AUTOREFERÁT
DISERTAČNÍ PRÁCE

Řídicí systémy se zvýšenou bezpečností

Ing. Luděk Elis

Plzeň, 2019

Autoreferát disertační práce

k získání akademického titulu doktor v oboru

Elektronika

Ing. Luděk Elis

Řídicí systémy se zvýšenou bezpečností

Školitel: Doc. Ing. Jiří skála, Ph.D.

Datum státní doktorské zkoušky: 20. 6. 2016

Abstrakt

Tato práce se zabývá funkční bezpečností elektronických řídicích systémů. V první části jsou popsány pojmy z oblasti bezpečnosti systémů obecně, dále jsou porovnány různé obory, ve kterých hraje požadavek bezpečnosti důležitou roli. V metodické části práce jsou teoreticky rozepsány jednotlivé kroky v procesu návrhu elektronického systému určeného pro aplikace vyžadující definovanou úroveň bezpečnosti se zaměřením na hardwarovou část. V této kapitole jsou podrobně vysvětleny jednotlivé požadavky pro usnadnění návrhu nebo přípravy systému pro možnost deklarace shody s požadavky normy ČSN EN 61508. V závěru práce je popsán rozbor příkladové aplikace od fáze konceptu a specifikace požadavků přes návrh až po konečné analýzy a hodnocení systému.

Klíčová slova

Řídicí systém, funkční bezpečnost, ČSN EN 61508, úroveň integrity bezpečnosti, spolehlivost, analýza rizika, míra přijatelného rizika, životní cyklus.

Abstract

This thesis deals with the function safety of electronic control system. The first part describes the terms of the system safety in general and presents the comparison of the various fields, in which the requirement of safety plays an important role. The design steps of an electronic system design are theoretically described in the methodological part of the thesis. The methodology is targeted for safety related applications focusing on the hardware part. This chapter explains in detail the individual requirements to facilitate the design or the system preparation for the possibility of declaring conformity with the requirements of the ČSN EN 61508 standard. At the end of the thesis the analysis of an example application is described from the concept stage and specification of requirements through design to final analysis and system evaluation.

Key words

Control system, function safety, ISO 61508, safety integrity level, reliability, risk analysis, tolerable hazard rates, life cycle.

Obsah

1 Úvod

Dnešní životní styl a potřeby současné společnosti kladou stále vyšší požadavky na vybavení a zařízení, která používáme v zaměstnání, doma nebo při samotné cestě do práce. Tento trend společně s ekonomickým hlediskem představuje motor, který pohání vývoj elektroniky kupředu, a stále připravuje prostor v oblastech, které nejsou plně automatizované, nebo kde již instalované technologie svým výkonem nedostačují. Ať už jde o nové funkce aktivních ochran automobilů, dokonalejší systémy pro stavbu vlakových cest, či modernější systémy řízení letového provozu, vždy to s sebou přináší nové přístupy a technologie. Ty samozřejmě nelze implementovat bez nutných vylepšení a modernizace stávajících systémů, jejichž jádrem se téměř bez výjimky stává mikroprocesorová elektronická řídicí jednotka (ECU – Electronic Control Unit). Moderní elektronické řídicí systémy sice přinášejí možnosti vykonávat nejrůznější funkce a náročné technologické procesy, zároveň však významným způsobem zvyšují složitost a komplexnost celého zařízení.

S navyšováním složitosti používaných technologií i rostoucími nároky na ně je nezbytné nezanedbávat nejdůležitější požadavek – bezpečnost. Vozidla, vlaky i letadla přepravují osoby rychleji a na větší vzdálenosti, vyrábíme i spotřebováváme mnohem více energie, používáme mnohem komplikovanější výrobní procesy. Proto je potřeba, aby vše fungovalo s co největší spolehlivostí a nedocházelo k nebezpečným situacím či dokonce haváriím.

U zařízení, jejichž funkcionalita již byla ověřena dlouhodobým provozem, může dojít v procesu modernizace ke změně dílčí, ale zásadní části. Tato inovace s sebou často přináší nová rizika, která je nutná kvůli zajištění bezpečnosti systému vždy důkladně zhodnotit. Zkoumání závažnosti těchto rizik by mohlo být snadné, pokud by byl systém průhledný a jeho jednotlivé funkce jednoduché. S takovýmto systémem se dnes ale téměř nesetkáme. Je tedy nutné se analýzou rizik podrobně zabývat a zajistit tak bezpečnost systému.

Dalším velkým problémem, s kterým se setkáváme při návrhu bezpečných systémů, je velmi omezený přístup k informacím. Tento fakt je dán velmi úzkou skupinou lidí, kteří se bezpečnosti věnují. Navíc je jen málo těch, kteří svoje poznatky publikují, jelikož jsou mnohdy vázáni podnikovým tajemstvím. Certifikovaná střediska sice poskytují školení, jejich cena je ale

v řádu desítek tisíc korun. Lze nalézt některé rozpracované části návrhu bezpečných systémů, často ale není dostupný celistvý popis pro celý proces návrhu. Ve většině případů jsou navíc odlišní autoři jednotlivých částí a proto i jejich návaznost je velmi malá. Často není použita ani stejná terminologie, čímž vznikají různá nepochopení a výklady z různých zdrojů jsou mezi sebou nesrozumitelné. Bohužel tento problém lze nalézt i v překladech norem do češtiny, mnohdy jsou zavádějící a nepoužívají jasnou terminologii.

Motivací vzniku práce bylo vytvoření interního pracovního postupu, který by byl ucelený a zároveň srozumitelný, s jehož pomocí by bylo možné bez časově náročného studování normy pochopit problematiku návrhu bezpečného systému splňujícího přísné požadavky na bezpečnost. Hlavním přínosem práce by měla být vzniklá metodika, v níž by obecné postupy byly transformovány do praktické roviny, a projektant ze složité struktury normy pochopil, jak má postupovat. Zároveň by měla být metodika otestována na praktickém příkladu, ve kterém postupy budou demonstrovat klíčové kroky procesu vývoje výrobku s požadavkem na bezpečnost. Metodika by měla vysvětlit vzájemnou provázanost mezi aktivitami, se kterými se lze setkat během životního cyklu vývoje výrobku. Navržené postupy budou použity při návrhu prototypu zařízení pro kompenzaci zemních poruch, který bude reálně nasazen do zkušebního provozu na rozvodnu společnosti ČEZ.

Pro tuto práci byly stanoveny následující dílčí cíle:

- zpracování problematiky návrhu systémů pracujících se stanovenou úrovní bezpečnosti s ohledem na základní požadavky normy ČSN EN 61508,
- sjednocení názvů, pojmů a používaných metod a analýz v oblasti funkční a technické bezpečnosti,
- vytvoření metodické příručky návrhu bezpečných systémů dle obecného standardu série normy ČSN EN 61508,
- modelová ukázka použití metodiky na praktickém příkladu.

Vznik studie této problematiky se také váže k řídicímu systému vyvíjeného v rámci projektu REMCS (RICE *Embeded Modular Control System*) výzkumného centra RICE Západočeské univerzity v Plzni. Projekt má za cíl navrhnout řídicí systém, který je určen pro bezpečné aplikace s požadavkem použití systémů souvisejících s bezpečností. V poslední kapitole této práce je uveden modelový příklad použití systému v reálné

aplikaci, pro kterou byla použita vytvořená metodika. Aplikace zahrnuje specifikaci požadavků, koncept, návrh a další nutné kroky s cílem deklarovat naplnění požadavků souvisejících norem.

2 Bezpečnost elektronických zařízení

Řídicí systémy jsou obecně tvořeny plně automatizovanými zařízeními, která jsou navržena ať už pro jednoduchá odvětví, nebo pro náročná průmyslová odvětví vyžadující vysokou spolehlivost a dlouhou dobu života. Bohužel spolehlivost nezaručuje bezpečnost a tyto pojmy nelze slučovat.

2.1 Obecná norma pro funkční bezpečnost

ISO 61508, potažmo ČSN EN 61508 [1], je mezinárodně uznávaná norma určená pro všechna odvětví průmyslu. Soulad s touto normou rovněž indikuje vysokou kvalitu komponentů i celků zaměřených na funkční bezpečnost. Na základech této normy vznikla řada dalších odvozených norem pro speciální použití (podle oborů a oblastí použití), ale bez velkých problémů může být použita i tam, kde specifické normy neexistují.

Norma se skládá ze sedmi dílů, kde první čtyři jsou normativní a další tři informativní. Zmíněné informativní díly poskytují doplňkové informace a představují návod na použití prvních čtyř dílů formou přehledů a příkladů. Soubor dílů normy ČSN EN 61508 má společný název *Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností*. Zkráceně se v názvu pro jednotlivé typy systémů používá zkratka E/E/PE.

2.2 Analýza rizik

Při aplikaci požadavků norem pro konkrétní zařízení je třeba správně chápat význam rizika a způsoby jeho hodnocení. Je třeba uváženě rozhodovat o přímé aplikaci příkladů hodnocení rizika uváděných v normách, především v informativních přílohách, protože jejich nesprávným použitím by mohlo dojít k podhodnocení, nebo nadhodnocení rizika a v důsledku toho k neefektivnímu řízení rizika.

Analýza rizika ve své podstatě představuje první krok při snižování rizika pomocí bezpečnostních systémů. Stanovuje rizika provozovaného zařízení, aby bylo dosaženo optimálního řešení. Pokud není riziko stanoveno korektně, může být bezpečnostní systém navržen buď s nadměrnou, nebo nedostatečnou odolností proti systematickým a náhodným poruchám. Z toho pak vyplývají příslušné bezpečnostní i ekonomické důsledky.

2.3 Funkční bezpečnost

Bezpečnost obecně znamená ochranu před úrazem elektrickým proudem, žárem a ohněm, nebezpečným zářením a nesprávnou funkcí. Pojem funkční bezpečnost poprvé zavedla norma ČSN EN 61508, v důsledku čehož je tento pojem nesprávně spojován pouze s elektronickými systémy.

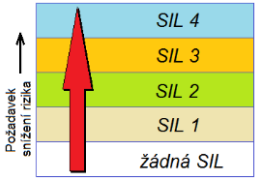
Požadavky na funkční bezpečnost stanovují takové funkce systému, které jsou z hlediska bezpečnosti relevantní a zároveň definují, za jakých podmínek smějí být konkrétní funkce vykonávány. Systém často obsahuje i funkce definované funkčními požadavky nebo základními technickými požadavky, ty však nejsou pro bezpečnost významné, a proto do funkční bezpečnosti nespadají.

2.4 Technická bezpečnost

Normy používané v oblasti bezpečnosti běžně pracují s *funkční bezpečností*, ovšem v obecnějším pojetí je nutné tento termín doplnit o pojem *technická bezpečnost*. Zatímco funkční bezpečnost se zabývá především chováním zařízení v bezporuchovém stavu, tj. stav, kdy zařízení vykonává předepsané a prověřené funkce tak, jak má, pojmem technická bezpečnost rozšiřuje požadavky o chování zařízení v poruchovém stavu. Požadavky na technickou bezpečnost stanovují, že v případě definované poruchy zařízení zaujme předem stanovený bezpečný stav.

