TECHNICKÁ UNIVERZITA
V LIBERCI
Fakulta machatroniky, informatiky
a mezioborových studií

Verifikace a validace informace o měřené veličině

Autoreferát disertační práce

Liberec, 2009 Ing. Jan Kamenický

Disertační práce byla vypracována v prezenční formě doktorského studia, studijní program Elektrotechnika a informatika, studijní obor Přírodovědné inženýrství, tematický okruh Pokročilé metody modelování spolehlivosti na ústavu Řízení systémů a spolehlivosti fakulty Mechatroniky, informatiky a mezioborových studií Technické univerzity v Liberci. Téma disertační práce bylo zvoleno ve znění „Verifikace a validace informace o měřené veličině“.

Uchazeč: Ing. Jan Kamenický
Ústav řízení systémů a spolehlivosti
Fakulta Mechatroniky, informatiky a mezioborových studií
Technická univerzita v Liberci
Studentská 2
461 17 Liberec

Školitel: Ing. David Vališ, Ph.D.
Katedra bojových a speciálních vozidel
Fakulta vojenských technologií
Univerzita obrany
Kounicova 65
662 10 Brno

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

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.

Klíčová slova:

verifikace a validace, spolehlivost, výběrové systémy „*k* z *n*“, zálohované systémy

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.

Key words:

verification and validation, dependability, „*k* out of *n*“ system, backup system

Obsah

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.

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 ČSN IEC 60880 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 ČSN IEC 61713:2001:

- **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 ČSN EN 61160:2006 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 ČSN EN 61160:2006 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

[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.

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 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 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.

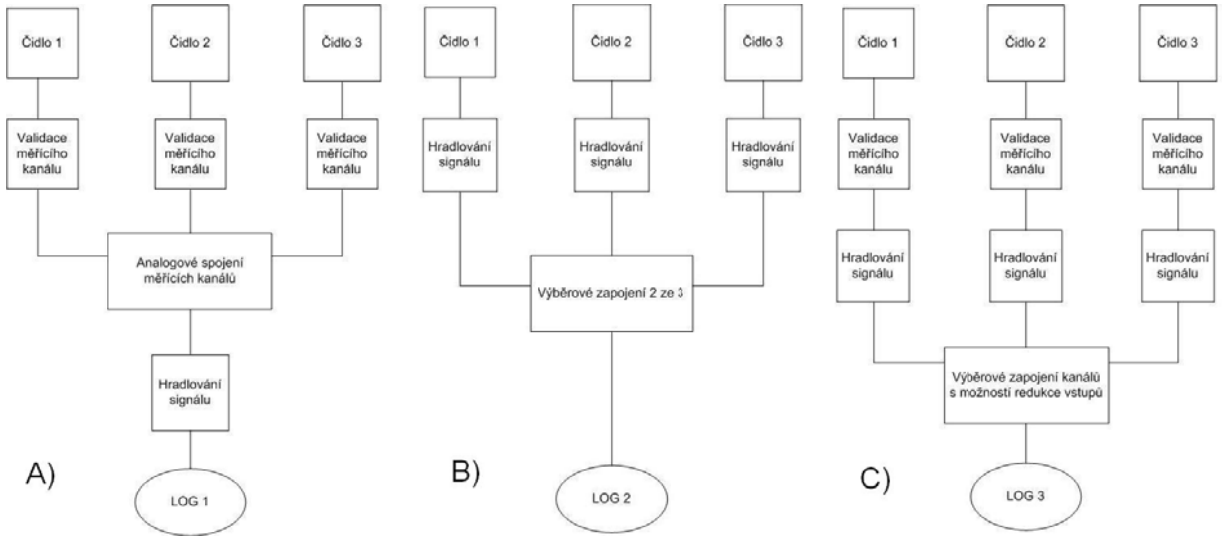
2.3 Validace pomocí logického spojování signálů

2.3.1 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. 1 (varianta A) a v další práci bude označeno jako LOG1.

---

[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.“.



Obr. 1: Možnosti spojení tří redundantních měřících kanálů do jedné výsledné hodnoty

2.3.2 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. 1 (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.

2.3.3 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. 1 (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.

2.3.4 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.

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.

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 vypočítat jednotlivé požadované spolehlivostní ukazatele. Předkládaná disertační práce může sloužit jako podklad pro doplnění metodického pokynu normy ČSN EN 61508 o metodiku výběru nejvhodnějšího zapojení násobných měřicích kanálů za účelem získání jediné výsledné hodnoty, použitelné pro řízení procesu nebo pro bezpečnostní systém.

