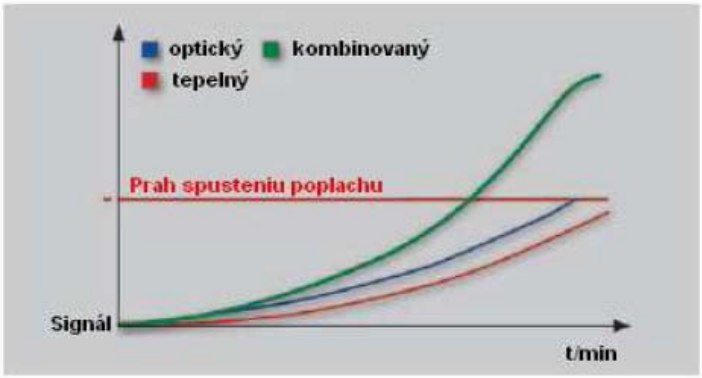
Ionizačný princíp

Ionizační hlásiče pracujú s rádioaktívnym zdrojom, ktorý generuje ióny medzi dvomi nabitými elektródami. Častice dymu zmenšujú prúd, ktorý preteká medzi elektródami, hlásič spustí poplach. Z dôvodu prítomnosti rádioaktívneho materiálu sa ionizačné hlásiče používajú už len v zvláštnych prípadoch. Dôvodom sú vysoké náklady na odbornou likvidáciu spracovania rádioaktívnych zdrojov.



Obr. 4-12 Schéma detekcie požiaru ionizačnou metódou

Bezpečnosť a spoľahlivosť s hlásičmi - IQ8Quad T, O & OT



Obr. 4-13 Graf včasnej detekcie požiaru hlásičmi

Prvky elektrickej požiarnej signalizácie

Hlásiče IQ8Quad

Okrem základných typov hlásičov O (opticko-dymový), TM/TD (termomaximálny /termodiferenciálny), 3D OT (multisenzorový opticko-dymový + teplotný) a O2T (multisenzorový dvojitý opticko-dymový + teplotní) sú v novej rade k dispozícii nové typy, a hoci OTG (multisenzorový opticko-dymový + teplotní + plyn CO) a OT Blue. [32]

Obr. 4-14 Rozdelenie a označenie hlásičov rady IQ8Quad

Obr. 4-15 Teplotný hlásič IQ8Quad

Tepelné hlásiče sa hodia do oblastí, v ktorých možno počítať s otvoreným a rýchle prebiehajúcim požiarom, pretože sú schopné detekovať zvýšenú teplotu, ale niekoľko dymov a plynné splodiny horenia vznikajúci pri požiari. V moderných budovách však kvôli použitiu rôznych stavebných materiálov, často vznikajú tlejúce požiare s intenzívnym vývojom dymu ešte predtým, než vypukne požiar s otvoreným ohňom. Tepelné hlásiče sa prevažne používajú k ochrane vecných hodnoť a nie sú vhodné k ochrane osôb. Človek v spánku by sa udusil plynovými splodinami horenia pri požiare skôr, ako by tepelný hlásič dokázal detekovať zvýšenou teplotu. Tieto hlásiče sú viditeľne odlíšiteľné od iných hlásičov čiernym prúžkom na spodnej časti hlásiča.

O hlásič IQ8Quad

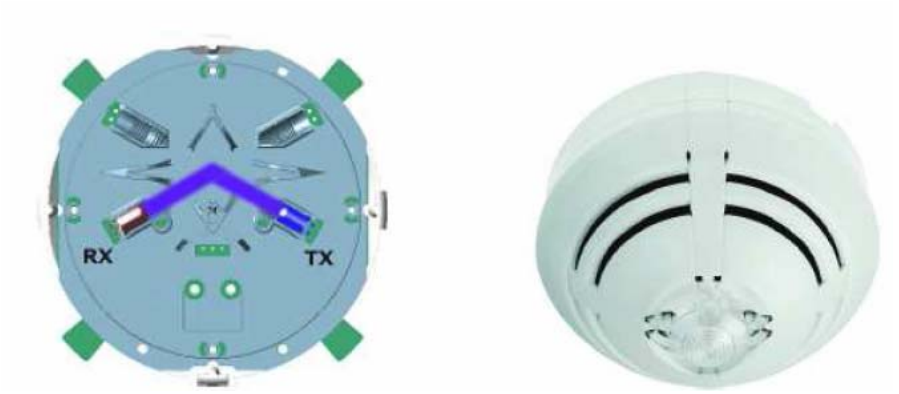
Optické hlásiče nedokážu detekovať neviditeľné častice aerosoly tak, jak vznikajú napr. pri otvorenom požiari dreva. Tento typ hlásičov sa používa hlavne tam, kde pri rozvoje požiaru počítať prevažne so “studeným” dymom (tlejúci dym požiaru).

OT hlásič IQ8Quad

Pri OT hlásiča je optický princíp detekcie spojený s princípom detekcie maximálnej teploty a rozdielu teploty. Prepojenie dát obidvoch častí hlásiča umožňuje spoľahlivú detekciu tlejúcich požiarov a požiarov s intenzívnym vývojom tepla. Týmto sa bezpečnosť a spoľahlivosť detekcie významnou mierou zlepšuje a odolnosť voči falošných poplachov sa výrazne znižuje. Samotný princíp detekcie často nestačí, napríklad kde sa pod jednou strechou skladuje tovar s rôznym požiarnym zaťažením, ako je: káblový materiál, textil, čistiace prostriedky a rozpúšťadlá. Tu sa ako optimálna ochrana osvedčuje princíp viacerých kritérií.

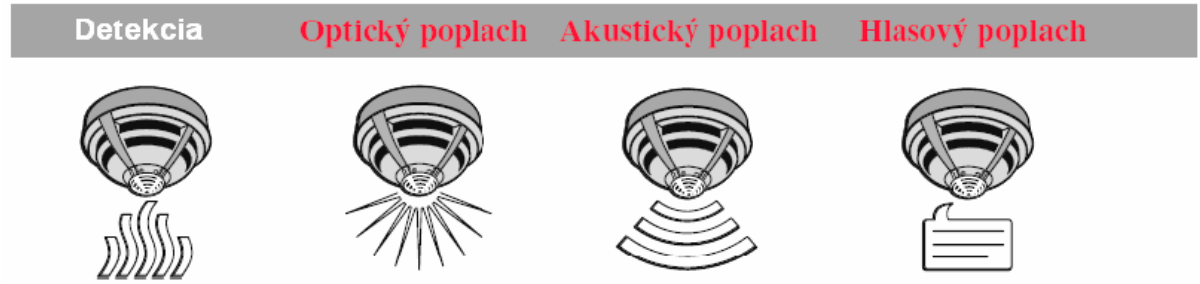
IQ8Quad – OT blue

Typ OT Blue používa novú technológiu detekcie. Výsledkom je podobná reakcia na požiar ako u ionizačného hlásiča, ale bez použitia rádioaktívneho preparátu. Detekuje veľmi malé častice dymu, ktoré boli doposiaľ možne detekovať iba ionizačným hlásičom, necitlivý voči prúdeniu vzduchu a agresívneho okolia. Výhodou hlásiča je schopnosť rýchla detekcia otvoreného ohňa a detekcie celého dymového spektra.



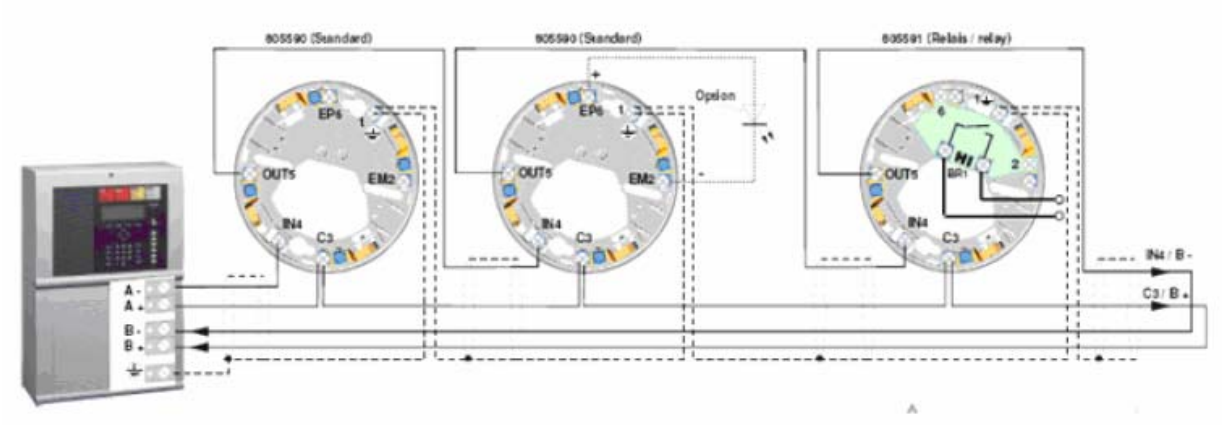
Obr. 4-16 Princíp OT blue hlásiča IQ8Quad a OT blue hlásič IQ8Quad

Hlásiče IQ8Quad s integrovanými signalizačnými prvkami



Obr. 4-17 Funkcie hlásiča IQ8Quad s integrovanými prvkami

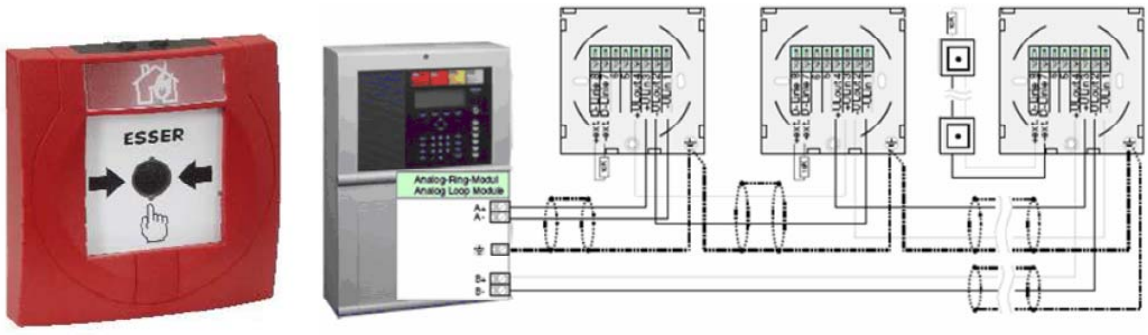
Hlásič IQ8Quad je navrhnutý tak aby zahrnul všetky signalizačné prvky. Existuje v rôznych vyhotoveniach podobne ako klasické IQ8Quad hlásiče. Znamená to že v hlásiči môže byť integrovaný maják, siréna, rečový modul, nebo kombinácia týchto signalizačných prvkov. Podobne ako hlásiče, sú i signalizačné prvky v hlásičoch napájané z vedení EsserbusPLus a nevyžadujú žiadne ďalšie napájanie. Aj keď hlásič môže mať až 4 funkcie, na vedení EsserbusPlus obsahuje iba jednu adresu pri uchovaní možnosti ovládať zvlášť hlásič, zvlášť optickú a zvlášť akustickou signalizáciu. Pri použití v každom hlásiči týchto prvkov a použitím kruhového vedenia je zaručená bezpečnejšia prevádzka hlásičov a hlavne signalizačných zariadení, než u bežne používaných signalizačných zariadení ovládaných výstupným relé.



Obr. 4-18 Zapojenie automatických hlásičov IQ8Quad kruhového vedenia Esserbus

Tlačidlový hlásič IQ8Quad

Nový dizajn a veľkosť tlačidlových hlásičov zabezpečuje neprehliadnutie ľuďmi v prípade požiaru. Pri každý únikovom východe musí byť umiestnený takýto hlásič. Ide o manuálny hlásič požiaru a nemôže byť v jednej skupine s automatickými hlásičmi. Všetky hlásiče od výrobcu Esser majú rovnaký kľúč, ktorým možno odistiť stlačení spínač, otestovať funkčnosť tlačidla a vymeniť rozbité sklo. Tlačidlo EPS ma krytie IP 54. No pre vonkajšie použitie sa vymení gumená manžeta čím tlačidlo získa krytie IP 55. Vrchné kryty tlačidla sú rôznych farieb. Podľa platnej legislatívy Slovenskej republiky pre hlásenie požiaru je dovolená červená farba. Iné farby sú dovolené použiť v prípadoch, keď signalizujeme technické alarmy. Napríklad zatopenie miestnosti, hasenie stabilným hasiacim zariadením a pod...



Obr. 4-19 Tlačidlový hlásič IQ8Quad a zapojenie manuálnych hlásičov do kruhového vedenia Esserbus

4.4 Kopplery

Kopplery sú vstupno-výstupné zariadenia, ktoré umožňujú monitorovať a ovládať rôzne zariadenia. Možno ich pripojiť na vedenie Esserbus a EsserbusPLus, potrebujú externé napájanie pre funkčnosť. Tieto kopplery sú umiestňované do plastových skriniek Esser.

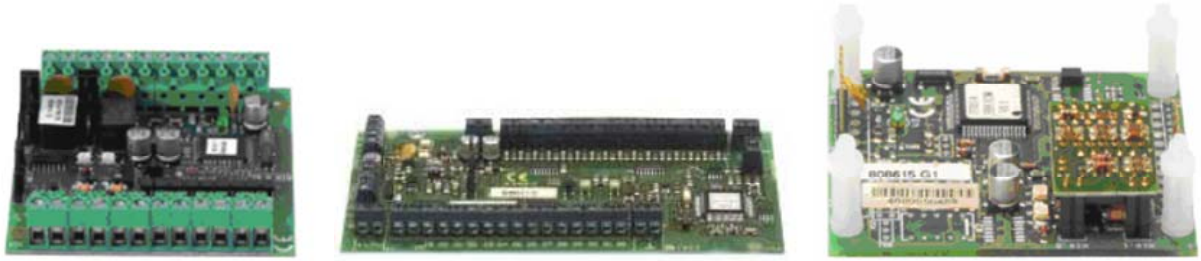
V súčasnej dobe je možné do systému použiť tieto kopplery: [32]

Koppler jednoskupinový – obsahuje jeden voľne programovateľným dvojito vyvážený vstup. Pre svoju funkciu musí byť externé napájaní.

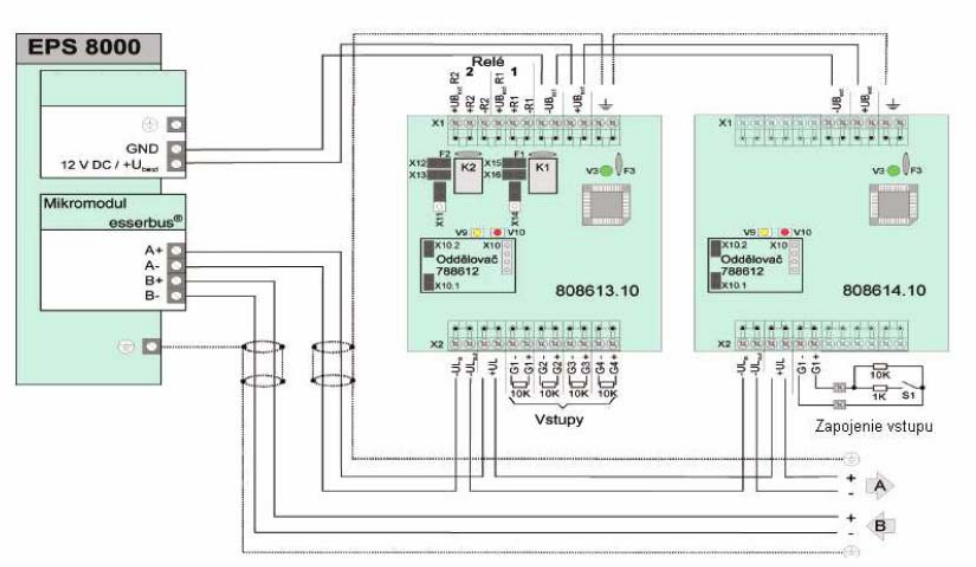
Koppler 4 skupiny/2 relé - obsahuje 4 voľne programovateľných dvojito vyvážených vstupov a 2 voľne programovateľnými reléovými výstupy s možnosťí pracovať v režimu monitorovaného vedení k ovládanému zariadeniu. Pre svoju funkciu musí byť taktiež externe napájaní.

Koppler 32 výstupov - obsahuje 32 voľne programovateľnými výstupy. Pre svoju funkciu nemusí byť externe napájaný. Ovládané zariadenie je nutné napájať.

Komunikačný Koppler – sa používa na prepojenie ústredne Esser 8010, ktorá ovláda riadenie stabilných hasiacich zariadení. Cez tento koppler je umožnené monitorovať a ovládať ústredňu Esser 8010.



Obr. 4-20 Rôzne druhy kopplerov



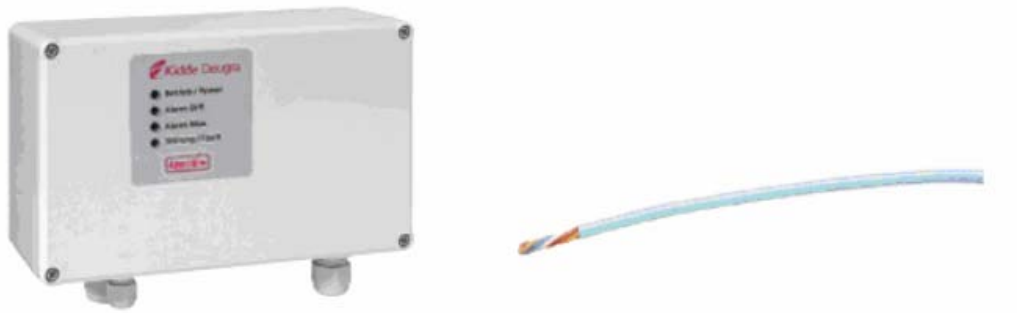
Obr. 4-21 Zapojenie kopplerov na kruhové vedenie Esserbus

4.5 Ostatné hlásiče:

Hlásič do vzduchotechniky – V podstate sa jedna o klasické opticko – dymové hlásiče s upravenou charakteristikou. Hlásiče sú umiestnené v špeciálnom kryte, do ktorého je pomocou venturiho trubice nasávaný vzduch z vzduchotechnického potrubia. Nasávaný vzduch prechádza hlásičom, tým dochádza k monitorovaniu vzduchu vo vzduchotechnickom potrubí. Hlásič je pripojení do systému pomocou vedenia Esserbus alebo EsserbusPLus.