2.5 Integrita bezpečnosti

Integrita bezpečnosti systému je podle definice normy ČSN EN 61508 pravděpodobnost, se kterou bude bezpečnostní systém uspokojivě plnit požadované bezpečnostní funkce za daných podmínek během stanovené doby. Vyjadřuje, jaké je tolerovatelné riziko – do jaké míry může být bezpečnostní funkce narušena vnějšími vlivy, omyly obsluhy nebo například poruchami vlastního zařízení.



Obrázek 1: Vztah úrovně SIL a požadavků na snížení rizika

Úroveň integrity bezpečnosti se podle ČSN EN 61508 dělí do čtyř kategorií (SIL 1 až SIL 4), kde SIL 1 znamená nejnižší úroveň a SIL 4 nejvyšší.

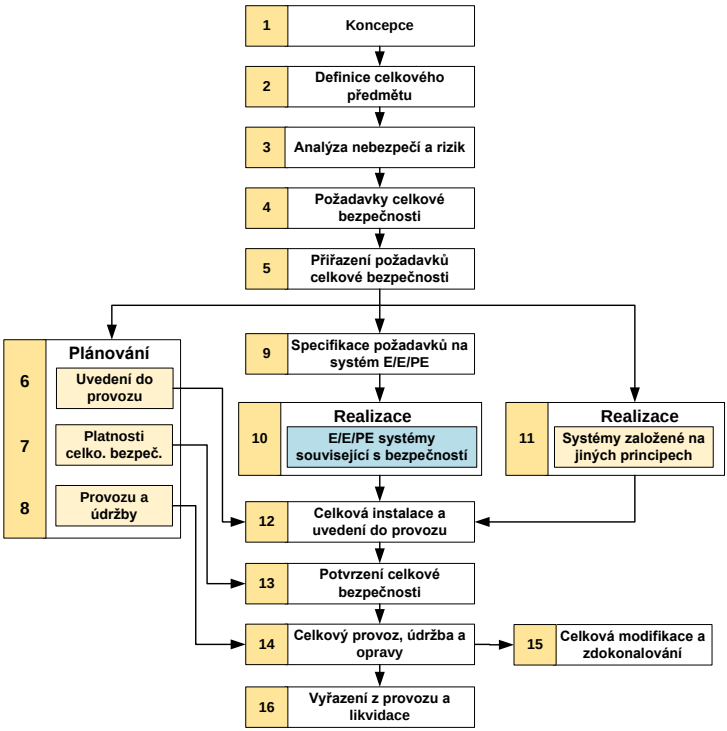
Kategorie SIL reprezentují výslednou pravděpodobnost výskytu nebezpečné poruchy pro jednotlivé bezpečnostní funkce. Čím je bezpečnostní funkce zařízení důležitější, tím je i vyšší požadavek na snížení rizika. Následně musí být i větší požadavek na systém neboli na jeho SIL.

3 Metodika návrhu systémů

Cílem této kapitoly je popsat jednotlivé kroky v procesu návrhu elektronického systému určeného pro aplikace vyžadující jistou úroveň bezpečnosti se zaměřením na hardwarovou část. Jelikož by tato vzniklá metodika měla být nápomocná pro obecný návrh elektronických systémů, je logicky jejím základem soubor norem ČSN EN 61508.

3.1 Životní cyklus celkové bezpečnosti

Různé aktivity a ochrany proti systematickým chybám, které jsou nezbytné pro dosažení bezpečnosti, se vyskytují v různých fázích návrhu a provozu každého zařízení. Proto vznikl nápad definovat (tj. popsat) životní cyklus zařízení, jehož mírně zjednodušený tvar zobrazuje obrázek 2.



Obrázek 2: Životní cyklus celkové bezpečnosti dle ČSN EN 61508

3.2 Koncept a definice systému

Koncept je prvním krokem životního cyklu bezpečnosti systému, jehož cílem je důkladné prozkoumání a pochopení celého navrhovaného (řídicího) systému - především však jeho prostředí, ve kterém by měl pracovat.

Druhým krokem životního cyklu je vymezení konkrétních částí, které budou předmětem analýz nebezpečí a rizik. Jak dobře je systém popsaný, tak dobře lze odpovídat na otázky, co se stane při vzniku poruchy a jaká rizika mohou následovat.

3.3 Analýza nebezpečí a rizik

Hlavním cílem správné aplikace funkční bezpečnosti je snížení rizika. K tomuto účelu se využívá různých metod analýzy rizika.

Mezi nejpoužívanější patří analýza FMEA (*Failure Mode and Effects Analysis*). FMEA je strukturovaná kvalitativní analýza, která slouží k identifikaci způsobů poruch systémů, jejich příčin a důsledků. Tato metoda má induktivní přístup – provádí kvalitativní analýzu od nižší k vyšší úrovni členění systému. Zkoumá, jakým způsobem mohou objekty na nižší úrovni selhat a jaký důsledek mohou mít tato selhání pro vyšší úrovně systému. [6] [19] [20] [21]

V praxi běžně není potřeba snižovat riziko až do okamžiku, kdy jej zcela odstraníme, jednak proto, že to není dobré využití zdrojů, ale také proto, že riziko ve svém důsledku ani zcela odstranit nelze. Na tomto principu je založena metoda ALARP (*As Low As Reasonably Practicable*) „co nejnižší rozumně dosažitelné riziko“. Tato metoda tedy respektuje snahu dosažení co nejnižšího rizika, avšak s ohledem na náklady spojené s tímto úsilím. Základní koncepce metody ALARP je založena na rozdělení rizika do tří oblastí. [22]

Kvalitativní metoda využívající grafu rizik je jednou z dalších metod, kterou lze využít pro stanovení míry integrity bezpečnosti. Metoda zavádí čtyři rizikové parametry charakterizující základní vlastnosti nebezpečné situace v případě selhání, nebo nedostupnosti systémů souvisejících s bezpečností.

3.4 Požadavky celkové bezpečnosti a jejich přiřazení

Konkrétní rizika a nebezpečné události určené rizikovou analýzou jsou v této fázi převedeny do konkrétní podoby. Pro jednotlivé bezpečnostní funkce se musí určit cílové požadavky na integritu bezpečnosti, které budou splňovat výslednou hodnotu tolerovatelného rizika. Pokud je hodnota rizika EUC příliš vysoká, je potřeba ji snížit. Jsou dvě možnosti, jak riziko snížit a splnit požadavky celkové integrity bezpečnosti tak, aby se dosáhlo tolerovatelného rizika:

- snížením dopadů nebezpečných událostí, nebo
- snížením četnosti nebezpečných událostí EUC a řídicího systému EUC.

Bezpečnostní funkce jsou následně přiřazeny navrhovaným systémům souvisejícím s bezpečností. Hlavním cílem přiřazení požadavků je přiřazení úrovně integrity ke každé bezpečnostní funkci, pokud tak již nebylo učiněno v předchozím kroku společně s analýzou nebezpečí a rizik. Pro dosažení požadované úrovně funkční bezpečnosti je většinou nutné snížení rizika, kterého je možné dosáhnout:

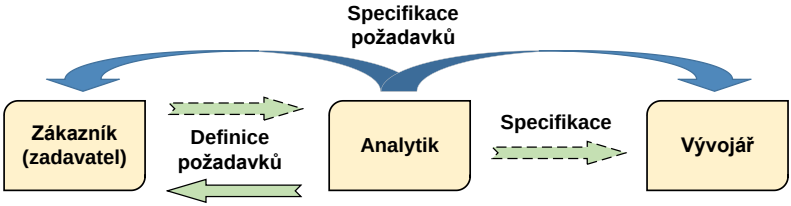
- Pomocí E/E/PE systémů souvisejících s bezpečností.
- Pomocí vnějších prostředků pro snížení rizika.
- Pomocí jiných opatření snižujících riziko.

3.5 Plánování

Plánování instalace, potvrzení celkové bezpečnosti, plánování celkového provozu, údržby a oprav jsou činnosti, které mají přímý vliv na celkový návrh systémů souvisejících s bezpečností, avšak musí být prováděny zcela odděleně od realizace systémů souvisejících s bezpečností. Oddělení je důležitým předpokladem pro eliminaci systematických chyb a zvyšuje robustnost celého plánování životního cyklu.

3.6 Specifikace požadavků na systém

Specifikace požadavků předchází samotnému návrhu a realizaci. Obecně specifikace spojuje jednotlivé články: zákazník – analytik – vývojář.

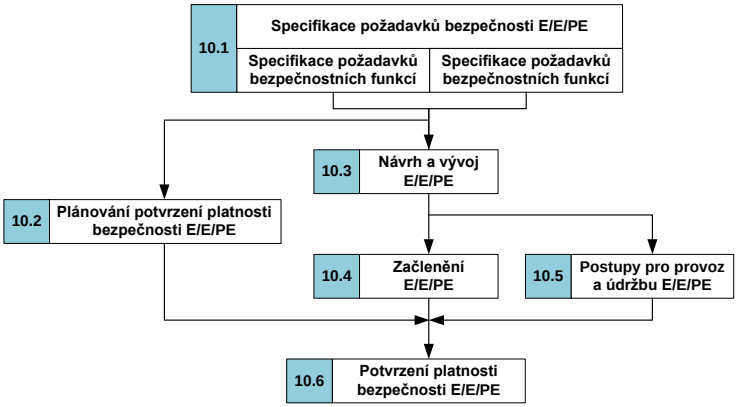


Obrázek 3: Souvislost rolí při specifikaci požadavků.

Specifikace požadavků je souhrnným předpisem pro vývojové pracovníky, kteří ji mohou použít pro výběr zařízení / architektury, návrh a realizaci. Specifikace požadavků neurčuje, jak se má systém navrhnout, ale určuje, co má systém dělat. Musí jasně definovat požadavky na integritu bezpečnosti a požadavky bezpečnostních funkcí, aby se zajistilo dosažení požadované funkční bezpečnosti.

3.7 Realizace systému souvisejícího s bezpečností

Kapitola realizace pojednává o návrhu a vývoji systému E/E/PE dle specifikace tak, aby se splnily požadavky s ohledem na požadované bezpečnostní funkce a požadavky integrity bezpečnosti dle specifikace z předchozího kroku. Realizace E/E/PE systému souvisejícího s bezpečností by měla probíhat podle normativně předepsaných kroků, které tvoří životní cyklus realizace E/E/PE systému. Jedná se o určitý subsystém životního cyklu celkové bezpečnosti (viz obrázek 2), který by měl mít podobu zobrazenou na obrázku 4 pro hardware.



Obrázek 4: Životní cyklus bezpečnosti systému E/E/PE souvisejícího s bezpečností – hardware.

Fáze návrhu a vývoje je prováděna souběžně s plánováním potvrzení platnosti bezpečnosti. Návrh a vývoj systému je v rukou vývojáře, který musí mít k dispozici přehled všech požadavků na hardware i software související s bezpečností – specifikaci požadavků. Vývojář je zodpovědný za tuto fázi životního cyklu, což dokládá dokumentací návrhu systému, ve které musí zdůvodnit techniky a opatření vybrané pro sestavení uceleného souboru splňujícího požadovanou úroveň integrity bezpečnosti.

