Západočeská univerzita v Plzni
Fakulta elektrotechnická

DISERTAČNÍ PRÁCE

Řídicí systémy se zvýšenou bezpečností

Ing. Luděk Elis **Plzeň, 2019**

FAKULTA
ELEKTROTECHNICKÁ
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

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. **Plzeň 2019**

Prohlášení

Prohlašuji, že jsem disertační práci vypracoval samostatně a použil jsem prameny, které cituji a uvádím v seznamu literatury. V předložené vědecké práci jsou použity obvyklé vědecké postupy.

V Plzni, datum

……
podpis

Poděkování

Na tomto místě bych chtěl poděkovat panu doc. Ing. Jiřímu Skálovi, Ph.D. za vedení mé práce. Mé poděkování patří též Ing. Pavlu Turjanicovi, Ph.D., Ing. Liboru Poláčkovi, Ph.D. a Ing. Tomáši Komrskovi, Ph.D. za spolupráci při získávání údajů pro výzkumnou část práce. Děkuji také své manželce za psychickou podporu v průběhu celého studia.

Prohlášení řešitele projektu

Tato práce vznikla s podporou Ministerstva školství, mládeže a tělovýchovy ČR v rámci grantů SGS-2012-019 (Moderní řešení elektronických řídících a informačních systémů) a SGS-2015-002 (Moderní metody řešení, návrh a aplikace elektronických a komunikačních systémů).

V Plzni, datum

……
podpis

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 té samé 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 is focused 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

Seznam použitých zkratek

Zkratka	***Význam***	***Meaning***
ALARP	Metoda „co nejnižší rozumně dosažitelné riziko“	*As Low As Reasonably Practicable*
ASIL	Úroveň integrity bezpečnosti v automobilovém sektoru	*Automotive Safety Integrity Level*
BPF	Aktivní propojovací modul systému REMCS	*Backplane Full*
CAN	Komunikační sběrnice	*Control Area Network*
CCF	Porucha se společnou příčinou	*Common Cause Failure*
CCA	Analýza příčin a následků	*Cause - Consequence Analysis*
CL	Kontrolní seznam	*Checklist Analysis*
DIF	Karta pro řízení měniče	*Direct Interface*
E/E/EP	Elektrických/elektronických/ programovatelných elektronických systémů	*Electrical/Electronic/Programmable Electronic Systems*
ECU	Elektronická řídicí jednotka	*Electronic Control Unit*
ETA	Analýza stromem událostí	*Event Tree Analysis*
FMEA	Analýza způsobů a důsledků poruch	*Failure Modes and Effects Analysis*
FMECA	Analýza způsobů, důsledků a kritičnosti poruch	*Failure Mode and Effect Criticality Analysis*
FTA	Analýza stromem poruch	*Fault Tree Analysis*
FPGA	Programovatelné hradlové pole	*Field Programmable Gate Array*
HAZOP	Analýza nebezpečí a provozuschopnosti	*Hazard and Operability Analysis*
HFT	Odolnost HW proti vadám	*Hardware Fault Tolerance*
HRA	Analýza lidského faktoru	*Human Reliability Analysis*
HW	Hardware	*Hardware*
LVDS	Komunikační sběrnice	*Low Voltage Differential Signaling*
MCU	Mikroprocesorová karta systému REMCS	*Main Controller Unit*
MTTR	Střední doba do obnovy	*Mean Time To Restore*
OIF	Karta otevřené platformy systému REMCS	*Open interface*
PDS	Systémy elektrických výkonových pohonů	*Power Drive System*
PFD	Pravděpodobnost selhání na vyžádání	*Probability of Failure on Demand*
PFH	Střední frekvence nebezpečné chyby za hodinu	*Probability of Failure per Hour*
PHA	Předběžná analýza ohrožení	*Preliminary Hazard Analysis*
PLC	Programovatelný logický automat	*Programmable Logic Controller*
PSU	Napájecí zdroj	*Power Supply*

Zkratka	***Význam***	***Meaning***
PWM	Pulzně šířková modulace	*Pulse Width Modulation*
RAMS	Bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti	*Reliability, Availability, Maintainability and Safety*
RBD	Spolehlivostní schémata bezporuchovosti	*Reliability Block Diagram*
RDF	Poměr nebezpečných poruch elektromechanických součástí	*Ratio of Dangerous Failure*
REMCS	Modulární řídicí systém	*RICE Embedded Modular Control System*
RICE	Regionální inovační centrum elektrotechniky	*Regional Innovation Centre for Electrical Engineering*
ŘS	Řídicí systém	*Control system*
SC	Systematická schopnost	*Systematic Capability*
SIM	Modul inkrementálního čidla otáček systému REMCS	*Sensor Interface Module*
SIL	Úroveň integrity bezpečnosti	*Safety Integrity Level*
SFF	Poměr bezpečných poruch	*Safe Failure Fraction*
SR	Revize bezpečnosti	*Safety Review*
SKiiP	Inteligentní výkonový prvek	*SEMIKRON integrated intelligent Power*
STO	Bezpečnostní funkce − Bezpečné vypnutí točivého momentu	*Safe Torque Off*
THR	Míra přijatelného rizika	*Tolerable Hazard Rates*
WI	Analýza „Co se stane, když…“	*What-If Analysis*
ŽC	Životní cyklus	*Life Cycle*

Seznam použitých symbolů a konstant

Symbol	***Jednotka***	***Význam***
β	(%)	*Faktor společných poruch bez uvažování diagnostických testů*
β_D	(%)	*Faktor společných poruch s uvažováním diagnostických testů*
B_{10}	(-)	*Doba nebo počet sepnutí, při kterém dojde k poruše 10 % zkoušených prvků*
B_{10d}	(-)	*Doba nebo počet sepnutí, při kterém dojde k nebezpečné poruše 10 % zkoušených prvků*
C	(1/h)	*Počet provozních cyklů (počet sepnutí / rozepnutí)*
λ	(1/h)	*Intenzita poruch*
λ_D	(1/h)	*Intenzita nebezpečných poruch*
λ_{Dd}	(1/h)	*Intenzita nebezpečných poruch detekovatelných diagnostickými testy*
λ_{Du}	(1/h)	*Intenzita nebezpečných poruch nedetekovatelných diagnostickými testy*
λ_e	(1/h)	*Intenzita nebezpečných poruch pro přerušovaný provoz*
λ_g	(1/h)	*Intenzita poruch generického prvku systému*
λ_S	(1/h)	*Intenzita bezpečných poruch*
λ_{sys}	(1/h)	*Intenzita poruch systému*
n	(-)	*Počet rozdílných generických kategorií prvků systému*
N_i	(-)	*Počet generických prvků systému*
t_{ce}	(h)	*Ekvivalentní střední doba prostoje kanálu*
t_{ge}	(h)	*Ekvivalentní střední doba prostoje systému*
T_1	(h)	*Interval kontrolní zkoušky*
T_f	(h)	*Doba fungování v přerušovaném provozu*
T_{mf}	(h)	*Doba bez fungování (bez namáhání) v přerušovaném provozu*

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. Novodobé technické prostředky umožňují návrhářům v krátkém čase vytvořit velmi rozsáhlá a důmyslná zařízení, která bychom bez těchto prostředků vyvíjeli i několik let. Také nové technologie, výkonnější a bezpečnější procesory nebo speciální součástky nabízí sice širokou škálu možných uspořádání kvalitních systémů s rozličnou architekturou, přesto nezaručují to, že budou správně použity a nebudou překračovány jejich limity. Především procesorová technika se v elektronických řídicích systémech stala velmi využívanou, jelikož je velmi jednoduché a rychlé změnit kompletní algoritmus řízení pouhým přepsáním kódu. Od počátku se stal software pro svou jednoduchost velice oblíbeným, postupně začal vytlačovat čistě hardwarová řešení a stále častěji se začal objevovat i v oblastech souvisejících s bezpečností. Lidí, kteří by znali programovací jazyk a dokázali vytvářet kódy pro řídicí systémy, nebylo mnoho a navíc jejich znalosti byly značně omezené. Programování tak bylo spíše uměním než projektováním a úvaha nad bezpečností softwaru byla zcela neznámá. Spoléhalo se na to, že pokud zařízení pracuje spolehlivě, je bezpečné. Bohužel spolehlivost nezaručuje bezpečnost a tyto pojmy nelze slučovat.

2.1 Obecná norma pro funkční bezpečnost – ČSN EN 61508 ed.2

Se stupňující se složitostí zařízení a nečitelností softwaru již nebylo možné ověřit, zda je zařízení v pořádku a nebude nebezpečné. Mezinárodní elektrotechnická komise (IEC – *International Electrotechnical Commission*) tedy přišla se studií, která se věnovala moderním programovatelným elektronickým systémům souvisejících s bezpečností zahrnující hardware i software. Tím položila základ pro návrh normy, původně označené IEC 1508, která měla být vodítkem pro konstruktéry při návrhu systémů a průzkumu jejich bezpečnosti.

Postupem času se návrh normy přesouval k přístupu založenému na výpočtu rizika, určování jeho podstaty a následného omezení. V okamžiku, kdy je možné efektivně určit rizikové faktory, které je třeba omezit, lze stanovit požadavky na bezpečnost vedoucí k efektivnímu snížení rizika. Podstatného zjednodušení a lepší přehlednosti lze dosáhnout oddělením požadavků na bezpečnost od požadavků na funkční schopnosti zařízení.

Návrh normy kladl důraz především na kroky související s bezpečností vycházející z rizika, které systém představuje pro své okolí. Tato myšlenka se přenesla i do vzniklé normy IEC 61508 (český překlad ČSN EN 61508).

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.

2.1.1 Struktura normy

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. Jednotlivé části ČSN EN 61508 jsou zaměřeny na tato konkrétnější témata:

Část 1: Stanovuje všeobecné požadavky, které jsou použitelné ve všech jejích částech,

Část 2: obsahuje doplňující a specifické požadavky na systémy E/E/PE související s bezpečností pro hardware,

Část 3: obsahuje doplňující a specifické požadavky na systémy E/E/PE související s bezpečností pro software,

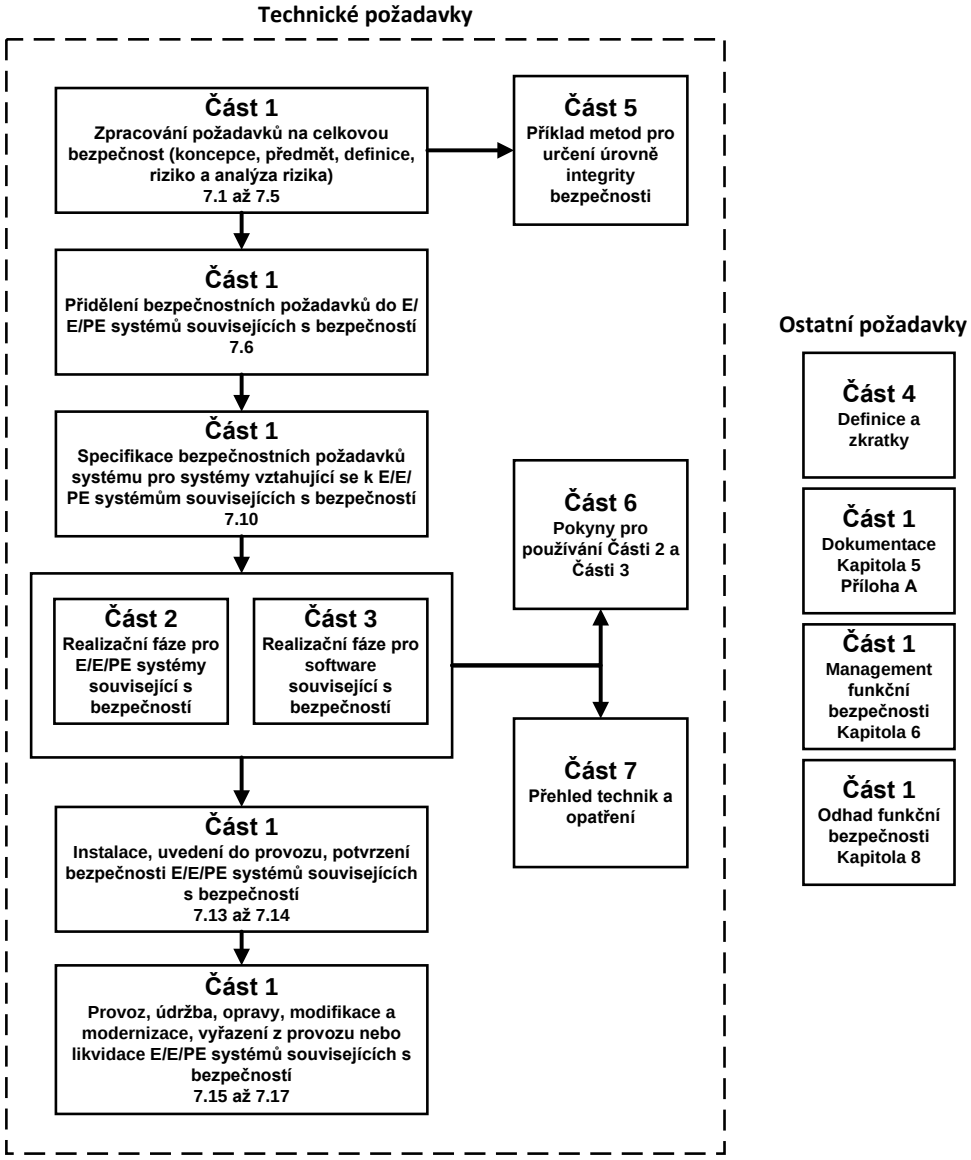
Část 4: obsahuje definice a zkratky používané v celé této normě,

Část 5: obsahuje metodické pokyny pro použití části 1 pro určování úrovní integrity bezpečnosti a to formou uvedení vzorových metod,

Část 6: obsahuje metodické pokyny pro používání částí 2 a 3,

Část 7: obsahuje přehled technik a opatření.

Na následujícím obrázku je graficky uveden celkový rámec souboru ČSN EN 61508 s vyznačením úloh, které mají jednotlivé části z hlediska dosažení funkční bezpečnosti systémů E/E/PE souvisejících s bezpečností.



Obrázek 1: Celkový rámec souboru norem ČSN EN 61508. [1]

2.1.2 Použití normy

Primárně je norma určena pro bezpečné prvky závislé na hardwaru a softwaru E/E/PE systémů, ale její využití může být daleko obecnější a může tvořit základ bezpečnosti při návrhu systémů i z jiných oblastí. Nemusí to být nutně oblast, kde adekvátní norma neexistuje, ale příslušné metody a postupy v konkrétní specifické normě nejsou uvedeny a cíleně se mohou odkazovat přímo na určité části normy ČSN EN 61508. Obecně se ale funkční a technická bezpečnost běžně aplikuje v oblastech:

- Elektrotechnika
- Zpracovatelský průmysl
- Energetika
- Infrastruktura a sítě
- Výškové budovy
- Protipožární ochrana
- Zábavní a sportovní zařízení

Seznam pokrývající všechny oblasti, kde je používána norma ČSN EN 61508 nebo její deriváty, je daleko rozsáhlejší než zde uvedený a ani nelze jednoznačně definovat všechny obory, ve kterých je na místě problematiku bezpečnosti řešit. Přestože je norma formálně určena pro E/E/PE systémy, nevylučuje ani jiné technické způsoby pro zajištění bezpečnostních funkcí, například použitím hydraulických či mechanických systémů.

2.2 Základní termíny funkční bezpečnosti

V oblasti systémů souvisejících s bezpečností je používáno mnoho pojmů, proto je namístě zde uvést základní z nich. Definice vycházejí z normy ČSN EN 61508, která je zastřešující a některé vybrané pojmy se v ostatních normách týkajících se funkční bezpečností liší jen minimálně.

Systémy

- **Řízené zařízení** (*Equipment Under Control - EUC*) – zařízení, stroj, přístroj nebo instance použité pro spojité i nespojité výrobní, dopravní, lékařské nebo jiné činnosti.
- **Systém řízení EUC** (*EUC Control System*) – systém reagující na signály z procesu anebo od operátora a vytvářející výstupní signály způsobující, že EUC pracuje požadovaným způsobem.
- **Riziko EUC** (*EUC Risk*) – riziko plynoucí z EUC nebo jeho interakce se systémem řízení EUC, tj. riziko související s funkční bezpečností.
- **Systém související s bezpečností** (*Safety-Related System*) – navržený systém který současně provádí požadované bezpečnostní funkce nezbytné pro dosažení nebo udržení bezpečného stavu v EUC, zajišťuje potřebnou integritu bezpečnosti požadované bezpečnostní funkce, a to buď sám, nebo spolu s dalšími E/E/PE systémy souvisejícími s bezpečností, systémy souvisejícími s bezpečností založenými na jiných technických principech nebo vnějšími prostředky pro zmenšení rizika.
- **Jiná opatření snižující riziko** (*Other Risk Reduction Measures*) – jsou založena na jiných technických principech než E/E/PE nebo to mohou být fyzikální struktury.
- **Elektrický/elektronický/programovatelný elektronický systém** (*Electrical/Electronic/Programmable Electronic System – E/E/PE systém*) – systém pro řízení, ochranu nebo monitorování založený na jednom nebo několika programovatelných elektronických zařízeních včetně všech prvků systému, jakými jsou např. napájecí zdroje, snímače a jiná vstupní zařízení, datové sběrnice a jiné přenosové cesty a akční členy i další výstupní zařízení.

Bezpečnost a riziko

- **Bezpečnost** (*Safety*) – schopnost systému omezit důsledky poruch zařízení (odstranění nepřijatelného rizika).

- **Funkční bezpečnost** (*Functional Safety*) – část celkové bezpečnosti týkající se rizika řízeného zařízení (EUC) a systému řízení EUC je závislá na správném fungování bezpečnostního přístrojového systému, systémů založených na jiných technických principech a vnějších prostředcích pro snížení rizika.
- **Technická bezpečnost** (*Technical Safety*) – splnění požadavku, aby při poruchách samotného zařízení nedošlo k přímému ohrožení bezpečnosti.
- **Poškození, újma** (*Harm*) – fyzické zranění nebo poškození zdraví lidí buď přímo nebo nepřímo v důsledku ztráty/zhoršení vlastností nebo prostředí.
- **Nebezpečí** (*Hazard*) – potenciální zdroj poškození.
- **Nebezpečná situace** (*Hazardous Situation*) – okolnosti, za nichž je osoba vystavena nebezpečí.
- **Nebezpečná událost** (*Hazardous Event*) – nebezpečná situace, jejímž výsledkem je poškození nebo újma.
- **Riziko** (*Risk*) – kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození.
- **Přípustné riziko** (*Tolerable Risk*) – riziko, které je přijatelné v daných souvislostech založených na běžných hodnotách společnosti.
- **Zbytkové riziko** (*Residual Risk*) – riziko zbývající po přijetí ochranných opatření.
- **Porucha** – (*Failure*) ukončení schopnosti bezpečnostního přístrojového systému, subsystému nebo prvku subsystému plnit požadovanou funkci.
- **Chyba** – (*Error*) rozdíl mezi správnou a skutečnou hodnotou konkrétní veličiny zjištěný měřením nebo pozorováním.
- **Nebezpečná porucha** – (*Dangerous Failure*) porucha, která je schopna uvést bezpečnostní přístrojový systém do nebezpečného stavu nebo do stavu, kdy není schopen plnit svou funkci.

- **Bezpečná porucha** – (*Safe Failure*) porucha, která není schopna uvést bezpečnostní přístrojový systém do nebezpečného stavu, v němž by nebyl schopen plnit svou funkci.
- **Systematická porucha** – (*Systematic Failure*) porucha související rozhodujícím způsobem s určitou příčinou, která může být vyloučena pouze modifikací návrhu nebo výrobního procesu, provozních postupů, dokumentací nebo jiných relevantních faktorů.
- **Odolnost proti vadám** – (*Hardware Fault Tolerant*) schopnost bezpečnostního přístrojového systému plnit bezpečnostní funkci za přítomnosti vad nebo chyb.

Integrita bezpečnosti a požadavky na bezpečnost

- **Integrita bezpečnosti** (*Safety Integrity*) – pravděpodobnost, s jakou bude bezpečnostní systém uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu.
- **Integrita bezpečnostního softwaru** (*Software Safety Integrity*) – míra vyjadřující pravděpodobnost, s jakou bude software v PE plnit své funkce související s bezpečností za všech stanovených podmínek a po stanovenou dobu.
- **Integrita bezpečnosti hardwaru** (*Hardware Safety Integrity*) – část integrity bezpečnosti systémů souvisejících s bezpečností týkající se náhodných poruch hardwaru v nebezpečném režimu poruchy.
- **Úroveň integrity bezpečnosti** (*Safety Integrity Level – SIL*) – diskrétní hodnota (jedna ze čtyř možných – SIL 1 – SIL 4) pro stanovení požadavků na integritu bezpečnosti bezpečnostních funkcí přiřazených E/E/PE systémům souvisejícím s bezpečností, kde SIL 4 znamená nejvyšší a SIL 1 nejnižší úroveň integrity bezpečnosti.
- **Specifikace požadavků na bezpečnost** (*Safety Requirements Specification*) – specifikace obsahující všechny požadavky na bezpečnostní funkce, které musejí systémy související s bezpečností plnit.

- **Specifikace požadavků na bezpečnostní funkce** (*Safety Functions Requirements Specification*) – specifikace obsahující požadavky na bezpečnostní funkce, které musejí systémy související s bezpečností plnit.
- **Specifikace požadavků na integritu bezpečnosti** (*Safety Integrity Requirements Specification*) – specifikace obsahující požadavky na integritu bezpečnosti bezpečnostních funkcí, které musejí systémy související s bezpečností plnit.

V celém souboru ČSN EN 61508 a v i této práci je používána celá řada dalších termínů a zkratek, jejichž přesnou definici je možné nalézt v ČSN EN 61508-4.

2.3 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.

Jednotlivé přístupy se pro příslušné obory mohou zásadně lišit v procesu posuzování rizika. Není možné stanovit jednotný postup hodnocení, který by byl aplikovatelný ve všech oborech. Jednotlivé obory si žádají naplnění specifických požadavků daných norem, které byly vytvořeny pro konkrétní oblasti s cílem nejlépe pokrýt speciální potřeby. Detailní porovnání různých oborů lze nalézt například v [2], kde se porovnává množství hodnocených faktorů, jejich

kvantifikace i výsledné zpracování pro stanovení potřebné úrovně spolehlivosti bezpečnostního systému.

2.4 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. Funkční bezpečnost zahrnuje širokou škálu zařízení, která se používají pro zajištění bezpečnostních systémů – blokovací spínače, světelné clony, ochranná relé, elektronické bezpečnostní systémy, ochranné stykače a další podobné prostředky. Ty buď samostatně, nebo společně vytvářejí bezpečnostní systém, který vykonává specifické bezpečnostní funkce. Jinými slovy se jedná o tu část bezpečnosti, na které závisí správná činnost zařízení a která zajišťuje jeho bezpečnost.

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.

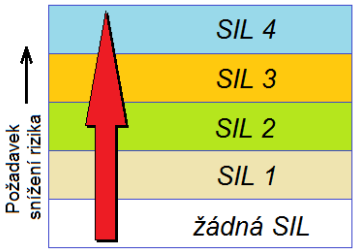
2.5 Technická bezpečnost

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. Tedy zařízení musí být zajištěno proti vzniku nebezpečného stavu, který by mohl vyvolat určité potenciálně nebezpečné jevy vedoucí k ohrožení osob nebo destrukci vlastního nebo jiného zařízení.

2.6 Integrita bezpečnosti

Je patrné, že systém může vykonávat řadu funkcí vytvořených pro různé operace, které jsou pro chod celého systému rozdílně důležité. Porucha méně důležité funkce není tak významná, než kdyby došlo k selhání hlavní funkce, čímž by systém přestal plnit požadovanou funkci, pro kterou byl navržen. Významu důležitých funkcí je věnována velká pozornost a z hlediska technického provedení musí mít i vyšší spolehlivost než funkce ostatní, méně důležité. Zvlášť významné a důležité jsou funkce bezpečnostní mající za úkol zajištění bezpečnosti. Platí, že čím vyšší je očekávaná bezpečnost, tím menší smí být výskyt nebezpečných poruch. Dopady selhání jednotlivých systémů se obecně liší a tím je kladen i rozdílný požadavek na pravděpodobnost jejich selhání. Pro pravděpodobnost (míru) četnosti výskytu nebezpečných poruch se zavádí nový pojem – integrita bezpečnosti (*Safety Integrity* – úplnost, celistvost, neporušenost).

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 2: Vztah úrovně SIL a požadavků na snížení rizika

Integrita bezpečnosti není určena pouze číselným rozmezím, ale závisí na splnění i dalších požadavků ve všech činnostech spojených s celým procesem návrhu bezpečných systémů. Integrita bezpečnosti určuje jednotlivé kategorie – úrovně, tzv. úroveň integrity bezpečnosti (*Safety Integrity Level* – SIL). 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.

Jednotlivé úrovně integrity bezpečnosti také vyžadují určité techniky, znalosti a zkušenosti pro dosažení výsledného snížení rizika.

SIL 4: Nejvyšší cíle a nejnáročnější na splnění, vyžadující nejmodernější techniky.

SIL 3: Méně náročné než SIL 4, ale stále vyžadují použití sofistikovaných návrhových technik.

SIL 2: Požaduje dobrý návrh a provozní praxi na úrovni srovnatelné se standardem ISO 9000.

SIL 1: Minimální úroveň, ale stále požaduje dobrou praxi s návrhem.

<SIL 1: Uvedeno (v ČSN EN 61508 a dalších dokumentech) jako "nesouvisející s bezpečností" z hlediska dodržování.

Poslední uvedená úroveň, se kterou se lze setkat <*SIL 1*, je někdy označována jako *SIL 0*, nebo ***žádná SIL*** a vztahuje se na zařízení, pro která nejsou kladeny z hlediska bezpečnosti žádné požadavky.

Podle normy ČSN EN 61508 je možné systém rozdělit dle jeho režimu provozu do tří skupin. Pro jednoduchost lze tyto z pohledu pravděpodobnosti výskytu poruchy sloučit do dvou skupin:

- Režim s nízkým (malým) vyžádáním
- Režim s vysokým (trvalým) vyžádáním nebo souvislý režim

V prvním případě jde o zařízení, kde činnost bezpečnostní funkce zajišťující převedení zařízení do bezpečného stavu je pouze na vyžádání a četnost vyžádání není vyšší než jednou za rok. U těchto zařízení se určuje pravděpodobnost selhání na vyžádání – PFD (*Probability of Failure on Demand*). Ve druhé skupině, tj. režim

s vysokým vyžádáním, je četnost vyžádání vyšší než jednou za rok, nebo je zařízení činné nepřetržitě. Pro tyto zařízení se určuje střední frekvence nebezpečné chyby za hodinu – PFH (*Probability of Failure per Hour*).

Určení režimu provozu zařízení je dalším rozhodujícím faktorem při stanovení cílové pravděpodobnosti výskytu nebezpečných poruch. Jednotlivé úrovně SIL pro oba režimy provozu jsou uvedeny v následující tabulce.

Tabulka 1: Úrovně integrity bezpečnosti – cílové míry poruch pro bezpečnostní funkci pracující v režimu provozu s nízkým nebo vysokým vyžádáním.

Úroveň integrity bezpečnosti	Režim s nízkým vyžádáním (PFD avg)	Režim s vysokým vyžádáním (souvislý režim) (PFH)
SIL 4	$\geq 10^{-5}$ až $< 10^{-4}$	$\geq 10^{-9}$ až $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ až $< 10^{-3}$	$\geq 10^{-8}$ až $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ až $< 10^{-2}$	$\geq 10^{-7}$ až $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ až $< 10^{-1}$	$\geq 10^{-6}$ až $< 10^{-5}$

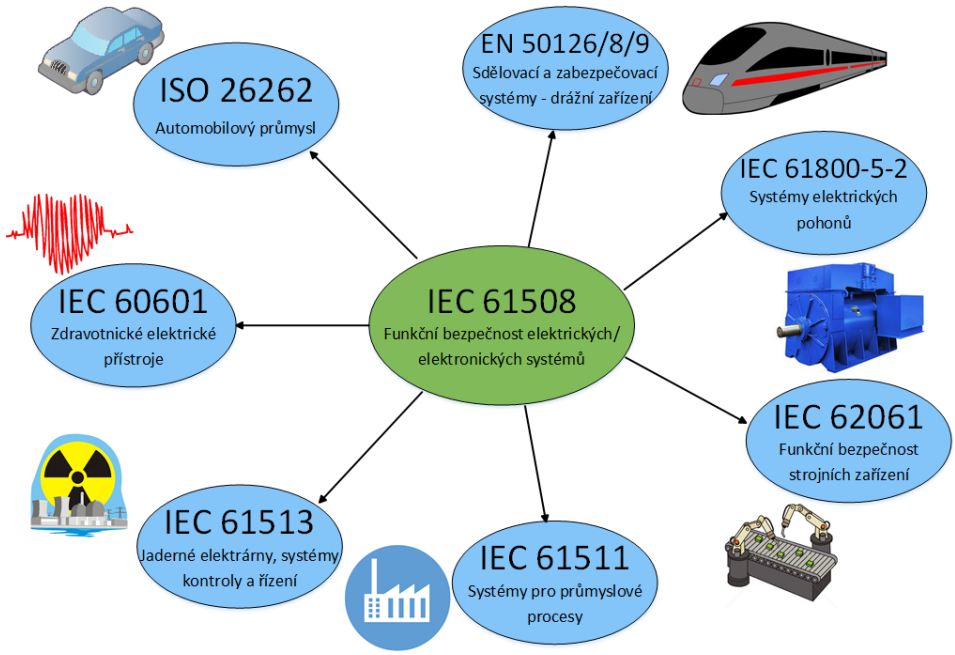
Porovnáním hodnot v tabulce zjistíme, že pravděpodobnosti výskytu nebezpečných poruch se pro stejné úrovně SIL liší o 10^4. Je to proto, že od systémů pracujících na vyžádání je požadována činnost méně než jednou za rok, čímž je dán rozdíl mezi hodnotami pravděpodobností (uvažuje se, že rok má 10 000 hodin).

Kategorie SIL lze také přeneseně chápat jako další úkoly, které je nutné splnit, aby bylo možné prokázat dosažení určité úrovně SIL. U jednoduchých systémů založených na jednoduché hardwarové konstrukci to lze jednoduše prokázat použitím údajů o četnosti poruch. Úroveň SIL tímto způsobem nelze prokázat u složitých systémů a především u programů (software), ve kterých poruchy nejsou náhodné, ale systematické, a nelze tak spolehlivě prokázat četnost nebezpečných poruch. [3]

2.7 Funkční bezpečnost v různých oborech

V této kapitole je zmíněno několik dalších odvětví, ve kterých je vhodné se problematikou spolehlivosti a bezpečnosti systémů zabývat. Samozřejmě cílem

všech firem produkujících elektronické a jiné systémy je splňovat určité požadavky na kvalitu a bezpečnost. Ne všechny podléhají nutnosti projít procesem tak důsledného schválení výrobku pro jeho používání, jako je tomu například u leteckých, jaderných, drážních a dalších podobných aplikací, kde je riziko nebezpečí v případě poruchy obrovské.



Obrázek 3: Návaznost funkční bezpečnosti s obecnou normou IEC 61508.

Jaká specifika a příslušné normy se konkrétních oblastí týkají, naznačuje obrázek 3. Výpis uvedených dokumentů není vyčerpávajícím výčtem a je vždy důležité danou oblast důkladně prostudovat. Velká část hodnotících kritérií je podobná pro všechny oblasti. Tento fakt je dán tím, že většina předpisů pro splnění požadavků na bezpečnost vychází ze společné normy ČSN EN 61508. Tato norma je obecnou pro všechny dílčí oblasti.

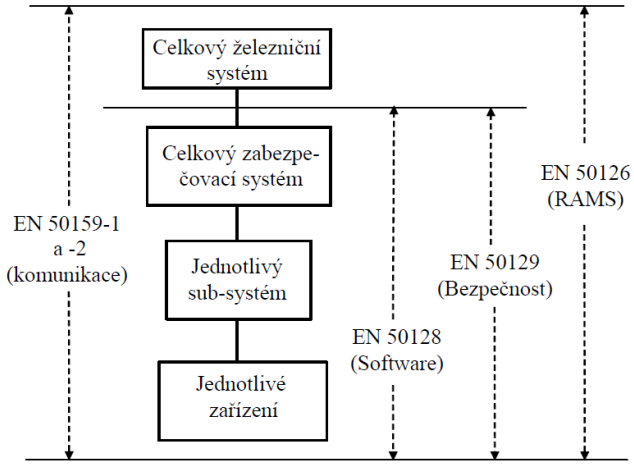
Přestože všechny normy pro jednotlivá odvětví vycházejí ze společného základu, nelze normy pro konkrétní oblasti mezi sebou zaměňovat. Mnohdy přístupy vychází z historického hlediska, kdy se konkrétní potřeby promítaly do příslušných norem, a v jiných oblastech nemají žádné opodstatnění.

V následující části jsou detailněji popsány přístupy norem železniční zabezpečovací techniky, automobilového průmyslu a výkonových pohonů, protože

blíže souvisí s předmětem této práce. Ostatní zmíněné oblasti (viz obrázek 3) jsou daleko specifičtější a jejich zkoumání je mimo záběr této práce.

2.7.1 Zabezpečovací technika ČSN EN 5012x

Všechna zařízení používaná v oblasti železniční zabezpečovací techniky musí být vždy schválena příslušnými orgány, pokud jsou použita na místech, kde by mohla způsobit ohrožení bezpečnosti. Předpisy, definice nebo požadavky na uznání a schválení všech drážních zařízení, včetně železničních zabezpečovacích zařízení, stanovuje soubor norem ČSN EN 50126, ČSN EN 50129, ČSN EN 50128 (viz obrázek 4) a některé další související normy (ČSN EN 50159-1, ČSN EN 50159-2).



Obrázek 4: Rozsah platnosti a obsah drážních norem. [4]

Tyto normy mají sjednotit přístup s danou problematikou ve všech zemích EU a umožnit tak snadnější vzájemné schvalování zařízení mezi jednotlivými státy.

Základním cílem normy ČSN EN 50126 [4] je poskytnout všem provozovatelům drážních zařízení procesy pro specifikaci a prokázání požadavků na RAMS (*Reliability, Availability, Maintainability and Safety*). RAMS zavádí důležitý přístup k managementu bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti. Snahou této normy je podpořit obecné chápání a přístup k managementu vývoje zařízení ve všech etapách životního cyklu.

Norma ČSN EN 50129 [5] definuje úrovně integrity podobně jako ČSN EN 61508 ve čtyřech kategoriích – SIL 1 nejnižší úroveň a SIL 4 nevyšší úroveň. Aby bylo možné zařízení zařadit do příslušné kategorie, musí vyhovovat všem faktorům:

- Podmínky řízení kvality
- Podmínky řízení bezpečnosti
- Požadavky na technickou bezpečnost
- Dosažení kvantitativního bezpečnostního cíle

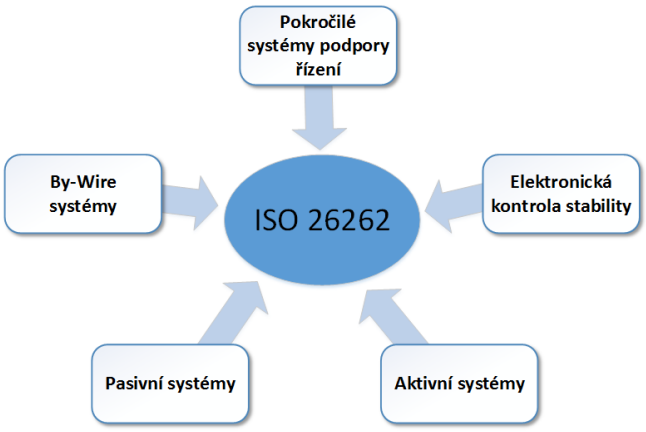
Odpovídající úrovně systému bude dosaženo pouze při splnění všech těchto podmínek, pro které norma ČSN EN 50129 určuje techniky, postupy a opatření v řízení náhodných a systematických poruch. Studiem normy lze nalézt významné rozdíly v uplatňovaných požadavcích pozorovatelných mezi skupinami SIL 1/2 a SIL 3/4. S přihlédnutím k velmi obtížnému prokazování dostatečnosti nižších úrovní integrity bezpečnosti je drtivá většina železniční zabezpečovací techniky v úrovni SIL 4.

Drážní normy mají oproti ČSN EN 61508 užší aplikační zaměření, protože požadavky byly utvářeny desítky let pomocí provozních zkušeností a událostí. Velký rozdíl je v přístupu k technické bezpečnosti. Norma ČSN EN 61508 je zaměřena především na funkční bezpečnost. Technické bezpečnosti se věnuje jen okrajově, zatímco drážní normy jsou v tomto ohledu daleko přísnější. Další důležitý rozdíl představují kvantitativní kritéria pro určení THR nebo PHD/PFH. Zatímco ČSN EN 61508 rozlišuje režimy provozu s nízkým vyžádáním (PFD) a režimy provozu s vysokým (nepřetržitým) vyžádáním (PFH), u kterých výrazně rozlišuje požadavky SIL, norma ČSN EN 50129 oba druhy sjednotila do jednoho kritéria (míra přijatelného rizika – THR – *Tolerable Hazard Rates*), které odpovídá režimu s vysokým vyžádáním. Životní cyklus, doporučení, cíle a další procesní stránky tvořící jádro drážních norem se ale od ČSN EN 61508 výrazně neodlišují, jelikož z ní vycházejí. [4][5][6][7]

2.7.2 Automobilový průmysl ISO 26262

Základem pro návrh a hodnocení elektronických systémů souvisejících s bezpečností v automobilovém průmyslu je mezinárodní norma ISO 26262 – *Functional safety – Road vehicles* [8] zahrnující i samotné dodavatele hardwaru a softwaru nebo vývojové nástroje, které se v automotivní oblasti používají.

Stejně jako ostatní normy musí i ISO 26262 stále zohledňovat zvyšující se složitost elektronických palubních systémů a úměrně tomu vést ke zvýšenému úsilí poskytovat bezpečné systémy. Například moderní automobily zcela běžně používají By-Wire systémů konkrétně pro plynový pedál. Poloha pedálu je snímána elektronickým čidlem a pomocí signálů informuje elektronickou jednotkou o své poloze, která údaj vyhodnotí společně s dalšími faktory (rychlost vozidla, otáčky motoru) pro správné nastavení tělesa škrtící klapky. Potenciálně riziková řešení – například zmíněné řízení pomocí By-Wire, nebo systémy elektronické kontroly stability – jsou v automobilovém průmyslu výzvou k testování a validaci těchto již tak složitých systémů, a proto cílem normy ISO 26262 je poskytnout jednotný bezpečnostní základ pro všechny automobilové elektronické systémy, který definuje požadavky pro jednotlivé procesy, určuje metody a nástroje používané během vývoje a stanovuje funkce systému vztahující se k bezpečnosti.



Obrázek 5: Norma ISO 26262 – příklady oblastí.

Úroveň integrity bezpečnosti v automobilovém sektoru je označována zkratkou ASIL (*Automotive Safety Integrity Level*) a obdobně jako v ČSN EN 61508 je rozdělena do čtyř tříd – od úrovně ASIL A až po ASIL D, přičemž do úrovně ASIL

D patří nejdůležitější bezpečnostní procesy s nejpřísnějšími předpisy testování vyžadující nejvyšší míru snížení rizika. Naopak úroveň ASIL A postačuje pro bezpečnostní funkce s relativně nízkou kritičností. Norma ISO 26262 konkrétně určuje minimální požadavky na testování v závislosti na úrovni ASIL, což významně pomáhá při určování konkrétních metod ve fázi testování.

Norma ISO 26262 poskytuje předpisy a doporučení v rámci celého procesu vývoje výrobku od návrhu až po vyřazení z provozu. Je zde popsáno, jak u systému nebo jeho části stanovit úroveň přijatelné míry rizika a jak celý proces vývoje a testování dokumentovat.

Klíčové části normy ISO 26262:

- Poskytuje životní cyklus automobilu (management, vývoj, výroba, provoz, servis, vyřazení z provozu) a podporuje přizpůsobení nezbytných činností při těchto fázích životního cyklu.
- Poskytuje specifický přístup pro automobilový průmysl se stanovením jednotlivých tříd rizika (ASIL).
- Používá třídy ASIL, které určují bezpečnostní požadavky pro dosažení přijatelného zbytkového rizika.
- Uvádí požadavky na ověření, zda bylo dosaženo přijatelné úrovně bezpečnosti.

Struktura ISO 26262 se velmi dobře přizpůsobuje aktuálním bezpečnostním pojmům v průmyslu a ukazuje se, že řada firem v posuzování rizik vidí velké výhody a snaží se jejich analýzy a testování aplikací přesunout do rané fáze procesu vývoje. [8][9]

2.7.3 Systémy elektrických výkonových pohonů ČSN EN 61800-5-2

Poněkud méně známá norma ČSN EN 61800-5-2 [10] je s výhodou použitelná jako reference pro systémy výkonových elektrických pohonů s možností nastavení

jejich rychlosti – jinak řečeno s proměnnými otáčkami (PDS – *Power Drive Systems*).

Norma specifikuje požadavky a uvádí doporučení pro návrh a vývoj systémů s ohledem na jejich bezpečnost. Stanovuje nutná opatření týkající se bezpečnosti systémů výkonových pohonů v rámci obecné normy ČSN EN 61508 s ohledem na použití těchto systémů jako dílčích částí bezpečného zařízení. Jedná se o normu usnadňující integraci bezpečnosti frekvenčních měničů, budičů a dalších výkonových systémů do aplikací jako jsou například obráběcí stroje, válcovací stolice, protlačovací lisy, dopravníky nebo trakční pohony.

Vzhledem k určení této normy pro systémy výkonových pohonů je striktně stanoven režim jejich provozu. Jedná se o velmi náročné aplikace vyžadující režim nepřetržitého provozu nebo režim s vysokým vyžádáním. Pro připomenutí norma ČSN EN 61508 rozlišuje režim s nízkým vyžádáním, režim s vysokým vyžádáním a režim s trvalým vyžádáním. Režim s nízkým vyžádáním je normou ČSN EN 61800-5-2 považován za nevhodný pro systémy výkonových pohonů.

V souvislosti s aplikačním určením tato norma uvádí konkrétní bezpečnostní funkce pro systémy výkonových pohonů, které jsou určeny pro aplikace související s bezpečností. Pro jednotlivé bezpečnostní funkce se zde rozlišuje, zda mají povinnost jen monitorovat a reagují pouze na překročení mezí, nebo musí zahájit reakci na poruchu detekovanou diagnostickými nástroji. Vedle řady uvedených bezpečnostních funkcí pro zastavení nebo sledování překročení mezních hodnot je možné systém výkonového pohonu vybavit vlastní specifickou bezpečností funkcí vhodnou pro konkrétní aplikaci. Také je možné využít dalších externích prvků (například mechanická brzda), které mohou být využity jako další technická opatření udržení bezpečnosti.

Norma definuje úrovně integrity bezpečnosti obdobně jako obecná norma ČSN EN 61508 do jednotlivých kategorií s jedním rozdílem. Aplikace systémů výkonových pohonů provádějících bezpečnostní funkce mohou být v úrovni integrity bezpečnosti ne větší než SIL 3. Pokud by bylo potřeba navrhovat bezpečnostní funkce s úrovní integrity bezpečnosti SIL 4, musely by se aplikovat požadavky podle obecné normy ČSN EN 61508.

