VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV ELEKTROTECHNOLOGIE

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF ELECTRICAL AND ELECTRONIC TECHNOLOGY

FUNKČNÍ BEZPEČNOST SNÍMAČŮ TLAKU BD SENSORS, S.R.O.

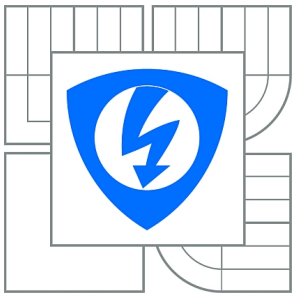
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN ŠIMONÍK
AUTHOR

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV ELEKTROTECHNOLOGIE

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF ELECTRICAL AND ELECTRONIC TECHNOLOGY

FUNKČNÍ BEZPEČNOST SNÍMAČŮ TLAKU BD SENSORS, S.R.O.

FUNCTIONAL SAFETY OF PRESSURE TRANSMITTERS OF BD SENSORS COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN ŠIMONÍK

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Pavel Fuchs, CSc.

SUPERVISOR

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav elektrotechnologie

Diplomová práce

magisterský navazující studijní obor
Elektrotechnická výroba a management

Student:	Bc. Martin Šimoník	***ID:***	119627
Ročník:	2	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Funkční bezpečnost snímačů tlaku BD SENSORS, s.r.o.

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou funkční bezpečnosti a SIL v měřicí a automatizační technice.
Popište zvolený přístup k určení SIL3 vybraných snímačů tlaku BD SENSORS jak pro HW, tak SW část snímačů.
Proveďte specifikaci technické dokumentace a dokladů potřebných pro certifikaci snímačů na úrovni SIL3.
Proveďte analýzy potřebné k určení SIL3 pro HW část a specifikování postupů pro tvorbu aplikačního SW snímačů.
Závěrem shrňte poznatky získané při řešení problematiky.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání:	10.2.2015	***Termín odevzdání:***	28.5.2015

Vedoucí práce: doc. Ing. Pavel Fuchs, CSc.
Konzultanti diplomové práce: Ing. Radek Burda, BD SENSORS s.r.o.

doc. Ing. Petr Bača, Ph.D.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato diplomová práce se zabývá otázkou funkční bezpečnosti snímače tlaku XMP i vyráběného firmou BD SENSORS. Cílem práce je prokázat splnění požadavků na funkční úroveň integrity bezpečnosti SIL 3.

Práce je rozdělena do tří částí. První část práce se zabývá pojmem funkční bezpečnost, definuje základní pojmy funkční bezpečnosti, porovnává přístupy funkční bezpečnosti dle vybraných norem a stanovuje obecný postup stanovení funkční bezpečnosti.

Druhá část práce pojednává o spolehlivosti technických systémů, definuje spolehlivostní ukazatele a popisuje vybrané typy spolehlivostních analýz užívaných v praxi a to zejména na analýzu FMEA/FMECA.

Poslední část se zabývá praktikováním spolehlivostních analýz na snímači XMP i a zhodnocením dosažených výsledků.

KLÍČOVÁ SLOVA

Bezpečnost, riziko, funkční bezpečnost, SIL, PL, úroveň integrity bezpečnosti, bezpečnostní funkce, úroveň vlastností, FMEA/FMECA, MTBF, intenzita poruch

ABSTRACT

This master thesis examines the functional safety of the pressure sensor XMP i which is produced by BD SENSORS Company. The aim of this thesis is the demonstration of compliance of the pressure sensor XMP I with functional safety integrity level SIL3 requirements.

The thesis is divided into three parts. The first part deals with the concept of functional safety, defines the basic concepts of functional safety, compares the approaches of functional safety according to selected standards and provides a general procedure for the functional safety determination.

The second part deal with technical systems reliability defines reliability indicators and describes selected types of reliability analysis used in practice, especially the FMEA/FMECA analysis.

Third part deals with the reliability analysis of the sensor XMP i and with evaluation of results.

KEYWORDS

Safety, risk, functional safety, SIL, PL, safety integrity level, safety function, performance level, FMEA/FMECA, MTBF, failure rate

ŠIMONÍK, M. *Funkční bezpečnost snímačů tlaku BD SENSORS, s.r.o*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav elektrotechnologie, 2015. 75 s., 1 s. příloh. Diplomová práce. Vedoucí práce: doc. Ing. Pavel FUCHS, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Funkční bezpečnost snímačů tlaku BD SENSORS, s.r.o. jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce doc. Ing. Pavlu Fuchsovi, CSc. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování své diplomové práce.

V Brně dne 28. 5. 2015 .....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK A SYMBOLŮ

A	Součinitel asymptotické pohotovosti
A(t)	Funkce okamžité pohotovosti
ALARP	As Low As Reasonably Practicible
EUC	Řízené zařízení – Equipment Under Control
E/E/PE	Elektrický/elektronický/programovatelný elektronický systém – Electrical/Electronical/Programable Electronic System
ETA	Analýza stromu událostí – Event Tree Analysis
FMEA	Analýza způsobů a důsledků poruch – Failure Mode and Effects Analysis
FMECA	Analýza způsobů, důsledků a kritičnosti poruch – Failure Mode, Effects and Criticality Analysis
FTA	Analýza stromu poruchových stavů – Fault Tree Analysis
IEC	Mezinárodní elektrotechnická komise – International Electrotechnical Commission
ISO	Mezinárodní organizace pro normalizaci – International Organization for Standartization
HRA	Analýza bezporuchové činnosti člověka – Human Reliability Analysis
HSE	Britský úřad pro zdraví a bezpečnost - Health and Safety Executive
λ	Intenzita poruch
$\lambda_{0,05}$	Dolní konfidenční mez intenzity poruch
$\lambda_{0,95}$	Horní kofidenční mez intenzity poruch
λ_{DD}	Intenzita nebezpečných detekovatelných poruch
λ_{DU}	Intenzita nebezpečných nedetekovatelných poruch
λ_{SD}	Intenzita bezpečných detekovatelných poruch
λ_{SU}	Intenzita bezpečných nedetekovatelných poruch
λ_{NE}	Intenzita poruch bez efektu na systém (modul)
λ_{DDMD}	Intenzita nebezpečných detekovatelných poruch modulu displeje
λ_{DUMD}	Intenzita nebezpečných nedetekovatelných poruch modulu displeje
λ_{SDMD}	Intenzita bezpečných detekovatelných poruch modulu displeje
λ_{SUMD}	Intenzita bezpečných nedetekovatelných poruch modulu displeje
λ_{NEMD}	Intenzita poruch bez efektu na modul displeje
λ_{DDSYS}	Intenzita nebezpečných detekovatelných poruch systému
λ_{DUSYS}	Intenzita nebezpečných nedetekovatelných poruch systému
λ_{SDSYS}	Intenzita bezpečných detekovatelných poruch systému

λ_{SUSYS}	Intenzita bezpečných nedetekovatelných poruch systému
λ_{NESYS}	Intenzita poruch bez efektu na modul displeje
MAV	Modul analogového výstupu
MD	Modul displeje
MDK	Modul digitální komunikace
MES	Modul elektroniky systému
MP	Modul procesoru
MMP	Modul mechanického pouzdra
MN	Modul napájení
MS	Modul senzoru
MTBF	Střední doba mezi poruchami (Mean Time Between Failure)
$MTBF_{0,95}$	Dolní konfidenční mez střední doby mezi poruchami
$MTBF_{0,05}$	Horní konfidenční mez střední doby mezi poruchami
$MTBF_{MD}$	Střední doba mezi poruchami modulu displeje
$MTBF_{SYS}$	Střední doba mezi poruchami systému (snímače)
MTTF	Střední doba do poruchy (Mean Time To Failure)
MTTR	Střední doba do obnovy (Mean Time To Restoration)
$MTTR_{0,95}$	Dolní konfidenční mez střední doby do obnovy
$MTTR_{0,05}$	Horní konfidenční mez střední doby do obnovy
PES	Programovatelný elektronický systém – Programmable Electronic System
PFH	Střední pravděpodobnost nebezpečné poruchy za hodinu provozu
PFD	Střední pravděpodobnost výskytu nebezpečné poruchy při vyžádání funkce
PIU	Postulovaná iniciační událost
PL	Úroveň vlastností (Performance Level)
Q(t)	Pravděpodobnost poruchy
R(t)	Pravděpodobnost bezporuchového stavu
SIF	Bezpečnostní přístrojová funkce (Safety Instrumented Function)
U	Součinitel asymptotické nepohotovosti
U(t)	Funkce okamžité nepohotovosti
U_D	Součinitel asymptotické nepohotovosti od nebezpečné poruchy
U_{DD}	Součinitel asymptotické nepohotovosti od nebezpečné detekovatelné poruchy
U_{DU}	Součinitel asymptotické nepohotovosti od nebezpečné nedetekovatelné poruchy

ÚVOD

V dnešní době rychlého rozvoje vědy a techniky se požadavky kladené na průmysl neustálé více stupňují. Do popředí se dostává výroba kvalitnějších, spolehlivějších a v neposlední řadě také bezpečnějších výrobků. Bezpečnost, to je vlastnost, na kterou je kladen čím dál tím větší důraz.

Tato práce se zabývá stanovením funkční bezpečnosti na výrobku firmy BD SENSORS, s.r.o. Jedná se o snímač tlaku XMP i. V první části této práce je uvedena teorie problému funkční bezpečnosti. Je zde uvedeno, dle kterých norem se funkční bezpečnost v oblasti automatizační a měřící techniky řídí. Jedná se tedy především o normu ČSN EN 61508 [5]. Tato část práce vysvětluje základní pojmy funkční bezpečnosti a udává vzájemný vztah mezi funkční bezpečností, celkovou bezpečností a rizikem. Stanovuje požadavky jak na hardware tak i software vybraného snímače XMP i. V závěru této kapitoly je uveden základní obecný postup pro určení funkční bezpečnosti spojený s pojmem PIU (postulovaná iniciační událost).

Druhá část této práce popisuje pojem spolehlivost. Definuje spolehlivostní ukazatele, jako je např. intenzita poruch λ, střední doba do poruchy MTTF, či střední doba mezi poruchami MTBF. Tyto spolehlivostní ukazatele je možné určit jak analyticky, numericky tak i empiricky. Určením těchto spolehlivostních ukazatelů se zabývají spolehlivostní analýzy.

Třetí část této práce popisuje spolehlivostní analýzy a to především spolehlivostní analýzu FMEA/FMECA jejíž vlastní provedení na snímači XMP i slouží jako hlavní podklad pro určení integrity funkční bezpečnosti SIL (Safety Integrity Level). Následuje vlastní návrh řešení.

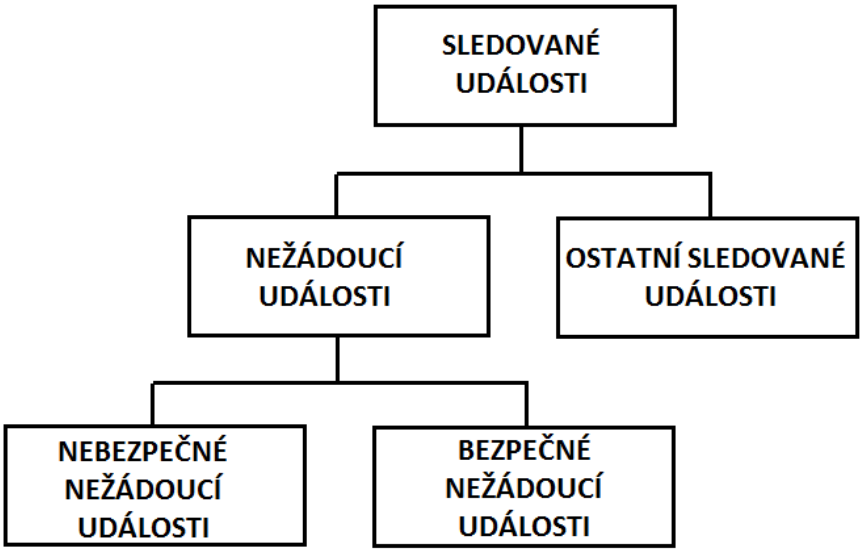
Závěrečná část práce porovnává data získaná z provozu snímače XMP i s daty získanými z provedení spolehlivostní analýzy FMEA/FMECA. V této části práce je prokázáno, zda daný snímač XMP i splňuje integritu funkční bezpečnosti SIL 3 či nikoliv.

1 FUNKČNÍ BEZPEČNOST V AUTOMATIZAČNÍ A MĚŘICÍ TECHNICE

Aby bylo možné problematice funkční bezpečnosti lépe porozumět, považuji za nutné nejprve definovat pojmy riziko a bezpečnost, jelikož tyto pojmy s problematikou funkční bezpečnosti velice úzce souvisí.

1.1 Riziko

V průmyslovém provozu se obvykle sleduje nějaká množina jevů (událostí). Pouze některé prvky množiny událostí mají charakter nežádoucích událostí. S každou nežádoucí událostí (z této množiny událostí) je spojen nějaký nepříznivý následek. K účinnému ovlivňování spolehlivosti a bezpečnosti je třeba definovat hierarchii jevů (událostí), které lze v průmyslovém provozu očekávat. Při návrhu hierarchie struktury událostí je zásadní definice nebezpečné události. Pojem bezpečí a nebezpečí se v původním významu vztahuje pouze k životu a zdraví člověka. Z toho vychází hierarchie událostí na obr. 6 a s ní spojené definice pojmů. Hierarchie událostí je sestavena na základě členění událostí podle jejich následků [15].



Obr. 1: Struktura událostí průmyslového provozu – podle následků [15]

Definice rizika

riziko = pravděpodobnost (nebo četnost) výskytu nebezpečné události x kvantifikované následky nebezpečné události

Riziko můžeme zapsat do symbolické rovnice ve tvaru:

$$R = P \cdot C$$

R – riziko (Risk)

P – pravděpodobnost vzniku nebezpečné události (Probability)

C – následky nebezpečné události (Consequences)

Pravděpodobnost nastání nebezpečné události je sice bezrozměrná veličina, v praxi bývá často vztažena k nějakému parametru (rok, km, počet cyklů apod.), rovněž následky mohou být kvantifikovány různě (hmotná škoda, počet úmrtí atd.), viz tab. 1 [15].

Tab. 1: Míry vztažené pravděpodobnosti a následků [15]

Vztažená pravděpodobnost	Následek
rok^{-1}	hmotná škoda [Kč]
km^{-1}	okamžité úmrtní [počet]
$km^{-2}.rok^{-1}$	úmrtí z pozdních následků [počet]

Při posuzování rizikovosti lidských aktivit se riziko hodnotí zpravidla prostřednictvím ekonomické ztráty nebo poškození lidského zdraví, tedy dvě míry rizika – finanční a zdravotní.

Druhy rizik

Z hlediska povahy vyvolaných následků nebezpečných událostí se např. podle ČSN EN 31010:2011 rozlišují čtyři základní kategorie rizik:

- individuální následky (s dopadem na jednotlivce),
- následky z povolání (s dopadem na pracovníky),
- společenské následky (s dopadem na veřejnost),
- škody majetku a ekonomické ztráty (včetně přerušení podnikání, pokut apod.).

1.2 Bezpečnost

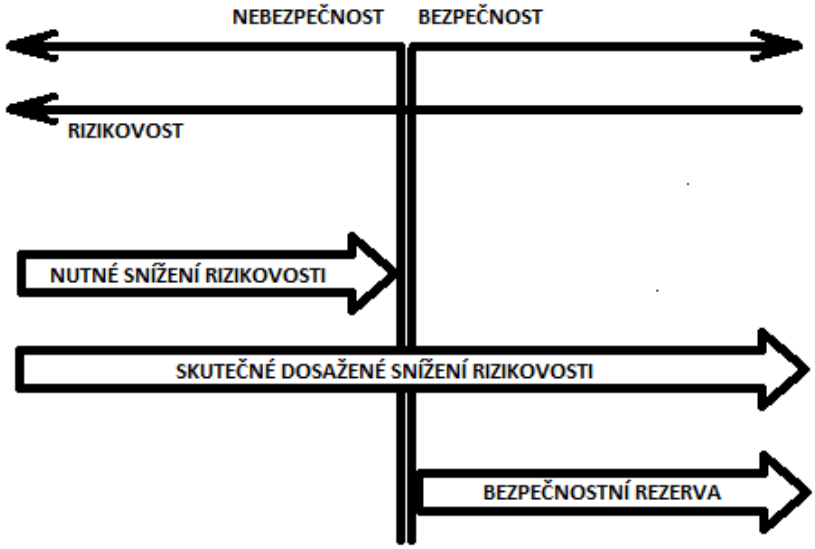
Bezpečnost patří beze sporu mezi nejvýznamnější inherentní znaky kvality. Spolu se spolehlivostí a funkčností ji řadíme mezi znaky kvality, které jsou v obecné definici kvality klíčové. Bezpečnost je obecně vymezena jako stav objektu (výrobku, produktu), procesu nebo systému, u kterého je riziko ohrožení veřejných oprávněných zájmů při běžném užívání omezeno na přijatelnou úroveň. Zajištění požadované úrovně bezpečnosti je tedy založeno na identifikaci, analýze, zhodnocení a ošetření rizik [20].

Definice bezpečnosti

bezpečnost = vlastnost, vyjadřující schopnost objektu (produktu, výrobku), procesu, systému, organizace atd.) být ve stavu, kdy riziko ohrožení života a zdraví lidí, životního prostředí a poškození majetku je omezeno na přijatelnou mez.

Zjednodušeně tedy můžeme říci, že bezpečnost je omezení rizika na určitou přijatelnou mez.

Filozofie posuzování bezpečnosti je naznačena na obr. 4. Vychází se z principu, že úplné vyloučení rizika je nemožné a vzhledem k soudobému stavu vědy, techniky a dalších poznatků s nimi souvisejících je určité zbytkové riziko akceptovatelné. Důležité však je, aby byl uživatel před takovýmto zbytkovým rizikem varován a aby toto zbytkové riziko bylo menší než riziko mezní, které je stanoveno příslušnými právními předpisy. Mezní riziko tedy tvoří hranici, kterou rozlišujeme, zda se jedná o výrobek bezpečný či nebezpečný.

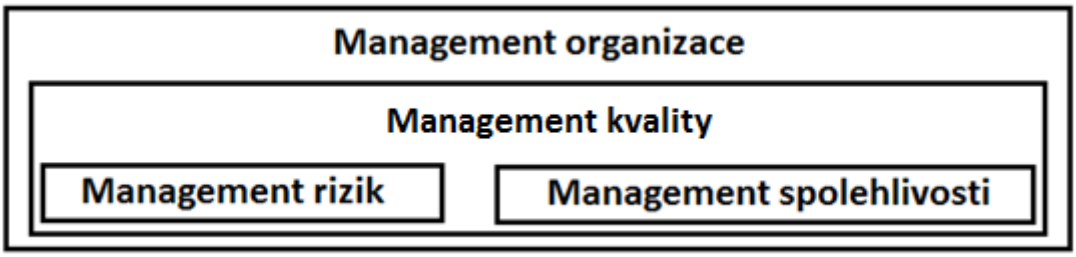


Obr. 2: Posuzování rizikovosti ve vztahu k bezpečnosti

Současné chápání bezpečnosti technických zařízení ctí zásadu, že kdo chce vyrábět nebo dovážet výrobky, musí znát všechna rizika spojená s jejich užíváním a všechny technické a právní aspekty, které tato rizika omezují nebo odstraňují. Dalším východiskem k řešení problematiky bezpečnosti těchto zařízení je vyjádření ztráty schopnosti plnit požadované funkce při jejich užívání, neboť jen samotné poškození, či vyřazení z provozu tohoto zařízení může způsobit riziko ohrožení veřejných oprávněných zájmů. Pozornost je tedy soustředěna na sledování stavu těchto systémů, ve kterých je riziko jejich poškození omezováno na přijatelnou úroveň.

1.3 Bezpečnost a management rizik

Zajišťování předem specifikované úrovně bezpečnosti je neoddělitelnou, velmi významnou a v současné době stále více zdůrazňovanou součástí péče o kvalitu v organizacích. Tudíž k dosahování očekávané bezpečnosti (a optimální spolehlivosti), je nutné se ve struktuře managementu společnosti systematicky zabývat viz obr. 3 [3].

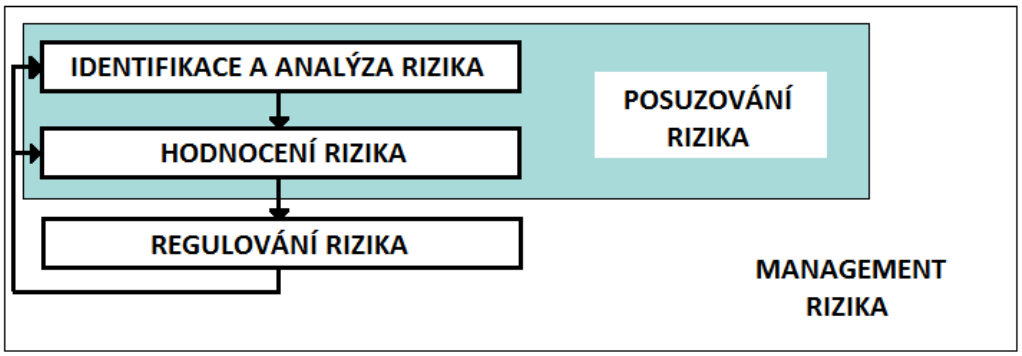


Obr. 3: Management rizik v managementu organizace [3]

Zajištění a realizace manažerské stránky se označuje jako management rizik a je definován následovně:

management rizik = systematické uplatňování politik, postupů a praktik managementu organizace při řešení úkolů identifikování analyzování, hodnocení, posouzení a regulování rizik.

