VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV AUTOMOBILNÍHO A DOPRAVNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF AUTOMOTIVE ENGINEERING

ZHODNOCENÍ SOUČASNÝCH TECHNOLOGIÍ V ZAJIŠŤOVÁNÍ FUNKČNÍ BEZPEČNOSTI STROJNÍCH ZAŘÍZENÍ

EVALUATION OF PRESENT TECHNOLOGIES IN ENSURING FUNCTIONAL SAFETY OF MACHINERY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE ŠTĚPÁN SMETANA
AUTHOR

VEDOUCÍ PRÁCE ING. JIŘÍ ZAHÁLKA
SUPERVISOR

BRNO 2014

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav automobilního a dopravního inženýrství
Akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

student(ka): Štěpán Smetana

který/která studuje v **bakalářském studijním programu**

obor: **Stavba strojů a zařízení (2302R016)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Zhodnocení současných technologií v zajišťování funkční bezpečnosti strojních zařízení

v anglickém jazyce:

Evaluation of present technologies in ensuring functional safety of machinery

Stručná charakteristika problematiky úkolu:

V současné době je bezpečnost velice důležitým faktorem ve výrobním procesu. Funkční bezpečnost strojních zařízení je poté velice důležitá vzhledem k ochraně zaměstnanců a majetku podniku. Výrobci proto musí neustále zlepšovat stávající a vyvíjet nové technologie pro zajišťování funkční bezpečnosti.

Cíle bakalářské práce:

Zpracování literární rešerše a přehledu technologií pro zajišťování funkční bezpečnosti strojních zařízení.

Seznam odborné literatury:

[1]SMITH, David John a Kenneth G SIMPSON. Functional safety: a straightforward guide to IEC 61508 and related standards. 2nd ed. Boston: Elsevier, 2004, p. cm. ISBN 07-506-6269-7
[2]ČSN EN ISO 13849-x: Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů. [s.l.]: ÚNMZ
[3]ČSN EN 61508-x: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. [s.l.]: ÚNMZ
[4]ČSN EN 62061: Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností. [s.l.]: ÚNMZ

Vedoucí bakalářské práce: Ing. Jiří Zahálka

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2013/2014.

V Brně, dne 18.11.2013

L.S.

prof. Ing. Václav Píštěk, DrSc. Ředitel ústavu	doc. Ing. Jaroslav Katolický, Ph.D. Děkan fakulty

ABSTRAKT

Tato bakalářská práce se zabývá funkční bezpečností jako celkem. V první části práce je nastíněno, co bychom si pod pojmem funkční bezpečnost mohli představit a proč bychom se jí měli věnovat. Práce také obsahuje seznámení s prvky používajícími se v rámci funkční bezpečnosti a jejich stručným popisem. Je zde popsán postup stanovení úrovně vlastností PL a úrovně integrity SIL pro strojní zařízení, tenhle postup je pak prakticky ukázán na příkladu pro funkci nouzového zastavení.

KLÍČOVÁ SLOVA

Funkční bezpečnost, bezpečnostní prvky, strojní zařízení, úroveň integrity, úroveň vlastností, bezpečnostní funkce

ABSTRACT

This bachelor’s thesis is concerning functional safety as a whole. The first part of the paper will provide a description of what we can imagine under the term of functional safety and why we should pay attention to it. The document also includes introduction of safety components used in a frame of functional safety and its brief description. You can find here methodical approach to calculation of performace level PL and safety integrity level SIL, this calculation is shown on an example of an emergency stop function.

KEYWORDS

Functional safety, machinery, safety components, performance level, safety integrity level, safety function

BIBLIOGRAFICKÁ CITACE

SMETANA, Štěpán. *Zhodnocení současných technologií v zajišťování funkční bezpečnosti strojních zařízení*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2014. 47 s. Vedoucí bakalářské práce Ing. Jiří Zahálka.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracoval jsem ji samostatně pod vedením Ing. Jiřího Zahálky a s použitím literatury uvedené v seznamu.

V Brně dne 30. května 2014 ……..……..……..

Štěpán Smetana

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce Ing. Jiřímu Zahálkovi za účinnou metodickou a odbornou pomoc a za další cenné rady při zpracování mé bakalářské práce.

OBSAH

Úvod 9
1 Úvod do funkční bezpečnosti 10
2 Právní rámec + Legislativní podpora 12
2.1 ČSN EN ISO 62061 15
2.1.1 Definice vybraných pojmů [4] 15
2.1.2 Postup a strategie stanovení SIL [4] 17
2.2 ČSN EN ISO 13849 – 1 20
2.2.1 Definice vybraných pojmů [5] 21
2.2.2 Obecný postup určení PL [5] 22
2.3 ČSN EN 61508 – 1 25
2.3.1 Definice vybraných pojmů [7] 25
3 Prvky používané v oblasti funkční bezpečnosti 27
3.1 Vstupní prvky 27
3.1.1 Blokovací zařízení ochranných krytů 27
3.1.2 Tlačítko nouzového zastavení 29
3.1.3 Dvouruční ovládání 30
3.1.4 Světelné bariéry + nášlapné rohože 31
3.2 Logické prvky 32
3.2.1 Bezpečnostní relé 32
3.2.2 PLC 34
3.2.3 Řídicí systémy 34
3.3 Výstupní prvky 35
3.3.1 Stykače 35
3.3.2 Relé 36
4 Stanovení PL a SIL 37
4.1 Stanovení PL pro bezpečnostní funkci nouzového zastavení 37
4.2 Stanovení SIL pro bezpečnostní funkci nouzového zastavení 40
Závěr 43
Seznam použitých zkratek a symbolů 46

ÚVOD

Cílem této bakalářská práce je vysvětlit problematiku funkční bezpečnosti, která je v dnešní době velice důležitou součástí strojního průmyslu a je nutné věnovat se jí už ve fázích výroby stroje.

V první části bakalářské práce vysvětlím co to vlastně funkční bezpečnost je a proč bychom se jí měli věnovat. Pro lepší představu slouží uvedení praktických příkladů.

Další část práce se zabývá normami, které se užívají v oblasti funkční bezpečnosti a to konkrétně ČSN EN 61508-1, ČSN EN 13849-1 a ČSN EN 62061. Je zde uveden jejich stručný popis a definice několika vybraných důležitých pojmů. Velkou část téhle kapitoly tvoří popis postupu stanovení úrovně vlastností PL podle normy ČSN EN 13849-1 a úrovně integrity SIL dle ČSN EN 62061.

Prvky používané v oblasti funkční bezpečnosti je téma další části práce. Je několik způsobů jak zajistit funkční bezpečnost strojních zařízení a existuje několik prvků, které nám s tím pomáhají. V téhle kapitole je uveden stručný popis a charakteristika vybraných vstupních, logických a výstupních prvků. Vybrány byly základní bezpečnostní prvky pro danou skupinu.

V poslední kapitole téhle práce je uveden postup stanovení úrovně vlastností PL a úrovně integrity SIL na praktickém příkladu pro funkci bezpečnostního zastavení.

1 ÚVOD DO FUNKČNÍ BEZPEČNOSTI

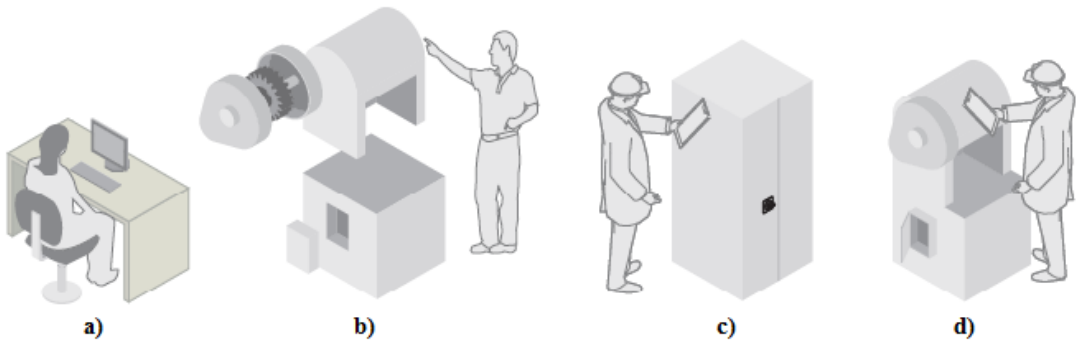
Definici bezpečnosti si můžeme vyložit jako vyloučení určitého rizika. Je ale prakticky nemožné vyloučit riziko kompletně, vždy nějaké riziko zbude. Je ale nutné tohle riziko omezit na co nejnižší úroveň, kterou pak můžeme označit jako přijatelnou. Tenhle proces mají na starost bezpečnostní systémy. Ale i když použijeme tu nejlepší techniku, nemusí to být nic platné, pokud do úvahy nezapočítáme lidský faktor. Právě lidský faktor má na svědomí asi 90% nehod a úrazů. Tahle statistika vyplívá z průzkumu Evropské komise, která nasbírala údaje o nehodách v chemickém průmyslu od roku 1982 do současnosti. Z největší části se jednalo o chyby v organizaci práce nebo nedodržení pravidel [1].