3 Metodika návrhu systémů

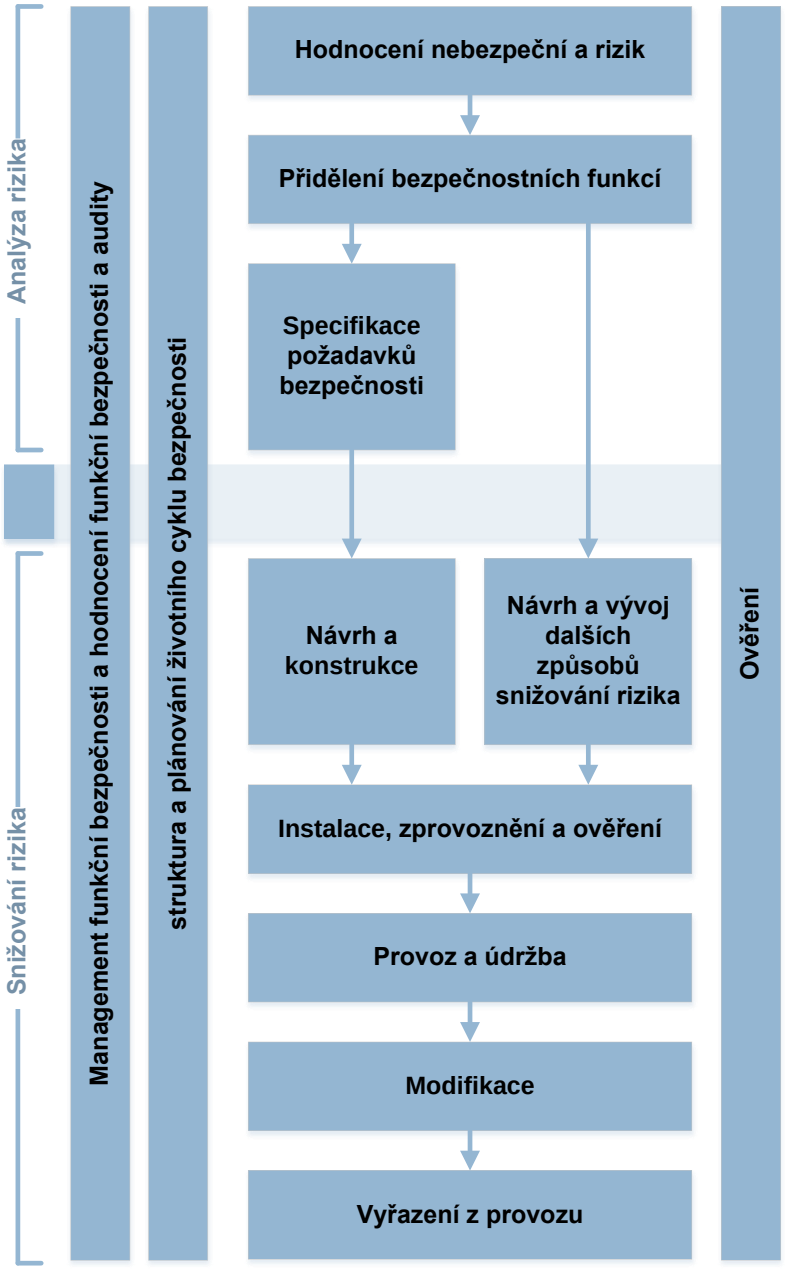
Cílem této kapitoly je popsat jednotlivé kroky v procesu návrhu elektronického systému určeného pro aplikace vyžadující jistou úroveň bezpečnosti se zaměřením na hardwarovou část. Jelikož by tato vzniklá metodika měla být nápomocná pro obecný návrh elektronických systémů, je logicky jejím základem soubor norem ČSN EN 61508. Tyto normy uvádí jednotlivé cíle a požadavky, které je nutné splnit, aby bylo možné prokázat určitou úroveň integrity bezpečnosti.

Aby bylo možné požadavky splnit, je nutné normou stanovené cíle objasnit, neboť lze jen velmi těžko zpracovávat konkrétní opatření bez pochopení možných důsledků. Proto bylo mou snahou v metodice teoreticky rozepsat klíčové kroky návrhu a podrobně vysvětlit významy stanovených cílů a požadavků tak, aby bylo možné pro navrhovaný systém deklarovat shodu s požadavky normy ČSN EN 61508.

Struktura následujících kapitol vyjadřuje postupné procesní kroky návrhu částečně návazné na strukturu obecné normy pro bezpečnost. Stejně jako v této normě jsou kroky seřazeny chronologicky podle fází životního cyklu. Převážná část metodiky z této normy vychází, ale pro některé části fází, které v ní nejsou srozumitelně definovány, je využito principů a technik z jiných norem nebo dalších uznávaných publikací.

3.1 Management funkční bezpečnosti

Funkční bezpečnost a její aplikace na návrh systému splňujícího definovanou úrovní bezpečnosti není jen koncept a návrh bezpečnostní funkce. Jde o souhrn veškerých aktivit spojených s přípravou, vývojem a výrobou bezpečného systému a dále s jeho provozem, modifikacemi a vyřazením z provozu. Veškeré tyto činnosti jsou zahrnuty do tzv. životního cyklu celkové bezpečnosti a správa nad nimi je pod hlavičkou managementu funkční bezpečnosti (viz obrázek 6).



Obrázek 6: Fáze životního cyklu celkové bezpečnosti.

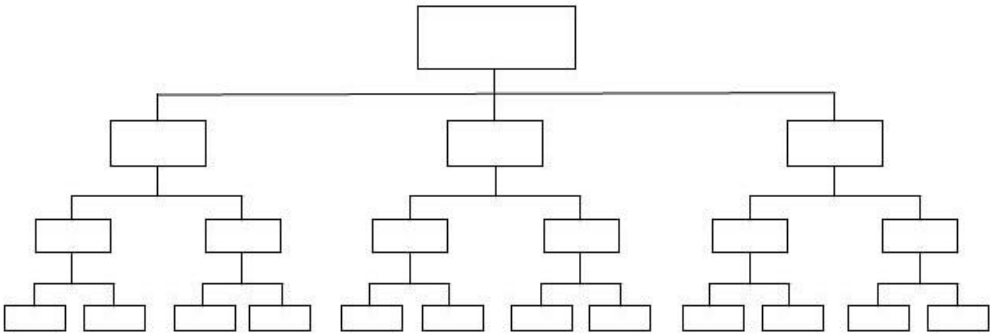
Management funkční bezpečnosti má dva základní cíle:

- stanovení odpovědností za systém související s bezpečností,
- stanovení činností, které je potřeba provádět.

Hlavním důvodem, proč byly normativně popsány procesy a postupy aplikace funkční bezpečnosti, bylo snížení rizika na úroveň, která je společností přijatelná. Poruchám se obecně nelze vyhnout a s jejich důsledky je nutno počítat. Mohou být různého charakteru – ekonomického, environmentálního nebo bezpečnostního

(mající vliv na zdraví a životy osob). Veškeré postupy funkční bezpečnosti se týkají posledního typu důsledku – bezpečnosti osob.

V každém projektu figuruje několik lidí, kteří mají klíčovou roli. Každý z těchto hráčů má specifické povinnosti, které, pokud se uskuteční podle předepsaného způsobu, zajistí úspěšný projekt, jelikož obecně většina nehod je zaviněna alespoň z části člověkem. Taktika a strategie pro dosažení funkční bezpečnosti musí být stanovena spolu s prostředky pro hodnocení jejich dosažení a prostředky s nimiž se komunikuje uvnitř organizace. Jedním z předpokladů dobré komunikace uvnitř organizace je její vhodná struktura. Organizace jsou většinou rozděleny do hierarchické struktury – nadřízený x podřízený, vedoucí skupiny x člen skupiny, koordinátor skupin x vedoucí skupiny atd. viz například obrázek 7.



Obrázek 7: Hierarchická struktura managementu.

Jednotlivé skupiny mají své vedoucí pracovníky, kteří mají za celé organizační celky (oddělení) odpovědnost, přímo je řídí a kontrolují. Oddělení se v hierarchickém managementu zaměřují na svou část projektu. Tato situace má za důsledek, že jsou jednotlivá oddělení specializovaná na svůj cíl. Úkolem vedoucích skupin a vyššího managementu je koordinovat jednotlivé skupiny a vést je podle plánu, aby byly splněny podmínky pro bezpečnost.

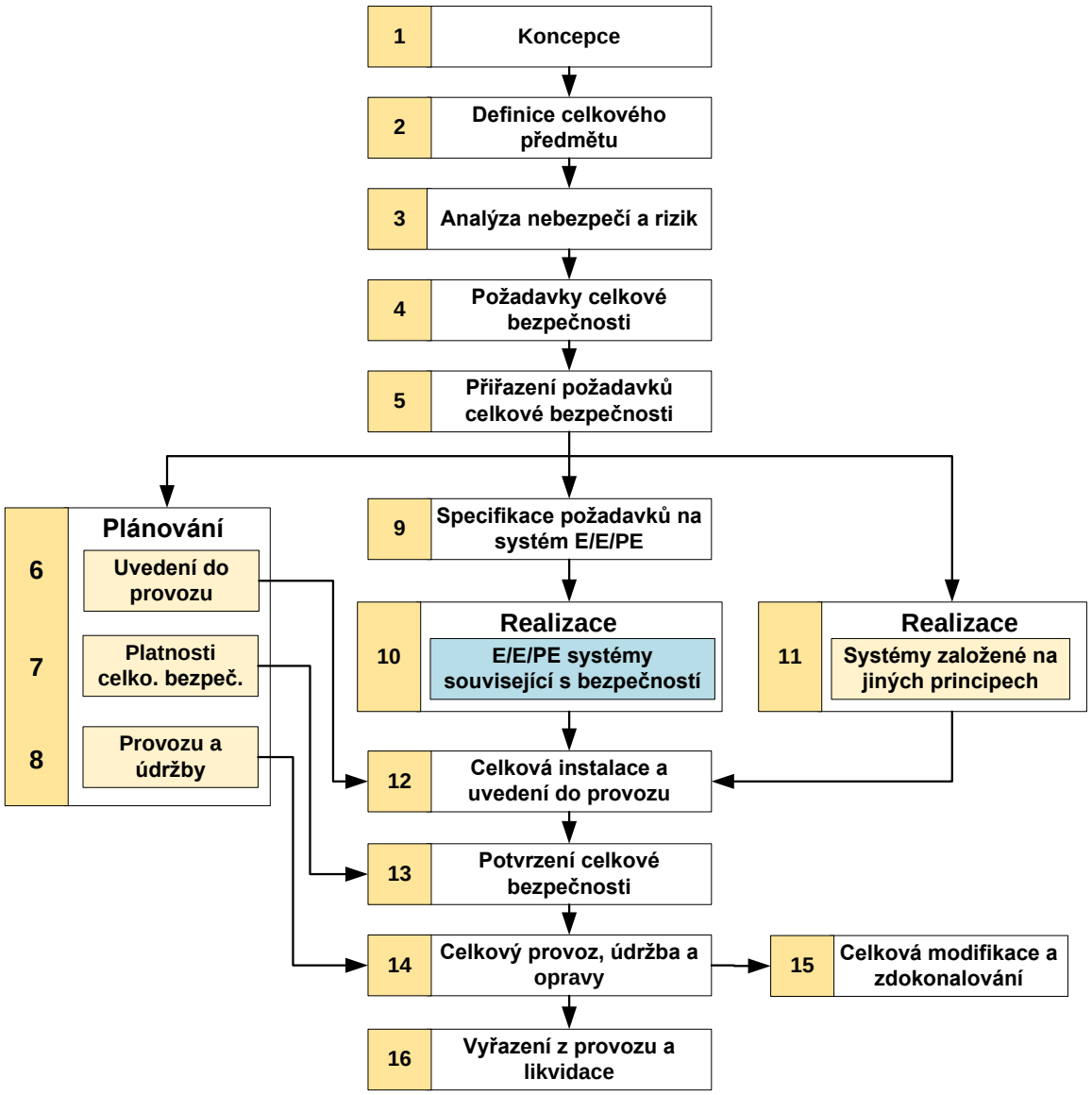
Pro dosažení a udržení cílů managementu funkční bezpečnosti stanovených normou ČSN EN 61508 musí být stanoveny a především dokumentovány požadavky, které uvádí tabulka 2.

Tabulka 2: Seznam nezbytných aktivit, které musí být vytvořeny a dokumentovány pro zajištění managementu bezpečnosti

#	
1	Jmenování odpovědnosti osob za celkovou funkční bezpečnost i za jednotlivé fáze.
2	Stanovení taktiky a strategie pro dosažení funkční bezpečnosti. Hodnocení taktik a strategií. Stanovení prostředků, s nimiž se komunikuje uvnitř organizace.
3	Určení a informování všech osob, oddělení a organizací odpovědných za činnosti na systému (včetně osob zodpovědných za ověřování a odhad funkční bezpečnosti a, kde je to příslušné, licencování pravomocí nebo regulačních bezpečnostních orgánů).
4	Stanovení informací, které mají být sdělovány mezi příslušnými stranami, a popis, jak tato komunikace bude prováděna.
5	Stanovení postupů pro nepřetržité sledování podnětů a doporučení vycházejících z: • analýzy nebezpečí a rizik • odhadu funkční bezpečnosti • ověřovacích činností • činností potvrzování platnosti • managementu konfigurace
6	Stanovení postupů a doporučení, která zajišťují, aby všechny detekované nebezpečné události byly analyzovány a minimalizovala se pravděpodobnost jejich opakování.
7	Stanovení požadavků na periodické funkční audity s definováním jejich frekvence a úrovně nezávislosti.
8	Vytvoření postupů pro modifikace a schvalování a autorizaci modifikací
9	Udržování správných informací o nebezpečí a nebezpečných událostech, bezpečnostních funkcích.
10	Vytvoření postupů pro management konfigurace navrhovaných systémů během fází celého životního cyklu celkové bezpečnosti.
11	Zajištění školení a dostupnost informací pro bezpečnostní služby.
12	Stanovení technických aktivit nezbytných pro zajištění funkční bezpečnosti.
13	Zajištění potřebných školení pro udržení potřebných technických znalostí a kompetencí příslušných ke specifickým službám, které mají odpovědné osoby vykonávat.

3.2 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 8.



Obrázek 8: Životní cyklus celkové bezpečnosti dle ČSN EN 61508

Jednotlivé bloky na obrázku 8 představují nejdůležitější kroky v procesu návrhu systému souvisejícího s bezpečností a šipky znázorňují pořadí, v jakém se jednotlivé úkony mají provádět. Bohužel v praxi je velmi často velká část

celého hodnocení omezena na posouzení, zda navrhovaná konfigurace konstrukce (architektura) splňuje cílovou pravděpodobnost selhání. Tomuto přístupu je dobré se vyvarovat. Většina nových norem zabývajících se funkční bezpečností, včetně ČSN EN 61508, vyžaduje široký přístup zahrnující kontrolu nad všemi činnostmi životního cyklu z důvodu systematického zajišťování všech činností nutných pro dosažení požadované úrovně integrity bezpečnosti.

V životním cyklu celkové bezpečnosti představuje první blok „Koncept“ důkladné prozkoumání a pochopení celého navrhovaného (řídicího) systému a především jeho prostředí, ve kterém by měl pracovat. Druhý blok „definice zařízení“ vyžaduje potřebu poznat systém z pohledu rizika. Ve třetím kroku se určují úrovně rizika a analyzuje se jejich přípustnost. V následujícím bloku se stanovují požadavky na bezpečnost zajišťující potřebné zmenšení rizika, které jsou převedeny do konkrétní podoby a v dalším kroku přiřazeny jednotlivým systémům. Následuje rozdělení do dvou[1] větví: „Plánování“ a „Realizace“. V tomto kroku se práce rozděluje do dvou směrů. Jak už samotný název napovídá, v jednom bloku jsou práce směřovány na plánování budoucích fází životního cyklu. Paralelně s tímto blokem probíhají práce na samotném návrhu E/E/PE systému a systému založeném na jiných principech, které pokračují instalací, zprovozněním a po ověření provozem, případně opravami. Poslední blok životního cyklu je věnován ukončení provozu bezpečnostního systému.

Životní cyklus bezpečnosti tedy představuje nejenom vývoj systému, ale i jeho dílčí životní fáze, jak je představují poslední 4 bloky. Daný model je jen určitým přiblížením a v žádném případě nemůže nahradit kvalitní projektování a řízení. Může ale vhodně posloužit jako podpůrná pomůcka.

Pro zajištění shody s ČSN EN 61508 by se měl použít uvedený životní cyklus celkové bezpečnosti. Ten se vztahuje na všechny elektrické a programové aspekty zařízení týkající se bezpečnosti. Pokud tedy systém související s bezpečností obsahuje elektrické, elektronické, programovatelné elektronické, nebo dokonce i mechanické a pneumatické elementy, pak se norma vztahuje na všechny prvky

[1] Ve skutečnosti po kroku přiřazení požadavků následuje rozdělení do tří větví: Plánování, Realizace E/E/PE systému souvisejícího s bezpečností a Realizace systému založeného na jiných principech.

tohoto systému. Norma tedy nevylučuje použití "jiných technologií" v místech, kde se jejich použitím docílí snížení rizika.

Norma sice připouští použití odlišného životního cyklu, ale pod podmínkou splnění cílů a požadavků všech kapitol normy. Ovšem ty jsou odrazem uvedeného životního cyklu a není tak důvod se výrazně od nastíněného životního cyklu odlišovat.

Tabulka 3: Přehled fází realizace životního cyklu celkové bezpečnosti.

Fáze životního cyklu		Předmět	Cíl
Označení v obr.	**Název fáze**		
1	Koncept	EUC (řízené zařízení) a jeho prostředí (fyzické, legislativní)	Dostatečně zvýšit pochopení EUC a jeho prostředí tak, aby bylo možné provádět další činnosti životního cyklu bezpečnosti.
2	Definice celkového předmětu	EUC a jeho prostředí	Vymezit hranice EUC a systém řízení EUC. Stanovit předmět analýzy nebezpečí a rizik.
3	Analýza nebezpečí a rizik	EUC, systém řízení EUC a lidské faktory (může být nutné provedení více než jedné analýzy nebezpečí a rizik)	Určit nebezpečí a nebezpečné události EUC a systému řízení EUC (ve všech režimech provozu) pro všechny rozumné předvídatelné okolnosti včetně podmínek závad a nesprávného použití. Stanovit sledy události vedoucích k určeným nebezpečným událostem.
4	Požadavky celkové bezpečnosti	EUC, systém řízení EUC a lidské faktory	Vypracovat specifikaci požadavků celkové bezpečnosti z hlediska požadavků na bezpečnostní funkce a integritu bezpečnosti pro E/E/PE systémy související s bezpečností a jiných opatření pro snížení rizika za účelem dosažená požadované funkční bezpečnosti.
5	Přiřazení požadavků celkové bezpečnosti	EUC, systém řízení EUC a lidské faktory	Přiřadit bezpečnostní funkce ze specifikace požadavků celkové bezpečnosti (jak požadavků na bezpečnostní funkce, tak požadavků na integritu bezpečnosti) určeným E/E/PE systémům souvisejícím s bezpečností, systémům souvisejícím s bezpečností založených na jiných technických principech a vnějším prostředkům pro snížení rizika. Přiřadit úrovně integrity bezpečnosti každé bezpečnostní funkci.
6	Plánování instalace a uvedení do provozu	EUC, systém řízení EUC. E/E/PE systémy související s bezpečností	Sestavit plán řízené instalace E/E/PE systémů souvisejících s bezpečností zajišťující dosažení požadované funkční bezpečnosti.

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

7	Plánování potvrzení platnosti bezpečnosti	EUC, systém řízení EUC a lidské faktory. E/E/PE systémy související s bezpečností	Vytvořit plán, který usnadní potvrzení platnosti celkové bezpečnosti E/E/PE systémů souvisejících s bezpečností.
8	Plánování provozu a údržby	EUC, systém řízení EUC a lidské faktory. E/E/PE systémy související s bezpečností	Vytvořit takový plán provozu a údržby E/E/PE systému souvisejících s bezpečností, který zajistí během provozu a údržby udržení požadované funkční bezpečnosti.
9	Specifikace požadavků na systém E/E/PE souvisejících s bezpečností	Systémy E/E/PE související s bezpečností	Definovat požadavky systému E/E/PE v rámci funkčních požadavků systému E/E/PE souvisejícího s bezpečností a požadavků integrity tohoto systému, aby se dosáhlo požadované funkční bezpečnosti.
10	Realizace systémů E/E/PE souvisejících s bezpečností	Systémy E/E/PE související s bezpečností	Postavit E/E/PE systémy související s bezpečností splňující specifikaci bezpečnostních požadavků na E/E/PE.
11	Specifikace a realizace jiných opatření pro snížení rizika	Jiná opatření pro snížení rizika	Vytvořit jiná opatření pro snížení rizika splňující požadavky na bezpečnostní funkce a požadavky na integritu bezpečnosti (není předmětem normy ČSN EN 61508).
12	Celková instalace a uvedení do provozu	EUC, systém řízení EUC. E/E/PE systémy související s bezpečností	Instalovat E/E/PE systémy související s bezpečností. Uvést do provozu E/E/PE systémy související s bezpečností.
13	Potvrzení platnosti celkové bezpečnosti	EUC, systém řízení EUC. E/E/PE systémy související s bezpečností	Potvrdit platnost, že E/E/PE systémy související s bezpečností splňují specifikaci požadavků na celkovou bezpečnost z hlediska požadavků na celkové bezpečnostní funkce a požadavků na celkovou integritu bezpečnosti při respektování přiřazených bezpečnostních požadavků E/E/PE systémům souvisejícím s bezpečnosti.
14	Celkový provoz, údržba a opravy	EUC, systém řízení EUC. E/E/PE systémy související s bezpečností	Provozovat, udržovat a opravovat E/E/PE systémy související s bezpečností tak, aby se udržela požadovaná funkční bezpečnost.
15	Celková modifikace a modernizace	EUC, systém řízení EUC. E/E/PE systémy související s bezpečností	Zajistit přijatelnou funkční bezpečnost E/E/PE systémů souvisejících s bezpečností jak během fáze modifikací, tak po jejím uskutečnění.
16	Vyřazení z provozu a likvidace	EUC, systém řízení EUC. E/E/PE systémy související s bezpečností	Zajistit přijatelnou funkční bezpečnost E/E/PE systémů souvisejících s bezpečností za okolnosti během a po provedení činnosti spojených s vyřazením EUC z provozu nebo jeho likvidace.

Následující kapitoly se věnují jednotlivým blokům životního cyklu bezpečnosti.

3.3 Koncept (fáze 1 ŽC)

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. Je nutné seznámit se se všemi fyzikálními vlivy prostředí, potenciálními zdroji nebezpeční, nebezpečnými událostmi, legislativními nařízeními, právními předpisy a dalšími vlivy, které mohou návrh a vývoj ovlivnit v průběhu dalších činností životního cyklu. K realizaci tohoto bodu je nutné:

- získat důkladné znalosti o EUC a jeho požadovaných řídících funkcích, jakožto i znalosti o fyzickém prostředí, kterými se realizuje EUC,
- stanovit potenciální zdroje nebezpečí a získat informace o jejich povaze (toxicita, nebezpečí výbuchu, apod.),
- získat informace o legislativním rámci, souvisejícím s celým systémem E/E/PE,
- vzít v úvahu nebezpečí, která mohou vzniknout interakcí mezi řešeným EUC a ostatními EUC (instalovanými, nebo plánovanými),
- vést u všech uvedených činností dokumentaci v rozsahu a smyslu podle konkrétní aplikace.

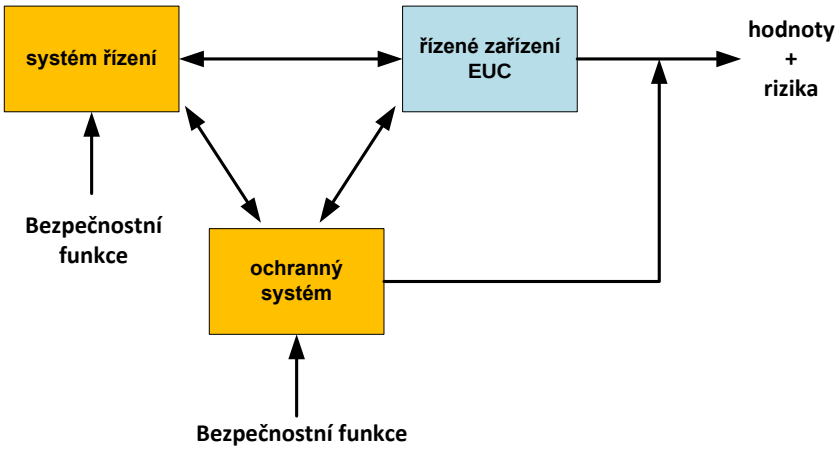
Výstupem 1. fáze životního cyklu (konceptu) by měla být dokumentace všech provedených analýz a informací týkajících se minimálně faktorů výše uvedených bodů, které shrnuje tabulka 4. Struktura každé organizace může být odlišná, a proto i dokumentace konceptu a všech dalších aktivit prováděných v průběhu celého životního cyklu návrhu bezpečného systému může být zpracovávána podle zavedených standardů. Ovšem pro splnění požadavků normy ČSN EN 61508 musí být dokumentovány minimálně uvedené aktivity.

Tabulka 4: Seznam nezbytných aktivit, které musí být analyzovány a dokumentovány ve fázi konceptu.

#	
1	Znalost řízeného zařízení a jeho řídicích funkcí
2	Znalost fyzického prostředí
3	Stanovení potenciálních zdrojů nebezpečí a jejich popis
4	Informace o bezpečnostních předpisech (národní i mezinárodní)
5	Interakce s jinými zařízeními a systémy v blízkosti

3.4 Definice systému (fáze 2 ŽC)

Druhým krokem životního cyklu je vymezení konkrétních částí, které budou předmětem analýz nebezpečí a rizik. Model, ze kterého norma ČSN EN 61508 vychází, je zobrazen na obrázku 9. Základ tvořený řízeným zařízením (EUC) vytváří spolu s řídicím systémem určité hodnoty (např. lisuje plechové díly, vyrábí elektřinu, ovládá železniční signalizaci), ale zároveň je zdrojem nebezpečí pro své okolí.



Obrázek 9: Model spojení systému řízení a EUC.

Jak dobře je systém popsaný, tak dobře lze odpovídat na otázky, co se stane při vzniku poruchy a jaká rizika mohou následovat. Jen dobře definované stavy a odezvy systému na vnější i vnitřní nehody mohou zajistit v průběhu analýz přesné

odpovědi na nejrůznější scénáře a sledy událostí vedoucích k možnému vzniku rizik.

Každé riziko spojené s EUC nebo jeho řídicím systémem musí být identifikováno a oceněno, zda je přijatelné (detailně se analýzou rizika zabývá následující kapitola). Každé riziko, které je shledáno nepřijatelným, je třeba zmenšit a to může vést ke změně uspořádání EUC nebo jeho řídicího systému. Pokud se riziko jeví stále jako nepřijatelné, je nutné buď vytvořit v řídicím systému bezpečnostní funkce, nebo zařízení doplnit jedním nebo několika ochrannými zařízeními (viz obrázek 9). Principiálně se doporučuje oddělit ochranný systém od systému řídicího.

Hranice mezi řídicím systémem a ochranným systémem na jednu stranu zajišťuje jejich nezávist, na druhou stranu ale musí zajistit mezi systémy spojení pro signály určené k monitorování a umožnit tak aktivní zásah ochranného systému v případě poruchy. Definice hraničních podmínek mezi systémy má své opodstatnění také při prokazování nezávislosti systému souvisejícího s bezpečností od systému nesouvisejícího.

Výstupem 2. fáze ŽC (definice systému) je podrobná dokumentace systému, včetně vymezení hranic a určení všech událostí, které mohou vyvolat nebezpečné události.

Tabulka 5: Seznam nezbytných aktivit, které musí být stanoveny a dokumentovány ve fázi definice systému.

#	
1	Definice všech částí systému, které budou předmětem analýzy nebezpečí a rizik (řídicí systém, řízený systém, ochranný systém)
2	Stanovení vnějších událostí, se kterými je třeba počítat v analýze nebezpečí a rizik (tedy v následujícím bodě)
3	Určení dílčích systémů, které mohou mít souvislost s nebezpečími zjištěnými v předchozím bodě
4	Určení všech předvídatelných událostí, které mohou vyvolat nebezpečné nehody (např. běžné typy poruch součástek, vady v procesech, lidské chyby, mechanismy závislých poruch, které mohou vyvolat sledy nehod apod.)

3.5 Analýza nebezpečí a rizik (fáze 3 ŽC)

Hlavním cílem správné aplikace funkční bezpečnosti je snížení rizika možnosti zranění lidí, velkých materiálních ztrát nebo poškození životního prostředí. Proto při aplikaci požadavků normy pro konkrétní technické řešení systému je třeba správně chápat podstatu rizika a způsob jeho hodnocení. Pokud není riziko v tomto kroku stanoveno korektně, mohou se v systému objevit nebezpečné poruchy, nebo nemusí být dosaženo optimálního řešení z ekonomického hlediska. Bezpečnostní systémy jsou pak navrhovány buď s nadměrnou, nebo nedostatečnou odolností proti systematickým a náhodným poruchám. Z toho pak vyplývají příslušné ekonomické a bezpečnostní důsledky. Úkolem je navrhnout systém, který by zabránil vzniku nebezpečných poruch, nebo alespoň ve smyslu bezpečnosti kontroloval jejich výskyt.

Obrázek 10: Obecná koncepce snižování rizik.

Riziko je výsledkem aktivace určitého nebezpečí a představuje pravděpodobnost, s jakou může dojít ke škodě či jinému negativnímu následku. Výklad pojmů riziko, nebezpečí a zdroje nebezpečí například podle [53] je:

Riziko

- je kvantitativní a kvalitativní vyjádření ohrožení, je to míra ohrožení, stupeň ohrožení

- tímto pojmem se vyjadřuje pravděpodobnost, že vznikne negativní jev a zároveň i jaké budou důsledky tohoto jevu
- vyjadřuje, kolikrát se negativní jev vyskytne a co způsobí
- definuje se jako kombinace pravděpodobnosti nežádoucí události a rozsahu, závažnosti možného zranění, škody nebo poškození zdraví.

Riziko má vždy dva rozměry:

- pravděpodobnost vzniku nebezpečné situace ohrožení
- závažnost možného následku

Nebezpečí

- stroje, materiály, technologie a pracovní činnosti se vyznačují tím, že mohou způsobit neočekávaný negativní důsledek - např. poškození člověka nebo majetku. Jde o nebezpečí nebo nebezpečné činnosti
- je to podstatná, ale skrytá vlastnost nebo schopnost něčeho (materiálu, stroje, pracovní činnosti), která muže zapříčinit vznik škody
- je to zdroj možného ohrožení nebo škody.

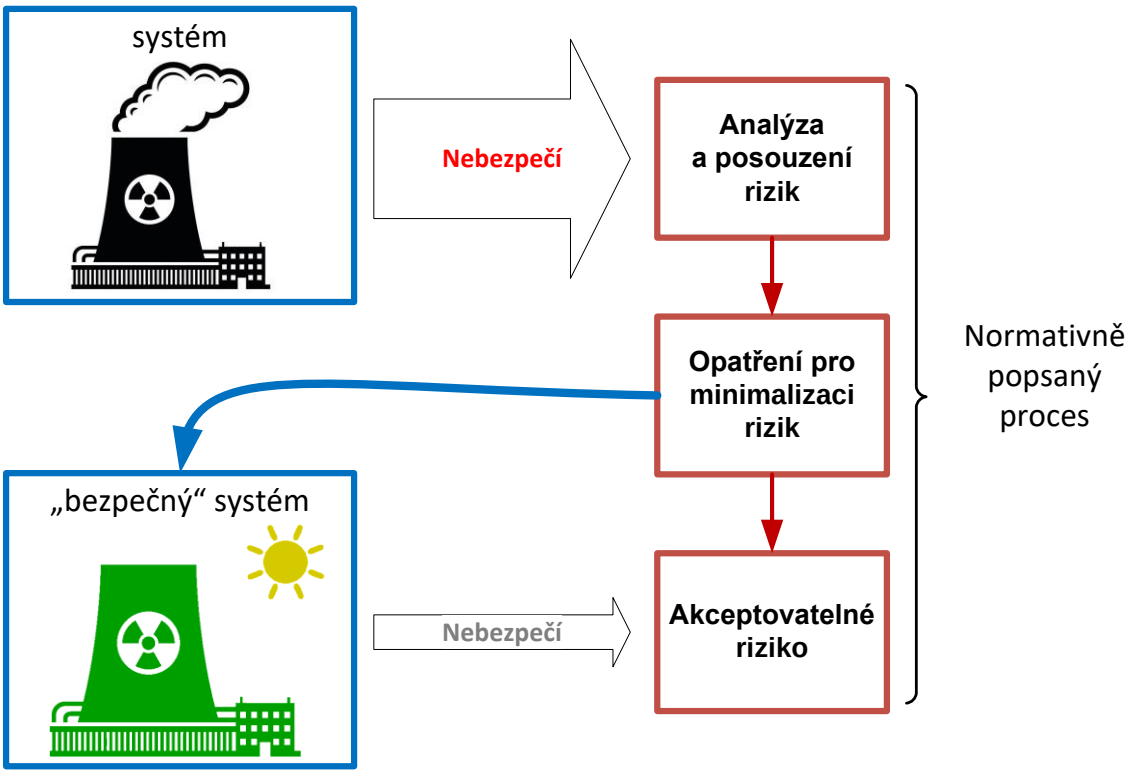
Zdroje nebezpečí

- stroje, materiály, technologie a pracovní činnosti, které mají aktivní vlastnost způsobit negativní jev, úraz nebo škodu
- zdroj nebezpečí je schopen aktivovat nebezpečí v konkrétním prostoru a času

Uvedené tři pojmy spolu velice úzce souvisejí. Nebezpečí je zdrojem ohrožení a riziko lze chápat jako míru tohoto ohrožení. Pro řízení a omezování rizika je nezbytné znát zdroje nebezpečí, charakter nebezpečí i pravděpodobné následky. K tomu slouží analýza a následně její hodnocení.

Riziková analýza musí být aktuální pro každý navrhovaný systém a v případě, že jsou provedeny změny zařízení v době po již provedené rizikové analýze, je nutné provést dodatečnou analýzu. Na základě určení pravděpodobnosti a

následku nežádoucí události je přiřazena úroveň bezpečnostního systému tak, aby po jeho realizaci byla míra rizika přijatelná.



Obrázek 11: Proces analýzy rizika.

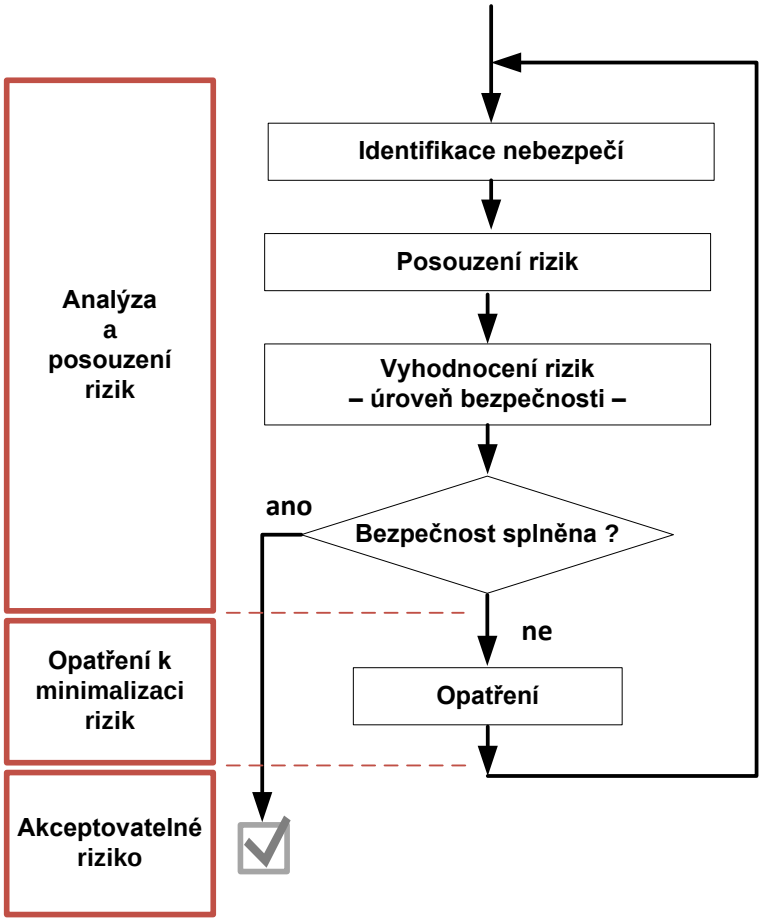
Analýza rizika a hodnocení rizika probíhají v jednom kroku pomocí diagramů, matic nebo semi-kvantitativních výpočtů uvedených přímo v normativních dokumentech (informativních přílohách). Norma ČSN EN 61508 pro analýzu nebezpečí a rizik definuje tři základní cíle, které z jejích požadavků vyplývají:

- Určení nebezpečí a nebezpečných událostí
- Stanovení sledu událostí
- Určení rizik spojených s událostmi

Cesta ke splnění uvedených cílů vede přes řadu kroků (viz tabulka 6 a obrázek 12), které se mohou dle konkrétní aplikace mírně odlišovat. V dalším textu budou představeny nejčastěji využívané metody analýzy rizik.

Tabulka 6: Seznam nezbytných aktivit, které musí být stanoveny a dokumentovány ve fázi analýzy nebezpečí a rizik.

#	
1	Provedení analýzy nebezpečí a rizik
2	Hodnocení opatření pro odstranění nebezpečí
3	Určení nebezpečí a nebezpečných událostí
4	Určení sledu událostí
5	Vyhodnocení pravděpodobnosti nebezpečných událostí
6	Určení potenciálních důsledků
7	Odhad rizik pro jednotlivé nebezpečné události



Obrázek 12: Kroky pro posouzení rizik.

Identifikace nebezpečí

Prvním krokem analýzy nebezpečí a rizika je identifikace všech závažných zdrojů nebezpečí vztahujících se k prováděným činnostem. Předpokladem jsou informace definované v předchozí fázi životního cyklu (Definice systému).

Posouzení rizik

Následujícím krokem je provedení subjektivního odhadu rizika spojeného s každým identifikovaným nebezpečím s uvedením plánovaných nebo stávajících bezpečnostních opatření. Při tom je třeba vzít v úvahu účinnost opatření, možnost jejich selhání a možné následky. Pro každé riziko musí být stanoveno, zda je nutné jej omezit. Pokud ano, je potřeba požadovanou míru omezení rizika kvantifikovat s využitím analýzy rizik.

Vyhodnocení rizik

Dalším krokem je vyhodnocení, zda plánované nebo existující bezpečnostní opatření jsou dostatečná a zajistí udržení nebezpečí pod legislativně stanovenými limity a požadavky (specifikace požadavků na SIL).

Opatření ke snížení rizika (jsou-li zapotřebí)

Pokud jsou stávající opatření vyhodnocena jako nedostatečná, musí být připraven plán zabývající se problémy zjištěnými v předchozích bodech. Organizace by měla zajistit, že nová a existující opatření jsou funkční a efektivní. Po realizaci plánu nápravných opatření musí být opětovně zhodnoceno riziko s ohledem na přijatá nápravná opatření a ověření, jestli je riziko přijatelné. To znamená, zda riziko bylo sníženo na nejnižší rozumně dosažitelnou mez.

Pro posouzení rizik a kvantifikaci nezbytné míry omezení daného rizika lze využít celou řadu metod a postupů, a to obvykle s využitím softwaru. Výběr vhodné metody pro bezpečnostní studii je jedním z nejdůležitějších faktorů, které ovlivňují kvalitu provedení bezpečnostní studie. V praxi je využíváno velké množství metod v různých variantách, ale většinou vycházející jen z několika nejznámějších a nejuznávanějších metod (tabulka 7), od kterých se zásadně neliší. [36] [37] [30] [38]

Tabulka 7: Přehled nejpoužívanějších dílčích metod pro bezpečnostní studie. [52]

Český název metody	Anglický název metody	Zkratka
Revize bezpečnosti	Safety Review	SR
Kontrolní seznam	Checklist Analysis	CL
Předběžná analýza ohrožení	Preliminary Hazard Analysis	PHA
Analýza „Co se stane, když…“	What-If Analysis	WI
Analýza nebezpečí a provozuschopnosti	Hazard and Operability Analysis	HAZOP
Analýza způsobů a důsledků poruch	Failure Modes and Effects Analysis	FMEA
Analýza stromem poruch	Fault Tree Analysis	FTA
Analýza stromem událostí	Event Tree Analysis	ETA
Analýza příčin a následků	Cause - Consequence Analysis	CCA
Analýza lidského faktoru	Human Reliability Analysis	HRA

Bohužel žádná z metod není univerzální a pro konkrétní aplikace musí uživatelé zvolit tu nejvhodnější. Nejvyužívanější metody pro práci s riziky mají rozdílné použití podle velikosti a složitosti aplikace, podávají různé druhy výsledků, jsou odlišně náročné na pracovní tým a čas. Některé metody lze používat návazně na sebe, jiné jsou zcela odlišné a nelze je spojovat. Faktory ovlivňující volbu metody zahrnují především cíl a typ studie, zkušenosti pracovního týmu, dostupnost potřebných informací a samozřejmě ekonomické náklady na studii. S výběrem konkrétní metody mohou pomoci následující faktory:

a) Kritéria přijatelnosti rizika, která je třeba splnit. Některé techniky nejsou vhodné, pokud je třeba prokázat, že riziko bylo sníženo na co nejnižší úroveň přiměřeně k možnostem, jak to provést.

b) Režim provozu bezpečnostních funkcí. Některé metody jsou vhodné pouze pro režim s nízkým vyžádáním.

c) Znalosti a zkušenosti osob, které provádějí rozhodnutí SIL.

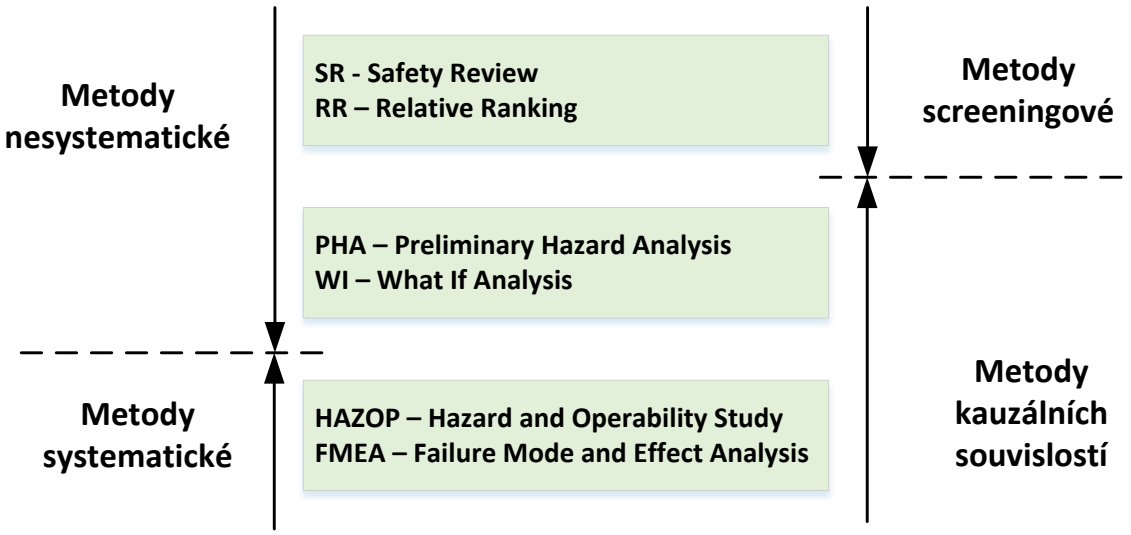
d) Potřebná důvěra, že výsledné zbytkové riziko splňuje kritéria stanovená organizací. Některé metody mohou být spojeny s kvantifikovanými cíli, ale některé přístupy jsou pouze kvalitativní.

e) Může být použito více než jedné metody. Lze použít jednu metodu pro účely prvotních průzkumů, po níž může následovat další metoda s přísnějším přístupem, jestliže první metoda ukazuje potřebu vysoké úrovně integrity.

f) Závažnost následků. Je možné zvolit přísnější metody pro důsledky, které zahrnují mnoho úmrtí.

g) Zda se vyskytuje společná porucha mezi jednotlivými systémy souvisejícími s bezpečností nebo mezi systémem souvisejícím s bezpečností a jiným systémem.

Ať je použita jakákoli metoda, měl by být zdůvodněn její výběr na odpovídající úrovni řízení bezpečnosti. Všechna rozhodnutí by měla být zaznamenána, aby bylo možné ověřit posouzení SIL a aby bylo možné nezávislého hodnocení funkční bezpečnosti.



Obrázek 13: Klasifikace metod.

V následujících kapitolách je stručně popsáno několik základních a nejpoužívanějších metod pro práci s riziky.

3.5.1 Revize bezpečnosti (SR)

Jednou z nejstarších metod je revize bezpečnosti. Tato metoda je založena na posuzování výkresů v době projektování, která potřebuje navázání spolupráce a konzultace mezi analytikem a návrhářem. Revize bezpečnosti identifikuje potenciálně nebezpečná místa v návrhu, analytik navrhuje ochranná opatření, která mohou být ověřována následnými kontrolami. Výsledkem revize bezpečnosti je kvalitativní popis možných bezpečnostních problémů a námět na nápravné kroky. Časová náročnost studie je často velmi malá (1 – 3 dny), ale pro rozsáhlé projekty se může pohybovat i řádu několika týdnů.