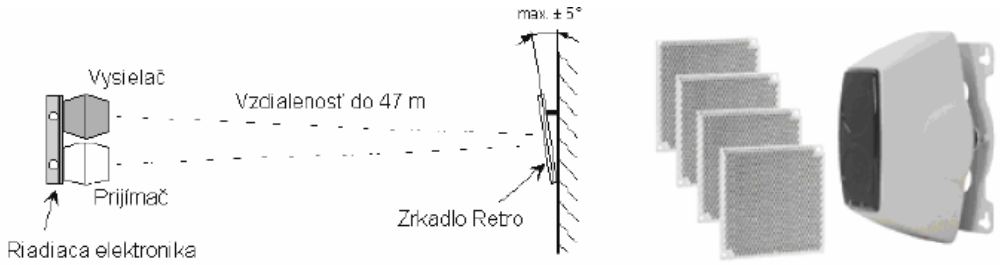
Obr. 4-22 Hlásič do vzduchotechniky

Lineárny teplotný hlásič LWM-1 -Pomocou riadiacej jednotky je meraný elektrický odpor špeciálneho teplo-citlivého kábla, ktorý je vhodný umiestiť do vlhkého stráženého priestoru. Pokiaľ dôjde k zmene teploty okolia v dôsledku požiaru zmení sa elektrický odpor káblu a dôjde k vyhláseniu požiaru. Tento teplo-citlivý kábel je odolný voči prachu a vlhku. Pripojenie do systému Esser je realizované pomocou vstupného kopplera. Reset riadiacej jednotky po poplachu alebo poruche je zabezpečené tzv. resetovacím modulom.



Obr. 4-23 Vyhodnocovacia jednotka a termodiferenciálny kábel

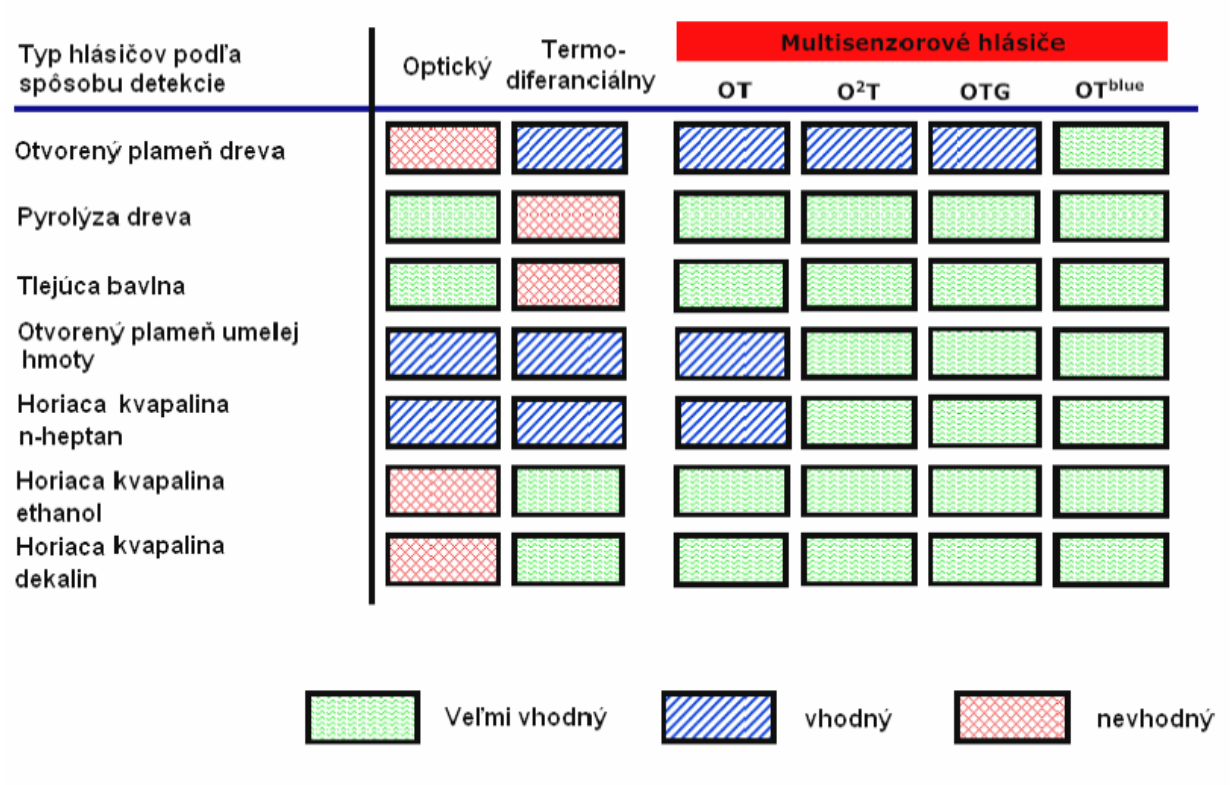
Lineárne optické dymové hlásiče Fireray - Tento hlásič sa používa k detekcii požiaru v rozsiahlych otvorených objektoch s možností stráženia až 1400 m2. Hlásič obsahuje prijímaciu a vysielaciu jednotku, prípadne prevedenie s odrazovým zrkadlom. Vysielač vysiela modulovaný, ľudským okom neviditeľný infračervený lúč, ktorý je prijímaný a vyhodnocovaný prijímacou jednotkou. Hlásič je aktivovaný - v závislosti na prednastaveným poplachovým prahom. Pracovná citlivosť a bezpečnosť je zvýšená vďaka chybovej kompenzácií, ktorá je riadená mikroprocesorom. Pripojenie do systému Esser je realizované pomocou vstupného kopplera.



Obr. 4-24 Schéma použitia lineárneho optického hlásiča Fireray

Návrh a naprogramovanie systému protipožiarnej ochrany

Elektrická požiarna signalizácia spadá do oblasti vyhradených technických zariadení, čomu zodpovedá samotné projektovanie a montáž, ktoré musia byť v rámci platnej legislatívy Slovenskej republiky vykonávané spoločnosťami spĺňajúcimi platnú legislatívu. K týmto činnostiam osoby musia vlastniť certifikát o tom, že sú oprávnené tento systém projektovať, inštalovať, programovať ale aj revidovať. Prvá fáza realizácie systému je samotné projektovanie. Sú to výpočty mnohých faktorov samotného objektu. Rozloženie hlásičov a ich umiestnenie závisí aj od koeficientu požiarneho zaťaženia stavby, ktorý určuje požiarny projekt vypracovaný požiarnym špecialistom, ale aj technickými charakteristikami uvedenými výrobcom jednotlivých hlásičov. [31]



Obr. 4-25 Detekčná schopnosť jednotlivých hlásičov

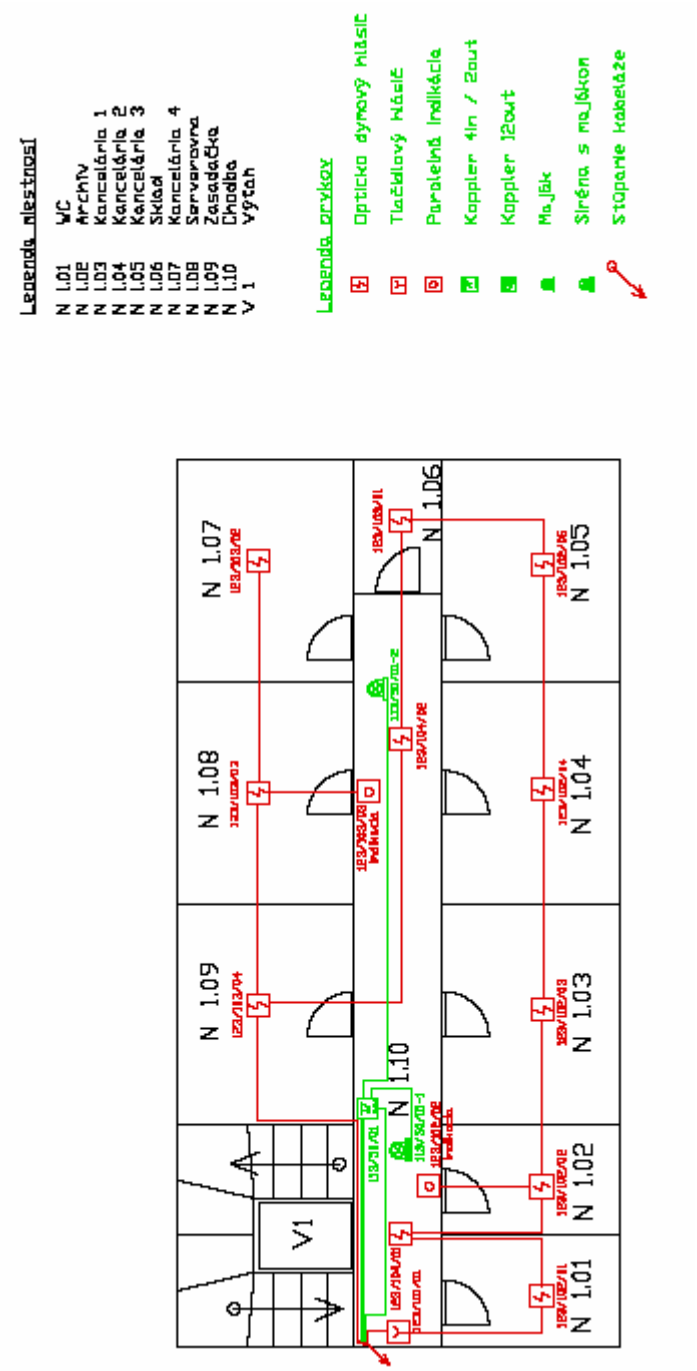
5 Posúdenie rizika pre navrhnutý bezpečnostný systém

V dizertačnej práci riešim elektrickú požiarnu signalizáciu jedného poschodia administratívnej budovy. Kancelárie administratívnej budovy majú centrálnu klimatizáciu. Na príslušnom poschodí je navrhnutých 11 automatických hlásičov a 1 manuálny tlačidlový hlásič Do priestorov serverovne je navrhnutý elektronický zámok, ktorý zabraňuje vstupu neoprávneným osobám Ústredňa je umiestnená na mieste, kde nie je 24- hodinová prevádzka t.j. v noci je budova bez dozoru bezpečnostnej služby. Z tejto informácie vyplýva nutnosť naprogramovať ústredňu na dva režimy, nočný a denný. Princíp detekcie a stráženia objektu pred požiarmi je ten istý v jednom aj v druhom režime. Rozdiel je v časoch aktivácií a overovaniach požiaru.

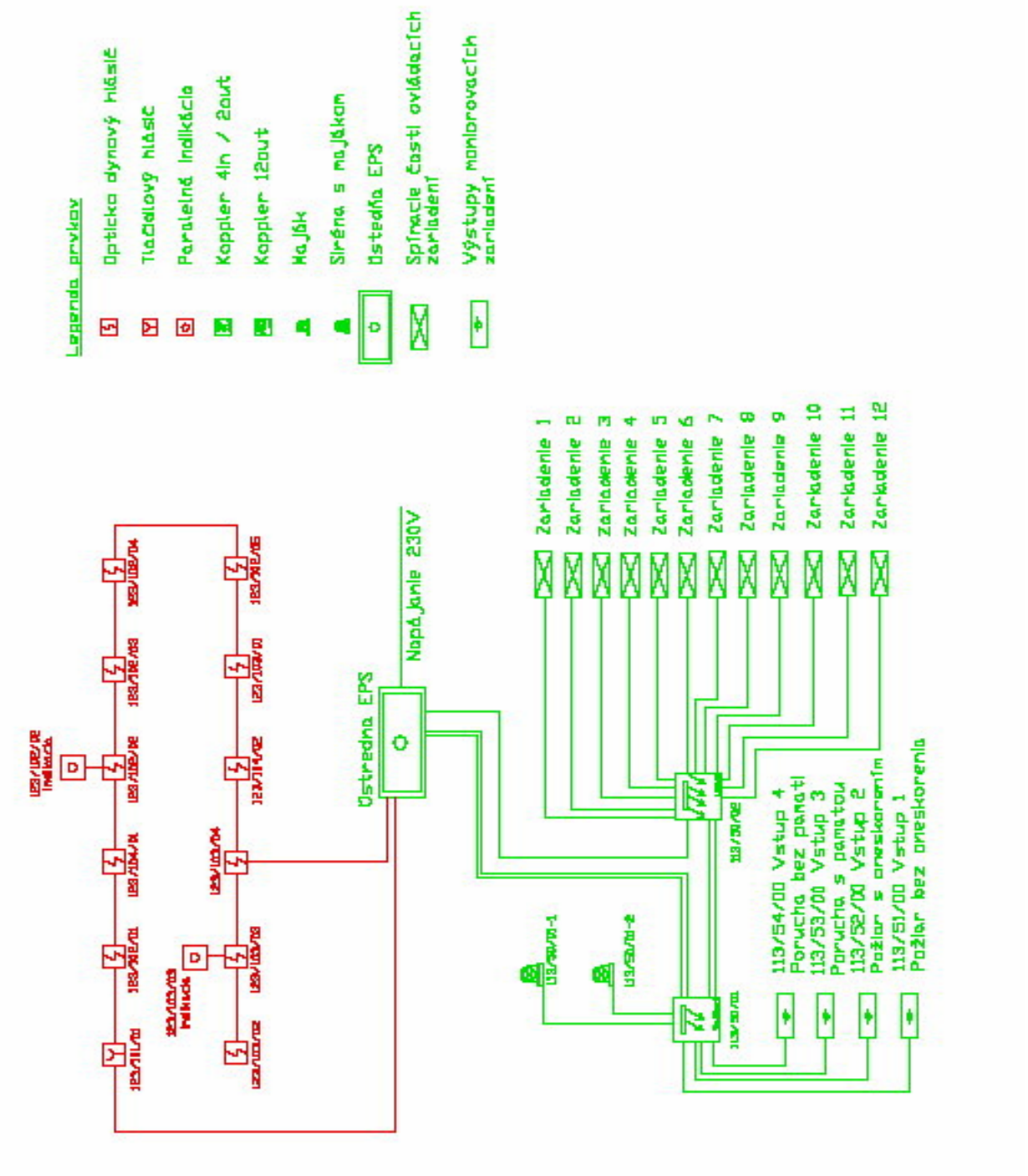
Nočný režim – v noci sa v budove nenachádzajú ľudia. Na základe tohto predpokladu sa môžeme domnievať, že po vyhlásení požiaru ústredňou nemá kto túto skutočnosť overiť. V tomto prípade sa čas aktivácií výrazne skráti na okamžitú reakciu systému, následnú aktiváciou jednotlivých zariadení pripojených k systému signalizácie a komunikácie na pult centrálnej ochrany alebo stredisko registrácie požiarnych poplachov.

Denný režim – jednotlivé hlásiče sa delia do skupín. Maximálne 32 prvkov do jednej skupiny možno naprogramovať. Podľa platnej legislatívy Slovenskej republiky nemožno automatické a manuálne hlásiče prideliť do tej istej skupiny hlásičov. Dôvod preto je jednoduchý. Z tlačidlových skupín hlásičov prebehne aktivácia okamžitá bez rozdielu či horí alebo nie. Automatické hlásiče vyhlásia poplach a obsluha musí tento stav vyhodnotiť a overiť. Preto platná norma a ústredňa elektrickej požiarnej signalizácie rozlišuje dva časy T1 a T2. Čas T1 je čas na potvrdenie a T2 je čas na overenie. Modelová situácia obsluhy: Po príchode do práce musí obsluha zatlačiť tlačidlo „Oneskorenie“. Týmto ústredňa vyhodnotí prítomnosť obsluhy a prepne sa do denného režimu. Ak ústredňa vyhlási požiar zo skupiny automatických hlásičov, obsluha má na reakciu potvrdenia hlásenia ústredne čas T1. V prípade, keď sa obsluha nenachádza na mieste a nepotvrdí hlásenie ústredne po uplynutí času na to určeného, nasleduje aktivácie. Druhá možnosť, je že obsluha potvrdí hlásenie a pošle pracovníka priamo na miesto predpokladaného vzniku požiaru. Po potvrdení hlásenia začína plynúť čas T2, čo je čas overenia. V okamihu, že sa požiar potvrdí, stlačí najbližší tlačidlový hlásič, čím spustí aktivácia. Pokiaľ sa požiar nepotvrdí, obsluha resetne poplachovú hlásenie a vypne aktivovaný hlásič. Ak počas časového intervalu T2 nepríde k reakcii obsluhy, ústredňa spustí aktivácie automaticky.

Do každej miestnosti vyúsťuje potrubie pre centrálny odvod dymu a spalín horenia. Na poschodí sa nachádza výťah, ktorý v prípade požiaru slúži aj ako evakuačný výťah. V priestoroch chodby je evakuačný rozhlas so svetelnou signalizáciou. Vstup do technickej miestnosti (serverovne) je umožnený len určitým osobám, dvere sú zabezpečené prístupovým systémom.



Obr. 5-1 Schéma rozloženia prvkov elektrickej požiarnej signalizácie



Obr. 5-2 Schéma zapojenia elektrickej požiarnej signalizácie doplnená o spínacie časti ovládacích zariadení

5.1 Identifikácia nebezpečenstiev a stromy poruchových stavov

V prvej časti práce sa budem zaoberať určením funkčnej bezpečnosti jednoduchého požiarneho systému firmy ESSER bez následných spínacích zariadení, t.j. EPS s požiarnymi čidlami, ústredňou a hlásičom požiaru a jeho zaradenie do príslušnej kategórie SIL. Druhá časť práce obsahuje analýzu spoľahlivosti tohto systému, doplneného ďalšími spínacími zariadeniami. Mechanické časti systému budú posudzované zvlášť.