4 Spolehlivost ve vybraných publikacích

4.1 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 [18] 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 [19]. 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. [20], 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. [21]. 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 [22] 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 [23]. 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 [24]. 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.

4.2 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 disertační práce je uveden přehled norem se vztahem k problematice spolehlivosti a u každé normy je uveden stručný komentář obsahu této normy.

4.3 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 v 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.

5 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 v níže. Zvýšení spolehlivosti měřicích systémů pomocí spolehlivějších snímačů nespadá do problematiky této disertační práce.

5.1 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.

5.1.1 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 2.3 a znázorněny na obr. 1. 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:

$$\lambda = \lambda_n + \lambda_f \quad (1)$$

$$\lambda_n = \lambda_1 + \lambda_2 \quad (2)$$

$$\lambda_f = \lambda_3 + \lambda_4 \quad (3)$$

$$\lambda = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 \quad (4)$$

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 vzájemně nezávislých možných stavů systému. Tato tabulka nebude v autoreferátu vzhledem ke svému rozsahu uvedena, v disertační práci se jedná o tab. 2.

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, jsou v ní pouze uvedeny logické důsledky poruch jednotlivých individuálních měřicích kanálů.

5.1.2 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. 2 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 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. Výsledky popsaného výpočtu jsou uvedeny v následující tabulce.

Tab. 1: 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		

Podle Schneeweissovy formule 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. 2.

Tab. 2: Parametry modelového případu hodnocení logických vyhodnocovacích členů

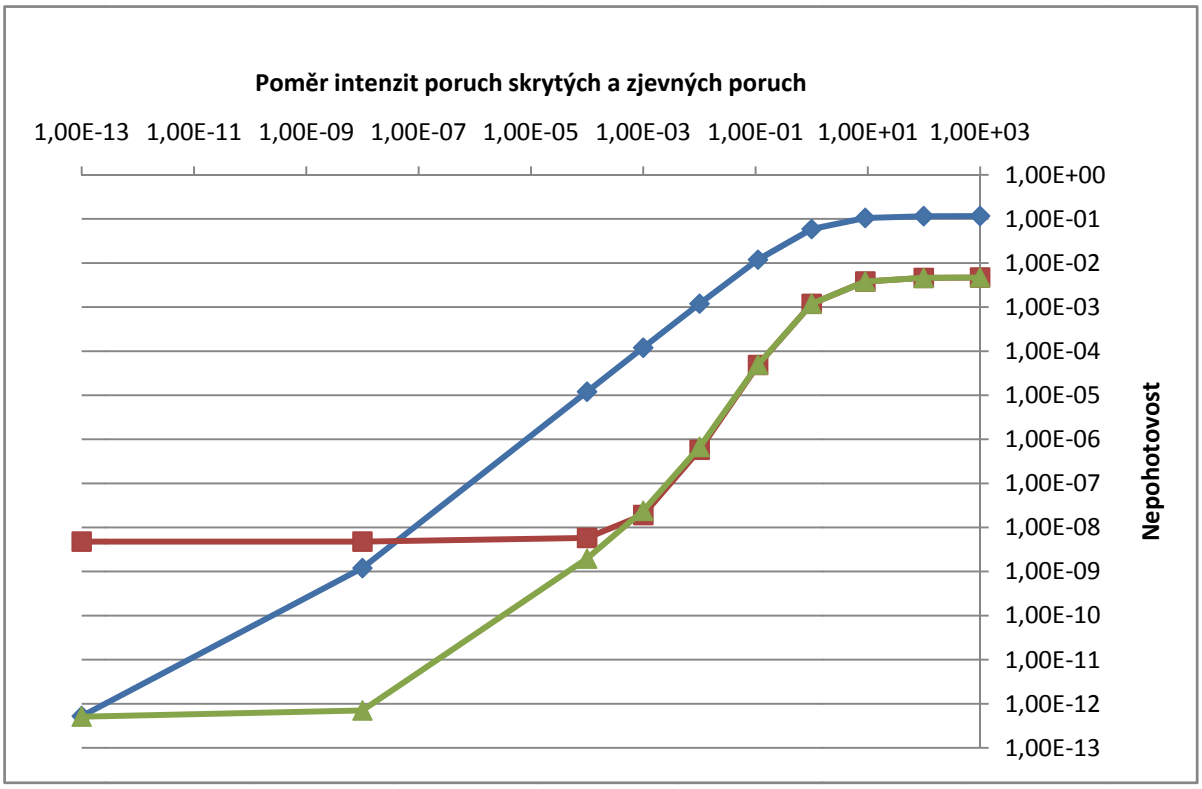
P. č.	λ_{celk} [h^{-1}]	U_{LOG1} [1]	T_{LOG1} [h]	U_{LOG2} [1]	T_{LOG2} [h]	U_{LOG3} [1]	T_{LOG3} [h]	$\lambda_{skrytá}$/ $\lambda_{zjevná}$ [1]
1	2,00E-05	1,17E-01	3,11E+04	4,69E-03	4,00E+05	4,69E-03	4,00E+05	1,00E+03
2	2,00E-05	1,16E-01	3,13E+04	4,61E-03	4,04E+05	4,61E-03	4,07E+05	9,90E+01
3	2,00E-05	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. 2 je střední doba mezi falešnými akcemi jednotlivých algoritmů označena z prostorových důvodů jako T_{LOGX}.