3.5.2 Kontrolní seznam (CL)

Analýza kontrolního seznamu je jedním z nejjednodušších a nejrychlejších způsobů identifikace rizik. Kontrolní seznam je obvykle vypracován na základě znalostí získaných z předchozích projektů, které jsou podobné současným a historickým informacím. V případě vytváření nového seznamu využívá analytik informace z příslušných norem a předpisů. Kontrolní seznam je vytvářen výpisem položek, kroků nebo úkolů a poté je analyzován podle kritérií, aby bylo možné zjistit, zda je postup správně dokončen. Pro svou jednoduchost je tato metoda vhodná pro méně zkušené, ale seznam vytvořený zkušeným týmem samozřejmě zajišťuje jeho lepší kvalitu.

3.5.3 HAZOP

HAZOP je systematická analýza, která velmi pečlivě identifikuje nebezpečné / havarijní stavy složitých zařízení a komplexních systémů. Dokáže odhalit možné příčiny a následky, včetně prověření stávajících bezpečnostních funkcí, a napomáhá formulovat opatření snižující míru rizika. Jako každá systematická studie je i aplikace této metody analýzy bezpečnosti náročná na čas, znalosti a zkušenosti. Proto byla zpočátku používána skutečně jen pro analýzu a posouzení nebezpečných (havarijních) stavů u značně rozsáhlých zařízení. Počet bezpečnostních studií realizovaných metodou HAZOP se ale stále zvyšuje a v současnosti je úspěšnou metodou, jakož i uznávaným evropským standardem.

Postup metody je založený na pravděpodobnostním hodnocení ohrožení a z něho plynoucích rizik. Tato metoda využívá tým s různým profesním zázemím. Experti pracují na společném zasedání formou brainstormingu. Soustřeďují se na posouzení rizika a provozní schopnosti systému (operability problems).

V porovnání s ostatními metodami spočívá základní přínos metody HAZOP především v systematickém a metodicky propracovaném systému prohlídek, při kterých se příčiny hledají klasickou otázkou:

„ co mohlo způsobit, že ….. ? “

a následky obdobnou otázkou:

„ co se stane, když ….. ? “

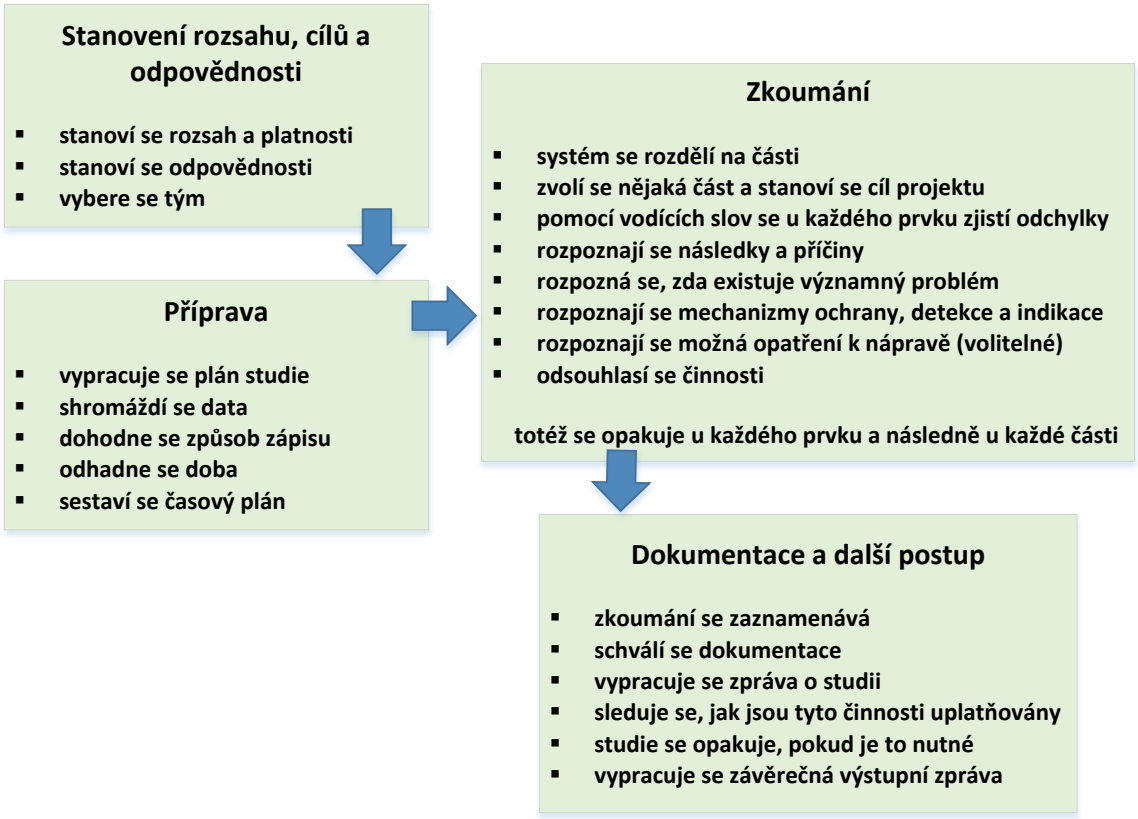
Otázky se však neformulují nahodile na základě subjektivních znalostí. Výraznou podporou při formulaci těchto dotazů je seznam tzv. klíčových slov (*Guide Words*).

Tabulka 8: Význam a výklad klíčových slov studie HAZOP.

Klíčové slovo	Logický význam	Příklad interpretace
není	úplná negace původní funkce	nejsou předávána žádná data nebo řídicí signály
větší	kvantitativní nárůst	data jsou předávána vyšší rychlostí, než je zamýšleno
menší	kvantitativní pokles	data jsou předávána nižší rychlostí, než je zamýšleno
a také, jakož i, a rovněž	kvantitativní nárůst (výskyt ještě jiného případu)	je přítomen nějaký další nebo rušivý signál
částečně	kvantitativní pokles	data nebo řídicí signály jsou neúplné
jiný	úplná náhrada	data nebo řídicí signály jsou nesprávné
předčasný	předčasná funkce (činnost)	signály přicházejí příliš brzy vzhledem ke stanovenému času
zpožděný	opožděná funkce (činnost)	signály přicházejí příliš pozdě vzhledem ke stanovenému času

Připojením klíčového slova k řádné funkci zařízení se generují prakticky všechny odchylky, které mohou třeba jen teoreticky nastat. Tabulka 8 uvádí základní klíčová slova, s nimiž metoda HAZOP pracuje.

Cílem HAZOP studie složitého procesního zařízení je identifikace nebezpečných stavů, která se mohou na zařízení vyskytnout. Postup analýzy zahrnuje tyto kroky:



Obrázek 14: Postup studie HAZOP.

Typicky se v rámci usnadnění systém rozdělí na jednotlivé části tak, aby mohl být pro každou část přiměřeně stanovena projektovaná funkce. Velikost částí závisí na složitosti systému a na závažnosti nebezpečí. V systémech, které představují velké nebezpečí, nebo ve velkých systémech, bývají tyto části zpravidla menší. V jednoduchých systémech nebo v systémech, které představují malé nebezpečí, postačí rozdělení na větší části, což urychluje studii. Cíl projektu pro danou část systému se vyjádří pomocí prvků, které jsou nositeli význačných vlastností dané části a které představují přirozené rozdělení systému na části. Volba prvků, které se mají zkoumat, je do určitého rozsahu subjektivním

rozhodnutím, jelikož může existovat několik kombinací, kterými bývá možné dosáhnout požadovaného účelu, a volba může též záviset na konkrétní aplikaci. Prvky mohou být samostatné kroky nebo etapy postupu, jednotlivé signály a objekty zařízení v řídicím systému, mohou to být zařízení nebo součástky v procesu nebo v elektronickém systému atd. Tým HAZOP zkoumá každý prvek (a charakteristiku, pokud to má význam) z hlediska odchylky od cíle projektu, která může vést k nežádoucím následkům. Rozpoznání odchylek od cíle projektu se dosahuje procesem kladení otázek s použitím předem stanovených klíčových slov. Role klíčového slova spočívá ve stimulaci nápaditého myšlení, jeho soustředění na studii a vyvolání nápadů a diskuse, čímž se maximalizují vyhlídky na úplnost studie.

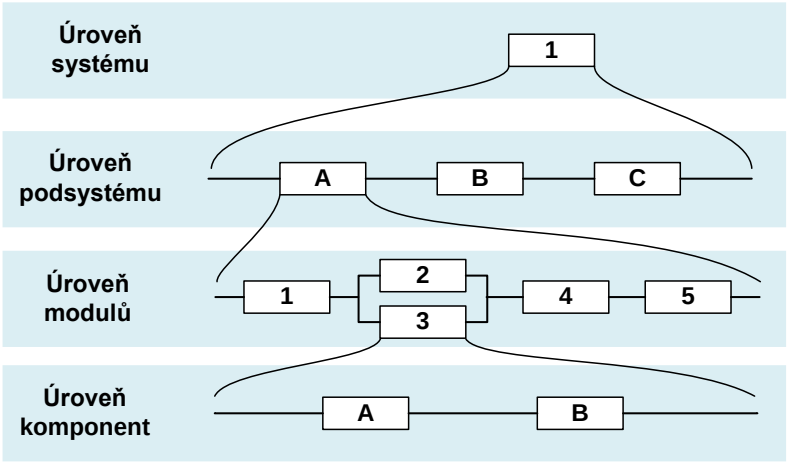
Technika HAZOP byla původně vyvinuta pro analýzu systémů v chemickém průmyslu, přičemž byla postupně rozšířena na ostatní typy systémů a složitých procesů. To zahrnuje mechanické a elektronické systémy, postupy a softwarové systémy. Příklad aplikace metody HAZOP, který se zabývá hodnocením příčin kolize cisterny ADR s vlakem na železničním přejezdu je například v [30]. [31]

3.5.4 FMEA

FMEA (*Failure Mode and Effects Analysis*) je strukturovaná kvalitativní analýza, která slouží k identifikaci způsobů poruch systémů, jejich příčin a důsledků. Rozšíří-li se o hodnocení kritičnosti důsledků s uvážením pravděpodobností (nebo četností) jejich výskytu, jedná se pak o metodu zvanou Analýza druhů, důsledků a kritičnosti poruchových stavů (FMECA - *Fault Modes, Effects and Criticality Analysis*). 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 (tomu předchází dekompozice a stanovení úrovní systému) viz obrázek 15.

Cílem studie metodou FMEA je především odhalit poruchy, které mají závažný vliv na bezpečnost a provozování systému. Hlavním dokumentem, ze kterého se při bezpečnostní studii vychází, je funkční schéma systému. V různých oborech se pro taková schémata používá různé označení (např. technologické schéma, konstrukční výkresová dokumentace atd.)

Pro správné provedení FMEA analýzy se vyžaduje znalost funkcí zařízení a způsobů poruch, znalost funkcí celého systému a znalost odezev na selhání zařízení. U každého zařízení jsou uvedeny potenciální poruchy a jejich možné nežádoucí účinky. V této metodě jsou identifikovány primární způsoby poruchy, které mohou vést k nehodě nebo k ní významně přispět.



Obrázek 15: Induktivní přístup analýzy FMEA.

Analýzu FMEA je nutno chápat jako týmovou metodu. Jen velmi obtížně by ji mohl kvalitně provádět jeden pracovník, neboť by mu chyběly pohledy na problematiku z dalších profesních oblastí. Při svém provádění musí být FMEA provázána s řídícími zásahy v podobě nápravných opatření vedoucích k odstranění příčin, které jsou identifikovány jako nejzávažnější potenciálně možné poruchové stavy.

Obecně je FMEA/FMECA podobná metodě HAZOP v tom, že identifikuje způsoby poruch v rámci systému nebo postupu jejich příčiny a důsledků. Zatímco FMEA/FMECA začíná své řešení identifikací způsobů poruch, metoda HAZOP se liší v tom, že tým posuzuje nechtěné výstupy a odchylky od chtěných/zamýšlených výstupů a podmínek a pracuje zpět k možným příčinám a způsobům poruch.

Pro přehlednost analýzy se běžně používají pracovní formuláře. Neexistuje však žádný závazný předpis upravující obsah nebo formu, pouze doporučení např.

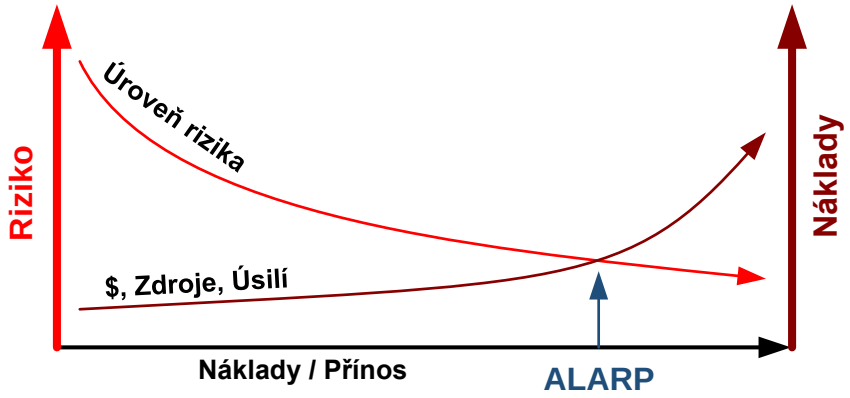
viz [30]. Vždy by měl ale obsah a uspořádání odpovídat specifickým cílům analýzy a charakteru systému. Příklad části analýzy uvádí obrázek 16. [32] [14] [33] [34]

#	Item / Function / Objekt / funkce	Potential Failure Mode(s) / Potenciální způsob poruchy	Potential Local Effect(s) of Failure / Potenciální místní důsledek poruchy	Potential Global Effect(s) of Failure / Potenciální konečný důsledek poruchy	SEV	Potential Cause(s)/ Mechanism(s) of Failure / Potenciální příčiny / mechanizmy poruchy	PROB	Detection Method / Metoda detekce	DET	RPN	Recommended Action(s) / Doporučená opatření	Action Result / Provedená opatření
Napájecí zdroj												
1	D2	Zkrat	Zkrat +pólu baterie na - zem	Vybití baterie "vrať se domů pěšky"	10	Vnitřní vada - průraz materiálu	3	Hodnocení a validační zkoušky bezporuchovosti	1	30		
2	D2	Přerušení	Žádná ochrana proti přepólování	Nezasluhuje pozornost	2	Vnitřní vada - vada kontaktování nebo prasklina v polovodiči	3	Hodnocení a validační zkoušky bezporuchovosti	2	12		
3	C7	Zkrat	Zkrat +pólu baterie na - zem	Vybití baterie "vrať se domů pěšky"	10	Vnitřní vada - průraz dielektrika nebo prasklina	3	Hodnocení a validační zkoušky bezporuchovosti	1	30		
4	C7	Přerušení	Žádná filtrace proti elmag. rušení	Provoz objektu mimo specifikaci	2	Přerušení kontaktu mezi přívodem a polepem, netěsnost, dutina či prasklina	2	Hodnocení a validační zkoušky bezporuchovosti	1	4		
5	L1	Přerušení	Žádné napětí -V1	Objekt je nefunkční - žádné varování	9	Vnitřní vada - Prasknutí materiálu	2	Hodnocení a validační zkoušky bezporuchovosti	1	18		
6	R5	Přerušení	Žádné napětí pro spínací obvod	Objekt je nefunkční - žádné varování	9	Vnitřní vada - Přerušení vodivého spojení nebo materiálu	2	Hodnocení a validační zkoušky bezporuchovosti	1	18		

Obrázek 16: Příklad části FMEA analýzy.

3.5.5 Metoda ALARP

Princip ALARP je konkrétní metoda pro hodnocení přípustného rizika. 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. Zkratka ALARP (*As Low As Reasonably Practicable*) znamená „co nejnižší rozumně dosažitelné riziko“. Tato metoda tedy respektuje snahu dosažení co nejnižšího rizika, avšak s ohledem na náklady spojené s tímto úsilím viz obrázek 17.



Obrázek 17: Náklady / přínosy zmírňování rizika ALARP.

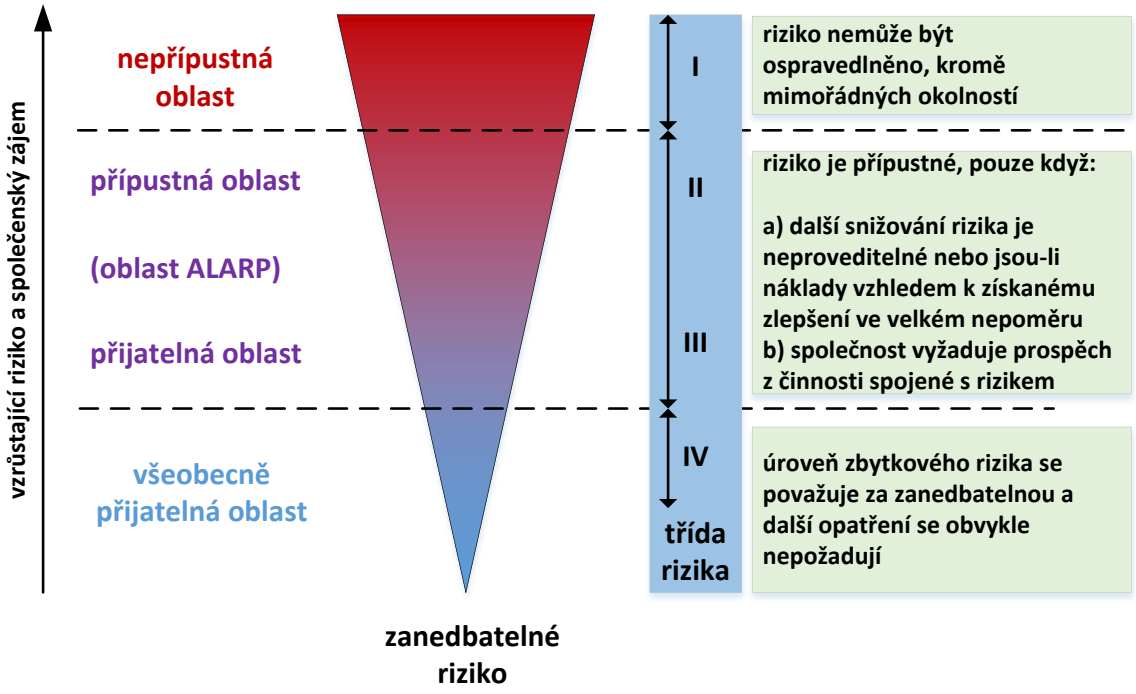
Vyvážení mezi přijatelnou oblastí rizika a investicemi do odstranění rizika je stanoveno na základě subjektivního standardu a je hledán bod, kde náklady překračují výhody. To si lze představit na příkladu: Pokud organizace zhodnotí lidský život na částku 10 000 000 Kč, tak použitím principu ALARP nebude organizace implementovat investice do opatření v hodnotě 20 000 000 Kč, které pravděpodobně ochrání jeden život za rok. Pokud však nejvyšší úřad uloží organizaci 50 000 000 Kč pokutu po smrtelné nehodě, pak se hodnota lidského života právě zvýšila na 50 000 000 Kč. V takovém případě již investice do odstranění rizika ve výši 20 000 000 Kč samozřejmě stojí za to.

Základní koncepce metody ALARP je založena na rozdělení rizika do tří oblastí:

- **Nepřípustná oblast** – riziko musí být bezpodmínečně odstraněno.
- **Oblast ALARP** – riziko se nachází mezi nepřípustnou a všeobecně přijatelnou oblastí. Udává povinnost snížit riziko do té míry, která je v rozumné míře investic proveditelná.
- **Všeobecně přijatelná oblast** – riziko je tak malé, že jeho existence je vzhledem k jeho povaze přijatelná.

Pokud je riziko hodnoceno jako nepřípustné, princip ALARP vyžaduje jeho snížení na co nejnižší rozumně proveditelnou úroveň. Je-li riziko zařazeno do oblasti ALARP, je dovoleno provádět dané činnosti za předpokladu, že s nimi spojená rizika byla snížena na co nejnižší rozumně proveditelnou úroveň. Čím vyšší riziko je, tím více úsilí se dá očekávat při jeho snižování. Do poslední oblasti

jsou zařazena rizika, pro která již není nutné prokazovat ALARP. Přesto je nutné věnovat pozornost tomu, aby se riziko na této konkrétní úrovni udrželo. Struktura této metody je zobrazena na následujícím obrázku.



Obrázek 18: Přijatelné riziko a princip ALARP.

Pro zařazení rizik do konkrétních oblastí zavádí metoda ALARP třídy rizika v rozmezí I – IV. Klasifikace tříd a výklad rizika je uveden v tabulce 9.

Tabulka 9: Výklad tříd rizika.

Třída rizika	Výklad rizika
Třída I.	Nepřípustné riziko.
Třída II.	Nežádoucí riziko, přípustné pouze v případě, že snížení rizika je neproveditelné nebo v případě, že náklady jsou výrazně neúměrné dosaženému zlepšení.
Třída III.	Přípustné riziko v případě, že náklady na snížení rizika by přesáhly dosažené zlepšení.
Třída IV.	Zanedbatelné riziko.

Následně je pro každé riziko odhadnuta četnost jeho výskytu a očekávaný následek. Stanovení určitého počtu následků, jimž se přiřadí přípustné četnosti, by

mělo být ve formě diskusí a dohod mezi zapojenými stranami. Z kombinací četností a následků se poté utvoří tzv. matice rizik (viz tabulka 10).

Tabulka 10: Příklad klasifikace rizika nehod dle koncepce ALARP.

Četnost	Následek			
	Katastrofální	Kritický	Nepodstatný	Zanedbatelný
Častá	I	I	I	II
Pravděpodobná	I	I	II	III
Příležitostná	I	II	III	III
Málo častá	II	III	III	IV
Nepravděpodobná	III	III	IV	IV
Neuvěřitelná	IV	IV	IV	IV

Zařazení jednotlivých rizik do kategorií četností a následků rizik ve velké míře záleží na skupině, která analýzu provádí. Proto je nutné tuto tabulku brát pouze jako příklad toho, jak by mohla být vyplněna. Skutečný stav pro všechny třídy rizika závisí na oblasti použití a také na tom, jaké jsou skutečné hodnoty četnosti. [35]

3.5.6 Metoda grafu rizik

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.

- Následek (C) (*Consequence risk parameter*)
- Četnost a doba vystavení v nebezpečné oblasti (F) (*Frequency and exposure time risk parameter*)
- Možnost se nebezpečné události vyhnout (P) (*Possibility to avoiding hazard risk parameter*)

- Pravděpodobnost nežádoucího výskytu (W) (*Probability of the unwanted occurrence*)

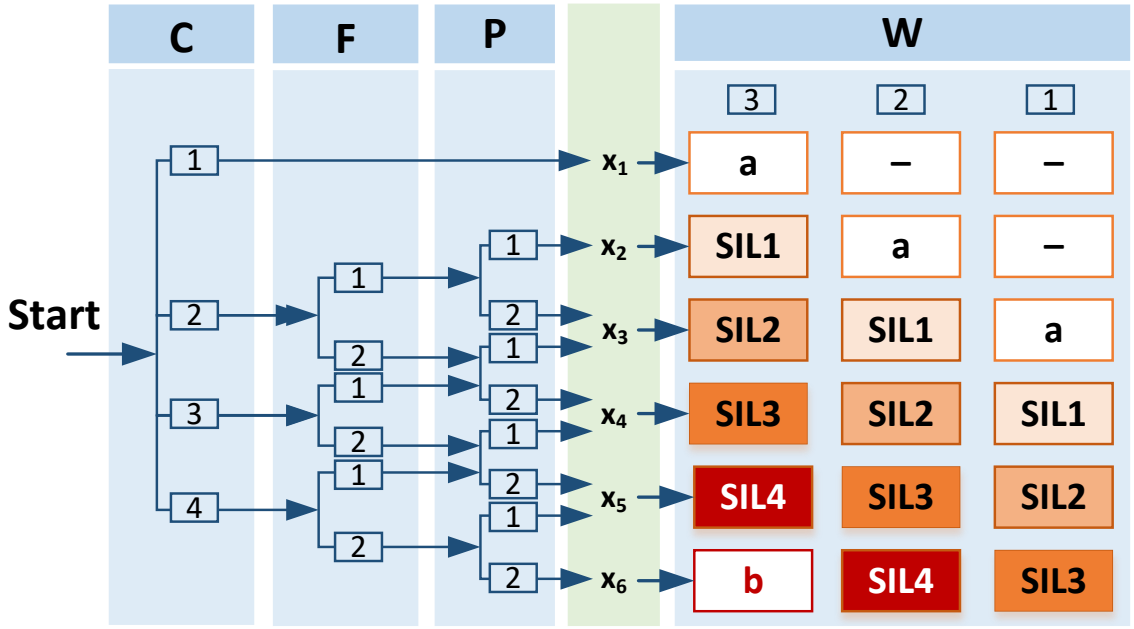
Hodnoty jednotlivých parametrů *C, F, P* a *W* lze určit na kvalitativním základě (viz tabulka 11), nebo na kvantitativním základě. Kvalitativní metoda určování hodnot parametrů je založena na subjektivním hodnocení a proto vyžaduje značný úsudek a tedy i potřebné znalosti a zkušenosti. Zbytkové riziko nelze vypočítat na základě znalosti parametrů, a proto není tato metoda vhodná v případě, že organizace vyžaduje důkaz, že zbytkové riziko bylo sníženo na stanovenou kvantitativní hodnotu. Ve druhém případě je při rozhodování o číselných hodnotách parametrů zapotřebí provést kalibrační proces.

Použití kalibrace při určování parametrů vede oproti kvalitativnímu určování na vysokou úroveň integrity bezpečnosti. Vyšší úroveň integrity bezpečnosti je způsobena faktem, že se kalibrace provádí za použití nejhorších případů každého parametru v průběhu dlouhého období.

Kalibrace je proces přiřazení číselných hodnot jednotlivým parametrům metody grafu rizik. Cílem kalibračního procesu je popsat všechny parametry takovým způsobem, aby bylo možné provést posouzení úrovně integrity bezpečnosti charakteristické aplikace v souladu s kritérii podnikového nebo jiného zdroje rizika.

Většině parametrů je v procesu kalibrace přidělen rozsah, který pomáhá týmu při rozhodování o tom, která hodnota parametru se má vybrat pro konkrétní aplikaci. Riziko spojené s každou kombinací parametrů je pak vyhodnoceno podle definovaných rizikových kritérií. Popisy parametrů se upraví tak, aby pro všechny kombinace hodnot parametrů byla stanovena definovaná kritéria rizika. V některých případech může být potřeba změnit rozsahy spojené s jinými rizikovými faktory tak, aby odrážely hodnoty parametrů, které se vyskytovaly například při zvažovaném rozšíření aplikace. Kalibrační proces probíhá a pokračuje, dokud nejsou splněna specifikovaná kritéria přijatelnosti rizika pro všechny kombinace hodnot parametrů.

Odpovídající úroveň integrity bezpečnosti je následně určena na základě kombinace parametrů popsaných výše vložených do grafu rizik.



Obrázek 19: Graf rizik - určení potřebné SIL

Tabulka 11: Kvalitativní základ pro klasifikaci parametrů metody grafu rizik

Rizikový parametr		Klasifikace
Následek (C)	C_1	Menší zranění
	C_2	Zranění jedné nebo více osob s trvalými následky, smrt jedné osoby
	C_3	Smrt několika osob
	C_4	Smrt velkého počtu osob
Četnost a doba vystavení v nebezpečné oblasti (F)	F_1	Vzácné až častější vystavení v nebezpečné oblasti
	F_2	Časté až trvalé vystavení v nebezpečné oblasti
Možnost se nebezpečné události vyhnout (P)	P_1	Možné za určitých podmínek
	P_2	Téměř nemožné
Pravděpodobnost nežádoucího výskytu (W)	W_1	Velmi malá pravděpodobnost
	W_2	Malá pravděpodobnost
	W_3	Poměrně vysoká pravděpodobnost

Uvedené čtyři parametry jsou považovány za dostatečně obecné pro řešení široké škály aplikací. Mohou však existovat aplikace, které mají aspekty, jež

vyžadují zavedení dalších rizikových parametrů, např. využívání nových technologií. Úkolem dalších parametrů by bylo přesněji odhadnout potřebné snížení rizika.

3.6 Požadavky celkové bezpečnosti (fáze 4 ŽC)

Konkrétní rizika a nebezpečné události určené rizikovou analýzou jsou ve fázi specifikace požadavků převedeny do konkrétní podoby. V praxi to znamená definovat pro jednotlivé nebezpečné události vhodné bezpečnostní funkce zajišťující snížení potenciálního nebezpečí. Pro každou nebezpečnou událost musí být vytvořena bezpečnostní funkce. Není při tom specifikováno technické provedení jednotlivých funkcí, neboť metoda a technologie jejich realizace bude známa až v dalších etapách. Příklady definic bezpečnostních funkcí mohou vypadat následovně:

- Zastavení vřetene při otevření krytu.
- Zabránění vzrůstu teploty v nádobě nad 250°C.
- Zabránění přesáhnout rychlost v mechanice 3 000 ot./min.

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:

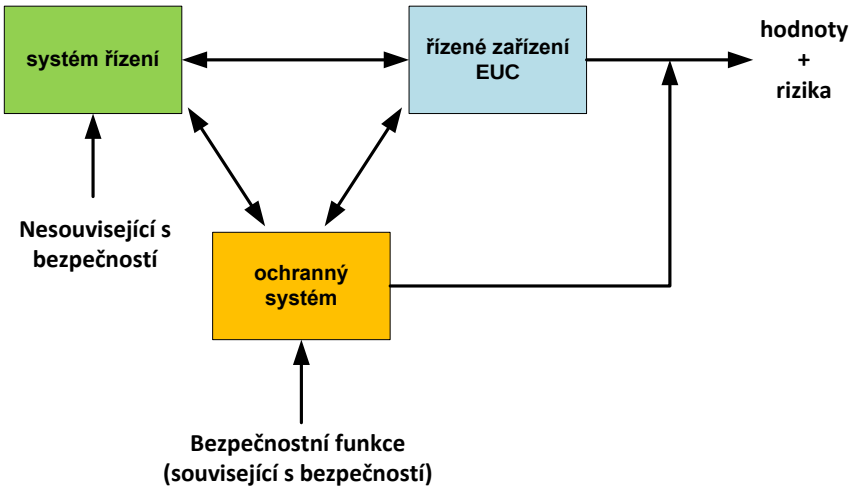
- snížením dopadů nebezpečných událostí, nebo
- snížením četnosti nebezpečných událostí EUC a řídicího systému EUC.

Přednost se dává snížení dopadů nebezpečných událostí před snižování četnosti nebezpečných událostí. Obecně jsou přijatelnější častější dopady, než výjimečné ale velmi vážné katastrofy.

Snížení četnosti (frekvence) nebezpečných událostí lze dosáhnout doplňkovými opatřeními obsahujícími E/E/PE systém(y) a/nebo jinými opatřeními snižujícími riziko. Dále lze četnost snížit použitím bezpečnostních systémů založených na

jiných technologiích nebo řízením opatření jako je doba úniku, obsazení nebo expozice.

Systém řízení EUC je možné vyjmout z požadavků na bezpečnost a považovat jej za řídicí systém nesouvisející s bezpečností - nemusí být aplikovány požadavky norem týkajících se funkční bezpečnosti.



Obrázek 20: Model spojení systému řízení a EUC.

Tento předpoklad je možné uplatnit pouze u systémů, kde snížení rizika je zajištěno jedním nebo několika E/E/PE ochrannými systémy souvisejícími s bezpečností a/nebo jinými opatřeními a dále při splnění následujících podmínek:

a) četnost nebezpečných poruch požadovaná u systému řízení EUC musí být podložena daty získanými na základě:

   – skutečných provozních zkušeností se systémem řízení EUC v podobné aplikaci

   – analýzy bezporuchovosti provedené uznávaným postupem

   – informací z průmyslové databáze bezporuchovosti generického zařízení

b) četnost nebezpečných poruch, která se může pro systém řízení EUC požadovat nesmí být nižší než 10^{-5} nebezpečných poruch za hodinu

c) musí se určit všechny rozumně předvídatelné režimy nebezpečných poruch systému řízení EUC a při zpracování specifikace požadavků celkové bezpečnosti se s nimi musí počítat

d) systém řízení EUC musí být nezávislý na systémech E/E/PE souvisejících s bezpečností a na jiných opatřeních pro snížení rizika.

V opačných případech, tj. nesplnění některé z podmínek, je nutné systém řízení EUC považovat za řídicí systém související s bezpečností a musí se aplikovat požadavky bezpečnostních norem.

Soubor všech nezbytných bezpečnostních funkcí představuje výslednou specifikaci požadavků celkové bezpečnosti, která musí být řádně dokumentována.

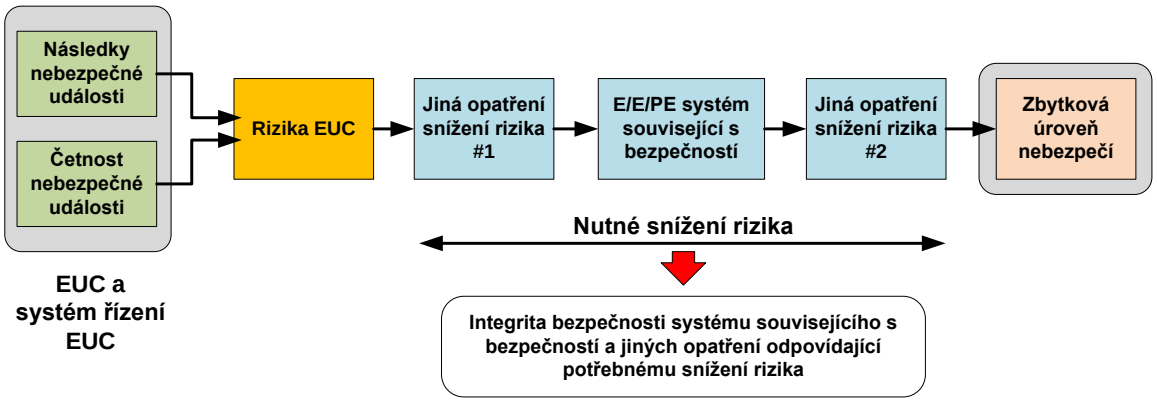
3.7 Přiřazení požadavků celkové bezpečnosti (fáze 5 ŽC)

Bezpečnostní funkce definované ve specifikaci požadavků celkové bezpečnosti jsou v této fázi životního cyklu 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 každou bezpečnostní funkci musí být specifikován konkrétní E/E/PE systém případně jiné opatření související s bezpečností, které zajistí potřebné snížení rizika.

3.7.1 Možnosti snížení rizik

Z pohledu požadavků je nutné v této fázi definovat systémy potřebné pro dosažení požadované úrovně funkční bezpečnosti. Nutného snížení rizika je pak možné dosáhnout:

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

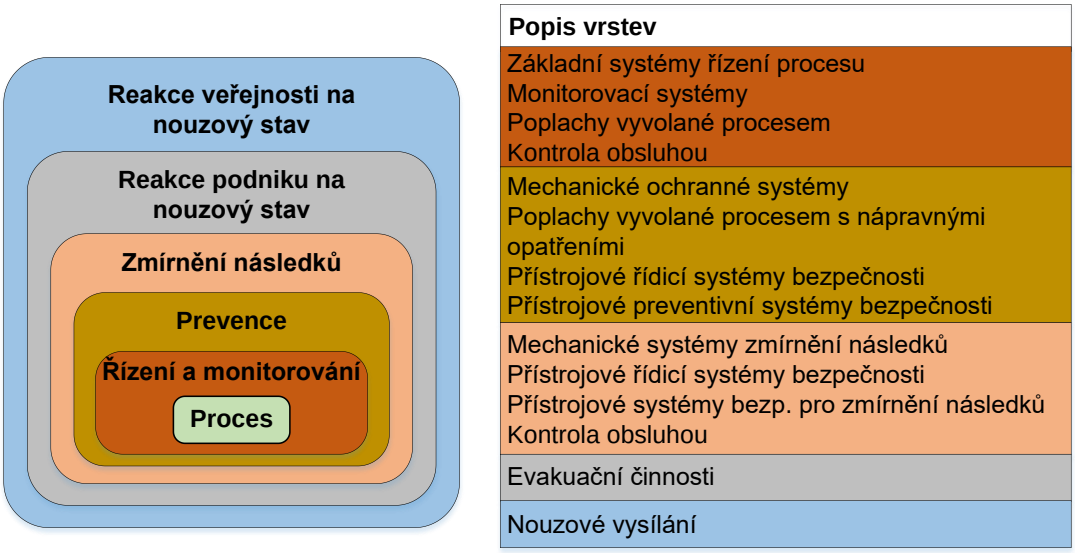


Obrázek 21: Koncept rizika a integrity bezpečnosti.

Systémy E/E/PE a jejich návrh spadají do normy ČSN EN 61508 a jsou předmětem této práce.

Pojmem *jiná opatření snižující riziko* se rozumí technologie, jež jsou založeny na jiných technických principech než elektrických / elektronických nebo programovatelných elektronických (například hydraulických, pneumatických apod.). Jiná opatření mohou být založena i na fyzikální struktuře jako jsou odtokový systém, protipožární stěna apod. Pro splnění požadavků bezpečnostních funkcí a požadavků na integritu bezpečnosti musí být všechna jiná opatření snižující riziko specifikována podobně jako E/E/PE systémy, ale jelikož se jedná o jiné technologie, nejsou předmětem normy ČSN EN 61508.

V případě závažných havárií by bylo neekonomické a zároveň nevěrohodné dosahovat požadovaného snížení rizika pouze technickými systémy. Proto se používají ochranné vrstvy tvořící jakousi nadstavbu použití E/E/PE systémů a systémů založených na jiných technických principech. Jedná se o přístup, který není zaveden přímo v ČSN EN 61508, ale v oborové implementaci ČSN EN 61511. Tento princip využívá ke snížení rizika tzv. *vnější prostředky*. Princip metody dobře vysvětluje obrázek 22 na imaginárním modelu, kde jsou také uvedeny příklady některých vnějších prostředků ke snížení rizika v konkrétní vrstvě. Podrobnější popis této metody je uveden v ČSN EN 61511 a může být omezen platnou legislativou, případně souvisejícími závaznými dokumenty.



Obrázek 22: Princip ochranných vrstev podle ČSN EN 61511.

Všechny tyto technologie mohou být začleněny do celkového životního cyklu, aby zajistily, že snížení rizika E/E/PE systémů souvisejících s bezpečností je určeno v kontextu snížení rizika z jiných opatření snižujících riziko.

3.7.2 Nezávislost systémů

Systémů podílejících se na vykonávání jedné konkrétní bezpečnostní funkce může být přitom i více. Rozhodnutí o konkrétním přidělení nezáleží pouze na rozsahu nebo vlastnostech bezpečnostní funkce, ale především na požadavku snížení rizika, kterého se má danou bezpečnostní funkcí dosáhnout. Čím větší snížení rizika se požaduje, tím je pravděpodobnější, že daná funkce bude rozprostřena přes více než jeden bezpečnostní systém.

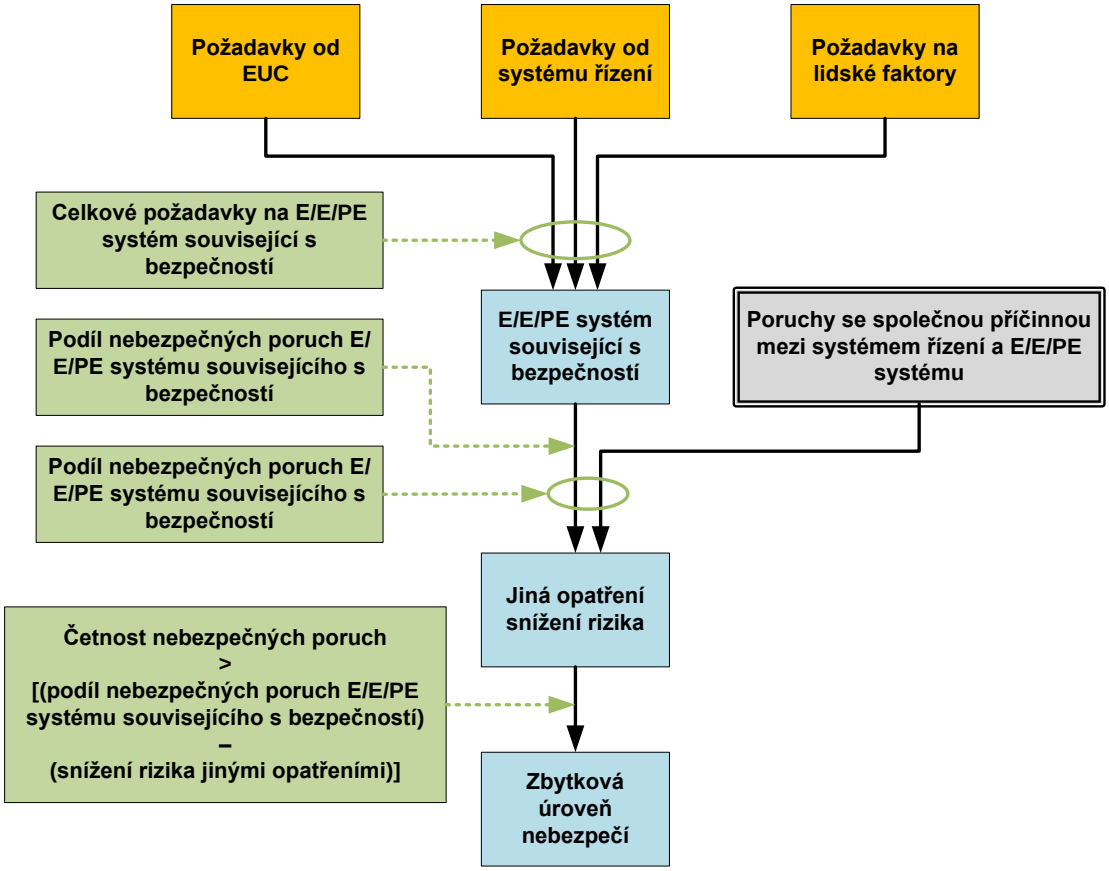
V případě, že pro dosažení tolerovatelného rizika je použito několik E/E/PE systémů souvisejících s bezpečností případně jiných opatření nezbytných pro snížení rizika, musí se zvážit možnosti společných poruch. Aktuální dosažené riziko závisí na vzájemných systematických závislostech a mají-li se řídicí systém

EUC, E/E/PE systém související s bezpečností a jiné prostředky pro snížení rizika brát jako nezávislé dle ČSN EN 61508:

- musí být nezávislé, aby pravděpodobnost současné chyby mezi dvěma nebo několika těmito různými systémy nebo opatřeními byla dostatečně malá ve vztahu k požadované integritě bezpečnosti,
- musí být funkčně odlišné (tj. pro dosažení stejných výsledků musí používat zcela odlišných přístupů),
- musí být založeny na odlišných technologiích (tj. pro dosažení stejných výsledků musí používat různé typy zařízení),
- nesmí sdílet společné části, služby nebo pomocné systémy (např. napájecí zdroje), jejichž porucha by mohla vést k nebezpečnému režimu poruchy všech systémů,
- nesmí mít společné provozní, údržbové nebo zkušební postupy.

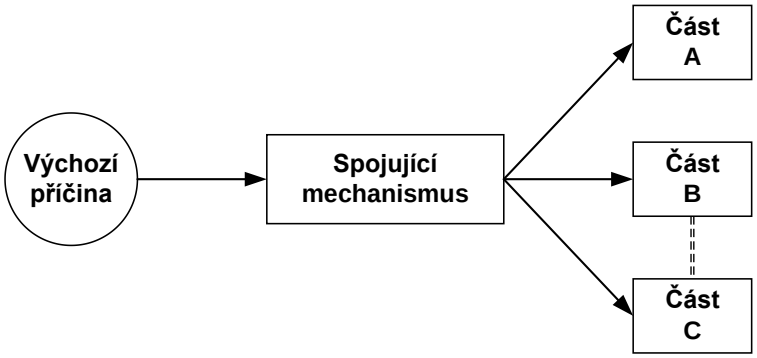
Pokud nelze všechny výše uvedené podmínky splnit, potom se systémy a jiná opatření pro snížení rizika nesmí brát jako nezávislé (pro účely přiřazení integrity bezpečnosti).

