TECHNICKÁ UNIVERZITA

V LIBERCI

Verifikace a validace informace o měřené veličině

Disertační práce

Vypracoval: Ing. Jan Kamenický

prosinec 2009

Prohlášení

Byl jsem seznámen s tím, že na mou disertační práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména §60 - školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé disertační práce pro vnitřní potřebu TUL.

Užiji-li disertační práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Disertační práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací se školitelem, Ing. Davidem Vališem, Ph.D..

Datum:

Podpis

Poděkování

Děkuji svému školiteli, panu Ing. Davidu Vališovi, Ph.D, za cenné rady, komentáře a připomínky v průběhu celého období vzniku disertační práce. Dále děkuji pánům Ing. Michalovi Markovi za konzultace, nápady, kontakty a trpělivost, se kterou se mi věnoval a panu Ing. Pavlovi Fuchsovi, CSc. za praktický pohled na zkoumanou problematiku a podporu při práci.

Anotace

V praxi jsou provozována některá relativně nebezpečná zařízení, jako jsou například petrochemické provozy nebo jaderné elektrárny. Přínosy z jejich provozu jsou hlavním důvodem, proč společnost jejich provoz akceptuje. Míra nebezpečnosti je mylně chápána širokou veřejností pouze jako následky nebezpečné události. Z oboru řízení spolehlivosti a rizika je známo, že riziko je kombinací více faktorů, minimálně však následků nežádoucí události a očekávaným průměrným počtem jejího nastoupení. Zmiňovanou nežádoucí událostí může být standardně chápaná porucha, ale také např. falešné zapůsobení bezpečnostního systému v době, kdy není toto zapůsobení vyžadováno (tzv. bezpečná porucha). Následkem falešného zásahu jsou ekonomické ztráty z odstavení provozovaného zařízení. Mnohem závažnější dopady pak má nezapůsobení bezpečnostního systému v případě vyžádání jeho funkce, typicky v případě nastoupení poruchy. Následky jsou pak nejen ekonomické, ale především se jedná o ohrožení zdraví a života osob a životního prostředí.

Právě problematika systémů souvisejících s bezpečností, a to zejména systémů založených na moderních elektronických prostředcích a digitálním zpracováním signálu, představuje oblast, které je věnována značná pozornost. Svědčí o tom i skutečnost, jakým způsobem je tato oblast pokryta mezinárodními normami. Při aplikaci požadavků těchto norem v různých bezpečnostních systémech v praxi řeší výrobci a dodavatelé těchto systémů řadu otázek souvisejících s jejich spolehlivostí. Někdy exaktním způsobem, často však intuitivně, na základě „technického citu“ a zkušenosti projektantů. Při řešení téhož problému se pak vyskytují u jednotlivých výrobců a dodavatelů různá řešení bez reálného zdůvodnění, proč právě tento přístup byl zvolen.

Předložená disertační práce se proto soustředí na dílčí problematiku výběru relevantního údaje o fyzikální veličině s ohledem na parametry spolehlivosti a tím i dlouhodobou ekonomickou vhodnost nasazení zvoleného řešení.

Abstract

In praxis there are operated some relatively dangerous equipment such as petrochemical refinery or nuclear power plant. The basic reason why human society accepts their processing is benefit which these machineries make. Their dangerousness rate is wrongly understood by general public only as a consequence of dangerous event. From the theory of dependability and risk controlling it is well known that risk is computed as combination of more factors, at least of consequences and expected number of occurrence of unwanted event. This mentioned unwanted event could be standardly understood failure but also e. g. false action of safety system when its impact is not needed (so-called safe failure). Consequence of false impact is economical loss, resulting from process stoppage. More important impacts results from no-action state of safety system in case of its action demand, typically in case of failure. Consequences are then not only economical, but there could be also exposure of human health and life and danger of environment damage.

Dilemma of systems related with safety, and especially systems based on modern electronic components and digital signal computing, is the area which is much focused today. The quantity of international standards dealing with reliability, risk and safety confirms this statement. Producers and suppliers of safety systems solve many problems related with request of dependability standards. Problems solved in scientific way, but some of them are solved intuitively, based on “technical feeling” and experiences of designers. It means that solutions of similar problem, made by different designers, are often diverse and there is no reason why their access was chosen.

Submitted doctoral thesis focuses on partial problem with choosing of relevant data about physical variable related with safety, where there exist more principles of solution. To be more concrete this work deals with problem of choosing relevant value of physical quantity with respect to reliability parameters and related long-term economical profitability of chosen solution.

Obsah

A Seznam příloh: 8

B Seznam tabulek: 8

C Seznam obrázků: 9

Seznam použitých zkratek a symbolů 10

1 Úvod 12

1.1 Definice problému 13

1.2 Cíle práce 13

1.3 Použitý aparát 14

1.4 Limity a omezení práce 14

1.5 Struktura disertační práce 15

2 Vymezení zkoumané oblasti 17

2.1 Význam pojmů verifikace a validace 17

2.2 Stručný úvod do problematiky systémů, souvisejících s bezpečností 19

2.3 Příklad použití výběrových systémů 20

2.4 Validace pomocí logického spojování signálů 23

2.4.1 Analogové spojování signálu 23

2.4.2 Výběrové zapojení 2/3 23

2.4.3 Výběrové zapojení s redukcí počtu vstupních kanálů 24

2.4.4 Zhodnocení uvažovaných možností zapojení 24

2.5 V praxi používané systémy verifikace 25

3 Cíle disertační práce 27

4 Stručný přehled teorie spolehlivosti 29

4.1 Ukazatele spolehlivosti 29

4.2 Výpočet základních ukazatelů spolehlivosti objektu 29

4.3 Struktura objektu 32
4.3.1 Sériové zapojení 32
4.3.2 Paralelní zapojení 35
4.3.3 Výběrové zapojení 37
4.3.4 Ukazatele spolehlivosti násobných zapojení 39
4.4 Vybrané metody analýz spolehlivosti 40
4.4.1 Analýza způsobů a důsledků poruch (FMEA) 41
4.4.2 Analýza způsobů, důsledků a kritičnosti poruch (FMECA) 42
4.4.3 Metoda blokových diagramů bezporuchovosti (RBD) 42
4.4.4 Metoda výpočtu bezporuchovosti z dílů (PC) 42
4.4.5 Metoda analýzy stromu poruchových stavů (FTA) 43
4.4.6 Metoda analýzy stromu událostí (ETA) 43
4.4.7 Markovova analýza (MA) 44
4.5 Spolehlivost v analýzách bezpečnosti 44
4.6 Zálohované systémy 44
5 Spolehlivost ve vybraných publikacích 46
5.1 Validace signálu v odborných publikacích 46
5.2 Spolehlivost v technické normalizaci 47
5.2.1 Normy pro zabezpečovací systémy 47
5.2.2 Názvoslovné normy spolehlivosti 50
5.2.3 Normy pro management kvality 50
5.2.4 Normy pro management spolehlivosti 51
5.2.5 Pokyny k udržovatelnosti a související normy 53
5.2.6 Normy pro analýzu spolehlivosti a odhady hodnot ukazatelů spolehlivosti 54
5.2.7 Normy pro ověřování, zjišťování a zlepšování hodnot ukazatelů spolehlivosti 56

5.2.8 Normy pro zlepšování ukazatelů spolehlivosti 58
5.3 Shrnutí poznatků o problematice verifikace a validace v publikacích 59
6 Zvýšení parametrů spolehlivosti pomocí validace 60
6.1 Násobné měření fyzikálních veličin 60
6.1.1 Porovnání možností logického spojování signálu 61
6.1.2 Rozhodovací model 66
6.1.3 Výsledky rozhodovacího modelu 70
6.2 Přínosy tématu práce 75
7 Možnosti a perspektivy v pokračování práce 77
7.1 Navržený ekonomický model 77
7.2 Autovalidační senzory 79
8 Závěr 81
Použitá literatura 83

A Seznam příloh:

Příloha A: Poznámky k tvorbě logických hodnot pro algoritmy, uvedené v tab. 2. 93

B Seznam tabulek:

Tab. 1: Přehled analýz spolehlivosti a vhodnosti jejich použití 41
Tab. 2: Výsledky logického spojování signálu od tří nezávislých čidel 63
Tab. 3: Výsledky výpočtu parametrů spolehlivosti 67
Tab. 4: Parametry modelového případu hodnocení logických vyhodnocovacích členů 70

C Seznam obrázků:

Obr. 1: Příklad logiky reálného propojení více systémů do jednoho výsledného údaje 22

Obr. 2: Možnosti spojení tří redundantních měřících kanálů do jedné výsledné hodnoty..... 23

Obr. 3: Sériové zapojení..... 33

Obr. 4: Paralelní zapojení..... 35

Obr. 5: Výběrové zapojení 2 ze 3..... 37

Obr. 6: Graf závislosti nepohotovosti systému na poměru intenzit skrytých a zjevných poruch..... 71

Obr. 7: Graf závislosti nepohotovosti systému v závislosti na poměru intenzit poruch skrytých a zjevných poruch, za předpokladu shodných středních dob do obnovy skrytých a zjevných poruch..... 72

Obr. 8: Závislost střední doby mezi poruchami na poměru intenzit skrytých a zjevných poruch..... 73

Obr. 9: Graf závislosti střední doby provozu mezi poruchami měřicího systému na poměru intenzit poruch skrytých a zjevných poruch, za předpokladu shodných středních dob do údržby zjevných a skrytých poruch..... 74

Obr. 10: Ilustrační graf hledání ekonomicky optimálního systému..... 77

Seznam použitých zkratek a symbolů

A	součinitel asymptotické pohotovosti (z angl. Availability)
C	následek (z angl. Consequence)
CCF	porucha se společnou příčinou (z angl. Common Cause Failure)
EDU	Jaderná elektrárna Dukovany
HAZOP	studie nebezpečí a provozuschopnosti (z angl. Hazard and Operability Study)
HF	lidský faktor (z angl. Human Factor)
HRA	analýza spolehlivosti lidského činitele (z angl. Human Reliability Analysis)
IMK	individuální měřicí kanál
JE	jaderná elektrárna
MK	měřící kanál
MTBF	střední doba provozu mezi poruchami
MTTF	střední doba do poruchy
MTTR	střední doba do obnovy
P	pravděpodobnost
r	celkový počet poruch
r_i	empirická četnost poruch za uvažovaný interval
$R(t_1, t_2)$	pravděpodobnost bezporuchového provozu (z angl. Reliability)
ŘS	řídicí systém
S_i	stav systému
SIL	úroveň integrity bezpečnosti (z angl. Safety Integrity Level)
t	kalendářní doba, po které byla ukončena zkouška
T	celková kumulovaná doba provozu

T_p	celková kumulovaná doba, po kterou bylo zařízení v poruše
U	součinitel asymptotické nepohotovosti
λ	intenzita poruch
λ_D, λ_H	dolní a horní mez dvoustranného konfidenčního intervalu skutečné hodnoty intenzity poruch
μ	intenzita oprav
χ^2	rozdělení chí-kvadrát

Zkratky a symboly, mající pouze místní význam, jsou vysvětleny při prvním použití v textu.

1 Úvod

Pro moderní společnost je jednou z životně důležitých služeb výroba a dodávka elektrické energie. Elektrická energie v současné době neodmyslitelně patří k životu každé vyspělé země a její ekonomiky. Její spotřeba neustále stoupá, proto nestačí pouze provozovat již existující a vyzkoušené zdroje a technická řešení, ale je nutné stávající systémy modernizovat a vyvíjet nové. Velký důraz je při tom kladen na dosažení vysoké míry spolehlivosti a bezpečnosti, a to již v etapě jejich návrhu, a zachování těchto vlastností při jejich provozu. Při tomto procesu je velmi vhodné poučit se z chyb a omylů předchozích konstrukcí a ideových pochodů.

Energetika je nezbytným předpokladem pro spokojený život každého jedince, přestože si to často ani neuvědomí. Energetika je však také jedním z pilířů fungování moderní lidské společnosti. Z hlediska státu je možné posuzovat její vazby na celou infrastrukturu, což je značně složitý problém. Při dlouhodobém výpadku dodávky elektrické energie může dojít k totálnímu kolapsu bankovnictví, telekomunikací, v návaznosti na to i dopravy a průmyslu. Proto lze tvrdit, že patří k důležitým prvkům národní infrastruktury (tzv. kritické infrastruktury). Z výše uvedených důvodů je zřejmé, že je nezbytné dále rozvíjet a zdokonalovat produkci a distribuci elektrické energie. To vyžaduje věnovat značnou pozornost problematice spolehlivosti a bezpečnosti energetických zařízení.

Z uvedených důvodů byla v rámci výzkumného centra „Progresivní technologie a systémy pro energetiku“, projekt č. 1M06059, řešena otázka, s jakou spolehlivostí je možné získat informaci o měřené veličině. Hodnoty fyzikálních parametrů v energetických provozech, informace o stavech technologie energetického bloku a další údaje představují základní informaci pro bezpečnou a ekonomicky efektivní výrobu tepelné a elektrické energie.

Teoretické základy, na nichž je tato disertační práce postavena, jsou obsaženy v teorii spolehlivosti. Tato vědní disciplína si klade za cíl neustále zlepšovat používané procesy a postupy a navrhovat řešení nalezených problémů. Při analýzách spolehlivosti se pak řeší otázka zvyšování spolehlivosti hledáním slabých míst (nejslabších článků řetězu) na základě komplexního přístupu k řešenému problému. Tj. při respektování ekonomických možností eliminace slabin ve spolehlivosti a tím i bezpečnosti zkoumaného systému.

1.1 Definice problému

Téma disertační práce ve znění „Verifikace a validace informace o měřené veličině“ bylo navrženo na základě diskuze s odborníky z oboru energetiky při formulování úloh pro řešení úkolů výzkumného centra „Progresivní technologie a systémy pro energetiku“ podporovaného z prostředků Ministerstva školství, mládeže a tělovýchovy České republiky (projekt č. 1M06059). Dosud nevyřešenou problematikou je u elektronických řídicích a bezpečnostních systémů nalezení optimálního způsob výběru (resp. výpočtu) řídicího (resp. havarijního) signálu z násobných měření fyzikálních veličin. Řídicí a havarijní systémy ke své správné funkci potřebují obdržet jediný, co nejvěrohodnější, údaj o procesu, který řídí, resp. hlídají. Vysoké spolehlivosti tohoto výsledného údaje je možno dosáhnout násobným snímáním hodnoty fyzikální veličiny a následnou kombinací naměřených hodnot do jedné výsledné informace. Algoritmů, které se v praxi používají pro získání jediného výsledného údaje z násobných vstupů, je několik a dosud neexistuje jednoznačná odpověď na otázku, zda je některý z používaných algoritmů kvalitnější, než ostatní. Touto problematikou se zabývá předkládaná disertační práce.

1.2 Cíle práce

Práce si klade za cíl jednoznačně odpovědět na otázky, jaký dopad na spolehlivost mají jednotlivé způsoby verifikace a validace výsledného údaje o měřené fyzikální veličině, získaného vzájemnou kombinací několika vstupních údajů. Dalším cílem práce je navrhnout vhodný aparát pro posouzení vhodnosti nasazení jednotlivých typických aplikací systémů řízení a zajištění bezpečnosti. V práci jsou popsány a analyzovány způsoby získávání výsledné hodnoty z násobných měření. Tyto možnosti nalezení výsledné hodnoty jsou porovnány z pohledu spolehlivosti, mezi jinými jsou posouzeny a porovnány hodnoty jejich asymptotické nepohotovosti (A) a střední doby provozu mezi poruchami ($MTBF$) za reálných podmínek provozu. Pro všechny uvažované algoritmy výběru/výpočtu věrohodné řídicí hodnoty jsou uvažovány stejné okrajové podmínky, a sice reálné podmínky provozu. Mezi okrajové podmínky dále patří nemožnost odhalit všechny poruchy diagnostickým signálem (míra diagnostického pokrytí), možnost nastoupení poruchy se společnou příčinou, vliv lidského faktoru, (ne)bezpečnost poruch atd. Práce popisuje, shrnuje a hodnotí výše uvedené skutečnosti a poskytuje návod pro výběr vhodného algoritmu pro získání výsledné hodnoty z násobných měření fyzikálních veličin. Výstupem práce je matematický model, který na základě variace

okrajových podmínek a parametrů spolehlivosti komponent měřicích systémů tabelárně a graficky vypočte a zobrazí hodnoty nepohotovosti a *MTBF* pro každý uvažovaný algoritmus měřicího systému. Výstupem tohoto modelu je dále doporučení výběru jedné konkrétní varianty algoritmu pro výběr/výpočet výsledné hodnoty z násobných měření.

1.3 Použitý aparát

Řešení problému nalezení nejvhodnějšího algoritmu pro získání výsledné hodnoty z násobných vstupních údajů vyžaduje znalosti z oblasti teorie spolehlivosti a rizik a samozřejmě také základního matematického aparátu. V práci jsou obecně popsány některé známé metody analýz spolehlivosti a způsoby výpočtu relevantních ukazatelů spolehlivosti pro jednotlivé typy zapojení algoritmů pro výběr/tvorbu vhodného výsledného údaje z násobných individuálních měření fyzikální veličiny. Teorie spolehlivosti je samozřejmě obsáhlejší, avšak předkládaná disertační práce si neklade za cíl seznámit čtenáře se všemi aspekty této vědní disciplíny, ale pouze s oblastmi, které se dotýkají řešeného problému.

1.4 Limity a omezení práce

Úplné vyřešení nastíněného problému bohužel přesahuje možnosti disertační práce. To je zapříčiněno omezujícími skutečnostnostmi, jako jsou:

- nedostupnost údajů o pořizovacích cenách jednotlivých řešení řídicích systémů,
- nedostatek dat o poruchách v provozu a jejich nevhodné třídění z hlediska jejich významu,
- žádné nebo zkreslené údaje o relativním zastoupení poruch se společnou příčinou a poruch, způsobených lidským faktorem,
- zkreslené údaje o dobách do obnovy funkce porouchaných zařízení,
- nedostupnost dat o ekonomických ztrátách při výpadku provozu,
- nedostupnost dat o ekonomických následcích falešného zapůsobení *ŘS*, resp. bezpečnostního systému,
- apod..

Většina těchto dat buď neexistuje, nebo je výrobci a provozovatelé řídicích systémů vnímají jako data příliš citlivá na to, aby mohla být zveřejněna. Z tohoto důvodu je práce pojata jako návod pro provozovatele řídicích/bezpečnostních systémů na vytvoření ekonomické rozvahy, který algoritmus pro kombinaci násobných měření použít. Do předloženého modelu

vstupují údaje o intenzitách poruch jednotlivých měřicích systémů, procentuální zastoupení zjevných/skrytých poruch atd., ale pro kompletní ekonomickou rozvahu by bylo nutné počítat také s následky, které mohou být způsobeny selháním (resp. falešným zásahem) měřicích/bezpečnostních systémů.

Uvažované řídicí a havarijní systémy pracují automaticky na základě předem definovaného algoritmu, nevyžadují tedy při své činnosti zásahy člověka a lidský faktor by mohl zasáhnout pouze při údržbě celého systému, případně v etapě návrhu algoritmu. Možné chyby lidského faktoru předpokládáme stejné pro všechny uvažované algoritmy, lidský faktor tudíž nebude mít rozhodující vliv na hodnoty pohotovostí každého algoritmu (resp. bude mít stejný vliv pro každý z uvažovaných způsobů kombinace více vstupů do jedné výsledné hodnoty) a jako takový nebude v analýze počítána hodnota příspěvku lidského činitele k celkové nepohotovosti *ŘS*. Také poruchy se společnou příčinou nebudou v modelu ohodnoceny, protože i jejich vliv na celkovou (ne)pohotovost *ŘS* předpokládáme stejný pro všechny uvažované algoritmy výběru/výpočtu jedné výsledné hodnoty z násobných měření fyzikální veličiny.

1.5 Struktura disertační práce

Disertační práce se věnuje problematice verifikace a validace násobných údajů z měřicích kanálů. Část tohoto problému je možno vyřešit pomocí nalezení algoritmu pro výběr/výpočet jedné výsledné hodnoty z násobných měření jedné fyzikální veličiny. Práce je členěna do osmi kapitol a doplněna jednou přílohou. První kapitola čtenáře seznamuje s okolnostmi vzniku potřeby práci vytvořit, s řešeným problémem, nástroji, které budou při řešení problému použity a s omezeními, které se v průběhu práce vyskytly. Druhá kapitola podrobně popisuje problém, který je třeba vyřešit. Jsou v ní také uvedeny tři možnosti kombinace násobných vstupů do jedné výsledné hodnoty, které budou v dalších kapitolách analyzovány. Třetí kapitola informuje o vytyčených cílech řešení disertační práce. Ve čtvrté kapitole je představena báze znalostí, na jejímž základě bude řešen problém výběru jedné výsledné hodnoty z násobných měření. Pátá kapitola obsahuje stručné shrnutí výsledků autorů, kteří se podobným problémem již zabývali. Následně jsou uvedeny technické normy se vztahem k problematice spolehlivosti a dále několik publikací, vztahujících se k problematice výběru validní hodnoty za pomoci násobných měření jedné fyzikální veličiny. Šestá kapitola je stěžejní částí práce, je v ní obsaženo vlastní řešení problému a tedy i myšlenkový přínos této

disertační práce. Součástí této kapitoly je de facto také příloha A, ve které jsou z prostorových důvodů a kvůli kontinuitě textu umístěny komentáře k výpočtovému aparátu vlastního řešení. Sedmá kapitola nabízí návrhy na možná pokračování řešení problematiky výběru/výpočtu jedné hodnoty z násobných měření fyzikální veličiny. A konečně závěrečná, osmá, kapitola shrnuje podstatné myšlenky a výsledky práce.

2 Vymezení zkoumané oblasti

2.1 Význam pojmů verifikace a validace

Disertační práce se zabývá problematikou verifikace a validace signálu. Co je však těmito pojmy míněno? Verifikace bývá v odborných publikacích často překládána jako ověřování, zatímco pojem validace se nepřekládá a používá se v tomto tvaru. V některých aplikacích je verifikace a validace považována za jeden nedělitelný proces, s čímž však nelze zcela souhlasit.

Ve slovníku cizích slov je pojem **verifikace** definován jako „potvrzení správnosti, pravosti; ověřování“. **Validace** je definována jako „ověřování, ověření, prověřování, prověření“. Je tedy zřejmé, že oba výrazy mají velmi podobný význam a bude nutné hledat jejich odlišnosti v technických publikacích, zabývajících se problematikou spolehlivosti.

V normě [87] je definován pojem

- **verifikace** - potvrzení zkouškou a doložením objektivních důkazů, že výsledky činnosti splňují cíle a požadavky definované pro tuto činnost,
- **validace** systému - potvrzení zkouškou a poskytnutím dalších důkazů, že systém jako celek splňuje příslušné požadavky specifikací (funkčnost, doba odezvy, tolerance k závadám, robustnost).

Na základě těchto definic lze verifikaci považovat za jakýsi nižší (dílčí) stupeň validace, protože pomocí ní pouze ověřujeme, zda nějaká činnost plní požadavky, které na ni klade provozovatel bez ohledu na činnost celého systému, jehož je celkem. Oproti tomu validace potvrzuje správnou funkci celého systému jako celku, ne pouze jednotlivých jeho součástí.

V některých detailech se liší definice pojmů verifikace a validace, uvedené v normě [71]:

- **verifikace -** potvrzení zkouškou a obstarání objektivního důkazu, že byly splněny specifikované požadavky (Při návrhu a vývoji se ověřování týká procesu přezkoušení výsledku dané činnosti, aby se určila shoda se stanoveným požadavkem pro tuto činnost. Odpovídající status bývá označován termínem „ověřeno“.)
- **validace** - potvrzení zkouškou a obstarání objektivního důkazu, že jsou splněny příslušné požadavky pro specifický cíl užití. Při návrhu a vývoji se validace týká

procesu testování produktu za účelem určení shody s požadavky uživatele. Validace se obvykle provádí u finálního produktu za definovaných provozních podmínek. Může však být potřebná i v dřívějších etapách. Odpovídající status bývá označován termínem „validováno“. Pokud jsou stanoveny různé cíle užití, může být validace prováděna vícekrát.[1]

Také v případě těchto definic je možné chápat verifikaci jako dílčí proces, sloužící k validaci funkce celého systému.

V normě [45] jsou definice verifikace a validace opět odlišné od výše uvedených:

- **ověřování** - potvrzení prostřednictvím poskytnutí objektivního důkazu, že specifikované požadavky byly splněny
- **validace** - potvrzení prostřednictvím poskytnutí objektivního důkazu, že požadavky na specifické zamýšlené použití nebo pro specifickou aplikaci byly splněny

I v případě definic uvedených v normě [45] je proces validace nadřazený procesu ověřování (verifikace) tím, že poskytuje důkaz o splnění požadavků zamýšleného použití.

Předkládaná disertační práce se zabývá nalezením správné výsledné hodnoty signálu, vzniklého kombinací několika vstupních údajů z měření jedné fyzikální veličiny. Tento proces je možné pojmenovat pouze „validace informace o měřené veličině“. Některé z uvažovaných algoritmů zpracování násobných vstupů do vyhodnocovacího algoritmu však předpokládají inteligentní vstupní údaje, které na základě porovnání aktuální hodnoty měření s hodnotou z historie umí rozeznat správnost/chybnost tohoto údaje. Tento proces rozpoznávání a ověřování dílčích hodnot vstupních údajů (tedy jejich verifikace) není sice předmětem práce, ale je nedílnou součástí uvažovaných algoritmů. Pojmy verifikace a validace jsou, viděno touto optikou, závislé na funkci, kterou od verifikovaného/validovaného systému vyžadujeme. Tak

[1] Je jistým rozporem, že výstupem verifikačního algoritmu je tzv. bit validity. Jedná se o terminologickou neshodu, vzniklou historicky. Z hlediska jednotlivého měřicího kanálu je totiž funkcí MK správné změření fyzikální veličiny a ověření této správnosti je potom validací takového měření. Z pohledu celého měřicího systému je však ověření správnosti individuálního MK pouze dílčím procesem a tudíž verifikací, zatímco validací nazveme ověření správnosti výsledného údaje, vzniklého kombinací verifikovaných vstupních údajů.

např. validace individuálního měřicího kanálu a její výstup - bit validity - je z hlediska algoritmu výběru/výpočtu jedné výsledné hodnoty z násobných IMK pouhou verifikací. Tato oblast není v odborné literatuře dostatečně objasněna a také proto bylo téma disertační práce zvoleno ve znění „Verifikace a validace informace o měřené veličině“.

2.2 Stručný úvod do problematiky systémů, souvisejících s bezpečností

Po technické stránce jsou nejzajímavějšími oblastmi jaderné elektrárny systémy, které se na „klasických“ typech elektráren nevyskytují, tedy zejména systémy kontroly a řízení štěpné reakce. Je třeba co nejvíce eliminovat nežádoucí nebezpečnou událost, kterou je poškození paliva, resp. tavení aktivní zóny reaktoru. Z tohoto důvodu je pro kontrolu správné funkce všech důležitých subsystémů použito násobnosti v měřících kanálech. Také zpracování měřeného signálu a jeho následné použití v řídicích a bezpečnostních systémech má nemalý vliv na bezpečnost provozovaného zařízení. Pokud do bezpečnostního systému vstoupí signál z nefunkčního měření v případě, kdy proces probíhá v normálních provozních podmínkách, dochází k nesprávným regulačním zásahům. Ty mohou vést k nežádoucím (ale zprostředkovaně i k nebezpečným) stavům systému, ve spolehlivostní praxi označovaným jako tzv. bezpečná porucha. Podobná situace nastává v případě, kdy bezpečnostní systém naopak dostane informaci o normalitě procesu v okamžiku, kdy došlo k vychýlení procesu z provozních mezí. V tomto případě se však jedná o tzv. nebezpečnou poruchu a následky této poruchy mohou být mnohem závažnější, než u poruchy bezpečné. Předkládaná disertační práce řeší problém výběru výsledného údaje o měřené veličině z násobných měření po stránce spolehlivosti.