3.8 Celková instalace a uvedení do provozu

Ve fázi instalace a následně i uvádění do provozu je důležité zajistit, aby se vzaly v úvahu interakce mezi (všemi) E/E/PE systémy souvisejícími s bezpečností a jinými opatřeními pro snížení rizika. Během instalace / uvádění do provozu jsou prováděny činnosti stanovené podle plánu. Všechny jednotlivé činnosti musí být dokumentovány, především případy, ve kterých byly řešeny poruchy a nekompatibility.

3.9 Potvrzení celkové bezpečnosti

Potvrzení celkové bezpečnosti probíhá podle plánu sestaveného v 7. fázi ŽC, který zohledňuje požadavky bezpečnostních funkcí a požadavky na integritu bezpečnosti definovaných ve specifikaci požadavků návrhu systému. Je nutné v potvrzení celkové bezpečnosti zohlednit interakce mezi E/E/PE systémy souvisejícími s bezpečností, jinými opatřeními pro snížení rizika a

systémy s bezpečností nesouvisejícími. Součástí ověření mohou být i měření kalibrovanými měřicími přístroji. Výstupem potvrzení celkové bezpečnosti je dokumentace výsledků zkoušek platnosti bezpečnosti.

3.10 Provoz, údržba a opravy

Celkový provoz, údržba a opravy představují nutné činnosti na udržení požadované funkční bezpečnosti definované plánem. V rámci činností musí být specifikovány technické požadavky nezbytné pro celkový provoz, údržbu i opravy E/E/PE systémů souvisejících s bezpečností. Tyto požadavky musí být poskytnuty odpovědným osobám za budoucí provoz a údržbu. Provozní a údržbové práce se musí provádět dle sestavených postupů a chronologicky dokumentovat.

3.11 Modifikace a zdokonalování

Opravy, rozšíření nebo přizpůsobení jsou modifikace systému, u kterých je nutné zaručit přijatelnou hodnotu funkční bezpečnosti v průběhu jejich realizace i po jejich ukončení. Před provedením jakékoliv modifikace je nutné naplánovat všechny nutné činnosti zahrnující například analýzu dopadů na E/E/PE systém, přičemž je nutné vzít v úvahu i možnosti ovlivnění jiných E/E/PE systémů, které nejsou přímo modifikovány / zdokonalovány.

Každá modifikace musí iniciovat návrat k příslušné fázi životního cyklu celkové bezpečnosti. Všechny modifikace ovlivňující funkční bezpečnost E/E/PE musí být podrobně zdokumentovány.

3.12 Vyřazení z provozu a likvidace

Poslední fází ŽC je vyřazení systému z provozu a jeho následná likvidace. I zde platí požadavky funkční bezpečnosti. Kroky v rámci této fáze jsou obdobné jako v případě provozu, údržby a oprav nebo modifikace. Patří mezi ně zejména provedení analýzy dopadů jakékoliv činnosti spojené s vyřazením z provozu. Zahájení jednotlivých činnost uvedených v postupu vyřazení z provozu je možné až po vydání oprávněné žádosti v souladu s managementem funkční bezpečnosti.

4 Aplikace metodiky pro návrh systému kompenzace zemních spojení

Na praktickém příkladu je snahou demonstrovat implementaci příslušných norem a poznatků z oblasti návrhu bezpečných systémů pro reálný systém nasazený pro konkrétní aplikaci. Jedním z velkých projektů, u kterého byla snaha aplikovat normy v maximální míře, je například univerzální řídicí systém REMCS (*RICE Embedded Modular Control System*). Tento systém, který byl vyvíjen zkušenými techniky, disponuje velkým množstvím bezpečnostních technických prvků. Při návrhu tohoto systému byl kladen velký důraz na splnění požadavků vybraných norem i na provádění řady procesních kroků (revize a jejich dokumentace, testy dílčích částí atd.) dle interních směrnic, nicméně se proces návrhu setkal s některými nedostatky (např. nedodržení posloupnosti kroků životního cyklu nebo odlišně cílená struktura projektové dokumentace). S nabývajícími zkušenostmi v této oblasti bylo přistoupeno ke změnám v návrhu a v rámci těchto činností i k postupné korekci zjištěných nedostatků.

Snahou této práce je tedy mimo jiné i objasnění nedostatků a aplikace všech získaných poznatků do návrhu nových verzí systému REMCS a to ve všech směrech procesu vývoje – především pak v oblasti technických opatření, ve stylu tvorby průvodní dokumentace nebo dodržení souslednosti jednotlivých procesních kroků.

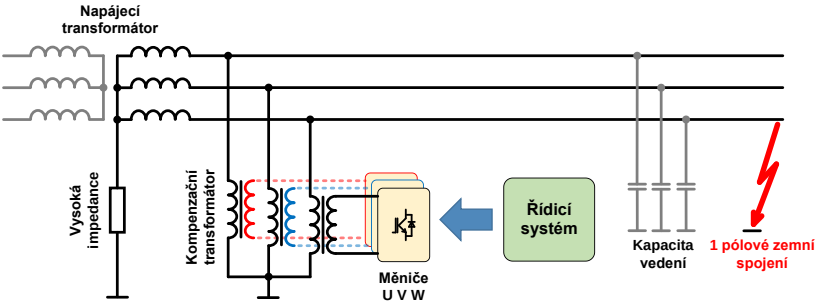
4.1 Vývojový proces na Západočeské univerzitě

Z hlediska návrhu systémů souvisejících s bezpečností je nutné postupovat podle životního cyklu příslušných norem. RICE FEL ZČU má kompletní směrnici, která implementuje celý proces vývoje výrobku již od roku 2016. Snahou směrnice je implementovat všechny kroky procesu, které umožní vývojovým centrům Západočeské univerzity vyvíjet ve spolupráci s průmyslovými partnery náročnější zařízení.

4.2 Koncepce a definice systému

Předmětem analýzy je systém REMCS, který je použitý jako řídicí systém v Zařízení pro kompenzaci zemních poruch na vedení vysokého napětí. Zařízení je založeno na řízeném zdroji proudu (výkonový měnič), který přes

kompenzační transformátor injektáží proudu do soustavy kompenzuje poruchové proudy a tím nahrazuje zhášecí tlumivku zapojenou mezi uzel transformátoru a zemnící soustavu rozvodny. Podrobnější vysvětlení principu kompenzace zemních poruch použitím výkonového měniče lze nalézt v [32].



Obrázek 5: Zjednodušené schematické znázornění připojení kompenzačního zařízení k rozvodné soustavě se znázorněnou 1pólovou poruchou.

Pasivní část Zařízení tvoří již zmíněný kompenzační transformátor. Jedná se o speciální třífázový transformátor 22 / 0,4 kV o výkonu 1,35 MVA, který je navržen pro připojení k fázovým vodičům distribuční sítě. Níže uvedený popis jednotlivých částí Zařízení vychází z [33].

Aktivní část Zařízení je tvořena výkonovým polovodičovým měničem a řídicím systémem REMCS. Celkového instalovaného výkonu výkonového měniče 1,35 MVA bylo dosaženo složením devíti modulárních bloků, které jsou vzájemně propojeny jediným stejnosměrným obvodem o napětí 700 V.

Klíčovou komponentou aktivní části Zařízení je řídicí systém REMCS zajišťující vedle samotného řízení také bezpečnostní ochrany, komunikaci, monitoring a sběr dat. Řídicí systém je vybaven několika řídícími kartami, což umožňuje distribuci řídících a monitorovacích úloh a paralelizaci procesů. Jelikož nelze nezávisle rozdělit systém na část nesouvisející od části související s bezpečností, musí být systém zahrnut do ŽC bezpečnosti jako celek.

4.3 Analýza nebezpečí a rizik

Analýzou byla odhalena rizika, která mohou vést k nebezpečné situaci. Celkem bylo identifikováno 26 rizik včetně určení jejich příčiny a konečného

důsledku. Výčet těchto rizik, jejich pravděpodobnou příčinu i důsledek uvádí tabulka 1.

Tabulka 1: Výčet rizik modelu

č.	Příčina	Riziko	Důsledek
1	Chyba v řídicím programu	Přepětí transformátoru / výkonových prvků	Poškození izolace transformátoru, poškození měniče, úraz
2	Chyba v řídicím programu	Nadproud transformátoru / výkonových prvků	Poškození vinutí transformátoru, poškození měniče, úraz
3	Výpadek napájení	Neočekávané vypnutí celého systému	Možné poškození výkonových částí zařízení
4	Normální provoz	Zahřátí výkonových prvků	Poškození měniče
5	Normální provoz	Zahřátí transformátoru	Poškození transformátoru
6	Neoprávněné / nechtěné otevření krytu Zařízení	Kontakt s živými částmi Zařízení	Úraz, trvalé poškození zdraví, smrt
7	Poškození elektroinstalace	Zkrat řídicích, kontrolních nebo měřících signálů	Těžké ublížení na zdraví až smrt, poškození zařízení
8	Poškození elektroinstalace	Rozpojení řídicích, kontrolních nebo měřících signálů	Těžké ublížení na zdraví až smrt, poškození zařízení
9	Porucha chlazení měniče	Přehřátí výkonových prvků	Poškození měniče
10	Neprůchodnost chladících otvorů	Přehřátí výkonových prvků	Poškození měniče
11	Přepětí ze strany sítě	Přepětí na transformátoru	Poškození izolace transformátoru, poškození měniče

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

12	Poškození izolace transformátoru	Zkrat na vinutí transformátoru	Poškození transformátoru
13	Porucha vinutí jedné fáze transformátoru	Nesprávné napětí jedné fáze	Špatná kompenzace, možnost poškození měniče
14	Porucha výkonového prvku měniče	Poškození měniče jedné fáze	Špatná kompenzace
15	Porucha měniče chopperu	Přepětí v meziobvodu	Poškození měniče
16	Porucha driveru výkonového měniče jedné fáze	Nesprávné řízení fázového měniče	Poškození měniče
17	Porucha řízení jedné fáze	Nesprávné řízení fázového měniče	Poškození měniče
18	Selhání / porucha průmyslového PC	Provoz bez vzdáleného přístupu, ztráta logování dlouhodobých dat	Provoz v autonomním režimu bez možnosti vzdáleného řízení, ztráta dat
19	Výpadek vzdálené komunikace	Provoz bez vzdáleného přístupu	Provoz v autonomním režimu bez možnosti vzdáleného monitorování / řízení
20	Výpadek vnitřní komunikace	Neřiditelné celé zařízení	Odstavení celého zařízení
21	Porucha / zarušení čidla teploty výkonového měniče	Přehřátí výkonových prvků	Poškození měniče
22	Porucha / zarušení čidla proudu	Špatná regulace, nekontrolovaná velikost proudu	Možné poškození výkonových měničů a kompenzačního transformátoru

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

23	Porucha / zarušení čidla napětí	Špatná regulace, nekontrolovaná velikost napětí	Možné poškození výkonových měničů a kompenzačního transformátoru
24	Porucha stykače pro odpojení výkonového měniče jedné fáze	Trvalé sepnutí stykače	Možné poškození výkonových měničů a kompenzačního transformátoru, úraz, poškození zdraví
25	Porucha stykače pro odpojení výkonového měniče jedné fáze	Trvalé rozpojení stykače	Není možná kompenzace sítě
26	Porucha kontrolky na panelu zařízení	Ztráta informace o stavu zařízení vizuální kontrolou	Úraz, trvalé poškození zdraví, smrt

Pro ohodnocení jednotlivých rizik spojených s provozem Zařízení pro kompenzaci zemních poruch je využito metody ALARP. Přesná specifikace parametrů *následek* a *četnost* byla určena potřebám zvolené aplikace. Rozdělení rizika pro identifikovaná rizika do kategorií na nepřijatelné, ALARP a přijatelné riziko uvádí tabulka 2.