Při určování úrovně integrity bezpečnosti je důležité vzít v úvahu poruchy se společnou příčinou. Jednotlivé modely znázorněné výše (obrázek 20 a obrázek 21) pracují s riziky na základě plné nezávislosti všech systémů bezpečnosti a jiných opatření snižující riziko. Existuje ale mnoho aplikací, kdy nelze jednoduše stanovit nezávislost systémů. Příklad systému, kde je nutné zohlednit i poruchy se společnou příčinou je na následujícím obrázku.



Obrázek 23: Příklad poruch se společnou příčinnou (CCF) částí systému řízení EUC a částí E/E/PE systému souvisejícího s bezpečností.

Příklad na obrázku 23 zobrazuje oddělený systém řízení EUC a systém související s bezpečností, kde oba nesou prvek, který je vystaven selhání ze stejné příčiny. Reálným příkladem může být situace, ve kterém řídicí a ochranný systém má sice svůj senzor, ale společná příčina by mohla vést k selhání obou.



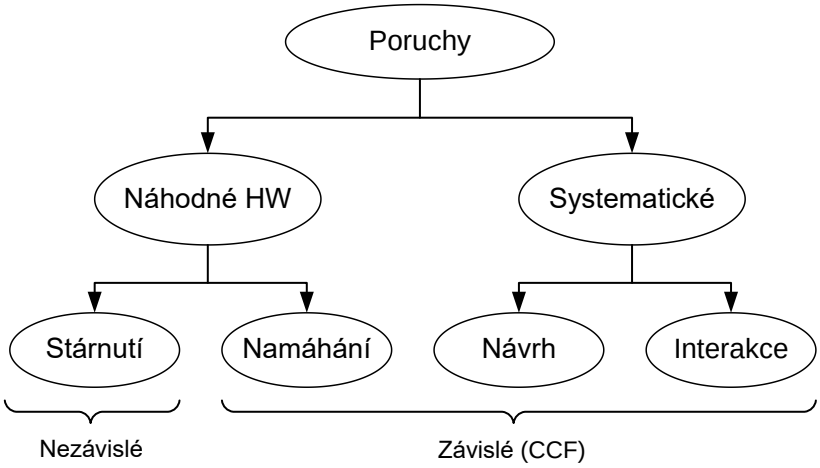
Obrázek 24: Fyzické prvky závislé události.

Účinky poruch se společnou příčinou jsou většinou významnější u aplikací s vysokou úrovní bezpečnosti. V některých aplikacích může být nutné zahrnout různorodost tak, aby byly minimalizovány příčiny společných poruch. Je však třeba poznamenat, že začlenění rozmanitosti může vést k problémům při návrhu, údržbě nebo úpravě/opravě. V konečném důsledku může vést k chybám kvůli neznalosti a nedostatku provozních zkušeností s různými zařízeními. Konečné důsledky poruch se společnou příčinou jsou jen velmi obtížně určitelné a často vyžadují konstrukce speciálních modelů (např. strom poruch nebo Markovovy modely).

3.7.3 Poruchy se společnou příčinou CCF

Obecně je možné poruchy systému rozdělit podle jejich příčiny na:

- náhodné poruchy hardwaru,
- systematické poruchy.



Obrázek 25: Klasifikace poruch podle příčiny.

Bez ohledu na to, jak dobře jsou uplatňována opatření zabývající se systematickými chybami, vždy existuje zbytková pravděpodobnost selhání, k níž jsou největším přispěvovatelem právě poruchy se společnou příčinou. Ačkoli to významně neovlivňuje výpočty spolehlivosti pro jednokanálové systémy, potenciál poruch se společnou příčinou může mít za následek podstatné chyby při výpočtech pro vícekanálové nebo redundantní systémy. Jsou důležitou součástí výpočtu spolehlivosti nebo modelu bezpečnosti, neboť jistým způsobem vyvracejí

přínos redundance. Často jsou největšími přispěvateli rizik a měly by být proto vždy pečlivě zváženy. Mohou být způsobeny systematickou poruchou (například chybou návrhu nebo specifikace) nebo externím stresem vedoucím k časné poruše hardwaru (například zvýšená teplota způsobená selháním společného chladicího ventilátoru vedoucí ke zrychlenému stárnutí součástek nebo provozování mimo jejich pracovní rozsah) nebo případně kombinace obou. Pravděpodobnost selhání se společnou příčinou bude pravděpodobně dominantním faktorem při určování celkové pravděpodobnosti selhání vícekanálového systému, protože selhání pravděpodobně ovlivní více než jeden kanál.

Obrany proti poruchám se společnou příčinou

Přestože tyto poruchy vyplývají z jediné příčiny, neprojevují se nutně současně ve všech kanálech. Architektura programovatelných systémů však umožňuje provádět interní diagnostické on-line testování během provozu. Jednokanálový systém může například průběžně kontrolovat své vnitřní funkce společně s funkčností vstupních a výstupních obvodů. Testy lze dosáhnout pokrytí i 99%. Pokud se zjistí velká část interních poruch předtím, než mohou vést k selhání, pravděpodobnost nebezpečného stavu bude výrazně snížena.

Kromě vnitřního testování může každý kanál ve vícekanálovém bezpečnostním systému monitorovat výstupy jiných kanálů. Pokud se tedy v jednom kanálu vyskytne porucha, může být detekována a bezpečně odstavena iniciací jednoho nebo více zbývajících kanálů, které poruchou (ještě) nebyli zasaženy a provádějí test křížového monitorování (*Cross-Monitoring*). Křížové monitorování bývá prováděno vysokou rychlostí, takže test může včas detekovat selhání prvního kanálu a tak celý systém převést do bezpečného stavu ještě před ovlivněním druhého kanálu.

Výše uvedené úvahy lze demonstrovat na příkladu selhání ventilátoru chlazení, u kterého mohou selhat všechny kanály vícekanálového systému, jedná se tedy o selhání ze společné příčiny. Je však nepravděpodobné, že se budou všechny kanály ohřívat stejnou rychlostí, náchylnost každého kanálu se tím pádem mírně liší, což vede k tomu, že druhý kanál selže několik desítek minut po prvním. To

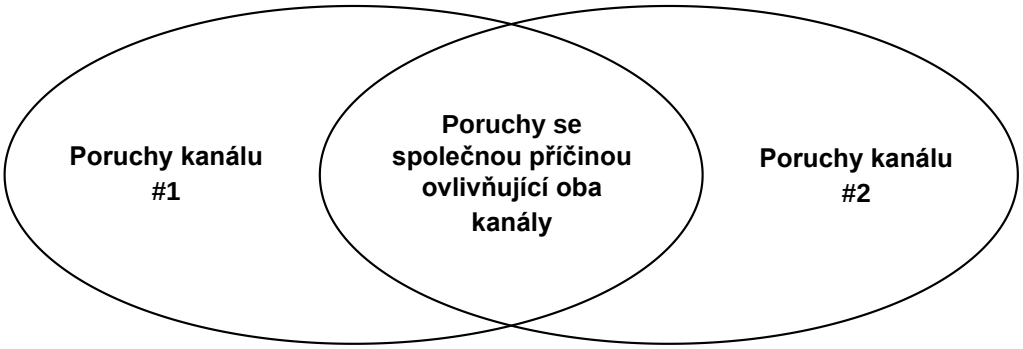
umožňuje, aby diagnostické testování iniciovalo bezpečné vypnutí předtím, než druhý kanál podlehne chybě.

Pro snížení pravděpodobnosti potenciálně nebezpečných poruch se společnou příčinou lze uvést tři obecná doporučení:

a) snížení celkového počtu náhodných hardwarových a systematických poruch, (snížení ploch elips na obrázku 26, což vede ke snížení oblasti překrytí)

b) maximalizace nezávislosti kanálů (separace a rozmanitost), (zmenšení oblasti překrytí mezi elipsami na obrázku 26 při zachování jejich plochy)

c) odhalit nesouběžné selhání ze společné příčiny v době kdy byl ovlivněn pouze jeden kanál (ještě před druhým kanálem), tzn. používat diagnostické testy nebo kontrolní zkoušky.



Obrázek 26: Souvislost poruch se společnou příčinou s poruchami jednotlivých kanálů.

Byla navržena řada matematických přístupů k modelování poruch se společnou příčinou. Přehled nejznámějších a nejpoužívanějších modelů je uveden v tabulce 12.

Všechny tyto modely byly vyvinuty za předpokladu, že selhání jednotlivých složek a události běžných příčin nastávají podle homogenního Poissonova rozdělení s konstantním rozdělením čase. [39]

Tabulka 12: Klíčové charakteristiky parametrických modelů pro kvantifikaci CCF.

Přístup odhadu			Model	Parametry modelu	Obecná forma
nešokové modely	přímý		Základní parametry	$Q_1, Q_2, \dots, Q_m$	$Q_k = Q_k \quad k = 1, 2, \dots, m$
	nepřímý	jedno parametrový	*Beta faktor*	Q_t, β	$Q_k = \begin{cases} (1-\beta)Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases}$
		více parametrový	*Faktory více řeckých písmen*	$Q_t, \underbrace{\beta, \gamma, \delta, \dots}_{m-1\ parametrů}$	$Q_k = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) (1-\rho_{k+1}) Q_t$ $\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \dots, \rho_{m+1} = 0$
			Alfa faktor	$Q_t, \alpha_1, \alpha_2, \dots, \alpha_m$	$Q_k = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \dots, m$ $\alpha_t = \sum_{k=1}^{m} k\alpha_k$
šokové modely			*Binomické rozdělení poruchovosti*	Q_t, μ, ρ, w	$Q_k = \begin{cases} \mu\rho^k (1-\rho)^{m-k} & k \neq m \\ \mu\rho^m + w & k = m \end{cases}$

Konkrétní analýzu je nutné vybrat podle cílové aplikace, především pak podle zvyklostí a zkušeností s konkrétní metodou. Jejich použití dokládá přesnější odhad integrity bezpečnosti systému než ignorování potenciálních poruch se společnou příčinou.

Výpočet pravděpodobnosti poruchy se společnou příčinou v systémech souvisejících s bezpečností použitím *β* faktoru

Jednou z hojně využívaných metod určených pro modelování poruch se společnou příčinou je výpočet za použití *β* faktoru. Jedná se o výpočet pravděpodobnosti selhání z běžných příčin, kde *β* faktor představuje číslo, kterým se jednoduše vynásobí míra selhání součásti. Určuje procento složky selhání

způsobeného běžnými příčinami a typicky se pohybuje v řádu několika jednotek procent.

β faktor lze určit různými způsoby, z nich norma ČSN EN 61508 uvádí postup založený na seznamu 37 kontrolních otázek rozdělených do 8 typů opatření, která vedou ke snížení CCF. Kontrolní seznam otázek a postup určení *β* faktoru je k nalezení v příloze D normy ČSN EN 61508-6. Jednotlivé otázky (opatření) jsou obodovány a v případě kladné odpovědi, jsou body přičteny. Počet bodů je pro logické obvody jiný než pro senzory a akční členy (logické subsystémy, senzory a akční členy). Dále je v této metodě rozlišeno, zda použití diagnostických testů zvýší účinnost daného opatření (sloupec X) či nikoli (sloupec Y).

Získané body pro kladné odpovědi se nakonec sečtou a danému součtu bodů S (*Score*) je přiřazená hodnota *β* faktoru dle tabulky 13.

Součet bodů pro stanovení *β* faktoru pro nedetekovatelné poruchy:

$$S = \sum_{i=1}^{n} X_i + \sum_{i=1}^{n} Y_i \tag{3.1}$$

Součet bodů pro stanovení β_D faktoru pro detekovatelné poruchy:

$$S_D = (Z + 1) \cdot \sum_{i=1}^{n} X_i + \sum_{i=1}^{n} Y_i \tag{3.2}$$

kde

Z – je faktor stanovený na základě intervalu diagnostického testování (tabulka 14 a 15),

n – je počet otázek.

Větší počet kladných odpovědí na kontrolní otázky (více opatření proti CCF) snižuje hodnotu *β* faktoru. Přístup poskytuje odhad *β* faktoru v rozmezí 0,5 % až 5 % pro logické systémy a 1 % až 10 % pro senzory a akční členy.

Tabulka 13: Výpočet β a β_D.

Součet S (*Score*)	Odpovídající hodnota *β* nebo β_D pro:	
	logický systém	senzor nebo koncový element
120 nebo více	0,5 %	1 %
70 až 120	1 %	2 %
45 až 70	2 %	5 %
méně než 45	5 %	10 %

Tabulka 14: Hodnota Z – programovatelná elektronika.

Diagnostické pokrytí	Hodnota Z dle intervalu diagnostických testů		
	méně než 1 min	mezi 1 min a 5 mi	více než 5 min
≥ 99%	2,0	1,0	0
≥ 90 %	1,5	0,5	0
≥ 60 %	1,0	0	0

Tabulka 15: Hodnota Z – senzory a koncové členy.

Diagnostické pokrytí	Hodnota Z dle intervalu diagnostických testů			
	méně než 2 h	mezi 2 h a 2 dny	mezi 2 dny a 1 týdnem	více než 1 týden
≥ 99%	2,0	1,5	1,0	0
≥ 90 %	1,5	1,0	0,5	0
≥ 60 %	1,0	0,5	0	0

Za předpokladu, že v každém kanálu běží diagnostické testy, lze všechny poruchy lze rozdělit do dvou kategorií: ty, které leží mimo pokrytí diagnostických tesů (nedetekovatelné) a ty, které spadají do pokrytí (detekovatelné).

Celkovou pravděpodobnost poruchy lze vypočítat jako součet intenzit poruch s vlivem a bez vlivu diagnostických testů na CCF:

$$\lambda_D\beta = \lambda_{DU}\beta + \lambda_{DD}\beta_D \tag{3.3}$$

kde

λ_D – je intenzita poruch jednoho kanálu,

β – je β faktor bez uvažování diagnostických testů (nedetekovatelných nebezpečných poruch),

λ_{DU} – je intenzita nebezpečných poruch nedetekovatelných diagnostickými testy,

λ_{DD} – je intenzita nebezpečných poruch detekovatelných diagnostickými testy,

β_D – je β faktor při uvažování nebezpečných poruch detekovatelných diagnostickými testy.

Jak již bylo zmíněno, hodnota β faktoru by se měla určovat pro jednotlivé subsystémy (snímače, logické systém a koncové prvky) samostatně.

Mezi **výhody** určování β faktoru pomocí kontrolního seznamu patří:

- určení β faktoru i bez nutných znalosti historických dat systému,
- určení β faktoru i bez nutnosti testování systému na CCF,
- určení β faktoru i bez jen ze znalosti návrhu systému,
- široká škála opatření proti CCF, plynoucí z kontrolních otázek.

Mezi **nevýhody** lze jmenovat:

- nutnost detailní znalosti návrhu a technického řešení analyzovaného systému,
- odpovědi na otázky ve formě ano/ne.

Možnost odpovídat na kontrolní otázky formou souhlasu nebo nesouhlasu s použitím daného opatření proti CCF se vždy vztahuje na celý analyzovaný systém. To znamená, že pokud je některé opatření z kontrolních otázek použité jen v části systému, je odpověď na danou kontrolní otázku záporná.

Nevýhodu odpovědí formou ano/ne je možné vyřešit doplňující metodou založenou na určování míry splnění daného patření. Jednotlivé odpovědi jsou ve formě vah, která se následně násobí s bodovým ohodnocením konkrétních kontrolních otázek.

Celkový bodový zisk S se poté vypočte pro systémy bez vlivu diagnostických testů na zlepšení opatření proti CCF:

$$S = \sum_{i=1}^{n} u_i \cdot X_i + \sum_{i=1}^{n} w_i \cdot Y_i \tag{3.4}$$

V případě, kdy jsou uvažovány diagnostické testy, je bodový zisk S:

$$S = (Z + 1) \cdot \sum_{i=1}^{n} u_i \cdot X_i + \sum_{i=1}^{n} w_i \cdot Y_i \tag{3.5}$$

kde

w_i – představuje míru splnění opatření proti CCF ve škále $1 \leq w_i \leq 1$, v odpovědích bez uvažování vlivu diagnostického testování,

u_i – představuje míru splnění opatření proti CCF ve škále $1 \leq u_i \leq 1$, v odpovědích s uvažováním vlivu diagnostického testování.

Přístup podle této metody spočívá v tom, že hodnota *β* faktoru odvozená z tabulky 13 je založená na duplexním systému 1oo2. Pro ostatní úrovně redundance (MooN) se používá násobící faktor odvozený v závislosti na celkovém počtu kanálů a provedení hlasovacích obvodů (viz tabulka 16). [40] [41] [42]

Tabulka 16: Výpočet β pro systémy s úrovní redundance vyšší než 1oo2.

MooN		N			
		2	3	4	5
M	1	*β*	0,5 *β*	0,3 *β*	0,2 *β*
	2	-	1,5 *β*	0,6 *β*	0,4 *β*
	3	-	-	1,75 *β*	0,8 *β*
	4	-	-	-	2 *β*

3.7.4 Průběh přiřazení bezpečnostních funkcí

Přiřazený bezpečnostní systém by měl odpovídajícím způsobem naplňovat kladené požadavky na snížení rizika s ohledem na kvalifikaci a prostředky, které jsou k dispozici a to v celém rozsahu životního cyklu celkové bezpečnosti. Už v samotném začátku vývoje bezpečného systému musí být voleny takové konstrukce, se kterými má daná organizace, potažmo přímo návrhář zkušenost a dokáže důsledně zhodnotit všechna rizika plynoucí z jeho použití v konkrétní aplikaci. S tím souvisí nejenom samotné klimatické prostředí, ale i především cílová obsluha a její kvalifikace. Tyto okolnosti je nutné sledovat a v přiřazování bezpečnostních funkcí zohlednit. Často se podcení všechny důsledky plynoucí z použití systémů souvisejících s bezpečností využívající složité technologie – realizace složité technologie si vyžaduje vyšší kvalifikaci na všech stupních, počínaje specifikací až po provoz a údržbu. Naproti tomu požití jednodušších technologických řešení může být stejně účinné a může mít z důvodu nižší složitosti i řadu výhod.

V průběhu přiřazování musí být sledován požadavek splnění nutného snížení rizika. Pokud se nepodaří dosáhnout nutného snížení rizika je přiřazování opakujícím se procesem. Následně se musí modifikovat specifikace řídicího systému EUC a navržené systémy E/E/PE související s bezpečností a přidělení bezpečnostních funkcí se musí opakovat.

Následně je na základě přiřazení klíčových parametrů možné provést přiřazení cílové úrovně integrity bezpečnosti pomocí tabulky 1 uvedené v kapitole 2.6.

Pokud nelze u systémů E/E/PE souvisejících s bezpečností a systémů založených na jiných technických principech prokázat dostatečně nezávislé provedení popsané v kapitole 3.7.2, je nutné použít nejnepříznivější stanovenou hodnotu integrity bezpečnosti. V případě použití úrovně integrity 4, je nutné přijmout doplňující požadavky (viz ČSN EN 61508-1, 7.6.2.11).

Veškeré kroky spojené s přiřazením požadavků a jejich modifikací (viz tabulka 17) musí být dokumentovány včetně všech osob, jejich funkcí, dat a dalších náležitostí nutných pro řádné prokázání shody s normou.

Tabulka 17: Seznam nezbytných aktivit, které musí být stanoveny a dokumentovány ve fázi přiřazení požadavků celkové bezpečnosti.

#	
1	Přidělení bezpečnostních funkcí bezpečnostním systémům a jiným prostředkům pro snížení rizika
2	Snížení rizika a)Použití E/E/PE systémů a b)Jiná opatření
3	Zvážení možnosti společných poruch – nezávislost mezi dvěma nebo několika systémy
4	Určení úrovně integrity bezpečnosti každé bezpečnostní funkce

3.8 Plánování (fáze 6 – 8 ŽC)

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. Požadavky plánování jsou rozděleny na:

- požadavky na instalaci a uvedení do provozu,
- požadavky na platnost celkové bezpečnosti,
- požadavky na provoz a údržbu.

3.8.1 Instalace a uvedení do provozu

Cílem této fáze je sestavení plánu instalace a uvedení do provozu systému souvisejícího s bezpečností.

Plán Instalace musí stanovit:

a) časový rozvrh instalace,
b) osoby odpovědné za instalaci jednotlivých součástí,
c) postupy instalace,
d) sledy činností při začleňování jednotlivých prvků,
e) kritéria pro hodnocení připravenosti k instalaci,
f) postupy řešení případných poruch.

Plán uvedení do provozu stanovuje:

a) časový rozvrh uvedení do provozu,
b) osoby odpovědné za uvedení do provozu,
c) postupy uvedení do provozu.

3.8.2 Platnost celkové bezpečnosti

Cílem tohoto bodu je sestavení plánu usnadňujícího potvrzení platnosti celkové bezpečností. Tento plán musí obsahovat zejména:

a) termín uskutečnění potvrzení platnosti,
b) informace o osobách realizujících a odpovídajících za tento plán,
c) specifikaci všech režimů provozu EUC, včetně vazeb těchto režimů na systémy související s celkovou bezpečností,
d) technickou strategii, která se použije pro ověření tohoto plánu,
e) konkrétní odkaz na každý prvek definovaný ve fázích 4 a 5 ŽC,
f) požadavky na prostředí a prostředky použité k potvrzování platnosti (např. kalibrační nástroje, teplota, apod.),
g) kritéria splnění / nesplnění požadavků jakožto i metody a postupy používané pro hodnocení těchto kritérií.

3.8.3 Provoz a údržba

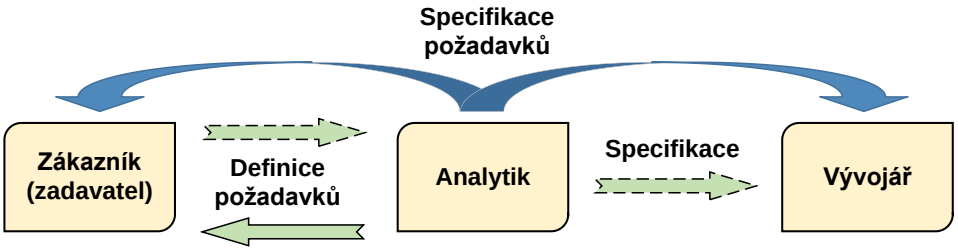
Cílem tohoto bodu je sestavení plánu provozu a údržby E/E/PE systémů a systémů založených na jiných technických principech a to tak, aby bylo zajištěno udržení požadované úrovně integrity bezpečnosti. Mezi požadavky na tuto fázi patří zejména připravit plán obsahující a určující:

a) preventivní činnosti pro udržení funkční bezpečnosti systému;
b) nezbytná omezení, pro jednotlivé činnosti během spouštění, normálního provozu, testování a zastavení provozu E/E/PE systémů;
c) pomocí systematické analýzy stanovit činnosti preventivní údržby za účelem detekce neodhalených vad;

d) zapojení osob odpovědných za budoucí provoz a údržbu systémů souvisejících s bezpečností do tvorby plánu údržby.

3.9 Specifikace požadavků na systém E/E/PE (fáze 9 ŽC)

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



Obrázek 27: Souvislost rolí při specifikaci požadavků.

Specifikace požadavků je souhrnným předpisem pro vývojové pracovníky, kteří ji mohou použít pro výběr zařízení / architektury, návrh a realizaci. Dalo by se říct, že specifikace požadavků je samostatný dokument, podle něhož vývojový pracovník navrhne a realizuje systém tak, aby splnil požadavky specifikace. 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 (důležité body specifikace uvádí tabulky 18 a 19).

V této fázi je nutné specifikovat, jakých požadavků má být v rámci požadované funkční bezpečnosti na daném produktu dosaženo. To se odvíjí především od požadované úrovně funkční bezpečnosti SIL (1-4). Konkrétní požadavky pro tyto úrovně pak předepisuje norma ČSN EN 61508 a to jak pro systém E/E/PE (HW), tak i pro integrovaný SW.

Nedílnou součástí specifikace požadavků je podrobná dokumentace minimálně bodů uvedených v tabulkách 18 a 19, včetně informací kdy a kdo jednotlivé kroky prováděl, jakou měl funkci a dalších náležitostí řádné dokumentace.

Tabulka 18: Důležité body specifikace požadavků pro bezpečnostní funkce.

#	Je nutné specifikovat:
1	Popis všech bezpečnostních funkcí
2	Vlastnosti časové odezvy
3	Rozhraní
4	Všechny příslušné informace k funkční bezpečnosti
5	Rozhraní mezi ostatními systémy
6	Režimy provozu
7	Režimy chování

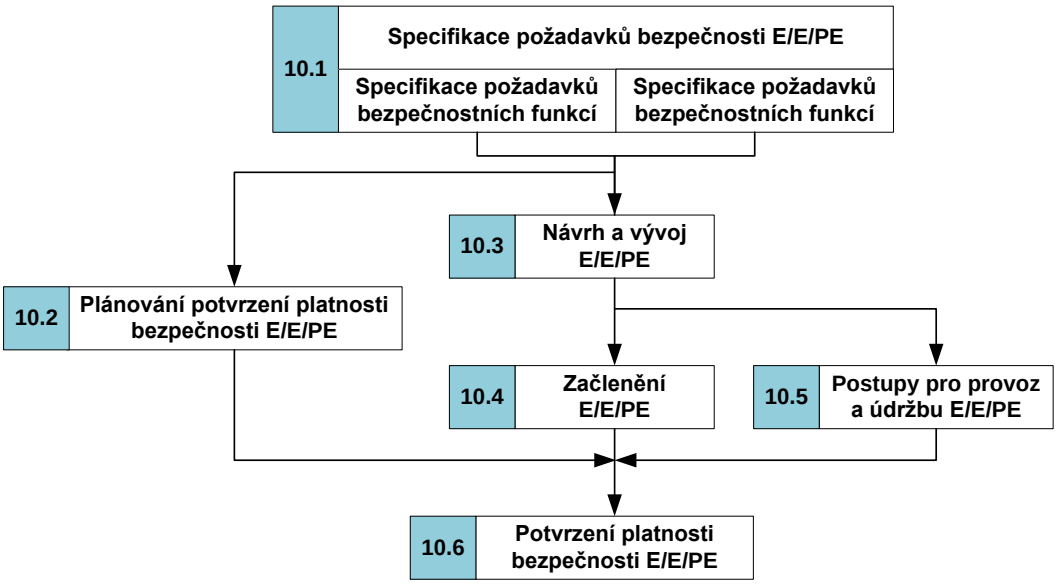
Tabulka 19: Důležité body specifikace požadavků integrity bezpečnosti.

#	Je nutné specifikovat:
1	Úroveň integrity bezpečnosti pro každou bezpečnostní funkci
2	Režim provozu
3	Požadovaný pracovní cyklus a dobu života
4	Požadavky, omezení, funkce a možnosti zkoušení HW před jeho převzetím do provozu
5	Extrémy v podmínkách prostředí
6	Meze elektromagnetické imunity
7	Omezení pro realizaci vlivem poruchy se společnou příčinou

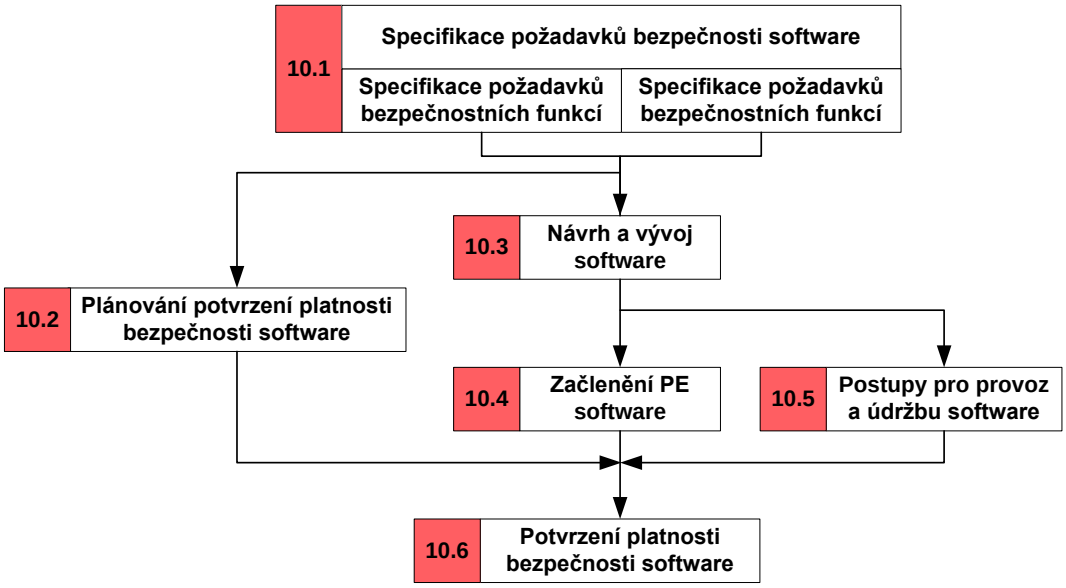
3.10 Systémy E/E/EP související s bezpečností – realizace (fáze 10 ŽC)

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 8), který

by měl mít podobu zobrazenou na obrázku 28 pro hardware a obrázku 29 pro software.



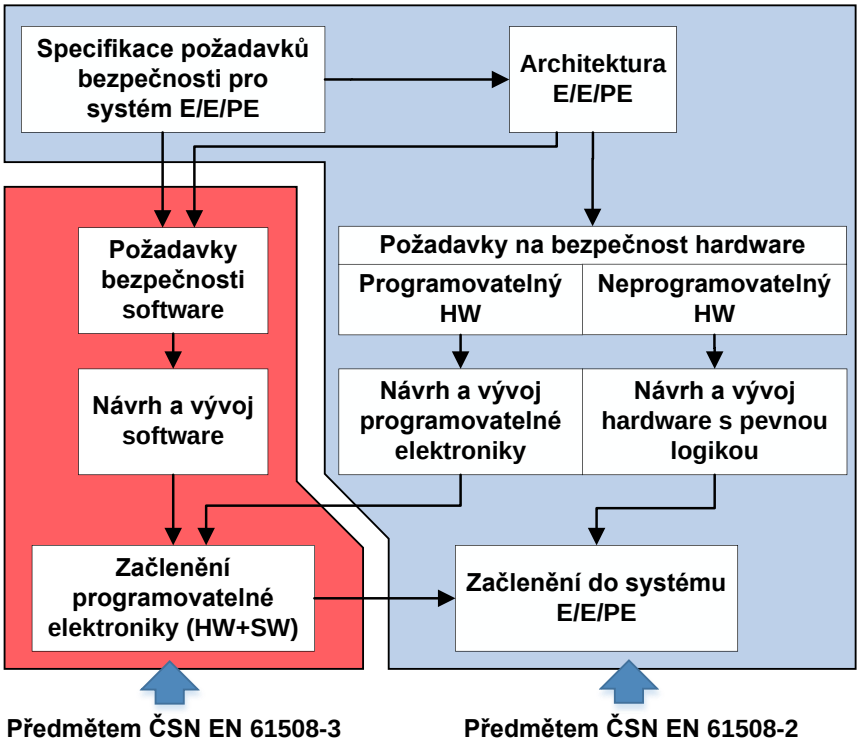
Obrázek 28: Životní cyklus bezpečnosti systému E/E/PE souvisejícího s bezpečností – hardware.



Obrázek 29: Životní cyklus bezpečnosti systému E/E/PE souvisejícího s bezpečností – software.

V případě použití struktury odlišné od struktury uvedené na těchto obrázcích je nutné toto rozhodnutí zdůvodnit a bez výjimek dodržet všechny požadavky uvedené v příslušných normách. Tyto požadavky jsou, stejně jako v předchozím

případě (životního cyklu celkové bezpečnosti), definovány pro jednotlivé fáze odděleně. Detailní požadavky fáze realizace jsou specifikovány v normách ČSN EN 61508-2 (hardware) a ČSN EN 61508-3 (software). Rozsah použití obou částí je znázorněn na obrázku 30, kde je v poměrně jednoduché formě vidět přímá provázanost mezi hardwarem a softwarem.



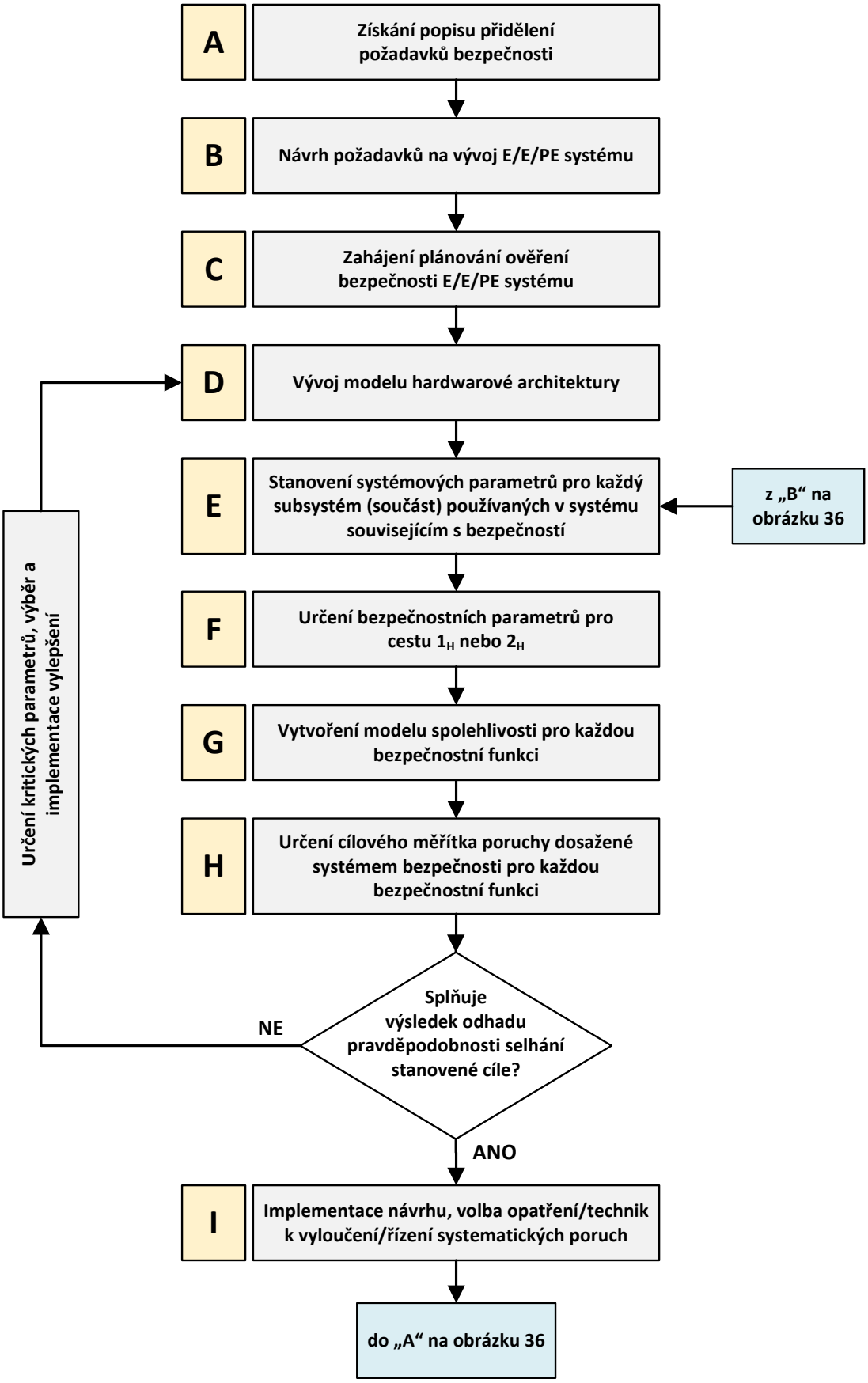
Obrázek 30: Vztah aplikačních oblastí ČSN EN 61508-2 a ČSN EN 61508-3.

ČSN EN 61508-2 definuje požadavky na dosažení integrity bezpečnostni hardwaru pro E/E/PE bezpečnostní systémy včetně snímačů a konečných prvků. Norma uvádí vhodnou kombinaci technik a opatření pro zajištění vlivu náhodných a systematických HW poruch.

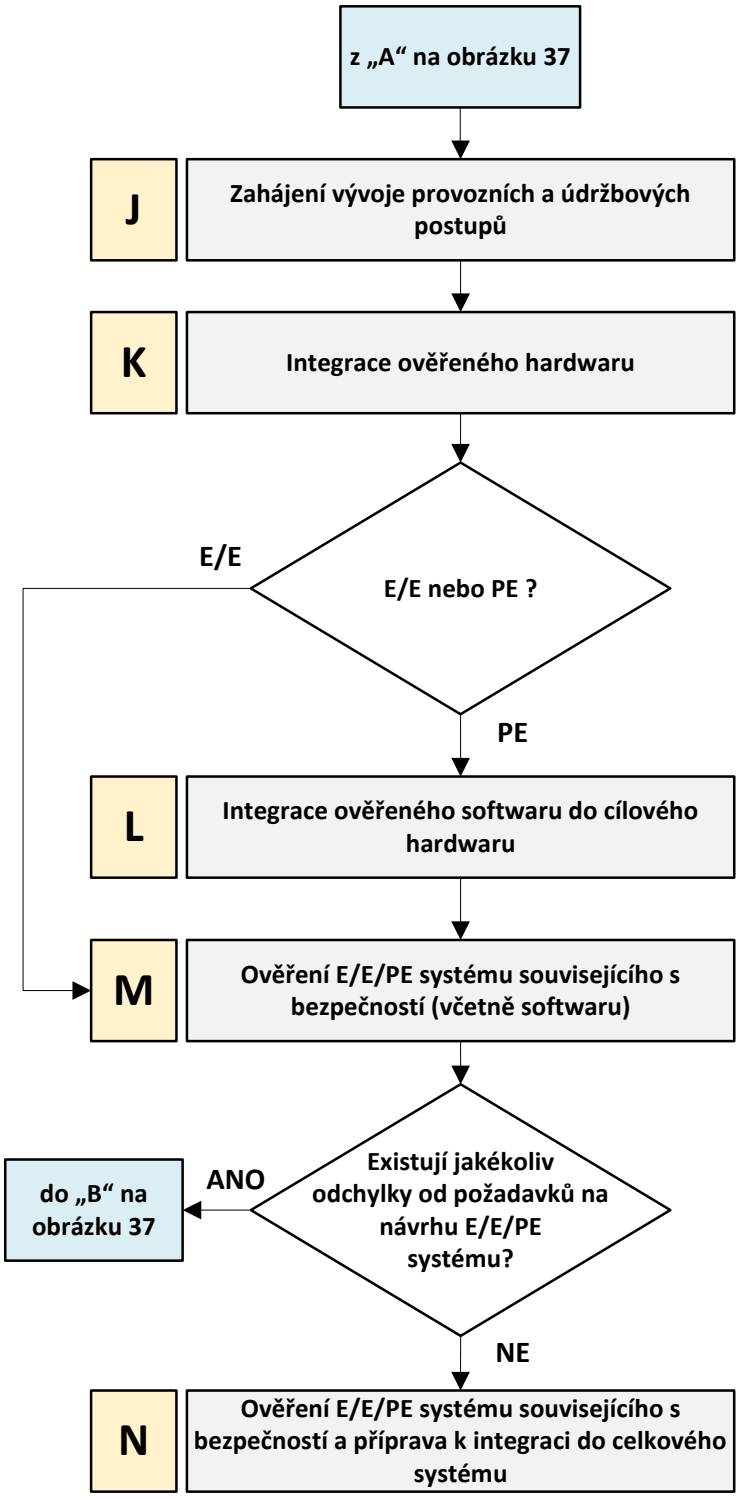
ČSN EN 61508-3 poskytuje požadavky na dosažení integrity bezpečnosti embedded (vestavěné, jednoúčelové systémy) nebo aplikačního software. Norma vyžaduje kombinaci principů softwarového inženýrství jako jsou: design shora dolů; modularita; ověření každé fáze vývoje životního cyklu; ověřené softwarové moduly a knihovny softwarových modulů a další metody k usnadnění ověřování a validace, protože neexistuje známý způsob, jak prokázat neexistenci závad v rozumně složitém softwaru souvisejícího s bezpečností.

Vzhledem k rozsahu této práce se následující kapitoly detailně věnují pouze hardwarové části, tj. požadavky na E/E/PE systémy související s bezpečností. Požadavky na software, jakož to druhá část realizace, jsou zpracovány stručněji a dávají pouze obecný přehled technik a opatření.

Způsob, jakým je běžně postupováno ve fázi realizace, se řídí definovaným životním cyklem, který jasně určuje strukturu uspořádání požadavků pomocí modelu vývojového procesu, ve kterém fáze navazují v definovaném pořadí s malou iterakcí. Někdy je označován jako model vodopádu. Proces vývoje je tedy složen z návazných kroků jejichž uspořádání zobrazují obrázky 31 a 32.



Obrázek 31: Funkční kroky aplikace normy ČSN EN 61508-2.



Obrázek 32: Funkční kroky aplikace normy ČSN EN 61508-2 (pokračování).

A) Získání přidělení požadavků bezpečnosti (viz kapitola 7.6 normy ČSN EN 61508-1) a případná aktualizace plánování bezpečnosti v průběhu vývoje systému bezpečnosti E/E/PE.

B) Návrh požadavků na vývoj bezpečnostního systému E/E/PE, včetně požadavků na integritu bezpečnosti pro každou bezpečnostní funkci (viz kapitola 7.2 normy ČSN EN 61508-2). Přidělení požadavků na software a předání dodavateli nebo vývojáři softwaru při aplikaci ČSN EN 61508-3.

C) Počátek fáze plánování ověření bezpečnosti systému E/E/PE (viz kapitola 7.3 normy ČSN EN 61508-2).

D) Specifikace (konfigurace) architektury logického podsystému, senzorů a koncových prvků souvisejících s bezpečností E/E/PE. Ověření architektury hardwaru a architektury softwaru s dodavatelem/vývojářem softwaru. Stanovení bezpečnostních důsledků z nekonzistentních rozdílů hardwaru a softwaru (viz Obrázek 30). Pokud je to nutné, je tento krok opakován.

E) Vývoj modelu hardwarové architektury pro E/E/PE bezpečnostní systém zkoumáním jednotlivých bezpečnostních funkcí samostatně a určení subsystémů (komponent), které se mají být využity k provádění těchto funkcí.

F) Stanovení systémových parametrů pro každý subsystém používaný v E/E/PE systému. Pro každý subsystém musí být určen:

- interval kontrolních testů na poruchy, které nejsou odhaleny samočinně,
- střední doba do obnovy,
- diagnostické pokrytí (viz příloha C normy ČSN EN 61508-2),
- pravděpodobnost poruchy,
- architektonická omezení pro cestu 1_H (viz kapitola 7.4.4.2 a příloha C normy ČSN EN 61508-2) a pro cestu 2_H (viz kapitola 7.4.4.3 normy ČSN EN 61508-2).

G) Tvorba modelu spolehlivosti pro každou bezpečnostní funkci, kterou má bezpečnostní E/E/PE systém provádět. Model spolehlivosti je matematický

vzorec, který ukazuje vztah mezi spolehlivostí a relevantními parametry zařízení a podmínek jeho použití.

H) Výpočet odhadu spolehlivosti pro každou bezpečnostní funkci pomocí vhodné techniky. K dispozici je řada modelovacích metod a analytik by si měl vybrat, která z nich je nejvhodnější (viz příloha B normy ČSN EN 61508-2). Porovnání výsledku s cílovými opatřeními stanovenými v bodě B výše a požadavky cesty 1_H (viz kapitola 7.4.4.2 normy ČSN EN 61508-2) nebo cesty 2_H (viz kapitola 7.4.4.3 normy ČSN EN 61508-2). Pokud odhadovaná spolehlivost nesplňuje cílovou míru selhání a / nebo nesplňuje požadavky cesty 1_H nebo cesty 2_H, pak je nutné změnit:

- jeden nebo více parametrů subsystému pokud je to možné (přechod zpět na F výše), a / nebo
- hardwarovou architekturu (přechod zpět na D výše).

I) Implementace návrhu E/E/PE systému bezpečnosti. Výběr opatření a technik pro kontrolu systematických poruch hardwaru, poruch způsobených vlivy prostředí a provozních poruch (viz příloha A normy ČSN EN 61508-2).

J) Tvorba manuálů a postupů pro uživatele a pracovníky údržby (viz kapitola 7.6 a příloha B normy ČSN EN 61508-2).

K) Začlenění a vyzkoušení systému podle stanoveného postupu (viz bod C). Zkoušky musí prokázat, že všechny moduly vzájemně správně reagují a plní jejich předpokládané funkce a jsou navrženy tak, aby neprováděly žádné nepředpokládané funkce.

L) Integrace ověřeného softwaru na cílový hardware (viz kapitola 7.5 a příloha B normy ČSN EN 61508-2).