V současnosti je k údaji o hodnotě měřené veličiny přidáván tzv. bit validity, který udává, zda je měření důvěryhodné. Tento bit je v případě bezporuchového stavu MK nastaven na logickou hodnotu „pravda“, v případě poruchy MK pak je tento bit negován na hodnotu „nepravda“. Validace signálu je však podle provedeného průzkumu[2] v ČR i u světových výrobců řídicích systémů nesystematická a nedosahuje všech možností, které by takováto

[2] Tento průzkum byl proveden autorem v rámci činností výzkumného centra „Progresivní technologie a systémy pro energetiku“, číslo projektu 1M06059 a výsledky byly publikovány ve výzkumné zprávě číslo B02 s názvem „Verifikace a validace měření fyzikálních veličin pro ŘS a tvorba věrohodných odvozených veličin.“.

informace mohla poskytovat. Významné měřené veličiny jsou snímány násobnými nebo zálohovanými měřeními. Pomocí digitální techniky se následně zjišťuje, zda je signál ve fyzikálně oprávněném pásmu a pro zvýšení spolehlivosti měřeného kanálu se násobná měření spojují výběrovými obvody pomocí logiky 1/2, 2/3, 2/4 apod. Je vhodné nejprve určit index validity pro jednotlivé kanály a následně uvažovat i ten. Tímto postupem je možné zvýšit parametry spolehlivosti celého měřicího systému. V současnosti někteří dodavatelé *ŘS* neřeší určení validity individuálního MK a následné zpracování validních naměřených hodnot fyzikálních veličin (určení výsledného údaje např. zprůměrováním, výběrem minimální/maximální hodnoty atp.). Dalším nedostatkem v současnosti používaných algoritmů zpracování násobných měření je fakt, že výběrový algoritmus zpracování signálu se u některých *ŘS* při poruše snímače (či snímačů) automaticky nepřizpůsobuje zbylému počtu platných měřících kanálů.

2.3 Příklad použití výběrových systémů

V jaderné elektrárně Dukovany existuje množství zálohovaných systémů, které pracují s výběrovým zapojením. V této kapitole bude představen systém, který se používá pro ochranu reaktoru, tedy pro jednu z nejdůležitějších bezpečnostních funkcí, které jsou na jaderné elektrárně vykonávány. Jedná se o digitální systém ochrany reaktoru (Digital Reactor Protection System - dále DRPS). Je to systém, ve kterém je implementována výběrová logika pro funkce systémů RTS (Reactor Trip System) a ESFAS (Engineered Safety Features Actuation System). Tento systém řídí výstupy ze snímačů do ovládacích obvodů akčních členů a řídí jednu sadu normálních vypínačů RTS a jednu sadu diverzních vypínačů RTS.

Druhým systémem, používaným pro ochranu reaktoru, je digitální limitační systém reaktoru (Digital Reactor Limitation System - dále DRLS). Jedná se o systém, ve kterém jsou realizovány limitační funkce reaktoru - RLS (Reactor Limitation System).

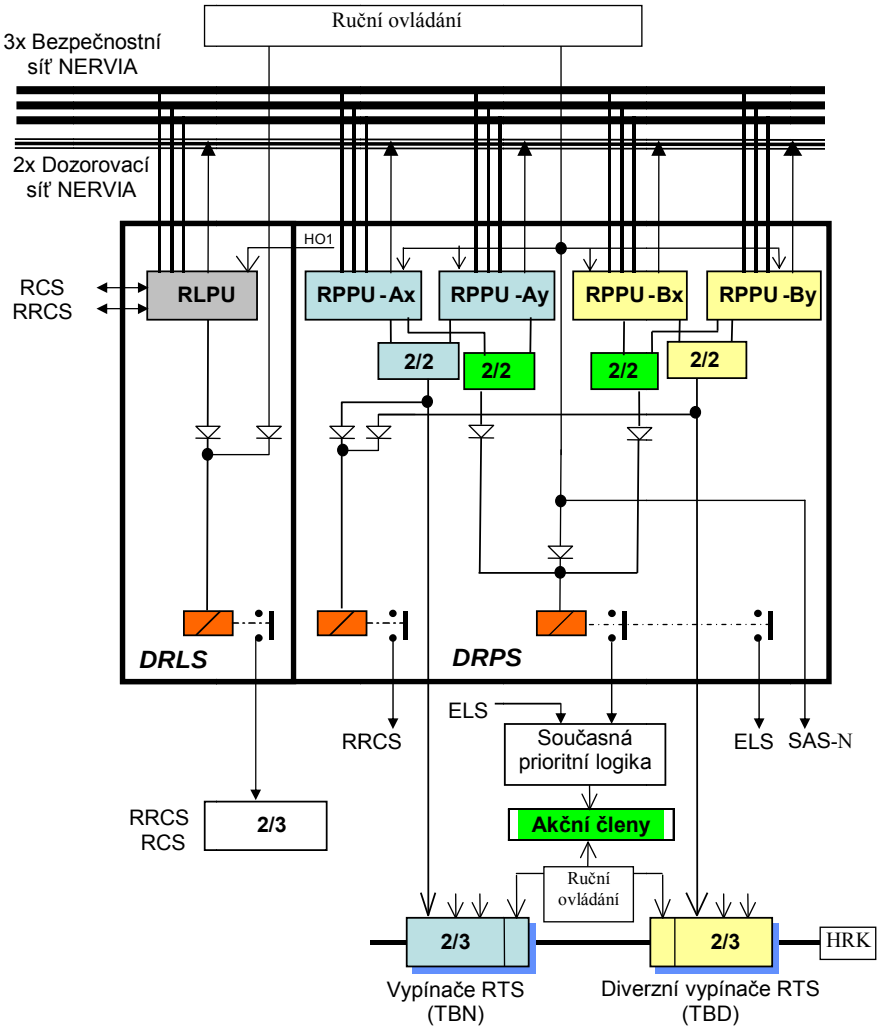
Systémy DRPS a DRLS jsou tedy složeny ze systémů RTS, ESFAS a RLS. Jejich krátký popis je uveden v následujících odstavcích a jejich vzájemná provázanost a logika je zobrazena na obr. 1.

Systém rychlého odstavení reaktoru (RTS - Reactor Trip System**)** je aktivován pro přerušení štěpné reakce v aktivní zóně reaktoru a pro ukončení provozu reaktoru. Aktivace signálu znamená plné odstavení reaktoru. Pokud je tento signál vytvořen, jsou všechny regulační tyče spuštěny do aktivní zóny vlastní vahou rychlostí 20÷30 cm/sec. I když bude

signál přerušen, budou tyče padat dále až do koncové polohy. Aktivace signálu vychází z koncepce “bezpečné poruchy", tj. jestliže nastane možnost výpadku bezpečnostní funkce (například z důvodu výpadku elektrického proudu), bude signál vyvolán.

Hlavní funkcí limitačního systému (RLS) je omezení nebo snížení výkonu reaktoru za jistých předepsaných podmínek. Spouštění limitačního systému spočívá v generování signálu „blokování zvednutí regulačních tyčí“ k omezení růstu výkonu reaktoru a v ovládání „zasunutí skupiny regulačních tyčí“ ke snížení výkonu reaktoru.

Účelem systému zajištění bezpečnosti (ESFAS) je likvidace předpokládaných havárií se zajištěním jaderné bezpečnosti celého bloku i okolí. V případě havárie spojené s porušením celistvosti primárního nebo sekundárního okruhu, až po rozsah maximální projektové havárie, uvádí systém ESFAS automaticky do činnosti zařízení bezpečnostních systémů. Signály systému ESFAS ovládají především akční členy havarijních systémů chlazení aktivní zóny, rychločinné oddělovací armatury pro lokalizaci unikajícího chladiva v hermetických boxech reaktorového bloku a další zařízení k lokalizaci a likvidaci uvedených havárií.



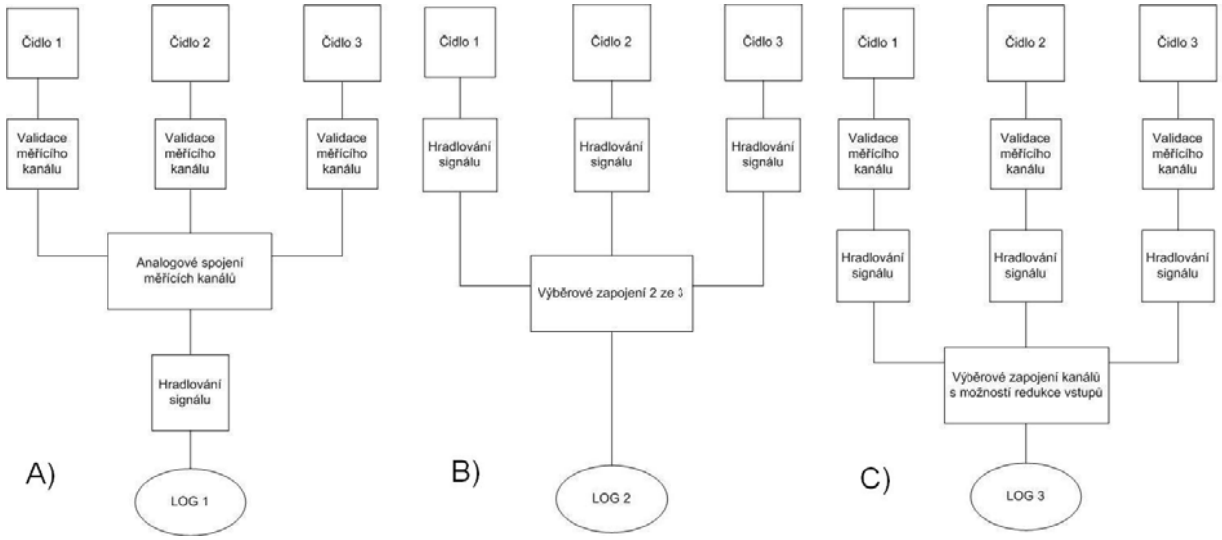
Obr. 1: Příklad logiky reálného propojení více systémů do jednoho výsledného údaje

V místech, kde je uvedena logika výběru řídicích signálů jako 2/3, je každý algoritmus prováděn ve třech na sobě nezávislých výpočetních celcích. Pomocí výběrového členu se určí výsledná hodnota měřené veličiny, vycházející z individuálních měření a tato verifikovaná hodnota je vrácena zpět do procesu řízení všech tří dílčích měřicích systémů. Skutečná pohotovost takovéhoto výběrového členu má tedy nemalý vliv na celkovou pohotovost reaktorového bloku. Výběrové zapojení 2 ze 3 však není jediným možným způsobem spojení několika individuálních měřicích kanálů do jedné výsledné hodnoty údaje o fyzikální veličině. Příklady dalších možností logického zapojení více měřicích kanálů jsou uvedeny v následujících kapitolách.

2.4 Validace pomocí logického spojování signálů

2.4.1 Analogové spojování signálu

Jednou z možností, jak z redundovaných měření téže fyzikální veličiny získat jediný výsledný údaj, je vzájemná kombinace signálů z měřících kanálů do jedné hodnoty. Tato operace se nejčastěji provádí běžným zprůměrováním vstupních hodnot, ovšem existují i jiné algoritmy pro nalezení výsledku, jako např. medián, geometrický průměr, vážený součet druhých mocnin apod. Do celého procesu měření je možné zapojit ještě validační algoritmus, který na základě porovnávání výstupních hodnot (např.: fyzikální realizovatelnost výsledku, spojitá hodnota derivace, fyzikálně realizovatelná hodnota derivace apod.) určuje validitu signálu. Vzniklý výsledný údaj je snadno použitelný jako hodnota zobrazovaná operátorovi nebo přímo vstupující do regulátoru. Schematické znázornění popsaného postupu měření je uvedeno na obr. 2 (varianta A) a v další práci bude označeno jako LOG1.



Obr. 2: Možnosti spojení tří redundantních měřících kanálů do jedné výsledné hodnoty

2.4.2 Výběrové zapojení 2/3

Další možností, jak určit z násobného měření fyzikální veličiny jednu hodnotu, je v praxi často používaný princip výběrového zapojení. Schematické znázornění logické posloupnosti akcí, vedoucích k výsledku, je na obr. 2 (varianta B) a budeme ho značit jako LOG2. Zde lze uvažovat zapojení 2 ze 3. Na rozdíl od prostého analogového spojování signálu v tomto případě není ohodnocena validita jednotlivých měřících kanálů a všechny bez rozdílu jsou zpracovávány ve výběrovém členu. Takovéto zpracování má nevýhodu v tom, že není

rozeznáno chybné individuální měření. Na druhou stranu porucha jednoho měřícího kanálu nezpůsobí chybu na výstupu, protože bude přehlasována zbývajícími dvěma platnými měřícími kanály. Porucha uvedeného měřicího systému tedy nastane až při současné poruše dvou nebo tří individuálních kanálů. Tato možnost se zdá být nepravděpodobná, ovšem je třeba si uvědomit, že spolehlivost výběrového zapojení může být snížena poruchou se společnou příčinou. Dalším faktorem, který ovlivňuje výslednou hodnotu pohotovosti výběrového zapojení, je možnost nastoupení skryté poruchy. V takovém případě pak již stačí, aby nastoupila porucha na jednom ze dvou zbývajících měřicích kanálů, a dojde k poruše celého měřicího systému.

2.4.3 Výběrové zapojení s redukcí počtu vstupních kanálů

Pokud jsou vzaty v úvahu nedostatky předchozích dvou způsobů zapojení násobných měřicích kanálů, není obtížné navrhnout takové uspořádání, které by tyto nedostatky potlačilo. Naopak vyzvedne pozitiva jednotlivých spolehlivostních kombinací. Jednou možností takové úpravy je připojení logického členu, který by určoval, jaká operace má být s vstupními kanály provedena. V kombinaci s navrženým logickým členem je možno použít hradla, která určí validitu každého individuálního měřícího kanálu. Princip takového zapojení je nastíněn na obr. 2 (varianta C) a pro naše účely bude označen LOG3. Do logické rozhodovací jednotky jsou přivedeny vstupní údaje, ohodnocené indexem validity, případně příznakem důvěryhodnosti daného měření. Rozhodovací člen potom na základě předem nastaveného algoritmu zvolí, jaká operace se s přivedenými vstupy provede (výběr 2 ze 3, průměr ze všech vstupních údajů atp.). Pokud ovšem verifikační algoritmus odhalí poruchu nějakého kanálu měření, je tu možnost tento údaj neuvažovat a pokračovat v řízení podle modifikovaného rozhodovacího kriteria. Tím je myšleno např.: redukce výběrového zapojení 2/3 na 2/2 resp. 1/2, vytvoření průměrné hodnoty pouze ze zbylých validních údajů atd. Takováto konstrukce se v praxi málo používá pro svou náročnost, ovšem lze předpokládat, že ta by mohla být vyvážena vyšší spolehlivostí celého zapojení, zde reprezentovanou zejména vyšší odolností proti poruše jednotlivého měřícího kanálu.

2.4.4 Zhodnocení uvažovaných možností zapojení

Z výše uvedených tří možností se průmyslově běžně používá pouze výběrové zapojení 2/3, které je kompromisem mezi neakceptovatelným stavem prostého průměrování (z důvodu nízké spolehlivosti zapojení - porucha jednoho měřícího kanálu vychýlí a znehodnotí celou

výslednou informaci) a příliš technicky náročným modelem výběrového zapojení s logickým členem pro redukci počtu vstupních kanálů.

Úkolem práce je porovnání spolehlivosti všech tří možností zapojení měření a potvrzení/vyvrácení zažitého názoru, že výběrové zapojení 2/3 je nejlepším možným.

2.5 V praxi používané systémy verifikace

Mezi výrobci a dodavateli řídicích systémů v ČR byl proveden průzkum[3] používaných verifikačních algoritmů pomocí strukturovaného dotazníku. Dotazováním se u většiny významných dodavatelů řídicích systémů pro naši energetiku (Foxboro, Siemens, Schneider Electric, Westinghouse, Honeywell, ZAT) byly získány následující poznatky o verifikačních algoritmech v jejich řídicích systémech:

- Verifikační algoritmy, ověřující platnost údajů ze snímačů nabývajících hodnot ze spojitého intervalu, využívají signálů z jednotlivého individuálního měřicího kanálu. Tato metoda je aplikována i v případě, že pro danou fyzikální veličinu je v *ŘS* k dispozici více redundovaných měření.
- Všichni dodavatelé *ŘS* mají ve svých firmwarových verifikačních algoritmech zavedeno detekování vystoupení signálu ze zadaného pásma a možnost zařadit jako příznak poruchy individuálního měřicího kanálu neodpovídající rychlost změny fyzikální veličiny - rychlé vybočení z mezí a někde i příliš pomalé, tzv. zamrznutí.
- Verifikační algoritmus, který by ověřoval platnost údaje právě prověřovaného snímače nejen použitím jeho signálů, ale i z redundovaných měření téže veličiny, se objevil pouze u jediného *ŘS*. Není to však standardně nabízený firmware daného dodavatele.
- Objeví-li se ověřování věrohodnosti posuzovaného měření pomocí údajů o veličinách jiného typu, nejde o opakovaný verifikační algoritmus nasazený na daný individuální měřicí kanál, ale o případ speciální vypočítávané veličiny, která se projektanty připraví v uživatelském software pouze ve zcela výjimečných případech.
- Verifikačními algoritmy snímače stavu uspořádaného na analogové přístrojové bázi

[3] Tento průzkum byl proveden autorem v rámci činností výzkumného centra „Progresivní technologie a systémy pro energetiku“, číslo projektu 1M06059 a výsledky byly publikovány ve výzkumné zprávě číslo B02 s názvem „Verifikace a validace měření fyzikálních veličin pro ŘS a tvorba věrohodných odvozených veličin.“.

pracují na základě potvrzování vzájemně se synchronně měnících hodnot přepínacího kontaktu u třívodičového uspořádání obvodu snímače stavu nebo sledování malých pomocných pracovních proudů v obvodu, kde je kontakt snímače stavu doplněn odporníky v sérii a paralelně s kontaktem, tj. u dvouvodičového uspořádání obvodu.

- Příznakem validity měření přidělovaným těmito verifikačními algoritmy je dvouhodnotová logická proměnná typu 0/1.
- V jediném zjištěném případě má řídicí systém jako příznakovou veličinu validity signál ze spojitého intervalu (0, 1), tedy 0% až 100%. V tomto případě se předpokládá jako verifikační algoritmus statistika nad minulými daty měřicího kanálu. Logika však je důvěrným know-how výrobce a není dostupná.
- Sofistikovanější algoritmy verifikace, za které je možné považovat například korelační metody, učící se algoritmy, metody rozpoznávání obrazců, fuzzy logiku a další, se v nabídce výrobců *ŘS* nevyskytují a ani nebyla zjištěna tendence k jejich zavedení.

Stav popsaný v předchozích odrážkách je prvotním impulzem k řešení problému verifikace a validace násobných měřicích kanálů formou předložené disertační práce, jejíž cíle jsou popsány v následující kapitole.

3 Cíle disertační práce

V současné době je kladen stále větší důraz na spolehlivost a bezpečnost průmyslových provozů. Přesto není ve světě rozhodnuto o tom, který princip logického zpracování násobných měřících kanálů je ze spolehlivostního hlediska tím nejlepším. Otázka tohoto zpracování není jednoduchá, protože je třeba uvažovat širší kontext provozovaného zařízení, jeho vztahy a vzájemné interakce s okolím a to z hlediska nejen bezpečnostního, ale také ekonomického a společenského. Z těchto důvodů se předpokládá, že neexistuje univerzální řešení nastíněného problému.

Práce si dává za cíl posoudit dosud v praxi používané přístupy ke zpracovávání měření z hlediska spolehlivosti (a tím potažmo i z ekonomického hlediska) a navrhnout nový způsob řešení výběru jedné výsledné hodnoty z násobných a výběrových měření elektrických i neelektrických veličin. Tím zacelí mezeru v problému řízení složitých průmyslových soustav na základě násobných měření s vysokým důrazem na spolehlivost a bezpečnost provozu. S využitím výsledků práce bude moci být dosaženo vyšší pohotovosti v současnosti provozovaných i navrhovaných zdrojů elektrické energie, ale i dalších průmyslových zařízení.

Cílem disertační práce je nalezení metody, která zhodnotí výhodnost jednotlivých návrhů zapojení redundovaných individuálních měřících kanálů. Toto hodnocení je provedeno na základě porovnání pohotovostí uvažovaných možností zapojení, parametrů spolehlivosti z hlediska bezpečnosti, ale i s ohledem na ekonomiku provozování. Disertační práce předkládá možný způsob řešení formou uceleného postupu pro určení nejvhodnějšího způsobu zapojení. V předložené práci je zpracována názorná aplikace uvedeného postupu na vhodně zvoleném, v praxi často používaném, příkladu. Rozhodnutí o tom, které logické zpracování informace o měřené veličině je pro konkrétní podnik nejvhodnější, však bude muset být provedeno na základě dat o provozu tohoto podniku a s pomocí předloženého postupu. Jako základní vstupní údaje budou použity údaje (expertní odhady) o poměru zjevná/skrytá a bezpečná/nebezpečná porucha v historii provozování analyzovaného systému, ale také možné následky poruchy tohoto systému na celý výrobní podnik. Zmiňované stavy prvků jsou vzájemně neslučitelné, vzájemně se vylučují a lze tedy poměrně snadno [9] vypočítat jednotlivé požadované spolehlivostní ukazatele. Předkládaná disertační práce může sloužit jako podklad pro doplnění metodického pokynu normy ČSN EN 61508 [77][75] o metodiku výběru nejvhodnějšího

zapojení násobných měřicích kanálů za účelem získání jediné výsledné hodnoty, použitelné pro řízení procesu nebo pro bezpečnostní systém.

4 Stručný přehled teorie spolehlivosti

V této kapitole jsou shrnuty základní spolehlivostní ukazatele a jejich vzájemné vztahy. Dále jsou zde popsány a demonstrovány základní typy rozdělení náhodné proměnné a možnosti zapojení elementárních prvků do složitých systémů z hlediska spolehlivosti a to včetně způsobů výpočtu hodnot jejich koncových spolehlivostních ukazatelů.

4.1 Ukazatele spolehlivosti

Před započetím definování ukazatelů spolehlivosti je třeba uvést, co se vlastně pod pojmem spolehlivost skrývá. Podle ČSN IEC 50(191) Mezinárodní elektrotechnický slovník - kapitola 191: Spolehlivost a jakost služeb [1], def. 191-02-03, je spolehlivost: Souhrnný termín používaný pro popis pohotovosti a činitelů, které ji ovlivňují: bezporuchovost, udržovatelnost a zajištěnost údržby.

V dokumentu [1] je definována řada ukazatelů spolehlivosti, pro účely disertační práce jsou však dostačující následující:

- funkce okamžité pohotovosti - $A(t)$ - def. 191-11-01
- funkce okamžité nepohotovosti - $U(t)$ - def. 191-11-02
- součinitel asymptotické pohotovosti - A - def. 191-11-05
- součinitel asymptotické nepohotovosti - U - def. 191-11-07
- pravděpodobnost bezporuchového provozu - $R(t_1,t_2)$ - def. 191-12-01
- intenzita poruch - $\lambda(t)$ - def. 191-12-02
- střední doba provozu mezi poruchami - $MTBF$ - def. 191-12-09
- střední doba do obnovy - $MTTR$ - def. 191-13-08

4.2 Výpočet základních ukazatelů spolehlivosti objektu

Pravděpodobnost nastoupení poruchy je závislá na několika parametrech, které se mohou měnit s obdobím života objektu. Intenzita poruch bývá vysoká v období zavedení objektu do provozu, neboť v tomto období se ještě mohou projevovat výrobní vady objektu. Období počáteční vysoké intenzity poruch bývá nazýváno obdobím časných poruch nebo také (zejména v elektrotechnice) obdobím „zahořování“. Po tomto období obvykle intenzita poruch klesne na určitou konstantu a s takovou pracuje po dobu svého užitečného technického života.

S postupujícím časem intenzita poruch opět roste a objekt se nachází na konci svého technického života. Tato závislost se nazývá vanová křivka pro svůj charakteristický tvar.

Pro spojitý popis poruchovosti objektů lze užít několik rozdělení:

- Normální (Gaussovo)
- Logaritmicko-normální
- Weibullovo
- Exponenciální

Pro popis diskrétního rozdělení náhodné veličiny lze potom použít např.:

- Binomické
- Poissonovo

Pro celou dobu užitečného technického života elektronických součástek se předpokládá konstantní intenzita poruch. Tento předpoklad je z hlediska řešení zadaného problému významný. Analyzovaný objekt je tvořen převážně elektronickými komponentami. Proto lze aplikovat exponenciální rozdělení času nastoupení poruchy.

Samozřejmě existuje velké množství jiných rozdělení pravděpodobnosti, ať už pro spojitý, ale také pro diskrétní popis poruchovosti objektů. Disertační práce si neklade za cíl podat ucelený přehled o všech známých rozděleních náhodné veličiny.

Hustota pravděpodobnosti nastoupení očekávané události (poruchy) pro exponenciální rozdělení je dána výrazem:

$$f(t) = \frac{1}{\nu} \cdot e^{-\frac{t-c}{\nu}} \tag{1}$$

kde:

f(t) je hustota pravděpodobnosti

ν je parametr polohy (střední hodnota náhodné proměnné - v našem případě hodnota střední doby do poruchy)

c je parametr posunutí

Předpokládáme začátek funkce posuzovaného objektu v časovém okamžiku t = 0, potom můžeme parametr posunutí považovat za nulový. Hustota pravděpodobnosti je v tomto případě dána výrazem:

$$f(t) = \frac{1}{\nu} \cdot e^{-\frac{t}{\nu}} \tag{2}$$

Exponenciální rozdělení se v odborné literatuře kromě vztahu (1) a (2) také vyjadřuje pomocí vztahu:

$$f(t) = \lambda \cdot e^{-\lambda \cdot t} \tag{3}$$

Porovnáním vztahů (2) a (3) lze odvodit vztah mezi střední dobou do poruchy a intenzitou poruch:

$$\lambda = \frac{1}{\nu} \tag{4}$$

Distribuční funkce F(t) je důležitá pro popis poruchovosti objektu. Funkce udává pravděpodobnost nastoupení očekávané události (v našem případě poruchy) do určitého časového okamžiku.

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

Často používaný doplněk k distribuční funkci, tedy funkce bezporuchovosti, se vypočítá jako:

$$R(t) = 1 - F(t) = P(T > t) = e^{-\lambda t} \tag{6}$$

kde:

R(t) je doplněk distribuční funkce, tedy funkce bezporuchovosti

F(t) je distribuční funkce

λ je intenzita poruch

Pokud lze předpokládat, že λ.t<<1, tedy v době blízké okamžiku zavádění systému do provozu nebo u vysoce spolehlivých systémů, můžeme vztah (6) zjednodušit[4] na:

$$R(t) = 1 - \lambda \cdot t \tag{7}$$

Až do tohoto okamžiku byly všechny vztahy odvozovány za předpokladu, že objekty jsou neobnovované a období jejich technického života začíná okamžikem t = 0. Pokud budeme uvažovat obnovované objekty, lze odvodit následující vztah pro ustálenou (asymptotickou) pohotovost - pohotovost za předpokladu, že se čas limitně blíží nekonečnu.

$$A(t \to \infty) = A = \frac{\mu}{\mu + \lambda} \tag{8}$$

4.3 Struktura objektu

Při analýze spolehlivosti je zapotřebí vzít v úvahu strukturu objektu. Strukturou objektu se rozumí zapojení (uspořádání) prvků, kterými je objekt tvořen.

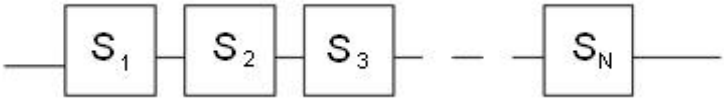
Při výpočtu spolehlivosti objektu vyznačujícího se strukturou (je tvořen více než jedním prvkem) jsou používány matematické operace s jevy (Booleova algebra) a pravidla pro sčítání a násobení pravděpodobností. Předpokládáme, že jevy (poruchy), které nastanou, jsou vzájemně disjunktní.

Zpravidla se při analýze spolehlivosti objektu vyskytují sériové, paralelní a smíšené spolehlivostní struktury zapojení prvků v objektu. Speciálním případem je výběrové zapojení. Smíšené zapojení lze rozdělit na sekvence sériově a paralelně zapojených bloků, proto nebude samostatně rozvedeno.

4.3.1 Sériové zapojení

Sériové zapojení lze blokově znázornit schématem uvedeným na obr. 3.

[4] Tento vztah je uveden pouze pro didaktickou návaznost a úplnost textu. V současné době se již nepoužívá a pracuje se s přesnými vzorci za využití výpočetní techniky.