Tabulka 2: Rozdělení rizik do kategorií

Oblast	Číslo rizika
Nepřijatelné riziko	6, 10
ALARP	1, 2, 3, 4, 6, 8, 9, 10, 11, 14, 15, 16, 17, 20, 21, 22, 23, 26
Přijatelné riziko	12, 13, 18, 19, 24, 25

Z tabulky 2 je vidět, že některá rizika se vyskytují v oblasti nepřijatelného rizika nebo v oblasti ALARP. Pro tato rizika je nutné navrhnout bezpečnostní opatření snižující jejich četnost nebo následek. Navržené metody a způsoby pro snížení rizik uvádí tabulka 3.

Tabulka 3: Navržená opatření pro snížení rizik

ID	Ovlivněné riziko	Opatření	Snížení
I	6	Koncové spínače dveří rozvaděče	Četnosti
II	3	Záložní zdroj energie	Četnosti
III	4, 5, 7, 8, 9, 11, 13, 14, 16, 17, 20	Celkové vypnutí Zařízení	Četnosti
IV	1, 2	Predikční algoritmus	Následku
V	10	Pravidelná kontrola větracích otvorů	Četnosti
VI	11	Bleskojistky a varistory na přívodu	Následku
VII	13, 14, 16, 17, 22, 23	Křížová kontrola proudů a napětí mezi fázemi	Následku
VIII	20	Odesílání paketů s časovou značkou	Četnosti
IX	21	Kontrola teplot výkonových prvků mezi fázemi	Následku

Použitím uvedených bezpečnostních opatření se všechny rizikové události přesunuly do oblasti přijatelného rizika, případně do oblasti, kde je vyžadován princip ALARP. Důležitým aspektem je absence rizikových událostí v oblasti nepřijatelného rizika.

Pro určení požadované úrovně integrity bezpečnosti bylo využito metody grafu rizik, ve které byly hodnoty jednotlivých parametrů *C, F, P* a *W* určeny na základě subjektivního hodnocení. Odpovídající úroveň integrity bezpečnosti je následně určena vložením parametrů do grafu rizik. Výsledky provedené analýzy jsou uvedeny v tabulce 4.

Tabulka 4: Určení výsledné úrovně SIL pro jednotlivá rizika

č.	Riziko	C	F	P	W	SIL
1	Přepětí transformátoru / výkonových prvků	C_1	-	-	W_2	-
2	Nadproud transformátoru / výkonových prvků	C_1	-	-	W_2	-
3	Neočekávané vypnutí celého systému	C_1	-	-	W_2	-
4	Zahřátí výkonových prvků	C_1	-	-	W_2	-
5	Zahřátí transformátoru	C_1	-	-	W_2	-
6	Kontakt s živými částmi Zařízení	C_2	F_2	P_2	W_2	SIL2
7	Zkrat řídicích, kontrolních nebo měřících signálů	C_2	F_1	P_1	W_1	-
8	Rozpojení řídicích, kontrolních nebo měřících signálů	C_2	F_1	P_1	W_1	-
9	Přehřátí výkonových prvků	C_1	-	-	W_1	-
10	Přehřátí výkonových prvků	C_1	-	-	W_3	a
11	Přepětí na transformátoru	C_2	F_1	P_1	W_2	a
13	Nesprávné napětí jedné fáze	C_1	-	-	W_1	-
14	Poškození měniče jedné fáze	C_1	-	-	W_1	-
16	Porucha driveru - Nesprávné řízení fázového měniče	C_1	-	-	W_1	-
17	Porucha řízení jedné fáze - Nesprávné řízení fázového měniče	C_1	-	-	W_2	-
20	Neřiditelné celé zařízení	C_2	F_2	P_1	W_1	a

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

21	Přehřátí výkonových prvků	C_1	-	-	W_1	-
22	Špatná regulace, nekontrolovaná velikost proudu	C_1	-	-	W_1	-
23	Špatná regulace, nekontrolovaná velikost napětí	C_1	-	-	W_1	-

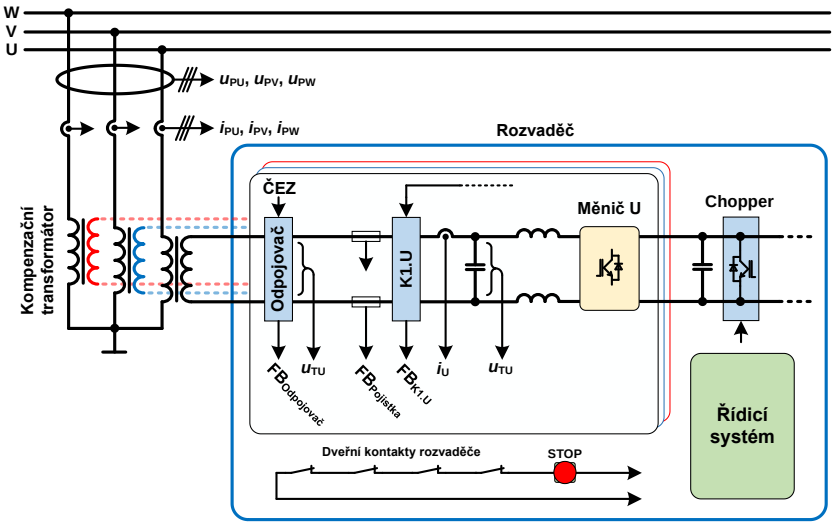
Výsledky analýzy zobrazené v tabulce 4**Chyba! Nenalezen zdroj odkazů.** uvádějí jeden požadavek na splnění integrity bezpečnosti v úrovni SIL2. Jedná se o riziko kontaktu s živými částmi Zařízení spojené s neoprávněným nebo nechtěným otevřením krytu v době, kdy je Zařízení spuštěno. Takové riziko musí být zajištěno, a proto je v následujících kapitolách věnována pozornost právě tomuto riziku.

Pro ošetření ostatních rizik není požadováno použití prvků splňujících požadavky funkční bezpečnosti a lze využít jiných opatření, například pomocí metod a prvků uvedených v tabulce 3.

Specifikace požadavků na bezpečnostní funkci bude zaměřena na ošetření rizika č. 6. Není ale vyloučeno, aby navržená bezpečnostní funkce svým rozsahem pokrývala i jiná rizika. Výsledné ohodnocení jednotlivých rizik s jediným požadavkem na úroveň zabezpečení (SIL 2) je dáno hlavně provozem bez obsluhy a tím i velmi malým rizikem, které vzniká pouze při servisních a údržbových činnostech.

4.4 Specifikace požadavků

Koncepční rozmístění základních částí celého Zařízení již bylo uvedeno na obrázku 5. Obrázek 6 rozkresluje uspořádání klíčových částí Zařízení z pohledu implementace bezpečnostních funkcí.



Obrázek 6: Základní části Zařízení pro kompenzaci.

Kompenzační transformátor je připojen k fázovým vodičům distribuční sítě a slouží jako rozhraní mezi přenosovou sítí a dalšími prvky Zařízení pro kompenzaci.

Odpojovač vývodu je řízen distributorem sítě a zajišťuje připojení Zařízení pro kompenzaci k distribuční síti. Řídicí systém není schopen ovládat odpojovač vývodu a má pouze informaci v podobě pomocného kontaktu o stavu připojení / odpojení. Pomocí tohoto odpojovače je distributor sítě schopen odpojit celé Zařízení od distribuční sítě.

Pojistka chrání Zařízení proti nadproudu v případě, kdy elektronika nebude schopná obvod ochránit. Přehoření pojistky je signalizováno pomocným kontaktem.

Stykač K1 má obdobnou funkci jako odpojovač vývodu, tedy připojení Zařízení pro kompenzaci k distribuční síti. Je ale řízen v rámci řídicího systému Zařízení pro kompenzaci. Stejně jako u odpojovače vývodu má systém zpětnou informaci o stavu (připojeno / odpojeno). Cívka stykače K1 je propojena přes tzv. zelenou linku (smyčka dveřních kontaktů a STOP tlačítka ve schématu na obrázku 6). Přerušením linky kterýmkoli dveřním kontaktem, kartou nebo STOP tlačítkem dojde k přerušení obvodu a tím odpadnutí stykače K1.

Výkonový měnič je jednofázový napěťový střídač v můstkovém zapojení, který napájí jedno ze tří oddělených sekundárních vinutí kompenzačního transformátoru.

Chopper je konstruován obdobně jako výkonový měnič. Je zapojen v můstkovém zapojení a jeho spínáním je schopen řízeně vybíjet energii v meziobvodu měničů do výkonového odporníku.

Řídicí systém je mozkem celého Zařízení pro kompenzaci a jeho úkolem je řídit jednotlivé měniče, měřit relevantní veličiny, provádět diagnostiku a především zajišťovat bezpečnostní funkci určenou analýzou rizika.

Čidla měří potřebná napětí, proudy, teploty a další veličiny potřebné pro zajištění bezpečného provozu Zařízení.

Dveřní kontakty rozvaděče jsou propojeny průchozí linkou zabezpečující detekci otevření kterýchkoli dveří rozvaděče. Do této linky bude pro zvýšení bezpečnosti přidáno tlačítko nouzového vypnutí STOP.

4.5 Bezpečnostní funkce

Z výsledků rizikové analýzy je patrné, že je nutné Zařízení zajistit před rizikem úrazu elektrickým proudem v době, kdy je Zařízení v činnosti (viz riziko č. 6). Z toho důvodu musí být všechny elektricky nebezpečné části uvnitř rozvaděče chráněné před nebezpečným dotykem a případné otevření jakýchkoli dveří musí zajistit vypnutí Zařízení. Na základě těchto požadavků byla definována bezpečnostní funkce:

Bezpečné vypnutí celého zařízení v případě neočekávaného otevření dveří rozvaděče nebo v případě detekce nebezpečné poruchy.

4.6 Návrh a realizace systému

V této kapitole jsou zohledněny všechny požadavky specifikované v předchozí kapitole a převedeny do technického řešení. To představuje např. rozvržení bezpečnostní funkce mezi hardware a software, rozdělení do funkčních bloků, definice rozhraní, stanovení konkrétních signálů apod.