5.1.1 Sériový systém

Systém je v poruche vtedy, pokiaľ akýkoľvek jeho komponent bude v poruche, resp. systém je funkčný, pokiaľ všetky komponenty sú funkčné. Potom výraz pre pravdepodobnosť je:

$$P(\mathrm{S}) = \mathrm{P(A).P(B).P(C)} \ldots\ldots \qquad \textbf{(5-1)}$$

Bezporuchovosť, pohotovosť systému sa vypočíta:

$$R_S(t) = R_A(t) \cdot R_B(t) \cdot R_C(t) \ldots \qquad \textbf{(5-2)}$$

Systém sériovo zapojených komponent bude v poruchovom stave, pokiaľ jedna z jeho komponent bude v poruchovom stave. Preto sa celková pravdepodobnosť bezporuchovej prevádzky vypočíta ako:

$$\mathbf{R_S=R_1.R_2.R_3.....} \qquad \textbf{(5-3)}$$

Tento vzorec možno zovšeobecniť pre akýkoľvek sériový systém, a je daný súčinom jednotlivých R(t). Vzťah pre intenzitu porúch systému je:

$$R_S = R_1 R_2 R_3 = e^{-\lambda_1 t} e^{-\lambda_2 t} e^{-\lambda_3 t} = e^{-(\lambda_1+\lambda_2+\lambda_3)t} \qquad \textbf{(5-4)}$$

Celková intenzita porúch sériového systému je daná súčtom jednotlivých intenzít komponent sériového systému. Celková pravdepodobnosť bezporuchovej prevádzky sériového systému je daná súčinom jednotlivých pravdepodobnosti bezporuchovej prevádzky komponent sériového systému.

5.1.2 Paralelný systém

Systém je v poruche vtedy, pokiaľ všetky jeho komponenty sú v poruche, resp. systém je funkčný, pokiaľ aspoň jeden komponent je funkčný.

Výraz pre pravdepodobnosť bezporuchového stavu systému:

$$P(S) = 1 - P(\overline{A}) \cdot P(\overline{B}) \cdot P(\overline{C}) \quad \textbf{(5-5)}$$

Bezporuchovosť, pohotovosť systému sa vypočíta:

$$R_S(t) = 1 - (1 - R_A(t)) \cdot (1 - R_B(t)) \cdot (1 - R_C(t)) \quad \textbf{(5-6)}$$

Pravdepodobnosť, že tri komponenty budú mať poruchu je $F_S=F_1F_2F_3$

$$F_S = F_1F_2F_3 = (1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t})(1 - e^{-\lambda_3 t}) \quad \textbf{(5-7)}$$

5.1.3 Strom porúch – kvantitatívna analýza

Metóda priameho výpočtu je použiteľná pre stromy porúch v ktorých sa každý elementárny jav objavuje len raz. Pri výpočte s využitím známych vzťahov postupne určujeme pravdepodobnosti javov od najnižšej úrovne až po vrcholovú udalosť. Postupne odspodu prechádzame logické členy stromu porúch a podľa typu určujeme pravdepodobnosť javov, ktoré sú týmito členmi logicky definované

V prípade použitia logického členu typu OR sa pravdepodobnosť toho, že jav G nastane určí podľa rovnice:

$$P(G) = 1 - \prod_{i=1}^{i=s} [1 - P(A_i)] \quad \textbf{(5-8)}$$

V prípade použitia logického členu typu AND sa pravdepodobnosť toho, že jav G nastane určí podľa rovnice:

$$P(G) = \prod_{i=1}^{i=s} P(A_i) \quad \textbf{(5-9)}$$

kde G je jav zložený s elementárnych javov A_i, ktoré sú jeho bezprostrednou príčinou.

5.1.4 Špecifikácia bezpečnostných požiadaviek

Interval skúšok požiarneho systému je stanovený na 1 rok (8760 h), čo je obvyklý interval stanovený normou ČSN 73 0875 a ČSN 34 2710

Požiadavky na toleranciu k poruchám hardvéru sú charakterizované hodnotou HFT, ktorá popisuje kvalitu bezpečnostnej funkcie a znamená schopnosť pri výskyte porúch ďalej správne vykonávať funkciu. [EN 61511-1 odstavec 11.4.4].

Určenie súčiniteľa β a β_D spoločných porúch

β je súčiniteľ spoločných porúch pre nezistené bezpečné chyby a β_D je súčiniteľ spoločných porúch pre zistené spoločné chyby. Systematické spoločné poruchy môžu byť spôsobené napr.:

- chybou návrhu SIS
- použitím nevhodného hardvéru
- chybou softvéru
- chybou človeka
- chybou návrhu hardvéru
- chybou úpravy systému

Určenie β a β_D pre kanály s architektúrou 1oo2 a 2oo3 je určené podľa normy EN 61508-6 príloha D. Pomocou tabuľky D1, D2 a D3 určíme parametre:

- pre podsystém logiky X_{LS}, Y_{LS}, Z
- pre snímače a koncové prvky X_{SF}, Y_{SF}, Z

Pre bezpečnostnú funkciu spustenia poplachu sú parametre:
Pre podsystém logiky: X_{LS}=23,5, Y_{LS}=25, Z=1,5
Pre snímače: X_{SF}=25,5, Y_{SF}=27,5, Z=1
Hodnoty ďalej spracujeme podľa:

$$S = X + Y \quad \textbf{(5-10)}$$

$$S_D = X.(Z+1) + Y \quad \textbf{(5-11)}$$

Hodnotu S použijeme pre určenie β podľa tabuľky D4 tejto normy. Obdobne použijeme S_D pre určenie β_D.

Pre podsystém logiky: β=2% a β_D=1%

Pre snímače: β=5% a β_D=2%

Výpočet pravdepodobnosti porúch

Pre výpočet pravdepodobnosti porúch na vyžiadanie bezpečnostnej funkcie existujú rôzne metódy, ktoré obsahujú:

- simuláciu
- analýzu príčin a následkov
- analýzu stromu porúch
- Markovové modely
- blokové diagramy spoľahlivosti

- bezporuchovostné blokové schémy

Pre vlastný výpočet pravdepodobnosti porúch na vyžiadanie bezpečnostnej funkcie, pre základný požiarny systém bez následných spínacích zariadení, som zvolil metódu bezporuchovostných blokových schém, popísanú v norme IEC 61508-6 príloha B. Pre výpočet pravdepodobnosti porúch na vyžiadanie bezpečnostnej funkcie, pre požiarny systém s následnými spínacími zariadeniami, som zvolil metódu vychádzajúcu z analýzy stromov porúch.

Vzorce použité pre výpočet sú platné za predpokladu, že intenzita λ porúch je konštantná t.j. SIS systém sa nachádza v prostrednej oblasti vaňovej krivky.

$$\lambda = \frac{1}{MTTF} \text{ pre obnoviteľné zariadenia} \qquad \textbf{(5-12)}$$

$$\lambda = \frac{1}{MCTF} \text{ pre neobnoviteľné zariadenia} \qquad \textbf{(5-13)}$$

Väčšina výrobcov zariadení udáva hodnotu MTBF a to v hodinách, rokoch, alebo v jednotkách FIT (1 FIT=1 porucha / 10^9 hodín). MTBF vyjadruje strednú dobu medzi poruchami, ktorá sa skladá zo strednej doby do poruchy a strednej doby do zotavenia. Poväčšine je hodnota MTTR zanedbateľne nízka voči hodnote MTBF. Hodnota MTTR je typicky menej ako 24 hodín.

Pre diskrétne časti zariadení ako napríklad relé, tlačítka sa udáva hodnota MCTF, ktorá zastupuje hodnotu MTTF. Následné výpočty sa vykonávajú rovnako s hodnotou MTTF. Výrobcovia často uvádzajú hodnotu B_{10}, čo je štatistických 10 % rozhrania pre elektrickú životnosť. Potom sa dá táto hodnota pri poznaní početnosti spínania C prepočítať na hodnotu MCTF.

$$MCTF = \frac{B_{10}}{0{,}1.C} \qquad \textbf{(5-14)}$$

$$MTTF = MTBF - MTTR \qquad \textbf{(5-15)}$$

Intenzita porúch sa delí na nebezpečné a bezpečné.

$$\lambda = \lambda_D + \lambda_S \qquad \textbf{(5-16)}$$

Tá sa ďalej delí na zistiteľné a nezistiteľné.

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \quad \textbf{(5-17)}$$

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \quad \textbf{(5-18)}$$

Pre ďalší výpočet sa predpokladá exponenciálne rozdelenie intenzity porúch.

$$PFD = 1 - e^{-\lambda_D . t_{CE}} \quad \textbf{(5-19)}$$

Ekvivalentná stredná doba prestoja kanálu, posudzuje kanál tak, akoby bol zložený z dvoch sériovo usporiadaných častí. Jedna s intenzitou nezistených nebezpečných porúch a druhá s intenzitou zistených nebezpečných porúch.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} . \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} . MTTR \quad \textbf{(5-20)}$$

Vo výpočtoch sa z dôvodu zjednodušenia vychádza z predpokladu, že

$$PFD \approx \lambda_D . t_{CE} \text{ za podmienky } \lambda_D . t_{CE} << 1 \quad \textbf{(5-21)}$$

Podiel bezpečných porúch uvádza pomer intenzity bezpečných porúch a intenzity porúch.

$$SR = \frac{\lambda_S}{\lambda} \text{ z čoho vyplýva } \lambda_D = \lambda . (1 - SR) \quad \textbf{(5-22)}$$

Diagnostické pokrytie vyjadruje pomer intenzity nezistených nebezpečných porúch k intenzite nebezpečných porúch. Hodnote DC > 0 % je pri zariadeniach, ktoré majú diagnostický SIS, alebo jeho subsystém. Vo väčšine prípadoch v elektrotechnike sú to zariadenia obsahujúce mikroprocesor, napr. PLC systémy a SMART prevodníky. Pri systémoch pracujúcich na iných princípoch (mechanickom, hydraulickom, pneumatickom) sa hodnota uvádza tam, kde je možnosť testovať prvok za prevádzky systému, pričom by to neovplyvnilo jeho funkciu.

$$DC = \frac{\lambda_{DD}}{\lambda_D} \text{ z čoho vyplýva } \lambda_{DU} = \lambda_D . (1 - DC) \quad \textbf{(5-23)}$$

Podiel bezpečných výpadkov

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \text{ z čoho vyplýva } SFF = 1 - \frac{\lambda_{DU}}{\lambda} \quad \textbf{(5-24)}$$

Ekvivalentná stredná doba prestoja rozhodovacej skupiny

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}.\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}.MTTR \quad \textbf{(5-25)}$$

Architektúra 1oo1

$$PFD_G = \left(\lambda_{DU} + \lambda_{DD}\right).t_{CE} \quad \textbf{(5-26)}$$

Architektúra 1oo2

$$PFD_G = 2.\left[\left(1-\beta_D\right).\lambda_{DD} + \left(1-\beta\right).\lambda_{DU}\right]^2.t_{CE}.t_{GE} + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.\left(\frac{T_1}{2} + MTTR\right) \quad \textbf{(5-27)}$$

Architektúra 2oo3

$$PFD_G = 6.\left[\left(1-\beta_D\right).\lambda_{DD} + \left(1-\beta\right).\lambda_{DU}\right]^2.t_{CE}.t_{GE} + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.\left(\frac{T_1}{2} + MTTR\right) \quad \textbf{(5-28)}$$

Pokiaľ bezpečnostná funkcia závisí na viacerých rozhodovacích skupinách snímačov, logík alebo koncových prvkov, príslušné hodnoty PFD sa sčítajú.

$$PFD_S = \sum_{i=1}^{n} PFD_{Gi} \quad \textbf{(5-29)}$$

$$PFD_L = \sum_{i=1}^{n} PFD_{Gi} \quad \textbf{(5-30)}$$

$$PFD_{FE} = \sum_{i=1}^{n} PFD_{Gi} \quad \textbf{(5-31)}$$

$$PFD_{SS} = \sum_{i=1}^{n} PFD_{Gi} \quad \textbf{(5-32)}$$

Priemerná pravdepodobnosť poruchy pri vyžiadaní bezpečnostnej funkcie SIS, sa skladá z obdobných hodnôt pre jednotlivé subsystémy snímačov, logík, koncových prvkov a podporných subsystémov. Snímače sú vstupnou časťou SIS a detekujú nebezpečné situácie. Subsystémy logiky spracúvajú tieto vstupy a generujú správne povely pre koncové členy tak, aby sa zabránilo nebezpečnej situácií. Podporné subsystémy umožňujú úspešnú funkciu SIS. Medzi ne patrí napr. napájací zdroj, pokiaľ ostatné subsystémy pracujú s funkciou, kde až po privedení napájacieho napätia sa inicializuje bezpečnostná funkcia.

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} + PFD_{SS} \quad \textbf{(5-33)}$$

5.2 Výpočet PFD jednotlivých komponentov

Snímače

Typ: OT hlásič IQ8Quad
Výrobca: ESSER
Zdroj údajov: Dokument ESSER Mean Time Between Failures z 20.10.2008
Hodnota: MTBF=21,8 rokov
Výpočet: Tabuľka 3

Typ: Tlačidlový hlásič IQ8Quad
Výrobca: ESSER
Zdroj údajov: Dokument ESSER Mean Time Between Failures z 12.8.2008
Hodnota: Životnosť kontaktov $B_{10}=10^5$ zopnutí, uvažovaných 5 zopnutí/rok ($5.71.10^{-4}$ zopnutí/h), $MCTF = \frac{10^5}{0,1.5,71.10^{-4}} = 1.752.10^9$
Výpočet: Tabuľka 4

Typ: Paralelná indikácia OT Blue
Výrobca: ESSER
Zdroj údajov: Dokument ESSER Mean Time Between Failures z 12.8.2008
Hodnota: MTBF=13,06 rokov
Výpočet: Tabuľka 5

Logika

Typ: Základová doska ústredne 8000/IQ8Control
Výrobca: ESSER
Zdroj údajov: Dokument ESSER Consideratiotion on MTBF times of the DOPS overspeed protection system z 21.10.2004
Hodnota: MTBF=31,24 rokov
Výpočet: Tabuľka 6

Typ: Zdrojová doska ústredne 8000/IQ8Control
Výrobca: Epro
Zdroj údajov: Dokument Epro Consideratiotion on MTBF times of the DOPS overspeed protection system z 21.12.2007
Hodnota: MTBF=13,1 rokov
Výpočet: Tabuľka 7

Typ: Periférna karta ústredne 8000/IQ8Control
Výrobca: ESSER
Zdroj údajov: Dokument ESSER Consideratiotion on MTBF times of the DOPS overspeed protection system z 21.10.2004
Hodnota: MTBF=19,6 rokov
Výpočet: Tabuľka 8

Typ: Karta pre mikromoduly ústredne 8000/IQ8Control

Výrobca: ESSER
Zdroj údajov: Dokument ESSER Consideratiotion on MTBF times of the DOPS overspeed protection system z 21.10.2004
Hodnota: MTBF=21,8 rokov
Výpočet: Tabuľka 9

Typ: Komunikačná jednotka ústredne 8000/IQ8Control
Výrobca: Siemens
Zdroj údajov: Dokument Siemens Mean Time Between Failures – list for Simatic products z 19.10.2007
Hodnota: MTBF=12,1 rokov
Výpočet: Tabuľka 10

Koncové prvky

Typ: Reproduktory evakuačného rozhlasu IDA4XM
Výrobca: Honeywell
Zdroj údajov: Dokument Honeywell z 21.12.2001
Hodnota: MTBF=12,5 rokov
Výpočet: Tabuľka 11

Podporný subsystém

Typ: toroidný transformátor ústredne 8000/IQ8Control
Výrobca: ESSER
Zdroj údajov: Typická hodnota
Hodnota: MTBF=23,3 rokov
Výpočet: Tabuľka 12

Typ: Stykač 3RT1044-1BM40
Výrobca: Siemens
Zdroj údajov: Dokument Siemens Recommendation of the standard B10 values z 1.2.2006
Hodnota: Životnosť kontaktov $B_{10}=10^6$ zopnutí pri indukčnej záťaži, uvažovaných 1 zopnutie/deň (0,042 zopnutí/h),

$$MCTF = \frac{10^6}{0{,}1.0{,}042} = 2{,}38.10^8$$

Výpočet: Tabuľka 13

Typ: Poistky 002312105 - DII/E27-16A
Výrobca: OEZ
Zdroj údajov: Katalóg výrobcu
Hodnota: Životnosť kontaktov $B_{10}=300$ pracovných cyklov pri prúde 16A, uvažovaných 1 zopnutie/rok ($1{,}1.10^{-4}$ zopnutí/h),

$$MCTF = \frac{300}{0{,}1.1{,}1.10^{-4}} = 2{,}72.10^7$$

Výpočet: Tabuľka 14

5.2.1 Tabuľky výpočtov

Tabuľka 3		
MTBF	190968	h
MTTR	8	h
SR	90	%
DC	99	%
β	5	%
β_D	2	%
T_1	24	h
MooN	2oo3	-
HFT	2	-
λ	$5{,}24.10^{-6}$	1/h
λ_D	$5{,}24.10^{-7}$	1/h
λ_{DU}	$5{,}24.10^{-9}$	1/h
λ_{DD}	$5{,}18.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$8{,}86.10^{-8}$	h

Tabuľka 4		
MTBF	$1{,}752.10^{9}$	h
MTTR	8	h
SR	90	%
DC	60	%
β	5	%
β_D	2	%
T_1	8760	h
MooN	1oo1	-
HFT	2	-
λ	$5{,}71.10^{-10}$	1/h
λ_D	$5{,}71.10^{-11}$	1/h
λ_{DU}	$2{,}28.10^{-11}$	1/h
λ_{DD}	$3{,}42.10^{-11}$	1/h
SFF	96	%
t_{CE}	1760	h
t_{GE}	1176	h
PFD_G	$1{,}0.10^{-7}$	h

Tabuľka 5		
MTBF	114405,6	h
MTTR	8	h
SR	90	%
DC	60	%
β	5	%
β_D	2	%
T_1	24	h
MooN	1oo2	-
HFT	2	-
λ	$8{,}74.10^{-6}$	1/h
λ_D	$8{,}74.10^{-7}$	1/h
λ_{DU}	$3{,}5.10^{-7}$	1/h
λ_{DD}	$5{,}24.10^{-7}$	1/h
SFF	96	%
t_{CE}	12,8	h
t_{GE}	11,2	h
PFD_G	$4{,}34.10^{-7}$	h