Obr. 3: Sériové zapojení

Sériový spolehlivostní systém se nachází v bezporuchovém stavu S_s, pokud jsou všechny jeho prvky funkční a naopak poruchový stav $\overline{S}_s$ nastává, pokud je alespoň jeden z prvků systému ve stavu poruchy. Tyto stavy lze vyjádřit vztahy:

$$S_s = S_1 \cap S_2 \cap \ldots \cap S_N = \bigcap_{i=1}^{N} S_i \tag{9}$$

$$\overline{S}_s = \overline{S}_1 \cup \overline{S}_2 \cup \ldots \cup \overline{S}_N = \bigcup_{i=1}^{N} \overline{S}_i \tag{10}$$

kde S_i je bezporuchový stav i-tého prvku systému

$\overline{S}_i$ je poruchový stav i-tého prvku systému

Pravděpodobnost toho, že sériový spolehlivostní systém se nachází v bezporuchovém stavu lze vyjádřit několika vztahy. Obecně je tato pravděpodobnost dána vztahem:

$$R_S = P(S_S) = P(S_1) \cdot P(S_2) \cdot P(S_3) \cdot \ldots P(S_N) = \prod_{i=1}^{i=N} R(S_i) \tag{11}$$

kde $P(S_i)$ je pravděpodobnost bezporuchového stavu prvku *i*.

Pravděpodobnost bezporuchového stavu může být pro neobnovované objekty udána hodnotou funkce bezporuchovosti R(t). Pro obnovované objekty lze pravděpodobnost bezporuchového stavu vyjádřit hodnotou funkce pohotovosti *A(t)*. Tuto pravděpodobnost je možné vyjádřit jako okamžitou, střední (v stanoveném časovém intervalu), případně ustálenou (asymptotickou) hodnotu funkce. Ze vztahu (11) lze odvodit výraz pro okamžitou bezporuchovost a pohotovost sériového systému:

$$R_s(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \cdot \ldots \cdot R_n(t) = \prod_{i=1}^{N} R_i(t) \tag{12}$$

$$A_s(t) = A_1(t) \cdot A_2(t) \cdot A_3(t) \cdot \ldots \cdot A_n(t) = \prod_{i=1}^{N} A_i(t) \tag{13}$$

Pravděpodobnost bezporuchového provozu a pohotovost systému lze tedy stanovit z dílčích pravděpodobností prvků.

Pokud naopak chceme vyjádřit pravděpodobnost toho, že se systém nachází ve stavu poruchy, využijeme vzájemné disjunktnosti poruchového a bezporuchového stavu a pravděpodobnost poruchy systému vyjádříme jako:

$$Q_S(t) = 1 - R_S(t) \tag{14}$$

$$U_S(t) = 1 - A_S(t) \tag{15}$$

Rovnice (14) je jiným zápisem distribuční funkce náhodné proměnné (v našem případě dob do poruchy systému) a $Q_S(t)$ vyjadřuje pravděpodobnost poruchy neobnovovaného systému. Vztah (15) platí pro obnovované systémy a $U_S(t)$ je funkce nepohotovosti systému.

Známe-li časovou závislost výskytu poruchy (tj. rozdělení dob do poruchy), lze do obecného vztahu (12) dosazovat výrazy obsahující rozdělení dob do poruchy. Tak pro exponenciální rozdělení nastoupení poruchy dostaneme:

$$R_S(t) = \prod_{i=1}^{N} R_i(t) = \prod_{i=1}^{N} e^{-\lambda_i \cdot t} = e^{-\sum_{i=1}^{N} \lambda_i \cdot t} \tag{16}$$

Tento vztah říká, že pro systém s prvky, jejichž čas nastoupení poruchy podléhá exponenciálnímu rozdělení, platí také exponenciální rozdělení času nastoupení poruchy s intenzitou poruch rovnou součtu dílčích intenzit poruch prvků.

Pro obnovované objekty lze vhodně odvodit výraz pro asymptotickou pohotovost systému A_S prostřednictvím nepohotovosti:

$$A_S = 1 - U_S = 1 - (U_1 + U_2 + \ldots + U_N) + (U_1 \cdot U_2 + U_2 \cdot U_3 + \ldots + U_{N-1} \cdot U_N) \\ - (U_1 \cdot U_2 \cdot U_3 + U_2 \cdot U_3 \cdot U_4 + \ldots U_{N-2} \cdot U_{N-1} \cdot U_N) + \ldots \tag{17}$$

V případě, kdy nepohotovost prvků je dostatečně malá, lze zanedbat všechny součiny nepohotovostí. Jejich hodnoty jsou totiž nižší o několik řádů a celkovou pohotovost objektu významně neovlivní. Vztah pro pohotovost systému potom bude:

$$A_S = 1 - U_S = 1 - \sum_{i=1}^{N} U_i = 1 - \sum_{i=1}^{N} \frac{\lambda_i}{\lambda_i + \mu_i} \tag{18}$$

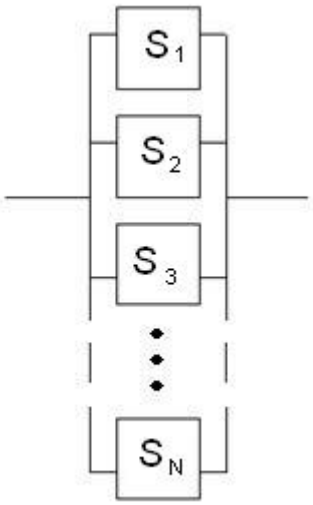
Pokud je intenzita poruch ve srovnání s intenzitou oprav zanedbatelná, je možné místo $\lambda + \mu$ uvažovat pouze hodnotu μ a předchozí vztah upravit následovně:

$$A_S = 1 - \sum \frac{\lambda_i}{\mu_i} \tag{19}$$

Je zřejmé, že při odvozování vztahů a výpočtu hodnot bezporuchovosti a poruchovosti, pohotovosti a nepohotovosti je výhodné využívat disjunktnosti jevů a dopočítávat složitě vyjádřitelnou hodnotu příslušného ukazatele spolehlivosti jako doplněk do jedné.

4.3.2 Paralelní zapojení

Paralelní zapojení lze blokově znázornit schématem uvedeným na obr. 4.



Obr. 4: Paralelní zapojení

Paralelní spolehlivostní systém je v bezporuchovém stavu S_s, pokud se alespoň jeden jeho prvek nachází v bezporuchovém stavu. Poruchový stav $\overline{S}_s$ paralelního spolehlivostního systému tedy nastává za předpokladu, že všechny prvky systému jsou ve stavu poruchy.

$$S_s = S_1 \cup S_2 \cup \ldots \cup S_N = \bigcup_{i=1}^{N} S_i \tag{20}$$

$$\overline{S}_s = \overline{S}_1 \cap \overline{S}_2 \cap \ldots \cap \overline{S}_N = \bigcap_{i=1}^{N} \overline{S}_i \tag{21}$$

kde S_i je bezporuchový stav i-tého prvku systému

$\overline{S}_i$ je poruchový stav i-tého prvku systému

Pravděpodobnost toho, že se paralelní spolehlivostní systém nachází v poruchovém stavu lze vyjádřit několika vztahy. Pokud budeme uvažovat neopravované prvky systému, bude tato pravděpodobnost dána vztahem:

$$Q_S = P(\overline{S}_S) = P(\overline{S}_1) \cdot P(\overline{S}_2) \cdot P(\overline{S}_3) \cdot \ldots \cdot P(\overline{S}_N) = \prod_{i=1}^{i=N} Q(S_i) \tag{22}$$

$P(\overline{S}_i)$ je pravděpodobnost nastoupení poruchy prvku *i*.

S využitím vztahu (14) lze dopočítat pravděpodobnost toho, že se paralelní systém nachází v bezporuchovém stavu:

$$R_S = 1 - Q_S = 1 - \prod_{i=1}^{i=N} (1 - R_i) \tag{23}$$

Pro systémy s prvky s exponenciálním rozdělením času nastoupení poruchy je možné vztah upravit:

$$R_S(t) = 1 - \prod_{i=1}^{i=N} \left(1 - e^{-\lambda_i \cdot t}\right) \tag{24}$$

Pokud budeme uvažovat obnovu prvků systému, je možné vyjádřit asymptotickou pohotovost systému:

$$A_S = \prod_{i=1}^{i=N} \frac{\mu_i}{\lambda_i + \mu_i} \tag{25}$$

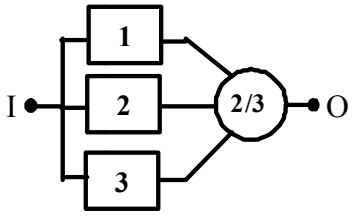
Asymptotickou nepohotovost systému pak vyjádříme jako doplněk vztahu (25) do jedné.

Bezporuchovost (a její doplněk do jedné - pravděpodobnost poruchy) bývá počítána zejména u neopravovaných objektů, zatímco pohotovost resp. nepohotovost je parametr, vztahovaný k obnovovaným prvkům. Ovšem i u neopravovaného objektu lze provést výpočet pohotovosti. Postačuje vyhodnocovat pohotovost funkce, kterou objekt vykonává, nikoli pohotovost samotného objektu. Právě výpočet pohotovosti, resp. bezporuchovosti je jedním z cílů předkládané disertační práce.

4.3.3 Výběrové zapojení

Výběrové zapojení „*K z N*" je takové propojení *N* prvků z hlediska spolehlivosti, kdy ke správné funkci systému postačí funkčnost pouze *K* prvků. Na obr. 5 je uveden příklad výběrového zapojení a sice výběrové zapojení 2 ze 3. Ke správné funkci systému postačuje funkčnost libovolných dvou prvků systému.

Matematicky je v případě tohoto zapojení možné vyjádřit počet možných funkčních stavů pomocí počtu větví *N* a nutného počtu funkčních větví *K* jako kombinaci bez opakování *C*.



Obr. 5: Výběrové zapojení 2 ze 3

$$C = \binom{n}{k} = \frac{n!}{k!\cdot(n-k)!} \tag{26}$$

Vzorec pro výpočet pravděpodobnosti bezporuchového provozu je potom možné napsat jako:

$$R_S = \sum_{i=k}^{i=n} \binom{n}{i} \cdot p^i \cdot (1-p)^{n-i} \tag{27}$$

Tento vzorec je univerzální pro všechna výše zmíněná spolehlivostní zapojení. Pokud za *K* dosadíme jedničku, bude se jednat o čistě paralelní systém, zatímco pokud bude *K* rovno *N*, dostaneme matematický model sériového systému.

Vzhledem k tomu, že výběrové zapojení bude stěžejním tématem zkoumaného problému, bude zde naznačeno několik možností a variací chápání tohoto typu zapojení. Mezi nejjednodušší modely každého, nejen výběrového, spolehlivostního zapojení patří tzv. dvoustavový model. Takovýto model předpokládá prvky systému pouze ve dvou možných stavech - stavu provozuschopném a stavu poruchovém. Toto dělení je v praxi často dostačující, provozovatele zařízení zajímá zejména funkčnost/nefunkčnost provozovaného zařízení. V této práci však bude uvažováno vícestavové hodnocení prvků systému. Toho lze opět dosáhnout několika způsoby. Prvním možným způsobem je tzv. „váhování“ funkce prvku [7], tím druhým analyzovaným pak rozdělení poruchového stavu prvku podle závažnosti a zjevnosti poruch [10].

Princip metody váhování funkce prvku spočívá v nalezení úrovně důležitosti funkce prvku pro funkci celého systému. Každému prvku bude přiřazena „váha“ W_i, součet všech vah, který udává neomezenou funkci systému, potom bude:

$$W = \sum_{i=1}^{i=N} W_i \tag{28}$$

Pro splnění funkce systému však není nezbytně nutné, aby bylo dosaženo maximálního možného součtu vah (kdyby tomu tak bylo, jedná se o speciální mutaci váhového výběrového systému - sériový systém). Ke splnění funkce stačí „nějaká“ předem zvolená úroveň váhy w.

Jako příklad pro snazší pochopení problematiky je v [7] uvedena rozvodná síť elektrické energie. Ta je složena z většího množství vodičů, z nichž každý má určenou váhu podle své maximální transportní kapacity. Tato kapacita s časem klesá s degradujícími vlastnostmi vodiče a s tím klesá i „váha“ jednotlivého vodiče vzhledem k systému rozvodné sítě. Při poklesu součtu všech „vah“ pod předem stanovenou úroveň dojde ke ztrátě funkce celé rozvodné sítě. Výhodou tohoto přístupu je možnost okamžité identifikace slabých míst systému, predikce poruch systému, možnost modelování systému složeného ze součástek s různými (i spolehlivostními) parametry, ovšem nevýhodou je obtížné měření stavu prvků systému.

Druhá zmiňovaná možnost separace poruchového stavu je bližší praxi, protože provozovatel zařízení má k dispozici častěji údaje o poruchách, než záznamy o degradovaných a stále ještě funkčních stavech prvků. Z těchto záznamů je možné rozhodnout, zda se jednalo

o poruchu bezpečnou nebo nebezpečnou, zjevnou nebo skrytou. Tímto dělením poruch se budeme zabývat v aplikačních kapitolách práce.

4.3.4 Ukazatele spolehlivosti násobných zapojení

Pro výše popsané typy zapojení více prvků do jednoho systému je možné dopočítat hodnoty ukazatelů spolehlivosti. Postačující podmínkou k takovým výpočtům je znalost dílčích parametrů spolehlivosti každého prvku. Podrobně se touto problematikou zabývá [9]. Vztahy pro výpočet pohotovosti, resp. nepohotovosti a pravděpodobnosti bezporuchového provozu byly uvedeny v předchozích kapitolách. Pro účely této práce bude dále uveden pouze vztah pro výpočet střední doby mezi poruchami systému, sestávajícího z několika prvků. Tento vztah je znám pod názvem Schneeweissova formule.

$$\frac{U_S}{MTTR_S} = \left(\sum_{i=1}^{i=N} \frac{1}{MTTR_i} \right) \cdot \prod_{k=1}^{k=N} U_k \tag{29}$$

Přínosem vztahu (29) je možnost vypočítat střední dobu provozu mezi poruchami systému ze znalosti parametrů spolehlivosti jeho dílčích prvků. Tento výpočet předpokládá, že nepohotovost systému je dána poměrem střední doby do obnovy a střední doby provozu mezi poruchami systému, tedy:

$$U_S = \frac{MTTR}{MTBF} \tag{30}$$

Tento předpoklad je akceptovatelný u vysoce spolehlivých zařízení (které tato práce předpokládá), kde *MTBF >>MTTR*. Schneeweissovu formuli je potom možné zapsat jako:

$$\frac{1}{MTBF_S} = \left(\sum_{i=1}^{i=N} \frac{1}{MTTR_i} \right) \cdot \prod_{k=1}^{k=N} U_k \tag{31}$$

Tato rovnice umožňuje výpočet střední doby provozu mezi poruchami systému ze znalosti střední doby obnovy a nepohotovosti prvků. Hodnotu střední doby provozu mezi poruchami systému je možné považovat za porovnávací ukazatel u bezpečných poruch, kdy je tato hodnota de facto rovna střední době mezi falešnými zapůsobeními systému.

4.4 Vybrané metody analýz spolehlivosti

Oblast spolehlivosti disponuje různými metodami k hodnocení systémů. Díky nim lze predikovat spolehlivostní ukazatele nebo identifikovat kritická místa systému, na která je pak možné aplikovat nápravná opatření. Obecně se spolehlivostní analýzy dělí do tří základních skupin: analýzy kvalitativní, semikvantitativní a kvantitativní. Zatímco u kvalitativních analýz je výsledkem slovní hodnocení či schéma, kvantitativní analýzy přiřazují událostem i číselné hodnoty. Speciální skupinou kvantitativních analýz jsou analýzy semikvantitativní, které namísto hodnocení pomocí reálných hodnot s fyzikálním významem pracují s bezrozměrnými hodnotami ve zvolených stupnicích, běžně 1-5 nebo 1-10. Existují metody, které lze provádět na úrovni kvalitativní i kvantitativní. Tato úroveň se volí na základě požadavků na výstupy analýz nebo dle dostupných vstupních dat.

V současné praxi se při provádění analýz spolehlivosti můžeme setkat zejména s následujícími metodami:

- analýza způsobů a důsledků poruch (FMEA)
- analýza způsobů, důsledků a kritičnosti poruch (FMECA)
- metoda blokových diagramů bezporuchovosti (RBD)
- metoda výpočtu bezporuchovosti z dílů (PC)
- metoda analýzy stromu poruchových stavů FTA, resp. stromů událostí ETA
- Markovova analýza (MA)

Tab. 1: Přehled analýz spolehlivosti a vhodnosti jejich použití

Metoda / Vlastnost	Vhodné pro:				Symbolická reprezentace	Přístup deduktivní / induktivní
	Počet komponent	Zálohované struktury	Závislé události	Strategie údržby		
FMEA	až tisíce	ne	ne	ne	seznam	induktivní
FMECA	až tisíce	ne	ne	ne	seznam	induktivní
RBD	až tisíce	ano	ano	ne	blokový diagram	deduktivní
PC	až stovky	ne	ne	ne	seznam	induktivní
FTA	až tisíce	ano	ano	ne	strom poruch	deduktivní
ETA	2 až 50	ano	ano	ne	strom událostí	deduktivní
MA	2 až 100	ano	ano	ano	stavový diagram	induktivní

Jak je patrné z tab. 1, každá metoda má své charakteristické uplatnění na základě velikosti analyzovaného systému, možnosti použití zálohovaných struktur atd.

Stručný popis jednotlivých výše zmíněných metod spolehlivostních analýz je uveden v následujících kapitolách. Disertační práce si neklade za cíl detailně rozebírat jednotlivé metody, takový popis je uveden v [1].

4.4.1 Analýza způsobů a důsledků poruch (FMEA)

FMEA (Fault Mode and Effects Analysis) je induktivní spolehlivostní metoda, vhodná pro analýzu velkých systémů. Jedná se o kvalitativní metodu. Začíná u nejnižšího stavebního prvku systému a postupuje k funkčním celkům, klasifikuje diagnostikovatelnost, opravitelnost a jiné charakteristické rysy součástek. Metoda je použitelná pro určení kritických prvků systému. Používá se v období návrhu a vývoje výrobku, má za úkol snížit náklady na výrobu včasnou diagnostikou kritických míst. Předpokladem pro úspěšné provedení analýzy FMEA je detailní znalost funkcí analyzovaného systému a znalost důsledků poruch jednotlivých komponent na funkce systému. [1], [14], [19]

4.4.2 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)

FMECA (Fault Mode, Effects and Criticality Analysis) je rozšířením metody FMEA o hodnocení kritičnosti. Jedná se již o metodu obsahující kvantitativní prvky. Protože kritičnost bývá zpravidla udávána formou rozsahu bodů stupnice kritičnosti a ohodnocení kritičnosti závisí na uvážení analytika, mohou se v jiné analýze stejného problému hodnoty lišit. Hodnoty kritičnosti tedy nejsou exaktní a proto je FMECA řazena mezi semikvantitativní metody spolehlivosti. Lze však porovnávat kritičnosti jednotlivých prvků a tím analyzovat kritická místa systému. Metoda je vhodná pro určení míry rizika rozsáhlých systémů, ovšem stejně jako metoda FMEA nepokrývá svými možnostmi chyby člověka a poruchy vnějšího prostředí. [1], [19]

4.4.3 Metoda blokových diagramů bezporuchovosti (RBD)

RBD (Reliability Block Diagram) je deduktivní metoda predikce bezporuchovosti. Spolu s analýzou blokového diagramu poruchy tvoří množinu analýz logických blokových diagramů. Prvky systému jsou znázorněny pomocí bloků a vazby mezi těmito komponentami jsou znázorněny hranami. Prvky musí být propojeny takovým způsobem, aby výsledné schéma reprezentovalo úplnou logiku systému. Výstupem analýzy je blokové schéma systému. V přehledném logickém diagramu lze snadno určit minimální úspěšné cesty systému. [15], [19]

4.4.4 Metoda výpočtu bezporuchovosti z dílů (PC)

PC (Part county) je induktivní metoda vhodná k odhadu přibližné intenzity poruch systému za předpokladu, že jeho poruchu způsobí porucha libovolného prvku (tzv. sériový poruchový model). Poskytuje předpověď bezporuchovosti systému na přijatelné úrovni přesnosti. Metoda se používá většinou během časných etap návrhu, zejména pro elektronická zařízení a systémy. Odhad spolehlivostních parametrů metodou PC dává konzervativní hodnoty (pesimistický odhad), což je způsobeno právě předpokladem sériového modelu systému (porucha jednoho libovolného prvku způsobí poruchu celého systému). [19]

Při analýze spolehlivosti pomocí počítání z dílů se často využívají databáze spolehlivostních parametrů, z nichž mezi nejznámější patří tzv. Military Handbook. [22] V tomto textu jsou uvedeny intenzity poruch (většinou elektronických) součástek. Výsledná intenzita poruch je závislá na základní intenzitě poruch a dále na multiplikativních faktorech, jako jsou např. koeficienty závislosti:

- na teplotě,
- na druhu použití,
- na jmenovitém výkonu,
- na elektrickém zatížení,
- na konstrukci,
- na kvalitě,
- na prostředí
- atd.

Základní intenzita poruch je známa ze zkušenosti a vychází ze sběru dat od výrobců a uživatelů součástek.

4.4.5 Metoda analýzy stromu poruchových stavů (FTA)

FTA (Fault Tree Analysis) je deduktivní metoda, vyvinutá pro analýzu možných poruchových stavů systému. Metoda pro vrcholovou událost nalezne požadovanou kombinaci stavů prvků na nejbližší nižší úrovni systému. Graficky zobrazuje vztahy mezi poruchovými stavy prvků systému, vztahy mezi stavy prvků na shodné úrovni analýzy systému jsou dány pomocí logických operací jako AND, OR apod. Opakováním postupu bude analyzován celý související systém až do nejnižší požadované úrovně. Metoda je vhodná zejména pro kvalitativní analýzu rozsáhlých systémů, ovšem jednotlivá hradla lze ohodnotit a s využitím Booleovy algebry následně metodu použít i kvantitativně. Kvantitativní analýza je v současné době standardem metody analýzy stromu poruchových stavů. [1], [17], [19]

4.4.6 Metoda analýzy stromu událostí (ETA)

ETA (Event Tree Analysis) je induktivní metoda, určená k nalezení možných kombinací jevů, vedoucích k nastoupení iniciační události. Každá iniciační událost má minimálně jednu podmínku nastoupení. Strom událostí zkoumá pravděpodobnost nastoupení této události na základě binární logiky, kdy odpovídá na otázku, zda podmínka k nastoupení iniciační události nastala či nikoliv. Každý jev, vedoucí k nastoupení iniciační události je ohodnocen pravděpodobností poruchového/bezporuchového stavu a výsledná pravděpodobnost nastoupení iniciační události je logickou kombinací těchto dílčích pravděpodobností. Metoda je vhodně aplikovatelná zejména pro jednodušší systémy. Výstupem této metody je grafické znázornění vztahů mezi možnými jevy. [19]

4.4.7 Markovova analýza (MA)

MA (Markov Analysis) je induktivní metoda, používající matematické modely a teorii Markovových řetězců. Metoda je použitelná pro analýzu složitých systémů, vyžaduje však znalost všech možných stavů systému. Kvalitativní určení diagramu přechodů lze ohodnotit spolehlivostními parametry a tím získat kvantitativní řešení analýzy. Metoda je vhodná pro určení strategií oprav a údržby funkčně složitých systémů. [18], [19]

4.5 Spolehlivost v analýzách bezpečnosti

Standardní výpočetní metody spolehlivosti využívají mnoho zjednodušení. Jedním z nejčastějších je uvažování pouze jedné poruchy komponenty v časovém intervalu. To znamená, že studie nepředpokládá poruchu druhé (třetí atd.) komponenty v okamžiku, kdy je jakákoliv jiná komponenta v poruchovém stavu. Takovéto zjednodušení je možné u nepříliš složitých systémů, které jsou složeny z nízkého počtu komponent, a jejichž střední doba do obnovy prvku je výrazně nižší, než střední doba mezi poruchami. Zcela odlišná situace nastává v případě složitých technologických celků. Zde je nutno uvažovat souběh nepříznivých událostí - poruchu prvku v okamžiku, kdy systém není v bezporuchovém stavu. Dalším podobným nepříznivým jevem je nastoupení poruchy se společnou příčinou. Všechny tyto události přispívají k celkovému ročnímu riziku provozování průmyslového zařízení.

4.6 Zálohované systémy

Jaderná elektrárna je v lidském podvědomí chápána jako velký zdroj rizika. Nejen proto je při jejím provozování kladen vysoký důraz na její bezpečnost. Za účelem sledování bezpečnosti vzniklo hodnocení provozních událostí, které se dělí na kategorie INES 0, tedy odchylky, při kterých nejsou porušeny limity a podmínky provozu a INES 1, kdy tyto limity a podmínky porušeny jsou. Mezi události, které spadají do kategorie INES 1 patří např. rychlé odstavení reaktoru, neúmyslná aktivace bezpečnostních systémů bez významných následků či menší rozšíření kontaminace uvnitř kontrolovaného pásma bez důsledků pro bezpečnost. [3] Překročení těchto limitů je trestáno státem. Z tohoto důvodu je ze strany ČEZ, a.s. kladen velký důraz na dodržování limitů. Management limitů rizika však není systematický, je pouze zpětně dopočtena hodnota rizika pro účely zprávy. V průběhu provozování bloku nemá operátor informaci, s jakým aktuálním rizikem (např. přepočteným na roční hodnotu) systém právě pracuje.

Je nutné si uvědomit, že riziko provozu průmyslového zařízení roste s každou poruchou, kdy se ze zálohovaných zapojení stane zapojení s nižším stupněm zálohování. Ve speciálním případě paralelního zapojení pouze dvou strojů/zařízení dojde k úplnému zrušení zálohování a následná porucha druhého stroje způsobí výpadek celého systému. V obecném případě tedy dojde ke snížení stupně zálohování (např. systém 3/4 se redukuje na systém 2/3 apod.) a tím i ke zvýšení nebezpečí výpadku celého systému. Bohužel, běžná výběrová zapojení nejsou schopná redukovat s výpadkem jednoho prvku svou výběrovou logiku a potom se ze zapojení 3/4 stane zapojení 3/3. Výpadek jednoho dalšího prvku vyvolá ztrátu věrohodnosti celého výběrového zapojení. Proto je nutné klást důraz nejen na spolehlivost použitých komponent, ale i na logiku zapojení těchto prvků a na následné zpracování signálu.

Doba, kdy je zařízení v poruchovém stavu ovšem není jedinou dobou, která snižuje výslednou spolehlivost zařízení. Z důvodu prevence skrytých (latentních) poruch na jednotlivých prvcích měřících obvodů se provádí pravidelné testování jejich jednotlivých součástí. Je třeba si uvědomit, že také v době testování je prvek odpojen od provozního kontextu a není možné ho uvažovat ve výběrové logice. Ve výše zmíněném případě by potom za předpokladu testování jednoho prvku z výběrového zapojení 3/4 , redukovaného na 3/3, stačila porucha jednoho (aktuálně netestovaného) prvku a nastala by porucha celého výběrového členu. Je vidět, že i úkony, prováděné kvůli odhalování poruch a zvýšení dlouhodobé spolehlivosti provozovaného zařízení, vedou ke snížení aktuální spolehlivosti a tím ke zvýšení příspěvku testovaného zapojení k výslednému riziku.

Skryté poruchy jsou zřejmě nejčastější příčinou ztráty funkce každého systému. Je to dáno jejich dlouhou dobou do obnovy. Do této doby totiž patří také doba do odhalení, logistické zpoždění a technické zpoždění při odstraňování poruchy. Metody analýz spolehlivosti nejsou většinou primárně určeny pro modelování skrytých poruch, je však možné tyto poruchy modelovat právě pomocí dlouhé doby do obnovy funkce systému. Mizí tím ale informace o různých druzích poruch - zjevných a skrytých. Teorie spolehlivosti často rozlišuje pouze dva stavy komponent a to stav provozuschopný a neprovozuschopný. Modelování poruchovosti vícestavových systémů je možné pomocí Markovovy analýzy. [21] Ta je ovšem výpočetně složitá a náročná na vyhodnocení. Tato práce řeší problém vícestavových systémů pomocí pravdivostní tabulky, která vyčerpávajícím způsobem pokrývá všechny možné stavy systému.

5 Spolehlivost ve vybraných publikacích

5.1 Validace signálu v odborných publikacích

Je relativně obtížné nalézt publikaci, která by komplexně postihovala oblast zájmu této disertační práce. Tato kapitola postihuje články v odborných publikacích, které mají nějaký vztah k problematice verifikace a validace výsledné hodnoty, vypočítávané z násobných měření jedné fyzikální veličiny.