Základní rozdělení managementu rizik je znázorněno na obr. 4 [21].



Obr. 4: Struktura posuzování rizika a management rizika [21]

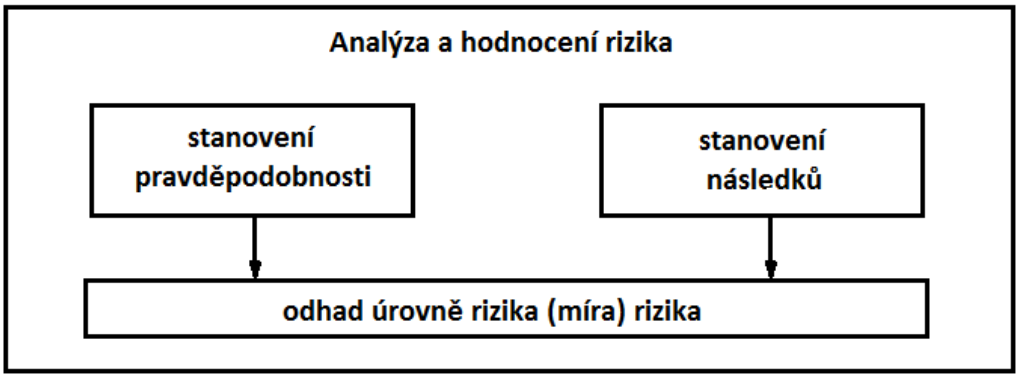
Obsahem **identifikace** rizik je zjišťování a zkoumání všech potencionálně možných rizik daného objektu. Účelem je tedy nalézt a charakterizovat všechna možná rizika, která mohou ovlivnit bezpečnost a to zejména ta, která se vztahují k požadavkům zákonů na bezpečnost. Proces identifikace bývá mnohdy nutné během procesu analýzy opakovat.

Analýzy jednotlivých identifikovaných rizik zahrnují:

- zjištění mezí a efektivních hranic rizika a jakékoliv jejich závislosti,
- odhad pravděpodobnosti výskytu a sním spojeného dopadu (následku) na odsouhlasené cíle.

Hodnocení identifikovaných rizik v rámci analýzy, viz obr. 5, bývá založeno na volbě míry rizika pro odhad úrovně rizika, tj. v kvantitativním vyjádření:

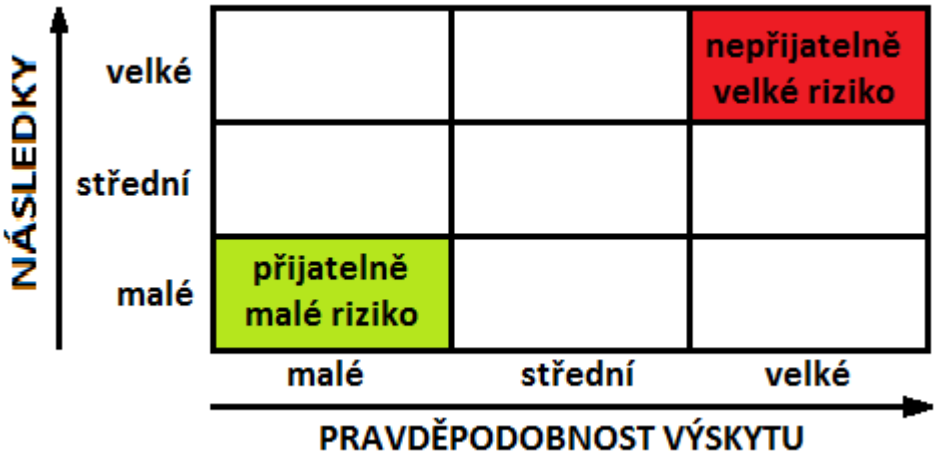
- pravděpodobnosti (četnosti) vzniku nebezpečných událostí,
- následků nebezpečných událostí.



Obr. 5: Analýza identifikovaných rizik [15]

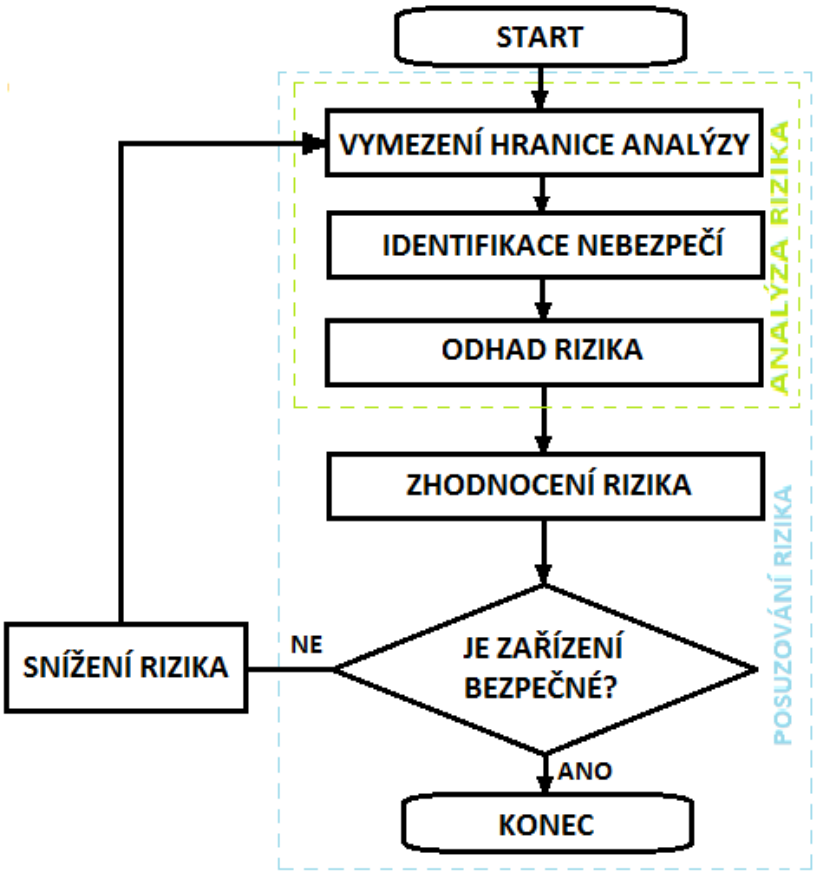
Termín **analýza rizik** se v praxi často používá pro identifikaci, vlastní analýzu a kvantitativní hodnocení. Někdy se pod tento termín zahrnuje i posuzování rizik.

Posuzování rizika začíná tedy jeho analýzou, při které se prošetřuje pravděpodobnost (četnost) výskytu, závažnost následků, možnost vyvarování se rizika a doba trvání rizika (expozice). Pro znázornění rizik se často používá grafická metoda znázornění např. v podobě matic (obr. 6) [20].



Obr. 6: Matice rizika [20]

Cyklus posuzování rizika se neustále opakuje, až do dosažení předepsané úrovně bezpečnosti, a je naznačen na obr. 7 [3].



Obr. 7: Posouzení rizika [3]

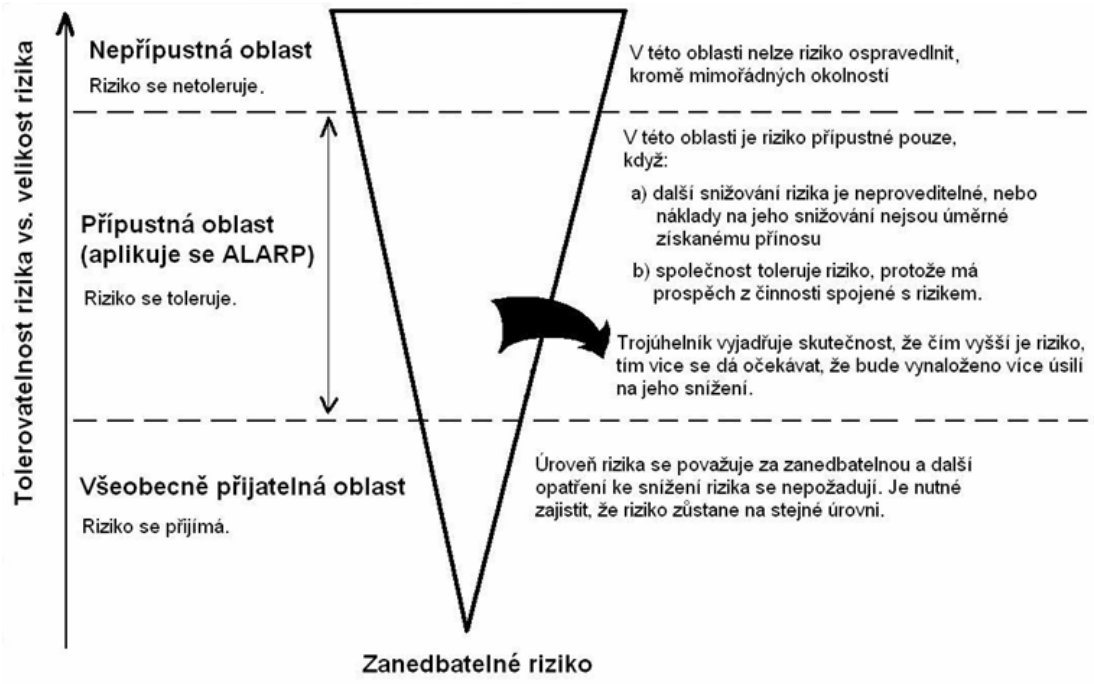
Management rizik tak prokazatelně hraje významnou roli v posuzování přijatelnosti rizik a tedy zajišťování požadované úrovně bezpečnosti technických zařízení.

1.4 Přijatelnost rizika

Exaktní hodnoty přijatelnosti rizika nám technické normy explicitním způsobem neuvádějí. Ovšem s implicitním vyjádřením se můžeme setkat v technických normách [5, 6, 7, 8, 9,] a to prostřednictvím úrovně integrity bezpečnosti, korespondující s oceněním rizika a představující požadovanou míru snížení rizika. Z rozhodovacích pravidel pro ocenění rizika a přiřazení SIL (Safety Integrity Level) lze obecně dedukovat, jaké následky s jakou pravděpodobností se považují za nepřijatelné riziko.

Mezi nejvýznamnější zásady užívané jako „pomůcky“ pro určení přijatelnosti rizika patři zásada ALARP.

Zásada ALARP (Velká Británie) – Tento „zákon“ vznikl ve Velké Británii a vyžaduje, aby bylo riziko omezeno na rozumně dosažitelnou úroveň. Britský úřad pro zdraví a bezpečnost (Health and Safety Executive – HSE) zavedl v této souvislosti princip ALARP (As Low As Reasonably Practicible). Záměrem je, aby byla brána v úvahu i ekonomická stránka věci, tj. náklady spojené s nutným zmenšením rizika. Současně ukládá projektantovi povinnost určit zbytkové riziko a to i s důkazem, že již není možné rozumným způsobem to zbytkové riziko dále zmenšit. Princip této metody je znázorněn na následujícím obrázku (obr. 8).



Obr. 8: Princip metody ALARP [5]

1.5 Funkční bezpečnost

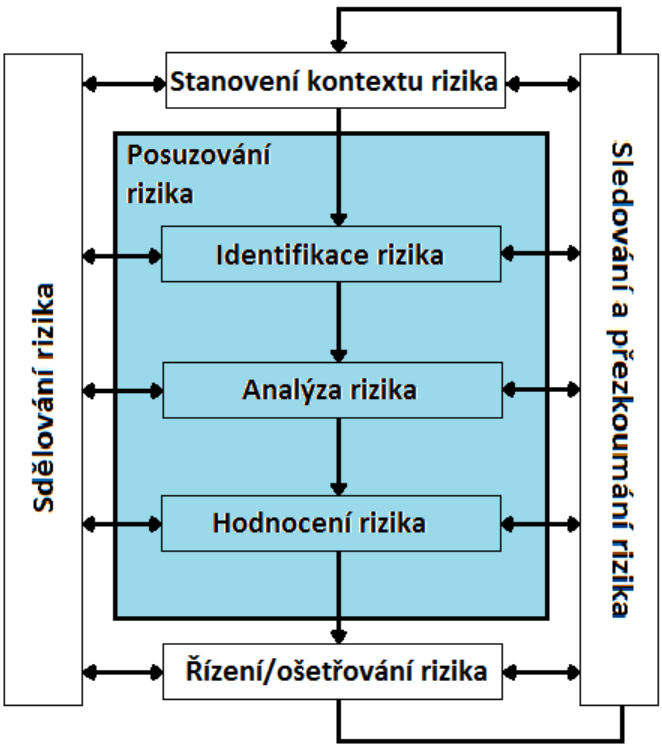
Pojem funkční bezpečnost byl poprvé představen v roce 1998 v normě IEC 61508. Je součástí celkové bezpečnosti systému. Celkovou bezpečnost systému nebo zařízení můžeme rozdělit do třech základních částí. První část – přímá bezpečnost se zabývá takovými riziky, jako jsou např. elektrické šoky a spáleniny bezprostředně zapříčiněné hardwarem. Druhou částí je funkční bezpečnost, která zahrnuje bezpečnost řízeného zařízení (EUC – viz dále). Úroveň funkční bezpečnosti závisí na opatřeních zavedených s cílem zmenšit riziko, a tudíž záleží i na správné činnosti těchto opatření. Třetí částí celkové bezpečnosti systému (zařízení) je tzv. nepřímá bezpečnost, která zahrnuje nepřímé důsledky nesprávné činnosti systému, jako např. poskytování nesprávných údajů apod. [20]. Funkční bezpečnost tedy zahrnuje identifikovatelné poruchy, které mají za následek vážné důsledky (např. úmrtí) a určení maximální přijatelné četnosti pro každý režim poruchy. Zařízení, jehož porucha přispívá ke každému z těchto rizik je označováno jako „safety related“ (související s bezpečností) [20]. Příkladem jsou systémy řízení průmyslových procesů, systémy nouzového vypnutí procesů, železniční signalizační zařízení, zařízení v automobilovém průmyslu, lékařské vybavení, jaderné elektrárny apod.

Za základní normy funkční bezpečnosti lze považovat normy ČSN EN 61508 [5] a ČSN 61511 [6]. Tyto normy bývají označovány jako normy zastřešující. Jejich principy pak přebírají normy z různých průmyslových odvětví se vztahem k funkční bezpečnosti, jako jsou např. normy ČSN EN 62061 [7], ČSN EN ISO 13849 [8], ČSN EN 50126 [9] a ISO 26262 [14].

1.5.1 Základní filozofie funkční bezpečnosti

Důvodem, proč byly normativně popsány procesy a postupy aplikace funkční

bezpečnosti, bylo řízení rizika na úroveň, která je společností přijatelná. Důsledky poruch mohou být různého charakteru – čistě ekonomického, environmentálního nebo bezpečnostního (vliv na zdraví a životy osob). Vše níže uvedené, a tedy to, co řeší postupy funkční bezpečnosti, se týká posledního typu následků – bezpečnosti osob. Funkční bezpečnost je v souladu se schématem managementu rizika na následujícím obr. 9.



Obr. 9: Management rizika [24]

Analýza a hodnocení rizika probíhají v jednom kroku pomocí diagramů, matic, nebo semikvantitativních výpočtů, uvedených přímo v normativních dokumentech (respektive v jejich informativních přílohách). Zjednodušeně řečeno, na základě určení pravděpodobnosti a následku nežádoucí události je přiřazena úroveň bezpečnostního systému tak, aby po jeho realizaci byla míra rizika přijatelná.

1.5.2 Základní pojmy funkční bezpečnosti

Níže budou uvedeny základní pojmy oboru funkční bezpečnosti dle normy ČSN EN 61508 [5], tato norma je prakticky norma zastřešující a vybrané základní 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.
- **Programovatelný elektronický systém** (Programmable Electronic System – PES) – 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
- **Elektrický/elektronický/programovatelný elektronický systém** (Electrical/Electronic/Programmable Electronic System – E/E/PE systém, E/E/PES) totéž jako PES systém

Bezpečnost a riziko

- **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 újmy
- **Nebezpečná situace** (hazardous situation) – okolnosti, za nichž je osoba vystavena nebezpečí
- **Nebezpečná událost** (hazardous event) – nebezpečná situace, jejímž výsledkem je poškození nebo újma
- **Bezpečnost** (safety) – odstranění nepřijatelného rizika
- **Funkční bezpečnost** (functional safety) – část celkové bezpečnosti týkající se EUC a systému řízení EUC závislá na správném fungování E/E/PE systému souvisejících s bezpečností, na systémech souvisejících s bezpečností založených na jiných technických principech a vnějších prostředcích pro snížení rizika
- **Bezpečnostní funkce** (safety function) – funkce, která má být realizována E/E/PE systémem souvisejícím s bezpečností, systémem souvisejícím s bezpečností založeným na jiných technických principech nebo vnějšími prostředky pro snížení rizika a která je určena pro zajištění nebo udržení bezpečného stavu EUC z hlediska konkrétní nebezpečné události
- **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

Integrita bezpečnosti

- **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 PES 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

Požadavky na bezpečnost

- **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

1.5.3 Životní cyklus funkční bezpečnosti

Z důvodů systematického zajišťování všech činností nutných pro dosažení požadované úrovně integrity bezpečnosti u systému E/E/PE souvisejících s bezpečností se v této normě zavádí, jako určitý technický rámec, životní cyklus celkové bezpečnosti.

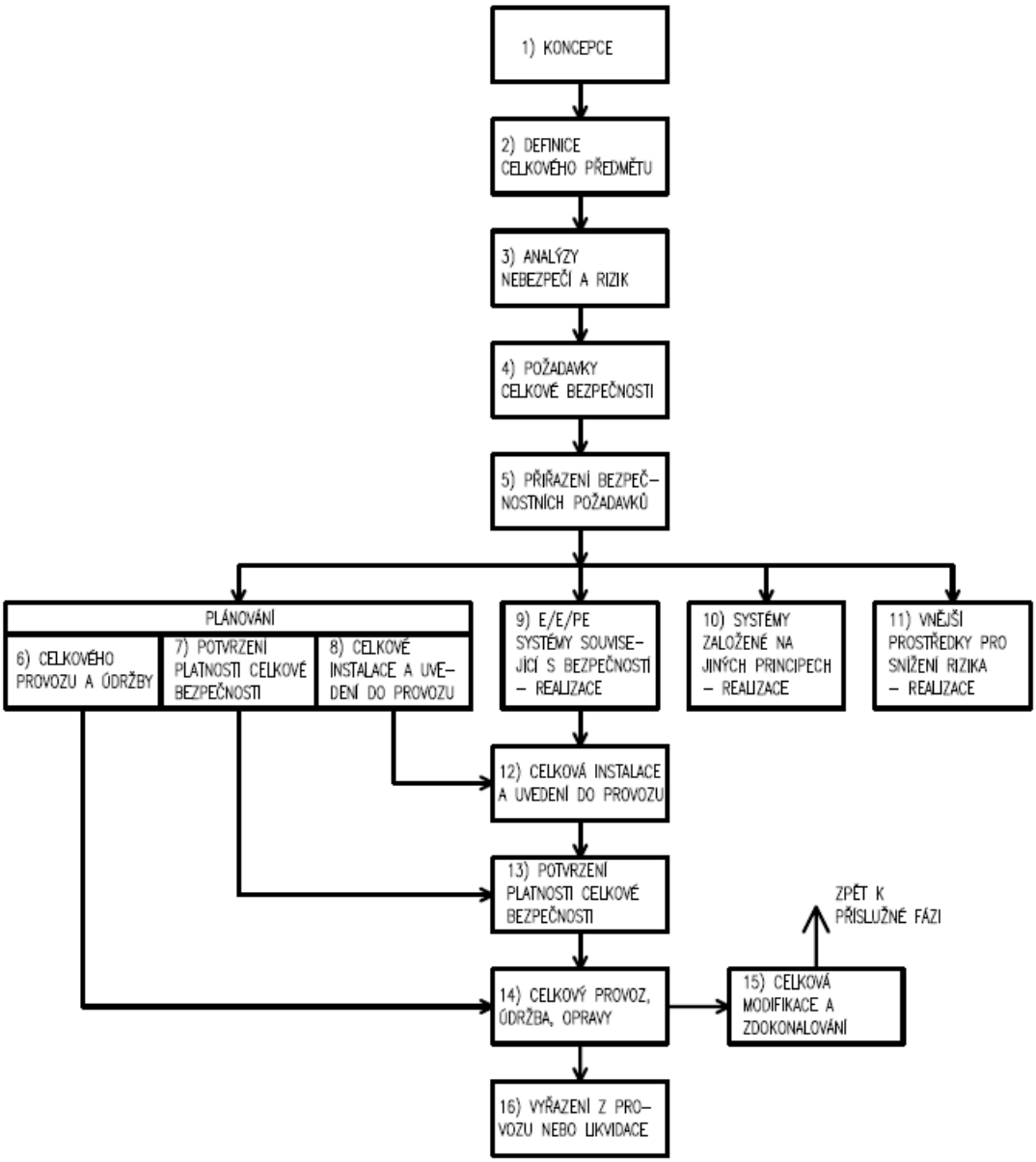
Životní cyklus celkové bezpečnosti zahrnuje tato patření pro snížení rizika:

- systémy E/E/EP související s bezpečností
- jiná opatření pro snížení rizika

Současně životní cyklus také představuje strukturu, na které je norma založena. Technické požadavky se tedy stanovují v pořadí určeném jednotlivými fázemi celkového životního cyklu bezpečnosti systému.