5.1.3 Výsledky rozhodovacího modelu

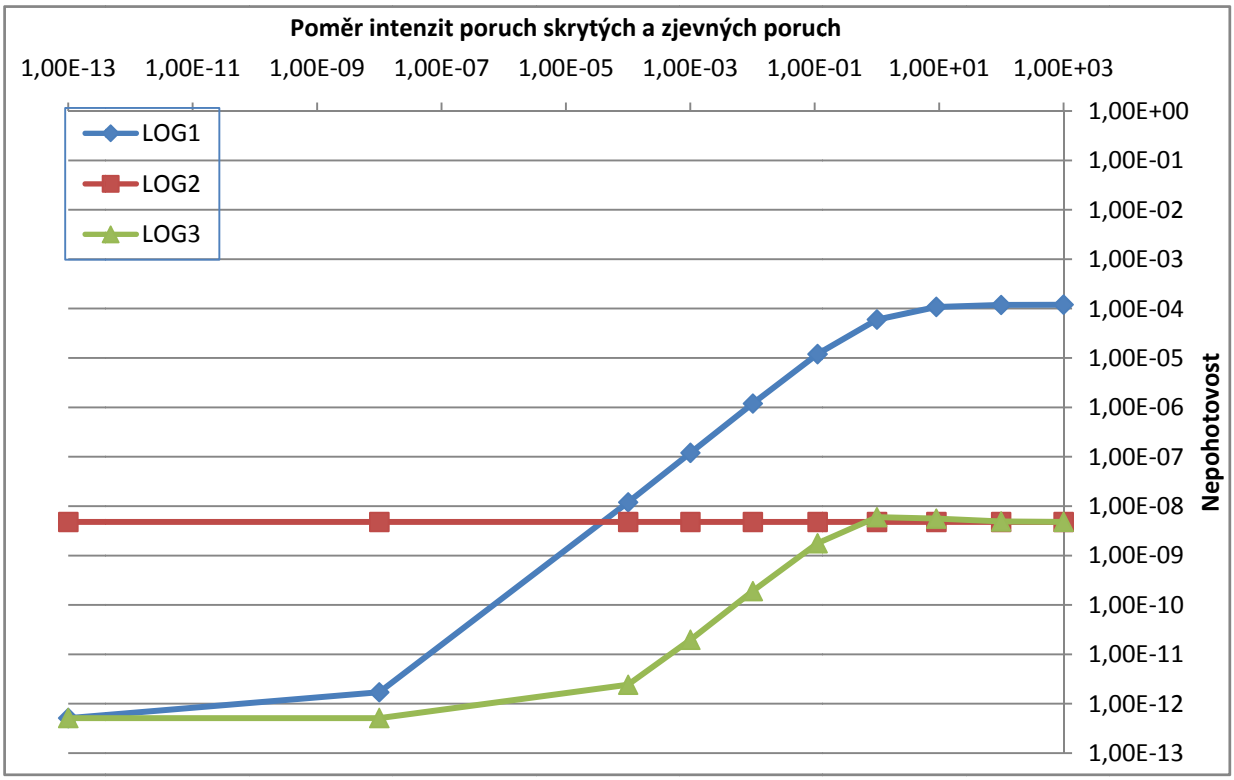
Tab. 2 přehledně shrnuje výsledky výpočtů nepohotovostí a středních dob mezi poruchami pro jednotlivé varianty poměrů skrytých a zjevných poruch, za předpokladu střední doby do obnovy u zjevné poruchy v délce 4h a v případě skryté poruchy 4000h. Bezpečné a nebezpečné poruchy nebyly variovány z důvodu 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 a střední doby mezi poruchami na poměru intenzit zjevných a skrytých poruch vidět v grafické reprezentaci, viz obr. 2 a obr. 4.