Článek [80] popisuje vliv bezpečné poruchy na výslednou spolehlivost bezpečnostních systémů s přihlédnutím ke skutečnostem, uvedeným v normě IEC 61508, jako je stupeň vyžádání služby a jeho vliv na celkovou úroveň bezpečnosti (SIL) celého systému. Chování takového systému je modelováno pomocí Markovských procesů.

Problematika systémů, u kterých je vyžadována vysoká úroveň integrity bezpečnosti, je postižena také v [81]. Autor se věnuje systémům, používaným v petrochemickém průmyslu. V textu se vyskytuje zmínka o nedokonalosti sady norem IEC 61508, kdy není definováno, jakou metodu analýzy spolehlivosti je vhodné použít pro systémy s nízkým/vysokým vyžádáním služby.

Důležitým předpokladem pro výpočty spolehlivosti výběrových členů je vzájemná nezávislost individuálních vstupů do vyhodnocovacího členu. Touto problematikou se zabývá např. [82], kde je navíc připomenuto, že i preventivní údržba má vliv na výslednou pohotovost výběrového systému, protože v době, kdy se tato údržba provádí, není vlastně udržovaný vstup ve stavu schopném plnit požadovanou funkci.

Výběrovým zapojením se zabývá např. [83]. Jednotlivým vstupním kanálům je přiřazena hodnota, udávající stupeň jejich spolehlivosti. Jednotlivé vstupy tedy nemají pouze atribut „dobrý“ / „špatný“, ale je možné klasifikovat je více stupni spolehlivosti. Na základě poznatku o kvalitě vstupního signálu je potom dále možné upravit vyhodnocovací algoritmus. V článku však není vypočtena výsledná pohotovost takovéhoto zapojení a také není porovnáno toto zapojení s dalšími používanými možnostmi.

Článek [84] na mezinárodní konferenci o bezpečnosti a spolehlivosti pojednává o údržbě systémů „*k* z *n*“. Je v něm nadefinován minimální počet funkčních komponent, se kterým je možné zahájit údržbu, aniž by byla ohrožena správná funkce celého systému. Tato úroveň je závislá na dostupnosti náhradních dílů a pracovníků údržby.

Problematikou zálohovaných výběrových systémů se zabývá také [85]. V tomto textu je věnována pozornost zejména problematice výpočtu výsledné spolehlivosti výběrového zapojení pro netriviální konfigurace, kdy počet prvků, nutných ke správné funkci celého výběrového systému „*k* z *n*“, není z množiny {1, 2, n-2, n-1, n}.

Problém nalezení optimálního stupně zálohování je řešen v publikaci [86]. Autoři předpokládají sério-paralelní strukturu systému a úroveň spolehlivosti je podle nich zvyšována pouze pomocí zvyšování zálohovanosti paralelních subčástí. Spolehlivost celého systému je optimalizována vzhledem k nákladům na tento systém. Příspěvek uvažuje vícestavové prvky, jako příklad budiž uveden generátor, který může pracovat v plném výkonu, ostrovním provozu nebo být zcela nefunkční.

5.2 Spolehlivost v technické normalizaci

Každé odvětví lidské činnosti s sebou nese určitá rizika. Abychom tato rizika minimalizovali, shromažďují se poznatky a zkušenosti do „návodů“, jak danou činnost vykonávat co nejlépe. Takovými dokumenty jsou pro oblast spolehlivosti zejména technické normy. V této kapitole bude uveden přehled norem se vztahem k problematice spolehlivosti a u každé normy bude stručný komentář obsahu této normy. K sestavení tohoto přehledu byly využity informace, získané od RNDr. Jaroslava Matějčka, CSc., odpovědného v rámci TNK 5 za zpracování a překlady norem z oboru spolehlivosti.

5.2.1 Normy pro zabezpečovací systémy

V této kapitole jsou uvedeny normy pro sdělovací a zabezpečovací systémy zařízení energetiky a normy pro zajištění funkční bezpečnosti elektronických systémů souvisejících s bezpečností. Tyto normy, přestože jsou založeny na problematice spolehlivosti a odvolávají se na normy spolehlivosti, byly vypracovány technickou normalizační subkomisí IEC 65A „Systémové aspekty“, pracující pro technickou komisi IEC TC 65 „Měření a řízení průmyslových procesů“. Překlad této skupiny norem do ČSN řešila technická normalizační komise TNK 56 „Elektrické měřicí přístroje“. Tato skutečnost negativně ovlivnila srozumitelnost norem. Běžný uživatel, který není detailně seznámen s problematikou spolehlivosti, pak s obtížemi chápe souvislosti popisované v této normě.

Předkládaná disertační práce si klade za cíl doplnit mezeru v této skupině norem. Jedná se zejména o nejasnosti při výběru validní informace při násobném měření jedné fyzikální veličiny za účelem zvýšení spolehlivosti výsledného signálu.

Mezinárodní norma [72] je první částí sedmidílného souboru evropských norem EN 61508 uváděných pod společným názvem "Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností", který stanovuje obecný přístup pro všechny životní cykly bezpečnosti elektrických a/nebo elektronických a/nebo programovatelných elektronických (E/E/PE) systémů používaných pro zajišťování bezpečnostních funkcí. První čtyři části z tohoto souboru jsou základní bezpečnostní normy. Hlavním cílem celé normy je možnost použití jednotného, racionálního a konzistentního technického přístupu u všech elektrických systémů související s bezpečností včetně usnadnění tvorby dalších aplikačních oborových norem. Vzhledem ke svému obecnému charakteru poskytuje norma také určitý základní rámec, na jehož základě je možné posuzovat i systémy související s bezpečností, založené na jiných technických principech. V části 1 jsou stanoveny všeobecné požadavky na E/E/PE systémy související s bezpečností, které jsou použitelné ve všech ostatních konkrétně zaměřených částech této normy.

2. část normy 61508 [73] stanovuje požadavky na E/E/PE systémy související s bezpečností.

3. část normy 61508 [74] stanovuje požadavky na software E/E/PE systémů souvisejících s bezpečností.

4. část normy 61508 [75] uvádí základní definice a zkratky používané v celém sedmidílném souboru norem 61508 a umožňuje tím jednotný výklad pojmů a zajišťuje srozumitelnost těchto norem.

5. část normy 61508 [76] uvádí příklady metod určování úrovní integrity bezpečnosti E/E/PE systémů.

6. část normy 61508 [77] uvádí metodické pokyny a příklady pro použití částí 2 a 3 této řady norem.

7. část normy 61508 [78] přímo souvisí s částmi 2 a 3 a uvádí stručný přehled různých bezpečnostních technik a opatření využívaných pro zajišťování bezpečnosti jak hardwaru, tak softwaru E/E/PES souvisejících s bezpečností.

Hlavním cílem normy EN 61508 je možnost používání jednotného, racionálního a konzistentního technického přístupu u všech elektrických systémů související s bezpečností včetně usnadnění tvorby dalších aplikačních oborových norem, což tato norma, vzhledem ke svému obecnému charakteru, umožňuje. Vzhledem ke svému charakteru může tato mezinárodní norma, přestože se zaměřuje na E/E/PES související s bezpečností, poskytnout také určitý základní rámec, na jehož základě je možné posuzovat i systémy související s bezpečností založené na jiných technických principech.

Soubor norem 61508 popisuje systémy související s bezpečností a kvantifikuje pravděpodobnosti nastoupení poruchy na vyžádání, resp. pravděpodobnost poruchy za hodinu do čtyř skupin tzv. úrovně integrity bezpečnosti. Této úrovně je možné dosáhnout s pomocí dokonalé znalosti architektury použitého bezpečnostního systému. Ovšem jak uvádí [72]: „Jednotlivý E/E/PE systém související s bezpečností neznamená nutně jednokanálovou architekturu.“ Norma však neřeší problematiku vícekanálových systémů z pohledu verifikace a validace údajů o měřené veličině.

V dalším textu této normy není dále rozveden problém vícekanálových systémů. Tento nedostatek řeší předkládaná disertační práce. Je v ní obsažena analýza několika možností spojení více vstupů (kanálů) do jedné výsledné hodnoty a dále jsou v ní porovnány parametry spolehlivosti těchto rozdílných algoritmů spojování (kombinace) násobných vstupů do výsledné řídicí resp. bezpečnostní informace.

V normě [79] se stanoví, co se má uvážit při prezentaci informací týkajících se předpovědí kvantitativních ukazatelů bezporuchovosti, udržovatelnosti a pohotovosti systémů a zařízení, včetně hardwaru, softwaru a lidských faktorů. Účelem této normy je poskytnout autorovi zprávy o předpovědi spolehlivosti a seznam všech položek, které musí být vzaty v úvahu, aby byla prezentace předpovědi správná a úplná.

Činnosti popsané v publikacích, uvedených v této kapitole, je možné provádět pouze se znalostí širších souvislostí teorie spolehlivosti. Z tohoto důvodu budou uvedeny normy z oblasti spolehlivosti, které pokrývají zkoumanou oblast. Ke každé uvedené normě bude také uveden její stručný obsah a přehled témat, kterých se norma týká.

5.2.2 Názvoslovné normy spolehlivosti

V oboru spolehlivosti, stejně jako v jiných technických oborech, se používají speciální odborné termíny, které jsou definovány v základních názvoslovných normách a jsou používány ve všech ostatních normách z tohoto oboru. Bez prostudování těchto názvoslovných norem je text ostatních norem obtížně pochopitelný nebo může dokonce dojít k jeho nesprávnému výkladu a k nedorozuměním.

Základní názvoslovná norma z oboru spolehlivosti [1] obsahuje definice pojmů a ekvivalenty termínů z tohoto oboru v 11 jazycích. Slovensky, česky a anglicky je definováno několik set hesel. Je opatřena abecedními rejstříky definovaných termínů ve všech 11 jazycích. Je všeobecně využitelná jako základní názvoslovná norma pro management spolehlivosti zařízení a služeb pro energetiku. Je nezbytná pro porozumění a jednotné používání základních termínů z oboru spolehlivosti.

Norma [23] obsahuje názvosloví z oboru spolehlivosti, používané v oboru informačních technologií. Česky a anglicky je definováno cca 42 hesel.

V normě [24] jsou specifikovány generické (základní) termíny a definice pro technické, administrativní a manažerské oblasti údržby. Česky a anglicky je v ní definováno cca 110 hesel. V přílohách je doplněna vysvětlujícími obrázky a tabulkami. Je využitelná k řádnému pochopení a jednotnému používání terminologie z oboru údržby zařízení energetiky.

5.2.3 Normy pro management kvality

Management kvality je běžnou součástí managementu organizace a v jeho rámci se provádí management spolehlivosti a ostatních činností v rámci RAMS. Normy z oboru managementu kvality jsou nadřazeny nad všechny ostatní normy, které je nutné v tomto smyslu chápat jako normy navazující.

V mezinárodní normě [25] jsou popsány základy a zásady systémů managementu kvality, které jsou předmětem norem souboru ISO 9000. Tato mezinárodní norma se týká

a. organizací, které se snaží získat výhody uplatňováním systému managementu kvality,
b. organizací, které se snaží získat důvěru, že jejich dodavatelé požadavky na produkty splní,
c. uživatelů produktů,

d. všech, kteří mají zájem na vzájemném pochopení terminologie používané v managementu kvality (např. dodavatelé, zákazníci, kompetentní orgány),
e. všech osob, které posuzují systém managementu kvality nebo provádějí jeho audit z hlediska shody s požadavky ISO 9001 (např. auditoři, kompetentní orgány, certifikační/registrační orgány),
f. všech osob, které poskytují poradenství nebo školení/výcvik týkající se systému managementu kvality, který je vhodný pro tuto organizaci,
g. zpracovatelů souvisících norem.

Je tato norma všeobecně využitelná jako základní norma pro systémy managementu kvality, jejíž použití je nezbytné pro pochopení terminologie a základů systémů managementu kvality zařízení a služeb pro energetiku.

5.2.4 Normy pro management spolehlivosti

Je třeba, aby dodavatel zařízení a služeb pro energetiku vytvořil a udržoval systém managementu spolehlivosti ke směrování a řízení spolehlivostních činností a ostatních činností ovlivňujících jak spolehlivost, tak i bezpečnost jeho produktu. Systém managementu spolehlivosti má být nedílnou součástí celkového systému managementu této organizace. Normy pro management spolehlivosti jsou v IEC vydávány v souboru norem IEC 60300 a postupně jsou doplňovány a starší verze jsou revidovány. Tyto normy IEC jsou zavedeny do následujících ČSN.

V normě [26] jsou popsány pojmy a principy systémů managementu spolehlivosti. Tato norma se zabývá problémy spolehlivosti v jednotlivých etapách životního cyklu produktů v oblasti plánování, navrhování, měření, analýzy a zlepšování spolehlivosti. Cílem této normy je usnadnit součinnost všech zúčastněných stran (dodavatele, organizace a zákazníka) a dosáhnout pochopení potřeb a významu spolehlivosti k dosažení celkových cílů spolehlivosti produktu.

Norma [27] navazuje na ČSN EN 60300-1 a navazují na ni další normy pro management spolehlivosti. Je v ní zaveden pojem životní cyklus produktu a pojednává se v ní o významných spolehlivostních činnostech a jejich načasování pro jejich efektivní uplatnění ke zlepšení spolehlivosti. Je v ní popsána návaznost jednotlivých etap životního cyklu produktu na příslušné prvky a úkoly programu spolehlivosti pro snadnější přizpůsobení programů spolehlivosti potřebám specifického projektu.

Metody analýzy spolehlivosti popsané v této normě [28] se používají k předpovědím, přezkoumání a zlepšování bezporuchovosti, pohotovosti a udržovatelnosti objektu. Tyto analýzy se provádějí v etapě koncepce a stanovení požadavků, v etapě návrhu a vývoje a v etapě provozu a údržby na různých úrovních a stupních rozčlenění pro vyhodnocení a stanovení ukazatelů spolehlivosti objektu. Je zde uveden přehled obecně používaných technik analýzy spolehlivosti.

Norma [29] je zaměřena na problémy základní filosofie sběru dat, jako je vzorkování či cenzurování dat a sběr dat v časových oknech. Je v ní též uveden návod týkající se přesnosti a shodnosti dat, technik automatického sběru dat a správcovství dat.

V normě [30] se poskytuje obecný návod pro provádění analýzy životního cyklu včetně vypracování modelu nákladů životního cyklu a jsou v ní uvedeny názorné příklady.

V normě [31] jsou uvedeny pokyny pro specifikování požadovaných ukazatelů spolehlivosti ve specifikacích výrobků a zařízení spolu se specifikacemi postupů a kritérií ověřování.

Tato norma [32] slouží jako návod pro volbu použitelných norem pro zkušební podmínky a statistickou analýzu. Je to též všeobecný návod k plánování, provádění a analýze dat ze zkoušek bezporuchovosti. Pomocí této normy je uživatel schopen zvolit jiné normy, které jsou vhodné a nezbytné pro plánování, provádění a analyzování dat získaných při specifické zkoušce bezporuchovosti. Tato norma obsahuje odkazy na statistické nástroje pro analýzu konstantního i nekonstantního parametru proudu poruch a intenzity poruch i jiných ukazatelů, jako je podíl úspěšných pokusů/podíl poruch.

V normě [33] je vysvětlena koncepce, účel a oprávněnost procesu třídění. Jsou v ní uvedeny hlavní prvky programu třídění spolu s obecným postupem jeho plánování.

V normě [34] se poskytují směrnice pro volbu a realizaci technik analýzy rizika, především pro posuzování rizika spojeného s technologickými systémy. Cílem této normy je zajistit kvalitu a vzájemný soulad plánování a provedení analýz rizika a prezentace jejich výsledků a závěrů.

Norma [35] se používá při vypracování a uplatňování programu udržovatelnosti, pokrývajícího etapy zahájení, vývoje a provozu výrobku, který je součástí úkolů popsaných v ČSN IEC 60300-2. V této normě se poskytuje návod na to, jak se u těchto úkolů mají brát v

úvahu hlediska údržby, aby se dosáhlo optimální udržovatelnosti. Norma svým zaměřením ovlivňuje také oblast udržovatelnosti, o které bude pojednáno v následující kapitole.

Údržba zaměřená na bezporuchovost (RCM), popsaná v normě [36], je metoda pro zavedení programu preventivní údržby, který umožní účelně a účinně dosáhnout požadované úrovně bezpečnosti a pohotovosti zařízení a konstrukcí. Konečným výsledkem práce je posouzení nutnosti provádění konkrétních úkolů údržby.

Náklady na logistické zajištění značně přispívají k nákladům životního cyklu produktu a je nutné je brát v úvahu při rozhodování o jeho nákupu. Integrované logistické zajištění popsané v normě [37] je metoda managementu, jejíž pomocí se všechny služby logistického zajištění sestavují strukturovaným způsobem v souladu s daným produktem, což umožňuje optimalizovat jeho řešení, aby bylo přínosem jak pro zákazníka, tak pro dodavatele.

V normě [38] je popsána základní struktura údržby a zajištění údržby, jakož i minimální všeobecné praktické postupy, které se při tomto provádějí. Účelem této normy je všeobecně použitelným způsobem popsat procesy a techniky, týkající se údržby a zajištění údržby, které jsou nutné k dosažení přiměřené spolehlivosti, splňující provozní potřeby zákazníka. Tato norma svým zaměřením spadá také do oblasti udržovatelnosti.

5.2.5 Pokyny k udržovatelnosti a související normy

Tato kapitola shrnuje problematiku norem z oblasti udržovatelnosti a zajištěnosti údržby.

Udržovatelnost je znak, který určuje snadnost, se kterou může být objekt udržován a zajišťován během období svého používání. Soubor norem IEC 60706 je určen k tomu, aby poskytoval návod, jak má návrhář do produktu nejlépe začlenit vysoké standardy udržovatelnosti tak, aby se náklady na údržbu snížily na přijatelnou úroveň. Norma [39] obsahuje úvod do koncepce udržovatelnosti a návod, jak začlenit udržovatelnost do specifikací a smluv a jak se má udržovatelnost považovat za součást procesu návrhu. Tvoří součást základní hierarchie norem na spolehlivost.

V normě [40] jsou vysvětleny postupy ověřování a příslušné techniky analýzy, užívané při sběru dat.

Norma [41] obsahuje pokyny, týkající se testovatelnosti při návrhu a vývoji a napomáhá při stanovení efektivních testovacích postupů jako nedílné součásti provozu a údržby.

V normě [42] jsou popsána některá kvantitativní hlediska inženýrství udržovatelnosti v různých etapách životního cyklu zařízení. Norma je vhodná pro řešení úloh přidělování hodnot ukazatelů udržovatelnosti, prokazování udržovatelnosti a hodnocení údajů o udržovatelnosti, jak jsou popsány v ČSN IEC 706-2 a 706-3.

Norma [43] obsahuje všeobecné směrnice pro technickou dokumentaci, která musí být pro zajištění údržby dodávána s objektem před jeho uvedením do provozu, a pro dokumentaci informací, které musí být pro splnění požadavků na údržbu zavedeny v etapě provozu. Je v ní uveden seznam základních dokumentů pro údržbu a jsou podány informace o možném obsahu každého dokumentu. V informativních přílohách je popsána dokumentace pro údržbu s ohledem na funkce údržby, které jsou součástí systému managementu kvality daného podniku.

5.2.6 Normy pro analýzu spolehlivosti a odhady hodnot ukazatelů spolehlivosti

Do této skupiny norem z oboru spolehlivosti byly zahrnuty zejména normy, v nichž jsou popsány základní metody analýz spolehlivosti systémů a normy zabývající se předpovědí a prezentací hodnot ukazatelů spolehlivosti.

V mezinárodní normě [44] je uveden návod pro sběr a prezentaci dat, nutných k pochopení charakteristik bezporuchovosti. Je zde uveden návod pro uživatele, zaměřený na způsob, jakým mají výrobcům součástek specifikovat své požadavky na bezporuchovost.

V mezinárodní normě [14] je popsána analýza způsobů a důsledků poruch (FMEA – Failure Mode and Effects Analysis) a analýza způsobů, důsledků a kritičnosti poruch (FMECA – Failure Mode, Effects and Criticality Analysis) a je v ní uveden návod, jak se tyto analýzy mohou používat, aby se dosáhlo různých cílů.

V normě [17] jsou popsány základní principy a kroky postupu analýzy FTA, předpoklady její aplikace, identifikace událostí a druhů poruch a pravidla pro identifikaci a značení událostí ve stromu poruchových stavů.

V mezinárodní normě [15] jsou popsány postupy pro modelování spolehlivosti systému a pro použití modelu za účelem výpočtu jeho ukazatelů bezporuchovosti a pohotovosti.

V mezinárodní normě [45] jsou uvedena doporučení pro praktické provádění postupů přezkoumání návrhu jako prostředku pro ověření, že byly splněny požadavky na vstupy pro návrh, a pro stimulaci zlepšování procesu.

V normě [18] je definována základní terminologie a jsou v ní stanoveny značky používané při aplikaci Markovových technik. Jsou v ní popsány základní pravidla pro vývoj, reprezentaci a aplikaci Markovových technik, jakož i předpoklady a omezení tohoto přístupu. Je v ní uveden návod pro aplikaci Markovových technik k modelování a analýze systému a k odhadu ukazatelů bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti.

Norma [46] obsahuje matematické výrazy, umožňující kvantifikovat ukazatele bezporuchovosti, pohotovosti, udržovatelnosti a zajištěnosti údržby popsané v ČSN IEC 50(191). Tato norma je základem pro většinu statistických výpočtů hodnot ukazatelů používaných v oboru spolehlivosti a odvolává se na ni mnoho norem z tohoto oboru.

Norma [47] obsahuje nezbytné základy pro předpověď bezporuchovosti elektronických zařízení pomocí výpočtu bezporuchovosti součástek. V normě jsou specifikovány referenční podmínky a matematické modely závislosti intenzity poruch součástek na namáhání, což umožňuje přepočítat hodnoty ukazatele bezporuchovosti (většinou intenzity poruch či parametru proudu poruch), zjištěné za určitých podmínek prostředí a provozního namáhání na hodnoty stejného ukazatele za jiných provozních podmínek prostředí a namáhání.

V normě [48] je popsán mocninový model, který je jedním z nejpoužívanějších modelů pro popis bezporuchovosti opravovaných objektů, a jsou v ní uvedeny pokyny pro jeho použití. Jsou v ní popsány postupy pro odhad parametrů mocninového modelu a pro test dobré shody dat s tímto modelem. V normě jsou uvedeny algoritmy, na jejichž základě lze snadno sestavit příslušné počítačové programy, a jsou v ní obsaženy příklady, na nichž je lze ověřit.

V normě [49] je uveden návod k použití techniky HAZOP, včetně definic, přípravy, pracovních porad, výsledné dokumentace a dalšího postupu. Je zde též uveden široký soubor příkladů, které ilustrují zkoumání pomocí studie HAZOP.

Norma [50] se zabývá používáním politik, postupů a pracovních technik managementu rizika projektu u úkolů, zabývajících se vytvářením kontextu, zjišťováním, analýzou, vyhodnocováním, hodnocením, ošetřováním, monitorováním a sdělováním rizik takovým způsobem, který umožňuje organizaci minimalizovat ztráty a nákladově efektivním způsobem maximalizovat vhodné příležitosti.

V mezinárodní normě [51] jsou popsány postupy, které jsou určeny k použití při posuzování bezporuchovosti objektů na základě dat, pocházejících z průzkumu trhu podobných objektů a dat z provozu a ze zkoušek od dodavatelů součástí a modulů.

Většina dílů moderních produktů je vyrobena se střední dobou života mnohem delší, než uživatel potřebuje, takže jsou produkty a jejich díly likvidovány, přestože jsou stále ještě použitelné. Moderní produkty jsou méně poruchové a současně stále rychleji a více zastarávají. K řešení tohoto problému se zavádí norma [52], která utvrdí zákazníky a výrobce, že mohou mít produkty vyrobené s použitím dílů, které již byly dříve použity, bez poklesu spolehlivosti. Tyto díly musí splňovat vysoká přejímací kritéria, aby mohly být kvalifikovány „stejně dobré jako nové“. Takový postup je přínosný jak pro výrobce, tak pro zákazníka.

5.2.7 Normy pro ověřování, zjišťování a zlepšování hodnot ukazatelů spolehlivosti

Základem této skupiny norem jsou normy, které byly původně označeny jako části 1 až 6 normy ČSN IEC 605 pro zkoušky bezporuchovosti zařízení. Část 1 této normy však byla v roce 2002 nahrazena normou ČSN EN 60300-3-5 a část 7 pro ověřovací zkoušky bezporuchovosti byla nahrazena normou ČSN IEC 61124. Tuto skupinu norem doplňují normy pro zkoušky pro podíl úspěšných pokusů (ČSN IEC 1123), pro postupy ověřovacích zkoušek pohotovosti (ČSN IEC 1070), pro testy dobré shody (ČSN IEC 61649) a pro porovnání dvou konstantních ukazatelů bezporuchovosti (ČSN IEC 61650).

Norma [53] poskytuje obecný postup pro vypracování zkušebních cyklů. Postup je popsaný krok za krokem a je určen pro libovolné specifické zařízení, které se má vyzkoušet, pokud se považuje za nezbytné věrně simulovat podmínky skutečného použití zařízení. V normě je též uveden pracovní příklad.

Norma [54] obsahuje doporučené zkušební podmínky (cykly klimatického, mechanického a provozního namáhání) pro zkoušky bezporuchovosti zařízení. Použití standardizovaných podmínek zlepšuje srovnatelnost výsledků zkoušek. Tato část normy ČSN IEC 605-3 obsahuje popis provozních podmínek pro přenosná zařízení s hmotností do 15 kg určená k vnitřnímu použití.

Oddíl normy [55] obsahuje doporučené zkušební podmínky při zkouškách bezporuchovosti zařízení pro stacionární použití na místech chráněných proti povětrnosti (v budovách) v klimatech popisovaných v ČSN IEC 721-2-1 jako „mírná“.

Oddíl normy [56] obsahuje doporučené zkušební podmínky při zkouškách bezporuchovosti zařízení pro stacionární použití v mírných klimatech.

Oddíl normy [57] obsahuje doporučeně zkušební podmínky při zkouškách bezporuchovosti přenosných a nestacionárních zařízení podle ČSN IEC 721-3-7.

Oddíl normy [58] obsahuje doporučené zkušební podmínky při zkouškách bezporuchovosti pozemních pohyblivých zařízení napájených stejnosměrným proudem, která jsou při přepravě v provozu, například ve vozidle nebo na něm, ale nejsou součástí tohoto vozidla a nejsou navržena k tomu, aby byla ve vozidle trvale instalována. Tato zařízení budou vystavena typům venkovního klimatu z „široké“ skupiny podle ČSN IEC 721-2-1.

Oddíl normy [59] obsahuje doporučené zkušební podmínky při zkouškách bezporuchovosti přenosných zařízení pro vnější použití, která jsou v provozu pouze ve stálé poloze v mírných klimatech.

V mezinárodní normě [60] jsou uvedeny statistické metody pro vyhodnocení bodových odhadů, konfidenčních intervalů, předpovědních intervalů a tolerančních intervalů pro intenzitu poruch objektů, jejichž doba do poruchy se řídí exponenciálním rozdělením.

V této části ČSN IEC 60605 [61] jsou specifikovány postupy pro ověření předpokladu konstantní intenzity poruch nebo konstantního parametru proudu poruch (například při zkouškách bezporuchovosti zařízení). Testy specifikované v této normě jsou určeny též k testování, zda nemají doby mezi poruchami jediného opravitelného objektu nějaký rostoucí nebo klesající trend.

V mezinárodní normě [62] jsou specifikovány postupy použití a přípravy plánů ověřovacích zkoušek pro podíl úspěšných pokusů (bezporuchových stavů) nebo pro podíl poruch. Postupy jsou založeny na předpokladu, že je každý pokus statisticky nezávislý. Předpokládá se, že požadavky na bezporuchovost budou specifikovány jako přípustný podíl poruch nebo přípustný podíl úspěšných pokusů.

V normě [63] jsou specifikovány postupy pro zkoušení, zda je pozorovaná hodnota daného ukazatele bezporuchovosti (intenzity poruch, parametru proudu poruch, střední doby do poruchy, střední doby provozu mezi poruchami) v souladu se zadaným požadavkem. Předpokládá se, že jsou během zkoušky časové intervaly do poruchy nebo mezi poruchami nezávislé a mají stejné exponenciální rozdělení. Jsou předepsány tři typy zkušebních plánů: plány postupných zkoušek; plány jednostupňových zkoušek ukončených časem/poruchou; plány jednostupňových zkoušek ukončených pevným kalendářním časem/poruchou..