Základem konceptu celkového životního cyklu bezpečnosti je pojetí funkční bezpečnosti jako nezávislé na spolehlivosti. Odmítá názor, že „provozně spolehlivý“ znamená také „funkčně bezpečný“. Formulováním samostatných požadavků na bezpečnost umožňuje posoudit bezpečnost nezávisle na funkčních schopnostech a poskytuje větší důvěru v bezpečnost za normálního i poruchového stavu EUC či jeho řídicího systému. Paradoxem ovšem je, že bezpečnostní aktivity nelze vytrhnout z celkového kontextu, ale je třeba je posuzovat v souvislosti s ostatními částmi technologického zařízení, a to v celém jeho životním cyklu.

Struktura celkového životního cyklu funkční bezpečnosti je zobrazena na následujícím obrázku (obr. 10), popis jednotlivých bloků životního cyklu znázorněných v obr. 10 je v tab. 2.



Obr. 10: Životní cyklus bezpečnosti [5]

Tab. 2: Životní cyklus celkové bezpečnosti [5]

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 přednosti	Vymezit hranice EUC a systém řízení EUC. Stanovit předmět analýzy nebezpečí a rizik.
3	**Analýzy nebezpečí a rizik**	Předmět bude záviset na fázi dosažené v životních cyklech celkové bezpečnosti E/E/PES a bezpečnosti softwaru (neboť může být nutné provedení více než jedné analýzy nebezpečí a rizik). U předběžné úvodní analýzy rizik a nebezpečí bude předmět zahrnovat EUC, systém řízení EUC a lidské faktory.	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, systémy souvisejících s bezpečností založené na jiných technických principech a vnější prostředky pro snížení rizika za účelem dosažená požadované funkční bezpečnosti.
5	**Přiřazení bezpečnostních požadavků**	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 celkového 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
7	**Plánování potvrzení platnosti celkové 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.

Fáze životního cyklu		Předmět	Cíl
Označení v obr.	**Název fáze**		
8	**Plánování celkové 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.
9	**E/E/PE systémy související s bezpečností: realizace**	E/E/PE systémy související s bezpečností.	Postavit E/E/PE systémy související s bezpečností splňující specifikaci bezpečnostní požadavků na E/E/PES.
10	**Systémy související s bezpečností založené na jiných technických principech.**	Systémy související s bezpečností založené na jiných technických principech.	Postavit systémy související s bezpečností založené na jiných technických principech splňující požadavky na bezpečnostní funkce a požadavky na integritu bezpečnosti pro takové systémy stanovené.
11	**Vnější prostředky pro snížení rizika**	Vnější prostředky pro snížení rizika.	Postavit vnější prostředky pro snížení rizika splňující požadavky na bezpečnostní funkce a požadavky na integritu bezpečnosti pro takové prostředky stanovené
12	**Celková instalace a uvedení do provozu**	EUC a 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 a systém řízení EUC. E/E/PE systémy související s bezpečností.	Potvrzení 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 a 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 zdokonalování**	EUC a systém řízení EUC. E/E/PE systémy související s bezpečností.	Zajistit přijatelnou funkční bezpečnost E/E/PE systémů souvisejících s bezpečností jak během, tak po uskutečnění fáze modifikací.
16	**Vyřazení z provozu nebo likvidace**	EUC a 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.

1.5.4 SIL (Safety Integrity Level)

Bezpečnostní kategorie

Důležitým krokem je definice bezpečnostních kategorií v procesu standardizace z hlediska rizika ohrožení osob, životního prostředí a okolí a stanovení zavazujících

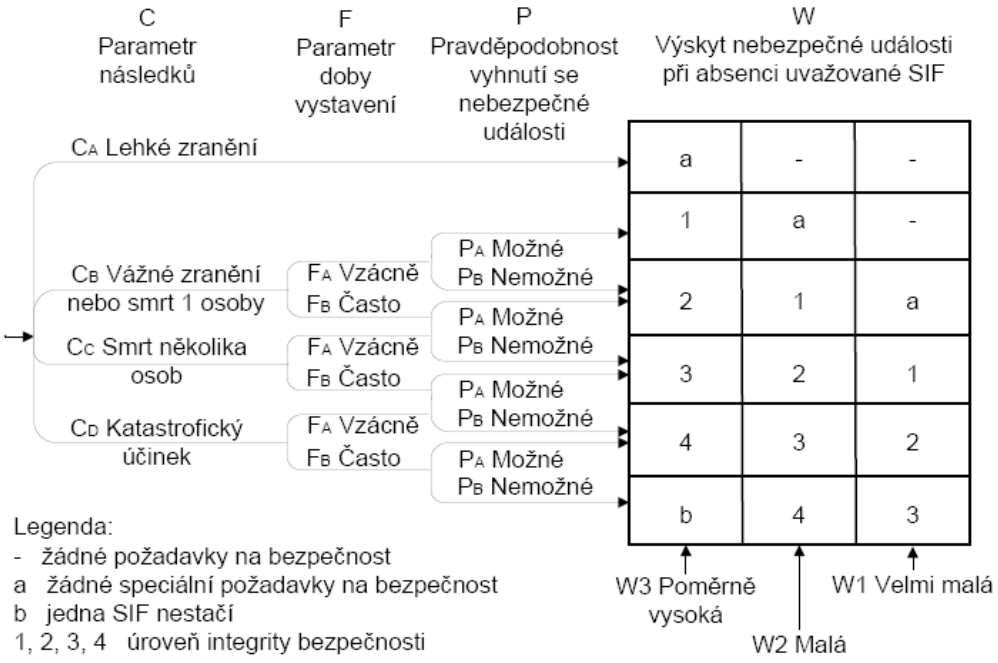
postupů k dosažení bezpečné funkce systémů a zařízení v definovaných kategoriích.

Pro vytvoření bezpečnostních funkcí, která ztělesňují hlavní principy normy, je nutné identifikovat a analyzovat všechna rizika spojená s řízením procesu nebo stroje (EUC), pro všechna identifikovaná rizika určit jejich přípustnou úroveň rizika, pro každé nepřípustné riziko určit jeho potřebné zmenšení a stanovit pro zmenšení rizika požadavky na bezpečnost včetně jejich úrovně integrity bezpečnosti (SIL).

Stanovení úrovně SIL

Ke stanovení úrovně (Safety integrity Level) se využívá rozhodovacího diagramu který, je součástí této normy. Norma definuje kvantitativní požadavky na ochranné systémy vůči náhodným poruchám a definuje čtyři úrovně SIL 1 až SIL 4 (systematické chyby nejsou kvantifikovatelné).

Norma ČSN EN 61508 [5] definuje pravděpodobnost výskytu nebezpečné události, přičemž bezpečnostní funkce selže (selžou). Jak často tato nebezpečná událost nastane, je dáno součinem požadavků na řešení havarijní situace a úrovně SIL.



Obr. 11: Schéma určení úrovně SIL dle ČSN EN 61508 [5]

Integrita bezpečnosti tedy definuje schopnost systému plnit požadované bezpečnostní funkce, přičemž čím je vyšší, tím nižší je pravděpodobnost, že systém při provádění bezpečnostních funkcí selže. Míra rizika je předem kvantifikována a určuje rozsah škod na zdraví osob čin na okolním prostředí.

Úroveň SIL lze tedy přibližně určit z výše uvedeného schématu (např. za pomoci bezpečnostního, konstrukčního a servisního technika daného testovaného zařízení (stroje). Ze stanovené úrovně SIL lze poté dle následujících tabulek (tab. 3 a tab. 4) určit interval četnosti (pravděpodobnosti) nebezpečných poruch.

Tab. 3: Vztah SIL a pravděpodobnosti výskytu nebezpečné poruchy za hodinu provozu jeho chodu u systémů s trvalou činností (kategorie „s vysokým, popř. trvalým vyžádáním“ dle ČSN EN 61508) [5]

SIL	Pravděpodobnost výskytu poruchy za hodinu provozu (PFH)
4	$\geq 10^{-9}$ až $< 10^{-8}$
3	$\geq 10^{-8}$ až $< 10^{-7}$
2	$\geq 10^{-7}$ až $< 10^{-6}$
1	$\geq 10^{-6}$ až $< 10^{-5}$

Tab. 4: Vztah SIL a pravděpodobnosti výskytu nebezpečné poruchy u systému činných na vyžádání (kategorie „ s nízkým vyžádáním“ dle ČSN EN 61508) [5]

SIL	Střední pravděpodobnost výskytu nebezpečné poruchy při vyžádání funkce (PFD)
4	$\geq 10^{-5}$ až $< 10^{-4}$
3	$\geq 10^{-4}$ až $< 10^{-3}$
2	$\geq 10^{-3}$ až $< 10^{-2}$
1	$\geq 10^{-2}$ až $< 10^{-1}$

Norma tedy jak je možné vidět z výše uvedených tabulek, dělí E/E/PE systémy na dva základní typy dle vyžádání:

- *Systémy provozu s velkým nebo trvalým vyžádáním* – jsou to systémy, kde bezpečnostní funkce je jedinou ochranou, pravděpodobnost poruchy je určena hodnotu PFH. Dle normy ČSN EN 61508 [5] je tento systém definován frekvencí požadavků na SIF a to častěji než jedenkrát za rok.
- *Systémy provozu s malým vyžádáním* – jsou to systémy, kde bezpečnostní funkci předchází zásah jiného systému, pravděpodobnost poruchy je určena hodnotou PFD. Příkladem z běžného života by mohl být např. airbag v osobním autě, požární hlásič v domě apod.)

1.5.5 Srovnání přístupů k funkční bezpečnosti dle vybraných norem

Níže budou porovnány přístupy dle norem ČSN EN 61508 [5], ČSN EN 62061 [7] a ČSN ISO 13849 [8]. Tyto přístupy byly podrobně popsány v mé semestrální práci na téma „Funkční bezpečnost a její aplikace v průmyslu [23]. Tyto uvedené postupy jsou v příslušných normách [5], [7], [8] popsány v informativních přílohách – tyto přílohy jsou nezávazné. V těchto postupech je již implicitně předdefinována přijatelná úroveň rizika (riziko je skryto v příslušných postupech pro určení SIL či PL).

Pro porovnání těchto přístupů byly použity tabulky 5 – 7. Tab. 5 dělí postupy dle typu hodnotících stupnic, způsobu stanovení SIL (PL), dle toho, jakým způsobem jsou úrovně požadované funkční bezpečnosti vůbec značeny, počtu hodnocených kritérií a počtu hodnotících stupnic.

Tab. 5: Způsoby dosažení požadované funkční bezpečnosti [25]

	Typ stupnic	**Způsob stanovení SIL (PL)**	**Označení požadavku**	**Počet hodnotících kritérii**	**Počet úrovní hodnotících stupnic**
ČSN EN 61508	Kvalitativní ordinální	Rozhodovací diagram	- a SIL1 SIL2 SIL3 SIL4 b	4	2 až 4
ČSN EN 62061	Sem kvalitativní	Kombinace sem kvantitativního výpočtu a matice	SIL1 SIL2 SIL3	4	3 až 5
ISO 13849	Kvalitativní ordinální	Rozhodovací diagram	a b c d e	3	2

Tab. 6: Porovnání značení funkční bezpečnosti a jejich kvantitativní význam [25]

		ČSN EN 61508	**ČSN EN 62061**	**ISO 13849**
Požadavek na průměrnou frekvenci nebezpečné poruchy bezpečnostní funkce [h^{-1}]	**žádné bezpečnostní požadavky**	**-**		
	žádné speciální bezpečnostní požadavky	**a**		
	> $1E^{-5}$ až < $1E^{-4}$			**a**
	> $3E^{-6}$ až < $1E^{-5}$	**SIL 1**	**SIL 1**	**b**
	> $1E^{-6}$ až < $3E^{-6}$			**c**
	> $1E^{-7}$ až < $1E^{-6}$	**SIL 2**	**SIL 2**	**d**
	> $1E^{-8}$ až < $1E^{-7}$	**SIL 3**	**SIL 3**	**e**
	> $1E^{-9}$ až < $1E^{-8}$	**SIL 4**		
	jediný bezpečnostní systém není dostatečný	**b**		

Tab. 7: Značení jednotlivých faktorů rizika [25]

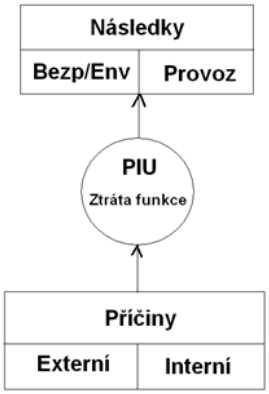
	Parametry pravděpodobnosti			Parametr následků	
	Výskyt	Vystavení	Vyhnutí	Počet osob	Stupeň zranění
ČSN EN 61508	W	F	P	C	
ČSN EN 62061	Pr	Fr	Av		Se
ISO 13849		F	P		S

Z porovnání uvedeného v těchto tabulkách je evidentní, že se jednotlivé normy snaží dosáhnout stejného cíle různým způsobem. Ovšem ani jeden z těchto postupů není plně kvantitativního charakteru → není tedy možná jej podrobit ověření – validaci. Je zřejmé, že různé metody povedou při posuzování stejné události k různým výsledkům a tedy se budou lišit i ve specifických požadavcích na funkční bezpečnost [24].

1.5.6 Základní postup pro stanovení funkční bezpečnosti v automatizační a měřicí technice

Aby bylo možné stanovit obecný postup pro stanovení funkční bezpečnosti v automatizační měřicí technice, je třeba ještě vysvětlit pojem PIU a jeho vztah k funkční bezpečnosti.

Základem je fakt, že nositelem rizika je nežádoucí událost, která má pravděpodobnost výskytu (danou zpravidla roční četností) a následky (obr. 12). Taková událost se nazývá postulovanou iniciační událostí (**PIU**).



Obr. 12: Základní schéma PIU

Nyní můžeme obecný postup stanovení funkční bezpečnosti shrnout do následujících 11 kroků:

KROK 1:

- Provede se vhodná analýza/y zkoumaného technického systému (FMEA, ETA, MARKOVOVA ANALÝZA apod.). Na základě této analýzy jsou poté určeny

PIU. Ty, když nastanou, vedou k možným následkům na zdraví a životech osob, ztrátě funkčních vlastností a životní prostředí (environment).

KROK 2:

- PIU jsou stanoveny pro základním způsobem řízený a ovládaný objekt (technický systém) označovaný dle výše uvedených norem [5 - 9] jako EUC (Equipment Under Control).

KROK 3:

- Pro takto definované PIU se následně odhadnou jejich pravděpodobnosti/ četnosti a následky.

KROK 4:

- Pro každou PIU je nutné stanovit (jako kombinaci pravděpodobnosti/četnosti a následků) zda je tolerovatelné či netolerovatelné (přijatelné nebo nepřijatelné).

KROK 5:

- Specifikují se bezpečnostní funkce, které snižují pravděpodobnost výskytu PIU na EUC či alespoň omezují následky PIU, u kterých byla stanovena nepřípustnost tohoto rizika.

KROK 6:

- Určí se, jaká má být hodnota intenzity nebezpečných poruch, resp. nepohotovosti bezpečnostní funkce, aby se hodnota rizika PIU na EUC snížila na přijatelnou úroveň.

KROK 7:

- Dle požadované hodnoty intenzity poruch, resp. nepohotovosti bezpečnostní funkce se této funkci přiřadí úroveň integrity bezpečnosti SIL (1, 2, 3, 4) či PL (a, b, c, d, e).

KROK 8:

- Alternativou může být, stanovení požadované úrovně SIL (1, 2, 3, 4) či PL (a, b, c, d, e) bezpečnostní funkce konzervativně jen z následků PIU z matice rizika, ve které jsou známy hodnoty následků PIU a neznámé pravděpodobnosti/četnosti PIU. Pak k takto odvozené úrovni SIL (1, 2, 3, 4) či PL (a, b, c, d, e) bezpečnostní funkce se přiřadí hodnoty intenzity nebezpečných poruch, resp. nepohotovosti z krajní přísnější hodnoty rozmezí pásma, které je pro danou úroveň SIL v normě uváděno.

KROK 9:

- Provede se návrh (design), jakým způsobem bude bezpečnostní funkce realizována, která zařízení (položky, komponenty) a v jaké konfiguraci (sériové zapojení, paralelní, zálohování, …) se použijí. Je nezbytné zde provést analýzu spolehlivosti, protože se právě zde rozhoduje, zda se použije zálohování a pak tedy postačí zařízení (komponenty) s nižšími parametry spolehlivosti (intenzita nebezpečných poruch, resp. nepohotovost) nebo zapojení bude sériové a nutně bude zapotřebí vysoké úrovně parametrů spolehlivosti zařízení.

KROK 10:

- Podle hodnoty intenzity nebezpečných poruch, resp. nepohotovosti zařízení (položek, komponent) stanovených v kroku 7 (alternativně v kroku 8) se stanoví úroveň SIL (1, 2, 3, 4) či PL (a, b, c, d, e) odvozené od požadované hodnoty intenzity nebezpečných poruch, resp. nepohotovosti bezpečnostní funkce. Zde se právě na základě volby uvedené v bodě 9 rozhoduje o úrovni SIL (1, 2, 3, 4) pro jednotlivá technická zařízení (položky, komponenty). Podle požadovaných hodnot se vyskytnou případy, kdy úroveň SIL (1, 2, 3, 4) či PL (a, b, c, d, e)) bude shodná, nižší nebo vyšší než úroveň SIL (1, 2, 3, 4) či PL (a, b, c, d, e)) bezpečnostní funkce.

KROK 11:

- Provede se soupis veškerých zařízení (komponent), které bezpečnostní funkci realizují a s přiřazenou úrovní SIL (1, 2, 3, 4) či PL (a, b, c, d, e) a požadovanými hodnotami intenzity nebezpečných poruch, resp. nepohotovosti.

Při nerespektovaní výše uvedených kroků, není proveden optimální návrh technického systému (zařízení, stroje), nejsou správně zadány požadavky na úroveň SIL či PL pro dodavatele Zařízení (komponent, položek) technického systému (zařízení, stroje) a nedaří se prokázat bezpečnost toho technického systému (zařízení, stroje).

2 SPOLEHLIVOST A SPOLEHLIVOSTNÍ UKAZATELE

Problematiku spolehlivosti můžeme odvodit od požadavku na správnou a je-li to možné i bezporuchovou funkci technického zařízení. Spolehlivost lze definovat jako souhrnný termín popisující vlastnosti objektu. V širším pojetí lze spolehlivost chápat jako komplexní vlastnost, která vyjadřuje schopnost objektu zachovávat požadované funkce v čase a to za stanovených provozních podmínek. Pod pojmem objektu pak rozumíme např. funkční přístroj, součást zařízení či celkový technický systém [2], [16].

Norma ČSN EN ISO 9001:2001 pak definuje spolehlivost jako pohotovost, která zahrnuje činitele, které ji ovlivňují, jako např. bezpečnost, bezporuchovost či udržovatelnost. Aby bylo možné spolehlivosti lépe porozumět, je třeba definovat základní pojmy spolehlivosti.

Norma ČSN IEC 50(191) [10] definuje spolehlivost jako: Obecná vlastnost objektu spočívající ve schopnosti plnit požadované funkce při zachování hodnot stanovených provozních ukazatelů v daných mezích a v čase dle stanovených pracovních podmínek.