Tabuľka 6		
MTBF	273662,4	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	8760	h
MooN	1oo2	-
HFT	1	-
λ	$3{,}65.10^{-6}$	1/h
λ_D	$3{,}65.10^{-7}$	1/h
λ_{DU}	$3{,}65.10^{-9}$	1/h
λ_{DD}	$3{,}62.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	51,8	h
t_{GE}	37,2	h
PFD_G	$3{,}52.10^{-7}$	h

Tabuľka 7		
MTBF	102966	h
MTTR	8	h
SR	90	%
DC	90	%
β	2	%
β_D	1	%
T_1	8760	h
MooN	1oo2	-
HFT	1	-
λ	$9{,}71.10^{-6}$	1/h
λ_D	$9{,}71.10^{-7}$	1/h
λ_{DU}	$9{,}71.10^{-8}$	1/h
λ_{DD}	$8{,}74.10^{-7}$	1/h
SFF	99	%
t_{CE}	446	h
t_{GE}	300	h
PFD_G	$9{,}48.10^{-6}$	h

Tabuľka 8		
MTBF	171696	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$5{,}82.10^{-6}$	1/h
λ_D	$5{,}82.10^{-7}$	1/h
λ_{DU}	$5{,}82.10^{-9}$	1/h
λ_{DD}	$5{,}77.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$4{,}86.10^{-8}$	h

Tabuľka 9		
MTBF	190968	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$5{,}24.10^{-6}$	1/h
λ_D	$5{,}24.10^{-7}$	1/h
λ_{DU}	$5{,}24.10^{-9}$	1/h
λ_{DD}	$5{,}18.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$4{,}37.10^{-8}$	h

Tabuľka 10		
MTBF	105996	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$9{,}44.10^{-6}$	1/h
λ_D	$9{,}44.10^{-7}$	1/h
λ_{DU}	$9{,}44.10^{-9}$	1/h
λ_{DD}	$9{,}34.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$7{,}89.10^{-8}$	h

Tabuľka 11		
MTBF	109500	h
MTTR	8	h
SR	90	%
DC	60	%
β	5	%
β_D	2	%
T_1	720	h
MooN	1oo2	-
HFT	2	-
λ	$9{,}13.10^{-6}$	1/h
λ_D	$9{,}13.10^{-7}$	1/h
λ_{DU}	$3{,}65.10^{-7}$	1/h
λ_{DD}	$5{,}48.10^{-7}$	1/h
SFF	96	%
t_{CE}	152	h
t_{GE}	104	h
PFD_G	$6{,}87.10^{-6}$	h

Tabuľka 12		
MTBF	204108	h
MTTR	8	h
SR	90	%
DC	60	%
β	-	%
β_D	-	%
T_1	8760	h
MooN	1oo1	-
HFT	0	-
λ	$4{,}9.10^{-6}$	1/h
λ_D	$4{,}9.10^{-7}$	1/h
λ_{DU}	$1{,}96.10^{-7}$	1/h
λ_{DD}	$2{,}94.10^{-7}$	1/h
SFF	96	%
t_{CE}	1760	h
t_{GE}	1176	h
PFD_G	$8{,}62.10^{-4}$	h

Tabuľka 13		
MTBF	$2{,}38.10^{8}$	h
MTTR	8	h
SR	50	%
DC	0	%
β	-	%
β_D	-	%
T_1	8760	h
MooN	1oo1	-
HFT	0	-
λ	$4{,}2.10^{-9}$	1/h
λ_D	$2{,}1.10^{-9}$	1/h
λ_{DU}	$2{,}1.10^{-9}$	1/h
λ_{DD}	0	1/h
SFF	50	%
t_{CE}	4388	h
t_{GE}	2928	h
PFD_G	$9{,}22.10^{-6}$	h

Tabuľka 14		
MTBF	$2{,}72.10^{7}$	h
MTTR	8	h
SR	50	%
DC	0	%
β	-	%
β_D	-	%
T_1	8760	h
MooN	1oo1	-
HFT	0	-
λ	$3{,}68.10^{-8}$	1/h
λ_D	$1{,}84.10^{-8}$	1/h
λ_{DU}	$1{,}84.10^{-8}$	1/h
λ_{DD}	0	1/h
SFF	50	%
t_{CE}	4388	h
t_{GE}	2928	h
PFD_G	$8{,}07.10^{-5}$	h

5.3 Výpočet PFD bezpečnostnej funkcie

Pre bezpečnostnú funkciu ohlásenia požiaru sa vychádza zo situácie, že koncové prvky sú síce dva, t.j. akustická signalizácia a optická signalizácia, ale môžeme taktiež použiť metódu bezporuchovostných blokových schém pre architektúru 1oo2.

Tabuľka 15 Výpočet PFD bezpečnostnej funkcie ohlásenia požiaru

	PFD_S	PFD_L	PFD_{FE}	PFD_{SS}	PFD_{SYS}
Tabuľka č.	3-5	6-10	11	12-14	
h	$6{,}22.10^{-7}$	1.10^{-5}	$6{,}87.10^{-6}$	$9{,}52.10^{-4}$	$9{,}69.10^{-4}$
% využitia PFD_{SYS}	0,06	1,03	0,71	98	

5.4 Určenie pravdepodobnosti vzniku porúch v jednotlivých moduloch.

Požiarny systém analyzovaný v kapitole 0, je doplnený o spínacie časti ďalších ovládacích zariadení, na čo je použitý esserbus-Koppler 12out, ktorý ovláda požiarna ústredňa. Ústredňa je taktiež spojená s esserbus-Koppler 4 vstupy/2out, ktorý slúži na výstupy monitorovacích zariadení, ako je napríklad paralelné tablo pre obsluhu. Tieto dva kopplery sú navzájom spojené (Obr. 5-2). Pre výpočet pravdepodobnosti vzniku poruchy, pri tomto systéme som zvolil aj analýzu stromov porúch z dôvodu toho, že takto navrhnutý systém je kombináciou mechanických a elektronických častí, resp. len mechanických častí.

Vzhľadom na to, že spínacie časti ovládacích zariadení závisia od spoľahlivosti jedného z kopplerov, musíme najprv spočítať pravdepodobnosť vzniku poruchy pre toto zariadenie a následne danú hodnotu pripočítať k pravdepodobnosti vzniku poruchy pre jednotlivé sekcie.

5.4.1 Výpočet PFD koplerov

Pre bezpečnostnú funkciu ohlásenia poplachu sú parametre:

Pre podsystém logiky: $X_{LS}=33$, $Y_{LS}=24{,}5$, $Z=1$ z čoho vyplýva $\beta=2\%$ a $\beta_D=1\%$

Logika

Typ: Esserbus-Koppler 12out
Výrobca: Honeywell
Zdroj údajov: Dokument Honeywell z 18.9.2003
Hodnota: MTBF=33,12 rokov
Výpočet: Tabuľka 16

Typ: Zdrojová doska kopplera
Výrobca: Honeywell

Zdroj údajov: Dokument Honeywell z 18.9.2003
Hodnota: MTBF=14,3 rokov
Výpočet: Tabuľka 17

Podporný subsystém

Typ: toroidný transformátor kopplera
Výrobca: ESSER
Zdroj údajov: Typická hodnota
Hodnota: MTBF=23,3 rokov
Výpočet: Tabuľka 18

Typ: Istič 5SY5206-7 2P 6A C
Výrobca: Siemens
Zdroj údajov: Katalóg výrobcu
Hodnota: Životnosť kontaktov $B_{10}=2.10^5$ zopnutí pri menovitom prúde, uvažovaných 1 zopnutie/rok ($1,1.10^{-4}$ zopnutí/h),

$$MCTF = \frac{2.10^5}{0,1.1,1.10^{-4}} = 1,82.10^{10}$$

Výpočet: Tabuľka 19

Tabuľky výpočtov

Tabuľka 16		
MTBF	290131,2	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$3,45.10^{-6}$	1/h
λ_D	$3,45.10^{-7}$	1/h
λ_{DU}	$3,45.10^{-9}$	1/h
λ_{DD}	$3,41.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$2,87.10^{-8}$	h

Tabuľka 17		
MTBF	125268	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$7,98.10^{-6}$	1/h
λ_D	$7,98.10^{-7}$	1/h
λ_{DU}	$7,98.10^{-9}$	1/h
λ_{DD}	$7,90.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$6,67.10^{-8}$	h

Tabuľka 18		
MTBF	204108	h
MTTR	8	h
SR	90	%
DC	60	%
β	-	%

Tabuľka 19		
MTBF	$1,82.10^{10}$	h
MTTR	8	h
SR	50	%
DC	0	%
β	-	%

β_D	-	%
T_1	8760	h
MooN	1oo2	-
HFT	0	-
λ	$4{,}9.10^{-6}$	1/h
λ_D	$4{,}9.10^{-7}$	1/h
λ_{DU}	$1{,}96.10^{-7}$	1/h
λ_{DD}	$2{,}94.10^{-7}$	1/h
SFF	96	%
t_{CE}	1760	h
t_{GE}	1176	h
PFD_G	$2{,}54.10^{-6}$	h

β_D	-	%
T_1	8760	h
MooN	1oo1	-
HFT	0	-
λ	$5{,}49.10^{-11}$	1/h
λ_D	$2{,}75.10^{-11}$	1/h
λ_{DU}	$2{,}75.10^{-11}$	1/h
λ_{DD}	0	1/h
SFF	50	%
t_{CE}	4388	h
t_{GE}	2928	h
PFD_G	$1{,}21.10^{-7}$	h

Tabuľka 20 Výpočet PFD bezpečnostnej funkcie pri ohlásení požiaru

	PFD_L	PFD_{SS}	PFD_{SYS}
Tabuľka č.	16,17	18,19	
h	$9{,}54.10^{-8}$	$2{,}66.10^{-6}$	$2{,}76.10^{-6}$
% využitia PFD_{SYS}	3,46	96,54	

Pre bezpečnostnú funkciu vizualizácie poplachu sú parametre:

Pre podsystém logiky: X_{LS}=31,5, Y_{LS}=24, Z=1 z čoho vyplýva β=2% a β_D=1%

Pre snímače a koncové prvky: X_{SF}=23, Y_{SF}=20,5, Z=1 z čoho vyplýva β=5% a β_D=2%

Logika

Typ: esserbus-Koppler 4 vstupy/2out
Výrobca: Honeywell
Zdroj údajov: Dokument Honeywell z 18.9.2003
Hodnota: MTBF=33,78 rokov
Výpočet: Tabuľka 21

Typ: Zdrojová doska kopplera
Výrobca: Honeywell
Zdroj údajov: Dokument Honeywell z 18.9.2003
Hodnota: MTBF=14,3 rokov
Výpočet: Tabuľka 17

Podporný subsystém je použitý rovnaký ako pre systém ohlásenia poplachu.

Koncové prvky

Typ: Paralelné tablo
Výrobca: Honeywell
Zdroj údajov: Dokument Honeywell z 18.9.2003
Hodnota: MTBF=32,7 rokov
Výpočet: Tabuľka 22

Tabuľky výpočtov

Tabuľka 21		
MTBF	295913	h
MTTR	8	h
SR	90	%
DC	99	%
β	2	%
β_D	1	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$3{,}38.10^{-6}$	1/h
λ_D	$3{,}38.10^{-7}$	1/h
λ_{DU}	$3{,}38.10^{-9}$	1/h
λ_{DD}	$3{,}35.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$2{,}82.10^{-8}$	h

Tabuľka 22		
MTBF	286452	h
MTTR	8	h
SR	90	%
DC	99	%
β	5	%
β_D	2	%
T_1	24	h
MooN	1oo2	-
HFT	1	-
λ	$3{,}49.10^{-6}$	1/h
λ_D	$3{,}49.10^{-7}$	1/h
λ_{DU}	$3{,}49.10^{-9}$	1/h
λ_{DD}	$3{,}46.10^{-7}$	1/h
SFF	99,9	%
t_{CE}	8,12	h
t_{GE}	8,08	h
PFD_G	$5{,}88.10^{-8}$	h

Tabuľka 23 Výpočet PFD bezpečnostnej funkcie pri signalizácií požiaru

	PFD_L	PFD_{SS}	PFD_{FE}	PFD_{SYS}
Tabuľka č.	21,17	18,19	22	
h	$9{,}49.10^{-8}$	$2{,}66.10^{-6}$	$2{,}88.10^{-8}$	$2{,}78.10^{-6}$
% využitia PFD_{SYS}	3,41	95,68	0,91	

Hodnoty uvedené v tabuľkách

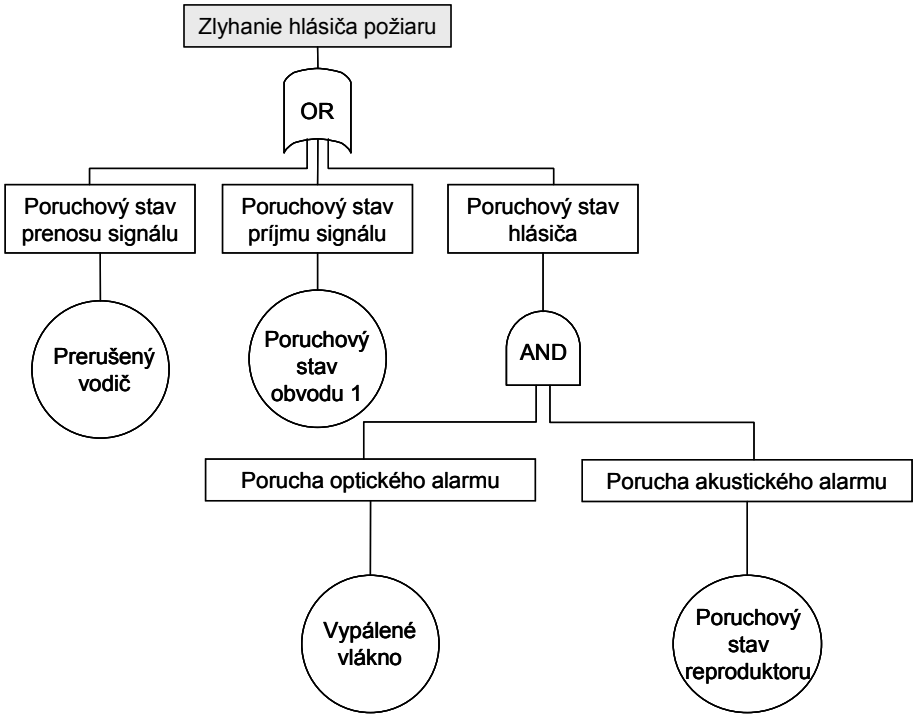
Tabuľka 20 a Tabuľka 23 sa pripočítajú k hodnotám PFD pre príslušnú sekciu spínacích častí ovládacích zariadení požiarneho systému.

5.4.2 Určenie PFD pre sekciu hlásič požiaru

Priemerná pravdepodobnosť vzniku poruchy pre túto sekciu je zanedbateľná, pretože táto sekcia je len doplnok k celému systému. Najdôležitejšou časťou tejto sekcie je blokovanie centrálneho rozhlasu a následne do systému rozhlasu pustenie evakuačného signálu. Tým, že systém má samostatný evakuačný rozhlas, táto sekcia len zdvojuje jeho funkciu.

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Nízka úroveň hlasitosti signálu	Zlé umiestnenie	Nedostatočná evakuácia osôb		Dodržiavať príslušnú normu
Nezrozumiteľnosť reči	Vysoká hladina šumu	Nedostatočná evakuácia osôb		Blokovanie hudobného pozadia.
Nefunkčnosť požiarneho hlásiča	Strata napájania	Nedostatočná evakuácia osôb	Druhotné energetické napájanie	Automatická indikácia stavu. Automatické monitorovanie závad

Systém požiarneho rozhlasu resp. ozvučenia sa skladá z rozhlasovej ústredne, ktoré sú rôznych veľkostí a typov podľa veľkosti aplikácie, z regulátorov hlasitosti a z reproduktorov. Reproduktory sú v rôznych vyhotoveniach, najčastejšie používané sú stropné kruhové reproduktory, do výrobných priestorov sú určené nástenné alebo závesné reproduktory. Do vonkajších priestorov alebo na ozvučenie veľkých hlučných priestorov je možné použiť tlakové reproduktory. Regulátor hlasitosti slúži na reguláciu intenzity zvuku v príslušnom reproduktore. Pomocou regulátorov je možné ovládať každý reproduktor v rozhlasovej linke ústredne individuálne.



Obr. 5-3 Strom poruchových stavov pre sekciu hlásič požiaru.

Tabuľka 24

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Poruchový stav prenosu signálu	$1{,}14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Poruchový stav obvodu 1	$2{,}51.10^{-7}$	Výpočet
P3 - Vypálené vlákno	$4{,}56.10^{-6}$	Štatistické údaje
P4 - Poruchový stav reproduktoru	$5{,}6.10^{-6}$	Výpočet

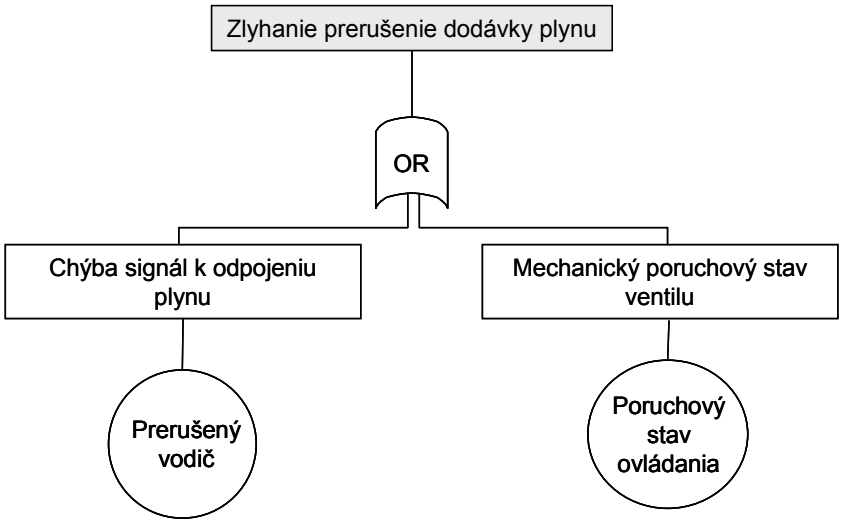
Pravdepodobnosti vzniku poruchy na sekcií hlásič požiaru boli stanovené expertnými úsudkami, resp. výpočtami, ktoré sú počítané podobnými výpočtami ako je uvedené v 5.2.1 a

sú uvedené v tabuľke (Tabuľka 24). Pre subsystém hlásič požiaru potom dostávame, podľa rovníc 5-8 a 5-9, konečný výsledok PFD=3,65.10^{-7}

5.4.3 Určenie PFD pre sekciu prerušenie dodávky plynu

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Neprerušenie dodávky plynu	Porucha elektromagnetického ventilu Mechanická porucha ventilu Porucha prenosu signálu	Výbuch plynu	Snímač polohy ventilu	Automatické monitorovanie závad

Termicko elektromagnetický bezpečnostný uzáver plynu zabraňuje úniku plynu v prípade požiaru. Akonáhle dosiahne teplota okolia dosiahne 100°C, uvoľní sa v telese uzáveru element, ktorý uzavrie prívod plynu. Musí odolať teplote 920°C po dobu jednej hodiny.