Pojem funkční bezpečnost byl poprvé představen v roce 1998 v normě IEC 61508. Od té doby byl tenhle termín občas spojován pouze s programovatelnými bezpečnostními systémy. Tohle ale samozřejmě je špatný úsudek. Funkční bezpečnost zahrnuje širokou škálu zařízení, které jsou používány k vytvoření bezpečnostního systému. Jedná se o zařízení, jako jsou například blokovací zařízení, světelné závory, bezpečnostní relé popřípadě stykače a bezpečnostní ovladač. Tyhle zařízení jsou poté propojeny s bezpečnostním systémem, který na základě obdrženého signálu provede určité bezpečnostní opatření.

Nejlíp si můžeme funkční bezpečnost vysvětlit na nějakém příkladu. Vezměme si jako příklad ochranu proti přehřátí motoru, kde za pomoci teplotního čidla umístěného ve vinutí elektromotoru dojde k vypnutí předtím, než se stihne motor přehřát. Tohle je jednoduchý příklad funkční bezpečnosti. Naproti tomu použití speciální izolace, která je navržena k odolání vysokým teplotám nemůžeme považovat za příklad funkční bezpečnosti (i když se pořád jedná o příklad zvýšení bezpečnosti a může chránit před stejným problémem).

Proč bychom se měli věnovat funkční bezpečnosti?

Existuje spousta zákonů, které vyžadují od zaměstnavatelů zajištění funkční bezpečnosti strojů a pádné ekonomické důvody pro prevenci nehod. Pokud se chceme vyvarovat rizikům vzniku nehod, je třeba se funkční bezpečností zabývat již ve fázi návrhu a výroby stroje. Stroj je poté nutné kontrolovat po celý jeho životní cyklus, který zahrnuje instalaci, seřizování, provoz, údržbu a případně i likvidaci.



Obr. 1 Životní cyklus stroje a) Návrh/Výroba b) Instalace c) Seřizování/Provoz d) Údržba [1]

Minimální požadavky na bezpečnost a ochranu zdraví pro používání pracovního zařízení jsou uvedeny ve směrnici 89/655/EHS (NV/378/2001 Sb.). Podle téhle směrnice se musí každý zaměstnavatel řídit a má povinnost provozovat strojní zařízení ve shodě s touhle směrnicí. Vztahuje se na používání všech zařízení, včetně mobilních a zdvihacích zařízení. Vyžaduje způsobilost k provozu všech zařízení. Je nutné poté pravidelnými kontrolami a údržbou tuhle způsobilost u strojů zajistit [2].

Dalším důvodem jsou finance a náklady z důvodu nehod a také samozřejmě zajištění bezpečí zaměstnanců. Pokud se stane nějaká nehoda, zaměstnavatel je povinen uhradit nemocenskou pro zraněné zaměstnance. Úřad pro bezpečnost a ochranu zdraví ve Velké Británii (HSE) uvádí jako příklad nehodu, která se stala u vrtačky. Tahle nehoda podnik celkově přišla na 45 000 liber (cca 51 300 eur). Tahle částka ale nezahrnovala řadu méně zřejmých nákladů, takže některé výpočty tuto částku až zdvojnásobují. Jako další příklad můžeme použít nehodu analyzovanou společností Schneider Electric, kde došlo k úrazu hlavy zaměstnance, tahle nehoda přišla firmu na cca 90 000 liber (102 000 eur). Je proto nutné se takovým nehodám vyvarovat, jelikož celkový finanční dopad může zahrnovat jak zvýšení pojistného a výrobní ztráty, tak také ztrátu zákazníků a reputace. Nemluvě o tom, jak důležitá je funkční bezpečnost z hlediska ochrany zdraví zaměstnanců [2].

Funkční bezpečnost má také pozitivní vliv na pohodlí zaměstnanců a pracovní produktivitu, kolikrát také může přispět k jejímu zvýšení. Jako příklad můžeme uvést užití světelných bariér, které slouží k ochraně přístupových zón strojů a zároveň usnadňují proces vkládání a vyjímání předmětů. Za velkou výhodu použití těchhle bariér můžeme považovat zónování oddělovacích zařízení, které umožňují vypnout určitou část stroje za účelem údržby a nechat ostatní části stroje v chodu.

2 PRÁVNÍ RÁMEC + LEGISLATIVNÍ PODPORA

Co je to Norma? Je to technická specifikace, která je schválená uznávaným normalizačním orgánem pro opakované nebo stálé používáni. Harmonizovanou se norma stává poté, co je vydána ve všech členských státech Evropské unie.

Odpovědnost výrobce

Výrobci, kteří uvádějí své stroje na trh evropské unie, musí jednat v souladu se směrnicí o strojních zařízeních. Výraz „uvedení na trh“ zahrnuje také případy, kdy společnost dodá stroj sama sobě – tedy vyrobí nebo upraví stroj pro své účely, a případy, kdy společnost vyveze stroj do EU [2].

Odpovědnost uživatele

Uživatel má povinnost přesvědčit se, zda mají zakoupené stroje označení CE a zda má k dispozici prohlášení o shodě s požadavky směrnice o strojních zařízeních. Stroje musí být užívány v souladu s pokyny výrobce.

Stroje, které byly uvedeny do provozu před začátkem platnosti směrnice o strojních zařízeních, nemusí být s touto směrnicí ve shodě.

Úpravy strojů lze považovat za výrobu nových strojů. Společnost, která stroj upravuje, si musí být vědoma toho, že bude možná muset vydat nové prohlášení o shodě a označení CE [2].

Uvádění výrobků na trh

Zákon 22/1997 Sb., který stanovuje:

a) Způsob stanovování technických požadavků na výrobky, které by mohly ohrozit zdraví nebo bezpečnost osob, majetek nebo přírodní prostředí – tzv. oprávněný zájem,
b) Práva a povinnosti osob, které uvádějí na trh výrobky, které by mohli ohrozit oprávněný zájem,
c) Práva a povinnosti osob pověřených k činnostem, které souvisí s tvorbou a uplatňováním českých technických norem nebo se státním zkušebnictvím.

Zákon nám říká, že bezpečný výrobek je takový výrobek, kde při jeho užívání za běžných podmínek při stanovené použivatelnosti nehrozí žádné nebezpečí nebo hrozí pouze minimální [3].

Normy pro bezpečnost strojních zařízení dělíme do následujících skupin:

- Normy typu A základní bezpečnostní normy
  - Uvádějí základní pojmy, konstrukční principy a všeobecná hlediska, která se dají aplikovat na všechna strojní zařízení.

- Normy typu B obecné bezpečnostní normy
  - Zabývají se jedním nebo více bezpečnostními hledisky nebo jedním nebo více typy ochranných zařízení, která mohou být použita pro větší počet strojních zařízení.
  - Normy typu B se dále dělí na:
    - Normy typu B1 – zabývají se konkrétními bezpečnostními faktory (například teplota povrchu, hluk, bezpečné vzdálenosti)
    - Normy typu B2 – zabývají se konkrétními bezpečnostními prvky (například blokovací zařízení, ochranné kryty)

- Normy typu C bezpečnostní normy strojních zařízení
  - Určují podrobné bezpečnostní požadavky na konkrétní stroj nebo skupinu strojů.

Norma typu C má přednost vždy pokud se její ustanovení nějak liší od normy typu A nebo B.

Závaznost jednotlivých norem je dána jejich vyhlášením ve Věstníku jako norem harmonizovaných (popřípadě norem určených) i když splnění základních požadavků stanovených evropskými směrnicemi nebo nařízením vlády je možné prokázat i jiným způsobem než těmito normami. Tahle možnost nebývá výrobci ke složitosti legislativního řešení využívána.