Obr. 2: Graf závislosti nepohotovosti systému na poměru intenzit skrytých a zjevných poruch

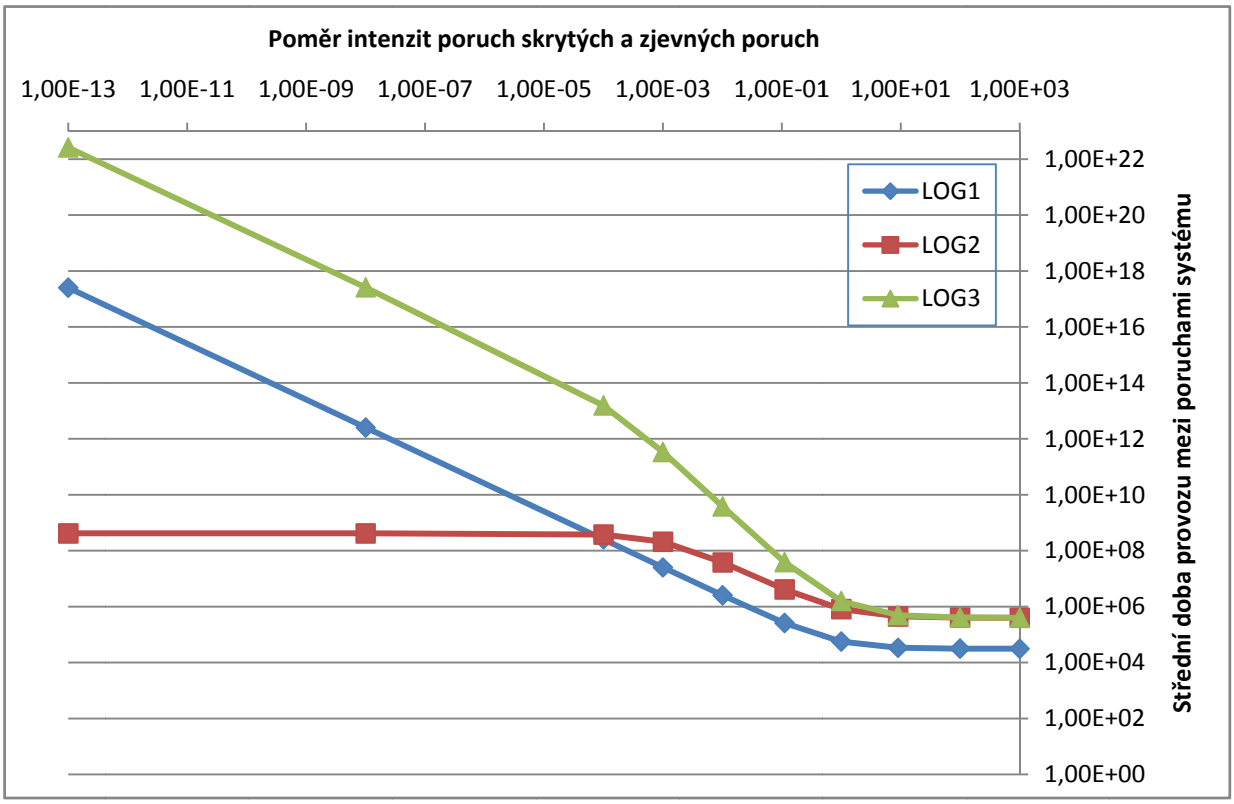
Na obr. 2 je zřetelně vidět, že nepohotovost celého měřicího systému, skládajícího se z kombinace tří snímačů, roste s rostoucím poměrem skrytých a zjevných poruch, tedy s rostoucí převahou poruch pro verifikační algoritmus skrytých. Zvláštním případem algoritmu je výběrové zapojení *2 ze 3*, u kterého 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. 3.