V normě [64] jsou popsány metody zkoušení pohotovosti často udržovaných objektů, pokud se u nich používá jako ukazatel pohotovosti buď ustálená hodnota součinitele pohotovosti, nebo ustálená hodnota součinitele nepohotovosti. Je to základní norma pro zkoušení pohotovosti zařízení.

V normě [65] jsou uvedeny numerické metody, které jsou doplňkem grafických metod při provádění testů dobré shody pro doby do poruchy s Weibullovým rozdělením a jsou v ní uvedeny postupy získání konfidenčních intervalů pro parametry dvouparametrického Weibullova rozdělení, pokud jsou odhadnuty metodou maximální věrohodnosti. Kromě toho jsou v ní uvedeny doporučené postupy získání dolních konfidenčních mezí pro 10% kvantily technického života a pro pravděpodobnost bezporuchového provozu. Tato norma je použitelná, kdykoliv je náhodný výběr objektů podroben zkoušce pro zjištění dob do poruchy za účelem odhadování ukazatelů bezporuchovosti základního souboru, ze kterého byly tyto objekty vybrány.

V normě [66] jsou specifikovány postupy pro porovnání dvou pozorovaných intenzit poruch, parametrů proudu poruch či intenzit/parametrů proudů příslušných událostí. Postupy se používají k určení, zda může být domnělý rozdíl mezi dvěma soubory pozorování považován za statisticky významný.

5.2.8 Normy pro zlepšování ukazatelů spolehlivosti

Do této skupiny norem z oboru spolehlivosti byly zahrnuty normy zabývající se tříděním a programy růstu bezporuchovosti.

V normě [67] jsou popsány speciální metody pro použití a optimalizaci procesů třídění namáháním pro dávky opravitelných hardwarových objektů v případech, kde mají objekty nepřípustně nízkou bezporuchovost a když nejsou použitelné jiné metody, jako jsou programy růstu bezporuchovosti a metody managementu kvality. Procesy uvedené v normě se používají v libovolné etapě sériové výroby opravitelných objektů.

V této části normy ČSN IEC 61163 [68] se poskytuje směrnice pro metody a postupy třídění namáháním pro zlepšení bezporuchovosti elektronických součástek. Tato norma je určena k použití pro výrobce součástek (jako směrnice), pro uživatele součástek (jako směrnice pro dohodnutí s výrobci součástek o požadavcích na třídění namáháním nebo pro plánování

procesu třídění namáháním u uživatele kvůli požadavkům na bezporuchovost) a pro smluvní subdodavatele, kteří poskytují třídění namáháním jako službu.

Zlepšování bezporuchovosti pomocí programu jejího růstu má být součástí celkové činnosti zajišťování bezporuchovosti při vývoji produktu. Tento program je možné realizovat s podporou důsledného managementu projektu, pomocí inženýrství návrhu a často i za účasti a při zapojení zákazníka. Přední průmyslové organizace během několika minulých let vyvinuly a aplikovaly analytické a zkušební metody plně integrované do návrhářského úsilí o zvýšení bezporuchovosti během etapy návrhu produktu. Tato technologie je základem pro integrovanou strategii růstu bezporuchovosti uvedenou v této normě [69].

V normě [70] je popsán mocninový model růstu bezporuchovosti a návazný model pro projektování a je v ní uveden návod, jak tyto modely krok za krokem používat. Tato norma představuje metodický nástroj umožňující realizaci programů popsaných v ČSN EN 61014.

Norma [71] obsahuje návod pro provádění procesů zajištění spolehlivosti v jednotlivých etapách životního cyklu softwaru popsaných v ČSN ISO/IEC 12207, na kterou tato norma navazuje, za účelem dosažení takového softwaru, který je bezporuchový a udržovatelný a má dobrou zajištěnost údržby. Tento návod je určen pro podporu normy ČSN IEC 60300-2.

5.3 Shrnutí poznatků o problematice verifikace a validace v publikacích

V předcházejících kapitolách byl uveden průřez publikacemi, majícími vztah ke spolehlivosti, bezpečnosti a validaci výsledné informace z násobných vstupních údajů. Teorie spolehlivosti je v dnešní době již značně propracovaná. Vzhledem k jejímu přirozenému historickému vývoji je zřejmé, že systémy, náchylné na jednoduché poruchy, je možno analyzovat bez toho, abychom se dopustili nějakého omylu. Jiná situace je však v případě výběrových systémů, popisovaných také jako „*k* z *n*“. Podle dostupné literatury je možné tyto systémy také analyzovat, ovšem nebyla nalezena publikace, která by vědecky doložila výhodnost použití konkrétního výběrového členu. V normách řady ČSN EN 61508 je např. popsána problematika zjevných/skrytých poruch, diagnostikovatelnosti, diagnostického pokrytí atp., ale chybí zde návod, jakým způsobem vybírat výslednou hodnotu do řídicího algoritmu z násobných měření jedné fyzikální veličiny. Změnou způsobu výběru finální hodnoty se samozřejmě změní také parametry spolehlivosti výběrového členu. Předkládaná disertační práce řeší tento problém a může sloužit jako podklad pro doplnění norem řady ČSN EN 61508.

6 Zvýšení parametrů spolehlivosti pomocí validace

Možností, jak zvýšit spolehlivost měřících kanálů, je několik. Pokud budeme považovat kabeláž a SW za absolutně spolehlivý (resp. nebudeme se zabývat možností zvýšení spolehlivosti systému pomocí HW a SW modifikace) , jedná se v zásadě o dva směry, kterými je možné se ubírat:

1. Zvýšení počtu čidel a následný výběr validních údajů měření [10]
2. Zvýšení spolehlivosti a věrohodnosti senzorů [11]

Je zřejmé, že obě možnosti s sebou přináší řadu překážek. Pokud jsou jako hlavní faktor uvažovány finance, jedná se zejména o zvýšené nároky na pořizovací a provozní náklady. Tyto náklady je možné optimalizovat pomocí vhodně nastaveného modelu. V případě první možnosti řešení bude relativně nízká pořizovací cena jednoho senzoru vykoupena nutně velkým množstvím těchto zařízení, zatímco u vysoce spolehlivých, tzv. inteligentních čidel bude pořízení jedné komponenty drahé, ovšem z hlediska spolehlivosti je možné dosáhnout podobných hodnot s nižším počtem čidel.

Pro lepší představu o možnostech jednotlivých řešení bude uveden stručný úvod do problematiky zálohovaných měření. Při použití zálohovaných snímačů je třeba s jednotlivými kanály měření v první úrovni zpracování signálu provést jejich verifikaci a přiřadit jednotlivým informacím index validity. Takto ohodnocený signál následně vstoupí do algoritmu určení jednoho údaje o měřené fyzikální veličině, který bude dále používán. Detailní popis je uveden níže. Zvýšení spolehlivosti měřicích systémů pomocí spolehlivějších snímačů nespadá do problematiky této disertační práce.

6.1 Násobné měření fyzikálních veličin

Násobné měření fyzikální veličiny je možné interpretovat jako nepřímé potvrzení správnosti měření jednoduchého. V praxi jsou běžně používána tzv. smart čidla, která jsou schopna rozpoznat chybu měření na základě hodnot závislých fyzikálních veličin. Tak například primární funkcí průtokoměru je měření průtoku, ovšem bude-li se jednat o zmiňované smart čidlo, bude tato hodnota ověřována např. měřením tlaku. Smart čidlo potom samo vyhodnotí, zda je fyzikálně realizovatelné, aby klesla/stoupla hodnota průtoku při změřené změně tlaku. Další možností využití „chytrého“ čidla je detekování malých, ještě

nedetekovatelných změn fyzikálních veličin zprostředkovaně pomocí sledování hodnot závislé veličiny. Pro takováto měření se často využívá vzájemné závislosti tlaku, teploty a objemu.[12]

V současném stavu poznání předpokládá logické spojování násobných měřících kanálů do jednoho výstupního údaje pouze dva stavy individuálního měření - stav, kdy je zařízení schopné provozu (tzv. použitelný stav) a stav nepoužitelný. Teorie spolehlivosti dělí dále nepoužitelný stav na dobu preventivní údržby a poruchový stav. Preventivní údržba je snadno plánovatelná, proto bude nadále zkoumán pouze poruchový stav čidla. Je běžné považovat poruchový stav objektu jako něco nežádoucího a potenciálně nebezpečného. Přesto ani tento stav není možné paušalizovat. Po podrobnějším prozkoumání možných příčin a důsledků poruchových stavů lze určit, že i tento stav je možné dále dělit. Tak např. poruchy je možné dělit na zjevné a skryté, bezpečné a nebezpečné.[1] Jednotlivé typy poruch se velmi výrazně liší ve spolehlivostních parametrech - skrytá porucha má mnohonásobně delší střední dobu do obnovy, než porucha zjevná, porucha bezpečná způsobí nižší škody, než porucha nebezpečná apod.

6.1.1 Porovnání možností logického spojování signálu

V této kapitole je uveden postup analýzy logického spojování signálu pro tři na sobě nezávislé měřící kanály a tři odlišné logické operace, které se s nimi mají provádět. Zmíněné logické operace jsou popsány v kapitole 2.4 a znázorněny na obr. 2. Pro umožnění zpracování kompletního seznamu možných stavů systému je nezbytné nadefinovat možné stavy jednotlivých snímačů.

- Stav 1 přísluší poruše nebezpečné a pro verifikační algoritmus zjevné, s intenzitou poruch λ_1.
- Stav 2 přísluší poruše nebezpečné, pro verifikační algoritmus skryté, s intenzitou poruch λ_2.
- Stav 3 přísluší poruše bezpečné a pro verifikační algoritmus zjevné, s intenzitou poruch λ_3.
- Stav 4 přísluší poruše bezpečné a pro verifikační algoritmus skryté, s intenzitou poruch λ_4.
- Stav 5 vyhradíme v následující analýze pro bezporuchový stav snímače.

Na základě toho platí triviální součty:

$$\lambda = \lambda_n + \lambda_f \quad (32)$$

$$\lambda_n = \lambda_1 + \lambda_2 \quad (33)$$

$$\lambda_f = \lambda_3 + \lambda_4 \quad (34)$$

$$\lambda = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 \quad (35)$$

kde:

λ_n označuje intenzitu nebezpečných poruch,

λ_f označuje intenzitu falešných zapůsobení (bezpečných poruch),

λ označuje celkovou intenzitu poruch komponenty.

Nyní je provedeno označení a rozdělení možných stavů „vstupů“ do rozhodovacího procesu, tedy signálů ze snímačů a zbývá pouze označit možné výsledné stavy systému. Pro jednotlivé logické operace se signály (LOG1, LOG2 a LOG3) budou výsledné výstupy označeny shodně, a sice následovně:

- N - nebezpečný stav systému (porucha vede ke ztrátě funkce systému)
- F - bezpečný stav systému (porucha vede k falešnému zapůsobení systému)
- D - bezporuchový stav systému

Logické operace se signály jsou popsány v kapitole 2.4, zde budiž pro přehlednost pouze zopakováno, že:

- LOG1 je analogové spojování signálu (např. průměrování, medián, maximum apod.) s možností redukce počtu vstupních signálů v závislosti na jejich validitě,
- LOG2 je výběrové zapojení, v tomto případě 2 ze 3,
- LOG3 je výběrové zapojení (2/3) s možností redukce počtu vstupních signálů v závislosti na jejich validitě.

Výsledná tabulka udává vyčerpávající přehled možných stavů vyhodnocovacího obvodu se třemi vstupními signály pro všechny tři výše popsané logické obvody. Jelikož každý ze tří vstupních signálů může být v pěti možných stavech (dobrý, bezpečný zjevný, bezpečný skrytý, nebezpečný zjevný, nebezpečný skrytý), dostáváme celkem 125 možných stavů systému, vzájemně nezávislých a disjunktních, viz tab. 2. Poznámky k logickému postupu, vedoucímu k volbě stavu logického algoritmu, obsahuje příloha A.

Tab. 2: Výsledky logického spojování signálu od tří nezávislých čidel

Pořadové číslo	C1	C2	C3	LOG1	LOG2	LOG3	Poznámky
1	1	1	1	N	N	N	P1
2	1	1	2	N	N	N	P2
3	1	1	3	N	N	N	P3
4	1	1	4	F	N	F	P4
5	1	1	5	D	N	D	P5
6	1	2	1	N	N	N	P6
7	1	2	2	N	N	N	P7
8	1	2	3	N	N	N	P8
9	1	2	4	N	N	N	P9
10	1	2	5	N	N	N	P10
11	1	3	1	N	N	N	P11
12	1	3	2	N	N	N	P12
13	1	3	3	N	F	N	P13
14	1	3	4	F	F	F	P14
15	1	3	5	D	D	D	P15
16	1	4	1	F	N	F	P16
17	1	4	2	N	N	N	P17
18	1	4	3	F	F	F	P18
19	1	4	4	F	F	F	P19
20	1	4	5	F	D	D	P20
21	1	5	1	D	N	D	P21
22	1	5	2	N	N	N	P22
23	1	5	3	D	D	D	P23
24	1	5	4	F	D	D	P24
25	1	5	5	D	D	D	P25
26	2	1	1	N	N	N	P26
27	2	1	2	N	N	N	P27
28	2	1	3	N	N	N	P28
29	2	1	4	N	N	N	P29
30	2	1	5	N	N	N	P30
31	2	2	1	N	N	N	P31
32	2	2	2	N	N	N	P32
33	2	2	3	N	N	N	P33
34	2	2	4	N	N	N	P34
35	2	2	5	N	N	N	P35
36	2	3	1	N	N	N	P36
37	2	3	2	N	N	N	P37
38	2	3	3	N	F	N	P38
39	2	3	4	N	F	N	P39
40	2	3	5	N	D	N	P40
41	2	4	1	N	N	N	P41
42	2	4	2	N	N	N	P42

Pořadové číslo	C1	C2	C3	LOG1	LOG2	LOG3	Poznámky
43	2	4	3	N	F	N	P43
44	2	4	4	N	F	F	P44
45	2	4	5	N	D	D	P45
46	2	5	1	N	N	N	P46
47	2	5	2	N	N	N	P47
48	2	5	3	N	D	N	P48
49	2	5	4	N	D	D	P49
50	2	5	5	N	D	D	P50
51	3	1	1	N	N	N	P51
52	3	1	2	N	N	N	P52
53	3	1	3	N	F	N	P53
54	3	1	4	F	F	F	P54
55	3	1	5	D	D	D	P55
56	3	2	1	N	N	N	P56
57	3	2	2	N	N	N	P57
58	3	2	3	N	F	N	P58
59	3	2	4	N	F	N	P59
60	3	2	5	N	D	N	P60
61	3	3	1	N	F	N	P61
62	3	3	2	N	F	N	P62
63	3	3	3	N	F	N	P63
64	3	3	4	F	F	F	P64
65	3	3	5	D	F	D	P65
66	3	4	1	F	F	F	P66
67	3	4	2	N	F	N	P67
68	3	4	3	F	F	F	P68
69	3	4	4	F	F	F	P69
70	3	4	5	F	F	D	P70
71	3	5	1	D	D	D	P71
72	3	5	2	N	D	N	P72
73	3	5	3	D	F	D	P73
74	3	5	4	F	F	D	P74
75	3	5	5	D	D	D	P75
76	4	1	1	F	N	F	P76
77	4	1	2	N	N	N	P77
78	4	1	3	F	F	F	P78
79	4	1	4	F	F	F	P79
80	4	1	5	F	D	D	P80
81	4	2	1	N	N	N	P81
82	4	2	2	N	N	N	P82
83	4	2	3	N	F	N	P83
84	4	2	4	N	F	F	P84

Pořadové číslo	C1	C2	C3	LOG1	LOG2	LOG3	Poznámky
85	4	2	5	N	D	D	P85
86	4	3	1	F	F	F	P86
87	4	3	2	N	F	N	P87
88	4	3	3	F	F	F	P88
89	4	3	4	F	F	F	P89
90	4	3	5	F	F	D	P90
91	4	4	1	F	F	F	P91
92	4	4	2	N	F	F	P92
93	4	4	3	F	F	F	P93
94	4	4	4	F	F	F	P94
95	4	4	5	F	F	F	P95
96	4	5	1	F	D	D	P96
97	4	5	2	N	D	D	P97
98	4	5	3	F	F	D	P98
99	4	5	4	F	F	F	P99
100	4	5	5	F	D	D	P100
101	5	1	1	D	N	D	P101
102	5	1	2	N	N	N	P102
103	5	1	3	D	D	D	P103
104	5	1	4	F	D	D	P104
105	5	1	5	D	D	D	P105
106	5	2	1	N	N	N	P106
107	5	2	2	N	N	N	P107
108	5	2	3	N	D	N	P108
109	5	2	4	N	D	D	P109
110	5	2	5	N	D	D	P110
111	5	3	1	D	D	D	P111
112	5	3	2	N	D	N	P112
113	5	3	3	D	F	D	P113
114	5	3	4	F	F	D	P114
115	5	3	5	D	D	D	P115
116	5	4	1	F	D	D	P116
117	5	4	2	N	D	D	P117
118	5	4	3	F	F	D	P118
119	5	4	4	F	F	F	P119
120	5	4	5	F	D	D	P120
121	5	5	1	D	D	D	P121
122	5	5	2	N	D	D	P122
123	5	5	3	D	D	D	P123
124	5	5	4	F	D	D	P124
125	5	5	5	D	D	D	P125

Z výše uvedené tabulky však není možné získat relevantní data a na jejich základě rozhodovat o výhodnosti/nevýhodnosti nasazení jednotlivých druhů logického zapojení snímacích kanálů.

6.1.2 Rozhodovací model

Pro rozhodnutí o výhodnosti nasazení jednotlivých zapojení je nutné znát alespoň přibližné hodnoty intenzit poruch a obnov prvků v případě skryté a zjevné poruchy. Pokud budeme uvažovat poruchy pro verifikační algoritmus zjevné i skryté, je nutné variovat poměr četností jejich nastoupení. Pro rychlou orientaci není nutné zadávat přesné hodnoty intenzit poruch a středních dob do obnovy funkce systému, postačí znát jejich poměrné zastoupení. Příklad variace parametrů je uveden v následujících tabulkách, kdy v Tab. 4 jsou uvedeny vstupní parametry a shrnuty výsledky hodnocení výhodnosti užití jednotlivých logických vyhodnocovacích členů v závislosti na poměru intenzit skrytých a zjevných poruch. Předpokládáme shodnou dobu opravy skryté a zjevné poruchy, ovšem je třeba si uvědomit, že doba do obnovy funkce závisí na zjevnosti poruchy. Pro uvedený příklad bude zjevná porucha odstraněna za 4 hodiny, zatímco porucha skrytá bude mít střední dobu do obnovy 4000 hodin. Tento předpoklad je založen na faktu, že jednou ročně je prováděn test každého systému, a proto je možné uvažovat střední dobu do obnovy pro skrytou poruchu jako polovinu testovacího intervalu, tedy cca 4000 hodin.

Pro porovnání parametrů spolehlivosti jednotlivých možností zapojení je nutné tyto parametry vypočítat. K tomuto účelu posloužila výpočetní tabulka v prostředí MS Excel. Tato tabulka využívala Schneeweissovu formuli (29) a s její pomocí byla vypočítána nepohotovost každého způsobu zapojení pro případ nebezpečné poruchy a dále střední doba mezi akcemi pro případ falešných zapůsobení systému. Ukázka popsaného výpočtu je uvedena v následující tabulce.

Tab. 3: Výsledky výpočtu parametrů spolehlivosti

Poř. číslo	U [1]	U.μ [h^{-1}]	LOG1			LOG2			LOG3		
			Stav	U	U.μ [h^{-1}]	Stav	U	U.μ [h^{-1}]	Stav	U	U.μ [h^{-1}]
1	8E-18	6E-18	N	8E-18		N	8E-18		N	8E-18	
2	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
3	8E-18	6E-18	N	8E-18		N	8E-18		N	8E-18	
4	8E-34	4E-34	F		4E-34	N	8E-34		F		4E-34
5	4E-12	2E-12	D			N	4E-12		D		
6	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
7	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
8	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
9	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
10	4E-28	1E-28	N	4E-28		N	4E-28		N	4E-28	
11	8E-18	6E-18	N	8E-18		N	8E-18		N	8E-18	
12	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
13	8E-18	6E-18	N	8E-18		F		6E-18	N	8E-18	
14	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
15	4E-12	2E-12	D			D			D		
16	8E-34	4E-34	F		4E-34	N	8E-34		F		4E-34
17	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
18	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
19	8E-50	2E-50	F		2E-50	F		2E-50	F		2E-50
20	4E-28	1E-28	F		1E-28	D			D		
21	4E-12	2E-12	D			N	4E-12		D		
22	4E-28	1E-28	N	4E-28		N	4E-28		N	4E-28	
23	4E-12	2E-12	D			D			D		
24	4E-28	1E-28	F		1E-28	D			D		
25	2E-06	5E-07	D			D			D		
26	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
27	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
28	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
29	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
30	4E-28	1E-28	N	4E-28		N	4E-28		N	4E-28	
31	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
32	8E-66	6E-69	N	8E-66		N	8E-66		N	8E-66	
33	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
34	8E-66	6E-69	N	8E-66		N	8E-66		N	8E-66	
35	4E-44	2E-47	N	4E-44		N	4E-44		N	4E-44	
36	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
37	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
38	8E-34	4E-34	N	8E-34		F		4E-34	N	8E-34	
39	8E-50	2E-50	N	8E-50		F		2E-50	N	8E-50	
40	4E-28	1E-28	N	4E-28		D			N	4E-28	
41	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
42	8E-66	6E-69	N	8E-66		N	8E-66		N	8E-66	
43	8E-50	2E-50	N	8E-50		F		2E-50	N	8E-50	
44	8E-66	6E-69	N	8E-66		F		6E-69	F		6E-69
45	4E-44	2E-47	N	4E-44		D			D		
46	4E-28	1E-28	N	4E-28		N	4E-28		N	4E-28	
47	4E-44	2E-47	N	4E-44		N	4E-44		N	4E-44	

Poř. číslo	U [1]	U.μ [h^{-1}]	LOG1			LOG2			LOG3		
			Stav	U	U.μ [h^{-1}]	Stav	U	U.μ [h^{-1}]	Stav	U	U.μ [h^{-1}]
48	4E-28	1E-28	N	4E-28		D			N	4E-28	
49	4E-44	2E-47	N	4E-44		D			D		
50	2E-22	5E-26	N	2E-22		D			D		
51	8E-18	6E-18	N	8E-18		N	8E-18		N	8E-18	
52	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
53	8E-18	6E-18	N	8E-18		F		6E-18	N	8E-18	
54	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
55	4E-12	2E-12	D			D			D		
56	8E-34	4E-34	N	8E-34		N	8E-34		N	8E-34	
57	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
58	8E-34	4E-34	N	8E-34		F		4E-34	N	8E-34	
59	8E-50	2E-50	N	8E-50		F		2E-50	N	8E-50	
60	4E-28	1E-28	N	4E-28		D			N	4E-28	
61	8E-18	6E-18	N	8E-18		F		6E-18	N	8E-18	
62	8E-34	4E-34	N	8E-34		F		4E-34	N	8E-34	
63	8E-18	6E-18	N	8E-18		F		6E-18	N	8E-18	
64	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
65	4E-12	2E-12	D			F		2E-12	D		
66	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
67	8E-50	2E-50	N	8E-50		F		2E-50	N	8E-50	
68	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
69	8E-50	2E-50	F		2E-50	F		2E-50	F		2E-50
70	4E-28	1E-28	F		1E-28	F		1E-28	D		
71	4E-12	2E-12	D			D			D		
72	4E-28	1E-28	N	4E-28		D			N	4E-28	
73	4E-12	2E-12	D			F		2E-12	D		
74	4E-28	1E-28	F		1E-28	F		1E-28	D		
75	2E-06	5E-07	D			D			D		
76	8E-34	4E-34	F		4E-34	N	8E-34		F		4E-34
77	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
78	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
79	8E-50	2E-50	F		2E-50	F		2E-50	F		2E-50
80	4E-28	1E-28	F		1E-28	D			D		
81	8E-50	2E-50	N	8E-50		N	8E-50		N	8E-50	
82	8E-66	6E-69	N	8E-66		N	8E-66		N	8E-66	
83	8E-50	2E-50	N	8E-50		F		2E-50	N	8E-50	
84	8E-66	6E-69	N	8E-66		F		6E-69	F		6E-69
85	4E-44	2E-47	N	4E-44		D			D		
86	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
87	8E-50	2E-50	N	8E-50		F		2E-50	N	8E-50	
88	8E-34	4E-34	F		4E-34	F		4E-34	F		4E-34
89	8E-50	2E-50	F		2E-50	F		2E-50	F		2E-50
90	4E-28	1E-28	F		1E-28	F		1E-28	D		
91	8E-50	2E-50	F		2E-50	F		2E-50	F		2E-50
92	8E-66	6E-69	N	8E-66		F		6E-69	F		6E-69
93	8E-50	2E-50	F		2E-50	F		2E-50	F		2E-50
94	8E-66	6E-69	F		6E-69	F		6E-69	F		6E-69
95	4E-44	2E-47	F		2E-47	F		2E-47	F		2E-47

Poř. číslo	U [1]	U.μ [h^{-1}]	LOG1			LOG2			LOG3		
			Stav	U	U.μ [h^{-1}]	Stav	U	U.μ [h^{-1}]	Stav	U	U.μ [h^{-1}]
96	4E-28	1E-28	F		1E-28	D			D		
97	4E-44	2E-47	N	4E-44		D			D		
98	4E-28	1E-28	F		1E-28	F		1E-28	D		
99	4E-44	2E-47	F		2E-47	F		2E-47	F		2E-47
100	2E-22	5E-26	F		5E-26	D			D		
101	4E-12	2E-12	D			N	4E-12		D		
102	4E-28	1E-28	N	4E-28		N	4E-28		N	4E-28	
103	4E-12	2E-12	D			D			D		
104	4E-28	1E-28	F		1E-28	D			D		
105	2E-06	5E-07	D			D			D		
106	4E-28	1E-28	N	4E-28		N	4E-28		N	4E-28	
107	4E-44	2E-47	N	4E-44		N	4E-44		N	4E-44	
108	4E-28	1E-28	N	4E-28		D			N	4E-28	
109	4E-44	2E-47	N	4E-44		D			D		
110	2E-22	5E-26	N	2E-22		D			D		
111	4E-12	2E-12	D			D			D		
112	4E-28	1E-28	N	4E-28		D			N	4E-28	
113	4E-12	2E-12	D			F		2E-12	D		
114	4E-28	1E-28	F		1E-28	F		1E-28	D		
115	2E-06	5E-07	D			D			D		
116	4E-28	1E-28	F		1E-28	D			D		
117	4E-44	2E-47	N	4E-44		D			D		
118	4E-28	1E-28	F		1E-28	F		1E-28	D		
119	4E-44	2E-47	F		2E-47	F		2E-47	F		2E-47
120	2E-22	5E-26	F		5E-26	D			D		
121	2E-06	5E-07	D			D			D		
122	2E-22	5E-26	N	2E-22		D			D		
123	2E-06	5E-07	D			D			D		
124	2E-22	5E-26	F		5E-26	D			D		
125			D			D			D		

Stavy čidel jsou popsány v tab. 2 a korespondují s pořadovými čísly řádků v tab. 3. Podle (29) je možné vypočítat parametry spolehlivosti systému ze znalosti hodnot parametrů spolehlivosti jednotlivých prvků tohoto systému. Celková nepohotovost každé možnosti zapojení tří čidel do jednoho algoritmu se potom spočítá jako prostý součet dílčích nepohotovostí všech (vzájemně disjunktních) možných stavů, kdy logickým výstupem algoritmu je nebezpečná porucha. Střední doba mezi falešnými akcemi je potom převrácenou hodnotou součtu všech členů Schneeweissovy formule, kde logickým výstupem algoritmu je falešné zapůsobení (bezpečná porucha). Po výpočtu parametrů spolehlivosti jednotlivých uvažovaných algoritmů dostáváme tabulku výsledků, kde nepohotovosti a střední doby mezi akcemi závisí na poměru intenzit poruch skrytých a zjevných, viz tab. 4.