Jak bylo v úvodu zmíněno, pro řízení bude použito modulárního systému REMCS.

4.6.1 Řídicí systém REMCS

Tento systém je určen především pro řízení výkonových real-time aplikací v oblasti energetiky a dopravní techniky vyžadujících zvýšené požadavky na

bezpečnost. Systém vznikl v Regionálním inovačním centru elektrotechniky (RICE), novém výzkumném centru Fakulty elektrotechnické Západočeské univerzity v Plzni.

Obrázek 7: REMCS – 19“rack systém pro 19 karet [13]

Univerzální řídicí systém tvoří skupina zásuvných modulů a propojovací část (backplane), které je možné podle potřeb zákazníka sestavit do požadované konfigurace. Zásadní výhodou této koncepce je vyšší flexibilita a modularita, která je vhodná pro nízký objem výroby.

Systém je navržen se zvýšenou HW bezpečností. Každá z klíčových komponent systému (zdroje, oscilátory, mikrokontrolér, FPGA aj.) podléhá trvalému monitorování čistě hardwarovými obvody. Selhání jakékoli komponenty automaticky vede k definovanému uvedení výstupů systému do bezpečného stavu (nezávisle na činnosti softwaru nebo FPGA).

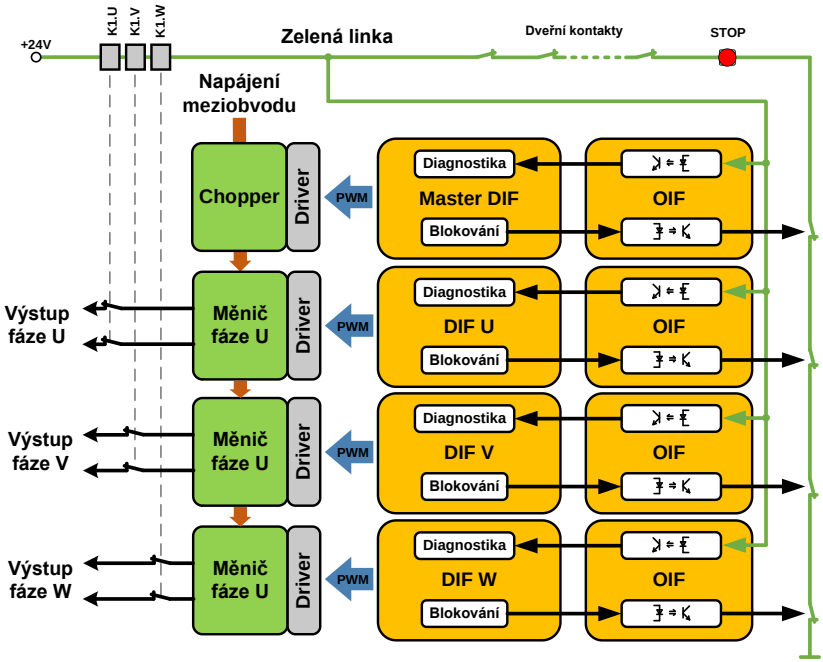
4.6.2 Struktura řídicího systému

Základní struktura řídicího systému je tvořena třemi samostatnými kartami DIF, nad kterými má správu tzv. *Master DIF*. Ke každé fázi je přidružena jedna rozšiřující karta OIF. Karta OIF je v této konfiguraci použita pouze jako HW rozšíření DIF karty o další signálové vstupy a výstupy galvanicky oddělené.

Z podstaty funkce třífázového měniče lze předvídat chování jednotlivých fází a jejich vzájemné ovlivňování. Na základě měření proudů a napětí jednotlivých fází, celkového proudu, napětí, teplot a dalších veličin je možné detekovat případné nesoulady mezi jednotlivými fázemi. Přestože jsou měniče jednotlivých fází řízeny vždy jedinou kartou DIF (jednokanálový systém bez redundance), je každá fáze nepřímo monitorována kartami

zbývajících fází. Porucha jedné fáze tak může být detekována kteroukoli ze tří karet, z nichž každá může aktivovat bezpečnostní funkci.

Bezpečnostní funkce vypnutí celého Zařízení realizovaná rozpojením K1, blokováním PWM výstupních signálů a vybitím meziobvodu pomocí chopperu je vidět na obrázku 8.



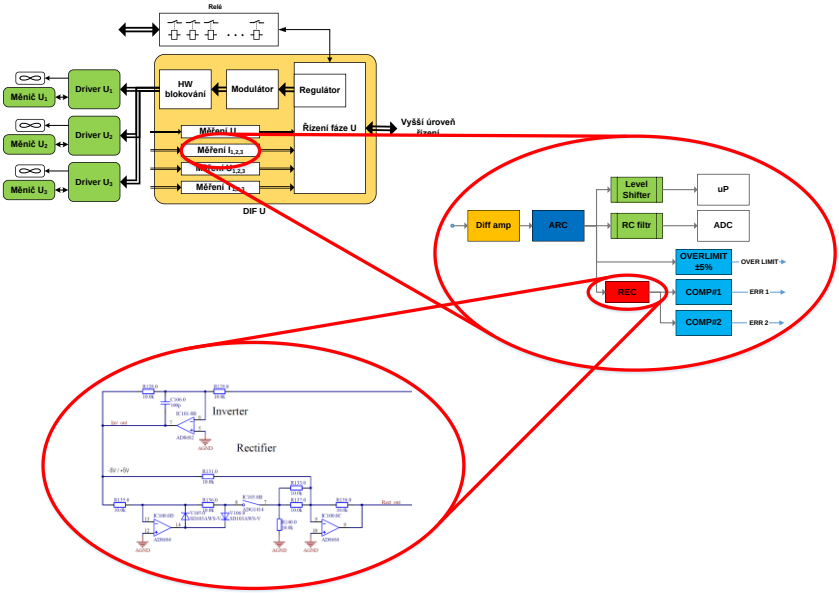
Obrázek 8: Struktura blokování bezpečnostní funkce

Zde je patrná tzv. Zelená linka, jejíž základ tvoří jeden okruh, na kterém jsou zapojeny ovládací cívky jednotlivých stykačů K1 (U, V, W). Přerušení linky zajistí rozpojení všech K1, čímž dojde k odpojení měničů od jednotlivých fází kompenzačního transformátoru. Zelenou linku může přerušit kterákoli karta, dveřní kontakt nebo bezpečnostní STOP tlačítko. Přerušení linky je detekováno všemi kartami. Pro zjednodušení je na obrázku 8 zakresleno napájení ovládacích cívek stykačů K1 jednotlivých fází pouze jedno společné. Ve skutečnosti jsou pro ovládání cívek stykačů K1 použity další pomocné stykače K3 a K6 s ovládacím napětím +24 V. Stykač K6 je ovládaný Zelenou linkou a fázové stykače K3 jsou spínané samostatně pomocí příslušné fáze rozšiřující kartou OIF. Pro sepnutí K1 musí být

sepnuty stykače K6 (nepřerušená Zelená linka) a stykače K3 (aktivní výstupní signály řídicího systému pro všechny fáze).

4.7 Potvrzení bezpečnosti

Bylo provedeno několik dílčích analýz FMECA pro identifikaci způsobů kritických selhání a tvorbu odezvy na potenciální poruchy jednotlivých částí Zařízení. Rozdělení jednotlivých analýz vychází z blokového schématu Zařízení. Výsledky analýz identifikují ideálně všechny možné poruchy, jejich příčiny a hodnotí jejich důsledek s odkazem na vhodná opatření.



Obrázek 9: Rozdělení Řídicího systému podle funkčních bloků do několika úrovní (příkladová část)

Následně byl řídicí systém REMCS pro účely použití v bezpečných aplikacích analyzován odhadem náhodných poruch na úrovni součástek. Systém byl rozdělen podle funkčních bloků na menší části do několika úrovní – od kompletních systémových bloků až po nejnižší úroveň elementárních bloků složených z několika málo prvků jak naznačuje obrázek 9.

Pro odhad intenzity náhodných hardwarových poruch na nejnižší úrovni elementárních bloků systému byla použita metoda počítání z prvků (*Parts*

Count). Tato metoda byla vybrána s ohledem na absenci specifických dat z provozu systému a jeho částí. Metoda počítání z prvků je ze své podstaty metodou silně konzervativní, a tudíž vhodnou pro prvotní určení intenzity náhodných poruch způsobených selháním hardwaru ve fázi vývoje a testování.

Pro jednotlivé elementární bloky systému analyzované metodou Parts Count byly následně definovány jejich módy selhání a určeny jejich dopady na výstup včetně možnosti detekce selhání. Takto byly sestaveny tabulky rozložení intenzit poruch pro karty DIF a OIF. Pro obě byly určeny hodnoty poměru bezpečných poruch SFF dle vztahu (4.1).

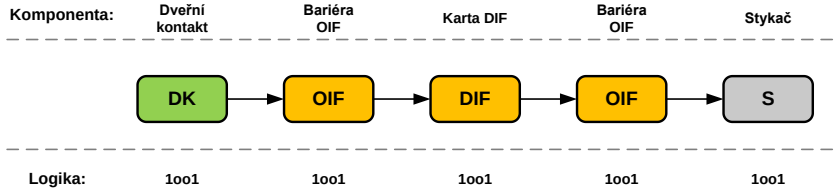
$$SFF = \frac{\lambda_S + \lambda_{Dd}}{\lambda_S + \lambda_{Dd} + \lambda_{Du}} \tag{4.1}$$

$$SFF_{DIF} = \frac{299 + 1457{,}7}{299 + 1457{,}7 + 172{,}6} = 91{,}1\% \tag{4.2}$$

$$SFF_{OIF} = \frac{59{,}5 + 446{,}5}{59{,}5 + 446{,}5 + 45{,}1} = 91{,}8\% \tag{4.3}$$

Ověření maximální úrovně integrity bezpečnosti je pro obě karty určeno pomocí tabulky 3 normy ČSN EN 61508-2. Zařízení spadá do kategorie B, jelikož není k dispozici dostatek spolehlivých dat o poruše ze zkušeností z provozu a nelze tak úplně určit chování při podmínkách poruchy. Obě katy mají SFF větší než 90 %, čímž splňují požadavek omezení integrity bezpečnosti úrovně SIL 2 pro systémy s nulovou odolností proti vadám hardwaru.

Jak již bylo zmíněno, na systém lze nahlížet jako na tři samostatné jednokanálové systémy vykonávající stejnou bezpečnostní funkci paralelně viz obrázek 8. Výslednou podobu jednoho kanálu rozdělenou na pět subsystémů ukazuje obrázek 10.