Obr. 5-4 Strom poruchových stavov pre sekciu prerušenie dodávky plynu.

Tabuľka 25

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Poruchový stav prenosu signálu	1,14.10^{-7}	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Mechanický poruchový stav ventilu	8,69.10^{-5}	Výpočet

Pravdepodobnosti vzniku poruchy na sekcií prerušenie dodávky plynu boli stanovené ako uvádza tabuľka (Tabuľka 25). Pre zníženie pravdepodobnosti vzniku mechanickej poruchy ventilu, môže byť ventil opatrený signalizáciou polohy. V tomto prípade sa zatiaľ s takýmto

opatrením neráta. Pre subsystém prerušenie dodávky plynu potom dostávame konečný výsledok PFD=8,7.10^{-5}

5.4.4 Určenie PFD pre sekciu prepnutie výťahu z normálneho chodu

V tejto sekcií sa nezaoberám stanovením bezpečnosti výťahu ako systému, ale len systémom, ktorý zabezpečí či funkcia výťahu sa prepne z normálneho chodu do chodu bezpečnostného.

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Zablokovanie výťahu	Prerušené vedenie	Uväznenie osôb vo výťahu	Dojazd výťahu s následným odblokovaním dverí	Snímač polohy výťahu
Zablokovanie dverí	Prerušené napájanie	Uväznenie osôb vo výťahu		Druhotné napájanie zámku
Nefunkčnosť požiarneho hlásiča	Zlyhanie hlásiča	Neprepnutie do bezpečnostného režimu s následným uväznením osôb vo výťahu	žiadne	Použiť kombinovaný hlásič 1oo2
Nefunkčnosť kľúčového spínača	Zlyhanie spínača			

Výťahy musia správne fungovať do 65°C v chránených nástupištiach a v priestoroch pre strojné zariadenie, riadenie výťahu musí byť funkčné i pri zadymení výťahovej šachty alebo strojovni najmenej 2 hodiny.

Šachtové dvere neurčené k používaniu musia byť chránené tak, aby neboli vystavené teplote vyššej ako 65 °C, pričom v strope kabíny musí byť otvor.

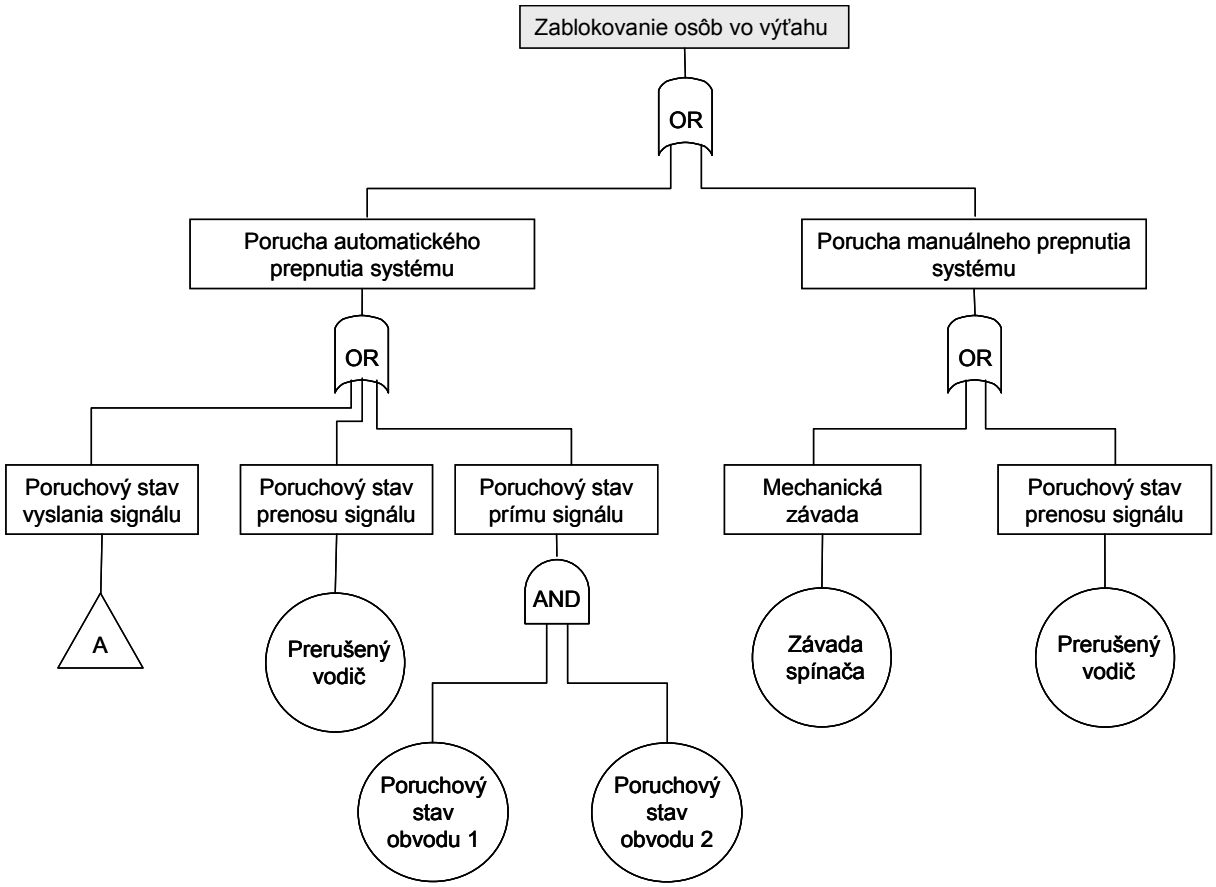
Elektroinštalácia výťahu je odolná proti stekajúcej a striekajúcej vode. A aby vyhovovala vysokým bezpečnostným požiadavkám, je vyrobená z bezhalogénového materiálu, ktorý pri horení nevytvára jedovaté plyny.

Dvere na strane vystavenej požiarnemu riziku sú konštruované so schopnosťou udržať prvok v neporušenom stave a udržať nízku po dobu 60 min.

V prípade požiaru musí byť umožnený dojazd kabíny do určenej stanice buď impulzom automatického požiarneho hlásiča, alebo privolaním pomocou kľúčového spínača. Výťah musí zostať vydaný z normálneho chodu a byť pripravený pre chod s jednotkami hasičského záchranného zboru pomocou zvláštneho ovládania z kabíny výťahu.

Bezchybná funkčnosť výťahu i pri výpadku energie je zaistená alternatívnym napájaním.

Pre strom poruchových stavov A je PFD určené podobne ako v kapitole 5.2, lebo ide o klasický požiarny hlásič IQ8Quad.



Obr. 5-5 Strom poruchových stavov pre sekciu prepnutia výťahu z normálneho chodu.

Tabuľka 26

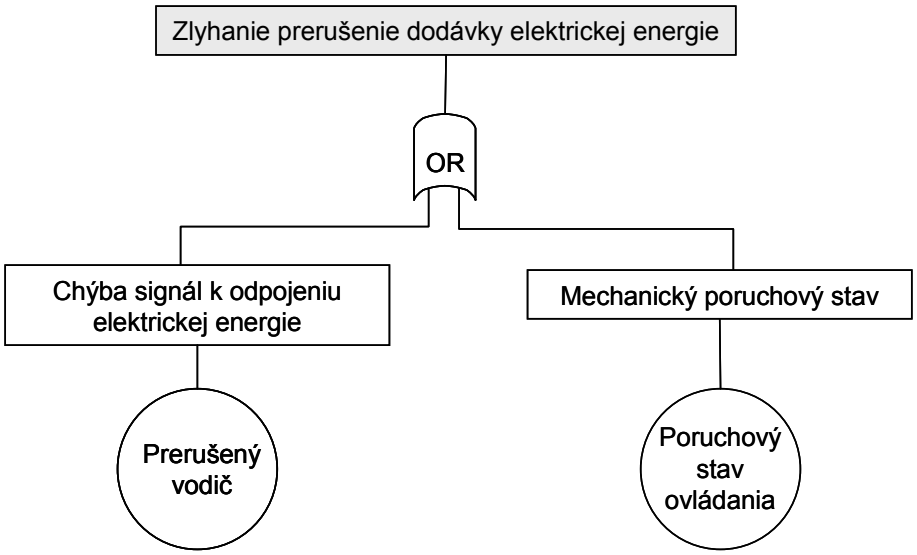
Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Poruchový stav vyslania signálu strom poruchových stavov A	$8{,}86.10^{-8}$	Výpočet
P2 P5 - Poruchový stav prenosu signálu	$1{,}14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P3 - Poruchový stav obvodu 1	$2{,}94.10^{-7}$	Výpočet
P4 - Poruchový stav obvodu 2	$2{,}48.10^{-7}$	Výpočet
P5 - Mechanická závada	$1{,}0.10^{-7}$	Výpočet

Pravdepodobnosti vzniku poruchy na sekcií prepnutie výťahu do bezpečnostného režimu boli stanovené ako uvádza tabuľka (Tabuľka 26). Pre subsystém prepnutie výťahu do bezpečnostného režimu potom dostávame konečný výsledok PFD=$4{,}17.10^{-7}$

5.4.5 Určenie PFD pre sekciu prerušenia dodávky elektrickej energie

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Neprerušenie dodávky elektriky	Mechanická porucha príslušného relé Porucha signalizačného vedenia	Vznik skratu	Kontrola napájania	Signálny systém

Systém na odpojenie príslušnej sekcie budovy od rozvodu elektrickej energie je ovládaný centrálne zo sekcie ohlasovne požiaru. Akonáhle dôjde k odpojeniu príslušnej sekcie od elektrického prúdu, spustí sa núdzové napájanie príslušných zariadení, ako napríklad núdzové osvetlenie a iné (sekcia náhradného zdroja elektrickej energie).



Obr. 5-6 Strom poruchových stavov pre sekciu prerušenie dodávky elektrickej energie.

Tabuľka 27

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Poruchový stav prenosu signálu	$1{,}14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Mechanický poruchový stav relé	$7{,}21.10^{-6}$	Výpočet

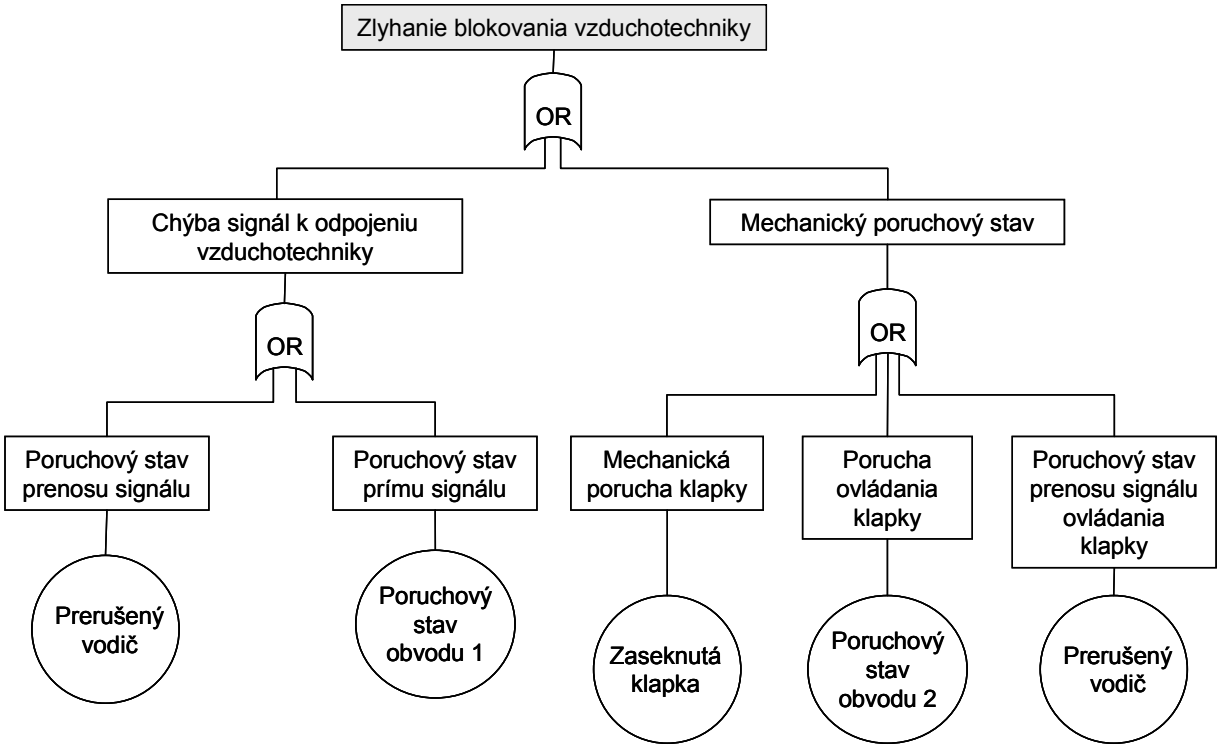
Pravdepodobnosti vzniku poruchy na sekcií prerušenie dodávky elektrickej energie boli stanovené ako uvádza tabuľka (Tabuľka 27). Pre zníženie pravdepodobnosti vzniku mechanickej poruchy relé, môže byť zariadenie opatrené signalizačnou kontrolou. V tomto

prípade sa zatiaľ s takýmto opatrením neráta. Pre subsystém prerušenie dodávky elektrickej energie potom dostávame konečný výsledok PFD=7,32.10^{-6}

5.4.6 Určenie PFD pre sekciu blokovanie vzduchotechniky

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Neodpojenie systému	Porucha signalizačného vedenia	Šírenie splodín horenia do priestoru	žiadne	Signálny systém
Klapky ostávajú otvorené	Mechanická porucha klapiek		žiadne	

Systém na odpojenie príslušnej sekcie budovy od rozvodu vzduchotechniky je ovládaný centrálne zo sekcie ohlasovne požiaru. Ak dôjde v príslušnej sekcií k požiarnemu poplachu, nastane odpojenie vzduchotechniky od rozvodu elektrickej energie s následným uzatvorením potrubných rozvodov (aby nedošlo k samovoľnému šíreniu škodlivých splodín horenia, resp. hasenia). K tomuto by nemalo dôjsť, ak došlo k odpojeniu príslušného úseku od elektrickej energie.



Obr. 5-7 Strom poruchových stavov pre sekciu blokovanie vzduchotechniky.

Tabuľka 28

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 P5 - Poruchový stav prenosu signálu	$1,14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Poruchový stav príjmu signálu	$2,53.10^{-7}$	Výpočet
P3 - Zaseknutá klapka	$2,18.10^{-4}$	Expertný úsudok
P4 - Porucha ovládania klapky	$5,32.10^{-6}$	Výpočet

Pravdepodobnosti vzniku poruchy na sekcií blokovanie vzduchotechniky boli stanovené ako uvádza tabuľka (Tabuľka 28). V samotnom systéme sa nachádza viacero klapiek, ktoré uzatvárajú prívod vzduchotechniky. Vo výpočtoch sa uvažuje len s jednou klapkou z dôvodu, že požiar vznikne len v jednej miestnosti v ktorej bude následne lokalizovaný. Ak by sme chceli vypočítať pravdepodobnosť vzniku poruchy na všetkých klapkách, následne by sa táto pravdepodobnosť vzniku poruchy zvýšila. Pre subsystém blokovanie vzduchotechniky potom dostávame konečný výsledok PFD=$2,24.10^{-4}$

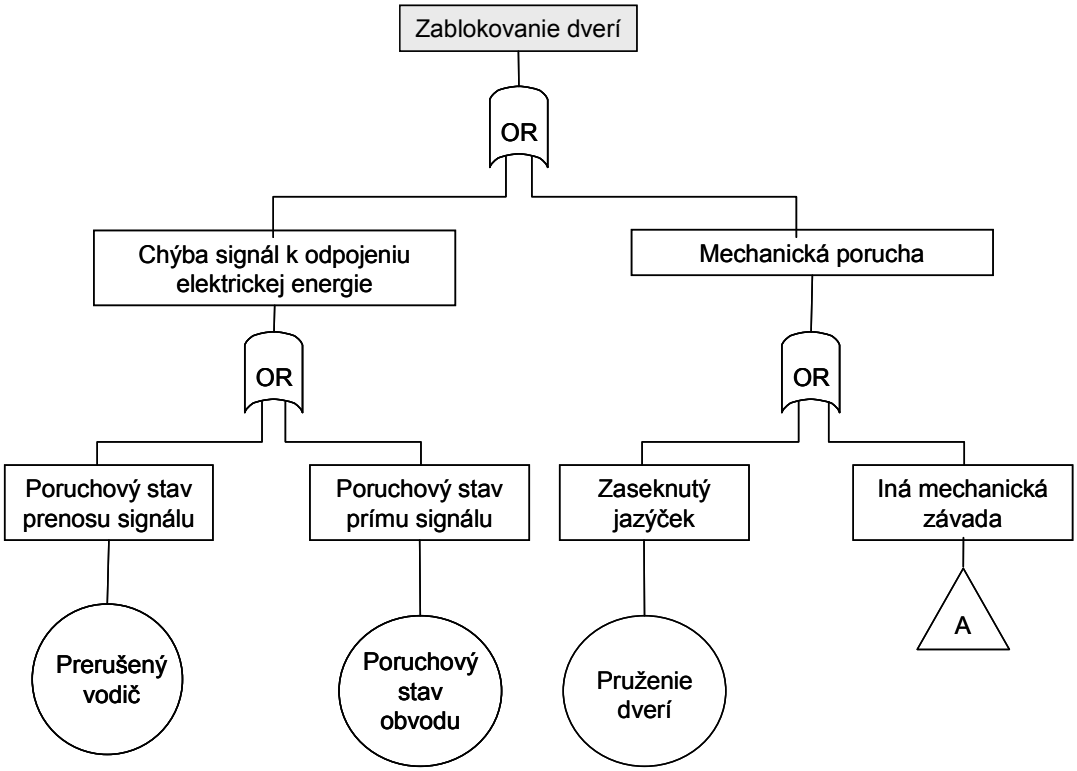
5.4.7 Určenie PFD pre sekciu odblokovanie zámkov

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Zaseknutý zámok	Mechanická porucha Nedošlo k odpojeniu od napájania	Uväznenie osôb v určitom sektore budovy		Bezpečnostná fólia na skle. Použiť zámok so signalizáciou zabezpečenia

Inverzný zámok, pre požiarne dvere je "zablokovaný", pokiaľ je k nemu privádzaný elektrický prúd. Zámky sú napájané cez záložný zdroj. Ak má byť zámok pri kritickej situácií odblokovaný, musí sa prerušiť prívodu elektrického prúdu aj zo záložného zdroja.