Tab. 4: Parametry modelového případu hodnocení logických vyhodnocovacích členů

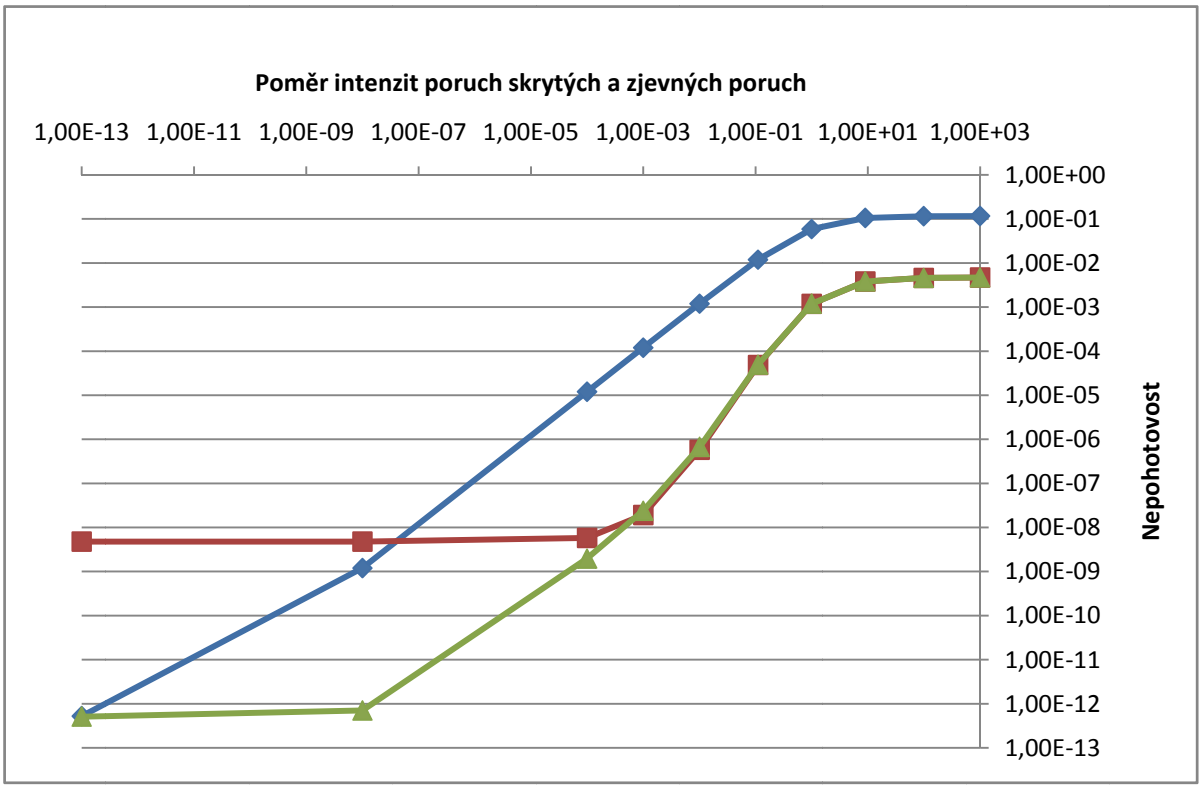
P. č.	λ_{celk} [h^{-1}]	U_{LOG1} [1]	T_{LOG1} [h]	U_{LOG2} [1]	T_{LOG2} [h]	U_{LOG3} [1]	T_{LOG3} [h]	$\lambda_{skrytá}/\lambda_{zjevná}$ [1]
1	2,00E-05	1,17E-01	3,11E+04	4,69E-03	4,00E+05	4,69E-03	4,00E+05	1,00E+03
2	2,00E-05	1,16E-01	3,13E+04	4,61E-03	4,04E+05	4,61E-03	4,07E+05	9,90E+01
3	2,00E-05	1,05E-01	3,38E+04	3,81E-03	4,46E+05	3,82E-03	1,60E+06	9,00E+00
4	2,00E-05	5,90E-02	5,60E+04	1,20E-03	8,20E+05	1,20E-03	3,90E+07	1,00E+00
5	2,00E-05	1,20E-02	2,60E+05	4,90E-05	4,10E+06	5,00E-05	3,80E+09	1,10E-01
6	2,00E-05	1,20E-03	2,50E+06	5,80E-07	3,80E+07	6,70E-07	3,40E+11	1,00E-02
7	2,00E-05	1,20E-04	2,50E+07	1,90E-08	2,10E+08	2,40E-08	1,60E+13	1,00E-03
8	2,00E-05	1,20E-05	2,50E+08	5,80E-09	3,80E+08	2,00E-09	2,40E+14	1,00E-04
9	2,00E-05	1,20E-06	2,50E+09	4,90E-09	4,10E+08	1,90E-10	2,40E+14	1,00E-13

V tab. 4 je střední doba mezi falešnými akcemi jednotlivých algoritmů označena z prostorových důvodů jako T_{LOGX}.

6.1.3 Výsledky rozhodovacího modelu

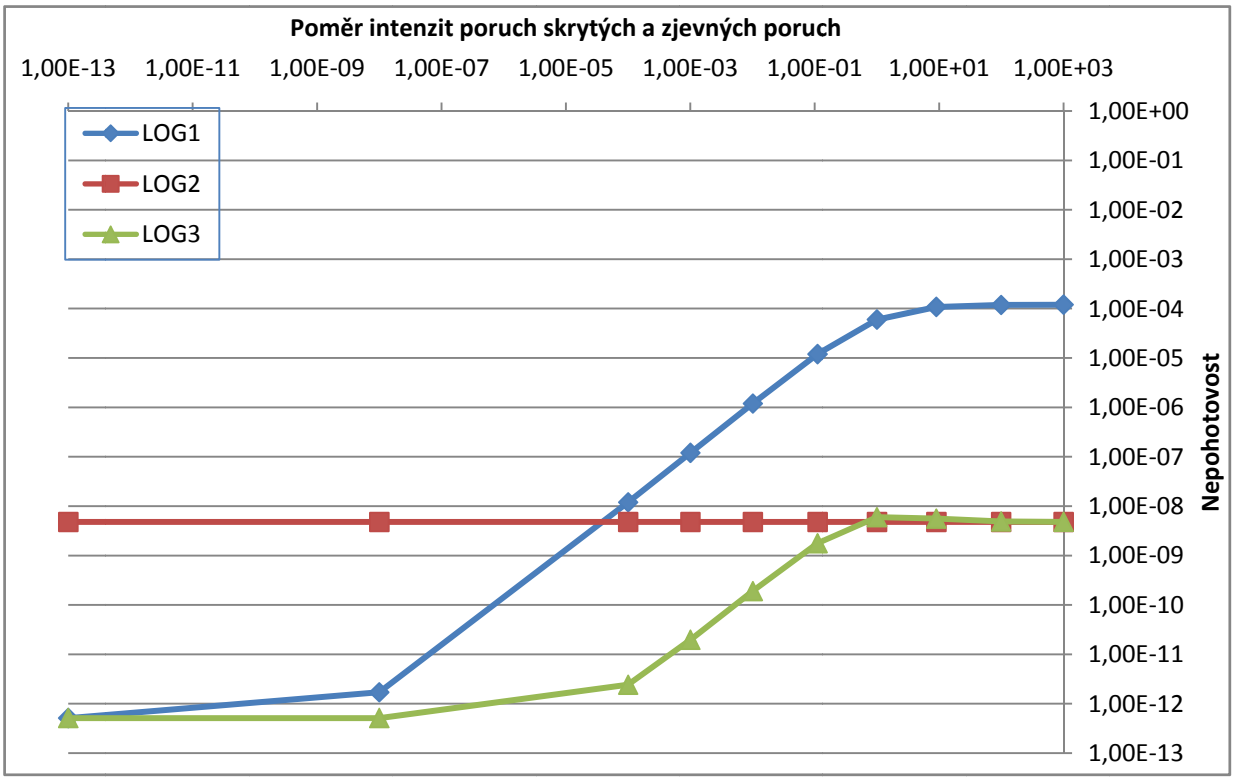
Tab. 4 přehledně shrnuje výsledky výpočtů nepohotovostí a středních dob mezi poruchami pro jednotlivé varianty poměrů skrytých a zjevných poruch, za předpokladu střední doby do obnovy u zjevné poruchy v délce 4h a v případě skryté poruchy 4000h. Bezpečné a nebezpečné poruchy nebyly variovány z důvodu nemožnosti ohodnocení příslušných následků poruch. Ty totiž závisí na konkrétní technologii, na které jsou řídicí, resp. bezpečnostní systémy s danou logikou nasazeny.

Lépe než v tabelární podobě jsou závislosti nepohotovosti (resp. střední doby mezi poruchami) na poměru intenzit zjevných a skrytých poruch vidět v grafické reprezentaci, viz obr. 6 a obr. 8.



Obr. 6: Graf závislosti nepohotovosti systému na poměru intenzit skrytých a zjevných poruch

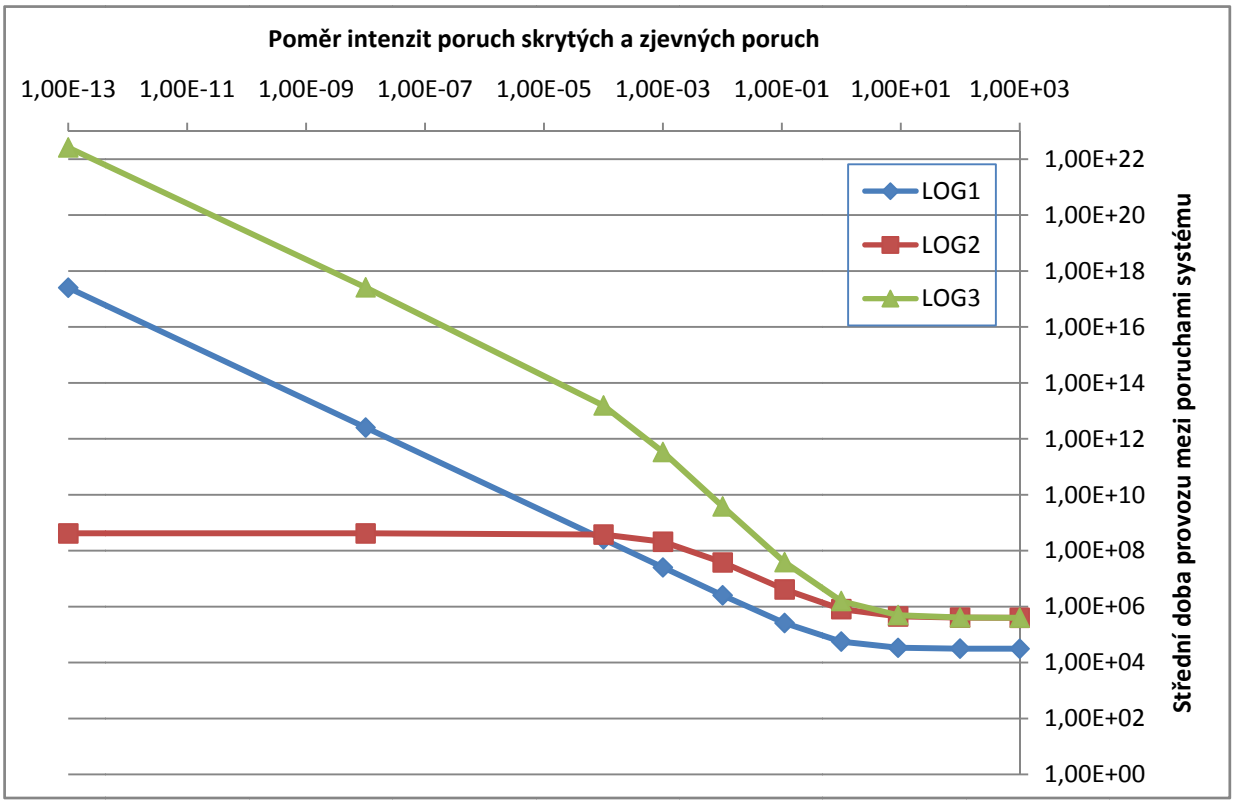
Na obr. 6 je zřetelně vidět, že nepohotovost celého měřicího systému, skládajícího se z kombinace tří snímačů, roste s rostoucím poměrem skrytých a zjevných poruch, tedy s rostoucí převahou poruch pro verifikační algoritmus skrytých. Zvláštním případem algoritmu je výběrové zapojení *2 ze 3*, u kterého je závislost nepohotovosti na poměru skrytých a zjevných poruch dána pouze rozdílnými dobami do obnovy u skryté a zjevné poruchy. Pokud bychom předpokládali shodnou střední dobu do obnovy skrytých i zjevných poruch, vývoj nepohotovosti v závislosti na poměru intenzit poruch skrytých poruch ku zjevným bude vypadat jako na obr. 7.



Obr. 7: Graf závislosti nepohotovosti systému v závislosti na poměru intenzit poruch skrytých a zjevných poruch, za předpokladu shodných středních dob do obnovy skrytých a zjevných poruch

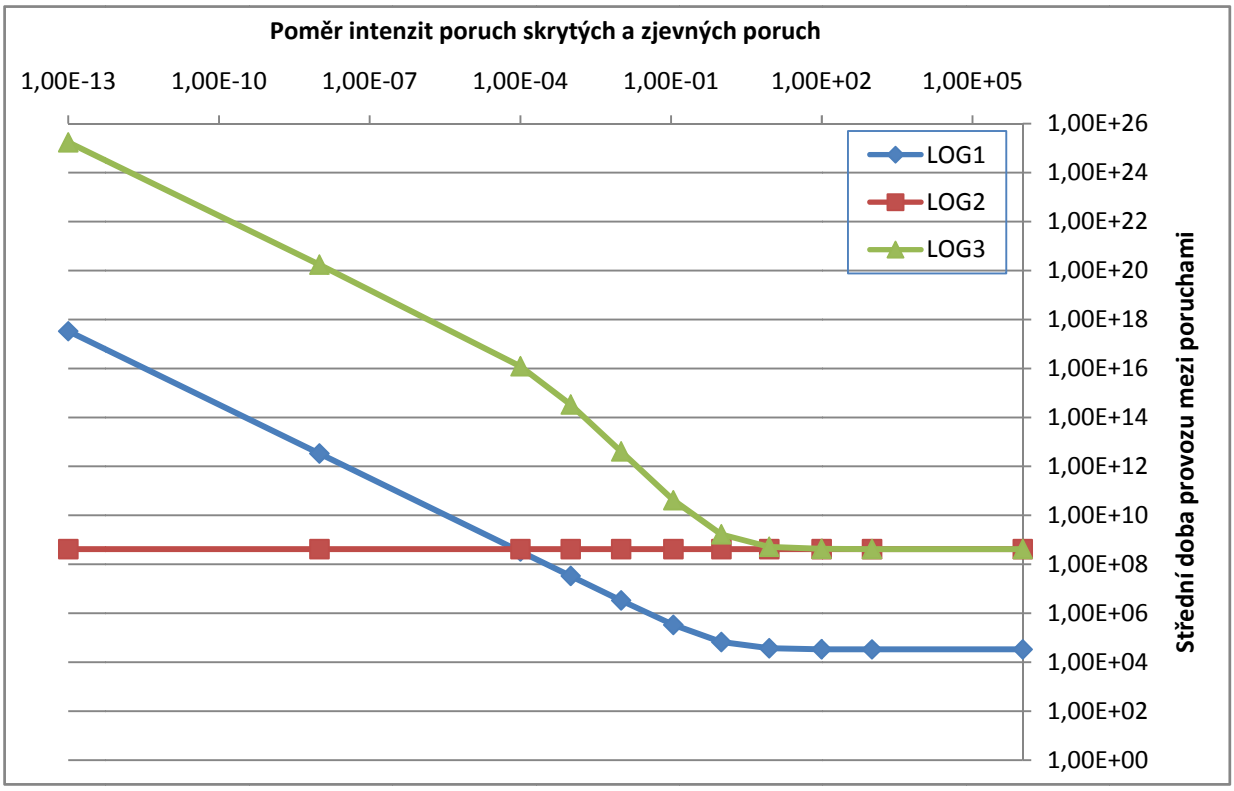
Také na obr. 7 je zřejmý trend růstu nepohotovosti se stoupajícím procentem zastoupení skrytých poruch. Výjimkou je v tomto případě výběrové zapojení LOG2, u kterého nemá poměr intenzit poruch skrytých a zjevných poruch vliv na hodnotu nepohotovosti. Je to dáno tím, že toto výběrové zapojení nebere v úvahu validitu jednotlivých individuálních vstupů. Na grafu z obr. 7 je také vidět dva extrémní stavy výběrového zapojení LOG3. Pokud budou dominantní poruchy skryté, je hodnota nepohotovosti algoritmu LOG3 blízká hodnotě nepohotovosti prostého výběrového zapojení LOG2. Naopak, pokud budou výrazně převládat poruchy validačnímu algoritmu zjevné, nepohotovost LOG3 se blíží hodnotě nepohotovosti LOG1, které také uvažuje validitu individuálních MK a její hodnota je závislá na střední době do obnovy zjevných poruch.

Nepohotovost není jediným parametrem spolehlivosti, který je možné ze získaných údajů vyhodnotit. V grafu na obr. 8 je vidět závislost *MTBF* měřicího systému na poměru intenzit poruch skrytých a zjevných poruch. *MTBF* u LOG1 a LOG3 s rostoucí dominancí zjevných poruch stále roste, zatímco u výběrového zapojení LOG2 lze vypozorovat dvě mezní hodnoty *MTBF*, závislé na *MTTR* skrytých a zjevných poruch.



Obr. 8: Závislost střední doby mezi poruchami na poměru intenzit skrytých a zjevných poruch

Stejně jako v případě grafu nepohotovosti z obr. 7, i v případě střední doby provozu mezi poruchami je možné předpokládat shodné *MTTR* zjevných a skrytých poruch. Graf střední doby provozu mezi poruchami celého měřicího systému v závislosti na poměru intenzit poruch skrytých a zjevných poruch je zobrazen na obr. 9.



Obr. 9: Graf závislosti střední doby provozu mezi poruchami měřicího systému na poměru intenzit poruch skrytých a zjevných poruch, za předpokladu shodných středních dob do údržby zjevných a skrytých poruch

Obr. 9 vypovídá mimo jiné o tom, že hodnota střední doby provozu mezi poruchami algoritmu LOG2 je závislá pouze na *MTTR* jednotlivých poruch, nikoliv však na jejich zjevnosti nebo skrytosti.

Z grafů na obr. 6-9 je patrný stejný trend u všech porovnávaných logických členů. S rostoucí převahou skrytých poruch nad zjevnými roste nepohotovost měřících kanálů a klesá jejich střední doba mezi poruchami. To ale není výsledek, kvůli kterému byl celý experiment vypracován. Důležité jsou rozdíly mezi jednotlivými logickými prvky pro různé poměry intenzit poruch skrytých a zjevných. Při vysokém procentuálním zastoupení poruch pro verifikační algoritmus zjevných se jasně ukazuje jako nejlepší možnost zapojení LOG3, tedy výběrové zapojení s možností redukce počtu vstupních čidel, které vykazuje nejvyšší hodnotu pohotovosti. S rostoucí převahou zjevných poruch se také projevuje výhodnost nasazení verifikačního algoritmu do algoritmu průměrování, naopak se ztrácí výhoda klasického výběrového zapojení, kterou je odolnost vůči jednotlivé poruše.

Na základě právě provedeného myšlenkového experimentu je možné doporučit používání varianty LOG3, tedy výběrového zapojení s možností redukce počtu vstupních signálů. Ovšem

technická a softwarová náročnost provedení (a tím pádem i vyšší cena) tohoto logického členu nahrávají variantě LOG2, prostému výběrovému zapojení. Záleží pouze na provozovateli, jak ohodnotí následky možného selhání systému, a pro který logický prvek se rozhodne.

6.2 Přínosy tématu práce

Téma bylo zvoleno jak na základě provedeného průzkumu dostupných publikací zabývajících se tematikou spolehlivosti a verifikace a validace výsledného údaje, tvořeného z více vstupních údajů, tak na základě zkušeností a současného stavu v technické praxi. Předložená disertační práce přispívá a doplňuje mezeru v problematice výběru jednoho výsledného údaje o fyzikální veličině z několika nezávislých měření. Důvodem k jejímu zadání byla absence dostatečně hlubokého řešení problému zpracování údajů o validitě signálu měřené veličiny s ohledem na výslednou spolehlivost celého měřicího systému. Přínosem disertační práce je zejména nalezení postupu pro určení výhodnosti/nevýhodnosti jednotlivých návrhů zapojení násobných měřících kanálů s ohledem na bezpečnost, ale i na ekonomiku provozování systému, systém preventivní údržby a požadovanou pohotovost provozovaného zařízení. Tento postup umožňuje vytvořit pro normu [77] doporučení, jak přistupovat k volbě způsobu výběru/výpočtu výsledné hodnoty z násobných měření fyzikální veličiny a v budoucnu by mohl doplnit zmiňovanou normu např. jako „Příloha F (normativní) Způsob výběru/výpočtu jedné výsledné hodnoty z násobných měření fyzikální veličiny“. Je totiž logicky navazujícím článkem řetězu pro výběr jedné výsledné hodnoty z násobných měření elektrické i neelektrické fyzikální veličiny. Tuto pasáž v současnosti norma neobsahuje a z toho vzniká vágnost v jejím provádění v praxi.

Analogií popsaného postupu je možnost nalezení optimálního hardwarového provedení násobného měření [16], tedy sestavení kombinací čidel pro násobné měření fyzikálních veličin a určení výhodnosti takového měření v porovnání s tzv. smart čidly[5]. Další možností užití předkládané myšlenky je kombinace požárních čidel, případně čidel plášťové ochrany objektu,

[5] V praxi by se jednalo o princip nalezení ekonomicky výhodnějšího řešení ze dvou možností. Tou první je nasazení několika smart čidel, které však jsou ze svého principu složena z několika čidel (např. 3 ks smart čidel průtoku, jejichž správnost je ověřována měřením tlaku) a následná kombinace výsledků těchto smart čidel do jedné výsledné hodnoty. Druhou možností je nasazení adekvátního počtu čidel (tedy v našem případě 3ks čidel průtoku a 3 ks čidel tlaku). Z hodnot čidel, měřících stejnou fyzikální veličinu by se vybrala/vypočetla výsledná hodnota (tedy jedna hodnota průtoku a jedna hodnota tlaku) a teprve z těchto hodnot by se určila validita měření.

kde dochází v důsledku falešného zapůsobení ochrany k finančním ztrátám např. nepotřebným výjezdem zásahové jednotky k objektu, který nebyl napaden nebo zbytečným skrápěním vnitřního prostoru objektu v případě falešného nahlášení požáru jedním vadným čidlem.

Princip změny stupně zálohovanosti je možné s úspěchem použít také při sestavování plánu preventivní údržby. V okamžiku, kdy je na nějakém prvku systému prováděna preventivní údržba, je tento prvek de facto mimo provoz. Pokud bychom se drželi používané terminologie, jednalo by se vlastně o zjevnou poruchu, i když terminologicky správné by bylo označit tento stav za provozuneschopný, nikoli poruchový.

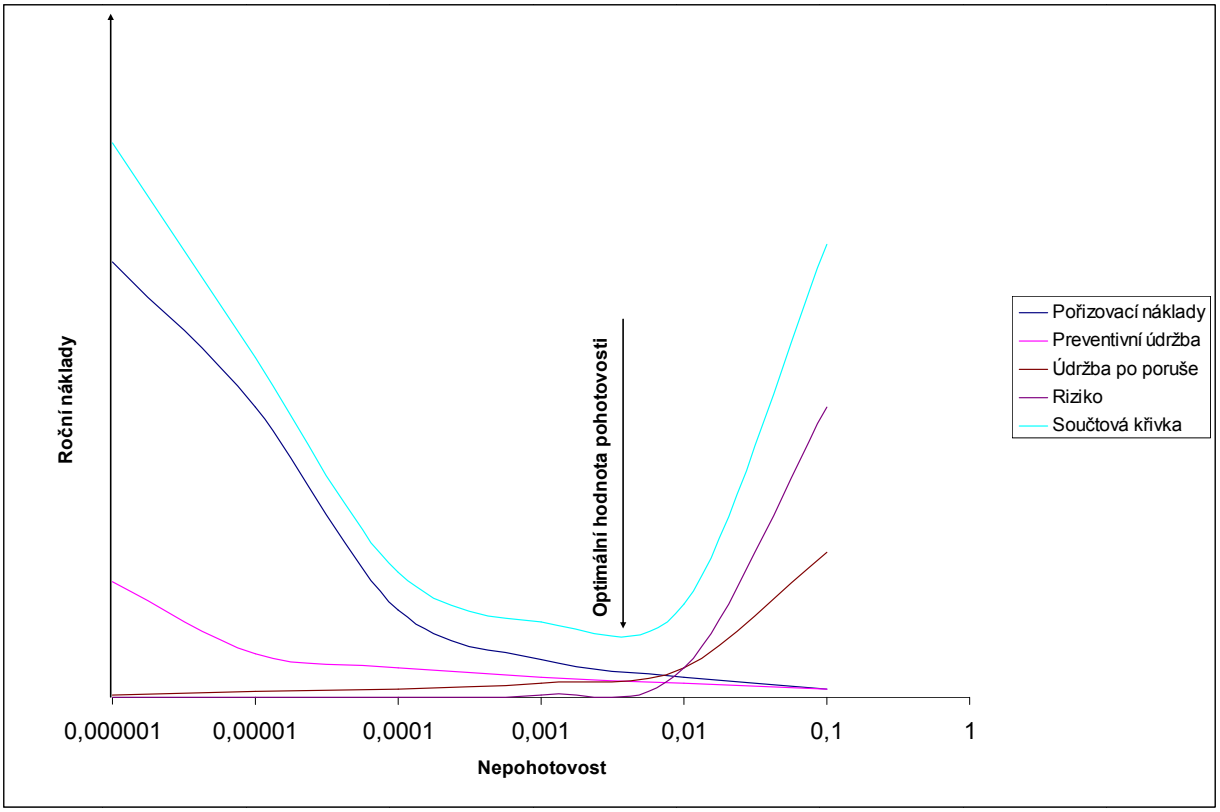
Další možností uplatnění předkládané disertační práce je plánování systému preventivních údržbářských zásahů a optimalizace nákladů životního cyklu (LCC) produktu, založené na více vstupních parametrech. Na základě výpočtu rizika, plynoucího z jednoho nefunkčního individuálního MK, je možné naplánovat preventivní údržbu souvisejících systémů a tím minimalizovat riziko toho, že budou současně mimo provoz (z důvodu preventivní údržby) řídicí nebo ochranné systémy, pracující na jednom funkčním bloku. Tímto postupem se sníží riziko výpadku celého výrobního bloku, přestože jeho řídicí, resp. havarijní systémy budou funkční, ale budou odstavené z důvodu prevence.

7 Možnosti a perspektivy v pokračování práce

V této kapitole jsou popsány možnosti dalšího rozpracování tématu. Je zde otevřeno předpokládané téma dalšího řešení ve vztahu k možnému zapojení ekonomických aspektů do problematiky zálohovaných systémů. Také jsou zde uvedeny možnosti řízení rizika pomocí snižování frekvence výskytu/vzniku nebezpečné události.

7.1 Navržený ekonomický model

Praxe často udává míru rizika provozování nějakého zařízení ve finančním ohodnocení za určité časové období, např. v Kč/rok. Tato hodnota je pro provozovatele snadno porovnatelná s náklady na provoz. Obě hodnoty jsou závislé na pohotovosti provozovaného systému, s rostoucí spolehlivostí klesají roční náklady na opravy po poruchách, klesá také roční riziko, ovšem lze předpokládat nárůst pořizovací ceny zařízení a nákladů na jeho preventivní údržbu. Vzhledem k tomu, že všechny výše zmiňované položky jsou závislé na jediném faktoru a to na pohotovosti, je možné sečíst náklady a nalézt minimum této součtové křivky. Ilustrační případ je zobrazen na následujícím grafu na obr. 10.



Obr. 10: Ilustrační graf hledání ekonomicky optimálního systému

Uvedený případ je typem multikriteriálního modelu optimalizace nákladové křivky. Vzhledem k velkému rozptylu hodnot nepohotovosti je její osa uvedena v logaritmických souřadnicích. Za účelem nalezení ekonomicky optimální výše pohotovosti je třeba nalézt globální minimum součtové křivky. Pro potřeby zkoumání bezpečnosti, která je v oblasti jaderné energetiky diskutovanější a důležitější, než pouhé ekonomické hodnocení nákladů a přínosů z provozování zařízení, je možné model upravit tak, že nebude uvažovat vliv pohotovosti na finanční aspekty provozování zařízení, ale bude ohodnocen vliv vybraných faktorů na přírůstek k ročnímu riziku uvažovaného systému.