Tab. 1 Příklady typů norem [2]

Tabulka s příklady typů norem:		
EN/ISO 12100	A	Bezpečnost strojních zařízení – Zásady pro posouzení a snížení rizika
EN 574	B	Dvouruční ovládací zařízení – Funkční hlediska – zásady pro konstrukci
EN/ISO 13850	B	Nouzové zastavení – Zásady pro konstrukci
EN/IEC 62061	B	Funkční bezpečnost elektronických a programovatelných řídících systémů souvisejících s bezpečností
EN/ISO 13849-1	B	Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci
EN 349	B	Nejmenší mezery k zamezení stlačení částí lidského těla
EN/ISO 13857	B	Bezpečnost strojních zařízení – Bezpečné vzdálenosti k zamezení dosahu k nebezpečným místům horními a dolními

		končetinami
EN/IEC 60204-1	B	Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 1: Všeobecné požadavky
EN 999/ISO 13855	B	Umístění ochranných zařízení s ohledem na rychlosti přiblížení částí lidského těla
EN 1088/ISO 14119	B	Blokovací zařízení spojená s ochrannými kryty – Zásady pro konstrukci a volbu
EN/IEC 61496-1	B	Elektrická snímací ochranná zařízení – Část 1: Všeobecné požadavky a zkoušky
EN/IEC 60947-5-5	B	Spínací a řídící přístroje nn – Část 5-5: Přístroje a spínací prvky řídících obvodů – Přístroje pro nouzové zastavení s mechanickým zajištěním
EN 842	B	Vizuální signály nebezpečí – Všeobecné požadavky, navrhování a zkoušení
EN 1073	B	Zamezení neočekávanému spuštění
EN 953	B	Všeobecné požadavky pro konstrukci a výrobu pevných a pohyblivých ochranných krytů
EN 201	C	Stroje pro zpracování pryže a plastů – Vstřikovací stroje – Bezpečnostní požadavky
EN 692	C	Obráběcí a tvářecí stroje – Mechanické lisy – Bezpečnost
EN 693	C	Obráběcí a tvářecí stroje – Bezpečnost – Hydraulické lisy
EN 289	C	Stroje pro zpracování pryže a plastů – Bezpečnost – Vyfukovací tvářecí stroje používané na výrobu dutých předmětů – Požadavky na konstrukci a stavbu
EN 422	C	Vyfukovací tvářecí stroje používané na výrobu dutých předmětů – Požadavky na konstrukci a stavbu
EN/ISO 10218-1	C	Roboty pro výrobní prostředí – Požadavky na bezpečnost – Část 1: Robot
EN 415-4	C	Bezpečnost balících strojů – Část 4: Paletizátory a depaletizátory
EN 619	C	Kontinuální manipulační zařízení a systémy – Požadavky na bezpečnost a elektromagnetickou kompabilitu na zařízení pro mechanickou manipulaci manipulačních jednotek

2.1 ČSN EN ISO 62061

Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností

Obecný úvod

Stanovuje požadavky a uvádí doporučení na návrh, začlenění a potvrzení platnosti (validace) elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností (SRECS) určených pro stroje. Platí pro řídicí systémy použité buďto jednotlivě nebo v kombinaci pro zajištění bezpečnostních řídicích funkcí strojů, které nejsou při své činnosti přenosné, včetně skupin strojů koordinovaně společně pracujících [4].

Tato norma se týká pouze požadavků na funkční bezpečnost týkající se snížení rizika poranění nebo poškození zdraví osob v bezprostřední blízkosti stroje a požadavků přímo souvisejících s používáním stroje. Je omezena na rizika vznikající přímo z nebezpečí samotného stroje nebo ze skupiny strojů pracující koordinovaně společně [4].

2.1.1 DEFINICE VYBRANÝCH POJMŮ [4]

řídicí systém stroje (machine control system)

- systém, který reaguje na vstup (obsluha, proces, vnější řídicí zařízení atd.) a generuje výstupy tak aby se stroj choval určeným způsobem

elektrický řídicí systém (electrical control system)

- všechny elektrické, elektronické a programovatelné elektronické části řídicího systému stroje použité např. pro zajištění funkčního řízení nebo ochranné a řídicí funkce související s bezpečností

elektrický řídicí systém související s bezpečností SRECS (Safety-Related Electrical Control System)

- elektrický řídicí systém stroje, jehož porucha může vést k okamžitému nárůstu rizika (může zahrnovat jak elektrické napájecí obvody, tak i řídící obvody)

subsystém (subsystem)

- první úroveň dělení systému = entita konstrukční architektury SRECS jejíž porucha má za následek poruchu SRECS. Části vznikající dalším dělením subsystému se nazývají „prvky subsystému“

funkční bezpečnost (functional safety)

- část celkové bezpečnosti stroje a řídicího systému stroje závislá na správném fungování SRECS, systémech souvisejících s bezpečností založených na jiných technických principech a vnějších prostředcích pro snížení rizika

řídicí funkce (control function)

- funkce, která vyhodnocuje vstupní informace nebo signály a vyvolává výstupní informace nebo činnosti

řídicí funkce související s bezpečností SRCF (Safety-Related Control Function)

- řídicí funkce realizovaná v rámci SRECS s předepsanou úrovní integrity určená pro zachování bezpečnosti stroje nebo pro zabránění okamžitému zvýšení rizika

diagnostická funkce SRECS (SRECS diagnostic function)

- funkce určená pro detekci poruchových stavů uvnitř SRECS a pro vyvolání předepsané výstupní informace nebo činnosti při detekci poruchového stavu

úroveň integrity bezpečnosti SIL (Safety Integrity Level)

- diskrétní úroveň (1 z 3) pro stanovení požadavků úrovně integrity bezpečnosti SRCF, které mají být přiřazeny k SRECS, kdy SIL 3 má nejvyšší úroveň bezpečnosti a SIL 1 nejnižší (existuje i vyšší úroveň bezpečnosti SIL 4, ta se zde neuvažuje, neboť nesouvisí se snižováním rizika normálně souvisejícím se stroji)

diagnostické pokrytí DC (diagnostic coverage)

- snížení pravděpodobnosti nebezpečných poruch hardwaru (technické vybavení) v důsledku provádění automatických diagnostických testů

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

podíl bezpečných poruch SFF (Safe Failure Fraction)

- podíl celkové intenzity poruch subsystému, který nemá za následek nebezpečnou poruchu

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

pravděpodobnost nebezpečné poruchy za hodinu $\boldsymbol{PFH_D}$ (Probability of Dangerous Failure per Hour)

- střední pravděpodobnost nebezpečné poruchy za 1h

střední doba do nebezpečné poruchy $\boldsymbol{MTTF_D}$ (Mean Time to Dangerous Failure)

- očekávaná střední doba do nebezpečné poruchy

2.1.2 POSTUP A STRATEGIE STANOVENÍ SIL [4]

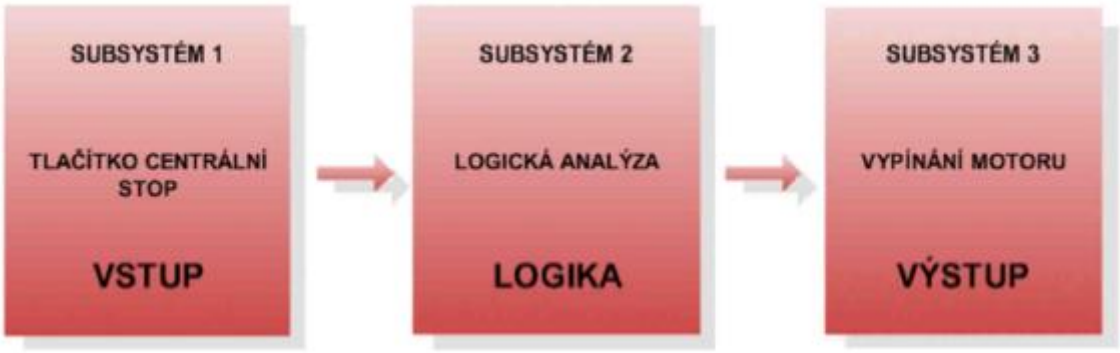
Krok 1 Stanovení požadované úrovně SIL CL

Na základě posouzení rizik je třeba stanovit požadovanou úroveň integrity bezpečnosti SIL. Odhad rizika by měl být proveden pro každé nebezpečí určením prvků rizika, které jsou znázorněny na obrázku Obr. 2.

Obr. 2 Prvky rizika [2]

Krok 2 Určení funkčního bloku bezpečnostní funkce

Funkční blok je výsledkem detailního rozboru funkce spojené s bezpečností. Ze struktury funkčních bloků vychází koncept architektury SRECS. Bezpečnostní požadavky každého bloku jsou odvozeny ze specifikace bezpečnostních požadavků odpovídající řídicí funkce související s bezpečností [2].