2.1 Základní pojmy spolehlivosti

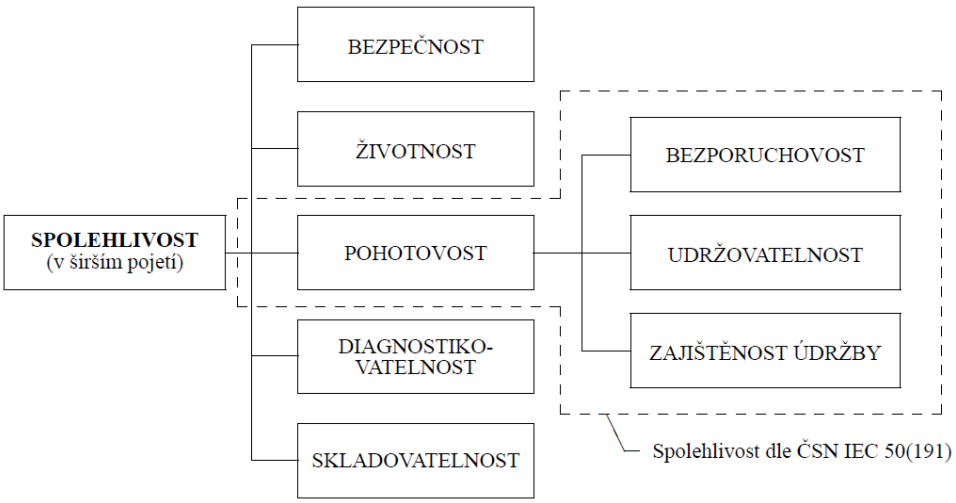
Pro porozumění spolehlivosti a jejímu studiu lze dále definovat řadu základních pojmů. V této kapitole budou vysvětleny základní pojmy dle mého výběru.

- **Objekt** (Object/Item) – objekt je obecný pojem, za nějž je možné dosadit libovolně velký celek (funkční blok, technický systém, součást technického zařízení apod.)
- **Systém** (System) – Pod pojmem systém pak uvažujeme celek tvořený jedním až

n objekty.

- **Poruchový stav** (Fault) – Je to stav objektu, který charakterizuje neschopnost objektu plnit požadovanou funkci. Výjimkou je neschopnost při preventivní údržbě nebo jiných plánovaných činnostech.
- **Porucha** (Failure) – ukončení schopnosti objektu plnit požadovanou funkci. Objekt po poruše je v poruchovém stavu. „Porucha“ je jev, na rozdíl od zmiňovaného „poruchového stavu“ který je stav. Takto definovaný pojem se nevztahuje na objekty, které se skládají jen ze softwaru.
- **Chyba** (Error) – Chyba je definována jako rozdíl mezi správnou a skutečnou hodnotou veličiny zjištěné např. měřením. Chyba je vždy důsledkem poruchy, ale porucha se ne vždy musí projevit chybou.
- **Životnost** (Durability) – je schopnost objektu plnit požadovanou funkci v daných podmínkách používání a údržby do dosažení mezního stavu. Mezní stav objektu lze pak charakterizovat ukončením užitečného života objektu.
- **Bezporuchovost** (Reliability) – schopnost objektu plnit požadovanou funkci v daných podmínkách a v daném časovém intervalu. Obecně se předpokládá, že na začátku časového intervalu je objekt ve stavu schopném plnit požadovanou funkci.
- **Udržovatelnost** (Maintainability) – schopnost objektu v daných podmínkách používaní setrvat ve stavu nebo se vrátit do stavu, v kterém může zcela plnit požadovanou funkci, pokud dochází k údržbě v daných podmínkách a pokud se užívají stanovené postupy a prostředky.
- **Obnova** (Restoration) – jev, kdy objekt po poruchovém stavu opět získává schopnost zcela plnit požadované funkce.

Na obr. 13 je znázorněna spolehlivost v jejím užším a širším pojetí.



Obr. 13: Širší a užší vymezení spolehlivosti [22]

Spolehlivost se nedá sama o sobě číselně vyjádřit, nelze ji jednoduše kvantifikovat, jelikož se jedná o velmi komplexní vlastnost. Proto se spolehlivost vyjadřuje za pomoci spolehlivostních ukazatelů a to za využití matematické pravděpodobnosti a statistiky. Dále je nutné při popisu spolehlivosti rozlišovat dva typy objektů – opravované (obnovované) a neopravované (neobnovované) objekty. Přičemž obnova je chápána jako vlastní přechod objektu z poruchového stavu do bezporuchového stavu a to

činností označovanou jako oprava. Mezi neobnovované objekty patří objekty, jejichž oprava je nemožná či nerentabilní. Typickým příkladem neobnovovaného objektu může být např. obyčejná žárovka. U neobnovovaných se sledují tři základní vlastnosti a to: životnost, bezporuchovost a udržovatelnost. Ukazatele spolehlivosti můžeme popsat jak teoretickými, tak empirickými charakteristikami, přičemž teoretické charakteristiky vychází z matematické pravděpodobnosti a empirické pak z bodového hodnocení statisticky oprávněného výběru. V teorii spolehlivosti je pak nejsledovanější veličinou *t*, což je časový interval od zavedení do provozu až do poruchy objektu [18].

2.2 Ukazatele spolehlivosti neobnovovaných objektů

Pravděpodobnost poruchy *Q(t)* – pravděpodobnost, že v čase $\tau \leq t$ dojde k poruše objektu. Je-li čas měřený od uvedení objektu do provozu, pravděpodobnost poruchy objektu v čase t je možné popsat distribuční funkcí:

$$Q(t) = P(\tau \leq t) = \int_0^t f(t)dt \tag{2.1}$$

Kde: *f(t)* je hustota pravděpodobnosti poruchy.

Pravděpodobnost poruchy *Q(t)* je možné vypočítat pomocí empirického vztahu

$$Q(t) = \frac{N_p}{N_0} \tag{2.2}$$

Kde: N_p je počet výrobků porušených za sledovaný interval 0 až t,

N_0 je počet výrobků ve zkoušeném souboru.

Pravděpodobnost bezporuchového provozu *R(t)* – pravděpodobnost, že v čase $\tau \leq t$ nedojde k poruše objektu a lze ji popsat vztahem:

$$R(t) = 1 - Q(t) - P(\tau > t) = 1 - \int_0^t f(t)dt \tag{2.3}$$

Pravděpodobnost bezporuchového provozu *R(t)* lze vyčíslit dle empirického vztahu:

$$R(t) = \frac{N_b}{N_0} = 1 - \frac{N_p}{N_0} \tag{2.4}$$

Kde: N_b je počet výrobků v bezporuchovém stavu.

Hustota poruch *f(t)* – je definována jako derivace *Q(t)* podle času

$$f(t) = \frac{dQ(t)}{dt} \tag{2.5}$$

Přičemž součin *f(t)dt* udává, s jakou pravděpodobností nastane ve sledovaném objektu porucha ve velmi krátkém intervalu *dt*, následujícím za okamžikem *t*.

Intenzita porucha λ(t) – pravděpodobnost, že se objekt neporouchaný v čase *t* porouchá v malém časovém intervalu *dt*, následujícím za časem *t*. Intenzita poruch patří k nejdůležitějším spolehlivostním ukazatelům používaným v praxi, a lze ji popsat vztahem:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - Q(t)} \tag{2.6}$$

Výše uvedené ukazatele spolehlivosti spolu velmi úzce souvisejí. Z tohoto důvodu je možné uvedené vztahy dále upravovat:

$$f(t) = -\frac{dR(t)}{dt} \tag{2.7}$$

$$\lambda(t) = -\frac{dR(t)}{dt} \cdot \frac{1}{R(t)} \tag{2.8}$$

Upravíme-li tuto diferenciální rovnici, získáme rovnici:

$$-\lambda(t)dt = \frac{dR(t)}{dt} \tag{2.9}$$

Integrací pak získáme rovnici:

$$R(t) = exp\left(-\int_0^t \lambda(t)dt\right) \tag{2.10}$$

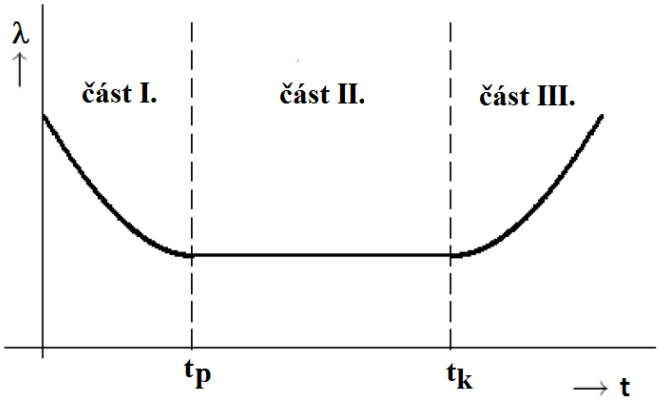
Střední doba bezporuchového provozu T_s – u neobnovovaných objektů se označuje také jako MTTF – střední doba do první poruchy (Mean Time To Failure). Je to střední hodnota provozní doby objektu, během které nenastane žádná porucha. Lze ji vypočítat následovně:

$$T_s = \int_0^\infty R(t)dt \tag{2.11}$$

Pro exponenciální průběh R(t) pak platí:

$$T_s = \int_0^\infty e^{-\lambda(t)}dt = \frac{1}{\lambda} \tag{2.12}$$

Pokud intenzitu poruch λ(t) dáme do souvislosti s časem, dostaneme časovou závislost intenzity poruch tzv. vanovou křivku, která je rozdělena do tří odlišných oblastí viz obr. 2.



Obr. 14: Vanová křivka [21]

Část I.: Oblast zahoření – Etapa časných poruch, v této části má λ(t) sestupný průběh a intenzita poruch je zde relativně vysoká. To je způsobeno především nedokonalostí výrobní technologie, vadami materiálu apod. Tento interval trvá řádově několik desítek až několik stovek hodin, avšak u složitějších systémů technické infrastruktury (např. elektráren, velkých investičních celků apod.) může tato etapa trvat až řádově několik let.

Část II.: Oblast normálního (ustáleného provozu) – tato část bývá nejdelším úsekem vanové křivky, intenzita poruch je v této části přibližně konstantní. Poruchy jsou zde způsobeny převážně náhodnými mechanismy. Můžeme tedy předpokládat, že intenzita poruch v této části nezávisí na době provozu a tedy platí následující:

$$\lambda(t) = \lambda \tag{2.13}$$

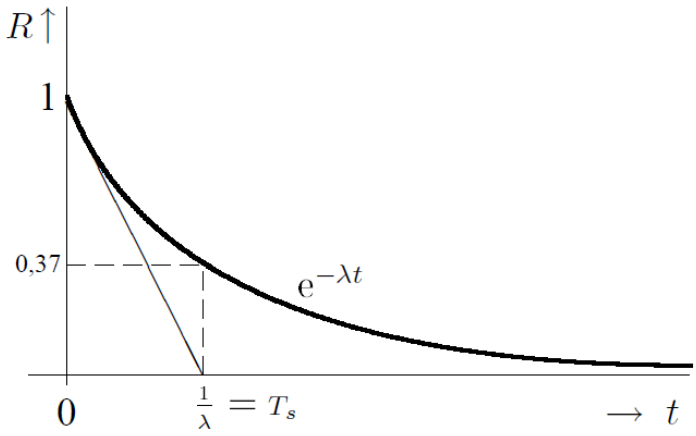
Dosazením do rovnice 2.10 pak získáme vztahy:

$$R(t) = e^{-\lambda t} \tag{2.14}$$

$$Q(t) = 1 - e^{-\lambda t} \tag{2.15}$$

$$f(t) = \lambda \cdot e^{-\lambda t} \tag{2.16}$$

Výše uvedené vztahy popisují exponenciální rozdělení dob do poruchy (obr. 3). Doba do poruchy je náhodně proměnná veličina, která může mít různé rozdělení, v praxi se nejčastěji aplikuje exponenciální rozdělení a to zejména pro elektronické systémy u kterých se neuplatňuje faktor opotřebení. Pro čas t = 0 má R(t) hodnotu 1, což koresponduje s předpokladem, že na začátku sledování je objekt v bezporuchovém stavu. Pro rostoucí t pak hodnota R(t) asymptoticky klesá k nule.



Obr. 15: Exponenciální závislost bezporuchového provozu R(t) na čase t.

Poruchy v této části vanové křivky mají převážně náhodný charakter. Tato část má trvání v délce tisíců hodin.

Část III.: Oblast stárnutí – v této části intenzita poruch postupně vzrůstá následkem stárnutí a opotřebení. V této etapě by měla následovat vyřazení či renovace objektu.

V následující tabulce (tab. 8) jsou shrnuty ukazatele spolehlivosti neopravovaných objektů.

Tab. 8: Vybrané ukazatele bezporuchovosti neobnovovaných objektů

Sledované vlastnosti	Sledované veličiny	Spolehlivostní ukazatel	Značení
Bezporuchovost	Doba provozu do poruchy	Pravděpodobnost bezporuchového provozu	R(t)
		Intenzita poruch	λ(t)
		Střední doba provozu do poruchy	MTTF,T_s
		p-kvantil doby do poruchy	t_{1p}

2.3 Ukazatele spolehlivosti obnovovaných objektů

Pro každý obnovovaný (opravovaný objekt) platí, že během svého života prochází stavy bezporuchovosti a poruchovosti. U obnovovaných objektů nelze dobu obnovy jednoduše zanedbat vzhledem k době bezporuchového provozu, a je třeba s tím počítat. Pokud jde o vliv údržby na pohotovost objektu, je třeba se zabývat jednotlivými složkami ve vztahu pro funkci pohotovosti *A(t).*

Funkce okamžité pohotovosti *A(t)* – udává pravděpodobnost, že v čase *t* bude objekt v provozuschopném stavu. Pro jednoduchost je použit vztah, ve kterém je použita konstantní intenzita poruch λ a konstantní intenzita oprav μ, a kde s rostoucím časem se pohotovost objektu blíží k ustálené (asymptotické) hodnotě $A(\infty)$.

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \cdot exp[-(\lambda + \mu) \cdot t] \tag{2.17}$$

$$A(\infty) = \frac{\mu}{\lambda + \mu} = \frac{MTBF}{MTBF + MTTR} \tag{2.18}$$

Střední doba provozu mezi poruchami *MTBF* – je stanovena jako aritmetický průměr všech naměřených dob bezporuchového provozu od ukončení opravy do výskytu následující poruchy. Tato doba ovšem nezahrnuje dobu opravy.

$$MTBF = \frac{t_p}{n} = \frac{\sum_{i=1}^{n} t_{pi}}{n} \tag{2.19}$$

Kde: t_p je kumulativní doba provozu, součet všech dob provozu za sledované období,
n je počet výpadků způsobených poruchami.

Střední doba do obnovy *MTTR* – je stanovena jako aritmetický průměr všech naměřených dob do obnovy, tedy od počátku vzniku poruchy na objektu až do uvedení objektu do provozu.

$$MTTR = \frac{t_0}{n} \tag{2.20}$$

Kde: t_0 kumulativní doba obnov,
n je počet poruch.

Funkce okamžité nepohotovosti *U(t)* – doplněk funkce okamžité pohotovosti do jedné, lze určit její ustálenou (asymptotickou) hodnotu.

$$U(t) = 1 - A(t) \tag{2.21}$$

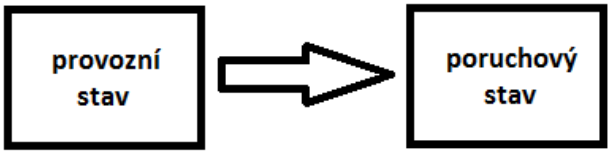
$$U(\infty) = \frac{\lambda}{\lambda + \mu} = \frac{MTTR}{MTBF + MTTR} \tag{2.22}$$

3 SPOLEHLIVOSTNÍ MODELY A ANALÝZY

Při hodnocení spolehlivosti je důležitá dobrá znalost struktury systému. Z tohoto důvodu je vždy dobré uvést, o jaký typ systému se jedná. Za základní rozdělení systému můžeme považovat rozdělení na dvoustavové a vícestavové systémy. Tyto dva systémy mohou být jak obnovované tak i neobnovované.

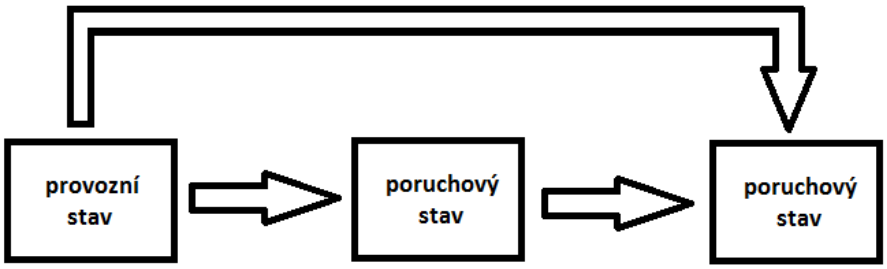
3.1 Dvoustavové a vícestavové systémy

Dvoustavové systémy jsou typické tím, že se mohou nacházet pouze ve dvou stavech a to ve stavu bezporuchovém (ve stavu provozu) anebo ve stavu poruchovém (porucha celého systému). Což znamená, že při poruše jakéhokoliv prvku systému přechází systém do poruchového stavu a nemůže tedy nadále konat svoji funkci (viz obr. 16)



Obr. 16: Schéma dvoustavového systému

Vícestavové systémy se odlišují od dvoustavových tím, že mají kromě stavu provozu a stavu poruchy i další stavy, jako je např. stav degradace nebo stav částečné poruchy. To znamená, že v případě poruchy některého z prvků může systém i nadále pracovat, avšak s omezenými funkcemi nebo v případě závažné poruchy může přejít přímo do stavu poruchy a ukončit svou funkci (viz obr. 17).



Obr. 17: Schéma vícestavového systému.

V praxi má převážná většina systémů právě takovou strukturu, avšak spolehlivostní analýzy pak vyžadují daleko větší znalost systému a bývají tím pádem značně složitější. Proto se v praxi, nejedná-li se o tzv. kritické aplikace, uvažuje pouze jednodušší varianta – dvoustavové systémy [19].

3.2 Spolehlivostní model sériového a paralelního sytému

V sériovém systému jsou prvky systému řazeny z hlediska spolehlivosti do série. Pro tento model tedy platí, že porucha jediného prvku vyvolá poruchu celého systému.

Sériový spolehlivostní model nelze ovšem chápat jako elektrické obvodové zapojení. Tento model pouze představuje fakt, jak jednotlivé prvky přispívají k poruchovosti daného systému. Na obr. 18 je znázorněn příklad sériového spolehlivostního modelu.

Pro pravděpodobnost bezporuchového provozu systému R(t) a intenzitu poruch systému λ pak platí [16], [18]:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} \exp(-\lambda_i t) = \exp(-\lambda t) \tag{3.01}$$

Kde: $R_i(t)$ je pravděpodobnost bezporuchového provozu i-tého prvku,

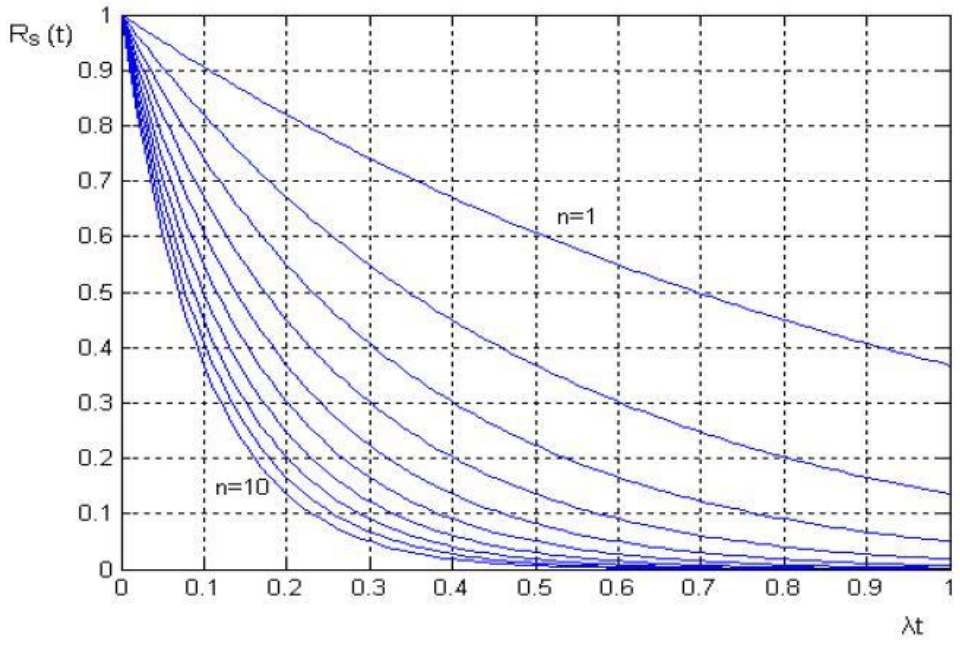
λ_i je střední intenzita poruch jednotlivých součástí [h^{-1}]

λ je intenzita poruch systému [h^{-1}]

a platí:

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{3.02}$$

Pro různé počty prvků n je závislost pravděpodobnosti bezporuchového provozu systému $R_s(t)$ s prvky se stejnou intenzitou poruch λ_i na tzv. normovaném čase λt zobrazena na obr. 18. [18].



Obr. 18: Závislost pravděpodobnosti bezporuchového provozu systému $R_s(t)$ na λt při počtu n identických prvků systému

V paralelním systému jsou prvky systému řazeny z hlediska spolehlivosti paralelně.