Riziko je obecně definováno jako součin pravděpodobnosti nastoupení nežádoucí události a jejích následků.

$$RIZIKO = P \cdot C \tag{36}$$

V případě specifických odvětví, jako je např. letectví, kosmonautika, výroba výbušnin, jaderná energetika apod., lze jako následky nebezpečných událostí předpokládat ztráty na životech, které jsou blíže obtížně finančně stanovitelné. Takové následky jsou považovány za nepřijatelné a vlastní řízení rizika se transformuje na dosažení akceptovatelné míry pravděpodobnosti nastoupení nebezpečné události. Globální ekonomická optimalizace se potom změní na problém nalezení nejlevnějšího provozního kontextu za splnění podmínek bezpečnosti. Roční riziko, v daném případě pravděpodobnost nastoupení nebezpečné události (poruchy), roste s klesající pohotovostí zařízení. [8]

Pro případ jedné provozované komponenty je nákladová optimalizace triviálním problémem. Odlišná situace nastává u zařízení s vysokými nároky na bezpečnost, které bývají složitě zálohované. Pro dosažení limitů ročního rizika celého provozovaného systému, které jsou provozovateli předepsány kontrolními orgány, je třeba monitorovat a snižovat riziko provozu jednotlivých podsystémů. Snížení pravděpodobnosti selhání nějakého systému lze dosáhnout, mimo jiné, těmito dvěma způsoby:

1. Zvýšením inherentní (vložené) spolehlivosti komponent systému
2. Zvýšením (zavedením) zálohování komponent systému

První řešení předpokládá např.:

- výrobu prvků systému z kvalitnějších materiálů,
- změnu prostředí, ve kterém bude zařízení provozováno,

- návrh vylepšené konstrukce zařízení.

Tyto změny s sebou nesou zvýšení nákladů na každý jednotlivý prvek. Materiály jsou do jaderné oblasti vybírány s ohledem na jejich budoucí použití. Prostředí, ve kterém jsou systémy umístěny, jsou projektem voleny jako klimatizované, s přísunem vzduchu filtrovaným od částeček prachu, tedy ani zde není většinou velká možnost zlepšení. Zbývá možnost zlepšeného návrhu struktury systému. Tato možnost může být s úspěchem aplikována za předpokladu využití nejmodernějších poznatků a s uvážením nových pohledů na sledované veličiny. Je však třeba počítat s náklady na výzkum, vývoj a výrobu nových zařízení a nahrazením v současnosti používaných prvků, které přestaly splňovat bezpečnostní požadavky.

Druhý způsob snížení pravděpodobnosti selhání funkce systému - zvýšení zálohování systémů - znamená zavedení násobností, případně zvýšení násobností zapojení. Je možné ho provést pouze tam, kde jsou k tomu dostatečné prostory a komplexní projekt takovýto zásah umožní. V případě použití zálohování je na první pohled zřejmá finanční náročnost takovéto změny. Kromě tohoto omezujícího faktoru je třeba si uvědomit, že zálohováním nelze do nekonečna zvyšovat spolehlivost zálohované funkce, neboť ta se brzy přiblíží limitující hodnotě, dané pravděpodobností nástupu poruchy se společnou příčinou. Tato možnost snížení četnosti nastoupení nebezpečné události je předmětem řešení předložené disertační práce. Pro úplnost bude v následující kapitole uvedena i možnost snížení rizika pomocí vysoce spolehlivých čidel, která však není předmětem řešení této práce.

7.2 Autovalidační senzory

Při použití inteligentních snímačů, např. snímače typu SEVA [11] (Self-Validating Sensors), je signál validity přiřazován jednotlivým měřícím kanálům automaticky. Touto technologií se zabývá oxfordská univerzita ve spolupráci s firmou Foxboro. Pod pojmem senzor je třeba si představit celý měřící aparát, včetně A/D převodníku. Senzory SEVA generují s každým měřením tři parametry:

1. VMV (Validated Measurement Value) - ověřená hodnota měření. Jde o konvenčně naměřenou hodnotu, která se však v případě poruchy senzoru nahradí opravenou hodnotou nejlepšího odhadu skutečné hodnoty.

2. VU (Validated Uncertainty) - ověřená nejistota neboli rozsah chyby VMV. Nejistota je spočítána na základě platných metrologických norem po uvážení všech zdrojů chyb, které ovlivňují měření (např. vlastní snímač, převodník, šum v procesu apod.).

3. MV Status - informace o kvalitě měřené veličiny, která může nabývat hodnot:

   - *Secure (diverse)* - v podstatě ideální stav senzoru, hodnota je bezpečně správná.
   - *Secure (common)* - hodnota měření je věrohodná, ovšem je náchylná k běžným chybám.
   - *Clear* - naměřená hodnota je platná a odpovídá jmenovitým hodnotám.
   - *Blurred* - naměřená hodnota neodpovídá skutečnosti, ale je znám problém a je aplikována kompenzace. Údaj je možné použít, ovšem je zvýšena nejistota měření.
   - *Dazzled* - hodnota je vypočtena z historických dat měření jako nejlepší odhad, zatímco je vyhodnocován chybový stav. Příslušným způsobem je zvýšena nejistota.
   - *Blind* - hodnota je založena pouze na historických datech, tedy naměřená hodnota nereprezentuje skutečný stav procesní veličiny. Opět je příslušným způsobem zvýšena nejistota.

V případě použití těchto senzorů je možné přejít při vyhodnocování údaje o měřené veličině přímo na druhou úroveň zpracování informace, tedy do algoritmu určení jednoho souhrnného validního a dále používaného signálu. Tímto odpadá nutnost předzpracování měřeného signálu, ovšem za cenu vyšších nákladů na senzory.

8 Závěr

Práce sestává z osmi kapitol, které jsou podle potřeby dále členěny na podkapitoly. V první kapitole je uveden problém, kterým se bude práce zabývat. Druhá kapitola seznamuje čtenáře s oblastí verifikace a validace. Ve třetí kapitole jsou stručně shrnuty cíle práce a na tuto kapitolu navazuje čtvrtá kapitola přehledem spolehlivostního a matematického aparátu, který bude použit při vlastním řešení problému. V páté kapitole je provedena rešerše publikací, zabývajících se problematikou verifikace a validace a také rešerše norem se vztahem ke spolehlivosti. Šestá kapitola obsahuje vlastní přínos disertační práce, je v ní vyřešen problém validace měření pomocí výběru/výpočtu jedné výsledné hodnoty z násobných měření téže fyzikální veličiny. V sedmé kapitole jsou nastíněny směry, kterými je možné pokračovat v práci s využitím výsledků této disertační práce a konečně osmá kapitola stručně a přehledně shrnuje podstatu celé disertační práce.

Předcházející kapitoly uváděly modely nastoupení nežádoucí události s vlivem na funkci zařízení, na bezpečnost práce, resp. životní prostředí. Všechny uvedené oblasti lze převést na jediného společného jmenovatele pro snazší porovnání následků. Jako nejvhodnější společný jmenovatel se ukazují být finance, na které je možné přepočítat náklady a ztráty z provozu zařízení a s jistými obtížemi i zranění, úmrtí a poškození životního prostředí. Pro vlastníka průmyslového systému je zásadní otázka, jak provozovat jednotlivá zařízení s co nejnižšími náklady. Výsledek této disertační práce může posloužit jako podklad pro rozhodování o ekonomické výhodnosti nasazení bezpečnostního/řídicího systému do praxe. Návodem, jak tyto hodnoty využít, je potom kapitola 7.1, ve které jsou obecně uvedeny vztahy mezi náklady a přínosy z provozování průmyslových provozů.

Poznatky z teorie spolehlivosti, do kterých patří oblasti uvedené v kapitolách 4.3, 4.4, 4.5 a 4.6, pomáhají provádět komplexní analýzy spolehlivosti. Jejich seznam není úplný, ovšem postihuje nejčastěji používané vztahy a metody z oblasti spolehlivosti, se kterými lze kvalitně zpracovat analýzy na dostatečné úrovni detailu. V předložené disertační práci jsou využity pouze některé z uvedených vztahů. Pro pochopení souvislostí mezi různými typy zapojení více prvků do jednoho systému čtenářem, nemajícím hlubší zkušenosti s problematikou zálohovaných systémů, je vhodné uvést matematické nástroje a logické pochody pro výpočet ukazatelů spolehlivosti základních druhů propojení více objektů do komplexního systému, přestože nebyly v disertační práci použity.

Předkládaná práce ukazuje rozdíly v parametrech spolehlivosti pro tři běžně používané metody získávání řídicí veličiny z násobných měření fyzikálních veličin. Byly vypočteny hodnoty (ne)pohotovosti pro algoritmus „průměrování“, „2 ze 3“ a „2 ze 3 s možností redukce počtu vstupů“. Tyto hodnoty mohou provozovateli průmyslového zařízení sloužit jako jeden ze vstupů do analýz rizika. Dalšími vstupy musí být ohodnocení následků selhání funkce, kterou měl analyzovaný algoritmus vykonávat. Tato data nejsou pro účely disertační práce dostupná, a proto nebyla provedena kompletní analýza rizika provozování průmyslového podniku. Zpracování takovéto analýzy je jedním z možných pokračování práce ve zkoumaném oboru.

Běžná spolehlivostní praxe, zejména modelování spolehlivosti systémů, neuvažuje současné nastoupení dvou a více poruch. Tento předpoklad je často odůvodnitelný, neboť většina systémů, které naši společnost obklopují, není složitě zálohována. Tato práce se zabývá provozy, jejichž porucha by mohla vést ke katastrofickým následkům. Právě kvůli těmto vysokým následkům nežádoucí události je nutné zkoumat pravděpodobnosti nastoupení poruch velmi detailně. Pro násobně zálohované zařízení je možné předpokládat, že souběžná porucha dvou individuálních subsystémů je méně pravděpodobná, než jedna porucha těchto prvků se společnou příčinou. Taková porucha může nastat v důsledku nedostatku v návrhu nebo konstrukci systému, ale také jako následek zapůsobení lidského faktoru. Zapracování těchto aspektů je dalším možným pokračováním disertační práce. Z důvodu nedostatku vstupních údajů není problematika spolehlivosti lidského činitele a poruch se společnou příčinou uvažována v aplikačním příkladu. Existuje oprávněný předpoklad, že pravděpodobnost selhání lidského činitele i pravděpodobnost nastoupení poruchy se společnou příčinou bude podobná pro všechny možné druhy zapojení více měřicích kanálů, a proto je účelné zabývat se možností kombinace poruch pro individuální měřicí kanály i bez znalosti konkrétních hodnot parametrů spolehlivosti pro *CCF* a *HF*.

Použitá literatura

[1] ČSN IEC 50(191) Mezinárodní elektrotechnický slovník - kapitola 191: Spolehlivost a jakost služeb

[2] ČEZ.a.s.. *Historie a současnost EDU*. [online]. [cit. 2007-10-26]. URL: <http://www.cez.cz/cs/energie-a-zivotni-prostredi/jaderna-energetika/jaderne-elektrarny-cez/edu/historie-a-soucasnost.html>

[3] ČEZ, a.s.: *Informace o provozních událostech v Jaderné elektrárně Temelín v letech 2002-2007*[online][cit. 20007-11-22], URL: <http://www.cez.cz/cs/o-spolecnosti/media/tiskove-zpravy/117.html>

[4] Babič P.: *Poruchy se společnou příčinou při vysokém stupni zálohování* in Modely poruch se společnou příčinou, Praha, 2006

[5] Hokstad P., Maria A., Tomis P.: *Estimation of common cause factors from systems with different numbers of channels*, Trondheim, Norway, 2006, ISSN: 0018-9529

[6] ČEZ, a.s.: *Roční zpráva 2006 jaderné elektrárny ČEZ, a.s.* [online] [cit. 2007-11-22] URL: <http://www.cez.cz/edee/content/file/energie_a_zivotni_prostredi/CEZ-Rocni-zprava-provozu-JE-06.pdf >

[7] Wei L., Ming J. Z.: *Optimal design of multi-state weighted k-out-of-n systems based on component design* in Risk, Reliability and Societal Safety, Stavanger, Norway, 2007

[8] Fuchs P., Vališ, D.: *Metody analýzy a řízení rizika.* Liberec: Technická universita v Liberci, 2004.

[9] Schneeweiss W.:*Teória spoľahlivosti*, Bratislava, 1981

[10] Marko M.: *Validace individuálních kanálů měření*, Praha, 1998

[11] Vaculíková E.: *SEVA - senzory s automatickým ověřováním*, časopis Automatizace, ročník 45, číslo 4-5, květen - červen 2002

[12] García-Díaz J. C.: *Fault detection and diagnosis in monitoring a hot dip galvanizing line using multivariate statistical process control.* in Safety, Reliability and Risk Analysis, Valencia, 2008

[13] Malý, S.: *Problematika spolehlivosti lidského činitele v bezpečnostní dokumentaci podle zákona č. 353/1999 Sb. o prevenci závažných havárií*. Praha: Výzkumný ústav bezpečnosti práce, 2002 [online] [cit. 2002-04-18]. URL: <http://www.bozpinfo.cz/citarna/clanky/lidsky_cinitel/lc020308.html>

[14] ČSN EN 60812:2006 Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)

[15] ČSN EN 61078:2006 Techniky analýzy spolehlivosti – Blokový diagram bezporuchovosti a booleovské metody

[16] Zhigang T., Levitin G., Zuo M. J.: *A joint reliability-redundancy optimization approach for multi-state series-parallel systems,* in Safety, Reliability and Risk Analysis, Valencia, 2008

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

[18] ČSN EN 61165:2007 Aplikace Markovových technik

[19] ČSN IEC 300-3-1 Řízení spolehlivosti – Část 3: Návod k použití – Oddíl 1: Metody analýzy spolehlivosti: Metodický návod.

[20] Calabro S.R.: *Základy spolehlivosti a jejich využití v praxi*, Praha, 1965

[21] Fang Y., Meliopoulos A. P. S., Cokkinides G. J., Dam Q. B.: *Effects of Protection System Hidden Failures on Bulk Power System Reliability* in Power Symposium, 2006. NAPS 2006, 38th North American, 2006

[22] MIL-HDBK-217F - Reliability Prediction of Electronic Equipment (Military Handbook)

[23] ČSN ISO/IEC 2382-14:1999 Informační technologie – Slovník – Část 14: Bezporuchovost, udržovatelnost a pohotovost

[24] ČSN EN 13306:2002 (01 0660) Terminologie údržby

[25] ČSN EN ISO 9000:2006 Systémy managementu kvality – Základní principy a slovník

[26] ČSN EN 60300-1:2004 Management spolehlivosti – Část 1: Systémy managementu spolehlivosti

[27] ČSN EN 60300-2:2005 Management spolehlivosti – Část 2: Směrnice pro management spolehlivosti

[28] ČSN IEC 60300-3-1:2003 Management spolehlivosti – Část 3-1: Pokyn k použití – Techniky analýzy spolehlivosti – Metodický pokyn

[29] ČSN EN 60300-3-2:2005 Management spolehlivosti – Část 3-2: Pokyn k použití – Sběr dat o spolehlivosti z provozu

[30] ČSN EN 60300-3-3:2005 Management spolehlivosti – Část 3-3: Pokyn k použití – Analýza nákladů životního cyklu

[31] ČSN IEC 300-3-4:1997 Management spolehlivosti – Část 3: Návod k použití – Oddíl 4: Pokyny ke specifikaci požadavků na spolehlivost

[32] ČSN IEC 60300-3-5:2002 Management spolehlivosti – Část 3-5: Návod k použití – Podmínky při zkouškách bezporuchovosti a principy statistických testů

[33] ČSN IEC 60300-3-7:2000 Management spolehlivosti – Část 3-7: Návod k použití – Třídění namáháním pro zlepšení bezporuchovosti elektronického hardwaru

[34] ČSN IEC 300-3-9:1997 Management spolehlivosti – Část 3: Návod k použití – Oddíl 9: Analýza rizika technologických systémů

[35] ČSN IEC 60300-3-10:2001 Management spolehlivosti – Část 3-10: Návod k použití – Udržovatelnost

[36] ČSN IEC 60300-3-11:2000 Management spolehlivosti – Část 3-11: Návod k použití – Údržba zaměřená na bezporuchovost

[37] ČSN IEC 60300-3-12:2000 Management spolehlivosti – Část 3-12: Návod k použití – Integrované logistické zajištění

[38] ČSN EN 60300-3-14:2005 Management spolehlivosti – Část 3-14: Pokyn k použití – Údržba a zajištění údržby

[39] ČSN EN 60706-2:2007 Udržovatelnost zařízení – Část 2: Požadavky na udržovatelnost a studie udržovatelnosti v etapě návrhu a vývoje

[40] ČSN EN 60706-3:2007 Udržovatelnost zařízení – Část 3: Ověřování a sběr, analýza a prezentace dat

[41] ČSN IEC 706-5:1996 Pokyny k udržovatelnosti zařízení – Část 5: Oddíl 4 – Diagnostické zkoušení

[42] ČSN IEC 706-6:1996 Pokyny k udržovatelnosti zařízení – Část 6: Oddíl 9 – Statistické metody pro hodnocení udržovatelnosti

[43] ČSN EN 13460:2003 Údržba – Dokumenty pro údržbu

[44] ČSN IEC 60319:2000 Prezentace a specifikace dat o bezporuchovosti elektronických součástek

[45] ČSN EN 61160:2006 Přezkoumání návrhu

[46] ČSN IEC 61703:2002 Matematické výrazy pro ukazatele bezporuchovosti, pohotovosti, udržovatelnosti a zajištěnosti údržby

[47] ČSN EN 61709:1998 Elektronické součástky – Bezporuchovost – Referenční podmínky pro intenzity poruch a modely namáhání pro přepočty

[48] ČSN IEC 61710:2002 Mocninový model – Testy dobré shody a metody odhadu parametrů

[49] ČSN IEC 61882:2002 Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití

[50] ČSN IEC 62198:2002 Management rizika projektu – Směrnice pro použití

[51] ČSN EN 62308:2007 Bezporuchovost zařízení – Metody posuzování bezporuchovosti

[52] ČSN EN 62309:2005 Spolehlivost produktů obsahujících opakovaně použité díly – Požadavky na funkčnost a zkoušky

[53] ČSN IEC 605-2:1996 Zkoušky bezporuchovosti zařízení – Část 2: Návrh zkušebních cyklů

[54] ČSN IEC 605-3-1:1992 Zkoušky bezporuchovosti zařízení – Část 3-1: Doporučené zkušební podmínky – Přenosné zařízení pro vnitřní použití – Nízký stupeň simulace

[55] ČSN IEC 605-3-2:1992 Zkoušky bezporuchovosti zařízení – Část 3-2: Doporučené zkušební podmínky – Zařízení pro stacionární použití na místech chráněných proti povětrnosti – Vysoký stupeň simulace

[56] ČSN IEC 605-3-3:1992 Zkoušky bezporuchovosti zařízení – Část 3-3: Doporučené zkušební podmínky – Zařízení pro stacionární použití na místech částečně chráněných proti povětrnosti – Nízký stupeň simulace

[57] ČSN IEC 605-3-4:1994 Zkoušky bezporuchovosti zařízení – Část 3-4: Doporučené zkušební podmínky – Přenosná a nestacionární zařízení – Nízký stupeň simulace

[58] ČSN IEC 605-3-5:1997 Zkoušky bezporuchovosti zařízení – Část 3: Doporučené zkušební podmínky – Oddíl 5: Zkušební cyklus 5: Pozemní pohyblivá zařízení – Nízký stupeň simulace

[59] ČSN IEC 605-3-6:1997 Zkoušky bezporuchovosti zařízení – Část 3: Doporučené zkušební podmínky – Oddíl 6: Zkušební cyklus 6: Přenosná zařízení pro vnější použití – Nízký stupeň simulace

[60] ČSN IEC 60605-4:2002 Zkoušení bezporuchovosti zařízení – Část 4: Statistické postupy pro exponenciální rozdělení – Bodové odhady, konfidenční intervaly, předpovědní intervaly a toleranční intervaly

[61] ČSN IEC 60605-6:1998 Zkoušení bezporuchovosti zařízení – Část 6: Testy platnosti předpokladu konstantní intenzity poruch nebo konstantního parametru proudu poruch

[62] ČSN IEC 1123:1994 Zkoušky bezporuchovosti – Plány ověřovacích zkoušek pro podíl úspěšných pokusů

[63] ČSN EN 61124:2007 Zkoušení bezporuchovosti – Ověřovací zkoušky pro konstantní intenzitu poruch a konstantní parametr proudu poruch

[64] ČSN IEC 1070:1994 Postupy ověřovacích zkoušek pro součinitele ustálené pohotovosti

[65] ČSN IEC 61649:1999 Testy dobré shody, konfidenční intervaly a dolní konfidenční meze pro data s Weibullovým rozdělením

[66] ČSN IEC 61650:1998 Techniky analýzy dat o bezporuchovosti – Postupy pro porovnání dvou konstantních intenzit poruch a dvou konstantních parametrů proudu poruch (událostí)

[67] ČSN IEC 1163-1:1996 Třídění namáháním pro zlepšení bezporuchovosti – Část 1: Opravitelné objekty vyráběné v dávkách

[68] ČSN IEC 61163-2:1999 Třídění namáháním pro zlepšení bezporuchovosti – Část 2: Elektronické součástky

[69] ČSN EN 61014:2004 Programy růstu bezporuchovosti

[70] ČSN EN 61164:2005 Růst bezporuchovosti – Metody statistických testů a odhadů

[71] ČSN IEC 61713:2001 Zajištění spolehlivosti softwaru pomocí procesů jeho životního cyklu – Návod k použití

[72] ČSN EN 61508-1:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky

[73] ČSN EN 61508-2:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností

[74] ČSN EN 61508-3:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 3: Požadavky na software

[75] ČSN EN 61508-4:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 4: Definice a zkratky

[76] ČSN EN 61508-5:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovní integrity bezpečnosti

[77] ČSN EN 61508-6:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3

[78] ČSN EN 61508-7:2002 Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností – Část 7: Přehled technik a opatření

[79] ČSN IEC 863:1992 Prezentace předpovědí bezporuchovosti, udržovatelnosti a pohotovosti

[80] Langeron Y., Barros A., Grall A, Bérenguer C.: *Safe failures impact on Safety Instrumented Systems* in Risk, Reliability and Social Safety 2007, London, 2007, ISBN 978-0-415-44786-7

[81] Signoret J.-P., Dutuit Y., Rauzy A.: *High Integrity Protection Systems (HIPS): Methods and tools for efficient Safety Integrity Levels (SIL) analysis and calculations* in Risk, Reliability and Social Safety 2007, London, 2007, ISBN 978-0-415-44786-7

[82] Matuzas V., Uspuras E., Augutis J.: *Degradation assessment and management of systems with dependent components* in Risk, Reliability and Social Safety 2007, London, 2007, ISBN 978-0-415-44786-7

[83] Li W., Zuo M. J.: *Optimal design of multi-state weighted k-out-of-n systems based on component design* in Risk, Reliability and Social Safety 2007, London, 2007, ISBN 978-0-415-44786-7

[84] Zhang T., Lei H.T., Guo B.: *Study on the availability of a k-out-of-N System given limited spares under (m, NG) maintenance policy* in Safety, Reliability and Risk Analysis: Theory, Methods and Applications, London, 2009, ISBN 978-0-415-48513-5

[85] Shingyochi K., Yamamoto H.: *A depth first search algorithm for optimal arrangements in a circular consecutive-k-out-of-n:F system* in Safety, Reliability and Risk Analysis: Theory, Methods and Applications, London, 2009, ISBN 978-0-415-48513-5

[86] Tian Z., Levitin G., Zuo M. J.: *A joint reliability-redundancy optimization approach for multi-state series-parallel systems* in Safety, Reliability and Risk Analysis: Theory, Methods and Applications, London, 2009, ISBN 978-0-415-48513-5

[87] ČSN IEC 60880: Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Softwarová hlediska počítačových systémů vykonávajících funkce kategorie A

Výběr z publikační činnosti autora:

Ročníkový projekt

[88] **Kamenický J.,** Zajíček J.: *Stanovení pravděpodobnosti pádu létajícího stroje na vybranou lokalitu ČR*, TU v Liberci, 2003

Diplomová práce

[89] **Kamenický J.:** *Aplikace stromu poruchových stavů na hodnocení spolehlivosti elektronického zabezpečovacího systému*, TU v Liberci, 2005

Články na konferencích

[90] **Kamenický J.**, Zajíček J.: *Specification of Probability of an Aircraft Disaster in a Selected Location of The Czech republic*, Reliability, Safety and Diagnostics of Transport Structures and means 2005, Pardubice 7.-8.7.2005, ISBN 80-7194-769-5

[91] **Kamenický J.**, Zajíček J.: *Determination of aircraft crash probability in a chemical plant area,* Věda a krizové situace, Konference mladých vědeckých pracovníků, Ostrava 8.11.2005, ISBN 80-248-0944-3

[92] Jirman M, **Kamenický J.**, Marko M.: *Hodnocení ekonomické výhodnosti nasazení elektronického zabezpečovacího systému,* Jednání Odborné skupiny pro spolehlivost - Spolehlivost ve vztahu k bezpečnosti a analýze rizik, Praha, 2006

[93] **Kamenický J.**, Zajíček J.: *Effectiveness optimization of RCM process* in Risk, Reliability and Social Safety, Stavanger, 25.-27.6.2007, ISBN 978-0-415-44786-7

[94] **Kamenický J.**: *Stanovení spolehlivosti zařízení z průmyslových dat*, Spolehlivost tradiční i netradiční (sborník přednášek), setkání OSS, Praha 2007, ISBN 978-80-02-01965-7, počet stran. 55, rozsah 5-17

[95] **Kamenický J.:** *Zkušenosti z analýz poruchovosti čerpadel, používaných v energetice* in Vývojové trendy v čerpací technice, Lutín, 4. 6. 2008, ISBN 978-80-254-2248-9

[96] **Kamenický J.:** *Evaluation methodology of industrial equipment reliability* in ESREL 2008 & 17th SRA Europe, Valencie, 22.-25.9.2008, ISBN 13 978-0-415-48513-5

[97] **Kamenický J**., Zajíček J.: *Typová údržba zařízení na základě vyhodnocení analýz RCM* in Údržba 2008, Liblice, 5.-7.11.2008, ISBN 978-80-254-2500-8

[98] **Kamenický J.:** *Je zapojení „k z n" skutečně nejlepší?* in Národné fórum údržby 2009, Štrbské Pleso, 26. - 27. 5. 2009, ISBN 978-80-554-0018-1

[99] **Kamenický J.:** *Is the "k out of n" system really the best?* in Reliability, Risk & Safety, Praha, 7.-10.9.2009, ISBN 978-0-415-55509-8

Technické zprávy

[100] **Kamenický J.:** *Efektivita procesu S-RCM*, ev.č. FM/KMO/F/Z/06/17

[101] **Kamenický J.:** *Stanovení provozní spolehlivosti chladících čerpadel 1600-BQDV*, ev.č.: FM/KMO/F/Z/06/33

[102] **Kamenický J.:** *Stanovení provozní spolehlivosti kondenzátních čerpadel 125-CVAV*, ev.č.: FM/KMO/F/Z/06/35

[103] **Kamenický J.:** *Stanovení provozní spolehlivosti kondenzátních čerpadel 150-CJNV*, ev.č.: FM/KMO/F/Z/06/36

[104] **Kamenický J.:** *Stanovení provozní spolehlivosti kondenzátních čerpadel 250-CVN*, ev.č.: FM/KMO/F/Z/06/37

[105] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel 250-KHX*, ev.č.: FM/KMO/F/Z/06/38

[106] **Kamenický J.:** *Stanovení provozní spolehlivosti kondenzátních čerpadel 200-CJMV,* ev.č.: FM/RSS/F/Z/07/11

[107] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel 300-QHX,* ev.č.: FM/RSS/F/Z/07/12

[108] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel 600HVBV,* ev.č.: FM/RSS/F/Z/07/13

[109] **Kamenický J.:** *Stanovení provozní spolehlivosti chladících čerpadel 1800-BQUV,* ev.č.: FM/RSS/F/Z/07/14

[110] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel KNE 4.1*, ev.č.: FM/RSS/F/Z/07/17

[111] Fuchs P., Ságl P., **Kamenický J.:** *Rozbor degradace komponent M3-5 EDU, celek 2*, ev.č. FM/RSS/F/Z/07/21

[112] **Kamenický J.:** *Stanovení provozní spolehlivosti průsakových čerpadel 350-CVFV*, ev.č.: FM/RSS/F/Z/07/27

[113] Fuchs P., **Kamenický J.,** Zajíček J.: *Posouzení postupů optimalizace údržby v České rafinérské v kontextu aplikace dle standardu ČSN IEC 60300-3-11*, ev.č. FM/RSS/F/Z/07/29

[114] **Kamenický J.:** *Stanovení provozní spolehlivosti podávacích čerpadel turbonapáječky 300-QHP*, ev.č.: FM/RSS/F/Z/07/30

[115] **Kamenický J.:** *Stanovení provozní spolehlivosti chladících čerpadel 600-BQLV*, ev.č.: FM/RSS/F/Z/07/31

[116] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel 150-CHP*, ev.č.: FM/RSS/F/Z/08/25

[117] **Kamenický J.:** *Stanovení provozní spolehlivosti kondenzátních čerpadel 300-CJMV*, ev.č.: FM/RSS/F/Z/08/26

[118] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel 300x2KHW*, ev.č.: FM/RSS/F/Z/08/27

[119] **Kamenický J.:** *Stanovení provozní spolehlivosti napájecích čerpadel CND4-10.1*, ev.č.: FM/RSS/F/Z/08/28

[120] **Kamenický J.:** *Předběžná analýza nebezpečí (PHA) čerpadla KNE 5.1*, ev. č.: FM/RSS/F/Z/08/36

[121] **Kamenický J.:** *Rozklad zařízení (SH) napájecího čerpadla KNE 5.1*, ev. č.: FM/RSS/F/Z/08/37

[122] **Kamenický J.:** *Analýza způsobů, důsledků a kritičnosti poruch (FMECA) čerpadla KNE 5.1,* ev. č.: FM/RSS/F/Z/09/14

Příloha A: Poznámky k tvorbě logických hodnot pro algoritmy, uvedené v tab. 2.