M) Ověření celého E/E/PE systému včetně integrovaného softwaru (viz kapitola 7.7 a příloha B normy ČSN EN 61508-2).

N) Předání hardwaru a výsledků ověření bezpečnosti systémovým inženýrům pro další integraci do celkového systému.

Řada činností, které na obrázcích nejsou zobrazeny, probíhá v průběhu celého bezpečnostního životního cyklu systému E/E/PE. Patří k nim ověření (viz kapitola 7.9 normy ČSN EN 61508-2) a posouzení funkční bezpečnosti (viz kapitola 8 normy ČSN EN 61508-1), které se provádějí v průběhu každé příslušné fáze.

Při uplatňování výše uvedených kroků musí být vybrány bezpečnostní techniky a opatření odpovídající požadované úrovni bezpečnostní integrity. Pro jejich vývěr byly formulovány tabulky, v nichž jsou různé techniky a opatření rozdělené podle čtyř úrovní integrity bezpečnosti (viz příloha B normy ČSN EN 61508-2).

Musí být zdůvodněny a dokumentovány výběry zvolených technik a opatření pro všechny uvedené kroky. Musí být také dokumentovány i ověření a posouzení funkční bezpečnosti každé fáze.

V následujících kapitolách jsou popsány důležité požadavky kladené normou ČSN EN 61508-2 na návrh a vývoj systému souvisejícího s bezpečností. Pro jednotlivé požadavky jsou uvedeny možnosti jak je splnit a tím dosáhnout shody s touto částí normy. Ve většině případů je možné si vybrat, jak požadavky splnit. Poté už záleží na konkrétní aplikaci a možnostech společnosti, jakou cestou se ke splnění požadavků vydá.

3.10.1 Specifikace požadavků návrhu systému E/E/PE (fáze 10.1 ŽC)

Specifikace požadavků návrhu systému E/E/PE musí obsahovat podrobnosti celého hardwaru a softwaru nezbytné pro realizaci bezpečnostních funkcí. Běžně je odvozena ze specifikace požadavků na systém E/E/PE rozložením bezpečnostních funkcí a k nim přiřazených subsystémů (např. skupina senzorů, logických prvků nebo akčních členů). Subsystémy mohou být dále rozloženy do prvků a architektur, tak aby byly jasné pro pochopení osobám, u nichž je pravděpodobné, že budou tyto informace využívat v rámci všech stupňů životního cyklu.

Horším případem je situace, kdy jsou v jednom E/E/PE systému souvisejícím s bezpečností implementovány jak bezpečnostní, tak i jiné než bezpečnostní funkce. Může to znamenat nejen zvýšení složitosti, ale především větší problémy

s plněním činností životního cyklu bezpečnosti E/E/PE (např. návrh, potvrzení platnosti, odhad funkční bezpečnosti a údržba).

Výstupem specifikace požadavků návrhu E/E/PE systému je podrobný popis (řádná dokumentace) nejen samotného zařízení a použité architektury, ale i celého hardwaru a softwaru, který je nezbytný pro realizaci bezpečnostních funkcí. Stejně jako u specifikace požadavků na systém je u specifikace požadavků návrhu systému řečeno, jaké požadavky bezpečnostních funkcí mají být naplněny, nikoli jak toho má být dosaženo.

3.10.2 Plánování potvrzení platnosti bezpečnosti systému E/E/PE (fáze 10.2 ŽC)

Fáze plánování potvrzení platnosti bezpečnosti je prováděna souběžně s návrhem a vývojem systému. Plán musí být zpracován tak, aby stanovoval jednotlivé kroky (jak procedurální, tak technické), které jsou nutné k tomu, aby se prokázalo, že E/E/PE systém související s bezpečností splňuje specifikaci požadavků návrhu systému E/E/PE (viz předchozí kapitola). Při jeho sestavování je třeba se zaměřit na body uvedené v tabulce 20.

Tabulka 20: Důležité body plánu potvrzení platnosti bezpečnosti E/E/PE systému

#	Musí se vzít v úvahu:
1	všechny požadavky definované ve specifikaci požadavků na systém E/E/PE a specifikaci požadavků návrhu systému E/E/PE
2	postupy použité pro potvrzení platnosti správné realizace každé bezpečnostní funkce a kritéria vyhověl / nevyhověl pro provádění zkoušek
3	postupy použité pro potvrzení platnosti, že každá bezpečnostní funkce má požadovanou integritu bezpečnosti a kritéria vyhověl/nevyhověl pro provádění zkoušek
4	požadované prostředí, ve kterém má zkoušení probíhat včetně všech nezbytných nástrojů a zařízení (a také plán týkající se kalibrace těchto zařízení)
5	postupy pro vyhodnocování zkoušek (spolu s příslušným odůvodněním)

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

6	zkušební postupy a kritéria hodnocení vlastností použitá pro potvrzení platnosti stanovených mezí odolnosti proti elektromagnetickému rušení
7	rozhodovací postupy pro řešení poruch při potvrzování platnosti

3.10.3 Návrh a vývoj systému E/E/PE (fáze 10.3 ŽC)

Jak již bylo v minulé kapitole zmíněno, 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.

Obecně jsou požadavky návrhu a vývoje systému souvisejícího s bezpečností založeny na těchto principech:

- Integrita bezpečnosti HW
  - Vhodná odolnost proti chybám (omezení daná architekturou HW)
  - Omezená pravděpodobnost nebezpečné chyby (bezpečnostní integrita HW)
- Předcházení systematickým chybám (systematická bezpečnostní integrita)
- Definované reakce na poruchu (zajištění nebezpečné vady)
- Zajištění komunikačního procesu (požadavky pro datové komunikace)
- Speciální archytektura IO s čipovou redundancí

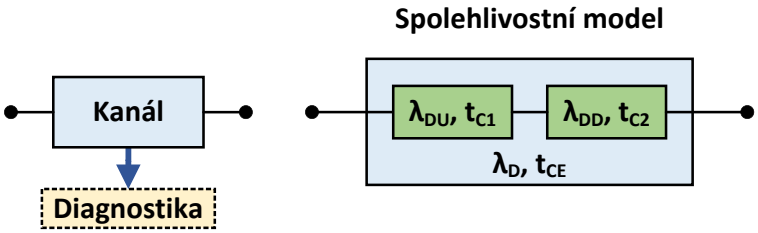
Pokud se vývojář zaměří na tyto zmíněné oblasti, naplní všechny důležité části návrhu. V následujících podkapitolách jsou zmíněné oblasti vysvětleny.

3.10.3.1 Používané architektury

Mezi nejpoužívanější architektury patří:

Architektura 1oo1

Blokové uspořádání této architektury a tomu odpovídající schéma spolehlivostního modelu uvádí obrázek 33. Architektura je tvořena jediným kanálem, kdy porucha znamená ztrátu bezpečnostní funkce při jejím vyžádání.



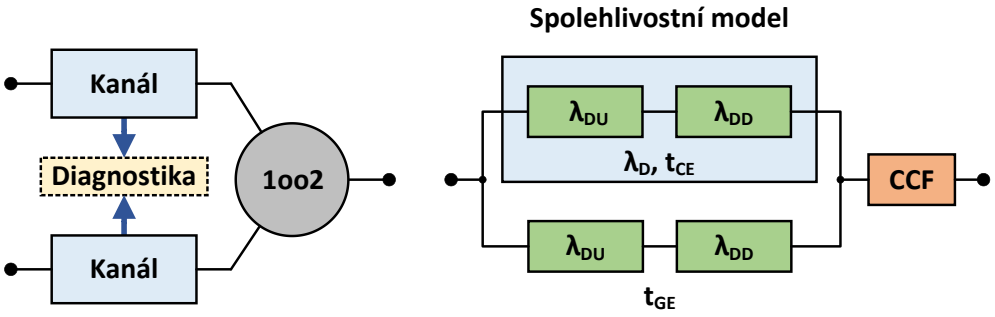
Obrázek 33: Blokové schéma architektury 1oo1 a tomu odpovídající spolehlivostní schéma.

Spolehlivostní model je sériové spojení dvou bloků, kdy první blok reprezentuje nebezpečné nedetekované poruchy a druhý blok poruchy nebezpečné detekovatelné.

Architektura 1oo2

Tuto architekturu tvoří dva nezávislé kanály, kde je účinek nebezpečného selhání minimalizován, jelikož každý kanál může zajistit přechod do bezpečného stavu. Architektura 1oo2 nabízí nízkou pravděpodobnost selhání, zvyšuje však bezpečnost systému. Diagnostika nemá vliv na žádné výstupní stavy nebo na

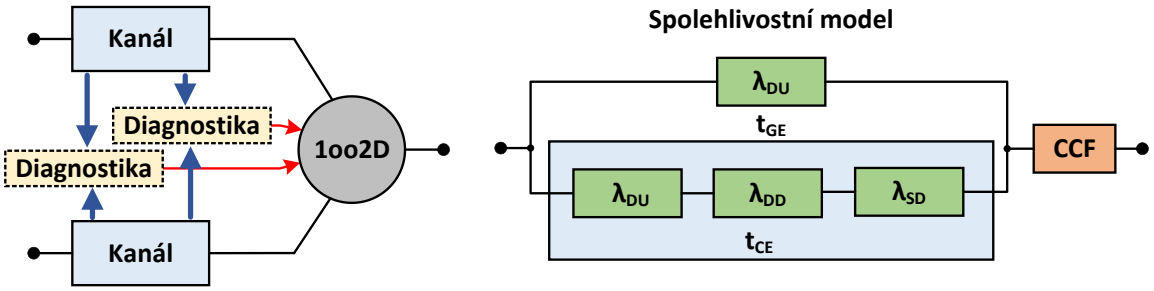
rozhodování výstupů při zjištění vady. Blokové schéma a spolehlivostní model pro tuto architekturu zobrazuje obrázek 34.



Obrázek 34: Blokové schéma architektury 1oo2 a tomu odpovídající spolehlivostní schéma.

Architektura 1oo2D

Tuto architekturu tvoří dva kanály stejně jako u předchozí architektury 1oo2, navíc ale zahrnuje diagnostiku pro zlepšení integrity bezpečnosti. Diagnostika umožňuje, aby detekované nebezpečné selhání bylo zajištěno přechodem systému do bezpečného stavu. Blokové schéma a spolehlivostní model pro tuto architekturu zobrazuje obrázek 35.

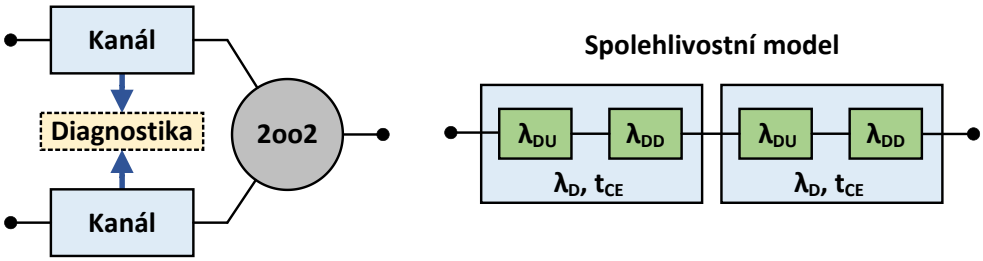


Obrázek 35: Blokové schéma architektury 1oo2D a tomu odpovídající spolehlivostní schéma.

Architektura 2oo2

Tato architektura je tvořena dvěma paralelně spojenými kanály tak, že v případě poruchy v jednom kanále je funkce zajištěna druhým kanálem. V této architektuře je sice zvýšena spolehlivost oproti architektuře 1oo2, ale naopak je snížena bezpečnost. K samotné aktivaci bezpečnostní funkce je totiž potřeba vyžádání obou kanálů. Diagnostika nemá vliv na žádné výstupní stavy nebo na rozhodování

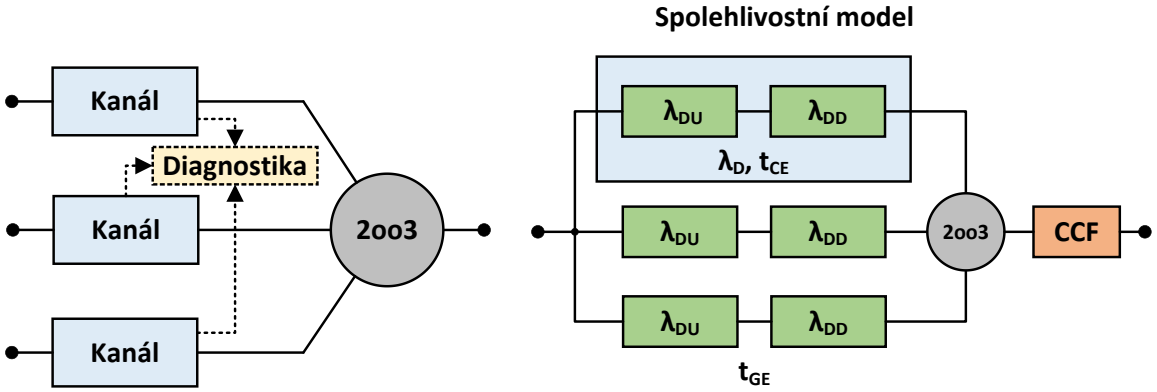
výstupů při zjištění vady. Blokové schéma a spolehlivostní model pro tuto architekturu zobrazuje obrázek 36.



Obrázek 36: Blokové schéma architektury 2oo2 a tomu odpovídající spolehlivostní schéma.

Architektura 2oo3

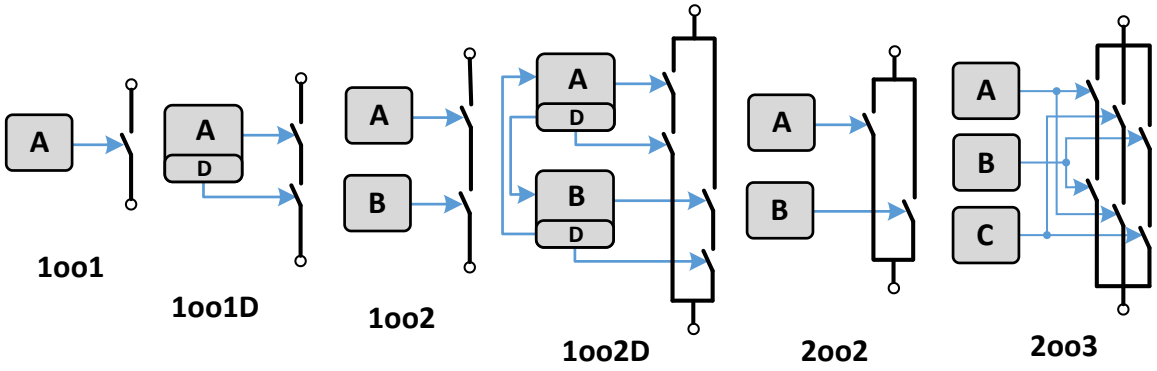
Architekturu tvoří tři paralelně spojené kanály s majoritním (většinovým) hlasovacím obvodem. Výstupní stav je dán shodným výsledkem minimálně dvou kanálů. Tato architektura slučuje výhody 1oo2 a 2oo2 – zajišťuje zvýšení jak spolehlivosti, tak integrity bezpečnosti, ale nese s sebou i vyšší systémové náklady. Diagnostika nemá vliv na žádné výstupní stavy nebo na rozhodování výstupů při zjištění vady. Blokové schéma a spolehlivostní model pro tuto architekturu zobrazuje obrázek 37.



Obrázek 37: Blokové schéma architektury 2oo3 a tomu odpovídající spolehlivostní schéma.

Hlasovací obvody

Všechny architektury, vyjma 1oo1 složené pouze z jednoho kanálu, využívají pro nastavení výstupního stavu hlasovací obvod. V závislosti na typu architektury se liší i struktura a hlasovací obvody a jejich způsob rozhodování.



Obrázek 38: Logická interpretace architektur a jejich hlasovacích obvodů.

Na obrázku výše je možné vidět interpretaci zmíněných architektur, včetně 1oo1D a 1oo2D, u nichž diagnostika umožňuje, aby detekované nebezpečné selhání bylo zajištěno přechodem systému do bezpečného stavu.

3.10.3.2 Architektonická omezení

Požadavky architektonického omezení stanovují maximální možnou úroveň SIL použitelnou pro konkrétní architekturu systému. Architektonická omezení jsou v návrhu zahrnuta za účelem dosažení dostatečně robustní architektury, přičemž se bere v úvahu úroveň komplexnosti subsystémů. Úroveň integrity bezpečnosti hardwaru odvozená prostřednictvím aplikace požadavků architektonického omezení je maximum, co se připouští nárokovat, přestože v některých případech by se mohla teoreticky odvodit vyšší úroveň integrity bezpečnosti, pokud byl pro systém schválen výhradně matematický přístup.

Pro určení maximální úrovně integrity bezpečnosti, která může být nárokována pro konkrétní bezpečnostní funkci, uvažuje norma dvě možné cesty:

- **Cesta 1_H** – založená na toleranci vady HW a koncepci poměru bezpečných poruch SFF (*Safe Failure Fraction*).
- **Cesta 2_H** – založená na složce spolehlivosti dat ze zpětné vazby od koncového uživatele, zvýšené úrovni víry a odolnosti proti hardwarovým vadám pro stanovené úrovně integrity bezpečnosti.

Výběr cesty závisí na oblasti použití a měly by se při jejím výběru uvážit následující faktory:

- porucha jedné bezpečnostní funkce může vytvořit nové nebezpečí nebo být dodatečnou událostí k existujícímu nebezpečí,
- redundance nemusí být praktická pro všechny funkce,
- opravy nejsou vždy možné nebo rychlé (např. ani proveditelné během doby, která je zanedbatelná vzhledem k intervalu kontrolních zkoušek).

Pokud navrhujeme bezpečnostní funkce v systému, který je nový a nemáme žádná data z předchozích verzí, případně z provozu podobných zařízení, je výhodnější použít cestu 1_H.

Dále je nutné jednotlivé prvky systému nebo celé subsystémy kategorizovat do dvou možných skupin:

- **Typ A**

Subsystém se může považovat za typ A, pokud u součástí požadovaných pro dosažení bezpečnostní funkce:

- jsou režimy poruchy všech podstatných součástí dobře definovány,
- lze úplně určit chování subsystému při podmínkách poruchy,
- jsou k dispozici dostatek spolehlivých dat o poruše ze zkušeností z provozu, aby se mohlo prokázat, že nárok na četnosti poruchy pro detekované i nedetekované nebezpečné poruchy je splněn.

- **Typ B**

Subsystém se musí považovat za typ B, pokud u součástí, u nichž se požaduje dosáhnout bezpečnostní funkce, není jedno nebo více kritérií pro Typ A splněno.

Cesta 1_H

Tato cesta je založená na toleranci vady HW a koncepci poměru bezpečných poruch (SFF – *Safe Failure Fraction*). Určení maximální úrovně integrity bezpečnosti nárokované pro s ohledem na stanovenou bezpečnostní funkci se řídí postupem, který uvádí tabulka 21.

Tabulka 21: Postup určení maximální úrovně integrity bezpečnosti nárokované s ohledem na stanovenou bezpečnostní funkci použitím cesty 1_H.

#	
1	Definování subsystému vytvořením systému E/E/PE souvisejícího s bezpečností.
2	Určení poměru bezpečných poruch pro všechny prvky v subsystému odděleně (tj. na základě jednotlivého prvku s každým prvkem s odolností k hardwarovým vadám 0).
3	Určení poměru bezpečných poruch a odolnosti k vadám hardwaru u každého prvku za účelem určení maximální úrovně integrity bezpečnosti, která může být požadována.
4	Určení maximální úrovně integrity bezpečnosti, která může být požadována pro subsystém použitím pravidel pro paralelní nebo sériovou kombinaci prvků.
5	Maximální úroveň integrity bezpečnosti, která může být požadována pro systém E/E/PE související s bezpečností, musí být určena subsystémem, který dosáhl nejnižší úroveň integrity bezpečnosti.

Odolnost hardwaru proti vadám

Určité struktury / architektury systému mohou být navržené tak, že chyba vzniklá v systému nezpůsobí ztrátu bezpečnostní funkce a říkáme, že systém má „odolnost proti hardwarovým vadám N“, někdy také uváděné jako „tolerance hardwarové poruchy N“ (HFT – *Hardware Fault Tolerance*).

Tabulka 22: Vztah mezi redundancí a HFT.

Architektura	Redundance	HFT
XooY		= Y - X
1oo1	No redundancy	0
1oo2	Dual	1
2oo2	No redundancy	0
1oo3	Triple	2
2oo3	Triple	1
2oo4	Quadruple	2

Odolnost hardwaru proti vadám 0 znamená, že pokud dojde k chybě, systém nebude schopen plnit svou bezpečnostní funkci. Obecně *N* + 1 vyjadřuje nejmenší počet chyb, které by způsobili ztrátu bezpečnostní funkce. Při určování odolnosti se nesmí brát v úvahu další opatření, která mohou účinky chyb řídit – například diagnostika.

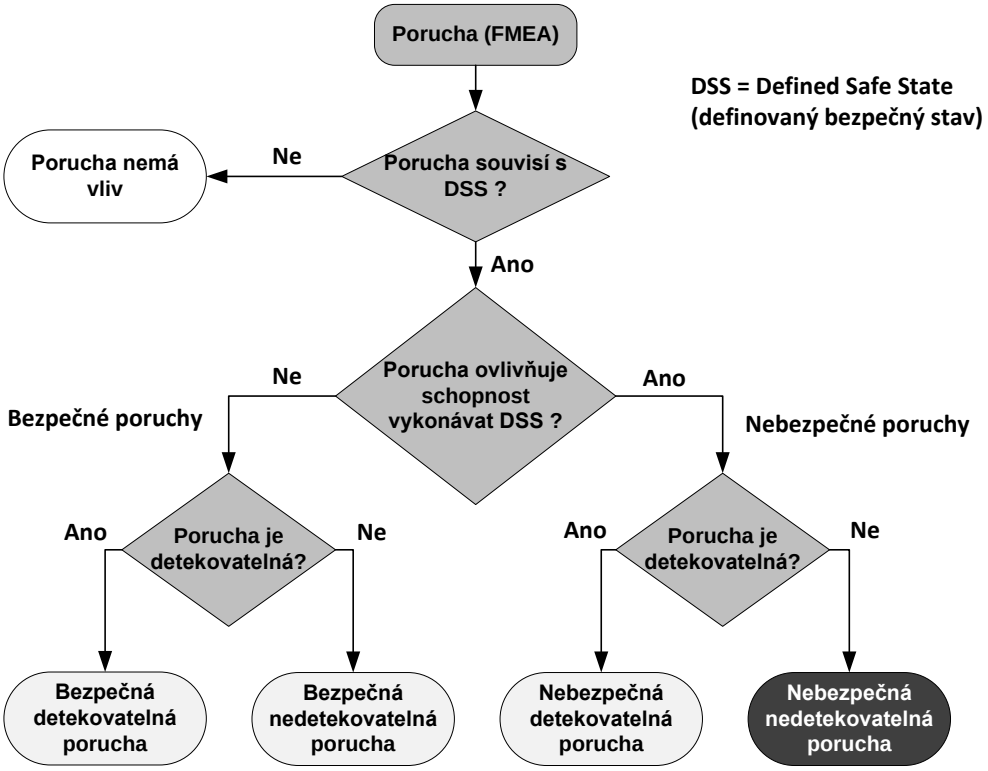
Odolnost proti vadám hardwaru mají obecně redundantní systémy. Například pokud tedy bude systém postaven na dvoukanálové struktuře, může systém dále pracovat s jednou poruchou (v jednom kanále) – odolnost proti hardwarovým vadám N = 1. Pro ztrátu bezpečnostní funkce takového systému by muselo dojít k poruše v obou kanálech.

Pro jednotlivé bezpečnostní funkce systému platí určitá omezení nejvyšší úrovně integrity bezpečnosti související se strukturou/architekturou systému.

Poměr bezpečných poruch hardwarových prvků

Při analýze systému je rozlišováno pět typů poruch, které je možné uvažovat. Klasifikace těchto pěti poruch závisí na bezpečnostní funkci systému a jeho architektuře.

První typ poruchy klasifikovaný jako *No Effect Failure* (Porucha nemá vliv) nemá vliv na bezpečnostní funkci systému (například informační indikátor) a nebude zahrnuta do žádného výpočtu PFD a PFH. Neměla by být zahrnuta ani do výpočtu poměru bezpečných poruch SFF (Safe Failure . Zbývající čtyři typy poruch jsou hodnoceny s ohledem na bezpečnostní funkci systému a musí být zahrnuty do výpočtu SFF, PFD a PFH. Pomůckou k rozdělení jednotlivých poruch je obrázek 39.



Obrázek 39: Klasifikace poruch.

Pokud porucha narušuje bezpečnostní funkci systému a není zjistitelná, je hodnocena jako nebezpečná nedetekovatelná porucha (λ_{Du}). Pokud porucha narušuje bezpečnostní funkci systému, ale je detekovatelná diagnostickými opatřeními, předpokládá se, že diagnostika zajistí odpovídající reakci systému, nebo že porucha bude opravena, je klasifikována jako nebezpečná detekovatelná porucha (λ_{Dd}). V případě, že je v systému pracujícího v režimu s vysokým vyžádáním diagnostikována porucha, dochází k automatickému aktivování bezpečnostní funkce systému nebo k převedení systému do bezpečného stavu. V případě systému pracujícího v režimu s nízkým vyžádáním je pro operátora postačující upozornění, aby bylo možné opravit systém. Pokud porucha nenarušuje bezpečnostní funkci systému, je hodnocena jako bezpečná porucha (λ_S).

Poměr bezpečných poruch SFF je definován jako poměr četnosti bezpečných poruch plus nebezpečných detekovatelných poruch a všech poruch:

$$SFF = \frac{\lambda_S + \lambda_{Dd}}{\lambda_S + \lambda_{Dd} + \lambda_{Du}} \tag{3.6}$$

Maximální úroveň integrity bezpečnosti

Nejvyšší úroveň integrity bezpečnosti, která se může nárokovat pro bezpečnostní funkci je omezena odolností hardwaru proti vadám a poměrem četnosti bezpečných poruch subsystému, který provádí takovou bezpečnostní funkci. Nejvyšší úroveň integrity bezpečnosti danou kombinací obou omezení uvádí tabulka 23 pro subsystémy typu A a tabulka 24 pro subsystémy typu B.

Tabulka 23: Maximální dovolená úroveň integrity bezpečnosti pro bezpečnostní funkci prováděnou prvkem nebo subsystémem typu A souvisejícím s bezpečností.

Poměr bezpečných poruch prvku	Odolnost proti vadám hardwaru		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

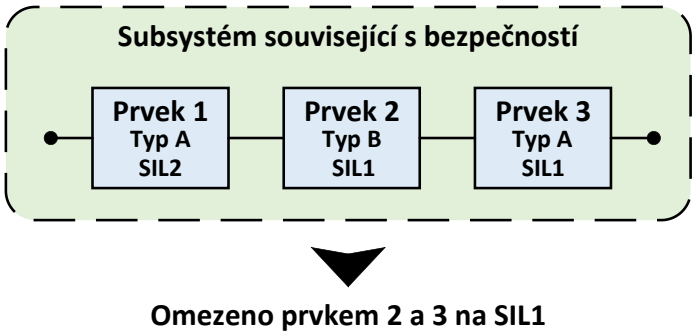
Tabulka 24: Maximální dovolená úroveň integrity bezpečnosti pro bezpečnostní funkci prováděnou prvkem nebo subsystémem typu B souvisejícím s bezpečností.

Poměr bezpečných poruch prvku	Odolnost proti vadám hardwaru		
	0	1	2
< 60 %	Není dovoleno	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Maximální úroveň integrity bezpečnosti kombinace více prvků

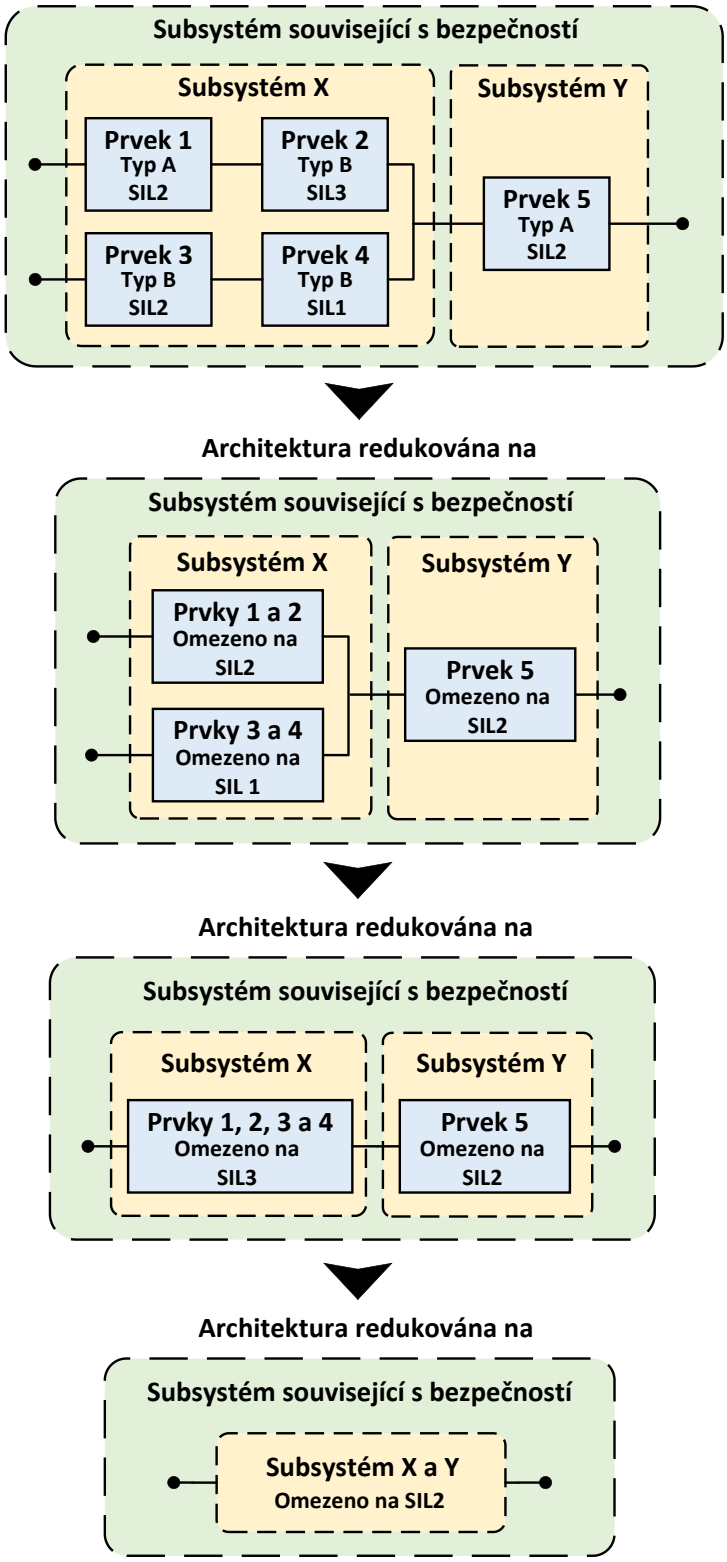
V subsystémech souvisejících s bezpečností, kde jsou prvky bezpečnostní funkce řazeny pomocí sériové kombinace (viz například obrázek 40), je uvažovaná

maximální úroveň integrity bezpečnosti určena prvkem s nejnižší úrovní integrity bezpečnosti.



Obrázek 40: Určení maximální SIL pro specifickou architekturu subsystému složeného z několika prvků v sérii.

V subsystému souvisejícího s bezpečností, kde je bezpečnostní funkce realizována prostřednictvím více kanálů (kombinace paralelních prvků) s odolností proti vadám hardwaru N, je maximální požadovaná úroveň integrity bezpečnosti určena výběrem kanálu s nejvyšší úrovně integrity bezpečnosti zvýšené o N. Příklad viz obrázek 41.



Obrázek 41: Určení maximální SIL pro specifickou architekturu subsystému složeného ze dvou subsystémů X a Y.

Cesta 2_H

Tato cesta je založená na složce spolehlivosti dat ze zpětné vazby od koncového uživatele, zvýšené úrovni víry a odolnosti proti hardwarovým vadám pro stanovené SIL. Určení minimální úrovně odolnosti HW proti vadám se řídí postupem, který uvádí tabulka 25.

Tabulka 25: Postup určení minimální úrovně odolnosti HW proti vadám nárokované s ohledem na stanovenou SIL použitím cesty 2_H.

#	
1	Definování subsystému vytvořením systému E/E/PE souvisejícího s bezpečností.
2	Získání spolehlivostních dat pro kvantifikaci vlivu náhodných HW vad.
3	Určení průměrné úrovně nejistoty každého parametru spolehlivosti (např. četnost poruch PFD nebo PFH) použitých pro výpočet.
4	Určení minimální úrovně odolnosti proti HW vadám pro funkce související s bezpečností.

Spolehlivost dat použitých pro kvantifikaci vlivu náhodných HW vad

V případě použití cesty 2_H musí být data pro kvantifikaci vlivu náhodných hardwarových vad získaná ze zpětné vazby prvků použitých v podobné aplikaci a prostředí nashromážděna dle příslušných norem (např. ČSN EN 60300-3-2 nebo ČSN EN ISO 14224), tak aby se určila průměrná úroveň nejistoty (např. rozsah důvěry 90 % nebo spolehlivost rozdělení) každého parametru spolehlivosti (např. četnost poruch) použitých pro výpočet. Cílem norem je povzbuzovat koncové uživatele organizovat příslušné sestavy dat spolehlivosti.

Při výpočtu cílových opatření proti poruchám se musí vzít v úvahu data spolehlivosti nejistoty a systém musí být vylepšován, dokud není důvěra větší než 90 %, aby se dosáhlo cílové míry opatření proti poruchám. Pro všechny prvky typu B nesmí být diagnostické menší než 60 %.

Určení minimální úrovně odolnosti proti HW vadám

Minimální úroveň odolnosti proti hardwarovým vadám, která se může nárokovat pro bezpečnostní funkci, je určena stanovenou úrovní integrity bezpečnosti viz tabulka 26.

Tabulka 26: Minimální odolnost proti HW vadám pro funkci souvisejícím s bezpečností.

Úroveň integrity bezpečnosti	Minimální odolnost proti HW vadám	
	Režim s nízkým vyžádáním	Režim s vysokým vyžádáním (souvislý režim)
SIL 4	2	2
SIL 3	1	1
SIL 2	0	1
SIL 1	0	0

Požadavky na minimální odolnost proti hardwarovým vadám definované v tabulce mohou být sníženy za předpokladu, že by mohly vnášet dodatečné poruchy a vést ke snížení celkové bezpečnosti EUC. To platí pro případy, kdy je požadovaná odolnost proti hardwarovým vadám větší než 0, a kdy jsou v subsystému použity prvky typu A. V takovém případě může být použita bezpečnější varianta architektury se sníženou odolností proti hardwarovým vadám, ale musí být zdokumentováno a zdůvodněno, že předpokládaná alternativní architektura poskytuje rovnocenné nebo lepší řešení. Například: zpětnovazební uspořádání; použití spolehlivějších položek se stejnou technologií; snížením dopadu poruch se společnou příčinou použitím diverzifikované technologie.

Když je odolnost proti hardwarovým vadám snížena na nulu, je možné určité chyby vynechat za předpokladu, že pravděpodobnost jejich výskytu je vzhledem k požadavkům integrity bezpečnosti subsystému velmi malá (četnost nebezpečných poruch všech sériových prvků, na něž je požadováno vypuštění poruch by nemělo nepřekročit 1 % uvažovaných cílových opatření proti poruchám). Všechna takováto vynechání musí být zdůvodněna a uvedena v dokumentaci a musí být posouzena při zvažování potenciálu k systematickým chybám.

3.10.3.3 Náhodné HW poruchy

Náhodná hardwarová porucha je způsobena jednou nebo několika možnými degradačními mechanizmy. Objevují se na různých součástech a jejich výrobní tolerance mohou vyvolat poruchu po různé nepředvídatelné době provozu (tj. náhodně). Četnost těchto poruch nelze přesně určit, protože závisí na mnoha okolnostech, které jednotlivé prvky ovlivňují – zvolená technologie výroby, typ stavebního prvku, kvalita výroby, způsob použití, pracovní prostředí atd. Lze ji ale s přihlédnutím ke zmíněným okolnostem odhadnout.

Pro analýzu integrity bezpečnosti E/E/PE systémů souvisejících s bezpečností je k dispozici celá řada metod pro odhad dosažené míry poruch (např. *analýza stromu poruch* (FTA), *analýza způsobů a důsledků poruch* (FMEA), *spolehlivostní schémata bezporuchovosti* (RBD), *Petriho sítě*, *Markovovy modely*, apod. viz ČSN EN 61508-7). Mezi nejpoužívanější patří metoda spolehlivostních schémat bezporuchovosti a Markovovy modely. Obecně všechny tyto metody poskytují pro méně složité systémy obdobné výsledky, ale v případě složitých programovatelných elektronických subsystémů se mohou získané výsledky drobně lišit. V případě spolehlivostních schémat je to způsobeno zejména nutností výsledné schémata zjednodušit, proto aby byla tyto schémata prakticky řešitelná.

Průměrná pravděpodobnost selhání bezpečnostní funkce určuje podle vztahu (3.7) pro systémy pracující v režimu s nízkým vyžádáním a (3.8) pro systémy pracující v režimu s vysokým nebo nepřetržitým vyžádáním.

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} \tag{3.7}$$

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} \tag{3.8}$$

kde

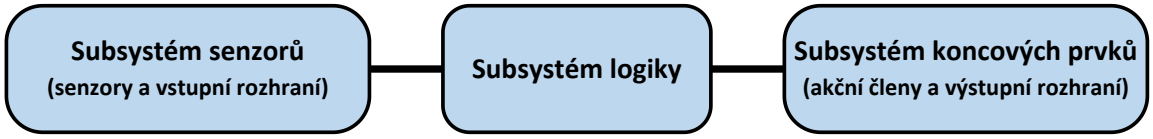
PFx_{SYS} – je průměrná pravděpodobnost selhání pro celý E/E/PE bezpečnostní systém,

PFx_S – je průměrná pravděpodobnost selhání pro subsystém senzorů,

PFx_L – je průměrná pravděpodobnost selhání pro subsystém logiky,

PFx_{FE} – je průměrná pravděpodobnost selhání pro subsystém koncových prvků.

V obou případech se jedná o součet pravděpodobností poruchy jednotlivých částí každého subsystému (senzorů, logiky a koncových prvků), jejichž základní strukturu naznačuje Obrázek 42.



Obrázek 42: Základní struktura systému.

Každý subsystém se řeší samostatně a může být tvořen libovolným počtem komponent. Při určení průměrné pravděpodobnosti selhání každého subsystému se postupuje podle přílohy B normy ČSN EN 61508-6 a podobně i v [43] dle následujícího schématu:

Tabulka 27: Postup při výpočtu pravděpodobnosti selhání.

#	
1	Nakreslit blokové schéma znázorňující jednotlivé součásti subsystému logiky, senzorů a koncových prvků. Do těchto subsystémů je možné zahrnout i přizpůsobovací obvody v podobě převodníků, oddělovačů, budičů, apod.
2	Určit režim provozu systému a jeho jednotlivých prvků. Zde přicházejí v úvahu dva režimy vyžádání: a) režim s nízkým vyžádáním; b) režim s vysokým (nepřetržitým) vyžádáním.
3	Pro každou rozhodovací skupinu subsystémů definovat: a) architekturu, b) diagnostické pokrytí každého kanálu, c) intenzitu poruch, d) činitele společných poruch.
4	V případech, kdy bezpečnostní funkce závisí na více než jedné skupině senzorů, logiky, nebo akčních prvků, se určí výsledná hodnota PFD_S, nebo PFH_S konkrétní skupiny podle vzorce (3.9).

$$PFx_S = \sum_i PFx_{Gi} \tag{3.9}$$

V souvislosti s výpočtem pravděpodobnosti selhání se výše uvedené výpočty vztahují vždy ke konkrétní architektuře a režimu systému.

Vztahy pro režim provozu s nízkým vyžádáním

- Ekvivalentní střední doba prostoje kanálu pro architektury:

  1oo1, 1oo2, 2oo2 a 2oo3

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{3.10}$$

  1oo2D

$$t_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) \cdot MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}} \tag{3.11}$$

  kde T_1 je interval kontrolní zkoušky a MTTR je střední doba do obnovy.

- Ekvivalentní střední doba prostoje systému pro architektury:

  1oo2 a 2oo3.

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{3.12}$$

  1oo2D

$$t_{GE} = \frac{\lambda_{DU}\left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) \cdot MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}} \tag{3.13}$$

- Pravděpodobnost selhání na vyžádání PFD kanálu pro architektury:

  1oo1

$$PFD = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \tag{3.14}$$

  1oo2

$$PFD = 2[(1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} \cdot t_{GE} + \\ +\beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \tag{3.15}$$

  1oo2D

$$PFD = 2(1-\beta_D) \cdot \lambda_{DU} \cdot [(1-\beta) \cdot \lambda_{DU} + (1-\beta_D) \cdot \lambda_{DD} + \lambda_{SD}] \cdot \\ \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \tag{3.16}$$

  2oo2

$$PFD = 2 \cdot \lambda_D \cdot t_{CE} \tag{3.17}$$

  2oo3

$$PFD = 6[(1-\beta_D) \cdot \lambda_{DU} + (1-\beta_D) \cdot \lambda_{DU}]^2 \cdot t_{CE} \cdot t_{GE} + \\ +\beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \tag{3.18}$$

Vztahy pro režim provozu s vysokým vyžádáním

- Ekvivalentní střední doba prostoje kanálu pro architektury se určuje shodně jako pro režim provozu s nízkým vyžádáním, tedy pomocí vztahu (3.10) případně (3.11).
- Pravděpodobnost selhání na vyžádání PFH kanálu pro architektury:

1oo1

$$PFH = 2 \cdot \lambda_{DU} \tag{3.19}$$

1oo2

$$PFH = 2[(1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{3.20}$$

1oo2D

$$PFH = 2(1-\beta) \cdot \lambda_{DU} \cdot [(1-\beta) \cdot \lambda_{DU} + (1-\beta_D) \cdot \lambda_{DD} \cdot \lambda_{SD}] \cdot t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{3.21}$$

2oo2

$$PFH = 2 \cdot \lambda_D \tag{3.22}$$

2oo3

$$PFH = 6[(1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{3.23}$$

Pro dosažení integrity bezpečnosti systému souvisejícího s bezpečností musí být dle uvedených vztahů proveden odhad pravděpodobnosti poruchy pro každou bezpečnostní funkci a musí být roven nebo menší než cílová míra poruch specifikovaná v požadavcích E/E/PE systému.

Jestliže pro určitý návrh nejsou dosaženy požadavky integrity bezpečnosti pro určitou bezpečnostní funkci, potom se musí určit prvky, subsystémy a/nebo parametry přispívající nejvíce k funkcím počítané četnosti poruch a zvážit vliv možného zlepšení opatření na identifikované kritické prvky, subsystémy nebo parametry (např. spolehlivější součástky, doplňkové ochrany proti poruchám se společnou příčinou, zvýšení diagnostického pokrytí, zvýšení redundance, snížení intervalu kontrolních zkoušek, rozložení zkoušek, atd.). Následně vybrat a realizovat použitelné zlepšení a opakovat nezbytné kroky pro zřízení nové pravděpodobnosti náhodné hardwarové poruchy.

3.10.3.4 Integrita systematické bezpečnosti

Integrita systematické bezpečnosti je část integrity bezpečnosti systému souvisejícího s bezpečností vztahující se k systematickým poruchám

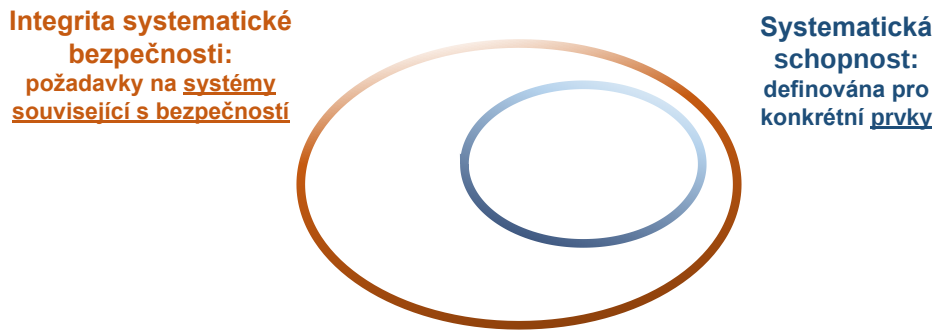
v nebezpečném stavu poruchy. Systematické poruchy oproti náhodným hardwarovým nelze vzhledem k jejich povaze odhadnout a přesně statisticky kvantifikovat, protože události vedoucí k nim nelze jednoduše předvídat. Je možné je odstranit jen změnou návrhu (konstrukce) nebo výrobního procesu, provozních postupů, dokumentace nebo jiných souvisejících činitelů. Typickými představiteli systematických poruch jsou:

- chyby v projektu (hardware i software),
- vliv okolí (např. teplota, vibrace),
- úpravy po uvedení do provozu,
- chyby v údržbě.