Obrázek 10: Schéma jednoho kanálu bezpečnostní funkce

Karty DIF a OIF mají architekturu 1oo1 pro kterou je pravděpodobnost selhání za hodinu PFH_i dle [1] dána vztahem:

$$PFH_i = 2 \cdot \lambda_{DU} \tag{4.4}$$

Pro výpočet bezporuchovosti komponent, jejichž mechanismus degradace je dán počtem sepnutí (komponenty, typu spínačů, relé, stykačů apod.), se uplatňuje znalost počtu pracovních cyklů, kterým je počet sepnutí. Pro přepočet počtu sepnutí na intenzitu poruch lze využít vhodné postupy uvedené v příslušných normách, např. pomocí hodnoty B_{10} a poměru nebezpečných poruch RDF (*Ratio of Dangerous Failure*). Hodnota B_{10} udává dobu nebo počet sepnutí, při kterém dojde k poruše 10 % zkoušených prvků a RDF udává procentuální rozdělení nebezpečných poruch. Pokud výrobce neudává přímo hodnotu B_{10d} odpovídající době nebo počtu sepnutí, při kterém dojde k nebezpečné poruše 10 % zkoušených prvků, lze ji vypočítat ze vztahu:

$$B_{10d} = \frac{B_{10}}{RDF} \tag{4.5}$$

Podle ČSN EN 62061 lze intenzitu poruch pro trvalý (nepřerušovaný) provoz určit podle vztahu:

$$\lambda_d = 0{,}1 \cdot \frac{C}{B_{10d}} \tag{4.6}$$

kde λ_d je intenzita nebezpečných poruch pro trvalý provoz a C je počet provozních cyklů (počet sepnutí / rozepnutí) za hodinu. Výsledná pravděpodobnost selhání za hodinu PFH_i pro elektromechanické komponenty v zapojení 1oo1 je dána vztahem:

$$PFH_i = \lambda_d \cdot 1h \tag{4.7}$$

Celkovou pravděpodobnost selhání za hodinu PFH pro každý kanál realizující bezpečnostní funkci lze určit podle vztahu (4.8).

$$PFH = PFH_{DK} + PFH_{OIF} + PFH_{DIF} + PFH_{OIF} + PFH_O \tag{4.8}$$

Částečné výsledky pro jednotlivé subsystémy a celkový výsledek intenzity poruch PFH jsou uvedeny v tabulce 5.

Tabulka 5: Výsledné hodnoty jednotlivých částí systému

Parametr	Dveřní kontakty	Bariéra (OIF)	DIF	Bariéra (OIF)	Stykače K1, K3, K6
Architektura	1oo1	1oo1	1oo1	1oo1	1oo1
HW tolerance	0	0	0	0	0
λ_{DU} (1/hod)	-	$45{,}1 \cdot 10^{-9}$	$172{,}6 \cdot 10^{-9}$	$45{,}1 \cdot 10^{-9}$	-
λ_D (1/hod.)	$1{,}67 \cdot 10^{-11}$	$491{,}6 \cdot 10^{-9}$	$1629 \cdot 10^{-9}$	$491{,}6 \cdot 10^{-9}$	K1: $1{,}71 \cdot 10^{-11}$ K3: $1{,}71 \cdot 10^{-11}$ K6: $1{,}66 \cdot 10^{-11}$
PFH_i	$16{,}7 \cdot 10^{-11}$	$9{,}01 \cdot 10^{-8}$	$3{,}45 \cdot 10^{-7}$	$9{,}01 \cdot 10^{-8}$	$8{,}52 \cdot 10^{-11}$
PFH	$5{,}25 \cdot 10^{-7}$				

Celková intenzita poruch PFH jednoho kanálu, který zajišťuje bezpečnostní funkci je $5{,}25 \cdot 10^{-7}$. Tato hodnota splňuje požadavek úrovně integrity bezpečnosti SIL2, pro který platí střední frekvence nebezpečné chyby za hodinu v rozmezí:

$$\geq 10^{-7} \text{ až } < 10^{-6}$$

Nutným předpokladem výpočtů je teorie, že všechny nedetekované poruchy budou objeveny pravidelnou zkouškou. V rámci této zkoušky je proto nutné provést kontrolu funkcí jednotlivých částí systému, kontrolu jejich propojení apod. Je důležité mít na paměti, že po provedení zkoušky je teoreticky Zařízení považováno za nové, a proto je nutné, aby zkouška byla komplexní a byla provedena podle kvalifikovaného plánu.

V rámci analýzy bylo odhaleno několik poruch, které vedou na selhání řízení, měření nebo špatné generace fázového napětí jedné fáze. Na základě doporučení z výsledků analýz byla zjednodušena reakce na tyto „fázové“ poruchy. Tento závěr vyplynul z velkého počtu částečných poruch vedoucích na omezený provoz.

Zařízení při detekci poruchy v jednom výkonovém bloku bylo původně navrženo tak, aby byl s ohledem na druh poruchy vadný výkonový blok odstaven a Zařízení bylo dále provozováno s omezením výkonu. Pro připomenutí, každá fáze kompenzačního transformátu byla buzena

paralelním spojením třech výkonových bloků. Došlo-li k poruše jednoho z nich, Zařízení mělo být provozováno dále, ale se sníženým výkonem, tedy s odstaveným vadným blokem. Od této úvahy bylo ale upuštěno, jelikož řada poruch odhalených v provedených analýzách směřovala právě na omezený provoz.

Dále bylo s odkazem na provedené analýzy navrženo doplňkové testování poruchových signálů. Uvažované poruchy na těchto signálech jsou při běžícím Zařízení nedetekovatelné a mohou vést na falešné poplachy, v horším případě na znemožnění aktivace chyby. Opatření spočívá v dodatečném testování před spuštěním systému v rámci self-testů.

Následně byla odhalena nedetekovatelná porucha na chybovém signálu mezi Řídicím systémem a driverem měniče, která by mohla způsobit chybnou generaci výstupního napětí. Navržené opatření proti této poruše bude založeno na zdvojení rizikového signálu využitím rezervních vodičů, čímž nebude významně zasahovat do změny HW návrhu Zařízení.

4.8 Návrh a posouzení softwaru

Návrh a posouzení softwaru tvoří druhou velkou část v rámci ČSN EN 61508. Při posuzování softwaru jsou používány kvalitativní metody, které vyžadují velmi dobré znalosti v oblasti elektroniky a především tvorby samotného kódu (software). Přestože cílem této práce nebylo se této části věnovat, alespoň v hrubé formě jsou v této kapitole zmíněny doporučené techniky a opatření.

Cest k vytvoření softwaru splňujícího požadavky bezpečnosti je několik. Nejjednodušší z nich je použití certifikovaného softwarového nástroje. Tyto nástroje jsou většinou dodávány k bezpečnostním PLC a disponují řadou certifikovaných knihoven bloků (časovače, komparátory apod.), s jejichž pomocí je možné splnit požadavky na software, aniž by musely být prováděny podrobné analýzy požadavků uvedených v normě. Předpokladem shody s požadavky normy je použití takového nástroje v souladu s pokyny dodavatele v použití s odpovídajícím hardware.

V případě, že není k dispozici certifikovaný nástroj, nezbývá než postupovat podle požadavků normy. Problematika návrhu softwaru je minimálně stejně tak rozsáhlá jako oblast hardwaru a její zpracování by bylo nad rámec této práce. Proto se tato práce problematikou návrhu softwaru nezabývá a v příloze pouze uvádí přehled doporučených technik a opatření.

5 Závěr

Přestože je funkční bezpečnost v současné době velmi diskutované téma − a to ve všech oborech, kde vznikají rizika spojená s provozem nejrůznějších zařízení – je představa o návrhu koncepčních systémů splňujících bezpečnost pro řadu firem stále zcela neznámá.

Mým přínosem do této problematiky byla nejen implementace příslušných norem, ale především vytvoření a použití samotné metodiky při návrhu reálného zařízení, ve kterém byla řešena problematika návrhu systému souvisejícího s bezpečností. Vytvoření metodiky naplňuje hlavní cíle této práce, která v sobě zahrnuje shrnutí požadavků funkční bezpečnosti, jednotlivých metod a analýz v jeden ucelený soubor, který má sloužit k ulehčení práce při návrhu bezpečného systému. V úvodu práce je proto představena obecná norma funkční bezpečnosti ČSN EN 615008 a následně jsou vysvětleny základní pojmy a principy používané v oblasti funkční bezpečnosti. V menším detailu jsou dále zmíněny pohledy norem funkční bezpečnosti z oblasti zabezpečovací techniky, automobilového průmyslu nebo výkonových pohonů.

Metodická část práce vychází z požadavků obecné normy ČSN EN 615008, na jejímž základě byla sestavena i struktura metodiky. Jednotlivé kapitoly metodiky navazují na postupné kroky návrhu bezpečného systému. Pro každý krok jsou vždy představeny cíle s detailním rozborem požadavků dané fáze, na které navazují základní metody a techniky použitelné pro naplnění požadavků daného kroku životního cyklu.

Návrh bezpečného systému se neobejde bez podpory příslušné normy, ale jasná definice požadavků a strukturovaná forma metodiky ulehčuje jinak komplikovaný návrh. Jazyk používaný v normách, zvláště české překlady norem, nejsou mnohdy zcela srozumitelné a stanovené požadavky nemusejí být vždy zcela jednoznačné. Při tvorbě metodiky bylo snahou vysvětlit vzájemnou provázanost mezi aktivitami, se kterými se lze setkat během životního cyklu.

V poslední kapitole jsou získané poznatky uplatněny v rámci reálného projektu běžícího na fakultě elektrotechnické ve spolupráci se společností ČEZ. Metodika byla uplatněna při vývoji prototypu Zařízení pro kompenzaci zemních poruch. Zařízení bude v rámci pilotního projektu nasazeno do zkušebního provozu v rozvodně společnosti ČEZ Kralovice. Předmětem aplikace metodiky je návrh řídící části Zařízení s využitím platformy systému REMCS určené právě pro nasazení v podobných aplikacích. Systém REMCS

byl tedy nasazen do konkrétní aplikace, pro kterou byla vytvořena základní specifikace požadavků. Na základě této specifikace byl navržen koncept systému zahrnující strukturu systému, jeho rozhraní a základní schéma s tím, že veškeré tyto kroky probíhaly dle definovaného ověřovacího plánu zahrnujícího i analýzy jako FMEA nebo odhad náhodných poruch. Převážná část provedených analýz byla vypracována především autorem s dílčí podporou kolektivu.

Výsledky provedených analýz systému ukázaly na některá slabá místa systému, pro která byla navržena vhodná opatření cílená především na splnění požadavků bezpečnosti. Na základě této práce tedy došlo rovněž k významnému posunu samotné vývojové platformy systému REMCS v oblasti plnění požadavků bezpečnosti. Přestože není možné vzhledem k rozsahu této práce představit veškeré dokumenty, které byly vypracovány v nezkrácené podobě (analýzy provedené pro jednotlivé části systému mají rozsah stovek stran), je z náznaku patrná jejich komplexnost. Výsledky těchto analýz dokazují splnění požadavků na bezpečnost v úrovni SIL2. Stejně jako v podobných projektech, tak i zde nelze zveřejnit veškerou dokumentaci, jako jsou například plná obvodová schémata, přesná koncepční řešení apod.

Právě proto, že rozsah projektu, na kterém bylo prakticky představeno použití metodické části, spadá mezi velké a náročné projekty, bylo vhodné jej využít jako ukázkový příklad použití systému REMCS.