Obr. 3 Struktura funkčních bloků

Krok 3 Přiřazení bloků jednotlivým subsystémům

Každý funkční blok musí být přiřazen k subsystému. Každý subsystém může obsahovat více funkčních bloků. Součástí subsystému mohou být podřízené prvky i vlastní diagnostické funkce. Subsystém musí mít alespoň stejnou úroveň SIL, jako celá řídicí funkce související s bezpečností [2].

Krok 4 Výběr součástí subsystému

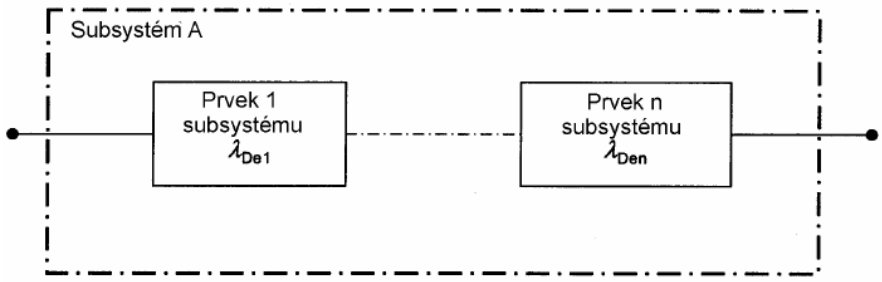
Výběr konkrétních výrobků ke každému subsystému. Potřebné údaje jako počet operací, procento nebezpečných poruch a životnost poskytne výrobce zařízení.

Krok 5 Návrh diagnostické funkce

Architektura A - nulová odolnost proti vadám bez diagnostické funkce

Pravděpodobnost nebezpečné poruchy:

$$\lambda_{DssA} = \lambda_{De1} + \ \ldots . + \lambda_{Den} \tag{1}$$



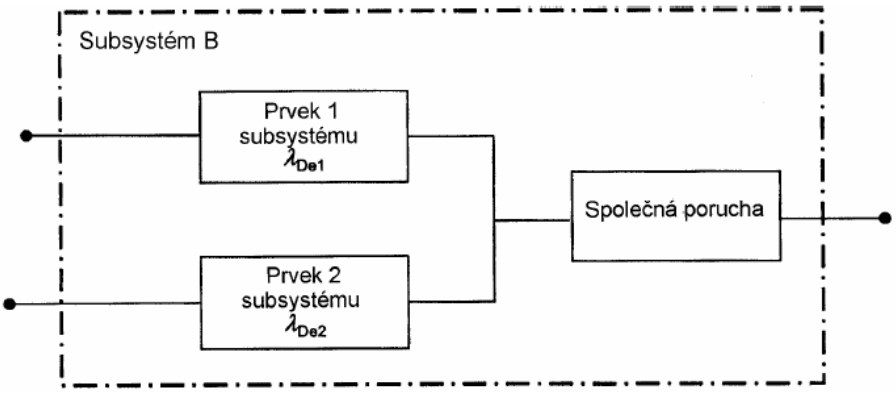
Obr. 4 Logické znázornění subsystému A [4]

Architektura B – odolnost proti jednotlivé vadě bez diagnostické funkce

Pravděpodobnost nebezpečné poruchy:

$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times \frac{(\lambda_{De1} + \lambda_{De2})}{2} \tag{2}$$

$$PFH_{DssB} = \lambda_{DssB} \ \times 1h \tag{3}$$



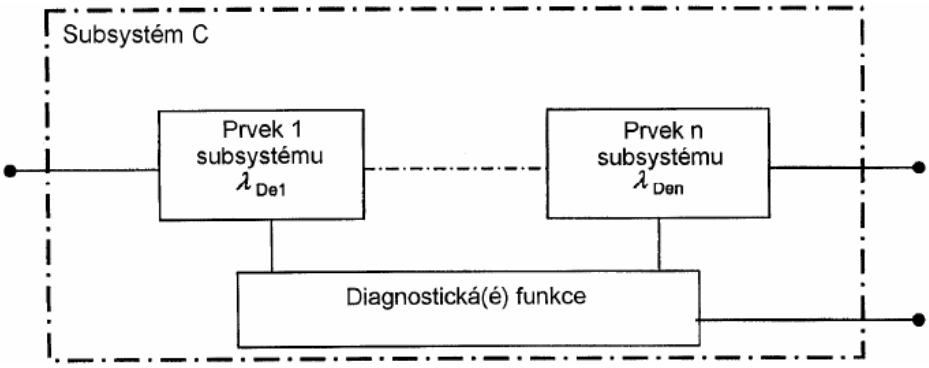
Obr. 5 Logické znázornění subsystému B [4]

Architektura C - nulová odolnost proti vadám s diagnostickou funkcí

Pravděpodobnost nebezpečné poruchy:

$$\lambda_{DssB} = \lambda_{De1}(1 - DC_1) + \ \ldots . + \lambda_{Den}(1 - DC_n) \tag{4}$$

$$PFH_{DssC} = \lambda_{DssC} \ \times 1h \tag{5}$$



Obr. 6 Logické znázornění subsystému C [4]

Architektura D – odolnost proti jednotlivé vadě s diagnostickou funkcí

Prvky subsystému rozdílné konstrukce

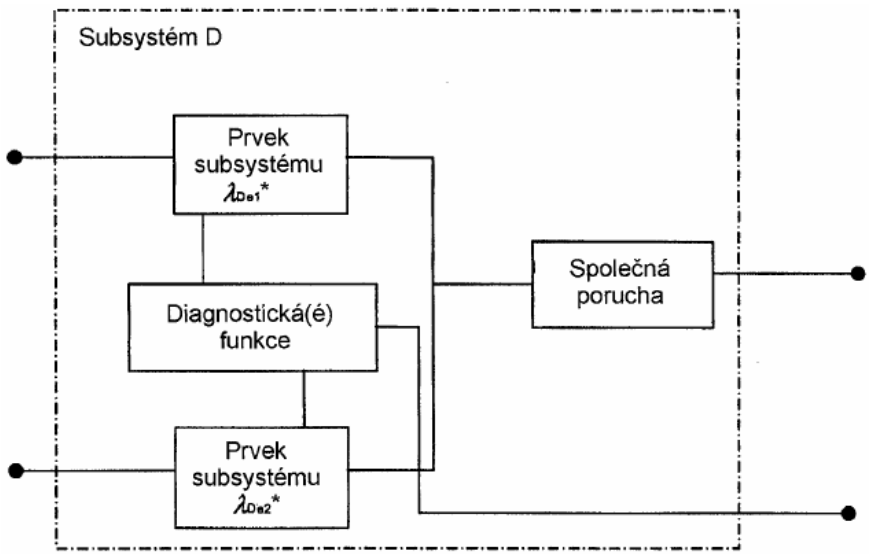
$$\lambda_{DssD} = (1-\beta)^2\{[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)]\} \times \frac{T_2}{2} + \left\{[\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 + DC_2)] \times \frac{T_1}{2}\right\} + \beta \ \times \frac{(\lambda_{De1} + \lambda_{De2})}{2} \tag{6}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h \tag{7}$$

Prvky subsystému stejné konstrukce

$$\lambda_{DssD} = (1-\beta)^2\left[\lambda_{De}{}^2 \times 2 \times DC\right] \times \frac{T_2}{2} + \left\{\left[\lambda_{De}{}^2 \times (1-DC) \times T_1\right]\right\} + \beta \times \lambda_{De} \tag{8}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h \tag{9}$$



Obr. 7 Logické znázornění subsystému D [4]

2.2 ČSN EN ISO 13849 – 1

Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci

Obecný úvod

Od července 2007 nahrazuje dosud používanou normu ČSN EN 954-1.

Norma slouží jako návod pro lidi zabývající se konstrukcí ovládacích systémů. Obsahuje bezpečnostní požadavky a pokyny pro zásady konstrukce a integrace bezpečnostních částí ovládacích systémů (SRP/CS), včetně návrhu software. Norma se uplatňuje v rámci bezpečnostních částí řídicích systémů strojních zařízení pro všechny druhy technologie a užívané energie. Norma neuvádí požadavky na konstrukci výrobků, které jsou součástí ovládacích systémů [5].

Přichází s novým způsobem výpočtu bezpečnostních obvodů, který dává lepší povědomí o tom, jak je bezpečnější technika implementována.