Elektrické zámky udržia požiarne dvere zablokované maximálne počas dvoch hodín, pričom odolajú teplote do 1150°C

Elektrické zámky pre požiarne dvere, sa využívajú pre úplné zablokovanie dverí a izolovanie požiarom zasiahnutej zóny na čo najdlhšiu dobu. Zabráni sa tak prenikaniu a šíreniu ohňa a dymu a umožní sa evakuácia osôb bez paniky. Sú napájané 12 VDC.



Obr. 5-8 Strom poruchových stavov pre sekciu odblokovanie zámkov.

Tabuľka 29

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Poruchový stav prenosu signálu	$1{,}14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Poruchový stav príjmu signálu	$2{,}53.10^{-7}$	Výpočet
P3 - Mechanická porucha - zaseknutý jazýček	$7{,}42.10^{-4}$	Štatistické údaje
P4 - Iná mechanická porucha	$3{,}26.10^{-5}$	FTA A

Pravdepodobnosť vzniku poruchy na sekcií odblokovania zámkov boli stanovené expertnými úsudkami, resp. výpočtom a sú uvedené v tabuľke (Tabuľka 29). Pre subsystém odblokovania zámkov potom dostávame konečný výsledok PFD=$7{,}75.10^{-4}$

5.4.8 Určenie PFD pre sekciu odvod tepla a spalín

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Nefunkčnosť vetracích klapiek	Zaseknutá vetracia klapka Porucha ovládania	Nedostatočné odvetranie objektu		Snímač polohy vetracej klapky

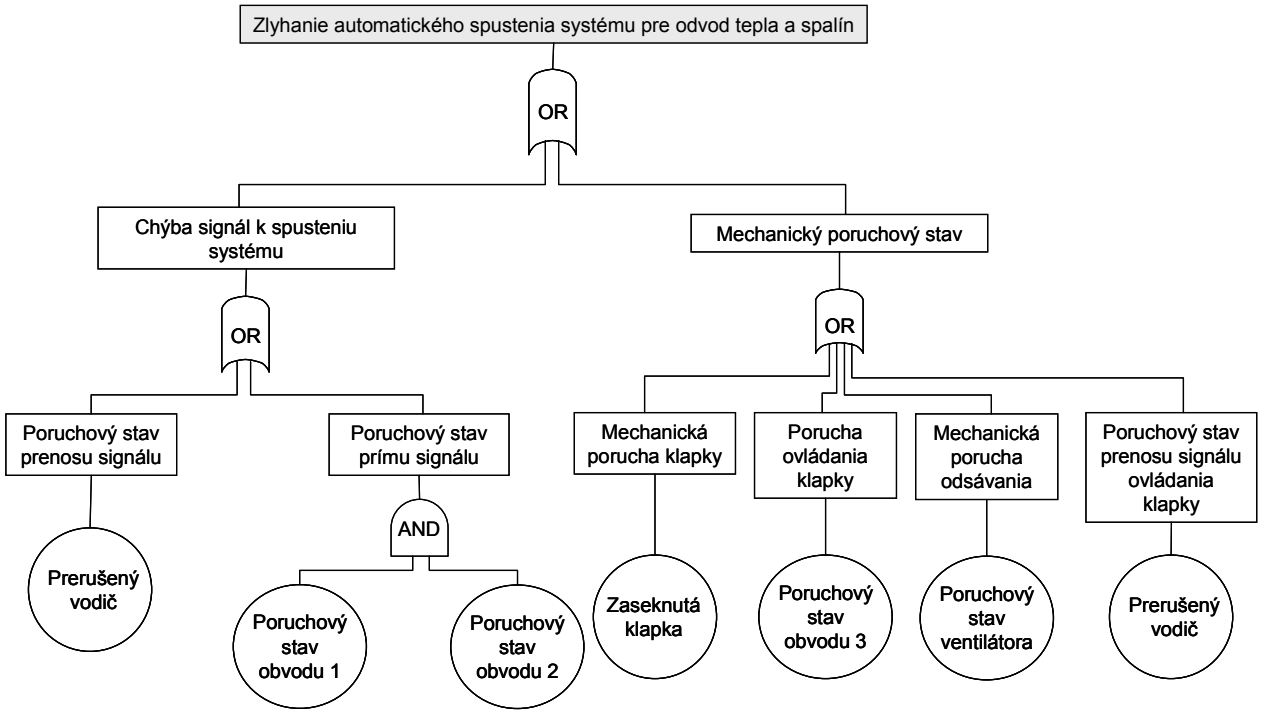
	klapiek			
Nefunkčné odvetranie	Porucha ventilátora Prerušené vedenie	Nedostatočné odvetranie objektu	Snímač napájania	Snímač otáčok motora Záložný zdroj energie

Zariadením na odvod dymu a tepla možno označiť riadene odsávanie produktov horenia, tzn, tepla, dymu, jedovatých plynov a vodnej pary, ktorá vzniká pri hasení vodou. Zariadenie pre odvod dymu a tepla zahŕňa okrem odvodov dymu a tepla taktiež prvky pre prívod čerstvého vzduchu a dymovej závesovej steny. Odvetrávanie je automatické preto, že v mnohých prípadoch sa nemožno spoliehať na rýchly zásah ľudského faktora, zvlášť v prípadoch, keď požiar vypukne v noci. Odvetrávanie sa spojí s ostatným protipožiarnym vybavením uvádza do chodu dymovými alebo tepelnými detektormi, prípadne elektrickou požiarnou signalizáciou.

Zariadenie na odvod dymu a tepla samo o sebe požiar neuhasí, ale v spojení s ostatnými faktormi znižuje straty a škody spôsobené požiarom tým, že:

- odvádza dym, vodnú paru a teplo von z objektu a tým pomáha udržať vrstvu relatívne čistého vzduchu nad podlahou.
- vymedzí dym do vrstvy, ktorá sa udržiava pod stropom, obmedzí jeho ďalšie šírenie do priľahlých priestorov. Nedochádza k nadmernému zvyšovaniu teploty a následnému samovznieteniu stavebných prvkov
- systém odvodu dymu a tepla znižuje nebezpečenstvo explózie náhlym znížením nespálených plynov so vzduchom;

V priebehu požiaru musí byť odvetrávacie zariadenie uvedené do činnosti čo najskôr a nikdy nesmie dôjsť k poruche jeho funkcie. Proti zlyhaniu je každé takéto zariadenie zaistené tepelnou poistkou. Na otváranie zariadenia pre prirodzený odvod dymu a tepla, sa najbežnejšie používa pneumatický ovládací systém. V objektoch, kde nie je vhodné zaviesť rozvod stlačeného vzduchu, sa klapky ovládajú pomocou elektromotora v kombinácii s pružinou. Elektrické ovládanie vyžaduje zapájanie samostatným nezávislým zdrojom elektrického prúdu. To isté platí pre požiarne ventilátory, pri ktorých motor ventilátora musí byť napojený na nezávislý elektrický zdroj energie.



Obr. 5-9 Strom poruchových stavov pre sekciu odvod tepla a spalín.

Tabuľka 30

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 P7 - Poruchový stav prenosu signálu	$1{,}14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Poruchový stav obvodu 1	$2{,}94.10^{-7}$	Výpočet
P3 - Poruchový stav obvodu 2	$2{,}48.10^{-7}$	Výpočet
P4 - Zaseknutá klapka	$4{,}12.10^{-5}$	Expertný úsudok
P5 - Poruchový stav obvodu 3	$2{,}55.10^{-7}$	Výpočet
P6 - Poruchový stav ventilátora	$7{,}28.10^{-5}$	Expertný úsudok

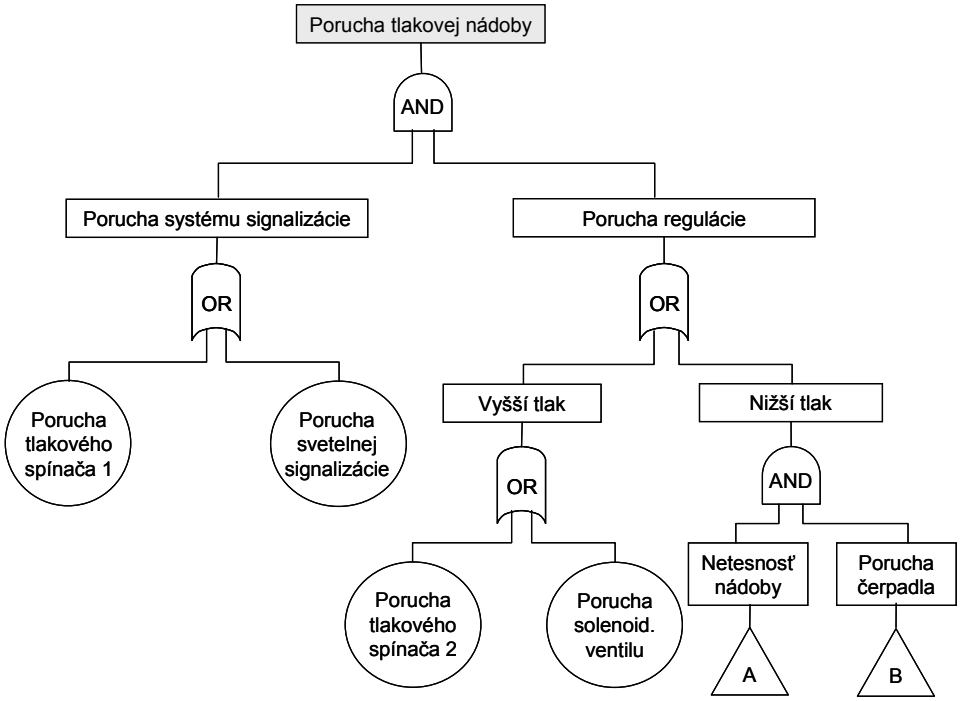
Mechanická časť daného zariadenia je dosť náročná. Preto neuvádzam výpočet jednotlivých častí zariadenia. Ďalšie pravdepodobnosti vzniku poruchy na sekcií odvod tepla a spalín boli stanovené výpočtami, resp. expertnými úsudkami a sú uvedené v tabuľke (Tabuľka 30). Pre subsystém odvod tepla a spalín, potom dostávame konečný výsledok PFD=$1{,}14.10^{-4}$

5.4.9 Určenie PFD pre sekciu tlaková nádoba

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Nižší tlak	Porucha regulácie	Nedostatočný hasiaci efekt	Tlakový spínač	
Vyšší tlak	Porucha regulácie	Poručenie nádoby	žiadne	Inštalácia poistného ventilu

Pozostáva z vodného tlakového zdroja, potrubných rozvodov, ventilových staníc, poplachového a monitorovacieho zariadenia a rozvádzacieho potrubia so sprinklerovými hlavicami pevne pripevneného k stavebnej konštrukcii.

Sprinklerová hlavica sa pri dosiahnutí otváracej teploty samočinne otvorí, čím dôjde k poklesu tlaku v rozvodnom potrubí, následnému otvoreniu ventilovej stanice a spusteniu sprinklerového stabilného hasiaceho zariadenia. Bezprostredne po otvorení hlavice dochádza u mokrej sústavy k výtoku vody vo forme sprchového prúdu. U suchej sústavy sa najskôr vytlačí vzduch a potom dôjde k výstreku vody. Pritom sa otvárajú len hlavice , ktoré sú nad ohniskom požiaru, čím dochádza len k haseniu nevyhnutne nutnej plochy.
Používajú sa v objektoch a technologických zariadeniach s rýchlym uvoľnením tepla, hotely, garáže, textilné závody, mlyny, divadlá, konferenčné sály, vysokoregálové sklady, atď.



Obr. 5-10 Strom poruchových stavov pre sekciu tlaková nádoba.

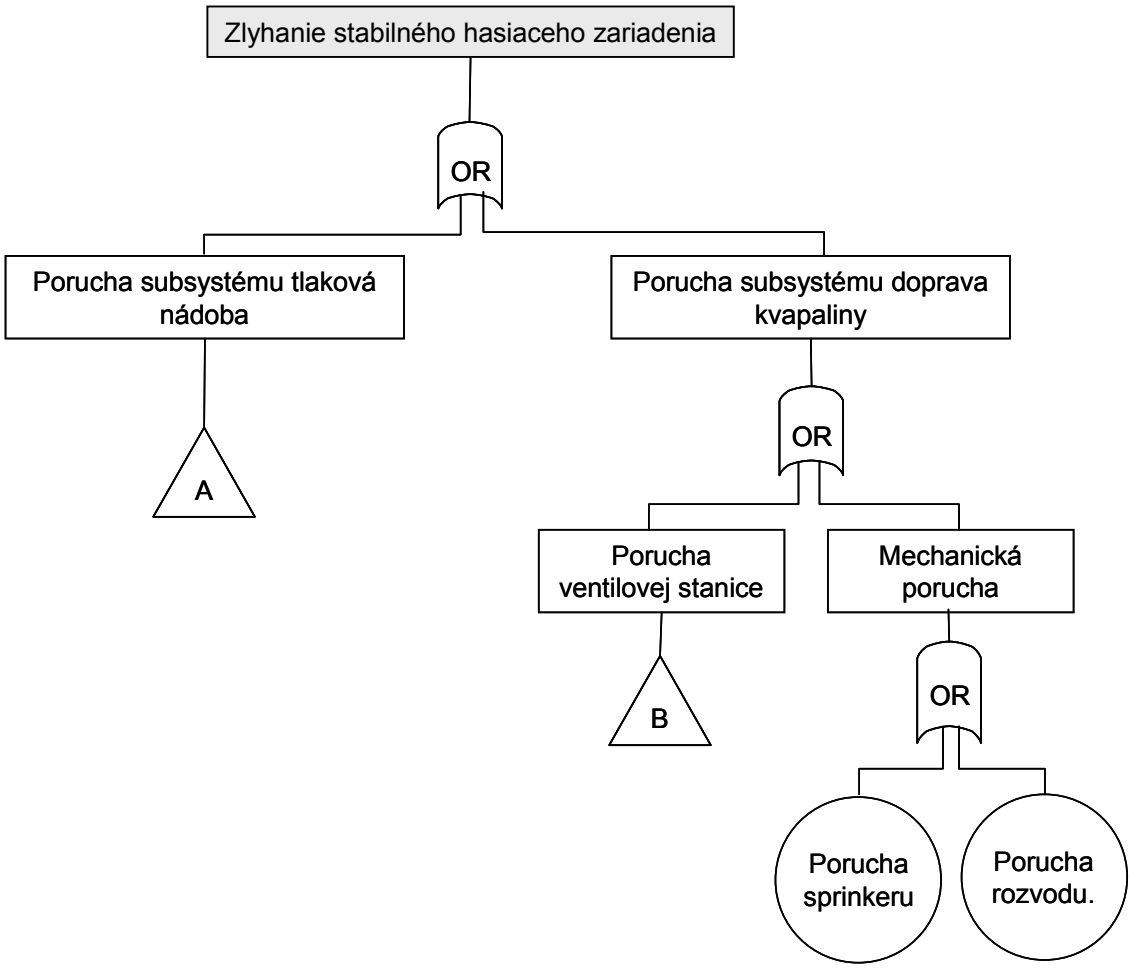
Tabuľka 31

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Porucha tlakového spínača1	$8{,}06.10^{-5}$	Výpočet
P2 - Porucha svetelnej signalizácie	$4{,}56.10^{-6}$	Štatistické dáta
P3 - Porucha tlakového spínača2	$8{,}06.10^{-5}$	Výpočet
P4 - Porucha solenoidového ventilu	$8{,}69.10^{-5}$	Výpočet
P5 - Netesnosť tlakovej nádoby	$1{,}31.10^{-4}$	Expertný úsudok FTA A
P6 - Porucha čerpadla	$4{,}14.10^{-4}$	Expertný úsudok FTA B

Predpoklad že na nádobe vznikne mechanická porucha by mal za následok stratu tlaku v systéme. Ďalšie pravdepodobnosti vzniku poruchy na sekcií tlaková nádoba boli stanovené expertnými úsudkami a štatistickou analýzou. Sú uvedené v tabuľke (Tabuľka 31). Pre subsystém tlaková nádoba, potom dostávame konečný výsledok PFD=1,43.10^{-8}

5.4.10 Určenie PFD pre sekciu doprava kvapaliny do sprinkerov

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Nižší prietok	Porucha regulácie Upchaný prívod kvapaliny	Nedostatočný hasiaci efekt	Mokrá ventilová stanica	Inštalácia regulácie prietoku na prívode kvapaliny Pravidelná údržba
Nižší tlak	Prasknutý prívod alebo chybný sprinker	Únik kvapaliny	Tlakový spínač	Pravidelná údržba



Obr. 5-11 Strom poruchových stavov pre sekciu doprava kvapaliny.