Obr. 3: 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

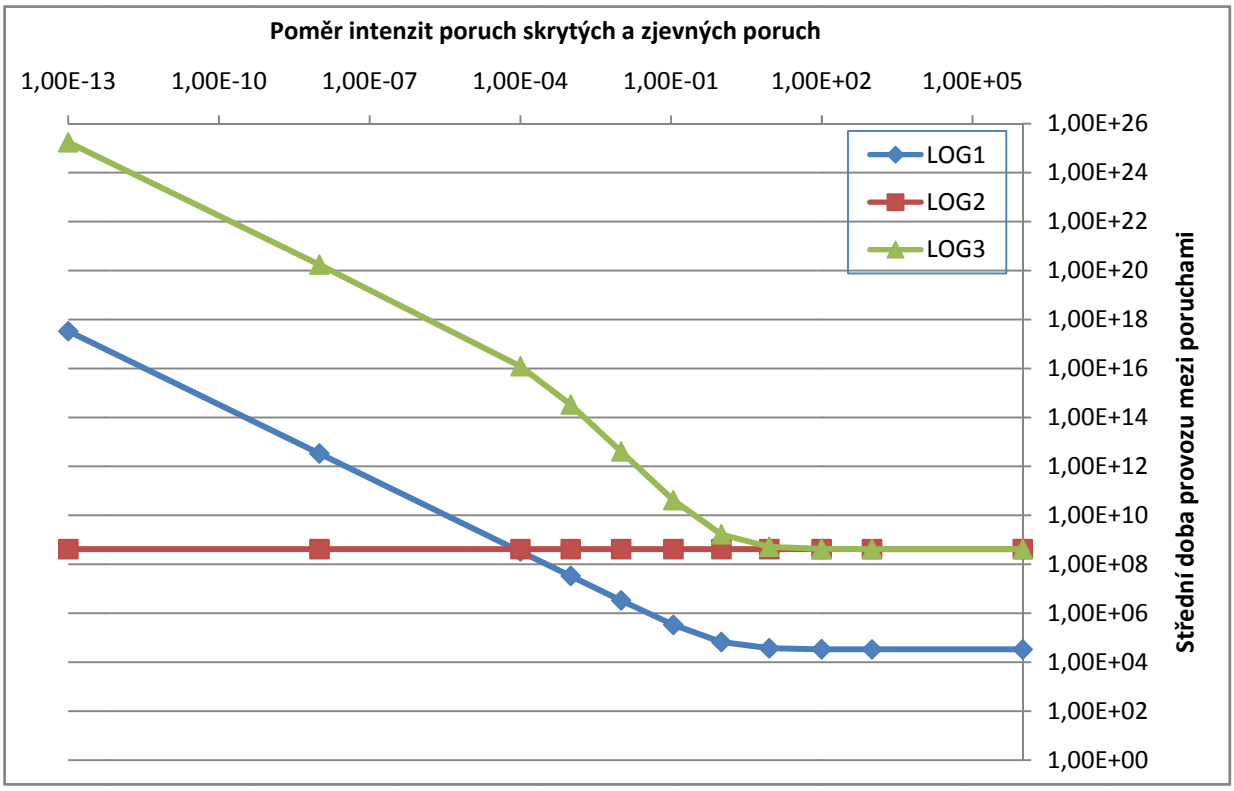
Na obr. 3 je zřejmý trend růstu nepohotovosti se stoupajícím procentem zastoupení skrytých poruch. Výjimkou je v tomto případě výběrové zapojení LOG2, u kterého nemá poměr intenzit poruch skrytých a zjevných poruch vliv na hodnotu nepohotovosti. Je to dáno tím, že toto výběrové zapojení nebere v úvahu validitu jednotlivých individuálních vstupů. Na grafu z obr. 3 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 měřicích kanálů 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. 2 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. 4: Závislost střední doby mezi poruchami na poměru intenzit skrytých a zjevných poruch

Stejně jako v případě grafu nepohotovosti z obr. 3, 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. 4.



Obr. 5: 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. 5 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. 2-5 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.

5.2 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 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, tedy sestavení kombinací čidel pro násobné měření fyzikálních veličin a určení výhodnosti takového měření v porovnání s tzv. smart čidly[3]. Další možností užití předkládané myšlenky je kombinace požárních čidel, případně čidel plášťové ochrany objektu,

[3] 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.