Výsledek práce může sloužit jako základ při návrhu bezpečného systému nebo při deklaraci úrovně bezpečnosti ve schvalovacím procesu. Tato oblast je v zájmu mnoha společností zabývajících se návrhem zařízení a prostředky nebo postupy k tomu použité jsou předmětem jejich interního know-how. Pokud ZČU bude mít k dispozici systém, který bude splňovat požadavky autority při schvalovacím procesu, poskytne jí to významný základ know-how pro další spolupráci v oblasti řídicích systémů a vývoje dalších aplikací s průmyslovými partnery.

Směry dalšího pokračování práce

Návrh hardwaru elektronického programovatelného systému s ohledem na bezpečnost není jedinou podmínkou na cestě za prohlášením bezpečného systému. V součinnosti s návrhem hardwaru je potřeba věnovat neméně tak velkou pozornost návrhu bezpečného softwaru. Použití certifikovaných SW nástrojů návrh významně usnadňuje, jejich

aplikovatelnost je však omezena na velmi úzkou řadu konkrétních hardwarových platforem.

Směr dalšího zkoumání tak jasně směřuje ke studiu třetího dílu normy ČSN EN 61508 věnovaného návrhu softwaru. Přestože je struktura návrhu bezpečného softwaru blízká návrhu hardwaru, jsou zde rozdíly, pro které nelze použít stejné metody, techniky a opatření. Autor si je velmi dobře vědom, že zpracování metodiky návrhu bezpečného softwaru nemůže být předmětem jedné přidané kapitoly v této práci, ale vede přinejmenším na novou práci v podobném rozsahu.

Literatura

[1] ČSN EN 61508 ed.2. *Funkční bezpečnost E/E/EP systémů souvisejících s bezpečností*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak 180301.

[2] ZAJÍČEK, J., KAMENICKÝ, J. *Porovnání přístupů stanovení funkční bezpečnosti*. Ostrava: VŠB-TUO, Výzkumné energetické centrum, 2013.

[3] CHUDÁČEK, V. a kol. *Železniční zabezpečovací technika*. Praha: ČD - VÚŽ, 2005.

[4] KOTEK, L., VOHRALÍKOVÁ, M. *Jak zvyšovat spolehlivost lidské obsluhy*. Automa, č. 5, s. 26-28. 2008.

[5] VROŽINA, M., DAVID, J. *Spolehlivost a diagnostika*. Ostrava: 2012. ISBN 978-80-248-2595-3.

[6] MYKISKA, A., VOTAVA, P. *Metody analýz spolehlivosti systémů a jejich výběr*. Zabezpečení spolehlivosti. Praha: 2001.

[7] TURJANICA, P., POLÁČEK, L. *General Requirements Specification - REMCS - Rice Embedded Modular Control System*. Plzeň: 2011. Interní specifikace.

[8] NETOLICKÝ, P., TURJANICA, P., POLÁČEK, L., ELIS, L., PITERKA, L. *Specifikace požadavků na bezpečnost PDS*. Plzeň: 2014. Interní specifikace.

[9] TURJANICA, P., POLÁČEK, L., ELIS, L., PITERKA, L. *Aplikace pro schvalovací proces*. Plzeň: 2014. Interní specifikace.

[10] NETOLICKÝ, P., TURJANICA, P., POLÁČEK, L., ELIS, L., PITERKA, L. *Koncept PDS*. Plzeň: 2014. Interní specifikace.

[11] NETOLICKÝ, P., TURJANICA, P., POLÁČEK, L., ELIS, L., PITERKA, L. *Návrh a vývoj PDS*. Plzeň: 2014. Interní specifikace.

[12] NETOLICKÝ, P., TURJANICA, P. *Proces vývoje výrobku*. Plzeň: 2015. Interní směrnice.

[13] TURJANICA, P., POLÁČEK, L., BURIAN, P. *Hardware Design Document - REMCS*. Plzeň: 2011. Interní specifikace.

[14] TURJANICA, P., POLÁČEK, L., BURIAN, P., JÁRA, M. *Hardware Design Document - REMCS - Direct interface*. Plzeň: 2011. Interní specifikace.

[15] TURJANICA, P., POLÁČEK, L., BURIAN, P., JÁRA, M. *Hardware Design Document - REMCS - Open interface unit*. Plzeň: 2012. Interní specifikace.

[16] ELIS, L., POLÁČEK, L. *Intenzita poruch - DIF01 MTBF*. Plzeň: 2015. Formát tabulky EXCEL. Interní specifikace.

[17] ELIS, L., POLÁČEK, L. *Intenzita poruch - OIF01 MTBF*. Plzeň: 2015. Formát tabulky EXCEL. Interní specifikace.

[18] UGLJESA, E., BÖRCSÖK, J. *Evaluation of sophisticated hardware architectures for safety applications.* XXII International Symposium on Information, Communication and Automation Technologies, pp. 1 – 8. 2009.

[19] ČSN EN 60812. *Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2007. Třídící znak 010675.

[20] HOLUB, R., VINTR, Z. *Spolehlivost letadlové techniky*. VUT FST. Brno: 2001. Elektronická učebnice.

[21] ELIS, L. *Analýza rizika elektronických systémů za použití metody FMEA*. Elektrotechnika a Informatika 2017. Str. 11-14. Plzeň: 2017.

[22] FAMFULIK, J., MÍKOVÁ, J. Příspěvěk k analýze rizika modulu automatického vedení vlaku. Perners Contacts, roč. 4, č. III. [online]. listopad 2009 [cit. 25. 2. 2017]. Dostupné z: http://pernerscontacts.upce.cz/15_2009/Famfulik2.pdf

[23] GUTMANN, K-H., (překlad KEBEŠ, K. a redakce). *Provozní přístroje a hledisko funkční bezpečnosti*. Automa, roč. 12, č. 6. 2006.

[24] UHER, J. *Úvod do funkční bezpečnosti I: norma ČSN EN 61508*. Automa, roč. 10, č. 8-9. 2004.

[25] ZAKUCIA, J. *Metódy posudzovania spoľahlivosti zložitých elektronických systémov pre kozmické aplikácie*. VUT FST. Brno: 2015. Disertační práce.

[26] HOCKSTAD, P., CORNELIUSSEN, K. *Loss of safety assessment and the IEC 61508 standard*. Reliability Engineering and System Safety, Vol. 83, č. 1, str. 111-120. 2004.

[27] WANG, CH., XING, L., LEVITIN, G. *Explicit and implicit methods for probabilistic common-cause failure analysis*. Reliability Engineering and System Safety, Vol. 131, str. 175-184. 2014.

[28] MLČÁK, T. *Funkční bezpečnost vyhrazených elektrických zařízení*. VŠB TUO. Ostrava: 2014. Učební text.

[29] MABOOK, E. Failure Modes, Effects and Diagnosti Analysis of Safety Device. Metropolia University of Applied Sciences. Helsinki: 2017. Baklářská práce.

[30] ŠIMONÍK, M. *Funkční bezpečnost snímačů tlaku BD Sensors, s.r.o*. VUT FEL. Brno: 2015. Diplomová práce.

[31] TOMAN, P., DRÁPELA, J., aj. *Provoz distribučbích soustav*. ČVÚT. Praha: 2011.

[32] MATULJAK, I. *Moderní systémykompenzace zemních poruchv rozvodné soustavě s využitím výkonové elektroniky*. Plzeň: 2013. Disertační práce.

[33] KOMRSKA, T. *Zařízení pro kompenzaci zemních poruch v izolovaných a neúčinně uzemněných sítích*. Plzeň: 2017. Odborná zpráva.

[34] ČSN EN 62061. *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností.* Český normalizační institut, 2005. Třídící znak 332208.

Seznam autorových publikací

Příspěvky na konferencích a články ve sbornících

A1. ELIS, L. *Analýza rizika elektronických systémů za použití metody FMEA*. In *Elektrotechnika a informatika 2017. Elektrotechnika, elektronika, elektroenergetika.* Plzeň: Západočeská univerzita v Plzni, 2017. s. 11-14. ISBN: 978-80-261-0712-5

A2. ELIS, L., KOSTURIK, K. Architektury systémů pracujících se zvýšenými požadavky na bezpečnost. In *Elektrotechnika a informatika 2016. Elektrotechnika, elektronika, elektroenergetika.* Plzeň: Západočeská univerzita v Plzni, 2016. s. 109-112. ISBN: 978-80-261-0516-9

A3. ELIS, L., KOSTURIK, K. Přepočet intenzity poruch součástek pro různé podmínky prostředí. In *Elektrotechnika a informatika 2015. Elektrotechnika, elektronika, elektroenergetika.* Plzeň: Západočeská univerzita v Plzni, 2015. s. 149-152. ISBN: 978-80-261-0514-5

A4. ELIS, L., KOSTURIK, K. The extrapolation of failure rate of electrical components in specific operational conditions. In *Proceedings of the*

23rd Telecommunications Forum (TELFOR 2015). Piscataway: IEEE, 2015. s. 658-661. ISBN: 978-1-5090-0055-5

A5. ELIS, L., TURJANICA, P., POLÁČEK, L., PITERKA, L. Evaluation of REMCS Control System for Safety Applications. In *Proceedings of the 22nd TELECOMMUNICATIONS FORUM - (TELFOR 2014)*. Belgrade: IEEE, 2014. s. 687-690. ISBN: 978-1-4799-6190-0

A6. ŽAHOUR, J., KŘIVKA, J., ELIS, L. Nepřímé určování tlaku ve vstřikovacím systému. In *Elektrotechnika a informatika 2014. Část 2., Elektronika*. Plzeň: Západočeská univerzita v Plzni, 2014. s. 93-96. ISBN: 978-80-261-0366-0

A7. KŘIVKA, J., ELIS, L., ŽAHOUR, J. Nový řídicí systém pro elektricky regenerovatelné filtry pevných částic. In *Elektrotechnika a informatika 2014. Část 2., Elektronika*. Plzeň: Západočeská univerzita v Plzni, 2014. s. 37-40. ISBN: 978-80-261-0366-0

A8. ELIS, L., KŘIVKA, J., ŽAHOUR, J. Požadavky na funkční bezpečnost REMCS systému a příkladové DEMO aplikace. In *Elektrotechnika a informatika 2014. Část 2., Elektronika*. Plzeň: Západočeská univerzita v Plzni, 2014. s. 25-28. ISBN: 978-80-261-0366-0

A9. ŠTĚTKA, P., KŘIVKA, J., ELIS, L., VLÁŠEK, J., ŽAHOUR, J., KOSTURIK, K. Control and navigation system for mobile platform. In *Proceedings of the 21st Telecommunications Forum (TELFOR 2013).* Bělehrad: IEEE, 2013. s. 584-586. ISBN: 978-1-4799-1419-7

A10. ŽAHOUR, J., KŘIVKA, J., ELIS, L., ŠTĚTKA, P., KOSTURIK, K. Control unit of monitoring airship and his communication interface. In *Proceedings of the 21st Telecommunications Forum (TELFOR 2013).* Bělehrad: IEEE, 2013. s. 587-589. ISBN: 978-1-4799-1419-7