Vedle integrity systematické bezpečnosti a systematické poruchy soubor norem ČSN EN 61508 určuje tzv. systematickou schopnost. Systematická schopnost (SC – *Systematic Capability*) je opatření důvěry, že prvek splňuje požadavky integrity systematické bezpečnosti stanovené úrovně SIL.

SC < N >	se vytahuje k	SIL < N >
SC 1 …	*splňuje požadavky na systematickou integritu bezpečnosti*	… SIL 1
SC 2 …		… SIL 2
SC 3 …		… SIL 3
SC 4 …		… SIL 4

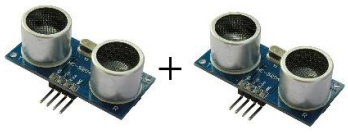
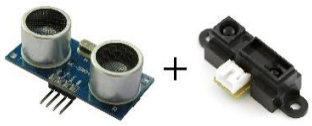
Vztahuje se vždy na konkrétní prvek, je-li použit podle pokynů příslušné bezpečnostní příručky.



Obrázek 43: Vztah integrity systematické bezpečnosti a systematické schopnosti.

E/E/PE systém související s bezpečností může být rozdělen na prvky s rozdílnou systematickou schopností, přičemž lze její koncepci použít na softwarové i hardwarové prvky. Vhodnou kombinací vzájemně nezávislých prvků lze dosáhnout systematické schopnosti (N+1).

Tabulka 28: Příklad systematické schopnosti.

Integrita HW	Systematická schopnost	Architektura	Celková schopnost SIL
SIL 2	SC 2		SIL 2 Omezeno integritou HW a systematickou schopností
SIL 3	SC 2		SIL 2 Systematická integrita je omezena na SC 2, chybí diverzita
SIL 2	SC 2		SIL 2 Omezeno integritou HW a systematickou schopností
SIL 3	SC 3		SIL 2 Diverzita umožňuje zvýšit SC o 1

Požadavky na systematickou integritu bezpečnosti (systematickou schopnost) je možné dle normy ČSN EN 61508 dosáhnout jednou z následujících cest:

- **Cesta 1S** – založená na použití vhodných technik a opatření v rámci ŽC,
- **Cesta 2S** – založená na doložení, že zařízení se osvědčilo v provozu,
- **Cesta 3S** – založená na shodě s požadavky ČSN EN 61508-3 (jen pro existující SW prvky).

Cesta 1S

Tato cesta směřuje na použití vhodných technik a opatření v celém rozsahu životního cyklu tak, aby se zabránilo zavádění systematických chyb během vývoje a návrhu hardwaru i softwaru. Doporučené techniky a opatření uvádí příloha B

normy ČSN EN 61508-2. V návrhu je také nutné počítat s lidskými schopnostmi pro předcházení kritických omylů operátorů nebo pracovníků údržby, kteří by měli mít odpovídající znalosti a úroveň výcviku.

Tabulka 29: Požadavky pro řízení a předcházení systematických chyb.

#	Pro vyhovění požadavků na integritu bezpečnosti je nutné:
1	Zvolit metody návrhu odpovídající dané úrovni integrity bezpečnosti.
2	Provádět zkoušky a testy použitím automatizovaných systémů a integrovaných vývojových prostředků.
3	V návrhu zohlednit odolnost proti: a) vnějším vlivům prostředí včetně EM rušení, b) omylům operátorů, c) zbytkovým vadám v návrhu HW a SW, d) chybám v procesech datové komunikace.

Cesta 2S

Požadavky integrity bezpečnosti lze naplnit i doložením, že zařízení se osvědčilo v provozu. Snahou této cesty je maximální uplatnění již existujících ověřených subsystémů. Ideálním stavem je 100 % shody funkčnosti, kapacity a charakteristiky existujícího subsystému s novými požadavky, ale pokud to struktura ověřeného subsystému umožňuje, je přípustné vybrat pouze funkce vyžadované danou aplikací. Na druhou stranu nevyužité funkce příliš složitého subsystému mohou být z hlediska bezpečnosti škodlivé.

Tabulka 30: Požadavky pro doložení, že se prvky osvědčily v provozu.

#	Prvek je pokládán za osvědčený z provozu:
1	Má-li jasně omezenou a specifikovanou funkcionalitu.
2	Je-li doloženo, že: a) pravděpodobnost nebezpečných systematických chyb je dostatečně nízká, b) předchozí podmínky používání jsou stejné, nebo dostatečně podobné, c) četnost nebezpečných poruch nepřekračuje předchozí použití, d) prvek podporuje požadovanou bezpečnostní funkci s požadovanou integritou systematické bezpečnosti.
3	Byla provedena analýza provozních zkušeností určité konfigurace prvku spolu s analýzou vhodností a zkoušek v zamýšlené aplikaci.

Cesta 3s

Tato cesta směřuje na již existující softwarové prvky a použití celé nebo části jejich bezpečnostní funkce. Existující softwarové prvky při tom původně nemusely být vyvinuty specificky pro systém související s bezpečností. Použití předběžného softwaru (*pre-existing software*) se řídí dle příručky bezpečnosti (viz příloha D normy ČSN EN 61508-2 a příloha D normy ČSN EN 61508-3), která poskytuje dostatečně přesný a úplný popis prvku, který umožňuje posouzení integrity určité bezpečnostní funkce.

Příručka bezpečnosti může být odvozena z vlastní dokumentace a záznamů o procesu vývoje dodavatele prvku, nebo může být vytvořena doplněním dalšími kvalifikačními činnostmi. V některých případech může být využito reverzního inženýrství pro vytvoření specifikace nebo projektové dokumentace odpovídající požadavkům této klauzule, s výhradou platných právních podmínek (např. autorských práv nebo práv duševního vlastnictví).

3.10.3.5 Reakce na poruchu

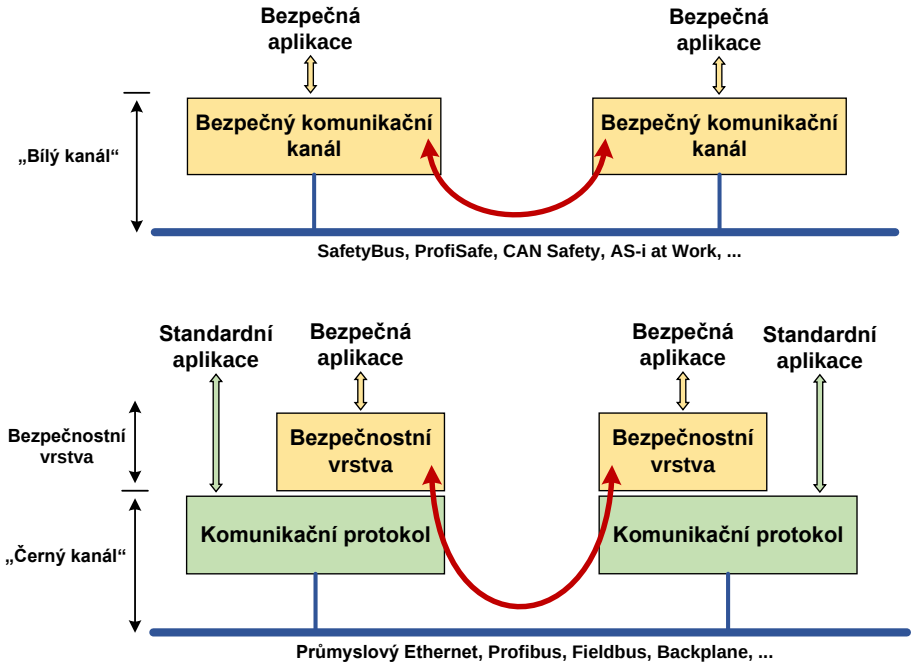
Vedle funkční bezpečnosti, která se zabývá především chováním zařízení v bezporuchovém stavu, tj. stav, kdy zařízení vykonává předepsané a prověřené funkce tak, jak má, existuje pojmem technická bezpečnost rozšiřující požadavky o chování zařízení v poruchovém stavu. Požadavky na technickou bezpečnost stanovují, že v případě definované poruchy zařízení zaujme předem stanovený bezpečný stav. Za bezpečný stav lze bez ohledu na režimu provozu a odolnosti proti vadám hardwaru považovat například bezpečné vypnutí EUC, nebo části EUC.

U redundantních struktur (HFT > 0) lze v případě detekce nebezpečné poruchy oddělit vadnou část subsystému tak, aby mohl pokračovat bezpečný stav EUC, zatímco je vadná část opravena.

Naproti tomu u jednokanálových struktur (bez redundance) je možné opravit vadný subsystém v rámci střední doby opravy (MRT – *Mean Repair Time*). Během opravy musí být zajištěna bezpečnost EUC doplňkovými opatřeními a omezeními, stanovených v provozních a údržbových postupech.

3.10.3.6 Datové komunikace

Pro většinu významných průmyslových sběrnic byly vyvinuty varianty splňující požadavky funkční bezpečnosti komunikačního kanálu (*SafetyBus, ProfiSafe* - bezpečné profily k protokolu *Profibus* a *Profinet*, *Interbus – safety, CAN safety, AS-i at work* a další). Princip bezpečné komunikace vychází především z normy ČSN EN 61508, která uvažuje dvě možnosti realizace, tzv. bílý kanál a černý kanál.



Obrázek 44: Princip „Černého kanálu“

V obou případech stále platí, že funkční bezpečnost musí být zaručena i v případě selhání bezpečnostních funkcí řídicího (nebo komunikačního) systému. Návrh i realizace bezpečné komunikace musí být potvrzeny podle souboru norem ČSN EN 61508-3 a ČSN EN 61784-3, případně ČSN EN 50159.

V případě bílého kanálu jsou požadavky uvedených norem implementovány do celého komunikačního kanálu (včetně protokolu a síťových součástí).

Princip černého kanálu je založen na standardním komunikačním kanálu, u kterého je funkční bezpečnost implementována v podobě bezpečné vrstvy vložené nad nebo do 7. vrstvy komunikačního modelu. Výhodou je, že není potřeba nějak koncepčně zasahovat do existujícího standardu, který přitom nebyl navržen s ohledem na budoucí požadavky funkční bezpečnosti.

3.10.3.7 Speciální architektury IO s čipovou redundancí

Vedle základních požadavků návrhu E/E/PE systémů umožňuje norma ČSN EN 61508 použití čipové redundance pro integrované obvody se společným polovodičovým substrátem (viz ČSN EN 61508-2 Příloha E). Jejich použití omezuje soubor požadavků jako je například omezení nejvyšší integrity bezpečnosti do úrovně SIL3. Tyto požadavky vzcházejí z faktu, že je tato metoda stále velmi mladá a norma se k ní staví velmi konzervativně. Proto také norma pracuje s požadavky vztahujícími se pouze na digitální integrované obvody. Pro analogové a smíšené integrované obvody s čipovou redundancí žádné požadavky neurčuje. Jejich použití se tím velmi komplikuje, jelikož není prokazování bezpečnosti podloženo splněním konkrétních požadavků na bezpečnost. Obecně je použití čipové redundance v systému souvisejícího s bezpečností podmíněno řádným zdůvodněním, že je dosaženo stejné úrovně nezávislosti mezi různými kanály pomocí různých souborů opatření.

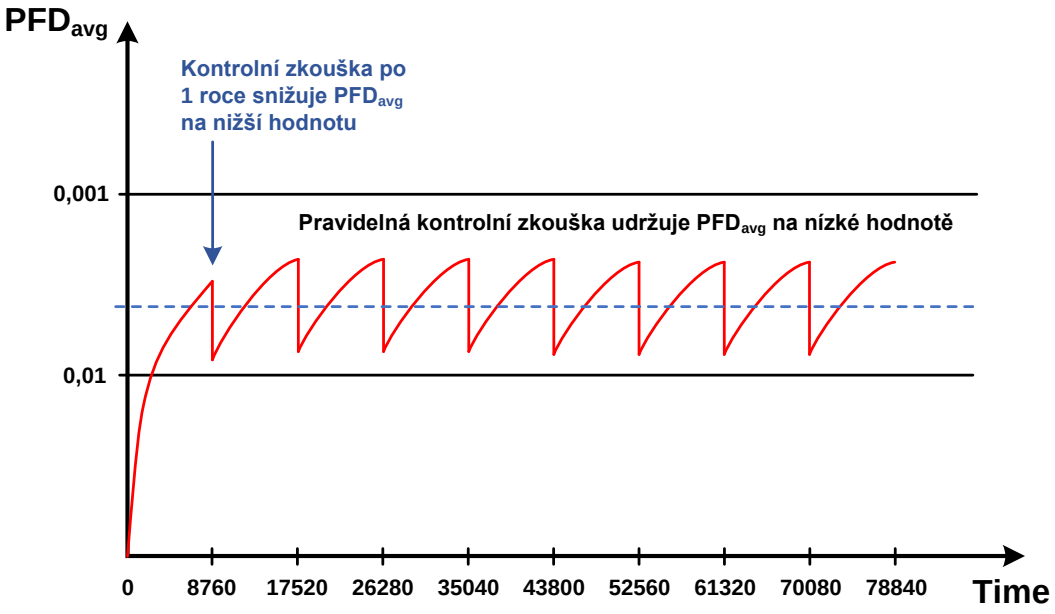
3.10.4 Začlenění systému E/E/PE (fáze 10.4 ŽC)

Začlenění všech modulů do E/E/PE systému souvisejícího s bezpečností provází zkoušky, které musí prokázat, že všechny moduly vzájemně správně reagují, plní jejich předpokládané funkce a neprovádí žádné nepředpokládané funkce. Veškeré výsledky zkoušek se musí dokumentovat. Z důvodu předcházení chybám během začleňování systému E/E/PE se musí používat vhodná skupina technik a opatření podle tabulky B.3 normy ČSN EN 61508-2.

3.10.5 Postupy pro provoz a údržbu systému E/E/PE (fáze 10.5 ŽC)

Posouzení lidských faktorů je klíčovým činitelem při určování činností požadovaných na udržení funkční bezpečnosti sestavy (tak jak byla navržena) systému souvisejícího s bezpečností. Musí být navrženy systematické metody postupů pro cílovou skupinu osob provádějících provoz a údržbu. Metody musí popisovat činnosti a omezení, která jsou nezbytná pro zabránění nebezpečných stavů. Vhodné techniky a opatření uvádí tabulka B.4 normy ČSN EN 61508-2.

Postupy provozu a údržby zahrnují vedle rutinních oprav a případné modifikace softwaru provádění analýzy bezporuchovosti hardwaru. Pravděpodobně největšími činiteli v udržování integrity bezpečnosti hardwaru jsou četnost kontrolních zkoušek a interval diagnostických testů. Proto úkolem analýzy bezporuchovosti hardwaru je zajistit, aby četnosti těchto dvou typů zkoušek odpovídaly cílové integritě bezpečnosti hardwaru.



Obrázek 45: Vztah mezi kontrolní zkouškou a PFD_{avg}.

3.10.6 Potvrzení bezpečnosti systému E/E/PE (fáze 10.6 ŽC)

Potvrzení bezpečnosti E/E/PE systému probíhá s ohledem na požadavky bezpečnostních funkcí a požadavků na integritu bezpečnosti definovaných ve specifikaci požadavků návrhu systému (viz kapitola 3.10.1) a probíhá, tak jak bylo naplánováno ve fázi 10.2 (viz kapitola 3.10.2). Součástí ověření mohou být i měření kalibrovanými měřicími přístroji.

Potvrzení se provádí ještě před instalací, nicméně je možné provést potvrzení až po instalaci. Například, pokud se vývoj aplikačního softwaru může dokončit až po instalaci.

Výstupem potvrzení bezpečnosti je dokumentace výsledků zkoušek platnosti bezpečnosti E/E/PE systému. Doporučený seznam zkoušek, technik a opatření proti chybám během potvrzování bezpečnosti E/E/PE systému je uveden v tabulce B.5 normy ČSN EN 61508-2.

3.11 Jiná opatření pro snížení rizika (fáze 11 ŽC)

Pojmem *jiná opatření snižující riziko* se rozumí technologie, jež jsou založeny na jiných technických principech než elektrických / elektronických nebo programovatelných elektronických (například hydraulických, pneumatických apod.). Jiná opatření mohou být založena i na fyzikální struktuře jako jsou odtokový systém, odstředivá brzda apod. Pro splnění požadavků bezpečnostních funkcí a požadavků na integritu bezpečnosti musí být všechna jiná opatření snižující riziko specifikována podobně jako E/E/PE systémy, ale jelikož se jedná o jiné technologie, nejsou předmětem normy ČSN EN 61508.

3.12 Celková instalace a uvedení do provozu (fáze 12 ŽC)

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 viz kapitola 3.8.1. Všechny jednotlivé činnosti musí být dokumentovány, především případy, ve kterých byly řešeny poruchy a nekompatibility.

3.13 Potvrzení celkové bezpečnosti (fáze 13 ŽC)

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. Oproti potvrzení bezpečnosti E/E/PE systému (viz kapitola 3.10.6) 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. Podobně mohou být součástí ověření i měření kalibrovanými měřicími přístroji. Výstupem potvrzení celkové bezpečnosti je dokumentace výsledků zkoušek platnosti bezpečnosti.

3.14 Provoz, údržba a opravy (fáze 14 ŽC)

Celkový provoz, údržba a opravy představují nutné činnosti na udržení požadované funkční bezpečnosti definované plánem (viz kapitola 3.8.3). 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.

3.15 Modifikace a zdokonalování (fáze 15 ŽC)

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.

3.16 Vyřazení z provozu a likvidace (fáze 16 ŽC)

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

Jasně definovat požadavky na bezpečnost a určitou úroveň integrity bezpečnosti pro generickou aplikaci je téměř nemožné, jelikož nejsou jasně stanoveny podmínky provozu a s tím spojené rizikové situace, které mohou nastat. Nelze předem předvídat, do jakého prostředí bude systém použit, jaká bude jeho přesná úloha a jaké bezpečnostní funkce budou od systému požadovány. Jedním z velkých projektů, u kterého byla snaha aplikovat normy v maximální míře, je například univerzální řídicí systém REMCS (podrobnější popis systému v kapitole 4.5.1). 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 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.

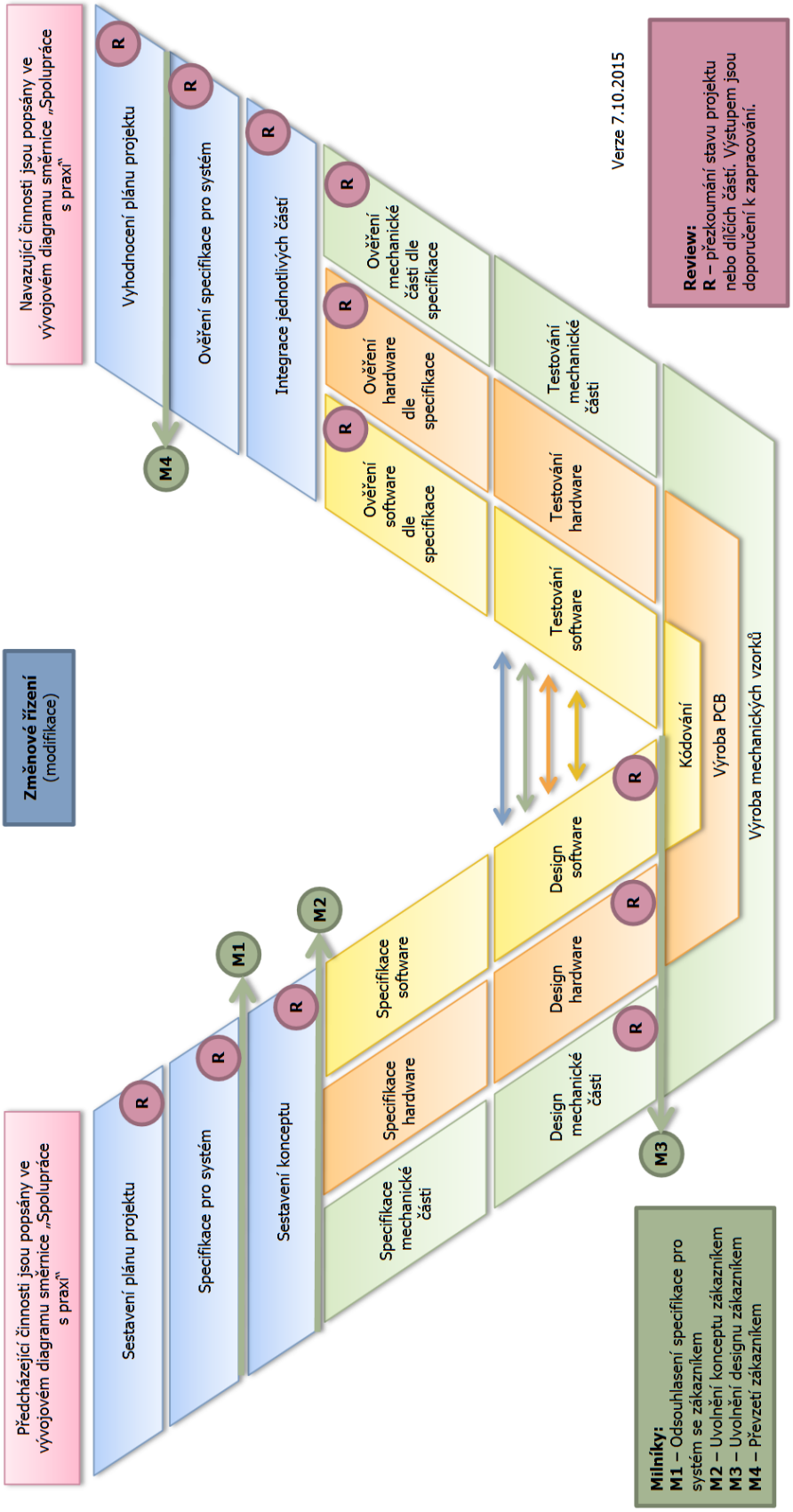
Jak bude v další kapitole detailněji popsáno, řídicí systém REMCS byl navrhován jako univerzální řídicí systém aplikovatelný do různých cílových aplikací. Bylo by proto výhodné projekt směřovat jako generický (obecný) systém, který by mohl být použit v řadě konkrétních aplikací bez nutnosti zásahu do základních funkcí při zachování stejného jádra. Ovšem prokázání splnění požadavků generického systému je mnohonásobně složitější oproti konkrétní aplikaci a ani v praxi se s podobným přístupem příliš nesetkáme. Obvykle je volen přístup, kdy je řešena konkrétní aplikace.

Proto bylo pro potřeby předkládané studie definováno cílové použití včetně jasně dané struktury, konfigurace jednotlivých karet a modulů celého systému REMCS.

Předkládaná aplikace by se neměla odlišovat od cílového použití, pro které byl systém vytvořen. Měla by co nejlépe vystihovat přednosti a výhody, které byly cíleně do systému integrovány již při jeho vývoji a návrhu. Jak bylo zmíněno v úvodu, prioritně byl tento systém vyvinut pro řízení výkonových měničů různých pohonů, a proto vytvořená aplikace zcela jasně směřuje do oblasti řízení výkonové elektroniky.

4.1 Vývojový proces na Západočeské univerzitě

Z hlediska návrhu systémů souvisejících s bezpečností je nutné postupovat podle životního cyklu příslušných norem a to od samotného začátku jejich vývoje. Vývoj bezpečných systémů se zásadně neliší od vývoje jiných složitých systémů, a proto se mohou použít podobné nástroje vedení projektu. Je ale nutné počítat s větším počtem opakovacích prací (například z důvodu špatného návrhu dílčí části), důkladnější dokumentací nebo velkým množstvím času věnovaného revizím a zpracování rozborů bezpečnosti. V průběhu vývoje se musí postupovat podle definovaného životního cyklu, který v klíčových místech vývoje stanovuje provádění revizí. V každé důležité fázi životního cyklu je přezkušována shoda návrhu se zadáním. Obrázek 46 ukazuje proces vývoje výrobku, který je v rámci RICE popsán a implementován. Jde pouze o přehledové schéma, kompletní směrnice implementující celý proces, včetně nezbytných šablon, popisu vstupů a výstupů jednotlivých procesních kroků včetně revizí atd., je součástí interních směrnic RICE FEL ZČU od roku 2016. Každá fáze vývoje, změna nebo úprava musí být řádně dokumentována a ověřena. Hlavním smyslem těchto prací je minimalizovat lidské chyby a tím redukovat riziko systematických chyb.



Obrázek 46: Proces vývoje výrobku v rámci ZČU RICE. [54]

Snahou je implementovat všechny kroky procesu, které umožní vývojovým centrům Západočeské univerzity vyvíjet ve spolupráci s průmyslovými partnery náročnější zařízení.

Porovnáním procesu vývoje výrobku v rámci ZČU RICE z obrázku 46 a ŽC dle normy ČSN EN 61508 (viz obrázek 8) lze nalézt drobné rozdíly. Oproti ŽC dle normy ČSN EN 61508 chybí poslední fáze životního cyklu - Celkový provoz, údržba a opravy, Celková modifikace a modernizace, Vyřazení z provozu nebo likvidace. Tyto fáze životního cyklu nejsou řízeny projektovým řízením RICE a musí být zajišťovány zákazníkem / spotřebitelem. RICE je však schopno zajistit podporu v těchto částech.

Na následujícím praktickém příkladu je demonstrována implementace příslušných norem a poznatků z oblasti návrhu bezpečných systémů pro reálný systém nasazený pro konkrétní aplikaci.

4.2 Koncepce a definice systému

Předmětem analýzy je systém REMCS, který je použitý jako řídicí systém v Zařízení pro kompenzaci zemních poruch[2] na vedení vysokého napětí.

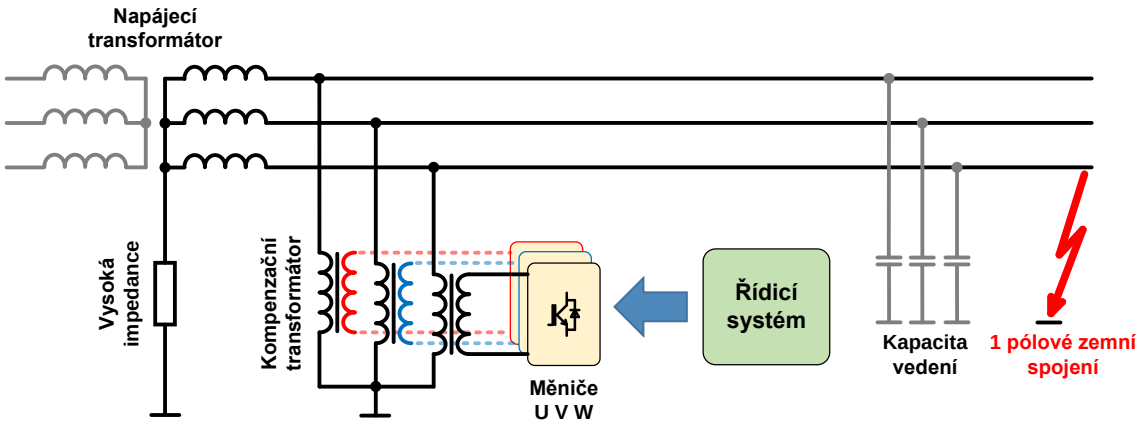
V rámci pilotního projektu pro společnost ČEZ probíhá posledních několik let stavba prototypu tohoto Zařízení, které bude reálně nasazeno do zkušebního provozu v rozvodně Kralovice již na podzim tohoto roku (9/2019). Jedná se o velký projekt, v němž je zapojena jak řada průmyslových firem, tak i velká skupina výzkumníků z fakulty elektrotechnické Západočeské univerzity. Do této skupiny jsem byl přizván na pomoc při zpracování částí návrhů a především analýz úzce souvisejících s bezpečností.

Navržené Zařízení je založeno na řízeném zdroji proudu (výkonový měnič), který přes kompenzační transformátor injektáží proudu do soustavy kompenzuje

[2] V případě poruchy u sítí neúčinně uzemněných či izolovaných, kdy dojde k vodivému spojení jedné fáze se zemí, poruchový proud nedosahuje tak vysoké úrovně a není tedy bezpodmínečně nutné okamžité vypnutí postiženého vývodu.

poruchové proudy a tím nahrazuje zhášecí tlumivku zapojenou mezi uzel transformátoru a zemnící soustavu rozvodny.

Běžně jsou během provozu tyto tlumivky laděny automatikou, která nastavuje zhášecí tlumivku do paralelní rezonance s celkovou kapacitou provozované sítě tak, aby místem poruchy procházel pouze malý zbytkový reziduální proud. Proto se někdy těmto tlumivkám říká rezonanční případně Petersenovy, dle jejich vynálezce. Nevýhodou zmíněných tlumivek je neschopnost eliminovat harmonické vyšších řádů poruchových proudů. V případě zemního spojení sice dochází k potlačení první harmonické zemního poruchového proudu, nicméně místem zemního spojení protékají obvykle i nezanedbatelné harmonické vyšších řádů zemního poruchového proudu. Zařízení pro kompenzaci zemních poruch odstraňuje výše uvedené nedostatky. Jedná se o řešení, ke kterému ZČU vlastní mezinárodní patenty č. EP2599179B1 (*The apparatus compensating ground currents connected to a transformer neutral point*) a EP2599180B1 (*The apparatus compensating ground currents connected to phase conductors of a distribution system*). Podrobnější vysvětlení principu kompenzace zemních poruch použitím výkonového měniče lze nalézt v [47].



Obrázek 47: 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. Základní parametry transformátoru uvádí tabulka 31. Níže uvedený popis jednotlivých částí Zařízení vychází z [48].

Tabulka 31: Základní parametry kompenzačního transformátoru.

Primární vinutí	
Zapojení	Y, střed uzemněn
Fázové napětí	12,7 kV (22 kV - v případě jednofázového zemního spojení)
Fázový proud	33,3 A
Proud uzemněním	100 A
Sekundární vinutí	
Zapojení	3x oddělené vinutí
Napětí	230 V (400 V - v případě jednofázového zemního spojení)
Proud	1200 A
Převod	55

Navržený transformátor představuje plnohodnotný ekvivalent tradiční zhášecí tlumivky a zajišťuje neúčinné uzemnění a ochranu distribuční sítě. V případě zemního spojení odebírá ze sítě netočivou složku proudu, která tvoří významnou část celkového generovaného kompenzačního proudu. Ten je prostřednictvím uzemněného uzlu primárního vinutí transformátoru sveden do bodu zemního potenciálu.

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. Základním stavebním blokem měniče je jednofázový napěťový střídač v můstkovém zapojení o výkonu 150 kVA umožňující paralelní řazení a výkonové dimenzování celého měniče (viz obrázek 48).

Obrázek 48: Základní výkonové bloky 150 kVA.

Každé ze tří oddělených sekundárních vinutí transformátoru je napájeno třemi paralelně spojenými výkonovými bloky proudově dimenzovanými na 375 A, celkem tedy 3x 1125 A na sekundární straně transformátoru. Na primární straně je tak měnič schopen generovat 3x 20 A (netočivé či točivé složky), tedy celkový kompenzační proud 60 A.

Klíčovou komponentou aktivní části Zařízení je řídicí systém REMCS zajišťující vedle samotného řízení také bezpečnostní ochrany, komunikaci, monitoring a sběr dat. Pro tuto aplikaci byl řídicí systém navržen v konfiguraci několika řídících karet, 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.

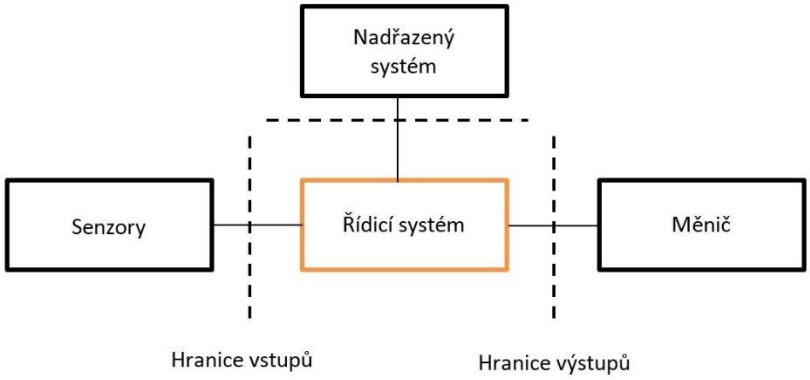
Skříň Zařízení je dále vyzbrojena soustavou stykačů, mechanických odpojovačů, pojistek a jističů pro zajištění bezpečného připojení a bezpečného provozu. Záložní zdroj napájení umožní uvedení systému do bezpečného stavu a uložení nezbytných dat v případě výpadku napájení.

4.2.1 Vymezení systému

Pro každou analýzu systému je nutné stanovit, co do analyzovaného systému patří a co je již mimo hranice analyzovaného systému. Rozsah prokazování bezpečnosti se v této aplikaci vztahuje pouze na řídicí systém REMCS. Aby bylo možné hodnotit pouze řídicí systém REMCS, je nutné stanovit hraniční podmínky,

které přesně definují všechny signály mezi řídicím systémem a ostatními prvky Zařízení. Řídicí systém REMCS bude měřit veškeré signály potřebné pro řízení a řídit hlavní i pomocné měniče celého Zařízení pro kompenzaci zemních poruchových proudů.

Hranice systému je na jedné straně definována připojením měřících čidel a pomocných kontaktů a na straně druhé připojením řídicích signálů k výkonovým měničům a pomocným stykačům celého Zařízení.



Obrázek 49: Hranice systému

Veškerá elektrická připojení uvedená výše (čidla, pomocné kontakty, budiče výkonových měničů, stykače) jsou realizována v rámci jednoho uzavřeného rozvaděče. Jak bude dále popsáno v kapitole 4.5.4, převážná většina vstupních i výstupních signálů je galvanicky oddělena a důležité signály jsou zdvojené.

Tento krok (definice hraničních podmínek) nelze chápat jako vyškrtnutí prvků za hranicemi a tím se nezajímat o jejich vlastnosti, ale umožňuje cíleně se zabývat návrhem dané části za pomoci definic chování okolí.

4.2.2 Podmínky provozu

Systém musí splňovat podmínky daného provozu. Veškeré elektrické a elektronické části celého Zařízení (mimo vybraných čidel a měničového transformátoru) budou umístěny v jedné rozvaděčové skříni. Rozvaděč musí odolávat venkovním povětrnostním vlivům, bude proto rozdělen do dvou oddělených sekcí: uzavřená a otevřená. Otevřenou částí se rozumí průduchy pro

chlazení výkonových prvků, uzavřenou se rozumí prostor, ve kterém jsou umístěny výkonové měniče, pomocné stykače, řídicí systém a další pomocná elektronika. Pod pojmem uzavřená sekce si lze představit uzavřenou část rozvaděče, ve které bude chlazení zajištěno klimatizační jednotkou. Otevřenou část tvoří vzduchové průduchy, v nichž budou umístěny chladiče výkonových prvků měničů.

Zařízení bude v nepřetržitém provozu s plánem pravidelných kontrol a testů. Dvakrát do roka bude Zařízení odstaveno a bude provedena periodická zkouška. Zařízení je k rozvodné soustavě připojeno přes samostatný stykač, který je v průběhu testů rozpojen a zajištěn proti sepnutí. V rámci zkoušky bude provedena kontrola funkce jednotlivých částí systému, kontrola jejich propojení (kabeláže) a další vizuální i testovací úkony. Proudová a napěťová čidla budou v rámci testů ověřena pomocí externích kalibračních zdrojů a měřících přístrojů. Na kompenzačním transformátoru a přívodních vodičích bude provedena zkouška izolačního stavu a důkladná vizuální prohlídka. Veškeré spínací relé a stykače musí splnit požadavky na bezpečné sepnutí/rozepnutí. Tyto a další zkoušky je nutné provádět důsledně, jelikož po jejich provedení je technicky zařízení považováno za nové. Proto je nutné, aby zkouška byla komplexní a prováděna podle kvalifikovaného plánu.

Odstranění detekované nebezpečné poruchy je možné zahájit okamžitě, hned po jejím odhalení, jelikož se nejedná o důležitou část nutnou k distribuci elektrické energie. Doba potřebná k odstranění poruchy je odhadována na 8 hodin. V této době je zahrnuta mobilizace personálu, nalezení závady a provedení opravy.

Pravidelné kontroly a odstraňování případných poruch nejsou v kompetenci RICE ZČU, ale provozovatele, čímž RICE ZČU neručí za jejich přesné nastavení a dodržování. Zde uvedené plány kontrol a oprav byly stanoveny na základě zkušeností provozovatele a doporučení RICE ZČU.

Obecné podmínky provozu celého Zařízení i řídicího systému REMCS jsou uvedeny ve specifikačních listech. Za nejdůležitější podmínky, které mohou ovlivnit funkci při překročení specifikovaných mezí, se považují přepětí sítě a překročení dovolených teplot.

4.3 Analýza nebezpečí a rizik

Koncepční návrh je nutné ověřit z pohledu možných rizik. Většina analýz byla provedena skupinově a to z důvodu podchycení nejlépe všech potenciálních rizik hned na samém začátku návrhu. Samotný výběr metod, řízení a průběh všech analýz byl koordinován na základě mých doporučení a poznatků.

4.3.1 Identifikovaná rizika

Cílem identifikace rizik je určit nebezpečí a nebezpečné události za všech rozumně předvídatelných okolností (včetně chybných podmínek nebo nesprávného použití) zahrnující všechny významné problémy vyplývající z lidského faktoru. Zvláštní pozornost je věnována abnormálním nebo málo se vyskytujícím režimům provozu řídicího systému. Výčet těchto rizik, jejich pravděpodobnou příčinu i důsledek uvádí tabulka 32.

Tabulka 32: 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

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

10	Neprůchodnost chladících otvorů	Přehřátí výkonových prvků	Poškození měniče
11	Přepětí ze strany sítě	Přepětí na transformátoru	Poškození izolace transformátoru, poškození měniče
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
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

(Pokračování tabulky na další straně)

(Pokračování tabulky z předchozí strany)

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

Všechna uvedená rizika musí být ohodnocena a zajištěna tak, aby byla zachována bezpečnost Zařízení.

4.3.2 Zařazení rizik

Pro ohodnocení jednotlivých rizik spojených s provozem Zařízení pro kompenzaci zemních poruch je využito metody ALARP. Přesná specifikace parametrů *následek* a *četnost* byla určena s ohledem k aplikaci. Konkrétní hodnoty uvádí tabulky 33 a 34. Rozdělení do matice rizik pro identifikovaná rizika pro hodnoty četností a následků jsou uvedeny v tabulce 35.

Tabulka 33: Specifikace pro zařazení rizik z hlediska následku

Následek	Specifikace
Katastrofální	Smrt, těžké ublížení na zdraví s trvalými následky, velké materiální škody
Kritický	Ublížení na zdraví, středně velké materiální škody
Nepodstatný	Úraz bez trvalých následků a malou pracovní neschopností, malé až zanedbatelné materiální škody
Zanedbatelný	Velmi lehký úraz (pohmožděniny, odřeniny), malé až zanedbatelné materiální škody

Tabulka 34: Specifikace pro zařazení rizik z hlediska četnosti

Četnost	Perioda opakování rizika
Častá	< den
Pravděpodobná	< týden
Příležitostná	< měsíc
Málo častá	< 1 rok
Nepravděpodobná	< 10 let
Neuvěřitelná	> 10 let

Tabulka 35: Matice rizik pro Zařízení kompenzace zemních poruch.

Četnost	Následek			
	Katastrofální	Kritický	Nepodstatný	Zanedbatelný
Častá				
Pravděpodobná		**10**		
Příležitostná	**6**	**4, 5**	**1, 2**	
Málo častá		**3, 11, 17**	**20**	**18, 19**
Nepravděpodobná	**7, 8, 22, 23, 26**	**9, 14, 15,16, 21**		
Neuvěřitelná	**24**	**12, 13**	**25**	

Rozdělení rizika do kategorií na nepřijatelné, ALARP a přijatelné riziko uvádí následující tabulka.

Tabulka 36: Rozdělení rizik do kategorií

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 36 je vidět, že rizika č. 6 a 10 se vyskytují v oblasti nepřijatelného rizika a musí být tedy bezpodmínečně ošetřena. Pro rizika z oblasti ALARP je nutné navrhnout bezpečnostní opatření snižující jejich četnost nebo následek.

Práce s těmito riziky je spojena s rozhodováním, zda je snižování rizika proveditelné a jsou-li investice přijatelné vzhledem k získanému zlepšení. Pro rizika z poslední oblasti již není nutné prokazovat ALARP, ale je nutné věnovat pozornost tomu, aby se na úrovni přijatelného rizika udržely.

4.3.3 Snížení rizik

V této fázi analýzy rizik by měly být navrženy metody a způsoby pro snížení nepřijatelných rizik a rizik z oblasti ALARP. Jakým konkrétním technickým řešením nebo opatřením budou konkrétní rizika snížena, je závislé na zkušenostech a možnostech dané organizace, v konečném důsledku technika, který implementaci opatření bude provádět. Nicméně je nutné v tomto kroku pro rizika navrhnout opatření a provést opětovné hodnocení, zda rizika byla snížena na přijatelnou úroveň. Pro tuto aplikaci bylo navrženo 9 základních opatření viz tabulka 37.

Tabulka 37: 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

I přes to, že opatření mají zásadní vliv na snížení hodnot četnosti a/nebo následků u jednotlivých událostí, jsou obecně nezávazná, jelikož lze mnoha

událostem předcházet více způsoby s různými finančními požadavky. Proto v této úrovni není struktura jednotlivých opatření striktně definována a jejich konečná forma se ukáže až ve fázi návrhu a realizace. Nicméně by se neměla od návrhů významně odlišovat.

Nyní je nutné ověřit, zda Zařízení bylo s navrženými opatřeními dostatečně zabezpečeno a rizika byla snížena na přijatelnou úroveň. Opatření uvedená v tabulce 37 snižují pro některá rizika jejich následek, četnost nebo kombinaci obou a to v různých úrovních. Pro nové hodnocení rizik (s použitím navržených opatření) je opět využito parametrů *následek* a *četnost* s hodnotami uvedenými v tabulkách 33 a 34. Při uvažování navržených opatření se změní matice rizik na tvar uvedený v tabulce 38.

Tabulka 38: Nová matice rizik pro Zařízení kompenzace zemních poruch.

Četnost	Následek			
	Katastrofální	Kritický	Nepodstatný	Zanedbatelný
Častá				
Pravděpodobná				
Příležitostná				1, 2
Málo častá				18, 19
Nepravděpodobná	26	3, 4, 15, 22, 23	11	17, 20, 21
Neuvěřitelná	6, 7, 8, 24	5, 9, 10, 12	13, 14, 25	16

Z tabulky je vidět, že použitím uvedených bezpečnostních opatření se všechny rizikové události přesunuly do oblasti přijatelného rizika, případně do oblasti, kde je vyžadován princip ALARP. Všechna rizika, která zůstala v oblasti ALARP, nebo se do ní přesunula z oblasti nepřijatelného rizika, se nacházejí ve III. třídě (na rozhraní oblasti ALARP a oblasti přijatelného rizika) a z hlediska poměru vynaložených investic k dalšímu snížení rizika jsou již přijatelná. Důležitým aspektem je absence rizikových událostí v oblasti nepřijatelného rizika.

Výčet rizik, určených k ošetření uvádí tabulka 39.