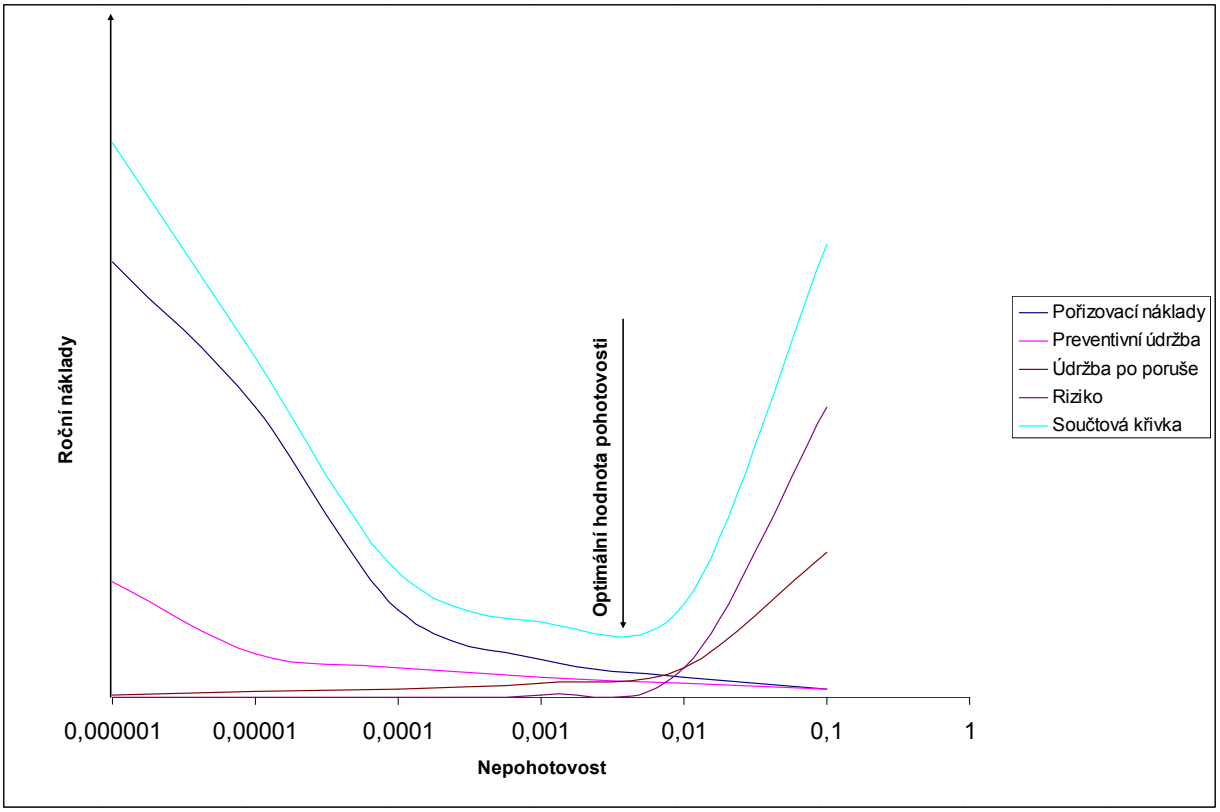
Další možností uplatnění předkládané disertační práce je plánování systému preventivních údržbářských zásahů a optimalizace nákladů životního cyklu (LCC) produktu, založené na více vstupních parametrech. Na základě výpočtu rizika, plynoucího z jednoho nefunkčního individuálního MK, je možné naplánovat 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.

6 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.

6.1 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. 6.



Obr. 6: 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.

$$RIZIKO = P \cdot C$$

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.

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 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 6.1, ve které jsou obecně uvedeny vztahy mezi náklady a přínosy z provozování průmyslových provozů.

Poznatky z teorie spolehlivosti 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] 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

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

[16] 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

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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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

Výběr z publikační činnosti autora:

Ročníkový projekt

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

Diplomová práce

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

Články na konferencích

[27] **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

[28] **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

[29] 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

[30] **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

[31] **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

[32] **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

[33] **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

[34] **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

[35] **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

[36] **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

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

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

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

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

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

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

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

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

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

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

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

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

[49] 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

Seznam použité literatury i vybraných publikací autora byl pro účely autoreferátu disertační práce omezen. Kompletní seznam použitých publikací je uveden v disertační práci.