Pokud jsou prvky vzájemně rovnocenné z hlediska funkce, jsou také vzájemně zastupitelné. Porucha celého systému může nastat pouze v případě, kdy dojde k poruše všech ostatních prvků systému, tedy s daleko menší pravděpodobností než u modelu sériového. Na obr. 20 je znázorněn jednoduchý model paralelního systému.

Pro pravděpodobnost bezporuchového provozu paralelního systému $R_p(t)$ a jeho intenzitu poruch platí: [18]

$$R_p(t) = \prod_{i=1}^{n}(1 - R_i(t)) = 1 - \prod_{i=1}^{n}(1 - \exp(-\lambda_i t)) \qquad (3.03)$$

Kde: $R_i(t)$ je pravděpodobnost bezporuchového provozu systému i-tého prvku

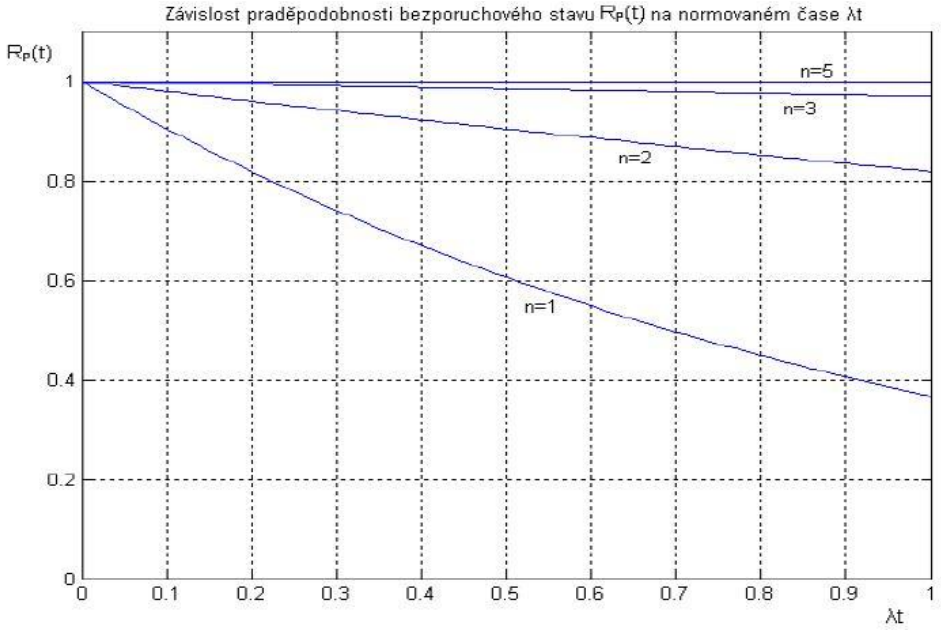
λ_i je střední intenzita poruch jednotlivých součástí [h^{-1}]

a platí:

$$\lambda = \prod_{i=1}^{n}\lambda_i \qquad (3.04)$$

Kde: λ je intenzita poruch systému [h^{-1}].

Pro různé počty prvků n je závislost pravděpodobností bezporuchového provozu systému $R_p(t)$ s prvky se stejnou intenzitou poruch λ_i na tzv. normovaném čase λt zobrazena na obr. 19 [18].



Obr. 19: Závislost pravděpodobnosti bezporuchového provozu systému $R_p(t)$ na λt při počtu n identických prvků systému

Výpočtové vztahy pro ostatní typy systémů (a jejich spolehlivostní modely) nejsou pro tuto diplomovou práci relevantní a nejsou tedy popisovány.

3.3 Spolehlivostní analýzy

Při řešení bezpečnosti technických zařízení je důležité stanovit v závislosti na právních předpisech oblasti přípustných a nepřípustných rizik. Stanovená oblast nepřípustných rizik musí být organizací v rámci jejího managementu rizik řádně ošetřena, což musí být prokázáno analýzou rizik a případně i odpovídajícími zkouškami. Obecné východisko řešení problematiky bezpečnosti objektů je stejné jako u jejich spolehlivosti. Požaduje se vyjádřit ztrátu schopnosti plnit požadované funkce. Tedy určit pravděpodobnost selhání a stanovit následky. Proto se postupy analýz spolehlivosti aplikují i v analýzách rizik.

Analýzy můžeme rozdělit na:

- kvalitativní analýzy (zahrnují analýzy funkční struktury systému a stanovení druhů poruchových stavů, mechanismů poruch, příčin, projevů a jejich následků, sestavení modelů bezpečnosti apod.),
- semikvantitavní analýzy (pro ocenění pravděpodobnosti a důsledků poruch se k ocenění používají zástupné hodnoty formou bodového hodnocení),
- kvantitativní analýzy (určují se referenční data, která se budou používat a provede se číselná vyhodnocení spolehlivosti, analýzy kritičnosti apod.).

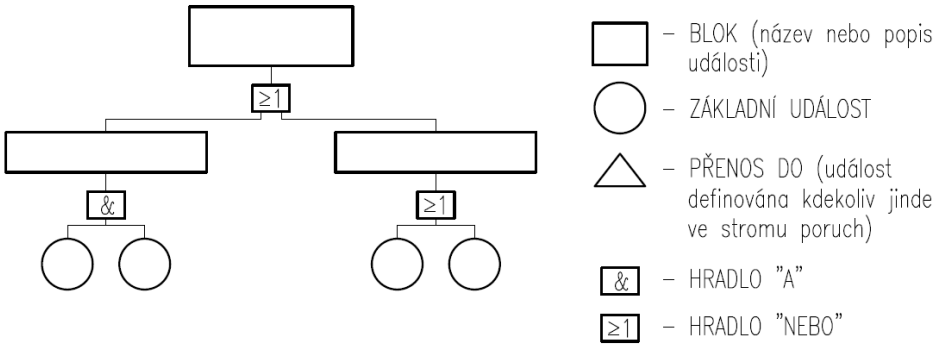
Objekty typu technických zařízení různé složitosti jsou charakterizovány jako systémy složené z různě na sebe funkčně vázaných prvků. Analýzy poruch těchto zařízení se provádějí buď **induktivně** (postup od nejjednodušších prvků analyzovaného systému směrem k nadřazeným, tedy od zdola nahoru), nebo **deduktivně** (postup od nadřazených systémů směrem k jednodušší, tedy shora dolů). Níže budou uvedeny velmi stručné popisy nejpoužívanějších metod spolehlivosti používaných v analýzách rizik.

Analýza druhů poruch a jejich důsledků – FMEA (Failure/Fault Mode and Effects Analysis), jinak také nazývána metodu možností vzniku vad a jejich následků, řadí se mezi kvalitativní metody analýzy s induktivním přístupem. Základem této metody je odhadování potenciálně možných poruch (poruchových stavů), které se mohu vyskytnout v každé části systému, a určování jejich možných důsledků na nejbližší vyšší funkční úroveň systému. Výrazně tak snižuje počet nezachycených možných poruch a to hned na nejnižší hladině analýzy.

Analýza druhů, důsledků a kritičnosti poruch – FMECA (Failure/Fault Mode, Effects and Criticality Analysis), stejně jako FMEA se řadí mezi kvalitativní metody s induktivním přístupem. Jedná se vlastně o metodu FMEA doplněnou o ohodnocení kritičnosti důsledků poruch. Avšak po doplnění o bodové či procentuální hodnocení jednotlivých faktorů přispívajících ke kritičnosti představuje typickou semikvantitativní metodu analýzy spolehlivosti. Je založena na studii vzniku možných poruch (poruchových stavů) a jejich účinků na systém s uvážením pravděpodobnosti jejich výskytu a závažnosti jejich důsledků (závažnost důsledků je posuzována podle specifické stupnice).

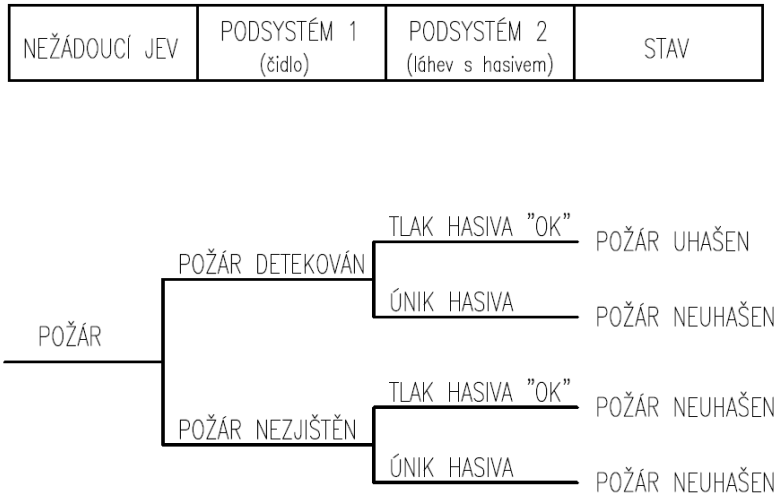
Analýza stromu poruch – FTA (Failure/Fault Tree Analysis) – jedná se také o kvalitativní analýzu, ale na rozdíl od FMEA/FMECA, s deduktivním přístupem. Jejím východiskem je jedna tzv. vrcholová událost systému (např. kritická porucha/poruchový stav), pro kterou se hledají příčiny v nižších funkčních prvcích. Takto se postupuje k nejnižším úrovním, až se nalezne možná příčina, obvykle porucha součástky. Výsledky analýzy se zobrazují jako strom poruch (obr. 20), který pak může být

základem kvantitativní analýzy. FTA analýza je vhodná pro systémy i s několika tisíci prvky, umožňuje zpracovávat i zálohované struktury, částečně i kombinace a závislost událostí, ale neumožňuje zpracovávat komplexní strategii údržby.



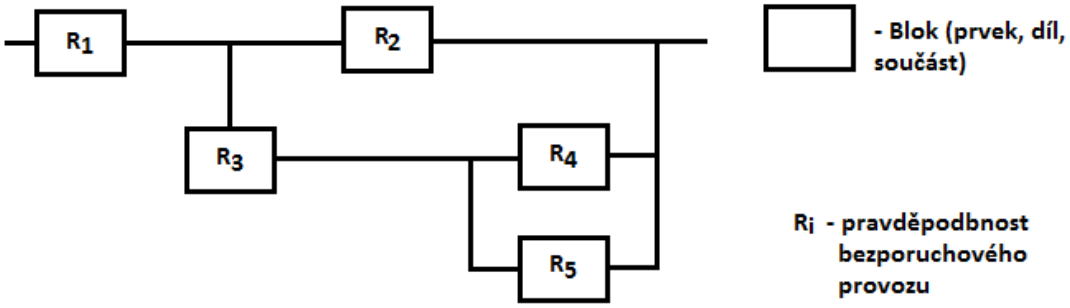
Obr. 20: Příklad stromu poruchových stavů a značek dle IEC 1025

Analýza stromu událostí – ETA (Event Tree Analysis), jedná se o induktivně deduktivní metodu analýzy s výraznějším uplatněním induktivního pojetí. Kvalitativní část analýzy ETA spočívá ve studiu možných stavů součástí nebo jiných počátečních událostí, které mají účinek na analyzovanou nežádoucí událost systému. Výsledek je zobrazen ve formě stromu (obr. 21), a pokud lze všem možným stavům přiřadit pravděpodobnosti jejich vzniku, kvalitativní část může být rozšířena o kvantitativní analýzu.



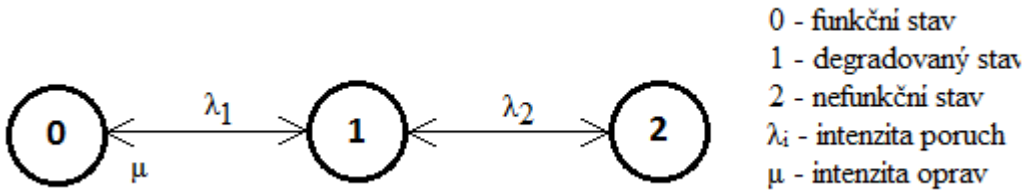
Obr. 21: Příklad stromu událostí pro jednoduchý protipožární systém

Analýza blokového diagramu bezporuchovosti – RBD (Reliability Block Diagram), deduktivní metoda, která pomocí blokového diagramu zobrazuje možnou cestu k bezpečnému (bezporuchovému) stavu systému. Blokový diagram je grafické vyjádření struktury systému prostřednictvím jeho prvků- bloků (obr. 22) a znázorňuje, jak poruchové stavy jeho prvků vedou k poruchovému stavu celého systému. Pro sestavení diagramu je možné použít různé metody kvalitativní analýzy. Pro kvantitativní zhodnocení je nutná znalost pravděpodobnostního modelu funkce každého prvku zobrazeného blokem diagramu.



Obr. 22: Příklad blokového diagramu bezporuchovosti

Markovova analýza – MA (Markov Analysis), kvantitativní metoda převážně induktivním přístupem, založena na teorii Markovových řetězců. Vyhodnocují se pravděpodobnosti, že prvky systému jsou v určitém stavu, nebo že nastanou určité události ve specifikovaných časových bodech (příp. intervalech). Východiskem analýzy je kvalitativní určení všech možných stavů objektu, znázorněných do diagramu stavových přechodů a definování jejich pravděpodobnosti přechodů z jednoho stavu do jiného (obr. 23). Toto umožňuje sestavit matici přechodů jako matematický model pro výpočty pravděpodobnosti bezporuchového stavu. Metoda je vhodná pro vyhodnocování funkčně složitých a vícestavových systémů.



Obr. 23: Příklad diagramu stavových přechodů

Předpověď bezporuchovosti výpočtem z dílů, nebo také Předpověď intenzity poruch – PC (Path County), kvalitativní a v podstatě induktivní metoda, při níž se odhadují přibližné intenzity poruch systému za předpokladu, že jeho poruchu způsobí porucha libovolného prvku. Metoda se používá v raných etapách návrhu pro elektronická zařízení (s počtem prvků řádově do 1000), a jestliže se provádí analýza namáhání dílů, poskytuje předpověď bezporuchovosti systému na celkem přijatelné úrovni přesnosti. Metoda neumožňuje zpracovávat komplexní strategii údržby ani zálohované struktury.

Je třeba zdůraznit, že při komplexních analýzách rizik se nevolí pouze jedna metoda, protože ta zpravidla nepostačí. Vždy je vhodné zvolit kombinace více metod analýz k dosažení optimální úrovně bezpečnosti analyzovaného systému ze strany výrobce (dodavatele) zákazníkovi.

V oboru spolehlivosti jsou používány i další analytické metody, které z hlediska zaměření této práce nejsou již popisovány. Jedná se zejména o metodu HAZOP (Hazard and Operability study), HRA (Human Reliability Analysis) a další. S ohledem na zaměření diplomové práce nejsou další metody v této práci blíže popisovány.

4 DATA VE SPOLEHLIVOSTI

Ve spolehlivosti se používají data různého charakteru. Jedná se především o data související s bezporuchovostí, udržovatelností a zajištěností údržby. To vede k tomu, že jsou k dispozici různé typy dat (doby provozu, ujeté vzdálenosti, cykly, počty poruch, náklady na údržbu, apod.)

Zdroje dat o spolehlivosti můžeme rozdělit do dvou skupin:

- zkoušky spolehlivosti (data výrobce)
- provozní zkušenosti (sběr dat z provozu)

4.1 Zkoušky spolehlivosti (data výrobce)

Zkoušky spolehlivosti jsou nedílnou součástí dnešního moderního programu spolehlivosti. Jsou také součástí zabezpečování kvality a jakosti každého výrobku, v čemž lze spatřit hlavní podstatu provádění zkoušek spolehlivost. Zkoušky spolehlivosti se dále vykonávají z obecné (společenské či podnikové) potřeby nadále zvyšovat jakost a spolehlivost všech výrobků a to k zajištění konkurenceschopnosti na celosvětových trzích. Dnes je již standardem systém řízení jakosti ISO 9000, ve kterém se klade důraz na prokázání a trvalé ověřování vysoké jakosti výrobku a tedy i na prokázání vysoké úrovně spolehlivosti [11].

Zkoušky spolehlivosti (bezporuchovosti) mají přinášet objektivní a reprodukovatelná data o spolehlivosti (bezporuchovosti) objektu. To vyžaduje, aby zkušební podmínky uvedené v plánech zkoušky a metody užívané k zpracování výsledků bylo co možná nejvíce reprodukovatelné a také aby byly použité vzorky reprezentativní.

Cíle zkoušek bezporuchovosti mohou být následující:

- určení či ověření (odhad) číselných hodnot ukazatelů bezporuchovosti (MTTF, λ apod.)
- odhalení slabin objektu a provedení úkonů směřujících ke zvýšení spolehlivosti objektu
- kontrola předpovědí a výpočtů učiněných během etapy návrhu
- odhalení faktorů způsobujících poruchy objektu, provedení činností směřujících k odstranění těchto faktorů
- stanovení vlivu technologických procesů na bezporuchovost
- propracování optimalizované údržby systému
- zlepšení odolnosti proti poruchám a provozní bezpečnosti
- zlepšení výkonnosti a celkové jakosti výrobku
- snaha o snížení počátečních nákladů
- analýza podmínek při používání a jejich vliv na bezporuchovost
- zjištění oprávněnosti ukazatelů bezporuchovosti pro technickou dokumentaci
- vyhodnocení nákladů na některé etapy životního cyklu výrobku

Specifikace zkoušky by měla obsahovat:

- podmínky při skutečném provozu
- cíle zkoušek
- vyjádření účelu zkoušky

- podmínky výběru zkušebních vzorků a typu zkoušky
- specifikace požadavků týkajících se znaků a parametrů zkušebních vzorků dle ČSN IEC 60300-3-4
- uspořádání zkoušky
- sběr a zpracování dat
- vyhodnocení výsledků zkoušky a jejich využití
- ověření metodiky zkoušky

Zkoušky spolehlivosti se dělí dle následujících kritérií.

Klasifikace dle všeobecného účelu

Ze statistického hlediska mohou být zkoušky bezporuchovosti klasifikovány dle svého všeobecného účelu na:

- odhad ukazatelů bezporuchovosti objektu („zkoušky určovací“)
- ověření ukazatelů bezporuchovosti uvedených například ve smlouvě nebo specifikaci
- srovnání dvou návrhů nebo dvou výrobků z hlediska bezporuchovosti

Klasifikace dle místa zkoušky

- laboratorní zkoušky – jejich výhodou je možnost provádět měření a hodnocení za řízených podmínek a tudíž zajistit jejich snadnou reprodukci. Při laboratorních zkouškách je často počet zkoušených objektů mnohem menší než při zkouškách za provozu. Podmínky laboratorních zkoušek jsou často navrženy tak, aby bylo co nejlépe zajištěno, že zkušební meze nebudou překročeny.
- zkoušky v provozu – zkoušenými objekty jsou v zásadě objekty, které užívá zákazník. Podmínky zkoušek v provozu jsou v zásadě totožné (části) reálného provozu. Poskytují realističtější výsledky zkoušek a vyžadují menší množství zkušebního vybavení avšak jejich reprodukovatelnost je obecně nižší než u laboratorních podmínek.

Klasifikace dle doby získávání výsledků

- normální zkoušky – zkouška za jmenovitých podmínek namáhání, trvá neomezeně dlouho, respektive do doby až je dosaženo požadovaných výsledků zkoušky
- zkrácené zkoušky – zkouška za jmenovitých podmínek namáhání ovšem ukončená v kratší době než bylo původně plánováno, nebo než nastane porucha všech zkoušených objektů
- zrychlené zkoušky – zkouška, při níž se použije vyšší namáhání než jmenovité nebo zkouška se zhuštěnou dobou či zhuštěnými cykly nebo zkoušky se stupňovitým namáháním.

4.2 Provozní zkušenosti (sběr dat z provozu)

Sběr dat

Pro zjištění provozní spolehlivosti jednotlivých technologických zařízení je zapotřebí získat data o jejich provozních podmínkách, politice údržby a samozřejmě o poruchách a následných opravách.

Pro statistické vyhodnocení poruchovosti zařízení je třeba získat co největší reprezentativní vzorek, tedy v ideálním případě data o všech zařízeních daného typu. Tato data lze pak roztřídit dle prostředí, v kterém jsou provozovány. Získávání těchto informací je důležitou částí spolehlivostních analýz. V dnešní době je již možné setkat se softwarovou databází údržby, ze které je možné jednoduchým tříděním a exportem potřebná data získat. Pokud takový software není k dispozici je potřeba pátrat v listinných záznamech údržby a ty pak následně převést do elektronické podoby. Nejhorším případem pak může být situace, kdy jsou informace o údržbě udržovány jen formou zkušeností zaměstnanců údržby zařízení. V tomto případě je pak nutné zapsat údaje pro účel reprodukovatelnosti dané analýzy.

Výpočet doby provozu

Celková kumulovaná doba provozu zkoumaného zařízení je základním údajem pro výpočty spolehlivostních ukazatelů. Celkovou kumulovanou dobu provozu zkoumaného zařízení získáme prostým součtem všech dob provozu zařízení. Jestliže není dostupné datum uvedení do provozu, bude za počátek provozování daného zařízení okamžik první poruchy.