2.2.1 DEFINICE VYBRANÝCH POJMŮ [5]

Bezpečnostní část ovládacího systému (safety-related part of a control system SRP/CS)

- jedná se o část ovládacího systému, která reaguje na bezpečnostní vstupní signály a vytváří bezpečnostní výstupní signály

Kategorie (category):

- klasifikace bezpečnostních částí ovládacího systému vzhledem k odolnosti proti závadám a jejich následnému chování v podmínce závady, kterého je dosaženo konstrukčním uspořádáním částí, detekcí závady a/nebo jejich spolehlivostí

Porucha (failure):

- ukončení schopnosti objektu plnit požadovanou funkci

Nebezpečná porucha (dangerous failure)

- porucha která má potenciál uvést bezpečnostní části ovládacího systému do stavu nebezpečí nebo selhání funkce

Porucha se společnou příčinou (common cause failure (CCF))

- poruchy různých objektů, vyplývající z jedné události, kde tyto poruchy nejsou vzájemným důsledkem každé z nich

Úroveň vlastností (performance level (PL))

- diskrétní úroveň používaná k určení schopností bezpečnostních částí ovládacích systémů k vykonávání bezpečnostní funkce při předvídatelných podmínkách

Požadovaná úroveň vlastností (required performance level (PL_r))

- úroveň vlastností (PL) používaná k tomu, aby bylo dosaženo pro každou bezpečnostní funkci požadovaného snížení rizika

Diagnostické pokrytí (diagnostic coverage (DC))

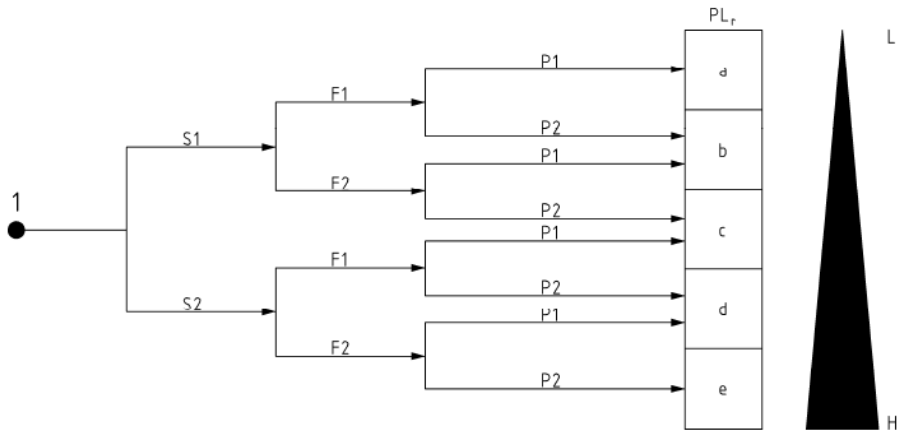
- míra účinnosti diagnostiky, která může být určena jako podíl intenzity poruch detekovaných nebezpečných poruch a intenzity poruch všech nebezpečných poruch

Střední doba nebezpečné poruchy; $MTTF_d$ (mean time to dangerous failure)

- očekávaná střední doba do nebezpečné poruchy

2.2.2 OBECNÝ POSTUP URČENÍ PL [5]

Krok 1 Identifikace nebezpečí (PL_r)



Obr. 8 Graf rizika pro určení PLr pro bezpečnostní funkci [5]

S – závažnost zranění

- S1 – lehké
- S2 – závažné

F – četnost a/nebo vystavení nebezpečí

- F1 – řídká až málo častá
- F2 – častá až nepřetržitá

P – možnost vyloučení nebezpečí nebo omezení škody

- P1 – možné za určitých podmínek
- P2 – sotva možné

Krok 2 Kategorie zapojení

<u>Kategorie B a 1</u>

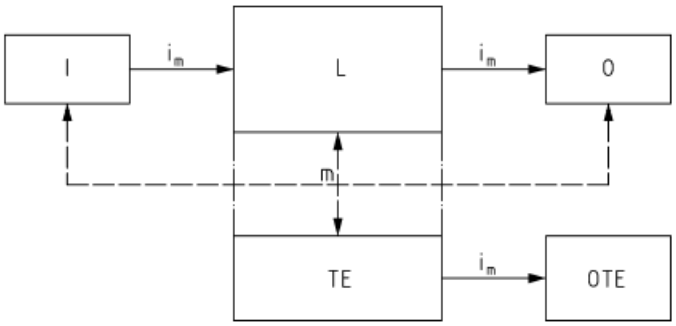
Pokud se vyskytne závada, může dojít ke ztrátě bezpečnostní funkce. U kategorie 1 je avšak střední doba do nebezpečné poruchy ($MTTF_d$) delší než v kategorii B. Maximální dosažitelná úroveň vlastností (PL) kategorií B je b, u kategorie 1 c.

Obr. 9 Stanovená architektura pro kategorii B a 1 [5]

I – vstupní zařízení; i_m - prostředky vzájemného propojení; L – logika; O – výstupní zařízení

Kategorie 2

Maximální dosažitelná úroveň vlastností (PL) je d.

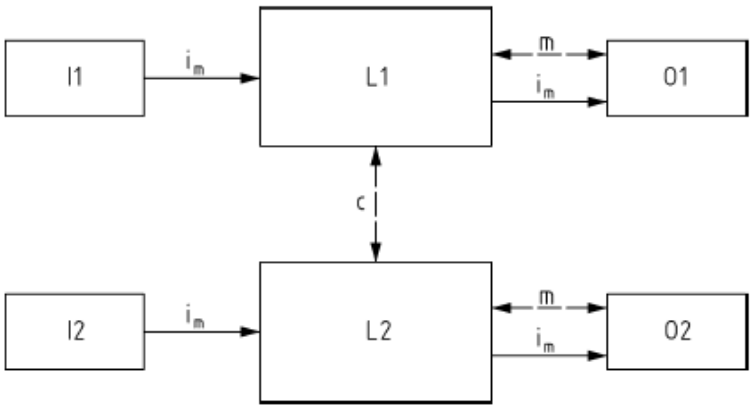


Obr. 10 Stanovená architektura pro kategorii 2 [5]

I - vstupní zařízení; L - logika; O - výstupní zařízení; m - monitorování; TE - zkušební zařízení; OTE - výstup ze zkušebního zařízení

Kategorie 3 a 4

Kategorie 4 má vyšší diagnostické pokrytí než kategorie 3.



Obr. 11 Stanovená architektura pro kategorie 3 a 4 [5]

Krok 3 Určení parametrů jednotlivých prvků

Potřebné hodnoty zjistíme od výrobce.

Hodnota B_{10d} – počet cyklů do doby, kdy 10% součástí nebezpečně selže; Hodnota DC – diagnostické pokrytí.

Krok 4 Výpočet $MTTF_d$, DC, kategorie

Určení střední doby do nebezpečné poruchy $MTTF_d$

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \tag{10}$$

Kde

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{cyklu}} \tag{11}$$

Doba provozu součásti je omezena na střední dobu T_{10d} do které 10% součástí nebezpečně selže.

$$T_{10d} = \frac{B_{10d}}{n_{op}} \tag{12}$$

Pokud je doba provozu součásti omezena na střední dobu T_{10d} do které 10% součástí nebezpečně selže, pak konstantní intenzita nebezpečné poruchy (λ_d) po dobu toho provozu je odhadnuta jako:

$$\lambda_d = \frac{0{,}1}{T_{10d}} = \frac{0{,}1 \times n_{op}}{T_{10d}} \tag{13}$$

Metoda součtů částí

$$\frac{1}{MTTF_d} = \sum_{i=1}^{n} \frac{1}{MTTF_{di}} \tag{14}$$

Odhad průměrného diagnostického pokrytí

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ \dots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d3}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dn}}} \tag{15}$$

Krok 5 Odhad CCF

Odhad účinků poruchy se společnou příčinou má být použit pro celý systém. Uvažována je každá část bezpečnostních částí ovládacího systému.

Krok 6 Ověření PL

Z vypočítaných hodnot ověříme, zda jsme se dostali k požadované úrovni vlastností, kterou jsme si určili v kroku 1. K tomuhle ověření nám slouží tab. 2

Tab. 2 Tabulka pro ověření PL [5]

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
$\boldsymbol{DC_{avg}}$	žádné	žádné	nízké	střední	nízké	střední	vysoké
$\boldsymbol{MTFF_d}$ **každého kanálu**							
Krátká	a	nepokryta	a	b	b	c	nepokryta
Střední	b	nepokryta	b	c	c	d	nepokryta
Dlouhá	nepokryta	c	c	d	d	d	e

2.3 ČSN EN 61508 – 1

Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky

Obecný úvod

Norma slouží jako návod, jak navrhovat zařízení související s bezpečností. Omezuje se na bezpečnostní prvky závislé na hardwaru a softwaru E/E/PE systémů, její zásady jsou obecné a tvoří základ bezpečnosti jiných systémů. Podle požadavků normy je třeba identifikovat a definovat každé riziko, které je spojené s EUC nebo s řídicím systémem. Pokud je tohle identifikované riziko větší, než riziko definováno jako přijatelné, je třeba ho zmenšit [6] [7].