P1

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav 1, tj. N, všech tří snímačů, ačkoliv jsou signálově připojeny k výpočtovému algoritmu LOG2, také způsobí jeho nečinnost v případě technologické potřeby, tj. LOG2 je také pro tento vstupní term ve stavu N.

P2

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav N všech tří snímačů, ačkoliv jsou signálově připojeny k výpočtovému algoritmu LOG2, také způsobí jeho nečinnost v případě technologické potřeby, tj. LOG2 je také pro tento vstupní term ve stavu N.

P3

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav 3, tj. falešný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako F, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P4

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F, který způsobí jejich falešný výstup. Stav 4, tj. falešný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako F, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P5

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. ve stavu D. Tyto algoritmy jsou tedy v případě

výskytu technologické situace, požadující jejich signál, schopné vydat správný povel, tj. jsou pro daný vstupní term ve stavu D. Stav 5, tj. jeden správný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako D, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P6

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav N všech tří snímačů, ačkoliv jsou signálově připojeny k výpočtovému algoritmu LOG2, také způsobí jeho nečinnost v případě technologické potřeby, tj. LOG2 je také pro tento vstupní term ve stavu N.

P7

Stav všech snímačů je N. Stav výstupů všech algoritmů LOG1, LOG2, LOG3 může mít pro vstupní term jen logickou hodnotu N. Počet rozeznaných a nerozeznaných poruch na trasách snímačů není rozhodující.

P8

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Dva snímače ve stavech 1 a 2, tj. N, nedovolují v algoritmu LOG2 uplatnění signálu ve stavu 3, tj. F. Algoritmus LOG2 není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P9

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P10

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující dobrý signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P11

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav 3, tj. falešný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako F, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P12

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy

v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Dva snímače ve stavech 1 a 2, tj. N, nedovolují v algoritmu LOG2 uplatnění signálu ve stavu 3, tj. F. Algoritmus LOG2 není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P13

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Do algoritmu pro vytváření LOG2 vstupují dva ze tří signálů s logickým hodnocením 3, tj. F, proto algoritmus vydává pro tento vstupní term falešný signál F.

P14

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F. Pro vstupní term vytvářejí algoritmy falešné působení F. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení.

P15

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. dobrý D. Pro vstupní term vytvářejí algoritmy správný povel D. Algoritmus LOG2 se vstupem dobrého a falešného signálu vydává povel ke správnému působení D.

P16

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F, který způsobí jejich falešný výstup. Stav 4, tj. falešný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako F, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P17

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P18

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F. Pro vstupní term vytvářejí algoritmy falešné působení F. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení.

P19

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů ve stavu 4, tj. v nerozeznaném F, v nich vytvoří falešné zapůsobení F. K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu F. Výstup algoritmu LOG2 je pro tento vstupní term ve stavu F.

P20

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude, při správné hodnotě z jednoho snímače, spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny snímače ve třech odlišných stavech N, F, D. Vstupující dobrý signál spolu s falešným se uplatní pro tento vstupní term jako správné působení D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu, vstupující jako dobrý spolu s falešným, se uplatní pro tento vstupní term jako správné působení D.

P21

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. ve stavu D. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, schopné vydat správný povel, tj. jsou pro daný vstupní term ve stavu D. Stav 5, tj. jeden správný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako D, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P22

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující dobrý signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P23

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. dobrý D. Pro vstupní term vytvářejí algoritmy

správný povel D. Algoritmus LOG2 se vstupem dobrého a falešného signálu vydává povel ke správnému působení D.

P24

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude, při správné hodnotě z jednoho snímače, spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny snímače ve třech odlišných stavech N, F, D. Vstupující dobrý signál spolu s falešným se uplatní pro tento vstupní term jako správné působení D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu, vstupující jako dobrý spolu s falešným, se uplatní pro tento vstupní term jako správné působení D.

P25

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1, LOG3. Hodnoty zbylých dvou snímačů jsou ve shodných D. Výstup obou algoritmů pro tento vstupní term je D.

K algoritmu pro tvorbu LOG2 jsou připojeny dva snímače ve stavu D. Vystupující signál má pro tento vstupní term hodnotu správného působení D.

P26

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav N všech tří snímačů, ačkoliv jsou signálově připojeny k výpočtovému algoritmu LOG2, také způsobí jeho nečinnost v případě technologické potřeby, tj. LOG2 je také pro tento vstupní term ve stavu N.

P27

Stav všech snímačů je N. Stav výstupů všech algoritmů LOG1, LOG2, LOG3 může mít pro vstupní term jen logickou hodnotu N. Počet rozeznaných a nerozeznaných poruch na trasách snímačů není rozhodující.

P28

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Dva snímače ve stavech 1 a 2, tj. N, nedovolují v algoritmu LOG2 uplatnění signálu ve stavu 3, tj. F. Algoritmus LOG2 není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P29

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P30

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující dobrý signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P31

Stav všech snímačů je N. Stav výstupů všech algoritmů LOG1, LOG2, LOG3 může mít pro vstupní term jen logickou hodnotu N. Počet rozeznaných a nerozeznaných poruch na trasách snímačů není rozhodující.

P32

Jako vstupy algoritmů pro LOG1, LOG2 i LOG3 přicházejí ze všech snímačů signály ve stavu 4, tj. nerozeznané N. Algoritmy jsou tedy v případě výskytu technologické situace požadující jejich působení nečinné, tj. ve stavu N.

P33

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty ze zbylých dvou snímačů jsou ve shodných stavech 2, tj. nerozeznaného N. Algoritmy jsou v případě technologické potřeby neschopné být činnými, tj. jsou pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P34

Do algoritmu pro tvorbu LOG1 vstupují signály ze všech tří snímačů s nerozeznanými poruchovými stavy. Dva jako N a jeden jako F. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P35

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy 2, tj. nebezpečná porucha N a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu N. Zbývající signál D se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen plnit svou funkci, tj. LOG3 je pro tento vstupní term ve stavu N.

P36

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Dva snímače ve stavech 1 a 2, tj. N, nedovolují v algoritmu LOG2 uplatnění signálu ve stavu 3, tj. F. Algoritmus LOG2 není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P37

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty ze zbylých dvou snímačů jsou ve shodných stavech 2, tj. nerozeznaného N. Algoritmy jsou v případě technologické potřeby neschopné být činnými, tj. jsou pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P38

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Algoritmy jsou tedy v případě výskytu technologické situace požadující jejich působení nečinné, tj. ve stavu N. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

P39

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P40

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dobrého, falešného a nebezpečného signálu vydává povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které přehlasují falešné působení. Při takovýchto vstupech překvapivě výběrový mechanismus vydá správný logický povel.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P41

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P42

Do algoritmu pro tvorbu LOG1 vstupují signály ze všech tří snímačů s nerozeznanými poruchovými stavy. Dva jako N a jeden jako F. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P43

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P44

Do algoritmu pro tvorbu LOG1 vstupují signály ze všech tří snímačů s nerozeznanými poruchovými stavy. Dva jako F a jeden jako N. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu F. Algoritmus LOG2 je pro tento vstupní term ve stavu F.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu F. Algoritmus LOG3 je pro tento vstupní term ve stavu F.

P45

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Jeden se stavem 2, tj. jako N, jeden se stavem 4, tj. jako F a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny snímače ve stavech N, F a D. Algoritmy LOG2 a LOG3 se vstupem dobrého, falešného a nebezpečného signálu vydají povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které společně

přehlasují falešné působení. Při takovýchto vstupech výběrový mechanismus vydá správný logický povel.

P46

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující dobrý signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P47

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy 2, tj. nebezpečná porucha N a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu N. Zbývající signál D se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen plnit svou funkci, tj. LOG3 je pro tento vstupní term ve stavu N.

P48

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dobrého, falešného a nebezpečného signálu vydává povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které přehlasují falešné působení. Při takovýchto vstupech překvapivě výběrový mechanismus vydá správný logický povel.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P49

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Jeden se stavem 2, tj. jako N, jeden se stavem 4, tj. jako F a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny snímače ve stavech N, F a D. Algoritmy LOG2 a LOG3 se vstupem dobrého, falešného a nebezpečného signálu vydají povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které společně přehlasují falešné působení. Při takovýchto vstupech výběrový mechanismus vydá správný logický povel.

P50

Do algoritmu pro tvorbu LOG1 vstupuje jeden signál se stavem 2, tj. jako nerozeznané N a dva se stavem 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N,

D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny dva snímače ve stavu a D. Logická hodnota jejich výstupů je tedy D.

P51

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Stav 3, tj. falešný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako F, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P52

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Dva snímače ve stavech 1 a 2, tj. N, nedovolují v algoritmu LOG2 uplatnění signálu ve stavu 3, tj. F. Algoritmus LOG2 není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P53

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Do algoritmu pro vytváření LOG2 vstupují dva ze tří signálů s logickým hodnocením 3, tj. F, proto algoritmus vydává pro tento vstupní term falešný signál F.

P54

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F. Pro vstupní term vytvářejí algoritmy falešné působení F. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení.

P55

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. dobrý D. Pro vstupní term vytvářejí algoritmy správný povel D. Algoritmus LOG2 se vstupem dobrého a falešného signálu vydává povel ke správnému působení D.

P56

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Dva snímače ve stavech 1 a 2, tj. N, nedovolují v algoritmu LOG2 uplatnění signálu ve stavu 3, tj. F. Algoritmus LOG2 není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P57

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty ze zbylých dvou snímačů jsou ve shodných stavech 2, tj. nerozeznaného N. Algoritmy jsou v případě technologické potřeby neschopné být činnými, tj. jsou pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P58

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Algoritmy jsou tedy v případě výskytu technologické situace požadující jejich působení nečinné, tj. ve stavu N. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

P59

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu

algoritmu LOG1 (N, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P60

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dobrého, falešného a nebezpečného signálu vydává povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které přehlasují falešné působení. Při takovýchto vstupech překvapivě výběrový mechanismus vydá správný logický povel.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P61

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace, požadující jejich signál, nečinné, tj. ve stavu N. Do algoritmu pro vytváření LOG2 vstupují dva ze tří signálů s logickým hodnocením 3, tj. F, proto algoritmus vydává pro tento vstupní term falešný signál F.

P62

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 2, tj. v nerozeznaném stavu N. Algoritmy jsou tedy v případě výskytu technologické situace požadující jejich působení nečinné, tj. ve stavu N. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

P63

Rozeznaná porucha všech tří snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Tyto jsou tedy v případě výskytu technologické situace požadující jejich signál nečinné, tj. ve stavu N. Signály všech tří snímačů ve stavu 3, tj. F připojených k výpočtovému algoritmu LOG2 způsobují jeho výstupní stav F.

P64

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F, který způsobí jejich falešný výstup F. Tři vstupy připojené k výpočtovému algoritmu LOG2 ve stavu F způsobují jeho výstup jako F.

P65

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 5, tj. ve stavu D. Tyto algoritmy jsou tedy v případě výskytu technologické situace požadující jejich signál schopné vydat správný povel, tj. jsou pro daný vstupní term ve stavu D.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

P66

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F. Pro vstupní term vytvářejí algoritmy falešné působení F. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení.

P67

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech

N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P68

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F, který způsobí jejich falešný výstup F. Tři vstupy připojené k výpočtovému algoritmu LOG2 ve stavu F způsobují jeho výstup jako F.

P69

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty ze zbylých dvou snímačů ve stavu 4, tj. v nerozeznaném F, v nich vytvoří falešné zapůsobení F. K algoritmu pro tvorbu LOG2 jsou připojeny tři snímače ve stavu F. Výstup algoritmu LOG2 je pro tento vstupní term ve stavu F.

P70

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou připojených snímačů do algoritmu vstupují jako dobrý spolu s falešným a uplatní se pro tento vstupní term jako správné působení D.

P71

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. dobrý D. Pro vstupní term vytvářejí algoritmy správný povel D. Algoritmus LOG2 se vstupem dobrého a falešného signálu vydává povel ke správnému působení D.

P72

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dobrého, falešného a nebezpečného signálu vydává povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které přehlasují falešné působení. Při takovýchto vstupech překvapivě výběrový mechanismus vydá správný logický povel.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P73

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 5, tj. ve stavu D. Tyto algoritmy jsou tedy v případě výskytu technologické situace požadující jejich signál schopné vydat správný povel, tj. jsou pro daný vstupní term ve stavu D.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

P74

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou připojených snímačů do algoritmu vstupují jako dobrý spolu s falešným a uplatní se pro tento vstupní term jako správné působení D.

P75

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty zbylých dvou snímačů jsou ve shodných stavech D. Výstup obou algoritmů je pro tento vstupní term D.

K algoritmu pro tvorbu LOG2 jsou připojeny dva snímače ve stavu D. Vystupující signál má pro tento vstupní term hodnotu správného působení D.

P76

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F, který způsobí jejich falešný výstup. Stav 4, tj. falešný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako F, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P77

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a

F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P78

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F. Pro vstupní term vytvářejí algoritmy falešné působení F. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení.

P79

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů ve stavu 4, tj. v nerozeznaném F, v nich vytvoří falešné zapůsobení F. K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu F. Výstup algoritmu LOG2 je pro tento vstupní term ve stavu F.

P80

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude, při správné hodnotě z jednoho snímače, spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny snímače ve třech odlišných stavech N, F, D. Vstupující dobrý signál spolu s falešným se uplatní pro tento vstupní term jako správné působení D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu, vstupující jako dobrý spolu s falešným, se uplatní pro tento vstupní term jako správné působení D.

P81

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani

logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 je v případě technologické potřeby neschopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P82

Do algoritmu pro tvorbu LOG1 vstupují signály ze všech tří snímačů s nerozeznanými poruchovými stavy. Dva jako N a jeden jako F. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující falešný signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P83

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P84

Do algoritmu pro tvorbu LOG1 vstupují signály ze všech tří snímačů s nerozeznanými poruchovými stavy. Dva jako F a jeden jako N. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu F. Algoritmus LOG2 je pro tento vstupní term ve stavu F.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu F. Algoritmus LOG3 je pro tento vstupní term ve stavu F.

P85

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Jeden se stavem 2, tj. jako N, jeden se stavem 4, tj. jako F a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny snímače ve stavech N, F a D. Algoritmy LOG2 a LOG3 se vstupem dobrého, falešného a nebezpečného signálu vydají povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které společně přehlasují falešné působení. Při takovýchto vstupech výběrový mechanismus vydá správný logický povel.

P86

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F. Pro vstupní term

vytvářejí algoritmy falešné působení F. Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení.

P87

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a F a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dvou falešných signálů ze tří vyvolává falešné působení F.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a F, což zabraňuje vytvoření falešného signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P88

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 4, tj. v nerozeznaném stavu F, který způsobí jejich falešný výstup F. Tři vstupy připojené k výpočtovému algoritmu LOG2 ve stavu F způsobují jeho výstup jako F.

P89

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty ze zbylých dvou snímačů ve stavu 4, tj. v nerozeznaném F, v nich vytvoří falešné zapůsobení F. K algoritmu pro tvorbu LOG2 jsou připojeny tři snímače ve stavu F. Výstup algoritmu LOG2 je pro tento vstupní term ve stavu F.

P90

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou připojených snímačů do algoritmu vstupují jako dobrý spolu s falešným a uplatní se pro tento vstupní term jako správné působení D.

P91

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1, LOG3. Hodnoty ze zbylých dvou snímačů ve stavu 4, tj. v nerozeznaném F, v nich vytvoří falešné zapůsobení F. K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu F. Výstup algoritmu LOG2 je pro tento vstupní term ve stavu F.

P92

Do algoritmu pro tvorbu LOG1 vstupují signály ze všech tří snímačů s nerozeznanými poruchovými stavy. Dva jako F a jeden jako N. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu F. Algoritmus LOG2 je pro tento vstupní term ve stavu F.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu F. Algoritmus LOG3 je pro tento vstupní term ve stavu F.

P93

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty ze zbylých dvou snímačů ve stavu 4, tj. v nerozeznaném F, v nich vytvoří falešné zapůsobení F. K algoritmu pro tvorbu LOG2 jsou připojeny tři snímače ve stavu F. Výstup algoritmu LOG2 je pro tento vstupní term ve stavu F.

P94

K algoritmům pro vytváření logických povelových signálů jsou připojeny tři vstupní signály s logickou hodnotou F. Výstupy všech hodnocených algoritmů pro tento vstupní term mohou být pouze F.

P95

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Dva se stavem 4, tj. F a jeden 5, tj. D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

K algoritmu pro tvorbu LOG3 jsou připojeny snímače se dvěma falešnými signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

P96

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude, při správné hodnotě z jednoho snímače, spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny snímače ve třech odlišných stavech N, F, D. Vstupující dobrý signál spolu s falešným se uplatní pro tento vstupní term jako správné působení D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu, vstupující jako dobrý spolu s falešným, se uplatní pro tento vstupní term jako správné působení D.

P97

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Jeden se stavem 2, tj. jako N, jeden se stavem 4, tj. jako F a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny snímače ve stavech N, F a D. Algoritmy LOG2 a LOG3 se vstupem dobrého, falešného a nebezpečného signálu vydají povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které společně přehlasují falešné působení. Při takovýchto vstupech výběrový mechanismus vydá správný logický povel.

P98

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou připojených snímačů do algoritmu vstupují jako dobrý spolu s falešným a uplatní se pro tento vstupní term jako správné působení D.

P99

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Dva se stavem 4, tj. F a jeden 5, tj. D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

K algoritmu pro tvorbu LOG3 jsou připojeny snímače se dvěma falešnými signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

P100

Do algoritmu pro tvorbu LOG1 vstupuje jeden signál ze snímače s nerozeznaným poruchovým stavem 4, tj. F a dva snímače ve stavu 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude i při

správné hodnotě ze dvou snímačů spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmům pro tvorbu logického povelového signálu LOG2 a LOG3 jsou připojeny snímače ve dvou odlišných stavech F, D, D. Vstupující dva dobré signály D spolu s falešným vyhodnotí oba algoritmy pro tento vstupní term jako správné působení D.

P101

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. ve stavu D. Tyto algoritmy jsou tedy v případě výskytu technologické situace, požadující jejich signál, schopné vydat správný povel, tj. jsou pro daný vstupní term ve stavu D. Stav 5, tj. jeden správný aktivující signál připojený k výpočtovému algoritmu LOG2 není schopen způsobit jeho výstup jako D, jelikož jej blokují stavy N zbývajících dvou snímačů. Algoritmus LOG2 je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

P102

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující dobrý signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P103

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. dobrý D. Pro vstupní term vytvářejí algoritmy

správný povel D. Algoritmus LOG2 se vstupem dobrého a falešného signálu vydává povel ke správnému působení D.

P104

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude, při správné hodnotě z jednoho snímače, spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny snímače ve třech odlišných stavech N, F, D. Vstupující dobrý signál spolu s falešným se uplatní pro tento vstupní term jako správné působení D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu, vstupující jako dobrý spolu s falešným, se uplatní pro tento vstupní term jako správné působení D.

P105

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1, LOG3. Hodnoty zbylých dvou snímačů jsou ve shodných D. Výstup obou algoritmů pro tento vstupní term je D.

K algoritmu pro tvorbu LOG2 jsou připojeny dva snímače ve stavu D. Vystupující signál má pro tento vstupní term hodnotu správného působení D.

P106

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v nesouhlasných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Vstupující dobrý signál se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P107

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy 2, tj. nebezpečná porucha N a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny dva ze tří snímačů ve stavu N. Algoritmus je v případě technologické potřeby neschopen být činný, tj. LOG2 je pro tento vstupní term ve stavu N.

K algoritmu pro tvorbu LOG3 jsou připojeny dva ze tří snímačů ve stavu N. Zbývající signál D se nemůže uplatnit. Algoritmus není v případě technologické potřeby schopen plnit svou funkci, tj. LOG3 je pro tento vstupní term ve stavu N.

P108

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dobrého, falešného a nebezpečného signálu vydává povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které přehlasují falešné působení. Při takovýchto vstupech překvapivě výběrový mechanismus vydá správný logický povel.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P109

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Jeden se stavem 2, tj. jako N, jeden se stavem 4, tj. jako F a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny snímače ve stavech N, F a D. Algoritmy LOG2 a LOG3 se vstupem dobrého, falešného a nebezpečného signálu vydají povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které společně přehlasují falešné působení. Při takovýchto vstupech výběrový mechanismus vydá správný logický povel.

P110

Do algoritmu pro tvorbu LOG1 vstupuje jeden signál se stavem 2, tj. jako nerozeznané N a dva se stavem 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny dva snímače ve stavu a D. Logická hodnota jejich výstupů je tedy D.

P111

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1, LOG3. Zbývající připojený snímač je ve stavu 5, tj. dobrý D. Pro vstupní term vytvářejí algoritmy správný povel D. Algoritmus LOG2 se vstupem dobrého a falešného signálu vydává povel ke správnému působení D.

P112

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v neshodných stavech N a D a není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu

algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

Algoritmus LOG2 se vstupem dobrého, falešného a nebezpečného signálu vydává povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které přehlasují falešné působení. Při takovýchto vstupech překvapivě výběrový mechanismus vydá správný logický povel.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu jsou v nesouhlasných stavech N a D, což zabraňuje vytvoření dobrého signálu. Algoritmus LOG3 není v případě technologické potřeby schopen být činný, tj. LOG3 je pro tento vstupní term ve stavu N.

P113

Rozeznaná porucha dvou snímačů je odpojí od algoritmů pro vytváření LOG1 a LOG3. Zbývající připojený snímač je ve stavu 5, tj. ve stavu D. Tyto algoritmy jsou tedy v případě výskytu technologické situace požadující jejich signál schopné vydat správný povel, tj. jsou pro daný vstupní term ve stavu D.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

P114

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou připojených snímačů do algoritmu vstupují jako dobrý spolu s falešným a uplatní se pro tento vstupní term jako správné působení D.

P115

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty zbylých dvou snímačů jsou ve shodných stavech D. Výstup obou algoritmů je pro tento vstupní term D.

K algoritmu pro tvorbu LOG2 jsou připojeny dva snímače ve stavu D. Vystupující signál má pro tento vstupní term hodnotu správného působení D.

P116

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude, při správné hodnotě z jednoho snímače, spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmu pro tvorbu LOG2 jsou připojeny snímače ve třech odlišných stavech N, F, D. Vstupující dobrý signál spolu s falešným se uplatní pro tento vstupní term jako správné působení D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou snímačů připojených k algoritmu, vstupující jako dobrý spolu s falešným, se uplatní pro tento vstupní term jako správné působení D.

P117

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Jeden se stavem 2, tj. jako N, jeden se stavem 4, tj. jako F a jeden 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D, F?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny snímače ve stavech N, F a D. Algoritmy LOG2 a LOG3 se vstupem dobrého, falešného a nebezpečného signálu vydají povel ke správnému působení D na základě shody dobrého a nebezpečného signálu, které společně přehlasují falešné působení. Při takovýchto vstupech výběrový mechanismus vydá správný logický povel.

P118

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG1. Hodnoty ze zbylých dvou snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

Rozeznaná porucha jednoho snímače ho odpojí od algoritmu pro vytváření LOG3. Hodnoty ze zbylých dvou připojených snímačů do algoritmu vstupují jako dobrý spolu s falešným a uplatní se pro tento vstupní term jako správné působení D.

P119

Do algoritmu pro tvorbu LOG1 vstupují dva signály ze snímačů s nerozeznanými poruchovými stavy. Dva se stavem 4, tj. F a jeden 5, tj. D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude při správné hodnotě z jednoho snímače spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K výpočtovému algoritmu LOG2 jsou připojeny dva falešné signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

K algoritmu pro tvorbu LOG3 jsou připojeny snímače se dvěma falešnými signály, které vyvolají jeho stav F, dříve než by se kombinovaly s oprávněným správným zapůsobením D.

P120

Do algoritmu pro tvorbu LOG1 vstupuje jeden signál ze snímače s nerozeznaným poruchovým stavem 4, tj. F a dva snímače ve stavu 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude i při správné hodnotě ze dvou snímačů spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmům pro tvorbu logického povelového signálu LOG2 a LOG3 jsou připojeny snímače ve dvou odlišných stavech F, D, D. Vstupující dva dobré signály D spolu s falešným vyhodnotí oba algoritmy pro tento vstupní term jako správné působení D.

P121

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1, LOG3. Hodnoty zbylých dvou snímačů jsou ve shodných D. Výstup obou algoritmů pro tento vstupní term je D.

K algoritmu pro tvorbu LOG2 jsou připojeny dva snímače ve stavu D. Vystupující signál má pro tento vstupní term hodnotu správného působení D.

P122

Do algoritmu pro tvorbu LOG1 vstupuje jeden signál se stavem 2, tj. jako nerozeznané N a dva se stavem 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Není možno rozhodnout, jaký bude číselný výsledek, tedy ani logická hodnota výstupu algoritmu LOG1 (N, D?). Arbitrárně volíme hodnotu N, kterou považujeme za nejhorší z hlediska spolehlivostního hodnocení.

K algoritmům pro tvorbu LOG2 a LOG3 jsou připojeny dva snímače ve stavu a D. Logická hodnota jejich výstupů je tedy D.

P123

Rozeznaná porucha jednoho snímače ho odpojí od algoritmů pro vytváření LOG1 a LOG3. Hodnoty zbylých dvou snímačů jsou ve shodných stavech D. Výstup obou algoritmů je pro tento vstupní term D.

K algoritmu pro tvorbu LOG2 jsou připojeny dva snímače ve stavu D. Vystupující signál má pro tento vstupní term hodnotu správného působení D.

P124

Do algoritmu pro tvorbu LOG1 vstupuje jeden signál ze snímače s nerozeznaným poruchovým stavem 4, tj. F a dva snímače ve stavu 5, tj. dobrý D. Hodnoty snímačů se v algoritmu LOG1 průměrují. Jsou v rozdílných stavech F a D a číselný výsledek bude i při správné hodnotě ze dvou snímačů spíše v oblasti falešného působení F. Arbitrárně volíme hodnotu F jako konzervativní spolehlivostní hodnocení.

K algoritmům pro tvorbu logického povelového signálu LOG2 a LOG3 jsou připojeny snímače ve dvou odlišných stavech F, D, D. Vstupující dva dobré signály D spolu s falešným vyhodnotí oba algoritmy pro tento vstupní term jako správné působení D.

P125

K algoritmům pro tvorbu LOG1, LOG2 a LOG3 jsou připojeny tři snímače ve stavu 5, tj, dobrý D. Logická hodnota výstupů všech tří algoritmů tedy může být pouze D.