Pro celkový výpočet je vhodné použití např. programu MS EXCEL, v němž je možné pro celkový výpočet využít funkci Rok360. Tato funkce počítá s tím, že 1 rok má 12 měsíců po 30 dnech a tedy 360 dnů za jeden kalendářní rok. Tato skutečnost může být užitečná a to tím, že částečně eliminuje plánované odstávky zařízení, které není možné z důvodu vysoké náročnosti na vstupní informace uvažovat.

Celková kumulovaná doba provozu je součtem dob, po které byla zařízení na pozicích, zatímco celková kumulovaná doba provozu, převedená na skutečný počet provozovaných strojů je odhadnutá skutečná doba provozu, tedy počet hodin, po které namontované provozované zařízení na svých pozicích skutečně provozovány (tj. bez doby kdy byly zařízení na pozicích pouze jako záložní).

Výpočet spolehlivostních parametrů

Ze sběru dat z údržby (z dat o údržbových zásazích) je potřeba odfiltrovat záznamy o generálních a běžných opravách a to tak, aby zůstala data pouze o poruchách zařízení. Ty je poté třeba chronologicky seřadit a vytvořit histogram (histogram – grafické znázornění distribuce dat pomocí sloupcového grafu se sloupci stejné šířky, vyjadřující šíři intervalu, přičemž výška sloupce představuje četnost sledované veličiny v tomto intervalu) četnosti poruch dle jednotlivých let provozu. Počet poruch v jednom roce udává počet poruch na všech provozovaných zařízeních.

Sledovaná zařízení bývají provozována ve stále stejných provozních podmínkách po dlouho dobu a lze tedy říci, že jejich intenzita poruch λ je konstantní. Takovému předpokladu odpovídá exponenciální rozdělení střední doby do poruchy. Exponenciální rozdělení má jediný parametr λ, který je převrácenou hodnotou střední doby mezi poruchami MTBF.

Provede se test dobré shody chí-kvadrát pro potvrzení či vyvrácení oprávněnosti použití exponenciálního rozdělení pro popis doby do poruchy. Protože exponenciální rozdělení má konstantní intenzitu poruch, lze zjistit očekávaný počet poruch v časovém intervalu A. Rozdělíme celkovou dobu testu na m stejných intervalů, kde očekávaná počet poruch A je [12]:

$$A = w \cdot \frac{d}{T} \tag{4.01}$$

kde *w* je délka intervalu zvolená tak, aby v každém intervalu bylo alespoň 5 poruch, *d* je počet poruch v testovaném intervalu. Následuje výpočet testové statistiky:

$$\chi^2 = \sum_{i=1}^{m} \frac{(r_i - A)^2}{A} \tag{4.02}$$

Pro potvrzení hypotézy nasazení exponenciálního rozdělení pro popis střední doby do poruchy musí být vypočtena hodnota kvantilu χ^2 menší, než teoretická hodnota kvantilu χ^2(v) pro v = m-1 stupňů volnosti. Provede se jednostranný test na např. 10% hladině významnosti.

Bodový odhad MTBF všech zařízení (jednoho typu) se vypočte dle normy ČSN IEC 60605-4:

$$\lambda = \frac{1}{MTBF} \tag{4.03}$$

Konfidenční intervaly se získají opět dle normy ČSN IEC 60605-4 podle vztahů pro výpočet dolní a horní konfidenční meze intenzity poruch, které jsou uvedeny v následujících dvou vzorcích při konfidenční úrovni 90%.

$$\lambda_{0,05} = \frac{{\chi^2}_{0,05}(2\mathrm{r})}{2T} \tag{4.04}$$

$$\lambda_{0,95} = \frac{{\chi^2}_{0,95}(2\mathrm{r}+2)}{2T} \tag{4.05}$$

kde ${\chi^2}_{\alpha}$(v) označuje α-kvantil distribuční funkce rozdělení χ^2 s *v* stupni volnosti.

$$\mathrm{MTBF}_{0,95} = \frac{1}{\lambda_H} \tag{4.06}$$

$$\mathrm{MTBF}_{0,05} = \frac{1}{\lambda_D} \tag{4.07}$$

Dolní a horní mez střední doby mezi poruchami na 90% konfidenční mezi označuje, že s pravděpodobností 90% bude střední doba mezi poruchami ležet uvnitř intervalu $\langle MTBF_{0,,95}, MTBF_{0,05} \rangle$.

Mezi další sledované ukazatele spolehlivosti je střední doba do obnovy (MTTR) zařízení. Tu je možné spočítat jako podíl součtu všech časů do obnovy k počtu poruch, pokud jsou data dostupná:

$$\mathrm{MTTR} = \frac{T_p}{r} \tag{4.08}$$

Dolní a horní mez konfidenčního intervalu střední doby do obnovy se při konfidenční úrovni 90% vypočítá následovně:

$$\mathrm{MTTR}_{0,95} = \frac{2T}{\chi^2{}_{0,95}(2\mathrm{r}+2)} \tag{4.09}$$

$$\mathrm{MTTR}_{0,05} = \frac{2T}{\chi^2{}_{0,05}(2\mathrm{r})} \tag{4.10}$$

Dolní a horní mez střední doby do obnovy na 90% konfidenční mezi udává, jaké je rozmezí dob do obnovy, které s 90% pravděpodobností spadnou do vypočteného intervalu.

Na základě výše uvedených spolehlivostních parametrů je možné vypočítat asymptotickou pohotovost či nepohotovost zařízení:

$$\mathrm{U} = \frac{MTTR}{MTTR + MTBF} \tag{4.11}$$

5 METODOLOGIE ŘEŠENÍ

Metodologie řešení je založena na výběru využití metod vhodných pro vyřešení daného problému. Řešenou problematikou v této diplomové práci je stanovení hodnoty úrovně integrity bezpečnosti SIL podle normy ČSN EN 61508 [5] jak pro hardwarovou, tak pro softwarovou část snímače tlaku XMP i firmy BD SENSORS.

Integrita bezpečnosti je podle uvedené normy chápána ve dvou rovinách:

- odolnost proti nenáhodné (systematické) poruše vnesené do výrobku během jeho návrhu a výroby (časných etap životního cyklu výrobku), tedy proti chybě způsobené nekvalitním pracováním a provedením výrobku,
- odolnost proti náhodným (zbytkovým) poruchám výrobku, které jsou dány přirozenou mírou nahodilosti materiálových a jiných parametrů výrobku.

Hodnoty úrovně integrity bezpečnosti podle ČSN EN 61508 [5] stanovuje tab. 9, která obsahuje 2 základním metriky:

- úrovně integrity bezpečnosti (hodnota 1 až 4)

– pravděpodobnostní ukazatele pro režim s vysokým a nízkým vyžádáním (hodnoty pravděpodobnosti ve stanovených rozsazích).

Tab. 9: Hodnoty úrovně integrity bezpečnosti dle normy ČSN EN 61508

SIL - úroveň integrity bezpečnosti	Pravděpodobnost výskytu poruchy za hodinu provozu (**PFH**)	Střední pravděpodobnost výskytu nebezpečné poruchy při vyžádání funkce (**PFD**)
SIL 4	$\geq 10^{-9}$ až $< 10^{-8}$	$\geq 10^{-5}$ až $< 10^{-4}$
SIL 3	$\geq 10^{-8}$ až $< 10^{-7}$	$\geq 10^{-4}$ až $< 10^{-3}$
SIL 2	$\geq 10^{-7}$ až $< 10^{-6}$	$\geq 10^{-3}$ až $< 10^{-2}$
SIL 1	$\geq 10^{-6}$ až $< 10^{-5}$	$\geq 10^{-2}$ až $< 10^{-1}$

Proti nenáhodné (systematické) chybě je třeba použít vhodné metody managementu kvality (dle normy ISO 9001) a to na úrovni odpovídající požadované úrovni integrity bezpečnosti (1 až 4) jak hardwarové, tak softwarové části. Pro stanovení hodnot pravděpodobnostních ukazatelů náhodných (zbytkových) poruch, a tedy pro specifikaci dosahované úrovně integrity hardwarové části, je třeba zvolit takové metody, které umožní určit:

a) pravděpodobnost výskytu poruchy za hodinu provozu – PFH pro režim s vysokým, popř. trvalým vyžádáním,

b) střední pravděpodobnost výskytu nebezpečné poruchy při vyžádání funkce – PFD pro režim s nízkým vyžádáním

K tomu je zapotřebí:

– funkční analýza snímače XMP i
– analýza možných způsobů a důsledků poruch na úrovni komponent a na úrovni snímače tlaku XMP i (FMEA)
– vyhodnocení kritičnosti poruch (rozšířením analýzy FMEA na FMECA)
– stanovení hodnot pravděpodobnosti výskytu poruchy za hodinu provozu na úrovni komponent (z intenzity poruch od výrobce komponent a ze sběru dat o poruchách snímače tlaku XMP i z provozu tohoto snímače)
– sestavení modelu spolehlivosti pro funkce snímače tlaku XMP i (sériový model)
– kvantifikace modelu spolehlivosti pro funkce snímače tlaku XMP i pro bezpečnou a nebezpečnou poruchu (výpočet z intenzit poruch komponent metodou PCA – Parts Count Analysis)
– stanovení podílu skrytých (nedetekovatelných) poruch komponent pro předepsání intervalu zkoušení snímače tlaku XMP i pro režim s nízkým vyžádáním

Pro softwarovou část snímače tlaku XMP i je třeba zvolit takové metody programování a kontroly softwarových chyb, které pro požadovanou úroveň integrity bezpečnosti (SIL 3) určují příslušné normy pro tvorbu softwaru, a to především norma ČSN EN 61508-3.

5.1 Funkční analýza

Funkční analýza analyzuje funkce technického objektu, v tomto případě snímače tlaku XMP i. Tato analýza identifikuje a popisuje kritické (klíčové) funkce snímače tlaku XMP i (funkce měření tlaku, teploty apod.) a rozděluje snímač tlaku na určité funkční moduly. Následně hodnotí důsledky ztrát těchto funkcí, zda nastane při selhání dané funkce kritická událost nebo je ztráta této funkce pouze minoritního charakteru. Na hodnocení funkční nebezpečnosti navazuje kvalitativní analýza spolehlivosti prvků.

5.2 Metoda FMEA/FMECA

Analýza bude realizována podle modifikovaného postupu uvedeného v normě ČSN EN 60812. Modifikace bude spočívat v tom, že k jednotlivým módům poruch bude stanovována intenzita poruch, detekovatelnost poruch a důsledky poruch na funkci snímače z pohledu funkční bezpečnosti. Tyto faktory pak vystihnou kritičnost jednotlivých módů poruch.

Navržený postup s ohledem na výše uvedené skutečnosti se skládá z následujících kroků.

KROK 1: Základní popis funkcí systému a jeho parametrů – viz kapitola 5.1 Funkční analýza

- stručný popis funkcí analyzovaného systému a popis součástí, ze kterých se systém skládá.
- základní parametry a vlastnosti systému.

KROK 2: Vymezení hranic systému

- získání informací o systému a určení co vše je předmětem analýzy.
- získání informací o provozních podmínkách a podmínkách prostředí.

KROK 3: Základní požadavky a definice

- stanovení struktury systému. Pro analýzu FMEA/FMECA je vhodné předpokládat dvoustavový systém (viz kapitola 3.1), který může být buď v provozu, nebo v poruchovém stavu. Vymezení pojmu poruchový stav.
- stanovení požadavků na spolehlivost.

KROK 4: Získávání informací o prvcích systému – viz kapitola 5.3

- vytvoření seznamu prvků systému, obsahujícího informace o daných prvcích (název, výrobce…).
- stanovení ukazatelů bezporuchovosti (intenzity poruch λ) jednotlivých prvku (součástek) systému.

KROK 5: Spolehlivostní model systému – viz kapitola 5.4

- rozčlenění systému na jednotlivé úrovně (nejnižší – součástky, nejvyšší – systém).
- pro jednotlivé úrovně vytvořit blokový diagram spolehlivosti.

KROK 6: Třídění intenzit poruch prvků

- dělení celkové intenzity poruch v závislosti na módu poruchy (zkrat, přerušení, …).

- dělení intenzity poruch na bezpečnou / nebezpečnou (λ_D, λ_S).
- dělení intenzity porucha na poruchu zjevnou / skrytou (λ_{DD}, λ_{SD}, λ_{DU}, λ_{SU}).

KROK 7: Vytvoření pracovního formuláře

- pracovní formulář obsahuje některé povinné údaje (název prvku a subsystému, mód předvídané poruchy, následek poruchy, …) a další volitelné údaje (ukazatele bezporuchovosti, typ poruchy skrytá/zjevná, detekovatelnou poruchy, …).

KROK 8: Vlastní provedení analýzy

- vlastní provedení analýzy probíhá dle následujícího algoritmu. Analýza musí pokrýt všechny prvky, ze kterých se daný analyzovaný systém (snímač tlaku XMP i skládá.

KROK 9: Vyhodnocení analýzy v závislosti na požadavcích zadání

- porovnání výsledků analýzy se zadáním (předem danými požadavky na spolehlivost snímače XMP i – splnění či nesplnění integrity bezpečnosti SIL 3).

5.3 Parametry bezporuchovosti komponent

Parametry bezporuchovosti komponent (intenzita poruch λ či střední doba mezi poruchami MTBF) budou zjištěny převážně z dat uvedených v katalogových listech výrobců daných komponent a to především pro rezistory a kondenzátory, u kterých výrobci ve svých katalogových listech tyto hodnoty uvádějí (výrobce rezistorů – Vishay, výrobce kondenzátorů – AVX). Pro ostatní komponenty budou parametry bezporuchovosti určeny ze sběru dat z provozu snímače XMP i a v krajních případech expertním odhadem (využití databank bezporuchovostních parametrů součástek dostupných na internetu apod.)

5.4 Model spolehlivosti

Spolehlivostní model analyzovaného systému (snímače tlaku XMP i) lze znázornit pomocí sériového blokového diagramu. Celý systém lze rozčlenit na několik částí (subsystémů). Analyzovaný systém neobsahuje žádnou zálohu, takže jej lze znázornit pomocí sériového spolehlivostního blokového diagramu, viz obr. 24. S ohledem na rozsah diplomové práce se zjednodušeně předpokládá, že pro každou funkci snímače XMP i jsou zapotřebí všechny jeho moduly. Model spolehlivosti je úzce svázán s poznatky získanými z funkční analýzy a z analýzy FMEA/FMECA, jelikož pracuje s daty (zejména s intenzitami poruch, detekovatelností poruch a důsledky poruch) získanými z těchto analýz.

Obr. 24: Příklad sériového modelu spolehlivosti

5.5 Počítání z dílů

Jelikož daný systém (snímač tlaku XMP i) vychází ze sériového blokového modelu spolehlivosti, bude tato metoda velmi jednoduchá. Bude se jednat o prosté sečtení příslušných typů intenzit poruch v závislosti na jejich parcelaci. Pro analýzu počítání z dílu pak pro daný model spolehlivosti bude platit:

– Pro intenzity poruch jednotlivých modulů:

$$\lambda_{modulu} = \sum_{i=1}^{n} \lambda_i \tag{5.01}$$

Kde: λ_{modulu} – je intenzita poruch daného modulu

λ_i – je intenzita poruch jednotlivých součástek modulů

– Pro intenzity poruch celého systému:

$$\lambda_{celk} = \sum_{i=1}^{n} \lambda_{modulu_i} \tag{5.02}$$

Kde: λ_{celk} – je intenzita poruch celého systému

$\lambda modulu_i$ – je intenzita poruch jednotlivých modulů systému

5.6 Analýza důsledků nedetekovatelných poruch pro režim nízkého vyžádání

Jelikož předem není možné určit, v jakém režimu bude daný analyzovaný snímač tlaku XMP i pracovat (zda v režimu s nízkým vyžádáním nebo v režimu s vysokým popřípadě trvalým vyžádáním), provádí se výpočet střední pravděpodobnosti výskytu nebezpečné poruchy při vyžádání (tedy hodnoty asymptotické nepohotovosti) a to v závislosti na podílu skrytých poruch a intervalu zkoušek funkčnosti snímače tlaku XMP i.

6 SNÍMAČ TLAKU XMP I

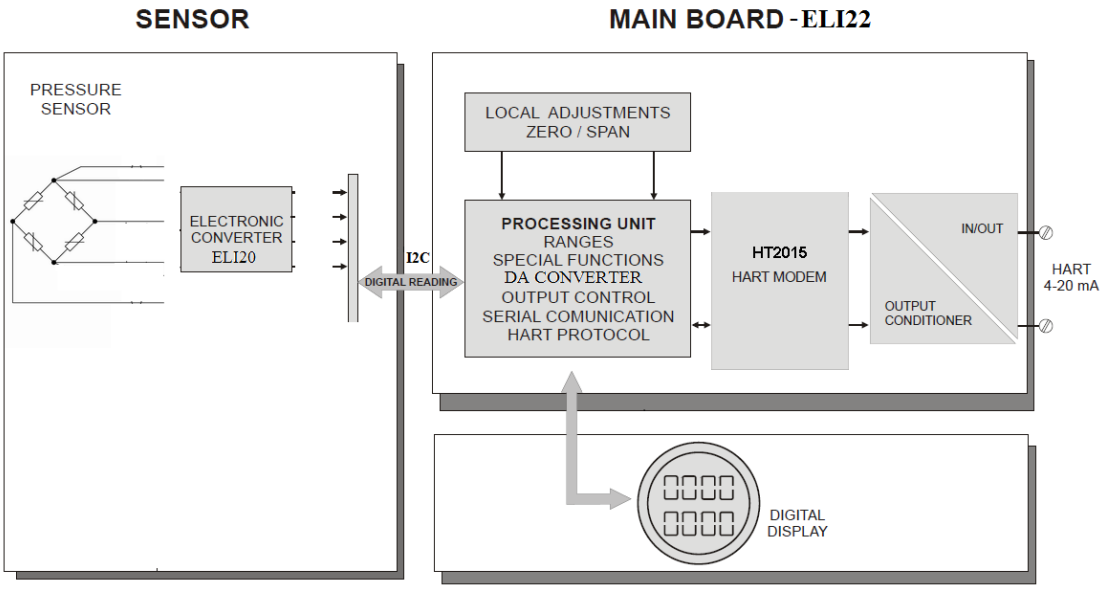
Snímač tlaku XMP i (obr. 25) vyráběný firmou BD SENSORS je navržený pro průmyslové procesy a to pro měření podtlaku, relativního a absolutního tlaku, tlakových rozsahů plynů, par, kapalin a prachů a to až do tlaku 600 bar. Snímač je již ve své základní verzi vybaven digitální komunikací HART. Na výběr je pak dvojice pouzder, a to nerezové polní pouzdro nebo pouzdro duralové dvoukomorové. Jako vlastní senzor tlaku, zde slouží senzor s interním označením firmy DSP 411 (obr. 26) pracující na bázi polovodičového tenzometru s oddělovací membránou o průměru 18 mm. Tento senzor je vhodný pro měření plynných a kapalných médií, která jsou

slučitelná s nerezovou ocelí.

Obr. 25: Snímač tlaku XMP i firmy BD SENSORS

Obr. 26: Senzor tlaku DSP 411

Základní blokové schéma zapojení snímače tlaku je zobrazeno na následujícím obrázku (obr. 27).



Obr. 27: Blokové schéma snímače tlaku XMP i

Vybrané technické údaje snímače tlaku XMP i jsou obsaženy v tab. 10. Kompletní parametry snímače jsou uvedeny v příloze A, část 2.

Tab. 10: Základní parametry snímače tlaku XMP i

Rozsah měřených tlaků	0,4 - 600 bar
Výstupní signál	2vodič: 4..20 mA
	jiskrově bezpečná verze s komunikací HART / U_B = 12…28 V_{DC}
	provedení Ex d - pevný závěr / U_B = 12…28 V_{DC}
Přesnost	≤ ± 0,1% FSO
Dlouhodobá stabilita	≤ ± 0,1% FSO / rok při referenčních podmínkách
Povolené teploty	bez displeje: okolí: -40…80°C
	s displejem: okolí:-20…70°C
	médium: silikonový olej -40…125°C
	médium: potravinářský olej: -10…125°C
Elektrická odolnost	odolnost proti zkratu: trvalá
	Odolnost proti přepólování: bez poškození, ale také bez funkce
	EMC: vyzařování a odolnost dle ČSN EN 61326
Mechanická odolnost	Vibrace: 5 g RMS dle DIN EN 60068-2-6
	Rázy: 100 g / 11 ms dle DIN EN 60068-2-27
Třída krytí	IP67
Hmotnost	minimálně 400g

Kompletní sestava snímače tlaku XMP i je v příloze A, část 11.

7 APLIKACE ŘEŠENÍ NA SNÍMAČI XMP I

7.1 Vymezení systému a podmínky jeho činnosti

Pro každou analýzu systému je nutné stanovit, co do analyzovaného systému patří a co je již mimo hranice analyzovaného systému. Analyzovaným systém je v tomto případě snímač tlaku XMP i firmy BD SENSORS s.r.o. a to v sestavě dané katalogovým listem snímače tlaku XMP i. Hranice systému je na jedné straně definována tlakový připojením (tlakovými přípojkami či tlakovou přírubou dle katalogového listu snímače tlaku XMP i viz příloha A, část 2) a na straně druhé jeho elektrickým připojením realizovaným skrz kabelovou průchodku do svorkovnice.