Základním principem zakotveným v normě IEC 61508 je vyváženost mezi opatřeními zajišťujícími bezpečnost a rizikem spojeným s EUC a jeho řídicím systémem. K tomu musí být ve fázi 3 životního cyklu bezpečnosti vykonána důkladná analýza rizika podle článku 7.4 část 1, 2 a 3 normy [6].

Analýza rizika se podle normy skládá ze tří kroků. Jsou to:

- určení nebezpečí,
- analýza nebezpečí,
- ocenění rizika.

2.3.1 DEFINICE VYBRANÝCH POJMŮ [7]

- **Bezpečnost** – odstranění nepřijatelného rizika
- **Primární bezpečnost** – bezpečnost, která se zabývá riziky jako jsou např. úrazy elektrickým proudem, šoky nebo popálení způsobená zařízením.
- **Nepřímá bezpečnost** – zahrnuje vedlejší důsledky nesprávné funkce zařízení, které přímo neohrožují zdraví osob.
- **Funkční bezpečnost** – část celkové bezpečnosti týkající se řízeného procesu stroje EUC (Equipment under Control) a systému řízení EUC, která je závislá na správném

fungování E/E/EP systémů souvisejících s bezpečností, a/nebo ba systémech souvisejících s bezpečností založených na jiných technických principech a konečně na vnějších prostředcích pro snížení rizika.

- **Riziko** – kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození.
- **Přípustné riziko** – riziko, které je přijatelné v daných souvislostech založených na běžných hodnotách společnosti.
- **Zbytkové riziko** – riziko zbývající po přijetí ochranných opatření.
- **Nebezpečí** – potenciální zdroj poškození, újmy.
- **Chyba** – ukončení schopnosti zařízení vykonávat požadovanou funkci.
- **Bezpečná chyba** – chyba, která není natolik závažná, aby narušila systém do nebezpečného stavu, kdy není schopen plnit svou funkci.

Jedny z nejdůležitějších pojmů jsou integrita bezpečnosti a pojmy s ní související:

- **Integrita bezpečnosti (safety integrity)** – pravděpodobnost systému souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu.
- **Integrita bezpečnosti software (software safety integrity)** – míra vyjadřující pravděpodobnost softwaru plnit své funkce v E/E/EP souvisejícího s bezpečností plnit své bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu.
- **Integrita bezpečnosti hardware (hardware safety integrity)** – část integrity bezpečnosti systémů, souvisejících s bezpečností, týkající se náhodných poruch hardware v nebezpečném režimu poruchy.
- **Úroveň integrity bezpečnosti (safety integrity level SIL)** – diskrétní úroveň (jedna ze čtyř úrovní, definovaných normou) pro stanovení požadavků integrity bezpečnosti bezpečnostních funkcí přiřazených E/E/EP systémům souvisejícím s bezpečností, kde úroveň integrity bezpečnosti 4 má nejvyšší úroveň integrity bezpečnosti a úroveň 1 nejnižší.

3 PRVKY POUŽÍVANÉ V OBLASTI FUNKČNÍ BEZPEČNOSTI

Cílem bezpečnostních prvků je snížit riziko vzniku nehody na přijatelnou úroveň dle platných norem. Normy ČSN EN 13849-1 klasifikují a definují různé bezpečnostní třídy, uplatňují se poté v závislosti na technologii, kategorizaci rizik a struktuře systému [8].

Pokud chceme nebezpečí snížit, postupujeme podle tří základních kroků. V prvním kroku zamezíme nebezpečí, nejčastěji již ve fázi návrhu a výroby stroje. V druhém kroku snížíme riziko nebezpečí zavedením různých ochranných opatření. V posledním, třetím, kroku identifikujeme zbývající zdroje nebezpečí a následně redukujeme riziko pomocí informování o daném zbytkovém riziku.

Bezpečnostní části ovládacích systémů jsou určeny k plnění bezpečnostních funkcí. Jejich součástí může být hardware i software a mohou být součástí bezpečnostního systému nebo mohou být oddělené. Jsou zahrnuté do celého řetězce bezpečnostní funkce.

Bezpečnostní prvky dělíme na:

- Vstupní prvky – jsou to prvky, které zachytí signál a detekují nebezpečí. Jedná se hlavně o ochranná zařízení, jako jsou například blokovací zařízení, světelné závory nebo třeba polohový spínač.
- Logické prvky – tyhle prvky zpracovávají signál, který obdrží od vstupního prvku a dále jej na základě bezpečnostní funkce vyhodnotí. Sem řadíme ovládací jednotky pro zpracování dat.
- Výstupní prvky – starají se o odepínání a spínaní silové části. Řadíme sem prvky silového ovládání, například ventily.

3.1 VSTUPNÍ PRVKY

Jsou určeny pro komunikaci jednotlivých prvků se strojním zařízením.

3.1.1 BLOKOVACÍ ZAŘÍZENÍ OCHRANNÝCH KRYTŮ

Pomocí blokovacího zařízení můžeme dosáhnout propojení jednotlivých strojů a jeho bezpečnostních zábran. Na strojích můžeme najít spoustu nebezpečných oblastí, díky blokovacímu spínači je přístup do těchhle oblastí možný jen v případě kdy je daný prostor opravdu bezpečný [8].

Blokovací zařízení rozdělujeme na zařízení bez přidržení a s přidržením. Při použití blokovacího zařízení bez přidržení můžeme stroj ovládat jen v případě, že je ochranný kryt uzavřen. Předchází tak nebezpečné situaci v případě otevřeného krytu. Pokud dojde k otevření krytu během provozu stroje, zařízení odešle signál k jeho zastavení. Pokud použijeme blokovací zařízení s přidržením, můžeme stroj ovládat pouze tehdy, je-li kryt uzavřený

a uzamčený. K odemčení krytu dojde jen v případě vyloučení rizika poranění nebezpečnou částí stroje [9].

Obr. 12 Bezpečnostní polohový spínač s ovladačem [9]

Jako příklad nám může posloužit využití blokovacího zařízení na soustruhu. Obsluha potřebuje vyndat obrobek z nebezpečné části, a proto je nutné otevřít ochranný kryt. Otevřením krytu dojde k přerušení přívodu energie a k vypnutí soustruhu. Do nebezpečné oblasti je možné se dostat až poté co soustruh dokončí veškeré nebezpečné pohyby, které vykonává.

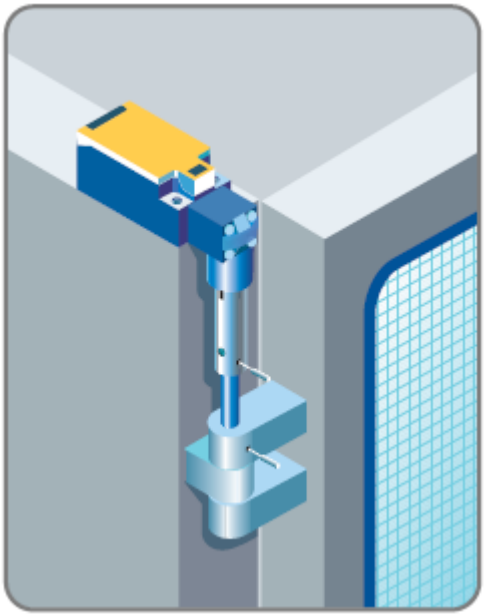
Kritéria pro výběr [9]:

- Podmínky používání a zamýšleného použití
- Nebezpečí na stroji
- Závažnost možného poranění
- Pravděpodobnost selhání blokovacího zařízení
- Čas potřebný k zastavení
- Doba, kterou je osoba vystavena nebezpečí

Bezpečnostní dveřní kloubový spínač

V oblasti bezpečnosti není radno si s ničím zahrávat a je proto nutné aby byla bezpečnost všech pracovníků zajištěna za všech okolností. Ve výrobních halách se proto užívají ochranné dveře a výklopné klapky, které zaměstnancům zaručují bezpečnost při vstupu

do nebezpečných a rizikových oblastí. Při pokusu otevření ochranných dveří během provozu stroje spínače okamžitě odpojují jeho napájení. Maximální bezpečnost je zaručena odpínáním již v úhlu 5°. [9]