Tabuľka 32

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Porucha subsystému tlaková nádoba	$1{,}43.10^{-8}$	FTA (tlaková nádoba)
P2 - Porucha ventilovej stanice	$2{,}81.10^{-6}$	FTA B
P3 - Porucha sprinkeru	$6{,}91.10^{-7}$	Údaje od výrobcu
P4 - Porucha rozvodu	$7{,}21.10^{-7}$	Expertný úsudok

Sprinker je mechanické zariadenie nezávislé na elektronike, ktoré nie je možné otestovať. Rozvod hasiaceho média je realizovaný tlakovými hadicami, ktorých pravdepodobnosť vzniku poruchy je minimálna. Jediné riziko je v spojoch jednotlivých súčastí systému. Ďalšie pravdepodobnosti vzniku poruchy na sekcií doprava kvapaliny boli stanovené expertnými úsudkami a údajmi z iných stromov porúch. Sú uvedené v tabuľke (Tabuľka 32). Pre subsystém doprava kvapaliny, potom dostávame konečný výsledok PFD=$4{,}24.10^{-6}$

5.4.11 Určenie PFD pre sekciu vedenia požiarnej signalizácie

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Strata signálu z príslušného prvku	Prerušené vedenie napájania. Prerušené vedenie dát	Nefunkčnosť EPS	Záložný zdroj napájania	Použitie zbernicových rozvodov signálu

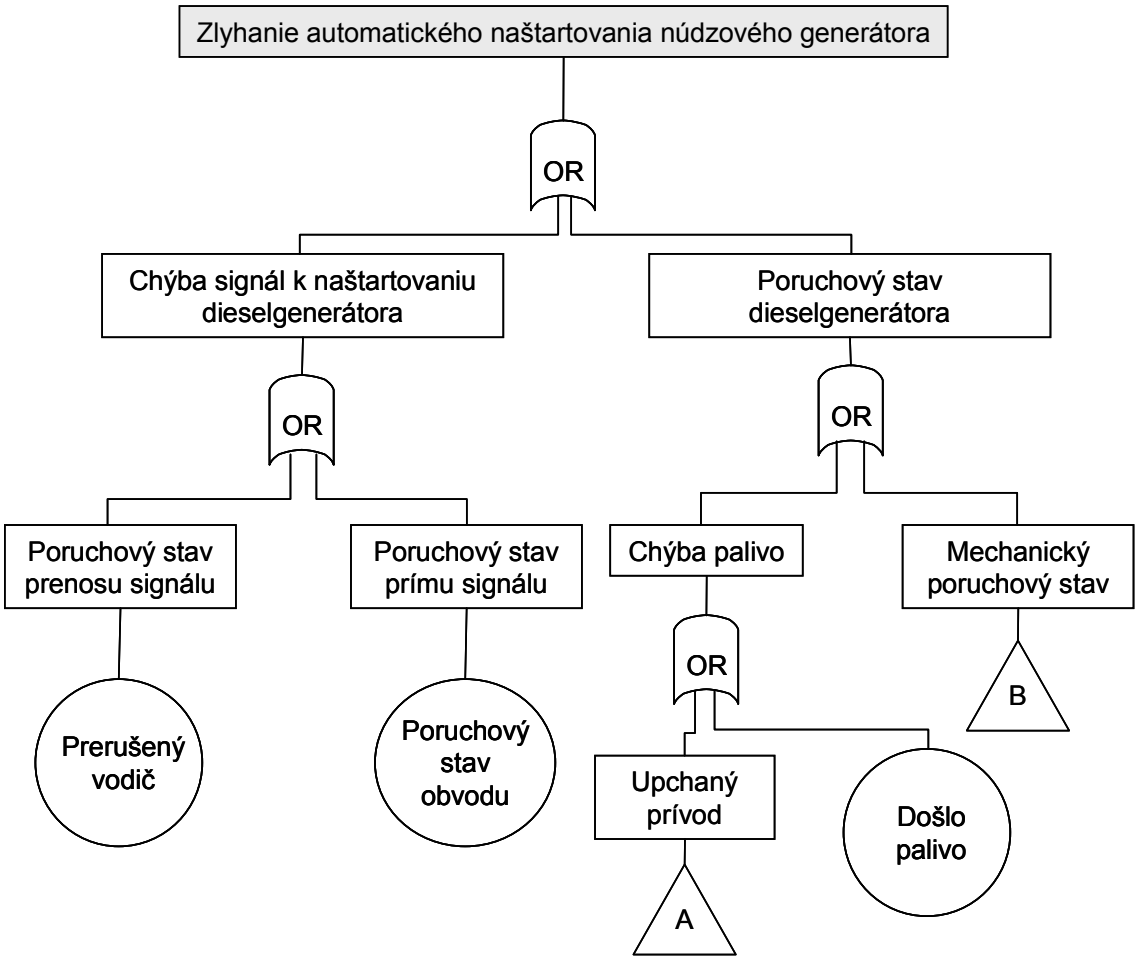
Inštalácia káblových rozvodov požiaru odolnými káblami s min. 30 minútovou odolnosťou Tak ako pri nezávislosti na výpadku napájania požiarno-evakuačného rozhlasu po dobu min. 30 minút, musia byť aj káblové rozvody reproduktorových liniek a samotného prívodu napájania 230 VAC realizované káblami Funkčnými počas požiaru po dobu minimálne 30 minút podľa STN IEC 60331. Pre sieťové napájanie 230 VAC.

Pravdepodobnosť vzniku poruchy na sekcií vedenie požiarnej signalizácie je stanovené expertným úsudkom Pre tento subsystém je stanovená pravdepodobnosť vzniku poruchy PFD=$1{,}14.10^{-7}$.

5.4.12 Určenie PFD pre sekciu náhradného zdroja energie

Odchýlka	Príčina	Následky	Existujúce opatrenia	Doporučenia
Chýba signál pre naštartovanie generátora	Prerušené vedenie	Odpojenie druhotného napájania	žiadne	Použitie vedenia ako pri EPS
Nenaštartovanie generátora	Mechanická závada Nedostatok paliva			Pravidelná údržba

Ako náhradný zdroj energie pri slaboprúdových zariadeniach, čiže do 12V DC, sa používa záložná batéria. V tomto prípade ako náhradný zdroj energie, 380V AC, sa používa dieselgenerátor striedavého napätia, ktorý sa dá použiť na chod výťahu a iných zariadení na 220V.



Obr. 5-12 Strom poruchových stavov pre sekciu náhradného zdroja energie.

Tabuľka 33

Udalosť	Frekvencia, alebo pravdepodobnosť	Zdroj dát
P1 - Poruchový stav prenosu signálu	$1{,}14.10^{-7}$	Expertný úsudok odvodený z celkovej pravdepodobnosti vzniku požiaru v budove
P2 - Poruchový stav obvodu	$2{,}82.10^{-7}$	Výpočet
P3 - Upchaný prívod paliva	$7{,}25.10^{-5}$	FTA A
P4 - Nedostatok paliva	$2{,}13.10^{-4}$	Expertný úsudok
P5 - Mechanický poruchový stav	$1{,}71.10^{-4}$	FTA B

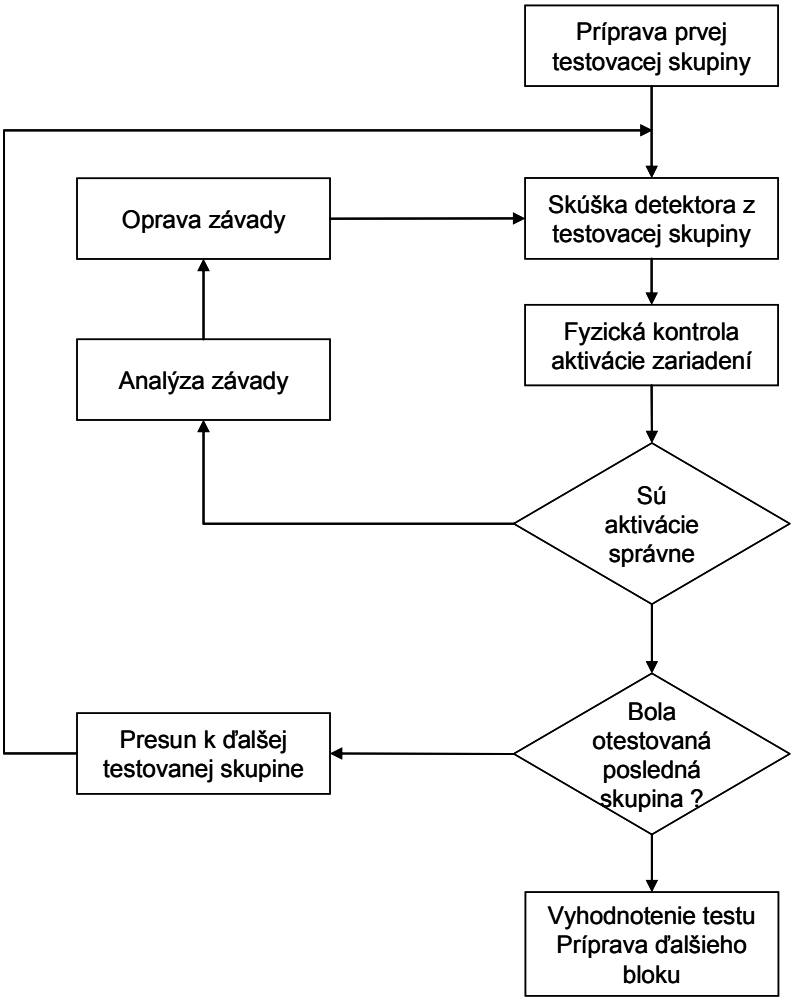
Pravdepodobnosť vzniku poruchy na sekcií náhradného zdroja energie boli stanovené expertnými úsudkami, resp. výpočtom a sú uvedené v tabuľke (Tabuľka 33). Pre subsystém náhradného zdroja energie potom dostávame konečný výsledok PFD=$4{,}57.10^{-4}$

5.5 Reálny scenár testovania softvéru požiarnej ústredne

V praxi je nevyhnutné podrobiť systém akceptačnému testovaniu. V prvom rade sa testuje schopnosť systému zachovať si funkčnosť pri výpadku sieťového napájania po minimálne stanovenú dobu. Pri tom to teste sa postupuje tak , že sa vypnú všetky body napájania systému. Po tomto vypnutí sa sleduje kedy systém ohlási výpadok napájania, a či správne rozpozná výpadok napätia na všetkých bodoch napájania. Pri tomto stave sa aktivujú všetky náväzné zariadenia systému a sleduje sa doba, po ktorú systém dokáže zabezpečiť aktiváciu týchto zariadení. Po uplynutí stanovenej doby sa opätovne zapne napájanie všetkých napájacích bodov systému a sleduje sa čas, za ktorý hlásenia porúch zmiznú. Následne sa testuje schopnosť detekcie požiaru hlásičmi spolu s reakciou náväzných zariadení podľa vopred vypracovanej tabuľky. Táto tabuľka prehľadne znázorňuje aké majú nasledovať reakcie na hlásenie požiaru z danej skupiny prvkov. Rovnako znázorňuje s akým časovým oneskorením majú byť reakcie spínané. Pri tomto druhu testovania je nutné otestovať funkciu každej skupiny hlásičov. V prípade tohto objektu je testovanie rozdelené na 2 bloky a 20 vybudení požiarom. Každý blok obsahuje všetky skupiny z konkrétneho dymového úseku. Takéto členenie uľahčuje vykonanie testu, nakoľko sa pracovník vykonávajúci aktiváciu hlásičov skúšobným plynom nemusí pohybovať po všetkých podlažiach. Takýmto spôsobom otestovania sa v maximálnej miere zamedzí prehliadnutiu chyby v obslužnom softvéri ústredne. V skutočnom prostredí by trvalo takéto testovanie dvom pracovníkom približne 1 hodinu.

Najčastejšie chyby softvéru požiarnych ústrední sú:

Chyba	Príčina	Následok	Oprava
Aktivácie zariadení sa vykonávajú s nesprávnym oneskorením	Nesprávne nastavenie poplachovej reakcie	Pri aktivácií tlačidlového hlásiča sa neaktivujú zariadenia okamžite.	Kontrola nastavenia reakcie tlačidlových hlásičov (reakcia-priamo/oneskorene)
Na ústredňu príde stav požiar, ale žiadne zariadenia sa neaktivujú	Skupina hlásičov nie je pridelená do žiadneho sektoru hlásičov	Nefunkčnosť požiarnotechnických zariadení. Možné ohrozenie zdravia a majetku	Pridelenie skupiny do sektoru hlásičov
	Výstup na zariadenie nie je pridelené do žiadneho sektoru ovládania		Pridelenie výstupu do sektoru ovládania
	Výstup je nastavený na nesprávne relé koppleru		Prekontrolovanie zapojenia vodičov na kopplery
Na ústredňu príde stav požiar, ale aktivujú sa nesprávne zariadenia	Hlásič je priradený do nesprávnej skupiny	Nesprávna reakčná schopnosť systému	Prekontrolovanie hlásičov a ich rozdelenie v skupinách
	Skupina hlásiča je nesprávne zatriedená do sektoru hlásičov		Prekontrolovanie skupín hlásičov a ich umiestnenie v sektoroch
Na ústredňa neprichádza žiadny stav hlásiča	Hlásič nie je zapojený na kruhu esserbus®	Nefunkčnosť detekcie jedného alebo viac detektorov	Kontrola kabeláže a topológie zapojenia



Obr. 5-13 Príklad otestovania softvéru pre skupinu hlásičov.

Pri tomto teste bloku sa pomocou skúšobného plynu aktivuje automatický dymový hlásič patriaci do konkrétnej skupiny hlásičov. Po detekcií tohto stavu ústredňou musia nasledovať aktivácie zariadení. Zoznam zariadení ako aj časové oneskorenia sú potom spracovávané v tabuľke aktivácií. Po časovom oneskorení 300sekúnd bez spätného nastavenia ústredne musia nasledovať aktivácie:

- odblokovanie automatických dverí
- zatvorenie uzáverov plynu
- zatvorenie uzáverov elektriny
- signál horí do systému MaR
- zastavenie núteného vetrania vzduchotechniky
- spustenie núteného vetrania
- spustenie evakuačného hlásenia
- spustenie výťahov do núdzovej polohy

Ak prebehnú aktivácie v poriadku môže sa pristúpiť k testovaniu ďalšej skupiny ak nie, musí sa lokalizovať a odstrániť chyba a test skupiny zopakovať.

5.5.1 Minimalizácia počtu testov na maximálne otestovanie systému

Pri iných typoch budov a inej štruktúre podlaží a priestorov sa môže počet nutných testov mnohonásobne zvýšiť. Takéto testovanie by už bolo časovo náročné a nie úplne prehľadné. S tohto dôvodu je nutné minimalizovať počet testov. Pri tomto druhu testu sa už netestuje každá skupina samostatne ale iba jedna skupina z daného požiarneho úseku. Rozdelenie týchto úsekov však musí kopírovať členenie skupín v sektoroch hlásičov. Testovanie pozostáva z náhodného výberu skupiny hlásičov z dymového úseku a vybudenia stavu požiar na hlásiči. Pri takomto druhu testovania je nutná kontrola rozčlenenia skupín hlásičov požiaru do sektorov hlásičov. Je to z dôvodu, že sa netestuje každá skupina samostatne a nedá sa vylúčiť, že niektorá zo skupín nie je priradená do sektoru hlásičov. K tomuto účelu postačuje jednoduché pravidlo a to, počet skupín hlásičov požiaru načítaných na linkách hlásičov musí byť totožný s počtom skupín priradených v sektoroch hlásičov.

Výsledkom takejto minimalizácie je zredukovanie počtu testov na 2. Takýto počet sa dá uskutočniť v 1 testovacom bloku. Takéto testovanie by v reálnom prostredí trvalo necelých 10 minút.

Počet testov a čas testovania závisí od zložitosti navrhnutého systému, jeho členenia a použitia následných spínacích zariadení.

5.6 Zhodnotenie riešenia

Pre výpočet priemernej pravdepodobnosti vzniku poruchy pre požiarnu signalizáciu bez následných spínacích zariadení som zvolil metódu bezporuchovostných blokových schém, na základe ktorých sa dá požiarny systém posúdiť ako celok. Priemerná pravdepodobnosť vzniku poruchy pri vyžiadaní bezpečnostnej funkcie pre navrhnutú elektrickú požiarnu signalizáciu bez následných spínacích zariadení je $9{,}69.10^{-4}$, čo ju radí do kategórie SIL 3 pre systémy v režime nepravidelnej prevádzky. Aj keď požiarna signalizácia je v 24 hodinovom režime stráženia, nie je pravdepodobnosť vzniku požiaru v danom objekte taká, aby sme ju posudzovali ako pre režim nepretržitej prevádzky. Ako vidno z tabuľky (Tabuľka 15), najvyššie percento využitia PFD je v podpornom subsystéme požiarnej ústredne, ktorý vykazuje najväčšiu pravdepodobnosť vzniku poruchy. Tento subsystém je však navrhnutý pre architektúru 1oo1, čo je však v praxi nerealizovateľné. Jeho hodnota PFD je $9{,}52.10^{-4}$. Pri

pridaní záložného zdroja (batéria) by tento subsystém pracoval s architektúrou 1oo2 a teda aj hodnota PFD by sa pohybovala rádovo nižšie. Konkrétne by bola $9{,}24.10^{-5}$. A teda aj celková hodnota PFD pre elektrickú požiarnu signalizáciu by bola nižšia $1{,}09.10^{-4}$, čo je približne 10 násobne nižšia a pri nepatrnom zvýšení životnosti toroidného transformátora by sa mohla posunúť do kategórie SIL 4.

Pri použití požiarneho systému s následnými spínacími zariadeniami je určovanie pravdepodobnosti vzniku poruchy dosť obtiažne pomocou metódy bezporuchovostných blokových schém. Preto v tomto prípade bola použitá metóda stromov poruchových stavov pre jednotlivé sekcie systému. Pri systéme požiarnej ústredne s následnými spínacími zariadeniami boli pridané do systému dva kopplery. Ich pravdepodobnosť vzniku poruchy (Tabuľka 20 a Tabuľka 23) je nutné pripočítať k pravdepodobnostiam vzniku porúch jednotlivých spínacích zariadení, ktoré ovládajú. Kopplery v tomto systéme majú za úlohu zopnúť jednotlivé následné časti systému. Takéto riešenie je variabilné, to značí, že pri návrhu môžeme použiť ďalšie ľubovoľné zariadenie. Každé ďalšie pridanie spínacieho zariadenia do systému, však zvyšuje pravdepodobnosť vzniku poruchy systému ako celku. Celkovú pravdepodobnosť vzniku poruchy pri takomto systéme potom nemôžeme vypočítať súčtom jednotlivých pravdepodobností, lebo ich použitie nemá vplyv na funkciu ohlásenia požiaru. Niektoré z týchto zariadení majú skôr za úlohu skrátiť čas potrebný napríklad na evakuáciu osôb z budovy, eliminovať následky požiaru, resp. minimalizovať škody na majetku.