Tabulka 39: Rizika určená k ošetření bezpečnostním systémem

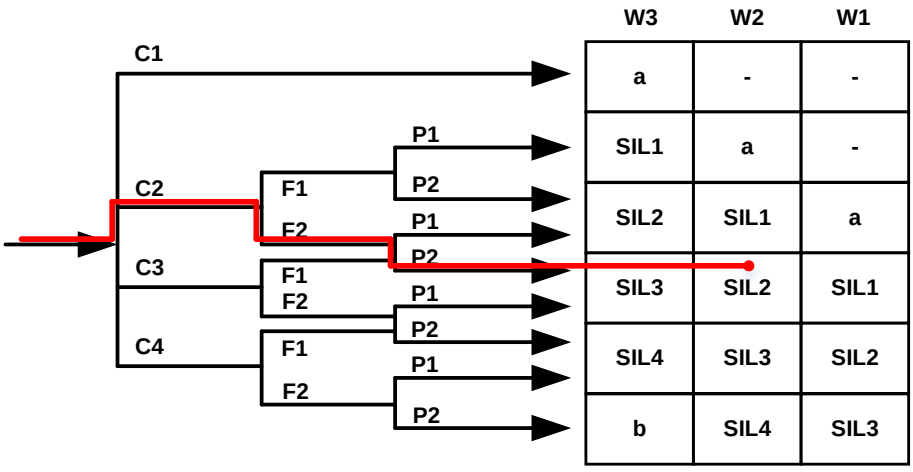
č.	Riziko
1	Přepětí transformátoru / výkonových prvků
2	Nadproud transformátoru / výkonových prvků
3	Neočekávané vypnutí celého systému
4	Zahřátí výkonových prvků
5	Zahřátí transformátoru
6	Kontakt s živými částmi Zařízení
7	Zkrat řídicích, kontrolních nebo měřících signálů
8	Rozpojení řídicích, kontrolních nebo měřících signálů
9	Přehřátí výkonových prvků
10	Přehřátí výkonových prvků
11	Přepětí na transformátoru
13	Nesprávné napětí jedné fáze
14	Poškození měniče jedné fáze
16	Nesprávné řízení fázového měniče
17	Nesprávné řízení fázového měniče
20	Neřiditelné celé zařízení
21	Přehřátí výkonových prvků
22	Špatná regulace, nekontrolovaná velikost proudu
23	Špatná regulace, nekontrolovaná velikost napětí

Přestože by se mohlo zdát, že se některá rizika určená k ošetření shodují, vznikají z různých příčin a jsou ošetřována jinými opatřeními. Například riziko přepětí na transformátoru (rizika č. 1 a 11) může vzniknout chybou programu, nebo přepětím ze strany sítě. V obou případech je důsledek rizika stejný, ale jejich ošetření je rozdílné z důvodu jiných příčin jejich vzniku. Proto jsou ve výčtu rizik v tabulce 39 uvedeny samostatně.

V následujícím kroku je stanovena požadovaná úroveň integrity bezpečnosti pro bezpečnostní funkce určující minimální požadavky na ošetření uvedených rizik. 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. Pro příklad je uvedeno určení požadované úrovně integrity pro riziko č. 6 - *Kontakt s živými částmi Zařízení*. Uvedenému riziku byly stanoveny tyto hodnoty parametrů:

- Následek C_2 – *Zranění jedné nebo více osob s trvalými následky, smrt jedné osoby*
- Četnost a doba vystavení v nebezpečné oblasti F_2 – *Časté až trvalé vystavení v nebezpečné oblasti*
- Možnost se nebezpečné události vyhnout P_2 – *Téměř nemožné*
- Pravděpodobnost nežádoucího výskytu W_2 – *Malá pravděpodobnost*

Odpovídající úroveň integrity bezpečnosti je následně určena vložením parametrů do grafu rizik. V případě rizika č. 6 je výsledkem požadavek na splnění úrovně zabezpečení SIL2.



Obrázek 50: Diagram rizika pro riziko č. 6.

Obdobným způsobem byla hodnocena všechna rizika z tabulky 39 a určena jejich požadovaná úroveň zabezpečení. Výsledky provedené analýzy jsou uvedeny v tabulce 40.

Tabulka 40: 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
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 40 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.

V tabulce se v ostatních případech vyskytují rizika, pro která není kladen požadavek na zabezpečení pomocí systému s definovanou úrovní integrity bezpečnosti. Jedná se o rizika, která budou zajištěna jinými opatřeními, a nebude pro ně platit prokazování splnění požadavků bezpečnosti dle normy ČSN EN 61508. Přesto je použití jiných opatření nutno zdokumentovat za účelem prokázání snížení rizika, jak bylo definováno v tabulce 38. Pro snížení rizika lze využít opatření uvedená v tabulce 37.

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. Samotná konstrukce uzavřeného rozvaděče Zařízení navíc zamezuje dotyku nebezpečných částí a tím i úrazu elektrickým proudem. K většině rizik dochází uvnitř rozvaděče, a pokud nedojde k otevření některých dveří, je obsluha chráněna. S tím souvisí požadavek na důkladné zabezpečení proti neúmyslnému otevření.

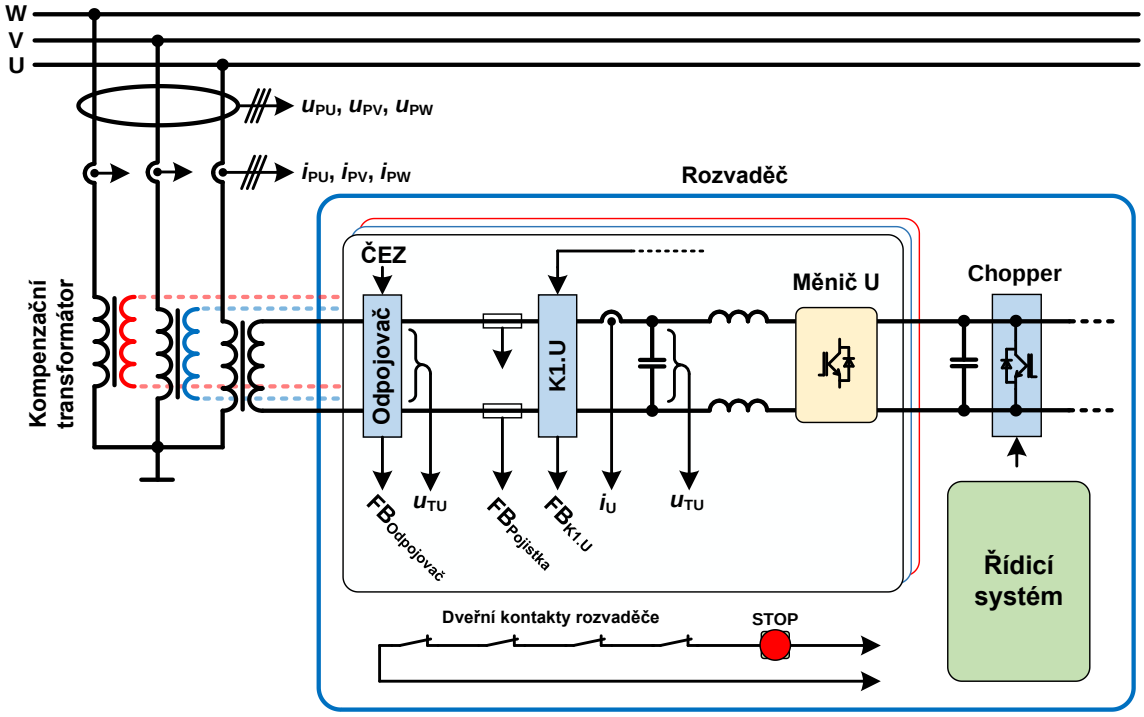
4.4 Specifikace požadavků

Aby bylo možné navrhnout bezpečnostní funkci tak, aby zajistila snížení nebo odstranění rizika, je nutné důkladně popsat její funkci a podmínky chování v konkrétním zařízení. Proto budou v této kapitole specifikovány základní části Zařízení související se zajištěním bezpečnosti. Přestože systém v sobě integruje řadu podružných a doplňujících funkcí, v této práci nebudou specifikovány, jelikož s bezpečností nesouvisejí a nemají na ně vliv.

4.4.1 Základní popis částí

Koncepční rozmístění základních částí celého Zařízení již bylo uvedeno na obrázku 47. Obrázek 51 rozkresluje uspořádání klíčových částí Zařízení z pohledu implementace bezpečnostních funkcí.

Zde je možné vidět řadu komponent vloženou mezi kompenzační transformátor a jednotlivé fázové měniče. Na obrázku 51 je rozkreslena pouze fáze U. Také je na obrázku již zakreslena tzv. zelená linka propojená přes všechny dveřní kontakty rozvaděče. Detailnější popis zelené linky bude uveden v kapitole 4.5.3 popisující strukturu řídicího systému.



Obrázek 51: 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 51). 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.

4.4.2 Životní cyklus

Určení norem, podle kterých má být systém vytvořen, obecně zadává zákazník včetně celé specifikace, která určuje veškeré funkční i technické požadavky pro specifické úkoly systému a identifikuje veškerá technická opatření a omezení. Díky tomu je možné vyvinout obecné zařízení, které dosáhne nejvyšší možné shody

s příslušnými normami. Přestože v tomto projektu nebyla žádná norma z hlediska funkční bezpečnosti zákazníkem stanovena, bylo snahou postupovat podle požadavků na bezpečný systém. Jelikož v této oblasti neexistuje specifická norma, celková specifikace požadavků na bezpečnost, návrh a vývoj by měly probíhat dle požadavků obecné normy ČSN EN 61508. Proto i životní cyklus systému odpovídá životnímu cyklu dle ČSN EN 61508 viz obrázek 8.

4.4.3 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.

Charakteristika bezpečnostní funkce zahrnuje tři hlavní akce: výstupy výkonových měničů jsou vypnuty, stykače K1 mezi měničem a kompenzačním transformátorem jsou rozpojeny a je sepnut vybíjecí obvod meziobvodu měničů (chopper).

Poškození hodnotných komponent jako jsou kompenzační transformátor, nebo výkonové měniče by znamenalo velké investice do jejich opravy, v nejhorším případě jejich celkové obměny. S odkazem na definovaná rizika spojená s poškozením těchto komponent je doporučené zahrnovat jejich ochranu v podobě integrovaných ochran a bezpečnostních funkcí, pro které však není vyžadován požadavek splnění funkční bezpečnosti. Mezi takové ochrany lze zahrnout:

- Nadproud dané fáze
- Nadproud dílčího výkonového bloku
- Přepětí na střídavé straně
- Kontrola správnosti měření čidel proudu
- Překročení povolené teploty

- Detekce odpadnutí stykače K1.x
- Detekce přehoření pojistky
- Detekce rozpojení odpojovače
- Detekce bezpečnostního signálu STOP

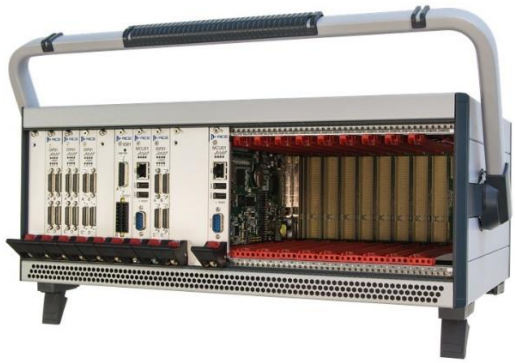
4.5 Návrh a realizace systému

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. Proto samotný návrh řídicí části Zařízení bude spočívat především v modulovém uspořádání a rozvržení jednotlivých stavebních bloků systému REMCS.

4.5.1 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 52: REMCS – 19“rack systém pro 19 karet [22]

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. Hodí se pro zákazníky, kteří mají vysoké nároky na rychlé nastavení konfigurace systému kvůli individuálním potřebám aplikací. Stejné řídicí jednotky lze tedy nasadit pro řízení měničů pomocných pohonů, nebo naopak do robustních měničových systémů určených pro hlavní pohon trakčních vozidel.

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). Standardem je několik úrovní watchdog časovačů jak čistě hardwarových, tak např. formou mikrowatchdogu v rámci FPGA. Každý z výstupů podléhá nezávislému zpětnému čtení. [16]

4.5.1.1 Části systému REMCS

Systém se skládá z jednotlivých modulů, které mohou pracovat samostatně v případě jednoduché aplikace, nebo je možné vytvořit konfiguraci několika karet vložených do 19“ racku (viz obrázek 52) pro řízení a monitorování rozsáhlých zařízení. Lze tak jednoduše zvýšit počet vstupů a výstupů, rozšířit systém o speciální rozhraní (typicky otáčková čidla absolutní polohy) nebo paralelizovat různá měření apod. Systém je průběžně inovován nejen na základě mých připomínek a výstupů z provedených analýz.

Zásuvné karty systému REMCS

- MCU – Mikroprocesorová karta – hlavní řídící jednotka
- DIF – Direct Interface – karta pro řízení měniče
- OIF – Open interface – karta otevřené platformy. Je osazena dvěma rozšiřujícími moduly
- PSU – Napájecí zdroj

Rozšiřující moduly pro OIF kartu

- AIM – Analog Input Module – modul analogových vstupů
- AOM – Analog Output module – modul analogových výstupů

- BIM – Binary Input Module – modul binárních vstupů
- BOM − Binary Output Module – modul binárních výstupů
- SIM – Sensor Interface Module – inkrementální čidlo otáček

4.5.1.2 Aktivní propojovací modul – Backplane (BPF)

Backplane tvoří propojovací aktivní modul systému REMCS pro vzájemné propojení až 19 zásuvných karet. Pro aplikace vyžadující větší počet karet v jednom systému je možné backplane vzájemně propojovat a systém tak jednoduše rozšířit. Naopak pro menší aplikace je v současné době vyvíjena kompaktnější verze s pěti pozicemi.

Backplane poskytuje všem kartám nezbytné napájení a především umožňuje jejich vzájemnou komunikaci pomocí vysokorychlostní sběrnice LVDS, několika sběrnic CAN a řady systémových a uživatelských signálů. Nejrychlejší komunikace LVDS (1,3 Gb/s) je určena pro vysokorychlostní přenos dat mezi kartami. Robustnost této komunikace zajišťuje topologie dvojitého kruhu procházejícího přes všechny pozice backplane. V případě přerušení komunikace v jednom směru je přenos dat zajištěn opačným směrem pomocí druhého kruhu.

Vlastnosti:

- 19 pozic pro zásuvné karty systému REMCS
- 1 pozice pro napájecí modul (včetně systémových signálů)
- Vysokorychlostní komunikace LVDS
- 1x systémový a 2x aplikační CAN
- 32 lokálních uživatelských signálů mezi každými dvěma sousedními pozicemi
- 16 globálních uživatelských signálů
- Systémové a synchronizační signály
- Napájení – 24V a 3,3V

4.5.1.3 Procesorová karta – Main Controler Unit (MCU)

Ve vícekartové konfiguraci systému REMCS obvykle představuje karta MCU hlavní jednotku neboli „master“. V této aplikaci je MCU karta v roli nadřazeného regulátoru požadovaného proudu a spojovacího členu mezi REMCS systémem a průmyslovým PC. Procesorová karta je vybavena procesorem s dvoujádrovou

architekturou určeným pro systémy vyžadující zvýšenou bezpečnost, zálohovanou pamětí pro diagnostické účely a bateriově zálohovanými hodinami reálného času.

Vnějším komunikačním rozhraním karty je jeden Ethernet port 10/100Mb (kterým je v této aplikaci připojeno průmyslové PC) a dva USB 2.0 host porty. Karta je v této aplikaci rozšířena pomocí přídavného komunikačního modulu o sběrnici CAN, která propojuje další moduly Zařízení. Obecně je možné kartu rozšířit o další komunikační moduly (FlexRay, USB, LIN, UART).

4.5.1.4 Karta analogových vstupů a digitálních výstupů − Direct interface (DIF)

Karta DIF je primárně určena jako regulátor měniče. Základ této karty má obdobnou strukturu jako výše zmíněná procesorová karta. Uživatelské rozhraní karty disponuje 8 analogovými vstupy, 10 PWM výstupy se zpětnými binárními vstupy, externím blokovacím vstupem pro hardwarové blokování PWM výstupů a výstupy pro napájení připojených periferií (+15V, -15V a +24V).

PWM výstupy s rozsahem 5V nebo 15V mohou budit přímo inteligentní výkonové prvky jako je například SKiiP (vždy binární pár vstup/výstup) proudem až 1A.

Analogové vstupy s nastavitelným kmitočtovým filtrem a šířkou pásma 96kHz umožňují měření symetrických i nesymetrických napětí s volbou čtyř rozsahů v obou případech. Každý kanál analogového vstupu má tři vlastní komparátory s vazbou na přímé blokování PWM výstupů. Díky dvěma externím AD převodníkům s rozlišením 16bit lze dosáhnout rychlosti převodu 3,5us. Analogové vstupy je možné použít pro připojení napěťových či proudových čidel.

V této aplikaci budou použity celkem 4 karty DIF. Tři karty DIF budou sloužit jako fázové regulátory a jedna karta DIF bude zajišťovat mastera pro komunikaci LVDS mezi všemi DIF a MCU. Také bude mít na starosti řídící algoritmy fázových měničů.

4.5.1.5 Karta pro dvojici rozšiřujících modulů – Open Interface (OIF)

Karta OIF slouží jako nosná základna pro dvojici rozšiřujících modulů uvedených v kapitole 4.5.1.6. Každému modulu poskytuje čtveřici izolovaných

napájecích zdrojů a dvacet galvanicky oddělených signálů. K dispozici jsou též neizolovaná napětí +-15V, 3,3V, sběrnice I2C včetně adresovacího signálu, signál blokování a až 23 uživatelských signálů. Ve výchozí verzi tato karta zajišťuje veškeré systémové služby pro osazené moduly (komunikace, identifikace atd.).

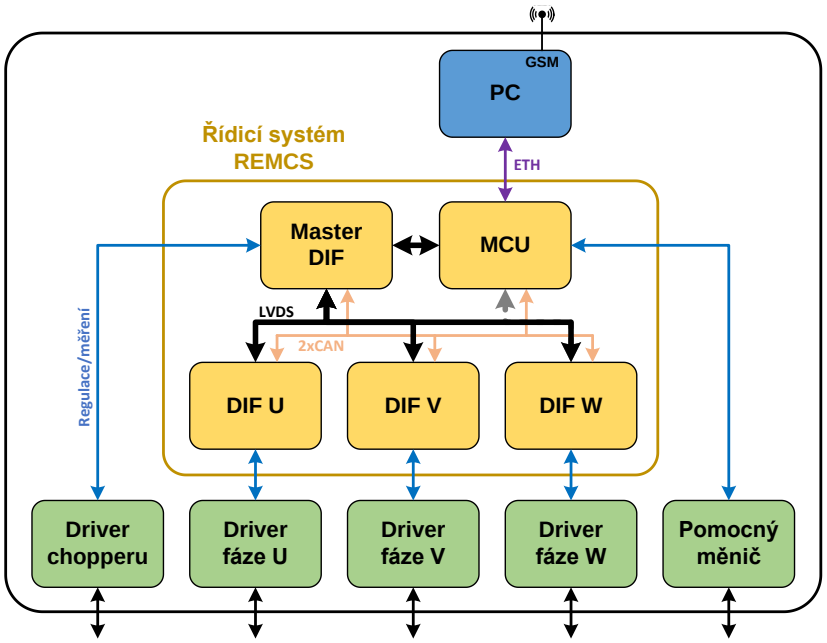
Na základě požadavků této aplikace vznikla upravená verze této karty. Oproti původní verzi byla významně upravena a především zjednodušena. Jednou z úprav bylo rozšíření vstupních a výstupních signálů karty DIF. Úpravou bylo dosaženo přímého propojení pomocí uživatelských signálů zavedených z karty DIF přímo na galvanické oddělovače umístěné na kartě OIF. Tím se z této karty stává pouze rozšiřující interface karty DIF.

4.5.1.6 Rozšiřující moduly pro OIF kartu

Moduly jsou navrženy jako rozšiřující desky pro univerzální řídicí kartu OIF. Různé varianty modulů (vstupní, výstupní, digitální, analogová) mají všechny vstupní resp. výstupní signály galvanicky oddělené jednak skupinově mezi sebou, jednak ke své základní desce (OIF). Jednoduchá konstrukce umožňuje rychlý návrh speciálních zákaznických modulů. Moduly představují možnost jednoduché konfigurace systému pro konkrétní potřeby aplikace volbou základních nebo speciálních zákaznických modulů.

4.5.2 Blokový diagram

Na základě specifikace požadavků byla navržena struktura a technické řešení jednotlivých modulárních karet systému REMCS. Strukturu řídicího systému určeného pro řízení Zařízení pro kompenzaci zemních poruch naznačuje obrázek 53. Na obrázku jsou zobrazeny vazby mezi řídicím systémem a ostatními bloky Zařízení.



Obrázek 53: Zjednodušené blokové schéma.

Základ řídicího systému je tvořen čtyřmi kartami DIF a jednou kartou MCU. Dále jsou v systému osazeny další karty OIF pro navýšení počtu vstupních a výstupních signálů karet DIF a MCU. Ve schématu na obrázku 53 nejsou karty OIF pro zjednodušení zakresleny. Všechny karty jsou v jednom racku zasunuty do aktivního propojovacího modulu Backplane zajišťujícího komunikaci mezi kartami a potřebné napájení. Funkce jednotlivých bloků jsou:

Regulátor Master DIF zajišťuje řídící algoritmy měničů, jejichž vstupní rozhraní tvoří požadovaná hodnota kompenzačního proudu ze strany regulátoru MCU a výstupní rozhraní tvoří modulační slova PWM na straně regulátorů DIF U, V, W. Master DIF tvoří mastera pro komunikaci LVDS mezi všemi DIF a MCU. Master DIF také zajišťuje měření veličin transformátoru na primární straně a regulaci chopperu – výkon brzdného odporu. Master DIF má přístup ke sběrnici CAN.

Regulátory DIF U, V, W zajišťují řízení příslušné fáze – trojice paralelně spojených výkonových bloků. Mají na starosti vlastní spínání a blokaci bloků, měření veličin v příslušné fázi, monitoring, zpracování chybových hlášení a obsluhu událostí. Regulátory komunikují s master DIF přes LVDS. Jsou přímo připojeny k DPS driverů výkonových bloků a mají přístup na sběrnici CAN.

Regulátor MCU zajišťuje generaci požadovaného proudu pro regulátor Mastera DIF. MCU má k dispozici měření vývodů a zhášecích tlumivek na rozvodně, data

z pomocného měniče přes RS485 a komunikuje s průmyslovým PC přes ethernet. Regulátor MCU má přístup na sběrnici CAN.

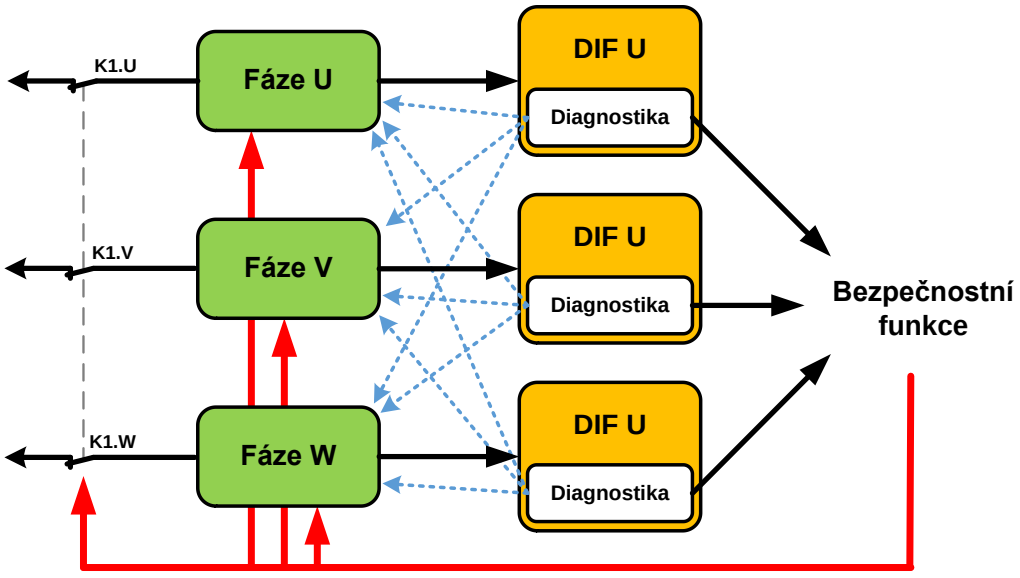
Průmyslové PC slouží ke sběru dat, jejich ukládání na disk a přenosu přes mobilní síť. Vedle funkce logování dat bude PC sloužit pro dálkové ovládání systému.

Desky driverů zajišťují vedle buzení výkonových prvků jednotlivých fází a chopperu měření veličin dané fáze či veličin primární strany transformátoru, měření teplot, monitorování chybových signálů a odeslání zpráv na sběrnici CAN.

Pomocný měnič je připojen k terciálnímu vinutí transformátoru. Jeho úkolem je měření a vyhodnocování dat z terciálního vinutí.

4.5.3 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.

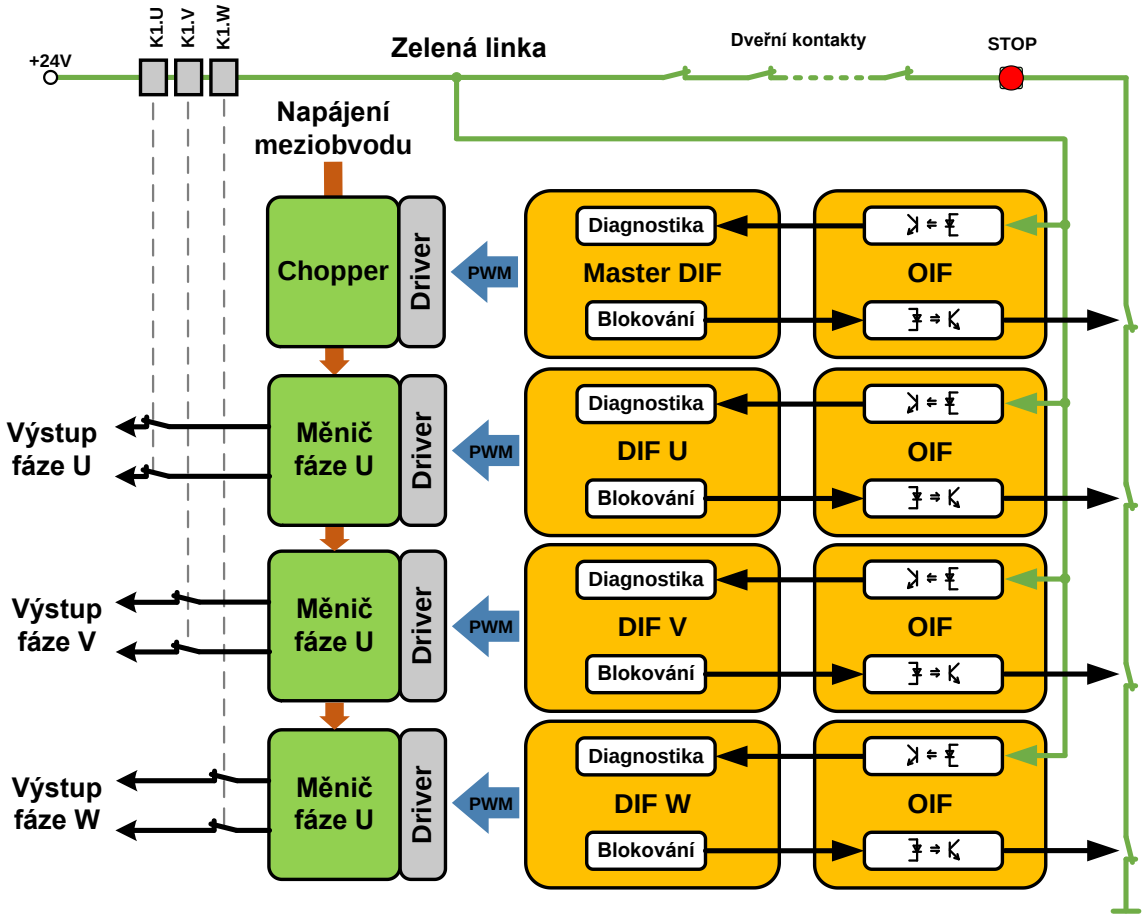


Obrázek 54: Architektura řídicího systému

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), každá fáze je nepřímo monitorována kartami zbývajících fází viz obrázek 54. Porucha jedné fáze tak může být detekována kteroukoli ze tří karet, z nichž každá může aktivovat bezpečnostní funkci.

Bezpečnostní funkce vypnutí celého Zařízení realizovaná zabezpečená rozpojením K1, blokováním PWM výstupních signálů a vybitím meziobvodu pomocí chopperu je vidět na obrázku 55.



Obrázek 55: 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 55 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 přes 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).

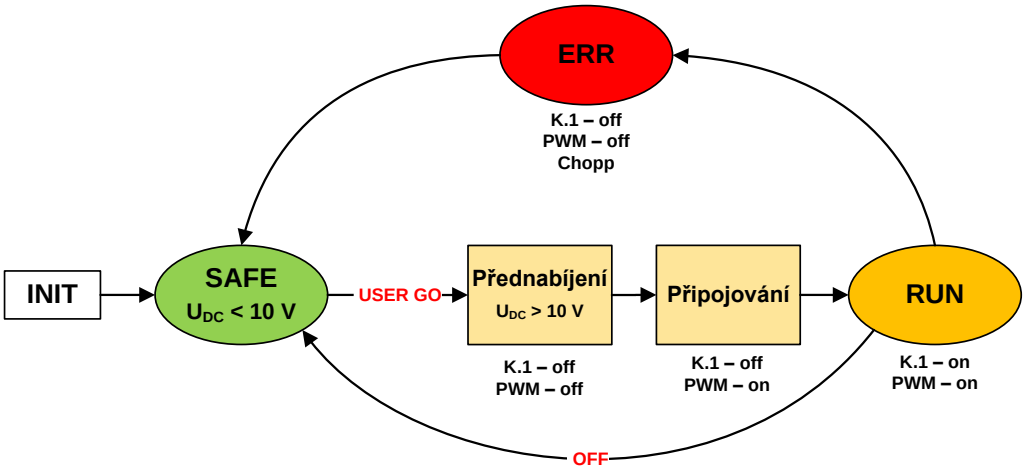
4.5.4 Rozhraní řídicího systému

Řídicí systém se bude chovat bezpečně za předpokladu, že jsou splněny tzv. exportované podmínky definované na rozhraní řídicího systému. Definice se týká všech vstupních i výstupních signálů včetně komunikačních sběrnic. Jsou definovány přesné úrovně, časování, sekvence a komunikační protokoly všech okolních prvků včetně detailního popisu jejich funkce. Veškeré tyto hodnoty vycházejí ze specifikačních listů [16]. Převážná většina vstupních i výstupních signálů řídicího systému REMCS je galvanicky oddělená a bezpečnostně důležité signály jsou zdvojené.

Napájení řídicího systému je zajištěno samostatným vedením 230V od provozovatele rozvodny. Provozovatel garantuje spolehlivý provoz tohoto napájení použitím záložních zdrojů v případě výpadku celé distribuční sítě. Bez ohledu na zálohování tohoto napájení ze strany provozovatele je toto napájení zálohováno náhradním zdrojem v rámci Zařízení. Tím je eliminováno riziko ztráty napájení v důsledku přerušení napájecí linky byť zálohované, ale vzdáleně.

4.5.5 Režimy

Velká komplexnost řídicího systému REMCS převyšuje požadavky bezpečnostních funkcí, proto řídicí systém realizuje i primární funkci Zařízení ve které monitoruje a kompenzuje distribuční síť. Primární funkce Zařízení je v pracovních režimech na obrázku 56 reprezentována režimem *RUN.* Detekce nebezpečné poruchy aktivuje bezpečnostní funkce reprezentované režimem *ERR*. Po odeznění poruchy může operátor povolit přechod do výchozího režimu *SAFE*, ve kterém je možné provádět kontrolu na „bezpečném“ Zařízení. V režimu SAFE jsou blokované výkonové součásti a meziobvod měničů je vybitý.



Obrázek 56: Režimy Zařízení

SAFE

Po inicializaci Zařízení přechází do *SAFE* režimu, ve kterém je možné provádět práci na Zařízení. V meziobvodu Zařízení je bezpečné napětí a nehrozí poranění vysoký napětím. Z tohoto stavu je možné příkazem *USER GO* přejít do režimu *RUN*.

RUN

Zařízení v režimu *RUN* vykonává primární funkci, pro kterou bylo navrženo, tedy kompenzaci poruchových proudů. Do tohoto stavu Zařízení přejde ze stavu *SAFE* po přijetí příkazu *USER GO* a definované sekvenci kroků zahrnující přednabíjení meziobvodu, kontrolu napětí, generaci PWM signálů a sepnutí stykače K1.

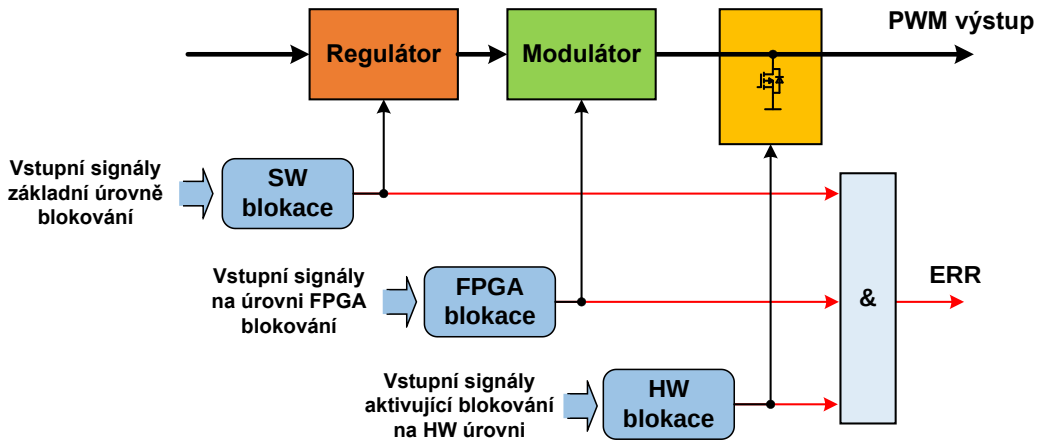
ERR

V tomto režimu je aktivována bezpečnostní funkce bezpečného vypnutí celého Zařízení, čímž přechází Zařízení do bezpečného stavu a není možné jej řídit. V tomto režimu Zařízení setrvává až do přímého nebo vzdáleného zásahu, při kterém jsou chyby vyčteny případně po jejich zhodnocení vymazány.

4.5.6 Cesty signálu související s bezpečností

S ohledem na použitelnost modulárního systému REMCS pro aplikace, ve kterých je kladen požadavek na bezpečnost, v sobě systém zahrnuje ochranné moduly zajišťující převedení výstupních signálů do bezpečného stavu v případě, že je detekována chyba. Struktura blokování výstupních PWM signálů souvisejících s bezpečností umožňuje aktivaci ochrany v jakýkoli okamžik nehledě na pracovní režim nebo stav systému.

Různé detekce chybových stavů jsou v řídicím systému řešeny ve třech základních úrovních, přičemž kterákoli z nich může iniciovat ochranu blokováním výstupních signálů a jejich převedením do bezpečného stavu. Na obrázku 57 je vidět koncepční struktura blokování výstupních signálů PWM.



Obrázek 57: Cesty signálů souvisejících s bezpečností

Toto schéma naznačuje pouze logickou funkci blokování. Signál ERR blokující PWM výstupy řídicího systému je v negativní logice a je propojen přes všechny karty, které jsou v systému použity. Kterákoli karta může vyvolat chybu aktivováním ERR signálu a tím zablokovat a převést do bezpečného stavu výstupní signály všech karet.

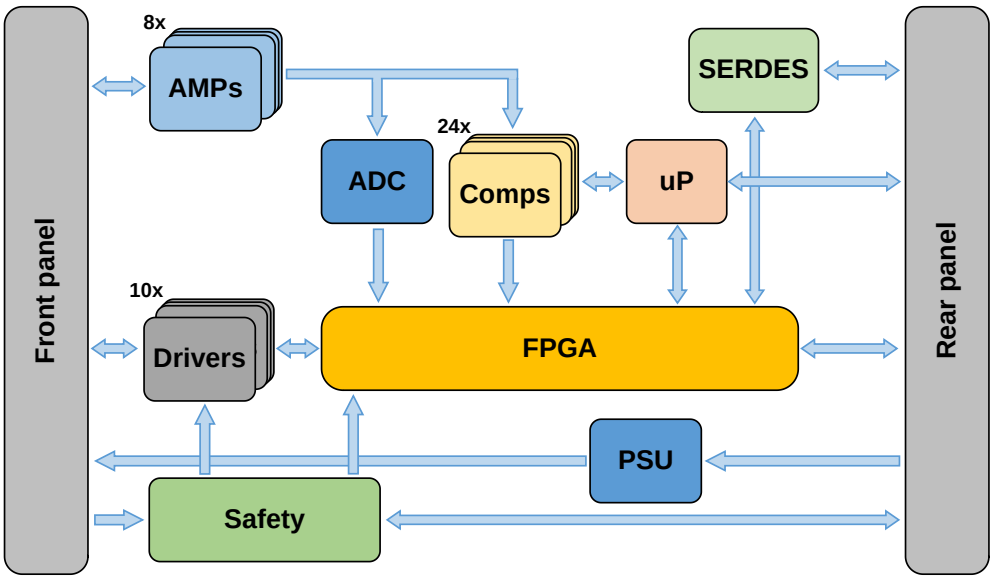
Blokování PWM výstupů je jeden z požadavků bezpečnostní funkce.

4.6 Potvrzení bezpečnosti

Následující analýzy byly provedeny za účelem potvrzení bezpečnosti s ohledem na požadavky bezpečnostních funkcí a požadavků na integritu bezpečnosti definovaných ve specifikaci požadavků.

4.6.1 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)

Velmi časově náročná část práce spočívala v provedených analýzách. Vzhledem ke komplexnosti samotného řídicího systému bylo provedeno několik dílčích analýz FMECA pro identifikaci způsobů kritických selhání a tvorbu odezvy na potenciální poruchy jednotlivých částí Zařízení. Analýza pokrývá celý řídicí systém, který sám o sobě je složen z 11 karet, přičemž každou kartu lze rozdělit na řadu vnitřních modulů. Například karta DIF byla nejen pro účely analýzy rozdělena na 18 modulů: ADC, Analog, CAN, DAC + Trimpot, ERR Comp, ETH, FPGA, IDN, OSC, Power, PWM Driver, Reset, Safety Block, Sequencer, Serdes, SPI, System signal a uP. Každý z těchto modulů má svou důležitou funkci a při analýze na ně bylo nahlíženo samostatně. Základní zjednodušenou strukturu karty DIF v podobě blokového schématu zobrazuje obrázek 58.



Obrázek 58: Zjednodušené blokové schéma karty DIF [23]

Vzhledem k rozsahu procesu analýzy je zobrazena pouze dílčí část analýzy jedné karty jak naznačuje Příloha A.

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 s ohledem na druh poruchy byl 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 upuštěno, jelikož řada poruch odhalených v provedených analýzách směřovala právě na omezený provoz. Na každou takovou poruchu by musel systém reagovat trochu odlišně, přestože konečným stavem by byl omezený provoz s odstavením porouchané části.

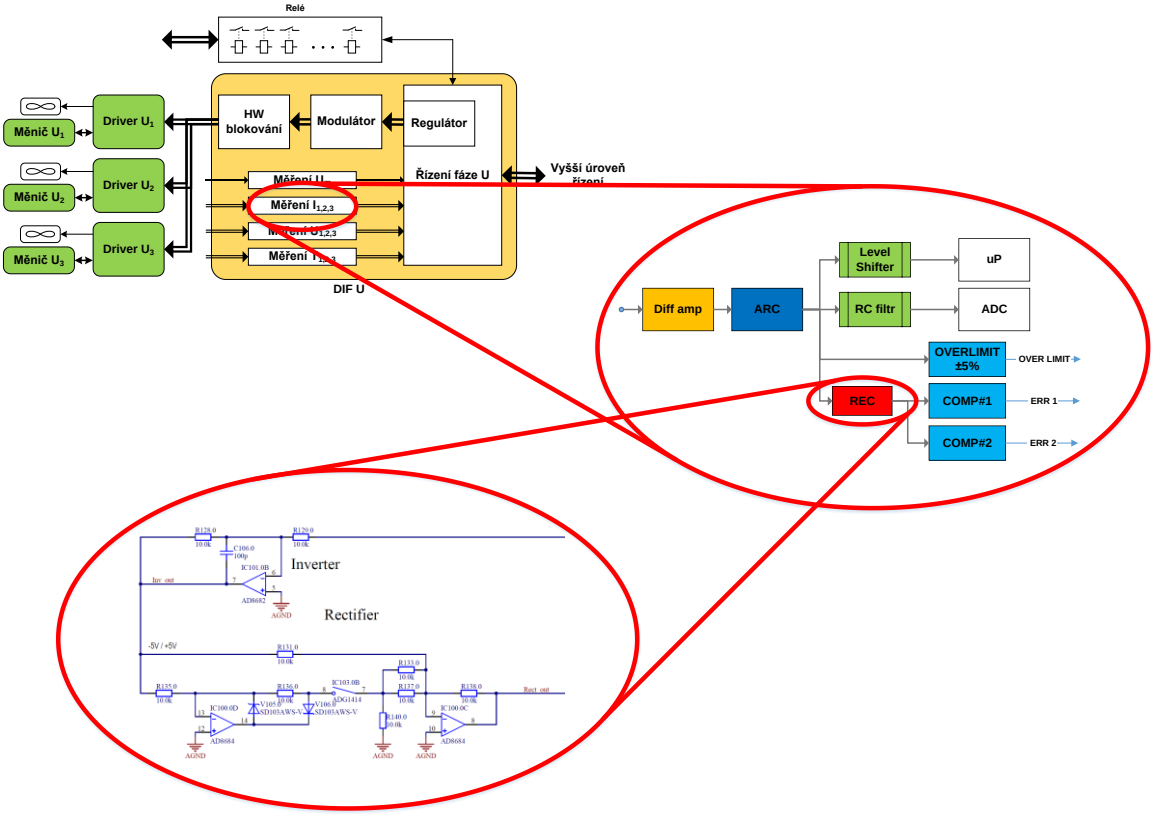
Dále bylo s odkazem na provedené analýzy navrženo doplňkové testování poruchových signálů. Uvažované poruchy na těchto signálech jsou při běžícím Zařízení nedetekovatelné a mohou vést na falešné poplachy, v horším případě na znemožnění aktivace chyby. Opatření spočívá v dodatečném testování před spuštěním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

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.

Řada dalších opatření navržených v souvislosti s analýzou spočívá v úpravě mezních hodnot v rámci vnitřních mezivýsledků nebo přímo měřených veličin.

4.6.2 Odhad náhodných poruch HW

Řídicí systém REMCS byl pro účely použití v bezpečných aplikacích analyzován také za účelem odhadu 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 59.



Obrázek 59: Rozdělení Řídicího systému podle funkčních bloků do několika úrovní (příkladová část)

Pro odhad intenzity náhodných hardwarových poruch na nejnižší úrovni elementárních bloků systému byla použita metoda počítání z prvků (*Parts Count*). Princip této metody spočívá v součtu intenzit poruch všech součástek systému.

$$\lambda_{sys} = \sum_{i=1}^{i=n} N_i \lambda_g \qquad (4.1)$$

kde

λ_{SYS} – je celková intenzita poruch systému

λ_g – je intenzita poruch i generického prvku i

N_i – je počet generických prvků i

n – je počet rozdílných generických kategorií prvků systému

V metodě Parts Count není řešena struktura zapojení a uvažuje se ten nejhorší případ (*Worst Case*), tedy že všechny součástky jsou řazeny sériově a jakákoli porucha může způsobit chybu. 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.

Rozsah této analýzy pro celý systém je opět velmi rozsáhlý. Příklad části provedené analýzy metodou Parts Count pro jeden z 18 modulů karty DIF je zobrazen v příloze (Příloha B).

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 (4.2). Strukturu tabulky provedené analýzy pro příklad karty DIF naznačuje Příloha C.

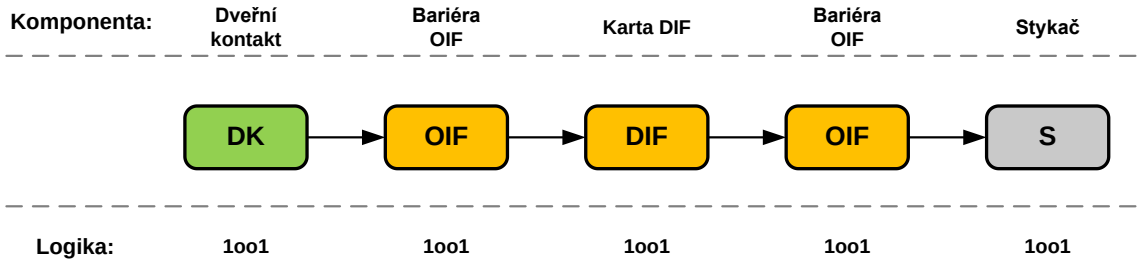
$$SFF = \frac{\lambda_S + \lambda_{Dd}}{\lambda_S + \lambda_{Dd} + \lambda_{Du}} \tag{4.2}$$

$$SFF_{DIF} = \frac{299 + 1457{,}7}{299 + 1457{,}7 + 172{,}6} = 91{,}1\% \tag{4.3}$$

$$SFF_{OIF} = \frac{59{,}5 + 446{,}5}{59{,}5 + 446{,}5 + 45{,}1} = 91{,}8\% \tag{4.4}$$

Ověření maximální úrovně integrity bezpečnosti je pro obě karty určeno pomocí tabulky 24 (komponenty typu 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 55. Výslednou podobu jednoho kanálu rozdělenou na pět subsystémů ukazuje obrázek 60.