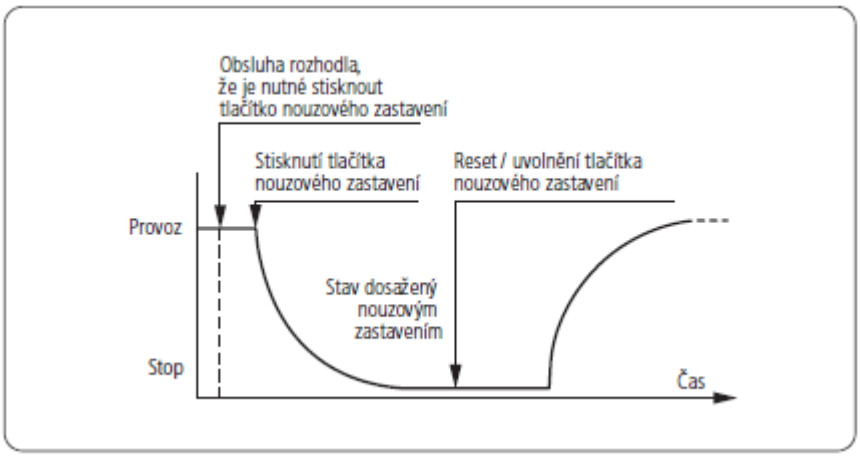
Obr. 13 Bezpečnostní dveřní kloubový spínač [9]

3.1.2 TLAČÍTKO NOUZOVÉHO ZASTAVENÍ

Nouzové zastavení předchází nebo omezuje nebezpečí zranění obsluhy, případně omezuje riziko vzniku nehody, která by měla za důsledek škodu na stroji nebo na pracovním materiálu. Nebezpečí může nastat v několika případech, jako porucha stroje nebo také vinou lidského faktoru.

Obr. 14 Tlačítko nouzového zastavení [2]

Norma ČSN EN ISO 13850 stanovuje povinné používání tlačítka nouzového zastavení pro každý stroj, s výjimkou ručních a ručně ovládaných strojů a strojů, na kterých použití tlačítka nouzového zastavení nesnižuje riziko.



Obr. 15 Sekvence funkcí nouzového zastavení [9]

Funkce nouzového zastavení se dělí do dvou skupin:

- STOP kategorie 0 – dochází k okamžitému odpojení
- STOP kategorie 1 – dochází ke kontrolovanému zastavení

Příkladem kategorie 0 je hlavní vypínač s funkcí nouzového zastavení nebo tlačítko nouzového zastavení ve spojení s podpěťovou spouští.

Příklad aplikace kategorie 1 je motor s DC brzděním nebo kontrolovaným doběhem.

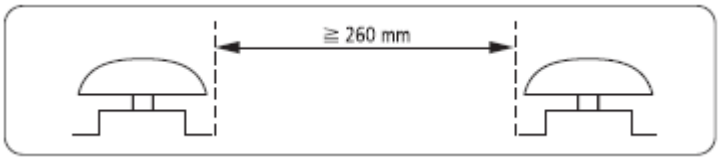
3.1.3 DVOURUČNÍ OVLÁDÁNÍ

Funkcí dvouručního ovládání je zamezení přístupu do rizikových oblastí během nebezpečného procesu. Při výběru vhodného typu a vhodné konstrukce dvouručního ovládání musíme brát v potaz úroveň nebezpečí, zhodnocení rizik, technologii aplikace a různé další vlivy jako jsou například prevence náhodného sepnutí nebo obcházení bezpečnostní funkce.

Pokud se chceme ujistit, že nedojde k obcházení funkce nebo náhodnému sepnutí, můžeme použít některé speciální postupy definované v normě ČSN EN 574.

Následující příklady je možné použít pro různé postupy obcházení bezpečnostní funkce [9]:

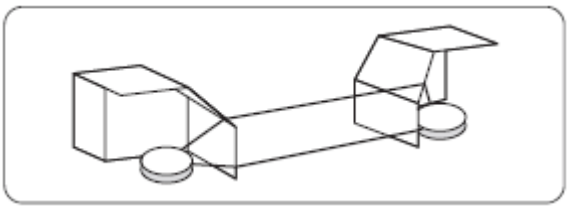
- Ovládání jednou rukou
    - Vnitřní vzdálenost mezi ovládacími prvky ≥ 260 mm



Obr. 16 Zabránění obcházení bezpečnostní funkce: vnitřní vzdálenost [9]

- Ovládání dlaní a loktem jedné ruky
  - Vnitřní vzdálenosti mezi ovládacími prvky ≥ 550mm (≤ 600 mm)

- Ovládání předloktím a loktem
  - Použití krytů



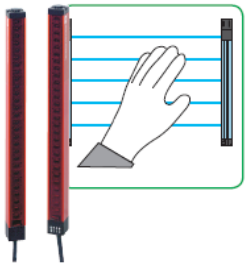
Obr. 17 Zabránění obcházení bezpečnostní funkce: použití krytů [9]

- Ovládání jednou rukou a kteroukoli další částí těla
  - Ovládací prvky pro vodorovné plochy umístit minimálně 1100 mm nad podlahu (přístupovou rovinu)

3.1.4 SVĚTELNÉ BARIÉRY + NÁŠLAPNÉ ROHOŽE

Světelné bariéry

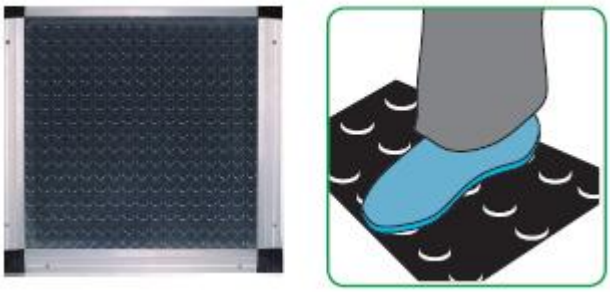
Světelné bariéry umožňují vstup do rizikových prostorů stroje, za podmínky je-li stroj v klidu. Během pracovního cyklu nám bariéry zabraňují před vstupem do nebezpečné oblasti stroje, čímž značně snižují riziko úrazu. Přerušením světelných paprsků se detekuje cizí těleso v nežádoucí oblasti. Pokud k takovému přerušení paprsků dojde, bezpečnostní systém sám zastaví nebezpečný pohyb stroje [2].



Obr. 18 Světelná bariéra [2]

Nášlapné Rohože

Bezpečnostní nášlapné rohože se obvykle používají u čelní strany nebo v okolí potenciálně nebezpečných strojů nebo robotů. Zajišťují ochrannou zónu mezi operátory a všemi nebezpečnými pohyby. Jsou určeny zejména k zajištění bezpečnosti pracovníků a obvykle se používají s doplňujícími bezpečnostními prvky, jako jsou světelné bariéry. Jejich funkce spočívá v detekci vstupu osob na rohož a zatavení nebezpečných pohybů [2].



Obr. 19 Nášlapné rohože [2]

3.2 LOGICKÉ PRVKY

Správný výběr logického prvku ovlivňuje spousta faktorů, musíme brát v potaz finanční náklady, počet zpracovávaných bezpečnostních funkcí, složitost samotných bezpečnostních funkcí nebo potřebu posílat bezpečnostní signály/data přes dlouhé vzdálenosti u velkých strojů respektive mezi stroji v rozlehlých provozech [2].

3.2.1 BEZPEČNOSTNÍ RELÉ

Jedná se o elektronické zařízení, které spolupracuje s ostatními bezpečnostními prvky za účelem zvýšení bezpečnosti obsluhy a stroje. Funkcí těchto logických modulů je zpracovávání signálu ze vstupních prvků a jeho následné vyhodnocení dle dané bezpečnostní funkce. Kontrola bezpečnostních obvodů probíhá hned po zapnutí zařízení, jejich sepnutí je poté realizováno pomocí výstupního relé. Je možné využít okamžitého odpojení motoru od sítě (STOP kategorie 0), nebo je možné provést kontrolované zastavení se zpožděním (STOP kategorie 2). Při potřebě více kontaktů je možné použít rozšiřující modul [9].

Obr. 20 Bezpečnostní relé [10]

Bezpečnostní relé jsou určeny pro následující funkce [2]:

- Kontrola obvodů nouzového zatavení
- Monitorování bezpečnostních krytů a světelných závor
- Monitoring dvouručního ovládání
- Obvody se zpožděním

Příklady použití [9]**:**

<u>Bezpečné sledování obvodů nouzového zastavení</u>

Elektronická bezpečnostní relé umožňují při aktivaci tlačítka nouzového zastavení buď přímé odpojení nebo odpojení se zpožděním napájecího napětí několika okruhů. V závislosti na jejich konfiguraci mohou detekovat chyby, jako jsou zkraty v obvodech, zemní zkraty nebo zkraty v okruhu nouzového zastavení. To vede buď k okamžitému odpojení, nebo zabránění spuštění do té doby, než bude chyba napravena.