Podmínky činnosti snímače XMP i jsou specifikovány v katalogovém listu snímače XMP i. Za nejdůležitější podmínky, které mohou ovlivnit funkci snímače při překročení specifikovaných mezí, se považují:

- teplota měřeného média,
- typ měřeného média,
- teplota okolí snímače,
- tlakový rozsah měřeného média.

7.2 Funkční analýza snímače

Funkční analýza systému (snímače tlaku XMP i) specifikovala následující funkce:

- F1 = funkce měření tlaku
- F2 = funkce měření teploty
- F3 = funkce digitální komunikace (HART)
- F4 = funkce analogového výstupu (standardní analogový výstup po proudové smyčce 4-20 mA)
- F5 = funkce zobrazení (displeje) – zobrazení měřených dat (tlaku, teploty), konfigurační možnosti snímače tlaku XMP i.

Kritičnost poruch funkcí

Všechny výše uvedené funkce F1-F5 snímače tlaku XMP i lze z hlediska bezpečnosti považovat za primární funkce snímače tlaku XMP i a jejich ztráta je tedy z hlediska bezpečnosti kritická. V modelu spolehlivosti se ztráta těchto funkcí hodnotí jako selhání snímače tlaku XMP i. Za nebezpečnou poruchu lze považovat i změnu přesnosti měření tlaku a teploty o více jak 0,1 % FSO (Full Scale Output) a to z důvodu udávané přesnosti snímače tlaku XMP i uvedené v tab. 9.

Funkce jednotlivých modulů snímače tlaku XMP i:

MP – modul procesoru

- P1 = měření
- P2 = komunikace s okolím
- P3 = výpočty
- P4 = komunikace s periferií
- P5 = řízení výstupu

MN – modul napájení

- N1 = napájení

MDK – modul digitální komunikace

- K1 = digitální komunikace – příjem dat
- K2 = digitální komunikace – odesílání dat

MAV – modul analogového výstupu

- A1 = analogový výstup

MD – modul displeje

- D1 = funkce zobrazovače
- D2 = ovládání menu přístroje

MES – modul elektroniky senzoru

- E1 = měření tlaku
- E2 = měření teploty
- E3 = napájení senzoru
- E4 = digitální komunikace

MS – modul senzoru

- S1 = měření tlaku
- S2 = měření teploty
- S3 = digitální výstup

MMP – modul mechanického pouzdra

- H1 = ochrana vnitřních součástí
- H2 = mechanické upevnění
- H3 = funkce tlakové přípojky

7.3 Analýza FMEA/FMECA snímače

Analýza je provedena od nejnižší úrovně systému, tzn. od úrovně jednotlivých součástek, ze kterých se systém skládá.

Pro účely této diplomové práce se analyzovaný systém, subsystémy a součástky uvažují jako dvoustavové. Každý prvek systému se tak může nacházet pouze v jednom ze dvou možných stavů – v bezporuchovostním stavu nebo ve stavu poruchy (viz kapitola 3.1).

Předvídané módy poruch jednotlivých součástek jsou:

- zkrat – pro součástky: rezistory, kondenzátory, varistory,
- přerušení – pro součástky: rezistory, kondenzátory, varistory,
- změna hodnoty – pro součástky: rezistory, kondenzátory,
- porucha – pro ostatní součástky mimo výše uvedených (diody, procesory, krystaly, stabilizátory napětí atd.).

Požadavky na spolehlivost jsou zaměřeny na výpočet intenzity poruch systému, určení skrytosti či zjevnosti poruchy, její detekovatelnosti a důsledků poruchy pro funkce podstatné z hlediska funkční bezpečnosti. To jsou podstatné náležitosti pro

zjištění, za sebe jedná o poruchu bezpečnou či nebezpečnou a detekovatelnou či nedetekovatelnou. Tyto informace pak zásadním způsobem ovlivňují zařazení snímače do příslušné úrovně funkční bezpečnosti.

Pracovní formulář FMEA/FMECA je sestaven s ohledem na definované požadavky plynoucí ze zadání diplomové práce – stanovení úrovně integrity bezpečnosti snímače tlaku XMP i. Podoba sestaveného pracovního formuláře je na obr. 28.

FMEA - FORMULÁŘ

	Produkt:		**Datum vypracování:**		**Strana:**													
	Modul:		**Vypracoval:**															
	Popis funkce:		**Schéma zapojení:**															
ID	**Prvek**	**λ [h^{-1}]**	**Mód poruchy**	**Následek poruchy na subsystém**	**Následek poruchy na systém**	**Selhání v %**	**Porucha bezpečná/nebezpečná %**	**Porucha zjevná/skrytá**	**λ_{DD} [h^{-1}]**	**λ_{DU} [h^{-1}]**	**λ_{SD} [h^{-1}]**	**λ_{SU} [h^{-1}]**	**λ_{NE} [h^{-1}]**	**Doporučená opatření**				

Obr. 28: Podoba vytvořeného pracovního formuláře FMEA/FMECA pro účely diplomové práce

7.3.1 Provedení analýzy FMECA

Vlastní provedení analýzy FMEA bylo řešeno vyplněním výše uvedeného pracovního formuláře (obr. 28) a to pro všechny moduly snímače tlaku XMP i. Pro každý analyzovaný prvek se vyplní:

- ID – identifikační číslo prvku (př. 1.01),
- prvek – název prvku dle výkresové dokumentace (př. R1 – rezistor),
- intenzita poruch prvku λ, vztažená na 1 hodinu provozu,
- mód poruchy – možnosti selhání daného prvku,
- následek poruchy na subsystém (modul),
- následek poruchy na systém (snímač tlaku XMP i),
- selhání v % - pravděpodobnost, že se daný prvek porouchá daným módem poruchy, vyjádřená v procentech,
- typ poruchy bezpečná/nebezpečná – podíl na typu poruchy bezpečná či nebezpečná vyjádřený v procentech,
- porucha zjevná/skrytá – rozdělení poruchy na zjevnou či skrytou
- λ_{DD}, λ_{DU}, λ_{SD}, λ_{SU}, λ_{NE} – parcelace celkové intenzity poruch na intenzitu poruch nebezpečných detekovatelných (Dangerous Detected), nebezpečných nedetekovatelných (Dangerous Undetected), bezpečných detekovatelných (Safe Detected), bezpečných nedetekovatelných (Safe Undetected) a intenzity poruch bez efektu (No Effect),
- doporučená opatření – návrh opatření pro zvýšení spolehlivosti.

Celkově provedená analýza FMEA/FMECA snímače tlaku XMP i je součástí přílohy této diplomové práce (příloha A, část 1). K provedení analýzy FMEA/FMECA je zapotřebí týmové práce. Pro účely této diplomové práce byli přiděleni firmou tito konzultanti:

- Ing. Radek Burda – pracovník vývojového úsek firmy BD SENSORS (obor elektrotechniky),
- Mgr. Miroslav Sochor – pracovník vývojového úseku firmy BD SENSORS (obor mechaniky).

7.3.2 Výsledky FMECA

Dosažené výsledky analýzy FMECA ukázaly, že nejkritičtějším modulem snímače tlaku XMP i je modul displeje MD a to z důvodu nejvyšší intenzity poruch λ, která dosahuje hodnoty v řádu pouze 10^{-7}. Součástky typu tlačítka a vlastní displej, které se na této intenzitě poruch podílejí nejvyšší mírou a zároveň je jejich případná porucha kritická (ztráta funkce displeje) by bylo vhodné vyměnit za součástky spolehlivější.

7.4 Parametry bezporuchovosti komponent snímače

Data pro určení bezporuchovosti komponent (intenzita poruch λ či střední doba mezi poruchami MTBF) byly zjištěny na základě:

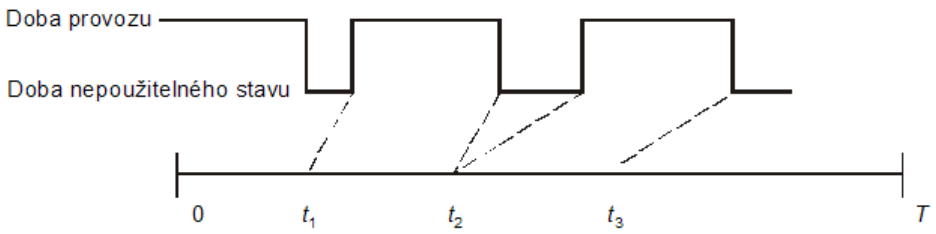
- dat od výrobce dané komponenty (z katalogových listů výrobce, či interních zkoušek spolehlivosti daného výrobce),
- dat z provozu snímače MTBF tlaku XMP i,
- expertním odhadem (např. na základě Military Handbook apod.).

Převážná část dat o bezporuchovosti komponent (λ, MTBF) byla získána z katalogových listů výrobce daných komponent. Jednalo se především o kondenzátory firmy AVX, rezistory a diody firmy Vishay, a dále pak o modem digitální komunikace HART od firmy SMAR. Takto získaným datům byla přidělena věrohodnost dat 100% a zahrnovala 84,31% komponent snímače tlaku XMP i. Pro ostatní komponenty byla data bezporuchovosti nastavena expertním odhadem. Těmto bezporuchovostním datům byla přidělena věrohodnost 75% a zahrnovaly zbylé komponenty (15,59% komponent snímače tlaku XMP i) typu procesor, oscilační krystal, operační zesilovače, stabilizátory napětí ad.

Data bezporuchovosti získané z katalogových listů výrobců daných komponent a data bezporuchovosti určená expertním odhadem jsou ve formě seznamu obsahujícího označení prvku, název prvku, intenzitu poruch λ daného prvku, střední dobu mezi poruchami MTBF daného prvku, zdroj dat bezporuchovosti prvku a věrohodnost zdroje pro daný prvek uvedeny v příloze A, část 1.

Data z provozu snímače tlaku XMP i

Data z provozu byla sbírána od počátku výroby snímače tlaku XMP i po konec roku 2014 (31. 12. 2014). V tomto období bylo celkem v provozu 1638 snímačů tlaku XMP i. Jedná se o zkoušku spolehlivosti na základě dat z provozu. V průběhu zkoušky se měnil počet vzorků ve zkoušeném souboru. Jedná se o zkušební plán s obecně cenzurovanými soubory. Na obr. 29 je uveden příklad dob mezi poruchami a dob oprav opravovaného objektu. Takovému procesu provozu (i zkoušky) se říká „alternativní proces obnovy“ a je typický pro obnovované objekty, u nichž zkouška končí ve zvoleném či pevněn daném okamžiku doby provozu. Celková akumulovaná doba provozu byla spočtena pomocí funkce ROK360 v programu MS EXCEL. Během doby provozu bylo zaznamenáno 8 poruch s následnou opravou daného snímače tlaku. Potřebná data jsou zpracována v příloze A, část 10. Níže jsou spočteny konfidenční intervaly pro intenzitu poruch λ a střední dobu mezi poruchami MTBF. Výpočty byly provedeny pro 90% konfidenční interval [12].



Obr. 29: Příklad náhodně cenzurovaného souboru

Bodový odhad střední doby do poruchy snímače tlaku XMP i:

$$MTBF = \frac{T}{r} = \frac{28182696}{8} = 3{,}52E^6 h \tag{7.01}$$

Bodový odhad intenzity poruch snímače tlaku XMP i:

$$\lambda = \frac{1}{MTBF} = \frac{1}{3{,}52E^{6}h} = 2{,}84E^{-7}h^{-1} \tag{7.02}$$

Konfidenční intervaly intenzity poruch snímače tlaku XMP i:

$$\lambda_{0,05} = \frac{\chi^{2}{}_{0,05}(2\mathrm{r})}{2T} = \frac{7{,}96}{2 \cdot 28182696} = 1{,}41E^{-7}h^{-1} \tag{7.03}$$

$$\lambda_{0,95} = \frac{\chi^{2}{}_{0,90}(2\mathrm{r}+2)}{2T} = \frac{28{,}87}{2 \cdot 28182696} = 5{,}12E^{-7}h^{-1} \tag{7.04}$$

Konfidenční intervaly střední doby mezi poruchami:

$$\mathrm{MTBF}_{0,95} = \frac{1}{\lambda_{0,95}} = \frac{1}{5{,}12E^{-7}} = 1{,}98E^{6}h \tag{7.05}$$

$$\mathrm{MTBF}_{0,05} = \frac{1}{\lambda_{0,05}} = \frac{1}{1{,}41E^{-7}} = 7{,}08E^{6}h \tag{7.06}$$

Hodnoty bezporuchovosti získané z provozu se vztahují na snímač tlaku XMP i jako celek (zkoumaný systém) a lze je následně porovnat s hodnotami z predikce bezporuchovosti získané počítáním z dílů v kapitole 7.6.

7.5 Model spolehlivosti snímače

Spolehlivostní model analyzovaného systému (snímače tlaku XMP i) lze znázornit pomocí blokového spolehlivostního diagramu. Celý systém se skládá z několika částí. Pro tvorbu blokového spolehlivostního diagramu je vhodné rozčlenit systém na jednotlivé moduly a to dle jejich primární funkce:

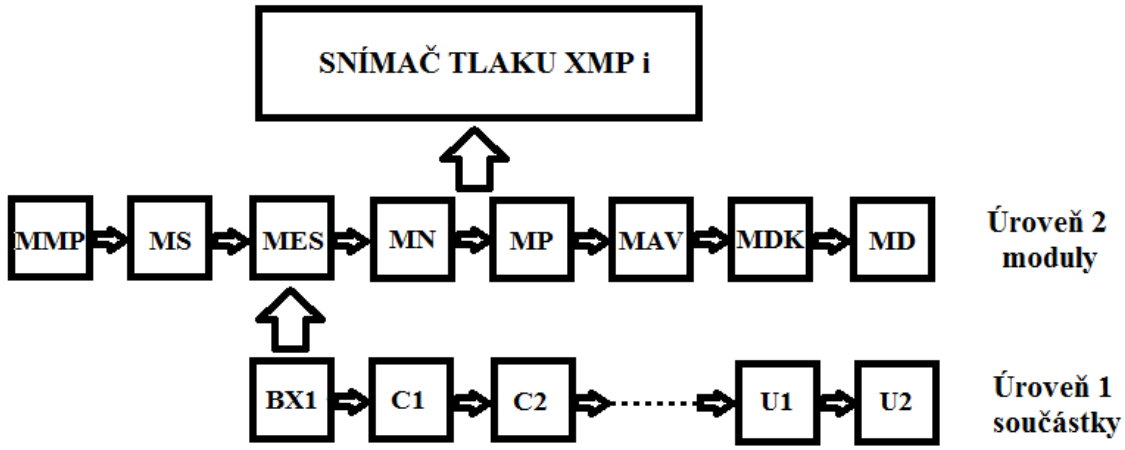
- MP = modul procesoru, část elektroniky s interním označením ELI 22 (zpracování, řízení a diagnostika),
- MN = modul napájení, část elektroniky s interním označením ELI 22 (zdroj stabilizovaného napětí elektroniky ELI 22),
- MDK = modul digitální komunikace, část elektroniky s interním označením ELI 22 (digitální komunikace HART – příjem a vysílání dat),
- MAV = modul analogového výstupu, část elektroniky s interním označením ELI 22 (standardní analogový výstup 4 – 20mA),
- MD = modul displeje, část elektroniky s interním označením ELI 22 (zobrazovací LCD jednotka s tlačítky),
- MES = modul elektroniky senzoru, elektronika s interním označením ELI 20,

- MS = modul senzoru, vlastní senzor pro měření tlaku s interním označením DSP 411,
- MMP = modul mechanického pouzdra.

Selhání jakéhokoliv modul z výše uvedených ja v rámci spolehlivostního modelu posuzováno jako ztráta funkce snímače tlaku XMP i. Pro tvorbu spolehlivostního modelu je zapotřebí specifikovat současná spolehlivostní opatření daného systému (snímače tlaku XMP i). Stávající spolehlivostní opatření:

- záloha redundance – žádná,
- metody detekce poruch – interní detekce (signál pod úrovní 4 mA nebo nad úrovní 20 mA = porucha).

Jelikož analyzovaný systém neobsahuje žádnou zálohu, je možné ho znázornit pomocí sériového spolehlivostního blokového diagramu, viz obr. 30.



Obr. 30: Spolehlivostní model analyzovaného systému (snímače tlaku XMP i)

7.6 Počítání z dílů snímače

Počítání z dílu PCA vychází z analýzy FMEA/FMECA a ze sestavení spolehlivostního modelu, který je čistě sériový. To znamená, že metoda PCA bude založena na prostém sečtení intenzit poruch prvků modulů a následném sečtení intenzit poruch jednotlivých modulů, čímž se získají jednotlivé intenzity poruch celého systému (snímače tlaku XMP i).

7.6.1 PCA modulů snímače

Ukázka metody PCA aplikované na jednotlivých modulech je prezentována na modulu displeje MD. Kompletní výpočty PCA všech modulů jsou uvedeny v příloze A, část 1 této diplomové práce.

Tab. 11: Výřez analýzy FMECA modulu displeje MD pro znázornění metody PCA

PRVEK	λ [h^{-1}]	Selhání v % pro módy poruchy	bezpečná / nebezpečná %	zjevná /skrytá	λ_{DD} [h^{-1}]	λ_{DU} [h^{-1}]	λ_{SD} [h^{-1}]	λ_{SU} [h^{-1}]	λ_{NE} [h^{-1}]
C29	3,05E-09	40%	50/50	skrytá	0	6,10E-10	0	6,10E-10	v
		40%	0/100	zjevná	1,22E-09	0	0	0	0
		20%	-	-	0	0	0	0	6,10E-10
C30	3,05E-09	40%	50/50	skrytá	0	6,10E-10	0	6,10E-10	0
		40%	0/100	zjevná	1,22E-09	0	0	0	0
		20%	-	-	0	0	0	0	6,10E-10
C31	3,05E-09	40%	50/50	skrytá	0	6,10E-10	0	6,10E-10	0
		40%	0/100	zjevná	1,22E-09	0	0	0	0
		20%	-	-	0	0	0	0	6,10E-10
R35	1,00E-10	40%	0/100	zjevná	4,00E-11	0	0	0	0
		40%	50/50	zjevná	2,00E-11	0	2,00E-11	0	0
		20%	-	-	0	0	0	0	2,00E-11
R36	1,00E-10	40%	0/100	zjevná	4,00E-11	0	0	0	0
		40%	50/50	zjevná	2,00E-11	0	2,00E-11	0	0
		20%	-	-	0	0	0	0	2,00E-11
R37	1,00E-10	40%	0/100	zjevná	4,00E-11	0	0	0	0
		40%	50/50	zjevná	2,00E-11	0	0	2,00E-11	0
		20%	-	-	0	0	0	0	2,00E-11
TL1	2,80E-07	100%	0/100	zjevná	2,80E-07	0	0	0	0
TL2	2,80E-07	100%	0/100	zjevná	2,80E-07	0	0	0	0
TL3	2,80E-07	100%	0/100	zjevná	2,80E-07	0	0	0	0
Displej - LCD	1,00E-07	100%	0/100	zjevná	1,00E-05	0	0	0	0

Parcelace intenzity poruch λ na intenzity poruch λ_{DD}, λ_{DU}, λ_{SD}, λ_{SU}, λ_{NE}:

- λ_{DD} = porucha nebezpečná zjevná,
- λ_{DU} = porucha nebezpečná skrytá,
- λ_{SD} = porucha bezpečná zjevná,
- λ_{SU} = porucha bezpečná skrytá,
- λ_{NE} = porucha bez efektu.