Obrázek 60: 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:

$$PFH_i = 2 \cdot \lambda_{DU} \tag{4.5}$$

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:

$$B_{10d} = \frac{B_{10}}{RDF} \tag{4.6}$$

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

$$\lambda_d = 0{,}1 \cdot \frac{C}{B_{10d}} \tag{4.7}$$

kde λ_d je intenzita nebezpečných poruch pro trvalý provoz a C je počet provozních cyklů (počet sepnutí / rozepnutí) za hodinu. V případě, že zařízení není trvale v provozu, se u komponent konzervativně předpokládá, že i v době mimo provoz podléhají komponenty určité míře degradace a používá se přepočet hodnoty intenzity poruch na hodnotu ekvivalentní intenzity poruch podle vztahu:

$$\lambda_e = \frac{\lambda_d \cdot T_f + 0{,}1 \cdot \lambda_c \cdot T_{nf}}{T_f + T_{nf}} \tag{4.8}$$

kde

λ_e – je intenzita nebezpečných poruch pro přerušovaný provoz,

T_f – je doba fungování,

T_{nf} – je doba bez fungování (bez namáhání).

Výsledná pravděpodobnost selhání za hodinu PFH_i pro elektromechanické komponenty v zapojení 1oo1 je dána vztahem:

$$PFH_i = \lambda_d \cdot 1h \tag{4.9}$$

kde λ_d je intenzita nebezpečných poruch. Na místo λ_d lze použít ekvivalentní intenzitu poruch λ_e v případě, že komponenta není trvale v provozu a je použit vztah (4.8).

Dveřní kontakty PFH_{DK}

Rozvaděč má celkem 9 dveří, z nichž dvoje umožňují přístup k řídicímu systému a průmyslovému PC. Při otevření těchto dveří nehrozí úraz elektrickým proudem, a proto nejsou opatřeny dveřními kontakty. Zbývajících 7 dveří je osazeno dveřními kontakty FR 555.

Výkonové výstupy fázových vodičů je možné odpojit i manuálně pomocí vsunuté páky do rozpojovače. Vsunutí páky je detekováno kontaktem, který je zapojen do zelené linky. Spínače pro detekci vsunuté páky jsou shodné s dveřními kontakty, tedy FR 555.

Vlastnosti FR 555: Typ – Pizzato – FR 555

B_{10d} – 4 000 0000

C – $\frac{1}{4380}\ h^{-1}$

Bariéra OIF PFH_{OIF}

Jednotlivé signály řídicího systému jsou galvanicky odděleny pomocí karet OIF. Pro uvažovaný kanál na obrázku 60 je využito vždy dvou kanálů jedné karty OIF.

Vlastnosti OIF: λ_d – $4{,}92 \cdot 10^{-7}$

λ_{du} – $4{,}51 \cdot 10^{-8}$

Karta DIF PFH_{DIF}

Pro uvažovaný kanál na obrázku 60 je využito vždy jedné řídicí karty DIF.

Vlastnosti DIF: λ_d – $1{,}63 \cdot 10^{-6}$

λ_{du} – $1{,}73 \cdot 10^{-7}$

Stykač PFH_o

Rozpojení stykače K1 jedné fáze je možno rozpojením stykače K3 dané fáze nebo K6. Stykač K6 zelené linky je společný pro všechny fázové K1.

K1 je výkonný linkový stykač určený pro palubní a stacionární užití s pomocnými kontakty. Primárně jsou určeny pro použití na elektrických zařízeních v přítomnosti nejtěžších otřesů a vibrací, ke kterým dochází v trakčních vozidlech. Přestože není tento stykač certifikován přímo podle ČSN EN 61508, splňuje požadavky norem pro elektrická zařízení drážních vozidel IEC 60077, IEC 61992 a IEC 60947. Pomocné stříbrné samočistící kontakty zaručují dvojité přerušení, vysokou bezpečnost a elektrickou a mechanickou odolnost. Výrobce udává odolnost $2 \cdot 10^6$ cyklů. Níže uvedená hodnota B_{10d} byla odvozena z předpokladu, že udaná odolnost je dvojnásobná oproti hodnotě B_{10} a poměr RDF = 75 %.

Vlastnosti K1: Typ – Microelettrica Scientifica - LTHS12502SA02

U_{max} – 2000 V AC/DC

I_{th} – 1300 A / pól

B_{10d} ≈ $1{,}33 \cdot 10^6$

C – $\frac{1}{4380}\ h^{-1}$

Vlastnosti K3: Typ – Siemens - *3RH1122-2KB40*

B_{10} – 1 000 000

RDF – 75 %

	C	–	$\frac{1}{4380}\ h^{-1}$
Vlastnosti K6:	Typ	–	Schneider Electric - LP1K0610BD
	B_{10d}	–	1 369 863
	C	–	$\frac{1}{4380}\ h^{-1}$

Celkovou pravděpodobnost selhání za hodinu PFH pro každý kanál realizující bezpečnostní funkci lze určit podle vztahu (4.10).

$$PFH = PFH_{DK} + PFH_{OIF} + PFH_{DIF} + PFH_{OIF} + PFH_{O} \quad (4.10)$$

Částečné výsledky pro jednotlivé subsystémy a celkový výsledek intenzity poruch PFH jsou uvedeny v tabulce 41.

Tabulka 41: 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/h)	-	$45{,}1\cdot10^{-9}$	$172{,}6\cdot10^{-9}$	$45{,}1\cdot10^{-9}$	-
λ_{D} (1/h)	$1{,}67\cdot10^{-11}$	$491{,}6\cdot10^{-9}$	$1629\cdot10^{-9}$	$491{,}6\cdot10^{-9}$	K1: $1{,}71\cdot10^{-11}$ K3: $1{,}71\cdot10^{-11}$ K6: $1{,}66\cdot10^{-11}$
PFH_i	$16{,}7\cdot10^{-11}$	$9{,}01\cdot10^{-8}$	$3{,}45\cdot10^{-7}$	$9{,}01\cdot10^{-8}$	$8{,}52\cdot10^{-11}$
PFH	$5{,}25\cdot10^{-7}$				

Celková intenzita poruch PFH jednoho kanálu, který zajišťuje bezpečnostní funkci, je $5{,}25\cdot10^{-7}$. 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.

4.7 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 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] UHER, J. *Úvod do funkční bezpečnosti: norma ČSN EN 61508*. Automa, č. 8, s. 66-81. 2004.

[4] ČSN EN 50126 ed.2. *Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS)*. Český normalizační institut, 2018. Třídící znak 333502.

[5] ČSN EN 50129. *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy*. Brno: Český normalizační institut, 2004. Třídící znak 342675.

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

[7] ČSN EN 50128 ed.2. *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. Třídící znak 342680.

[8] ISO 26262. *Road vehicles — Functional safety*. Switzerland: International Organization for Standardization. 2011.

[9] *What is the ISO 26262 Functional Safety?* National Instruments [online]. 3. 4. 2014 [cit. 20.2.2017]. Dostupné z: http://www.ni.com

[10] ČSN EN 61800-5-2. *Systémy elektrických výkonových pohonů s nastavitelnou rychlostí - Část 5-2: Bezpečnostní požadavky - Funkční*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2008. Třídící znak 351720.

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

[12] ČSN ISO 50(191). *Medzinárodný elektrotechnický slovník. Kapitola 191: Spoľahlivosť a akosť služieb*. 1993. Třídící znak 010102.

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

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

[15] ČSN IEC 706-2. *Pokyny na udržiavateľnosť zariadení. Časť 2: Oddiel 5: Štúdie o udržiavateľnosti v etape návrhu*. 1994. Třídící znak 010661.

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

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

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

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

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

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

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

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

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

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

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

[27] WANG, C., XING, L., LEVITIN, G*. Explicit and Implicit Methods for Probabilistic Common-Cause Failure Analysis.* Reliability Engineering and System Safety, vol. 131, pp. 175 – 184. 2014.

[28] JOSEPH, R., BELLAND *Modeling common cause failures in diverse components with fault tree applications.* Annual Reliability and Maintainability Symposium (RAMS), pp. 1 – 6. 2017.

[29] 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.

[30] *Hodnocení rizik (HRI), Metody analýzy rizik (MAR)*. Sbírka příkladů

[31] ČSN EN 61882. *Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití.* Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. Třídící znak 010693.

[32] 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.

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

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

[35] 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

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

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

[38] PROCHÁZKOVÁ, D. *Metodiky hodnocení rizik*. Řízení BOZP, č. 3, str. 22-23. [online]. 1. 4. 2004 [cit. 6. 3. 2017]. Dostupné z: https://www.bozpinfo.cz/metodiky-hodnoceni-rizik

[39] HOCKSTAD, P., RAUSAND, M. *Common Cause Failure Modeling: Status and Trends*. Handbook of Performabillitz Engineering. Springer, str. 621-640. London: 2008.

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

[41] 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.

[42] 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.

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

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

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

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

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

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

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

[50] UHER, J. *Funkční bezpečnost*. Course-Hinds series, D-Ex Instruments, Eaton - MTL. 2016

[51] NOVOTNÝ, R. *TIA Safety Integrated, Náhled do norem*. Siemens, s.r.o. divize Industry Automation and Drive Technologies. Brno, 2009.

[52] BERNATÍK, A. *Analýza nebezpečí a rizik*. VŠB TU – Ostrava, 2016.

[53] KOUDELKA, C., VRÁNA, V. *Rizika a jejich analýza*. VŠB TU – Ostrava, FEL. Ostrava, 2006.

[54] NETOLICKÝ, P. *Proces vývoje výrobku*. Směrnice RICE ZČU, RICE-S-03-2016, Plzeň, 2016.

[55] NECID, J. *Bezpečnost strojů a opatření ke snížení rizik*. ČVUT FEL. Praha, 2011. Diplomová práce.

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

Příloha

Příloha A: Část tabulky s analýzou FMECA pro řídicí systém

Failure Mode and Effects Analysis
(Design FMEA)

RICE

Project	ČEZ		System	Řídicí systém měniče - provozní režim		Prepared by	L. Elis							
FMEA Number	1.00		Subsystem	Regulátor DIF U		Design Lead	J. Michalík							
Revision Date	03.08.2017		Component	rozhranní - Interface		Core team	T. Komrska, J. Michalík, P. Turjanica, L. Elis, L. Poláček							

#	Item / Function / Signal		Potencial Failure Mode(s) / Potenciální způsob poruchy	Potencial Local Effect(s) of Failure / Potenciální místní důsledek poruchy	Potencial Global Effect(s) of Failure / Potenciální konečný důsledek poruchy	SEV	Potencial Cause(s)/ Mechanism(s) of Failure / Potenciální příčiny / mechanizmy poruchy	PROB	Detection Method / Metoda detekce	Detection frequency / Četnost detekce	Detection Succes / Úspěšnost detekce	DET	Recommended Action(s) / Doporučená opatření
			trvalé připojení na VCC	Riziko poškození výstutpu DIF Top výkonový tranzistor trvale sepnutý	Větvový zkrat / nadproud				odpojení desaturační ochranou	kontinuuální	100%		
			trvalé připojení na GND	Riziko poškození výstutpu DIF Top výkonový tranzistor trvale zavřený	špatná generace napětí				Porovnání proudů DIFuvw Ix.1-Ix.3	v rámci reg. Smyčky	99%		odstavit identfikovaný vadný blok, provoz na snížený výkon, upravit rovnici součtového proudu
1	1PWM1T_EN	Output - PushPull	rozpojení	Top výkonový tranzistor trvale zavřený	špatná generace napětí				Porovnání proudů DIFuvw Ix.1-Ix.3	v rámci reg. Smyčky	99%		odstavit identfikovaný vadný blok, provoz na snížený výkon, upravit rovnici součtového proudu
2	1PWM1B_DR	Output - PushPull	stejné jako 1PWM1T										
3	1PWM2T_EN	Output - PushPull	stejné jako 1PWM1T										
4	1PWM2B_DR	Output - PushPull	stejné jako 1PWM1T										
			trvalé připojení na VCC	aktivace chyby	zničení driveru				HW v FPGA	kontinuální	100%		blokování příslušného měniče
			trvalé připojení na GND	nedetekovatelná porucha	špatná generace napětí				Diagnostika CAN	diagnostická smyčka	0%		zdvojení signálu 1ERR (využití 1Bi_Res)
5	1ERR	Input	rozpojení	aktivace chyby	(vypnutí měniče)				HW v FPGA	kontinuální	100%		viz předchozí poznámka
			trvalé připojení na VCC										
			trvalé připojení na GND										
6	1WARN	Input	rozpojení										
			trvalé připojení na VCC	využít pro 1ERR "zdvojený signál"									
			trvalé připojení na GND	využít pro 1ERR "zdvojený signál"									
			rozpojení	využít pro 1ERR "zdvojený signál"									
7	1Bi_Res	Input	odlišný od druhého 1ERR	aktivace chyby	(vypnutí měniče) logování chyby				SW v DIF	kontinuální	100%		blokování příslušného měniče
			zkrat	čtení nulové hodnoty	Špatná funkce měniče Mx.1				Porovnání proudů DIFuvw Ix.1-Ix.3 a Ix	v rámci reg. Smyčky	99%		blokování měniče M.x1
			rozpojení	čtení nulové hodnoty	Špatná funkce měniče Mx.1				Porovnání proudů DIFuvw Ix.1-Ix.3 a Ix	v rámci reg. Smyčky	99%		blokování měniče M.x1
8	1LEM I1.x +	Analog Input	nesprávná hodnota	čtení nesprávné hodnoty	Špatná funkce měniče Mx.1				Porovnání proudů DIFuvw Ix.1-Ix.3 a Ix	v rámci reg. Smyčky	99%		blokování měniče M.x1
			zkrat	čtení nulové hodnoty									
			rozpojení	čtení nulové hodnoty									
9	1LEM I1.x -	Analog Input	nesprávná hodnota	čtení nesprávné hodnoty									
			zkrat	čtení nulové hodnoty	vyhodnocení jako vadné čidlo								nezapojovat tento signál do HW komparátoru a dalších ochran (vyhodnotí master DIF)
			rozpojení	čtení nulové hodnoty	vyhodnocení jako vadné čidlo								nezapojovat tento signál do HW komparátoru a dalších ochran (vyhodnotí master DIF)
10	1LEM Udc.x+	Analog Input	nesprávná hodnota	čtení nesprávné hodnoty	vyhodnocení jako vadné čidlo								nezapojovat tento signál do HW komparátoru a dalších ochran (vyhodnotí master DIF)
			zkrat	čtení nulové hodnoty	vyhodnocení jako vadné čidlo								

Příloha B: Analýza odhadu náhodných poruch pro modul „analog“ karty DIF

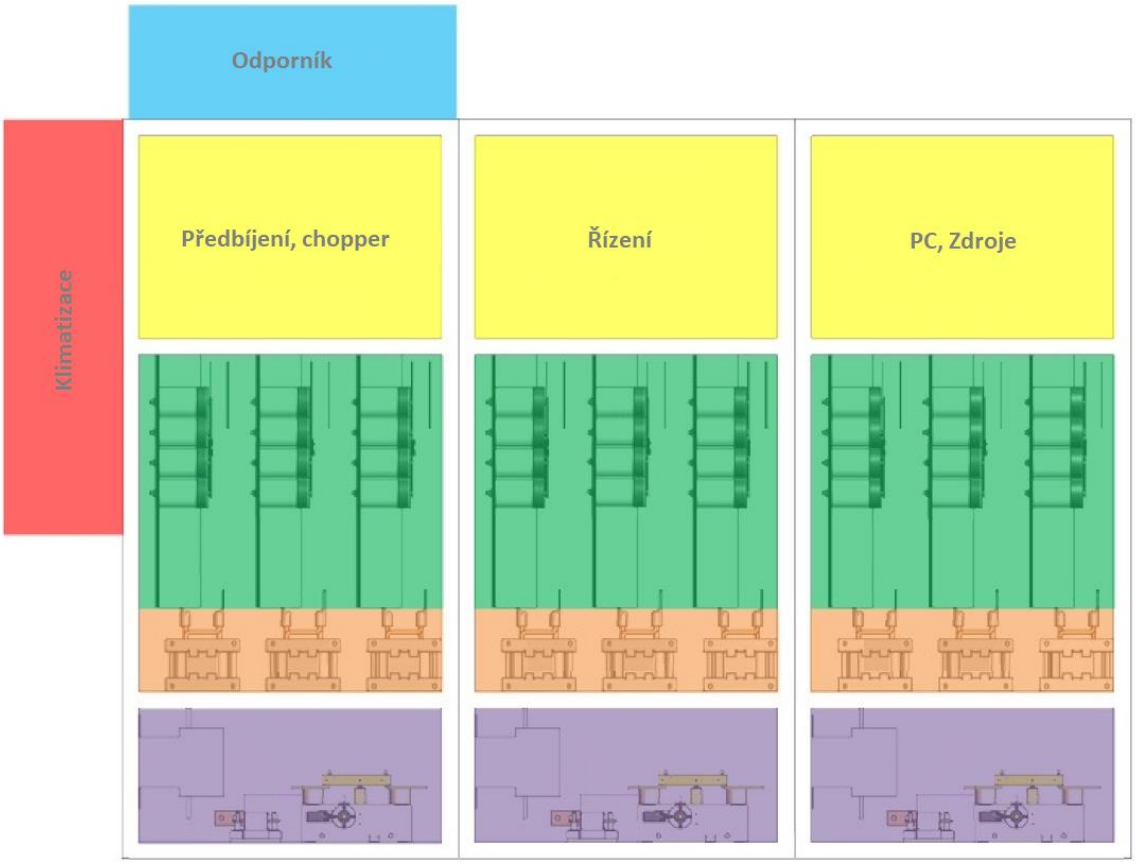
λ Total	194,0 FIT

		Results		STRESS				
Model	**Component type**	**λ Total**	**Quantity**	**Thermal**	**Thermal Cycling**	**Mechanical**	**Humidity**	**Thermo-Elec**
Active Filter		**45,983**	**23**					
ELECTRONIC COMPONENT	Ceramic capacitors [ECCC]	4,2525599	8		1,181648288	0,066644958		3,004266651
ELECTRONIC COMPONENT	Integrated Circuits [ECIC]	40,533086	2	40,447579	0,02078182	0,000137233	0,064587515	
ELECTRONIC COMPONENT	Resistors [ECRE]	1,1973445	13		1,150903098	0,009368588	0,013116023	0,023956809
Comparator User		**1,874**	**8**					
ELECTRONIC COMPONENT	Ceramic capacitors [ECCC]	1,06314	2		0,295412072	0,01666124		0,751066663
ELECTRONIC COMPONENT	Discrete semiconductors [ECDS]	0,4421031	2	0,0722267	0,104349745	0,001369479	0,264157208	
ELECTRONIC COMPONENT	Resistors [ECRE]	0,3684137	4		0,35412403	0,002882642	0,004035699	0,007371326
Comaprator Overlimit		**22,021**	**9**					
ELECTRONIC COMPONENT	Ceramic capacitors [ECCC]	1,06314	2		0,295412072	0,01666124		0,751066663
ELECTRONIC COMPONENT	Discrete semiconductors [ECDS]	0,2210516	1	0,0361133	0,052174872	0,000684739	0,132078604	
ELECTRONIC COMPONENT	Integrated Circuits [ECIC]	20,275984	1	20,22379	0,012578652	8,30631E-05	0,039532874	
ELECTRONIC COMPONENT	Resistors [ECRE]	0,4605171	5		0,442655038	0,003603303	0,005044624	0,009214157
Diff Amp		**50,021**	**26**					
ELECTRONIC COMPONENT	Ceramic capacitors [ECCC]	0,956826	3		0,265870865	0,014995116		0,675959997
ELECTRONIC COMPONENT	Discrete semiconductors [ECDS]	6,5255587	2	6,1556823	0,104349745	0,001369479	0,264157208	
ELECTRONIC COMPONENT	Integrated Circuits [ECIC]	40,683686	2	40,447579	0,065337513	0,000431456	0,1703375	
ELECTRONIC COMPONENT	Magnetic Components: Inductors and Transformers [ECIN]	0,1970543	1		0,151392042	0,042575587		0,003086666
ELECTRONIC COMPONENT	Resistors [ECRE]	1,6578616	18		1,593558136	0,012971891	0,018160647	0,033170966
Rectifier		**1,803**	**12**					
ELECTRONIC COMPONENT	Ceramic capacitors [ECCC]	0,53157	1		0,147706036	0,00833062		0,375533331
ELECTRONIC COMPONENT	Discrete semiconductors [ECDS]	0,4421031	2	0,0722267	0,104349745	0,001369479	0,264157208	
ELECTRONIC COMPONENT	Resistors [ECRE]	0,8289308	9		0,796779068	0,006485945	0,009080324	0,016585483
Reference		**72,280**	**56**					
ELECTRONIC COMPONENT	Ceramic capacitors [ECCC]	7,9735498	15		2,21559054	0,124959297		5,632999971
ELECTRONIC COMPONENT	Integrated Circuits [ECIC]	60,806749	3	60,671369	0,030201025	0,000199432	0,104979761	
ELECTRONIC COMPONENT	Resistors [ECRE]	3,4999301	38		3,364178287	0,027385103	0,038339144	0,070027594

Příloha C: Analýza rozložení intenzit poruch pro kartu DIF systému REMCS

blok	subblok	módy selhání	detekovatelnost	dopad na výstup	λ pro subblok	podíl poruch pro mód	λ módu	DC	λs	λd	λdd	λdu
					FIT	%	FIT	%	FIT	FIT	FIT	FIT
ADC	ADC	Zaseknutí ADC: několikrát po sobě stejná hodnota - detekovatelné	ano	dangerous	96,62	50%	48,31	95%	0	48,31	45,895	2,416
		Nesprávná hodnota: lze srovnávat s paralelním měřením s převodníkem integrovaným v uP	ano	dangerous	96,62	50%	48,31	95%	0	48,31	45,895	2,416
Analog	Diff amp	Změna hodnoty nad rámec pracovních mezí: detekovatelá chyba pomocí komparátorů	ano	dangerous	50,02	50%	25,01	95%	0	25,01	23,76	1,251
		Změna hodnoty v rámci pracovních mezí: nedetekovatelná chyba - mylná informace pro procesor	ne	dangerous	50,02	50%	25,01	5%	0	25,01	1,2505	23,76
	Active filter	Změna hodnoty nad rámec pracovních mezí: detekovatelá chyba pomocí komparátorů	ano	dangerous	45,98	33%	15,1734	33%	0	15,17	5,0072	10,17
		Změna hodnoty v rámci pracovních mezí: nedetekovatelná chyba - mylná informace pro procesor	ne	dangerous	45,98	33%	15,1734	5%	0	15,17	0,7587	14,41
		Změna nastavení kmitočtových vlastností filtru: může ovlivnit přesnost měřené veličiny	ne	dangerous	45,98	33%	15,1734	10%	0	15,17	1,5173	13,66
	Rectifier	Změna hodnoty nad rámec pracovních mezí: detekovatelá chyba pomocí komparace s naměřenou hodnotou	ano	dangerous	72,28	33%	23,8524	95%	0	23,85	22,66	1,193
		Změna hodnoti v rámci pracovních mezí: nedetekovatelná chyba - mylná informace pro procesor	ne	dangerous	72,28	33%	23,8524	20%	0	23,85	4,7705	19,08
		Změna nastavení konfigurace usměrňovače: Ovlivní chování komparátoru v kladné a záporné polaritě signálu. Detekovatelné pomocí srovnání s měřenou hodnotou	ano	dangerous	72,28	33%	23,8524	30%	0	23,85	7,1557	16,7
	Comp Over	Nesprávné vybavení komparátoru: detekovatelné pomocí srovnání s měřenou hodnotou - v rámci regulační smyčky	ano	dangerous	22,02	100%	22,02	95%	0	22,02	20,919	1,101
	Comp User	Nesprávné vybavení komparátoru: detekovatelné pomocí srovnání s měřenou hodnotou - v rámci regulační smyčky	ano	dangerous	1,87	100%	1,87	95%	0	1,87	1,7765	0,094
	Reference	změna hodnoty >2%: detekovatelné pomocí komparátorů	ano	dangerous	72,28	50%	36,14	95%	0	36,14	34,333	1,807
		změna hodnoty o méně než 0,2%: nedetekovatelné. Ovlivňuje přesnost měření	ne	dangerous	72,28	50%	36,14	30%	0	36,14	10,842	25,3
CAN	CAN	Výpadek komunikace: chybná komunikace po CAN lince. Lze detekovat CRC chybou	ano	dangerous	22,79	100%	22,79	95%	0	22,79	21,651	1,14
DAC + Trimpot	DAC	Chybná hodnota DAC: nedekovatelná chyba. DAC je však používán pouze pro ladění a diagnosstické účely. Nemá přímý vliv na regulaci	ne	safe	87,91	100%	87,91	38%	87,91	0	0	0
	Trimpot	Chybné nastavení trimpotu: ovlivní komparační úroveň uživatelských komparátorů. Lze detekovat srovnáním s měřenou veličinou	ano	dangerous	88,19	100%	88,19	95%	0	88,19	83,781	4,41
	Trimpot Switch	Nesprávné nastavení switch: Má za následek nesprávné nastavení komparátorů. Týká se maximálně komparátoru 0, 1. Lze detekovat srovnáním s měřenou hodnotou	ano	dangerous	1,41	100%	1,41	95%	0	1,41	1,3395	0,071
ERR in	ERR in	Aktivace ERR, když chyba není: Systém reaguje, jako by přišla chyba driveru, blokuje prvky	ne	dangerous	200,05	50%	100,025	0%	0	100	0	100
		Neaktivace v chybě: nedetekovatelné	ne	dangerous	200,05	50%	100,025	0%	0	100	0	100
ETH	ETH		ano	safe	33,86	100%	33,86	95%	33,86	0	0	0
FPGA	FPGA APL		ano	safe	34,9	100%	34,9	95%	34,9	0	0	0
	FPGA JTAG	Výpadek JTAG: nelze programovat	ano	dangerous	31,4	100%	31,4	70%	0	31,4	21,98	9,42
	FPGA systém		ano	dangerous	7,2	100%	7,2	95%	0	7,2	6,84	0,36
	FPGA user		ano	dangerous	37,9	100%	37,9	95%	0	37,9	36,005	1,895
	FPGA power		ano	dangerous	22,2	100%	22,2	95%	0	22,2	21,09	1,11
	FPGA comm		ano	dangerous	0,2	100%	0,2	95%	0	0,2	0,19	0,01
OSC	OSC	Výpadek oscilátoru: uP i FPGA přepnou na záložní OSC, detekují první chybu	ano	dangerous	84	100%	84	95%	0	84	79,8	4,2
PWM driver	PWM out	Trvalá log. 1: Trvalá aktivace výkonového prvku. Lze detekovat nadproudem. Je třeba odpojit jiný výkonový prvek pro odpojení proudu. Může zasáhnout driver na nadproud	ano	dangerous	43,7	50%	21,85	95%	0	21,85	20,758	1,093
		Trvalá log. 0: Mírnější stav, výkonový prvek není sepnut, neteče pracovní proud	ano	dangerous	43,7	50%	21,85	95%	0	21,85	20,758	1,093
Reset	Reset	Trvale aktivován RESET: DIS je v resetu, pulzu jsou blokovány	ano	dangerous	49,55	100%	49,55	95%	0	49,55	47,073	2,478
Safety	Safety block	Vybaví, když nemá: zablokuje PWM výstupy všech karet	ano	dangerous	36,24	60%	21,744	95%	0	21,74	20,657	1,087
		Nevybaví, když má: nutno spolehnout na jiný typ ochrany např nadproud.	ne	dangerous	36,24	40%	14,496	0%	0	14,5	0	14,5
	Safety block control	Quitace je aktivována, kdy nemá být: Je detekovatelné pomocí FPGA, jak FPGA tak i uP může dostat tento obvod do neaktivního stavu	ano	dangerous	12,49	50%	6,245	95%	0	6,245	5,9328	0,312
		Quitace není aktivována, ale má být: Nelze odmazat HW chybu, PWM výstupu zůstávají zablokované	ano	dangerous	12,49	50%	6,245	95%	0	6,245	5,9328	0,312
Serdes	Serdes	Výpadek komunikace: chybná komunikace po CAN lince. Lze detekovat CRC chybou	ano	dangerous	12,29	100%	12,29	95%	0	12,29	11,676	0,615
Systém sygnal	System signals	Výpadek aktivace systémového signálu: lze detekovat měření tého signálu vstupní linkou	ano	dangerous	40,3	50%	20,15	95%	0	20,15	19,143	1,008
		Výpadek sledování signálu: Je detekovatelné pouze na jednotce, které tento signál momentálně ovládá	ne	dangerous	40,3	50%	20,15	50%	0	20,15	10,075	10,08
uP	uP	Procesor nereaguje: aktivuje se WDT, FPGA blokuje pulzy	ano	dangerous	69,5	100%	69,5	95%	0	69,5	66,025	3,475
	uP filter	Hodnoty mimo rozsah: srovnáním z hodnotou z ADC lze detekovat chybu	ano	dangerous	7,2	100%	7,2	80%	0	7,2	5,76	1,44
Power	Power main	Nejde zdroj, nejde nic	ano	dangerous	611	100%	611	95%	0	611	580,45	30,55
IDN	IDN	Nefunkční IDN: neprobíhá běžná komunikace. Buď systém není ani zapnut, nebo nastala-li chyba v průběhu zapnutí a IDN nekomunikuje, tak se aktivuje chyba, protože IDN neodpovídá	ano	dangerous	81,3	100%	81,3	95%	0	81,3	77,235	4,065
	IDN JTAG		ne	safe	44,69	100%	44,69	0%	44,69	0	0	0
	IDN Adress	Nesprávná identifikace pozice jednotky. Nastane-li kolize s jinou kartou, systém se nerozběhne	ano	safe	42,28	100%	42,28	20%	42,28	0	0	0
	IDN Supply		ano	safe	24	100%	24	95%	24	0	0	0
Sequencer	Sequencer	Výpadek sequenceru: Nenaběhnou všechna napájecí napětí. Detekovatelné měřením vlastních napětí	ano	dangerous	7,15	100%	7,15	95%	0	7,15	6,7925	0,358
SPI	SPI	Chyba konfigurace kanálů: v rámci pomalejší smyčky je informace nastavena znovu a je detekována původní konfigurace systému. Tím lze detekovat chybu	ano	dangerous	13,48	33%	4,4484	20%	0	4,448	0,8897	3,559
		Chyba nastavení trimpotů: v rámci pomalejší smyčky je informace nastavena znovu a je detekována původní konfigurace systému. Tím lze detekovat chybu	ano	dangerous	13,48	33%	4,4484	20%	0	4,448	0,8897	3,559
		Chyba nastavení DAC: v rámci pomalejší smyčky je informace nastavena znovu a je detekována původní konfigurace systému. Tím lze detekovat chybu	ano	dangerous	13,48	33%	4,4484	20%	0	4,448	0,8897	3,559
									267,64	1839	1400,1	439,1

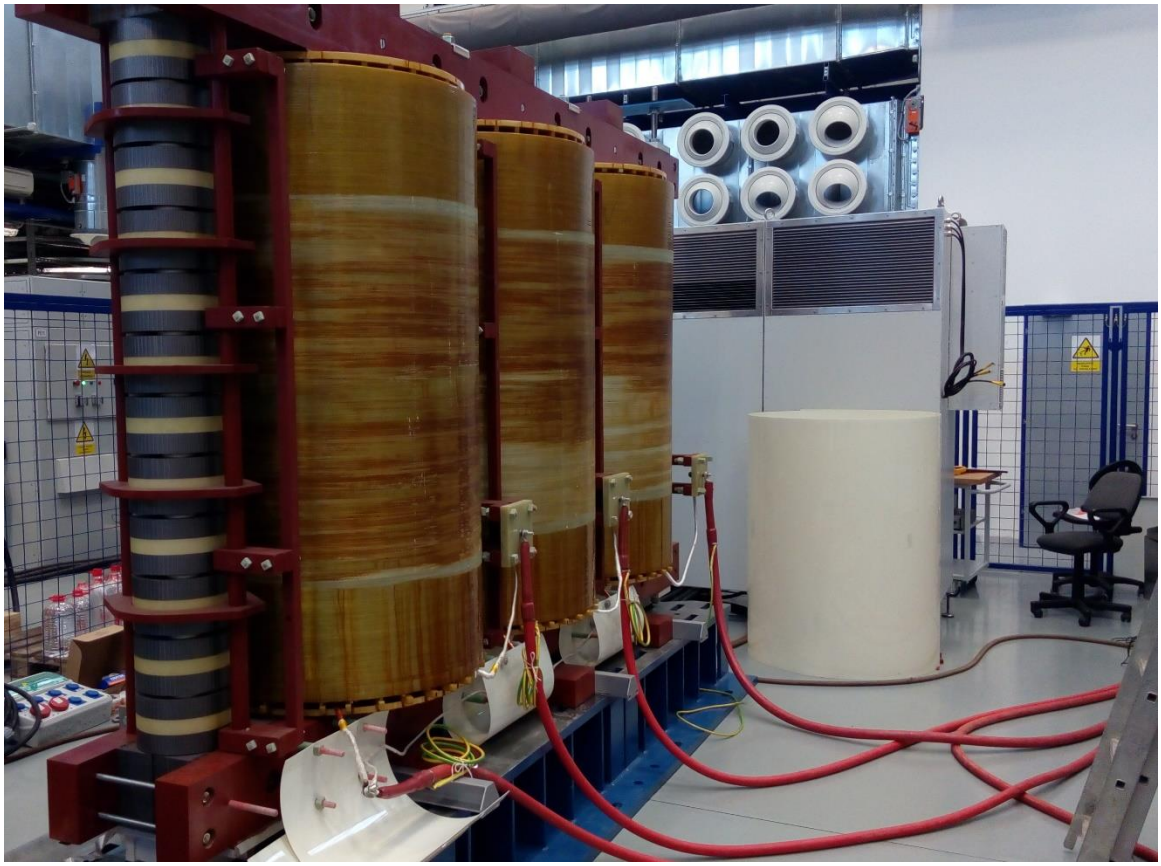
Příloha D: Prostorové uspořádání rozvaděče Zařízení pro kompenzaci



Příloha E: Rozvaděč Zařízení pro kompenzaci na zkušebně

Příloha F: Pohled na otevřenou část rozvaděče Zařízení pro kompenzaci

Příloha G: Pohled na kompenzační transformátor na zkušebně, v pozadí část rozvaděče Zařízení pro kompenzaci



Příloha H: Doporučené techniky a opatření pro jednotlivé fáze životního cyklu bezpečnosti softwaru

1 Specifikace požadavků bezpečnosti softwaru					
Technika / opatření	Odkaz v ČSN EN 61508-7	SIL1	SIL2	SIL3	SIL4
Polo-formální metody	Tabulka B.7	R	R	HR	HR
Formální metody	B.2.2, C.2.4	-	R	R	HR
Postupná sledovatelnost mezi systémovými požadavky na bezpečnost a softwarovými požadavky na bezpečnost	C.2.11	R	R	HR	HR
Zpětná sledovatelnost mezi požadavky na bezpečnost a pochopenými potřebami bezpečnosti	C.2.11	R	R	HR	HR
Počítačem podporované nástroje pro podporu vhodné techniky / opatření	B.2.4	R	R	HR	HR
2 Návrh a vývoj softwaru: architektura softwaru					
Zjišťování a diagnóza vad	C.3.1	-	R	HR	HR
Detekční a samoopravné kódy	C.3.2	R	R	R	HR
Programování s ověřováním předpokládaných poruch (failure assertion programming)	C.3.3	R	R	R	HR
Rozdílné techniky monitorování (s nezávislostí mezi monitorovací a monitorovanou funkcí ve stejném počítači)	C.3.4	-	R	R	-
Rozdílné techniky monitorování (s oddělením monitorovacího a monitorovaného počítače)	C.3.4	-	R	R	HR
Rozdílná redundance, implementace stejných specifikací požadavků na bezpečnost softwaru	C.3.5	-	-	-	R
Funkčně různorodá redundance, implementace různých požadavků na bezpečnost softwaru	C.3.5	-	-	R	HR
Zpětné zotavení	C.3.6	R	R	-	NR
Bezstavový návrh software (nebo stavově omezený návrh)	C.2.12	-	-	R	HR
Mechanizmus opakovaného zotavení po vadě	C.3.7	R	R	-	-
Řízené zhoršení vlastností	C.3.8	R	R	HR	HR
Oprava vad s využitím technik umělé inteligence	C.3.9	-	NR	NR	NR
Dynamická rekonfigurace	C.3.10	-	NR	NR	NR

Modulární přístup	Tabulka B.9	HR	HR	HR	HR
Použití důvěryhodných / ověřených softwarových prvků (jsou-li k dispozici)	C.2.10	R	HR	HR	HR
Postupná sledovatelnost mezi softwarovými požadavky na bezpečnost a architekturou softwaru	C.2.11	R	R	HR	HR
Zpětná sledovatelnost mezi softwarovými požadavky na bezpečnost a architekturou softwaru	C.2.11	R	R	HR	HR
Strukturované schematické modely	C.2.1	HR	HR	HR	HR
Polo-formální metody	Tabulka B.7	R	R	HR	HR
Metody formálního návrhu a zdokonalovací metody	B.2.2, C.2.4	-	R	R	HR
Automatické generování softwaru	C.4.6	R	R	R	R
Počítačem podporované specifikace a návrhové nástroje	B.2.4	R	R	HR	HR
Cyklické chování s garantovanou maximální dobou cyklu	C.3.11	R	HR	HR	HR
Časově spouštěná architektura	C.3.11	R	HR	HR	HR
Řízená událost s garantovanou maximální dobou odezvy	C.3.11	R	HR	HR	-
Statická alokace zdrojů	C.2.6.3	-	R	HR	HR
Statická synchronizace přístupu ke sdíleným zdrojům	C.2.6.3	-	-	R	HR
3 Návrh a vývoj softwaru: podpůrné prostředky a programovací jazyk					
Vhodný programovací jazyk	C.4.5	HR	HR	HR	HR
Programovací jazyk s přísnou kontrolou typů	C.4.1	HR	HR	HR	HR
Jazykový podsoubor	C.4.2	-	-	HR	HR
Certifikované nástroje a překladače	C.4.3	R	HR	HR	HR
Nástroje a překladače: vyšší důvěra na základě používání	C.4.4	HR	HR	HR	HR
4 Návrh a vývoj softwaru: podrobný návrh					
Strukturované metody	C.2.1	HR	HR	HR	HR
Polo-formální metody	Tabulka B.7	R	HR	HR	HR
Metody formálního návrhu a zdokonalovací metody	B.2.2, C.2.4	-	R	R	HR
Počítačem podporované návrhové nástroje	B.3.5	R	R	HR	HR

Defenzivní programování	C.2.5	-	R	HR	HR
Modulární přístup	Tabulka B.9	HR	HR	HR	HR
Pravidla pro návrh a kódování	C.2.6 Tabulka B.1	R	HR	HR	HR
Strukturované programování	C.2.7	HR	HR	HR	HR
Použití důvěryhodných / ověřených softwarových prvků (jsou-li k dispozici)	C.2.10	R	HR	HR	HR
Postupná sledovatelnost mezi systémovými požadavky na bezpečnost a návrhem softwaru	C.2.11	R	R	HR	HR
5 Návrh a vývoj softwaru: začlenění a zkoušení softwarových modulů					
Pravděpodobnostní zkoušky	C.5.1	-	R	R	R
Dynamická analýza a zkoušky	B.6.5 Tabulka B.2	R	HR	HR	HR
Záznam a analýza dat	C.5.2	HR	HR	HR	HR
Funkční zkoušky a zkoušky typu „černé skříňky“	B.5.1 B.5.2 Tabulka B.3	HR	HR	HR	HR
Výkonnostní zkoušky	Tabulka B.6	R	R	HR	HR
Modelové zkoušky	C.5.27	R	R	HR	HR
Zkoušky rozhraní	C.5.3	R	R	HR	HR
Řízení testů a automatizační nástroje	C.4.7	R	HR	HR	HR
Postupná sledovatelnost mezi softwarovými požadavky a specifikací modulů a integračních zkoušek	C.2.11	R	R	HR	HR
Formální ověření	C.5.12	-	-	R	R
6 Začlenění programovatelné elektroniky (hardwaru a softwaru)					
Funkční zkoušky a zkoušky typu „černé skříňky“	B.5.1 B.5.2 Tabulka B.3	HR	HR	HR	HR
Výkonnostní zkoušky	Tabulka B.6	R	R	HR	HR
Postupná sledovatelnost mezi systémovými a softwarovými návrhovými požadavky pro HW / SW integraci a specifikací HW / SW integračních zkoušek	C.2.11	R	R	HR	HR
7 Potvrzení platnosti bezpečnosti softwaru					
Pravděpodobnostní zkoušky	C.5.1	-	R	R	HR

Simulace procesu	C.5.18	R	R	HR	HR
Modelování	Tabulka B.5	R	R	HR	HR
Funkční zkoušky a zkoušky typu „černé skříňky“	B.5.1 B.5.2 Tabulka B.3	HR	HR	HR	HR
Postupná sledovatelnost mezi softwarovými požadavky na bezpečnost a plánem ověření bezpečnosti softwaru	C.2.11	R	R	HR	HR
Zpětná sledovatelnost mezi plánem ověření bezpečnosti softwaru a softwarovými požadavky na bezpečnost	C.2.11	R	R	HR	HR
8 Modifikace					
Analýza dopadů	C.5.23	HR	HR	HR	HR
Opakované ověření změněných softwarových modulů	C.5.23	HR	HR	HR	HR
Opakované ověření ovlivněných softwarových modulů	C.5.23	R	HR	HR	HR
Opakované potvrzení platnosti celého systému	Tabulka A.7	-	R	HR	HR
Regresivní potvrzení platnosti	C.5.25	R	HR	HR	HR
Management konfigurace softwaru	C.5.24	HR	HR	HR	HR
Záznam a analýza dat	C.5.2	HR	HR	HR	HR
Postupná sledovatelnost mezi softwarovými požadavky na bezpečnost a plánem modifikace softwaru (včetně opakovaného ověření a potvrzení platnosti)	C.2.11	R	R	HR	HR
Zpětná sledovatelnost mezi plánem modifikace softwaru (včetně opakovaného ověření a potvrzení platnosti) a softwarovými požadavky na bezpečnost	C.2.11	R	R	HR	HR
9 Ověření softwaru					
Formální zkouška	C.5.12	-	R	R	HR
Animace specifikace a designu	C.5.26	R	R	R	R
Statická analýza	B.6.5 Tabulka B.8	R	HR	HR	HR
Dynamická analýza a zkoušení	B.6.5 Tabulka B.2	R	HR	HR	HR
Postupná sledovatelnost mezi požadavky na návrh softwaru a plánem ověření softwaru (včetně ověření dat)	C.2.11	R	R	HR	HR

Zpětná sledovatelnost mezi plánem ověření softwaru (včetně ověření dat) a požadavky na návrh softwaru	C.2.11	R	R	HR	HR
Offline numerická analýza	C.2.13	R	R	HR	HR
Začlenění a zkoušky softwarových modulů	Viz Tabulka A.5				
Zkouška začlenění programovatelné elektroniky	Viz Tabulka A.6				
Zkoušky systému softwaru (potvrzení platnosti)	Viz Tabulka A.7				
10 Odhad funkční bezpečnosti					
Kontrolní seznamy	B.2.5	R	R	R	R
Rozhodovací / pravdivostní tabulky	C.6.1	R	R	R	R
Analýza poruch	Tabulka B.4	R	R	HR	HR
Analýza poruch se společnou příčinnou u různě řešeného softwaru (je-li tento software skutečně použit)	C.6.3	-	R	HR	HR
Bezporuchovostní blokové schéma	C.6.4	R	R	R	R
Postupná sledovatelnost mezi požadavky Klauzule 8 a plánem hodnocení funkční bezpečnosti softwaru	C.2.11	R	R	HR	HR