V tabuľke (Tabuľka 34) sú uvedené jednotlivé pravdepodobnosti vzniku poruchy následných spínacích zariadení, používaných v EPS. Z tejto tabuľky je vidno, že najslabším členom celého systému je sekcia odblokovania zámkov, ktorá však nemá priamy vplyv na celkovú bezpečnosť. Používanie tohto zariadenia je veľmi časté a preto aj porucha na tomto zariadení sa dá skôr identifikovať a odstrániť ako pri ostatných spínacích zariadeniach. Jedným z opatrení ako umožniť evakuáciu z takýchto priestorov je použitie kľučky zo strany miestnosti. Horšie je na tom sekcia blokovanie vzduchotechniky a sekcia odvodu tepla a spalín, ktoré užšie súvisia so vznikom požiaru. Tieto sekcie sa používajú až pri vzniku požiaru a preto odhalenie vzniku poruchy na týchto zariadeniach je možné len pravidelnými kontrolami a revíziami.

Ďalším kritickým členom je sekcia náhradného zdroja energie. Tento sa však používa len pre zariadenia pracujúce s napätím 220V. Väčšina následných spínacích zariadení pracuje

s napätím 12V. Pri týchto zariadeniach je ako náhradný zdroj energie použitý akumulátor, ktorý sa mení v intervale každé dva roky.

Tabuľka 34

Sekcia	Údaje	PFD_{SYS}
Hlásič požiaru	Tabuľka 24	$3{,}65.10^{-7}$
Prerušenia dodávky plynu	Tabuľka 25	$8{,}7.10^{-5}$
Prepnutia výťahu z normálneho chodu	Tabuľka 26	$4{,}17.10^{-7}$
Prerušenia dodávky elektrickej energie	Tabuľka 27	$7{,}32.10^{-6}$
Blokovania vzduchotechniky	Tabuľka 28	$2{,}24.10^{-4}$
Odblokovania zámkov	Tabuľka 29	$7{,}75.10^{-4}$
Odvodu tepla a spalín	Tabuľka 30	$1{,}14.10^{-4}$
Tlaková nádoba	Tabuľka 31	$1{,}43.10^{-8}$
Dopravy kvapaliny do sprinkerov	Tabuľka 32	$4{,}24.10^{-6}$
Vedenia požiarnej signalizácie		$1{,}14.10^{-7}$
Náhradného zdroja energie	Tabuľka 33	$4{,}57.10^{-4}$

Norma STN/EN 54 uvádza pravdepodobnosť vzniku požiaru 1.10^{-6} na m^2 za rok, pričom pravdepodobnosť chyby budovy je $1{,}3.10^{-6}$ za rok a pravdepodobnosť chyby pri evakuácii osoby pri normálnej evakuácii je $1{,}3.10^{-4}$ za rok. Z tohto je možné odvodiť, že pravdepodobnosť vzniku požiaru a teda aj pravdepodobnosť vzniku poruchy na požiarnom zariadení, závisí od veľkosti budovy a teda aj od počtu členov elektrickej požiarnej signalizácie.

Záver

Vstupom do Európskej únie sú kladené vysoké nároky, hlavne na dodržiavanie európskych noriem, spoľahlivosť, dlhú životnosť, nízku cenu a neposlednom rade na bezpečnosť. Preto je snaha navrhovať také zariadenia, ktoré by pri riadení minimalizovali vplyv ľudského faktoru. Čo má za následok zvyšovanie stupňa automatizácie riadenia. Medzi dominantné oblasti s vyšším stupňom automatizácie riadenia patria oblasti jadrových technológií, potravinárskej a chemickej výroby, dopravné systémy a v neposlednom rade aj systémy ochrany a zabezpečenia budov, ako napríklad EPS Tým že autor v minulosti spolupracoval s firmou, zaoberajúcou sa bezpečnostnými systémami (požiarnymi, kamerovými, prístupovými a inými) vznikla aj táto téma dizertačnej práce, ktorá poukazuje, že nestačí len navrhnúť a realizovať bezpečnostný systém, ale je nutné aj posúdiť, či tento návrh aj vyhovuje prísnym požiadavkám dnešnej doby. Jednou z noriem, ktorá sa zaoberá funkčnou bezpečnosťou elektrických, elektronických a programovateľných elektronických bezpečnostných systémov je norma IEC EN 61508.

Úvodná časť práce je zameraná na testovanie, ktoré je neoddeliteľnou časťou celkového životného cyklu riadiacich systémov. Pojem testovania sa taktiež vyskytuje v už spomínanej norme IEC EN 61058, ktorá sa nezaoberá testovaním ako takým, ale testovanie, okrem iného, tu figuruje ako podklad pre výpočty slúžiace pre určovanie bezpečnosti riadiacich systémov. Ďalšia časť práce je zameraná na bezpečnosť, kde sú zadefinované pojmy s ňou súvisiace, ako chyba, porucha, nebezpečenstvo a riziko. S týmito pojmami súvisia aj metódy analýzy rizika, ktorým je venovaná podstatná časť predkladanej práce. Pomocou vhodne vybraných metód sa dá v konečnom dôsledku určiť, resp. vypočítať, úroveň integrity bezpečnosti (SIL), ktorá určuje či daný systém je vhodný na príslušné použitie.

Predkladaná dizertačná práca ukazuje, ako možno aplikovať normu IEC EN 61508 v praxi a to konkrétne na systéme elektrickej požiarnej signalizácie. Toto bolo dokumentované v návrhovej časti práce, ktorej predchádzal opis jednotlivých technických zariadení používaných v EPS systémoch. Jednotlivé technické zariadenia EPS sú od firmy Honeywell-Esser, ktoré z hľadiska štatistiky majú najväčšie zastúpenie na našom trhu. Tieto jednotlivé komponenty boli použité pre navrhnutý požiarny systém jedného poschodia administratívnej budovy. Celý požiarny

systém tejto budovy je však oveľa zložitejší, preto bola vybratá iba časť požiarneho systému, ktorá môže fungovať samostatne.

Najprv bolo definované prípustné riziko a riziko EUC pre jednoduchý systém, bez následných spínacích zariadení, z ktorých bola vypočítaná požadovaná stredná pravdepodobnosť poruchy PFD_{avg} a následne požadovaná SIL bezpečnostného systému. Výpočtami bolo určené, ktorý člen celého systému je najviac náchylný na vznik porúch, a ktorý najmenej. Následne boli do systému pridané spínacie zariadenia a pomocou analýzy stromov porúch bolo zistené, že každým pridaním ďalšieho spínacieho zariadenia, sa zvýši pravdepodobnosť vzniku poruchy v celom systéme.

Praktická časť práce bola ešte doplnená o testovanie celého systému bez následných spínacích zariadení. Bol určený minimálny počet testov potrebných pre otestovanie časti požiarneho systému zobrazeného na (Obr. 5-1). Testovanie celého požiarneho systému aj s následnými spínacími zariadeniami je však omnoho zložitejšie a náročnejšie, vzhľadom na to, že určité zariadenia nie je možné v praktickom dôsledku otestovať. Ide hlavne o mechanické časti systému, ako sú sprinkre, prípadne doprava kvapaliny k nim.

Práca sa zaoberala len bezpečnostným požiarnym systémom. Treba pripomenúť, že norma IEC EN 61508 má širší záber a obsahuje i ďalšie požiadavky na celé zariadenia bezpečnostných systémov. Danú prácu je možné použiť pri určovaní rizika bezpečnostne kritických systémov, nielen požiarnych, ale aj iných, súvisiacich s bezpečnosťou.

Ako bolo naznačená v kapitole 5.1.4, pre výpočet pravdepodobnosti porúch na vyžiadanie bezpečnostnej funkcie existujú rôzne metódy. V práci boli použité dve metódy a to metóda analýzy stromu porúch a metóda bezporuchovostných blokových schém.

Z výsledkov uvedených v práci je vidieť, že analyzovanie bezpečnosti pomocou metódy bezporuchovostných blokových schém možno použiť ako ekvivalent ku konvenčným metódam kvalitatívnej a kvantitatívnej analýzy. Prínosom práce je vytvorenie informačného prístupu k analýze bezpečnosti systémov, pričom je nutné poznať jednotlivé komponenty systému, a znalosť závislostí medzi blokmi analyzovaného systému. Metódu stromov poruchových stavov je možné použiť pri analýze zložitejších riadiacich systémov, pričom je nutné intuitívne určenie kombinácií porúch vedúcich k výskytu analyzovanej udalosti (nebezpečného stavu, poruchy).

Použitie iných metód na analýzu rizika by presiahlo rámec tejto dizertačnej práce, preto použitie týchto metód by mohlo slúžiť v budúcnosti ako námet ďalšej dizertačnej práce. Taktiež v dnešnej dobe už existujú integrované prostredia na analýzu rizík (CARE), a prostredia na predikciu udalostí a modelovania scenárov (CLEMENTINE), ktorých využitie otvára možnosti formulácie nových problémov s predmetnej oblasti a vývoj efektívnych metodík na ich riešenie.

Použitá literatúra

[1] IEEE, „IEEE standard for Software Verifikation and Validation“ in IEEE Std. 1012-1998, 1998.

[2] ARMOUR, P. G.: The Unconscious Art of Software Testing, COMMUNICATIONS OF THE ACM January 2005/Vol. 48, No.1

[3] BERTOLINO, A.: Software Testing Research and Practice, The 10th International Workshop on Abstract State Machines, Italy, 2003, str. 1-21

[4] BINDER, R.V.: Testing Object-Oriented Systems, Addison-Wesley, 1999

[5] MCGREGOR, J.D.; Sykes, D.A.: A Practical Guide to Testing Object-Orienred Software, Addison-Wesley, 2001

[6] BERTOLINO, A.: Knowledge Area Decription of Software Testing – Version 0.9, Instituto di Elaborazione della Informazione, Pisa, Italy, 2002

[7] LEE Copeland: A Practitioner's Guide to Software Test Design, Artech House Publishers, 2003, ISBN 158053791X

[8] JACOBSON, I.; Christerson, M.; Jonsson, P.; Övergaard, G.: Object-Oriented Software Engineering, Addison-Wesley, 1994

[9] PATTON, R.: Testování softvéru. Computer Press, Praha: ISBN 80-7226-636-5

[10] Hagar, J.D.: Testing Critical Software: Practical Experiences, Lockheed Martin Astronautics, Denver, USA, 1997

[11] Jacobson, I.; Christerson, M.; Jonsson, P.; Övergaard, G.: Object-Oriented Software Engineering, Addison-Wesley, 1994

[12] Moravčík, O.; Vaský, J.; Mišút, M.: Softvérová Technika, STU Bratislava, Bratislava, 1997.

[13] IEEE Std 610.12, Standard Glossary of Software Engineering Terminology, IEEE, 1990

[14] Weyuker, E.J.: More Experience with Data Flow Testing, IEEE Transactions on Software Engineering, 19/1993, str. 919-919

[15] Harrold, M.J.; McGregor, J.D.; Fitzpatrick, K.J.: Incremental Testing of Object-Oriented Class Structure, 14th International Conference on Software Engineering, ACM, 1992, str. 68-80

[16] Malaiya, Y.K.; Li, N.; Bieman, J.; Karcich, R.; Skibbe, B.: The Relationship Between Test Coveraqe and Reliability, Technical Report CS-94-110, Colorado State University, USA, 1994

[17] Zhu, H.; Hall, P.; May, J.: Software Unit Test Coverage and Adequacy, ACM Computing Surveys, 29/1997, str. 366-427

[18] Ježek, D.; Pavlik, V.: VŠB – Technická Universita Ostrava, Fakulta elektrotechniky a informatiky, http://www.cs.vsb.cz/jezek/vyuka/tss2008/download/Testing Software Systems CZ.pptx

[19] Avižienis, A. – Laprie, J.-C., Randell, B.: Dependability And Its Threats: A Taxonomy. http://www.cs.ncl.ac.uk/research/pubs/inproceedings/papers/779.pdf

[20] C.P. Pfleeger, “Data security”, in Encyclopedia of Computer Science, A.Ralston, E.D. Reilly, D. Hemmendinger, eds, Nature Publishing Group, 2000, pp. 504-507.

[21] Pačaiová, H.: Posudzovanie rizík - porovnanie definícií, metód a postupov http://www.ebts.besoft.sk/part_UVOD/odborne_forum/prispevky/clanky/BP_ARB.doc

[22] Procházková, D.: Metodiky hodnocení rizik http://www.movoz.cz/download/metud.doc

[23] Spalek, J. et al.: Princípy eSafety a komplexná bezpečnosť IDS. In: Sborník abstraktů medzinárodní konference "Intelligent Transport Systems", Praha 22. - 23. 3. 2005, s. 57-58.

[24] STN EN 61508 (18 4020) Funkčná bezpečnosť elektrických (elektronických) programovateľných elektronických bezpečnostných systémov. SÚTN Bratislava, 2002

[25] STN EN 61511 (18 0303) Funkčná bezpečnosť. Bezpečnostné riadiace systémy spojitých technologických procesov. SÚTN Bratislava, 2005

[26] STN EN 62061 (35 2220) Bezpečnosť strojov. Funkčná bezpečnosť elektrických, elektronických a programovateľných elektronických bezpečnostných riadiacich systémov. SÚTN Bratislava, 2005

[27] Development Guidelines for Vehicle Based Software, MISRA 1994.

[28] Peters, D.K.; Parnas, D.L. Requirements-based monitors for real-time systems. Software Engineering, IEEE Transactions on, Volume: 28 Issue: 2, Feb. 2002, On page(s): 146 – 158.

[29] Response of the OMG’s Request for proposal on Schedulability, Performance, and Time http://www.omg.org/techprocess/meetings/schedule/UML_Profile_for_Scheduling_FTF.html

[30] STN EN 54 Elektrická požiarna signalizácia SÚTN Bratislava 1996

[31] Novar Austria GmbH, Technické parametri zařízení EPS, 2007

[32] Novar Austria GmbH, Protipožární technika – produktový katalóg 2007

Zoznam publikovaných príspevkov

[1] Sakál, Peter - Božek, Pavol - Nemlaha, Eduard: Číslicové riadiace systémy. - 1. - Trnava: Tripsoft, 1999. - 193 s. - ISBN 80-968294-1-6

[2] Nemlaha, Eduard - Miksa, František: Možnosti exportovania dát z MYSQL do textového editora MS Word. The data export possibilities from MYSQL into MS Word editor. In: Materials Science and Technology [online]. - ISSN 1335-9053. - Roč. 8, č. 8 (2008)

[3] Božek, Pavol - Nemlaha, Eduard: Integrácia obsahu a tvorba stredoškolskej učebnice. Zabezpečovacia technika interaktívnou multimediálnou formou. In: Informačné technológie v riadení a vzdelávaní : Medzinárodný vedecký seminár, Nitra 28.1.2010. - Nitra : Slovenská poľnohospodárska univerzita v Nitre, 2010. - ISBN 978-80-552-0336-2

[4] Hrenák, Juraj - Klačo, Marián - Husárová, Bohuslava - Nemlaha, Eduard: Implementácia distribuovaných databáz v prostredí MS SQL Server. In: CO-MAT-TECH 97. : 5. vedecká konferencia s medzinárodnou účasťou. Sekcia: aplikované prírodné a inžinierske vedy. Humanitné a spoločenské vedy v technike. Zväzok 3. - Bratislava : STU v Bratislave, 1997. - ISBN 80-227-0979-4. - S. 195-199

[5] Miksa, František - Nemlaha, Eduard: Napätia a deformácie vo zvarových spojoch z tenkostenných materiálov. In: Spawanie w energetyce. Zváranie v energetike : VIII Medzinárodná konferencia, Tatranská Lomnica - Matliare, 24.-27.09.1996. - , 1996. - S. 147-151

[6] Miksa, František - Nemlaha, Eduard: Odolnosť vybraných materiálov proti abrazívnemu a erozívnemu opotrebeniu. In: CO-MAT-TECH 96 : 4.vedecká konferencia s medzinárodnou účasťou. Sekcia 1: materiálové inžinierstvo, strojárske výrobné technológie. - Bratislava,Trnava : STU v Bratislave, 1996. - ISBN 80-2270901-8. - S. 89-93

[7] Miksa, František - Nemlaha, Eduard: Voľba návarových materiálov z hľadiska podmienok opotrebenia. In: Techreno `96 : 4. medzinárodná konferencia spojená s výstavou a prezentáciou firiem. Žilina, 4.-6.6.1996. - , 1996. - ISBN 90-231-0317-2. - S. 99-104

[8] Vaský, Jozef - Hančin, Milan - Nemlaha, Eduard - Masár, Ladislav: Fakultný intranet. In: CO-MAT-TECH 2000 : 8. medzinárodná vedecká konferencia. Časť 4.: Aplikované prírodné a inžinierske vedy. - Bratislava : STU v Bratislave, 2000. - ISBN 80-227-1413-5. - S. 55-62

[9] Božek, Pavol - Miksa, František - Nemlaha, Eduard: Projektovanie výrobných systémov II. - Trnava : Tripsoft, 2005. - CD. - ISBN 80-969390-1-7

[10] Vaský, Jozef - Nemlaha, Eduard - Masár, Ladislav: CAD/CAM systémy. - 1. vyd. - Bratislava : STU v Bratislave, 2003. - 255 s. - e-skriptá. - ISBN 80-227-1882-3 (https://sweb.mtf.stuba.sk)

[11] Miksa, František - Nemlaha, Eduard: Fire safety system with continuity of control switching equipment. In: Process Control 2010 : 9th International Conference. Kouty nad Desnou, 7.-10. 6. 2010. - Pardubice : University of Pardubice, 2010. - ISBN 978-80-7399-951-3. - C084a-1-5

Poďakovanie

Prácu som vypracoval ako externý doktorand na Katedre aplikovanej informatiky a automatizácie MTF STU v Trnave pod vedením školiteľa doc. Ing. Pavla Važana, PhD

Chcem sa týmto poďakovať školiteľovi za vedenie a smerovanie a hlavne prof. Ing. Dušanovi Mudrončíkovi, PhD za cenné rady a odborné pripomienky.