A11. ŠTĚPÁNEK, J., BEDNÁŘ, B., STREIT, L., ELIS, L. Electric Kart "FeLis" with LiFeYPO4 Batteries. In *4th International Conference on Clean Electrical Power Renewable Energy Resources Impact.* New York: IEEE, 2013. s. 151-154. ISBN: 978-1-4673-4430-2

A12. STREIT, L., ŠTĚPÁNEK, J., ELIS, L., BEDNÁŘ, B. Electric Kart as a Student Project. In *EPE 13 ECCE Europe.* Brussel: EPE Association, 2013. s. "P.1"-"P.6". ISBN: 978-1-4799-0116-6

A13. ŠTĚPÁNEK, J., BEDNÁŘ, B., STREIT, L., ELIS, L. Elektrická motokára "FeLis". In *Elektrotechnika a informatika 2013. Část 1. Elektrotechnika.* Plzeň: Západočeská univerzita, 2013. s. 151-154. ISBN: 978-80-261-0233-5

A14. KŘIVKA, J., ELIS, L., VLÁŠEK, J., ŽAHOUR, J., ŠTĚTKA, P., KOSTURIK, K. Hardware for rail traffic simulator. In *Proceedings of the 21st Telecommunications Forum (TELFOR 2013).* Bělehrad: IEEE, 2013. s. 590-593. ISBN: 978-1-4799-1419-7

A15. KŘIVKA, J., ELIS, L., ŽAHOUR, J. Simulátor kolejových vozidel. In *Elektrotechnika a informatika 2013. Část 2., Elektronika.* Plzeň: Západočeská univerzita, 2013. s. 49-52. ISBN: 978-80-261-0232-8

A16. VLÁŠEK, J., KŘIVKA, J., ELIS, L., ŽAHOUR, J., ŠTĚTKA, P., KOSTURIK, K. Software for rail traffic simulator. In *Proceedings of the 21st Telecommunications Forum (TELFOR 2013).* Bělehrad: IEEE, 2013. s. 594-596. ISBN: 978-1-4799-1419-7

A17. ELIS, L., KŘIVKA, J., ŽAHOUR, J. Zabezpečení RC systému vzducholodě. In *Elektrotechnika a informatika 2013. Část 2., Elektronika.* Plzeň: Západočeská univerzita v Plzni, 2013. s. 21-24. ISBN: 978-80-261-0232-8

A18. STREIT, L., ŠTĚPÁNEK, J., BEDNÁŘ, B., KUBÍK, M., ELIS, L. Electric Kart with LiFeYPO4 Batteries. In *Proceedings of the International Conference on Applied Electronics 2012.* Plzeň: Západočeská univerzita v Plzni, 2012. s. 305-308. ISBN: 978-80-261-0038-6, ISSN: 1803-7232

A19. ELIS, L. Naprogramování emulátoru řídicí jednotky ve spojení s uHiL simulátorem. In *Elektrotechnika a informatika 2012. Část 2., Elektronika.* Plzeň: Západočeská univerzita v Plzni, 2012. s. 25-28. ISBN: 978-80-261-0119-2

Článek přijatý na konferenci

SCHARFENBERG, G., ELIS, L., HOFMANN, G. New design methodology – Using VHDL-AMS models to consider aging effects in automotive mechatronic circuits for safety relevant functions. In *2019 International Conference on Applied Electronics.* Plzeň: Západočeská univerzita v Plzni.

Připravovaná publikace do odborného časopisu

HOFMANN, G., ELIS, L., Georgiev, V., Temperature aging measurements of commercial resistors

Prototypy a funkční vzorky

A20. ELIS, L., ŠVARNÝ, J., PUŠMAN, L., TURJANICA, P. Firmware pro *autonomní elektronický zámek*. 2018. 22190-SW008-2018

A21. ELIS, L., ŠVARNÝ, J., PUŠMAN, L., TURJANICA, P. *Autonomní elektronický zámek*. 2018. 22190-PR001-2018

A22. ELIS, L., ŠVARNÝ, J., PUŠMAN, L., TURJANICA, P. *Door lockcontrol unit with emergency power bank*. 2018. Výzkumná zpráva

A23. BEDŘICH, B., BLAHÍK, V., BURIAN, P., ELIS, JÁRA, M., L., KINDL, V., KOMRSKA, T., KOŠAN, T., MICHALÍK, J., MOLNÁR, J., PEROUTKA, Z., POLÁČEK, L., STREIT, L., SKALA, B., ŠTENGL, J., ŠTĚPÁNEK, J., TALLA, J., TURJANICA, P. *Zařízení pro kompenzaci zemních poruch 22/0,4 kV 1,35 MVA*. 2017. 22190-PR006-2017

A24. ELIS, L., POLÁČEK, L., TURJANICA, P. Zařízení pro měření parametrů sítě. 2017. 22190-FV025-2017

A25. ELIS, L., ŠVARNÝ, J., PUŠMAN, L., TURJANICA, P. Řídicí jednotka zámku dveří: Prototyp „A“. 2017. 22190-FV020-2017

A26. ELIS, L., ČENGERY, J., FREISLEBEN, J., KAŠPAR, P., HAMÁČEK, A. *Modul senzoru teploty a relativní vlhkosti pro zásahový hasičský oblek*. 2017. 22190-PR002-2017

A27. ELIS, L., ČENGERY, J., KAŠPAR, P., KUBERSKÝ, P., HAMÁČEK, A. *Modul senzoru plynu CH4 pro zásahový hasičský oblek*. 2017. 22190-FV005-2017

A28. ELIS, L., ČENGERY, J., KAŠPAR, P., KUBERSKÝ, P. *Modul senzoru plynu NO2 pro zásahový hasičský oblek*. 2017. 22190-FV004-2017

A29. ELIS, L., ČENGERY, J., KAŠPAR, P., KUBERSKÝ, P., HAMÁČEK, A. *Modul senzoru plynu CO pro zásahový hasičský oblek*. 2017. 22190-FV003-2017

A30. BRICHCÍN, J., ELIS, L., POLÁČEK, L. *MRE inteligentní wattmetr*. 2016. 22190-FV042-2016

A31. KŘIVKA, J., ŽAHOUR, J., ELIS, L., KOSTURIK, K. *High-speed P-MOSFET driver*. 2015. 22110-FV003-2015

A32. ELIS, L., KŘIVKA, J., ŽAHOUR, J., KOSTURIK, K. *Komunikační modul mezi* sběrnicemi RS-232 a LIN. 2015. 22110-FV008-2015

A33. KŘIVKA, J., ŽAHOUR, J., ELIS, L., KOSTURIK, K. *Testovací platforma pro automotive aplikace založená na modulech NI USB-6008 OEM - základní provedení.* 2015. 22110-FV004-2015

A34. ŽAHOUR, J., KŘIVKA, J., KOSTURIK, K., ELIS, L. *Řídící jednotka digitálně řízeného audiozesilovače.* 2015. 22110-FV006-2015

A35. ŽAHOUR, J., KŘIVKA, J., KOSTURIK, K., ELIS, L. *Řídící jednotka kotle na tuhá paliva*. 2015. 22110-FV007-2015

A36. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Bateriová elektronika monitorovací vzducholodě*. 2014. 22110-FV026-2014

A37. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Elektronický šesti-kanálový signálový přepínač*. 2014. 22110-FV028-2014

A38. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Lokalizační elektronika pro kolejový simulátor*. 2014. 22110-FV025-2014

A39. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Přesný dvoukanálový generátor fázově posunutých pulsů*. 2014. 22110-FV027-2014

A40. KŘIVKA, J., ŽAHOUR, J., ELIS, L., KOSTURIK, K. *Universální komunikační modul mezi sběrnicemi USB 2.0, USB 1.1 a RS-232*. 2014. 22110-FV024-2014

A41. ŽAHOUR, J., KOSTURIK, K., KŘIVKA, J., ELIS, L. *Zařízení pro detekci mechanického opotřebení točivých strojů*. 2014. 22110-FV016-2014

A42. ŽAHOUR, J., KOSTURIK, K., KŘIVKA, J., ELIS, L. *Řídící jednotka akčního členu dveřní jednotky*. 2014. 22110-FV017-2014

A43. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Autonomní solární zavlažovací systém*. 2013. 22110-FV026-2013

A44. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J., GEORGIEV, V. *Dispečerské stanoviště simulátoru kolejových vozidel*. 2013. 22110-FV014-2013

A45. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J., GEORGIEV, V. *Elektronická výzbroj modelu kolejového vozidla*. 2013. 22110-FV017-2013

A46. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J. *Inovace extruderu pro 3D tiskárnu Ultimaker*. 2013. 22110-FV020-2013

A47. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J. *Laserové detekční zařízení*. 2013. 22110-FV021-2013

A48. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Lokalizační elektronika monitorovací vzducholodě*. 2013. 22110-FV024-2013

A49. KOSTURIK, K., ELIS, L., KŘIVKA, J., ŽAHOUR, J. *Manuální spínač pro testování DPF filtrů*. 2013. 22110-FV007-2013

A50. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J. *Měřící elektronika monitorovací vzducholodě*. 2013. 22110-FV019-2013

A51. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Nízkonapěťový záložní zdroj s využitím Li-Ion akumulátorů*. 2013. 22110-FV027-2013

A52. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J. *Přípravek pro testování dosahu bezdrátových modulů*. 2013. 22110-FV023-2013

A53. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Rotační displej*. 2013. 22110-FV025-2013

A54. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J., GEORGIEV, V. *Senzory a akční členy kolejového simulátoru*. 2013. 22110-FV018-2013

A55. KOSTURIK, K., ELIS, L., KŘIVKA, J., ŽAHOUR, J. *Systém pro měření vibrací v prostoru výfuku*. 2013. 22110-FV036-2013

A56. KOSTURIK, K., ELIS, L., KŘIVKA, J., ŽAHOUR, J. *USB vysílač s modulem Xbee PRO*. 2013. 22110-FV031-2013

A57. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J., GEORGIEV, V. *Vlaková kabina simulátoru kolejových vozidel*. 2013. 22110-FV015-2013

A58. ELIS, L., KOSTURIK, K., KŘIVKA, J., ŽAHOUR, J. *Řídicí elektronika monitorovací vzducholodě*. 2013. 22110-FV022-2013

A59. KOSTURIK, K., KŘIVKA, J., ELIS, L., ŽAHOUR, J., GEORGIEV, V. *Řídicí jednotka stanice kolejového simulátoru*. 2013. 22110-FV016-2013

A60. KOSTURIK, K., ELIS, L., KŘIVKA, J., ŽAHOUR, J. *Řídící elektronika DPF pro 24 voltový systém*. 2013. 22110-PR001-2013

A61. STREIT, L., ELIS, L. *Zobrazovací jednotka elektrické motokáry*. 2012. 22160–FV010–2012

A62. STREIT, L., ELIS, L. *Interface k procesoru AT90CAN*. 2011. 22160-FV004-2011

A63. KUBÍK, M., ELIS, L. *Soubor modulů vícevstupého jakostního předzesilovače*. 2011. 22110-FV008-2011