Výpočet celkových intenzit poruch modulu displeje MD:

$$\lambda_{MD} = \sum_{i=1}^{n} \lambda_i = 9{,}47E^{-7}h^{-1} \tag{7.07}$$

$$\lambda_{DD_{MD}} = \sum_{i=1}^{n} \lambda_{DD_i} = 9{,}44E^{-7}h^{-1} \tag{7.08}$$

$$\lambda_{DU_{MD}} = \sum_{i=1}^{n} \lambda_{DU_i} = 1{,}83E^{-9}h^{-1} \tag{7.09}$$

$$\lambda_{SD_{MD}} = \sum_{i=1}^{n} \lambda_{SD_i} = 4{,}00E^{-11}h^{-1} \tag{7.10}$$

$$\lambda_{SU_{MD}} = \sum_{i=1}^{n} \lambda_{SU_i} = 1{,}85E^{-9}h^{-1} \tag{7.11}$$

$$\lambda_{NE_{MD}} = \sum_{i=1}^{n} \lambda_{NE_i} = 1{,}89E^{-9}h^{-1} \tag{7.12}$$

$$MTBF_{MD} = \frac{1}{\lambda_{MD}} = 1{,}06E^{6}h \tag{7.13}$$

7.6.2 PCA snímače

Výpočet pro systém, tedy pro snímač tlaku XMP i jako celek, je založen na sériovém modelu spolehlivosti a spočívá v součtu intenzit poruch jednotlivých modulů.

$$\lambda_{SYS} = \sum_{i=1}^{n} \lambda_{M_i} = 2{,}16E^{-6}h^{-1} \tag{7.14}$$

$$\lambda_{DD_{SYS}} = \sum_{i=1}^{n} \lambda_{DD_{Mi}} = 1{,}91E^{-6}h^{-1} \tag{7.15}$$

$$\lambda_{DU_{SYS}} = \sum_{i=1}^{n} \lambda_{DU_{Mi}} = 3{,}83E^{-8}h^{-1} \tag{7.16}$$

$$\lambda_{SD_{SYS}} = \sum_{i=1}^{n} \lambda_{SD_{Mi}} = 4{,}00E^{-11}h^{-1} \tag{7.17}$$

$$\lambda_{SU_{SYS}} = \sum_{i=1}^{n} \lambda_{SU_{Mi}} = 3{,}83E^{-8}h^{-1} \tag{7.18}$$

$$\lambda_{NE_{SYS}} = \sum_{i=1}^{n} \lambda_{NE_{Mi}} = 1{,}84E^{-7}h^{-1} \tag{7.19}$$

$$MTBF_{SYS} = \frac{1}{\lambda_{SYS}} = 4{,}63E^{5}h \tag{7.20}$$

7.7 Analýza důsledků nedetekovatelných poruch snímače pro režim nízkého vyžádání

Na základě hodnot intenzity nebezpečných detekovatelných a nedetekovatelných poruch spočítaných metodou PCA pro jednotlivé moduly systému a následně pro celý systém (snímač tlaku XMP i), je prováděn výpočet střední pravděpodobnosti výskytu nebezpečné poruchy při vyžádání (tedy hodnoty asymptotické/ustálené nepohotovosti U viz vzorec 4.11). Asymptotická nepohotovost U_D od nebezpečné poruchy je součtem složky asymptotické nepohotovosti U_{DD} od nebezpečné detekovatelné poruchy a složky asymptotické nepohotovosti U_{DU} od nebezpečné detekovatelné poruchy.

Složka asymptotické nepohotovosti U_{DD} od nebezpečné detekovatelné poruchy je vypočtena ze vztahu:

$$U_{DD} = \frac{MTTR_1}{MTTR_1 + MTBF_{DD_{SYS}}} = \frac{MTTR_1}{MTTR_1 + \frac{1}{\lambda_{DD_{SYS}}}} = \frac{8}{8 + 5{,}25E^{5}} = 1{,}52E^{-5} \tag{7.21}$$

Kde: $MTTR_1$ – je střední doba do obnovy stanovená expertním odhadem na 8h. Což reprezentuje skutečnost, že po zjištěné nebezpečné poruše je snímač opraven (nebo nahrazen novým) během jedné pracovní směny.

Složka asymptotické nepohotovosti U_{DU} od nebezpečné detekovatelné poruchy je vypočtena ze vztahu:

$$U_{DU} = \frac{MTTR_2}{MTTR_2 + MTBF_{DU_{SYS}}} = \frac{MTTR_2}{MTTR_2 + \frac{1}{\lambda_{DU_{SYS}}}} = \frac{4380}{4380 + 2{,}61E^{7}} = \\ = 1{,}68E^{-4} \tag{7.22}$$

Kde: $MTTR_2$ – je střední doba do obnovy a je závislá na intervalu zkoušek snímače tlaku XMP i prováděných k odhalení nedetekovatelných (skrytých) nebezpečných poruch snímače viz tab. 12. Pro Výpočet U_{DU} byl použit interval zkoušek jeden rok.

Tab. 12: Závislost hodnoty $MTTR_2$ na intervalu zkoušek snímače

Interval zkoušek snímače T_i [rok]	MTTR [h]
1	4380
2	8760
5	21900
10	43800

Platí:

$$MTTR_2 = \frac{T_i}{2} \tag{7.23}$$

Celková asymptotická nepohotovost U_D od nebezpečných poruch a za předpokladu zkoušek snímače tlaku prováděných s periodou 1 rok je dána vztahem:

$$U_{DD} = U_{DD} + U_{DU} = 1{,}52E^{-5} + 1{,}68E^{-4} = 1{,}83E^{-4} \tag{7.24}$$

7.8 Stanovení úrovně integrity bezpečnosti HW části snímače

V tomto bodě je nutné stanovení úrovně integrity bezpečnosti HW části snímače XMP i a to jak pro režim s nízkým vyžádáním PFD, tak i pro režim s vysokým či trvalým vyžádáním PFH. Pro tyto režimy platí:

a) pro pravděpodobnost výskytu poruchy za hodinu provozu – PFH pro režim s vysokým, popř. trvalým vyžádáním,

$$PFH = \lambda_{DU_{SYS}} + \lambda_{DD_{SYS}} = 1{,}94E^{-6} \tag{7.25}$$

b) pro střední pravděpodobnost výskytu nebezpečné poruchy při vyžádání funkce – PFD pro režim s nízkým vyžádáním (a intervalu zkoušek prováděných

s periodou 1 rok).

$$PFD = U_D = U_{DD} + U_{DU} = 1{,}83E^{-4} \tag{7.26}$$

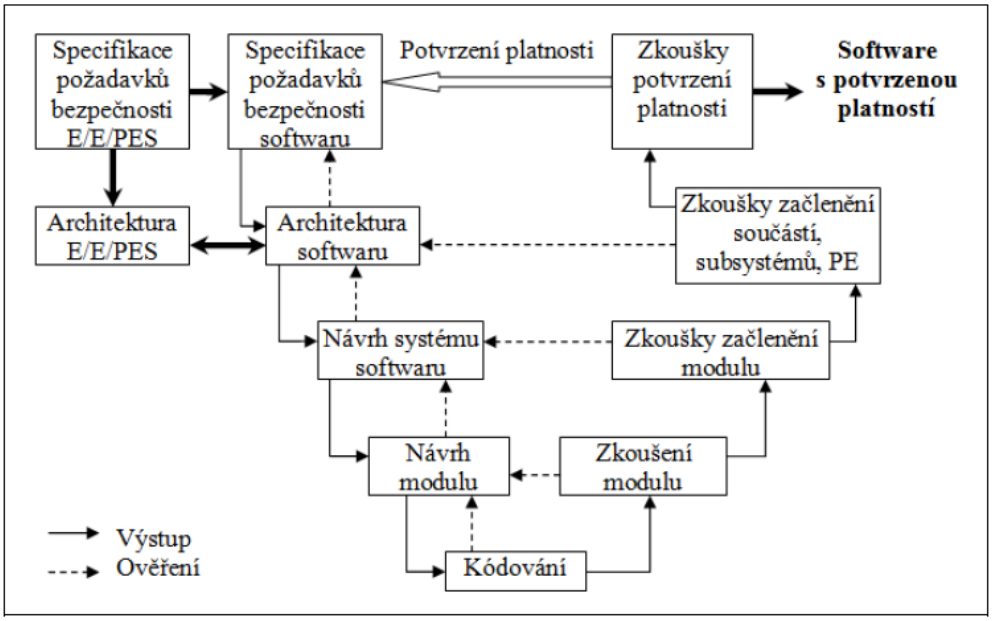
Tab. 13: Vypočítané hodnoty střední pravděpodobnosti výskytu nebezpečné poruchy při vyžádání funkce – PFD

Interval zkoušek snímače tlaku T_i [rok]	$MTTR_2$ [h]	PFD
1	4380	$1{,}83E^{-4}$
2	8760	$3{,}50E^{-4}$
5	21900	$8{,}53E^{-4}$
10	43800	$1{,}69E^{-3}$

7.9 Specifikace postupů pro tvorbu aplikačního SW snímače

Při tvorbě aplikačního SW snímače tlaku XMP i je nutné dodržet následující funkční kroky pro životní cyklus softwaru:

- získání požadavků na E/E/PE systémy související s bezpečností a příslušné části plánování bezpečnosti. Vhodná aktualizace plánování bezpečnosti během vývoje softwaru,
- stanovení architektury softwaru všech bezpečnostních funkcí přiřazených softwaru,
- prověření architektury hardwaru a softwaru i bezpečnostních důsledků vzájemných kompromisů v hardwaru a softwaru s vývojářem. Pokud je to nutné, tato etapa se opakuje,
- zahájení plánování a potvrzení platnosti bezpečnosti softwaru,
- návrh, vývoj a ověření softwaru podle:
  - plánování bezpečnosti softwaru,
  - úrovně integrity bezpečnosti softwaru,
  - životního cyklu bezpečnosti softwaru.



Obr. 31: Integrita bezpečnosti softwaru a životní cyklus vývoje softwaru [5]

- dokončení konečného ověření softwaru a začlenění ověřeného softwaru do cílového hardwaru a souběžná tvorba postupů pro uživatele a pracovníky údržby používaných při provozu systému,
- v součinnosti s vývojářem HW potvrzení platnosti softwaru v začleněných E/E/PE systémech souvisejících s bezpečností,
- předání výsledků potvrzení platnosti bezpečnosti softwaru systémovým inženýrem pro jeho další začlenění do celého systému,
- v případě, že software E/E/PES vyžaduje během doby svého provozního života modifikaci, potom se vhodným způsobem tato fáze provede.

Při realizaci výše uvedených kroku pro zajištění funkční bezpečnosti softwaru se volí bezpečnostní metody a techniky vhodné pro požadovanou úroveň integrity bezpečnosti dle předepsaných norem a to především dle normy ČSN EN 61508 [5]. V tabulkách 14 a 15 jsou uvedeny různé techniky a opatření z hlediska úrovní integrity bezpečnosti.

Tab. 14: Potvrzení platnosti bezpečnosti softwaru [5]

Technika/opatření	**SIL 1**	**SIL 2**	**SIL 3**	**SIL 4**
1. Pravděpodobnostní zkoušky	-	R	R	HR
2. Simulace a modelování	R	R	HR	HR
3. Funkční zkoušky a zkoušky typu „černé skříňky“	HR	HR	HR	HR
Pozn.: Číslem označená technika/opatření se musí zvolit podle úrovně integrity bezpečnosti.				

Tab. 15: Funkční zkoušky a zkoušky typu „černé skříňky“ [5]

Technika/opatření	**SIL 1**	**SIL 2**	**SIL 3**	**SIL 4**
1. Provádění zkušebních případů vycházející z diagramů příčin-následků	-	-	R	R
2. Prototypy/animace	-	-	R	R
3. Analýza mezních hodnot	R	HR	HR	HR
4. Zkoušení ekvivalentních tříd a segmentů dělených vstupů	R	HR	HR	HR
5. Simulace procesu	R	R	R	R
Pozn. Číslem označená technika/opatření se musí zvolit podle úrovně integrity bezpečnosti.				

U každé techniky/opatření je v tabulkách 12 a 13 uvedeno doporučení pro úrovně integrity bezpečnosti SIL 1 až 4. Interpretace těchto doporučení je následující:

- HR – technika/opatření pro tuto úroveň integrity bezpečnosti je velmi doporučené,
- R – technika/opatření pro tuto úroveň integrity bezpečnosti doporučené jako horší než doporučení HR,
- - technika/opatření, u kterých nejsou výrazná žádná pro a proti,
- NR – technika/opatření, která se pro tuto úroveň integrity bezpečnosti jednoznačně nedoporučují.

Pro účely diplomové práce (certifikace snímače tlaku na úroveň integrity bezpečnosti SIL 3) jsou vhodné metody v tabulkách 12 a 13 ve sloupci SIL 3 označeném šedou barvou. A to především metody „Simulace a modelování“, „Analýza mezních hodnot“ a „Zkoušení ekvivalentních tříd a segmentů dělených vstupů“.

8 ZHODNOCENÍ VÝSLEDKŮ

Z výsledků dosažených v této diplomové práci je zřejmé, že snímač tlaku XMP i splňuje úroveň integrity bezpečnosti SIL 3 pouze pro střední pravděpodobnost výskytu nebezpečné poruchy při vyžádání funkce – PFD pro režim s nízkým vyžádáním (dosahuje hodnoty $1{,}83E^{-4}$). Pro pravděpodobnost výskytu poruchy za hodinu provozu – PFH pro režim s vysokým, popř. trvalým vyžádáním snímač tlaku úroveň integrity bezpečnosti SIL 3 nesplňuje a pro tento režim vyhovuje pouze SIL 2 (dosahuje hodnoty $1{,}94E^{-6}$). To je způsobeno především modulem displeje MD, jehož velká část součástek disponuje relativně vysokou hodnotou intenzity poruch λ. Řešením je nahrazení těchto součástek součástkami s lepšími parametry bezporuchovosti. Zde je zároveň potřeba zmínit, že funkce modulu displeje je zařazena z důvodu konzervativního řešení mezi funkce kritické, ale reálně se jedná spíše o funkci doplňkovou. Druhým řešením dosažení úrovně SIL 3 i pro režim s vysokým, popř.

trvalým vyžádáním PFH je tedy možnost certifikování verze snímače tlaku bez displeje.

Při porovnání výsledků hodnot bezporuchovosti (MTBF, λ) dosažených metodou PCA a výsledků dosažených z provozních dat můžeme vidět, že hodnoty získané z provozu jsou o řád lepší. To lze přisuzovat například nepřesnému expertnímu odhadu intenzit poruch λ některých součástek a zvolenému konzervativnímu přístupu k řešení.

Relativně vysoký podíl nedetekovatelných nebezpečných poruch by mohl být snížen aplikováním účinného softwaru pro detekování poruch (vhodným algoritmem v řídícím procesoru elektroniky snímače tlaku XMP i). To by vedlo ke snížení hodnoty λ_{DU} a umožnilo tak prodloužit interval zkoušek funkčnosti snímače tlaku XMP i na 10 let při zachování úrovně integrity bezpečnosti SIL 3. Toto opatření by tedy umožnilo uživateli snížit náklady na údržbu snímače tlaku XMP i a zvýšilo konkurenceschopnost snímače tlaku XMP i.

9 ZÁVĚR

Tato diplomová práce se zabývá problematikou funkční bezpečnosti snímače tlaku BD SENSORS s.r.o. Cílem práce bylo stanovení úrovně integrity bezpečnosti (SIL) snímače tlaku XMP i.

V úvodu práce je nejdříve věnována pozornost získání teoretických znalostí v oboru funkční bezpečnosti a to především z normy ČSN EN 61508 [5] a norem z ní vycházejících. Mezi základní principy zakotvené v normách týkajících se funkční bezpečnosti patří vyváženost mezi opatřeními, které zajišťují bezpečnost a riziko. V této části práce jsou popsány základní pojmy a přístupy k funkční bezpečnosti.

Další část práce se zabývá teorií spolehlivosti a spolehlivostními analýzami. Pro řešení problematiky byla zvolena metoda FMEA/FMECA. Aby bylo možné vhodným způsobem zvládnout požadavky zadání (stanovení úrovně integrity SIL snímače tlaku XMP i) byla metoda FMEA/FMECA modifikována tak, aby umožnila kvantifikaci módů poruch pomocí hodnot intenzit poruch.

Poslední část práce popisuje realizaci zvoleného řešení. Popisuje princip vypracování metody FMECA, sestavení spolehlivostního modelu a výpočet potřebných parametrů bezporuchovosti modulů a následně celého snímače tlaku metodou PCA. Součásti je i výpočet parametrů bezporuchovosti pomocí dat z provozu snímače tlaku XMP i, který slouží k vzájemnému porovnání s výsledky dosaženými metodou PCA.

Cíle práce bylo dosaženo a to zjištěním, že snímač tlaku ve svém stávajícím provedení vyhovuje úrovni integrity bezpečnosti SIL 3 jen pro režim s nízkým vyžádáním PFD, pro režim s vysokým vyžádáním vyhovuje snímač tlaku XMP i pouze úrovni integrity bezpečnosti SIL 2.

Pro získání certifikátu je nutné, aby firma BD SENSORS zajistila tyto náležitosti:

- dosáhnout snížení intenzity poruch modulu displeje a tím docílit potřebné úrovně hodnoty PFH pro režim s vysokým vyžádáním pro certifikaci na úroveň SIL 3, či rozhodnout, že snímač tlaku XMP i bude splňovat úroveň integrity bezpečnosti SIL 3 jen pro verzi bez displeje,
- zkompletovat dokumentaci o zajišťování kvality, jak HW, tak SW části snímače tlaku XMP i),
- kompletní dokumentaci předložit příslušným certifikačním orgánům k certifikaci.

LITERATURA

[1] BABINEC, F. *Bezpečnostní inženýrství.*, Brno 2000 Učební text VUT v Brně (73 s.)

[2] BEDNAŘÍK, J.: *Technická spolehlivost v elektronické praxi.* Praha: SNTL, 1990. 336s. ISBN 80-03-00422-5

[3] BLECHA, P.: *Posuzování rizik u strojních zařízení.*[PDF dokument]. Prezentace pro SZÚ, s.p. Brno, 7.10.2008 [cit. 8. 1. 2009].

[4] ČSN EN ISO 31100:2010, *Management rizik – Principy a směrnice*

[5] ČSN EN 61508:2011, *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systému souvisejících s bezpečností*

[6] ČSN EN 61511: 2005, *Funkční bezpečnost*. *Bezpečnostní přístrojové systémy pro sektor průmyslových procesů*

[7] ČSN EN 62061:2005, *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností.*

[8] ČSN EN ISO 13849-1:2006, *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci.*

[9] ČSN EN 50126-1:2001, *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Základní požadavky a generický proces*

[10] ČSN IEC 50(191):1993, *Mezinárodní elektrotechnický slovník – kapitola 191: Spolehlivost a jakost služeb*

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

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

[13] ČSN IEC 61513:2003, *Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Všeobecné požadavky na systém*

[14] ISO 26262-9:2011, *Road vehicles – Functional safety – Part 9: Automotive Safety Integrity Level (ASIL) – oriented and seafetx-oriented analyses*

[15] FUCHS, P.: *Pravděpodobnostní hodnocení rizika.,* In: Sb. semináře „Spolehlivost a analýza rizik“ odborné skupiny pro spolehlivost při ČSJ. Česká společnost pro jakost (ČSJ), Praha 2003

[16] HLAVIČKA, J.: *Diagnostika a spolehlivost.* Elektronická skripta. Praha: ČVUT, 1998. 153s.

[17] HOLUB, R., VINTR, Z.: Spolehlivost letadlové techniky. Elektronická skripta. Brno: VUT FSI, 2001. 233s.

[18] JIRGL, M.: *Spolehlivost technických systémů*. Brno: VUT, Fakulta elektrotechniky a komunikačních technologií, 2010. 76s.

[19] LEITL, R.: *Spolehlivost elektrotechnických systémů*. Praha: SNTL, 1990. 288s. ISBN 80-03-00408-X

[20] MYKISKA, A.: *Bezpečnost a spolehlivost technických systémů*, 2 přepracované vydání, Praha: Nakladatelství ČVUT, 2006. 206s. ISBN 80-01-02868-2.

[21] MYKISKA, A.: *Bezpečnost strojů a výrobních systémů.* [online], [cit. 2009-2-22]. Dostupné z: <http://www.josef.posta.sweb.cz/KONF/Mykiska.doc>

[22] POLSTEROVÁ, H.: *Spolehlivost v elektrotechnice.* Vysokoškolská skripta. Brno: VUT, 2003

[23] ŠIMONÍK, M.: *Funkční bezpečnost v průmyslu.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2015. 60s Vedoucí semestrální práce doc. Ing. Pavel Fuchs, CSc.

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

[25] ZAJÍČEK, J.: *Porovnání přístupů stanovení funkční bezpečnosti*, In: Sb. semináře „Bezpečnost a spolehlivost nových technologií“ odborné skupiny pro spolehlivost při ČSJ. Česká společnost pro jakost (ČSJ), Praha 2013

PŘÍLOHY

Příloha A: Analýzy spolehlivosti a jejich průvodní dokumentace v elektronické formě

Příloha A obsahuje následující části:

- 1 XMP_i_FMECA_PCA – analýza FMECA a PCA snímače tlaku XMP i
- 2 XMP_i_katalog – katalogové listy snímače tlaku XMP i
- 3 DSP411_modul_senzoru – výkresová dokumentace modulu senzoru
- 4 ELI22_4-modul_analog_vystup – výkresová dokumentace modulu analogového výstupu
- 5 ELI20_5s-modul_elektroniky_senzoru – výkresová dokumentace modulu elektroniky senzoru
- 6 ELI22_4-modul_displeje – výkresová dokumentace modulu displeje
- 7 ELI22_4-modul_HART – výkresová dokumentace modulu digitální komunikace
- 8 ELI22_4-modul_napajeni – výkresová dokumentace modulu napájení
- 9 ELI22_4-modul_procesoru – výkresová dokumentace modulu procesoru
- 10 Data_z_provozu – získaná data z provozu snímače tlaku XMP i
- 11 Sestava_XMP_i – sestava snímače tlaku XMP i

Příloha B: CD ROM s elektronickou formou diplomové práce