<u>Monitorování pohyblivých ochranných mechanismů</u>

V závislosti na úrovni bezpečnosti jsou použity jeden nebo dva polohové spínače, které kontrolují, zda jsou bezpečnostní dveře zavřené. V tomto případě je možné implementovat automatický start bezpečnostního relé.

3.2.2 PLC

Funkce PLC (programovatelný logický automat) je určena programem, který je uložen v operační paměti systému. Základním cílem při vzniku PLC bylo vytvoření "přátelského" programovacího prostředí, které by umožnilo vytvářet programy i technikům neprogramátorům (liniová schémata). Postupem času a rozvojem výpočetní techniky začaly pronikat i do úloh monitorování a měření a nahrazují dokonce i samotné regulátory.

Řízení technologie je spojeno s PLC prostřednictvím snímačů a akčních členů (zařízení provádějící zásahy do regulované soustavy - relé, stykače, servo-pohony, tranzistory atp.). PLC načítá prostřednictvím svých vstupů, signály ze snímačů a ovládacích prvků. Programově je zpracovává a prostřednictvím svých výstupů zasahuje do řízené soustavy.

PLC se skládá z:

- Centrální procesorové jednotky,
- Systémové paměti,
- Uživatelské paměti,
- Vstupních a výstupních jednotek pro připojení řízeného systému,
- Komunikačních jednotek pro komunikaci se souřadnými a nadřazenými řídicími systémy

Jsou navzájem propojeny systémovou sběrnicí.

3.2.3 ŘÍDICÍ SYSTÉMY

<u>Sinumerik</u>

Jedná se o řídicí systém pro obráběcí stroje od firmy Siemens. Tenhle řídicí systém byl uveden na trh v roce 1960 a jednalo se o první systém pro číslicové řízení obráběcích strojů. První verze umožňovala jen spojité řízení dráhy nástroje, následující verze už zahrnovaly operace soustružení, frézování, broušení a prostřihování [10].

V roce 1973 byla na trh uvedena verze Sinumerik 500C, byl to první systém obsahující počítač pro řízení soustruhů a frézek. Během několika let se na trhu objevily první PLC řídicí systémy Sinumerik.

V roce 1992 byla představena řada 840, která zasahuje i do současnosti. Sinumerik 840C obsahoval kombinované analogové a digitální ovládání pohonů. Pozdější verze 840D byla doplněna o číslicové ovládání pohonů a otevřené jádro řídicího programu s možností integrovat do systému CNC další softwarové komponenty [11].

V současné době jsou k dispozici verze Sinumerik 840D sl a Sinumerik 802D sl, které nabízí vše potřebné k efektivnímu návrhu a výrobě obrobků [10] [11].

<u>HEIDENHAIN</u>

V roce 1981 přišla společnost HEIDENHAIN na trh se systémem TNC 145, jednalo se o jejich první souvislý CNC řídicí systém. Po 30 letech výzkumu, v roce 2011, byl vydán systém iTNC 530 s řízením komponentů přes HSCI (Heidenhain Serial Controller Interace). Systém iTNC je vhodný jak pro řízení jednoduché tříosé frézky pro výrobu nástrojů apod., tak také pro obráběcí centra v sériové výrobě. Programy pro frézování a vrtání se připravují přímo

na stroji nebo v otevřeném textu pomocí DIN/ISO kódu. NC systém může být vytvořen také externě pomocí CAD/CAM systému. Rychlé zpracování NC programů vygenerovaných v CAM a rychlý přenost dat umožňuje řízení vysokorychlostního frézování. Systém umožňuje i manuální režim práce na stroji, většinou pro jednoduché účely jako např. rovinné frézování [12] [13].

3.3 VÝSTUPNÍ PRVKY

3.3.1 STYKAČE

Stykač slouží pro spínání nebo rozepínání elektrického spojení. Stykače se používají v ovládacích obvodech, např. jako řídicí stykače pro střední výkony. Zařízení s větším výkonem, například motory, jsou napájena přes výkonové stykače.

Stykače umožňují klasické připojení motoru k síti. Jsou to vlastně spínací přístroje, které mají zajištěnou jen polohu při vypnutí. V zapnuté poloze je kontakt držen vnější silou.

Podle způsobu ovládání můžeme stykače rozdělit na:

- elektromagnetické
- vačkové
- pneumatické

Jelikož jsou stykače určené na dálkové spínání elektrických obvodů, požaduje se od nich velká hustota spínání a dlouhá životnost.

Podle přenášeného proudu rozdělujeme stykače na:

- stykače na střídavý proud
- stykače na stejnosměrný proud

Princip činnosti

Do spínací cívky stykače se přivede elektrický proud, který vybudí magnetické pole. Silové účinky působí skrz vzduchovou mezeru na pohyblivou část magnetického obvodu (kotvu), kde jsou uložené pohyblivé kontakty. Přitáhnutím kotvy se spínají hlavní kontakty.

Stykač se vypne krátkým přerušením proudu v obvodu spínací cívky.

Obr. 21 Stykač [15]

3.3.2 RELÉ

Přístroj, který obsahuje elektromagneticky ovládané vypínače s jednou stabilní polohou. Používá se na podobné aplikace jako stykač. Nejčastěji se používá elektromagnetické relé

Rozdělení podle druhu napájecího proudu:

- Stejnosměrné
- Střídavé
- Univerzální

Relé může pracovat s časovým zpožděním, takové relé nazýváme časové. Podle časové odezvy dělíme relé na:

- Se zpožděným přítahem kotvy
- Se zpožděným odpadem kotvy

Relé pracuje na elektromagnetickém principu, tzn. využívá magnetické účinky elektrického proudu protékajícího cívkou, relé se mechanicky spíná.

V blízkosti elektromagnetu tvořeného cívkou a jádrem z magnetické měkké oceli je pohyblivá kotva. Kotva se dotýká pružných kontaktů, ke kterým je připojený obvod ovládaného zařízení. Jakmile elektromagnetem začne protékat ovládací proud, jádro cívky se zmagnetizuje a přitáhne kotvu relé, čímž se sepnou pružné kontakty. Tím je ovládané zařízení uvedeno do chodu. Proud v řídicím obvodu nemusí být velký, ale proud v řízeném obvodu musí být několikrát větší.

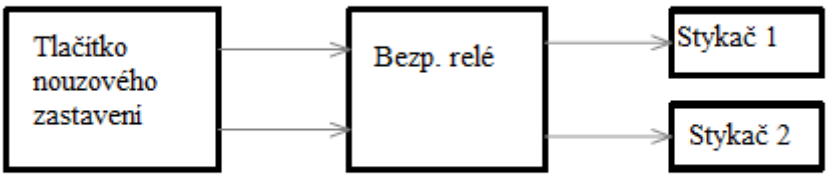
4 STANOVENÍ PL A SIL

4.1 STANOVENÍ PL PRO BEZPEČNOSTNÍ FUNKCI NOUZOVÉHO ZASTAVENÍ

Vstup – Tlačítko nouzového zastavení od firmy Siemens.

Logika – Bezpečnostní relé od firmy Siemens, typ EM138 4/8 F-DI.

Výstup – Dva stejné stykače od firmy Siemens, typ Contactor 3RT.



Závažnost zranění jsme si určili jako lehké (S1), četnost vystavení nebezpečí častou až nepřetržitou (F2). Možnost vyloučení nebezpečí je možná za určitých podmínek (P1). Požadovanou úroveň vlastností jsme si tedy určili jako PL_d. (Obr. 8)

Zapojení kategorie 3.

Hodnoty B_{10d} a DC jsou voleny z katalogu firmy Siemens [16].

Tlačítko nouzového zastavení

$B_{10d1} = 500\,000\ cyklů$

$h_{op} = 8\ h\ za\ den$ h

$d_{op} = 252$ dnů za rok

$t_{cyklu} = 14\,400\ s\ na\ cyklus$

$DC_1 = 90\%$

<u>Výpočet $MTTF_d$</u>

$$n_{op1} = \frac{d_{op} \times h_{op} \times 3600 s/h}{t_{cyklu}} = \frac{252 \times 8 \times 3600}{14\,400} = 504\ cyklů/rok$$

$$T_{10d1} = \frac{B_{10d1}}{n_{op}} = \frac{500\ 000}{504} = 992{,}06\ roků$$

$$MTTF_{d1} = \frac{B_{10d1}}{0{,}1 \times n_{op1}} = \frac{500\ 000}{0{,}1 \times 504} = 9\ 920{,}63\ roků$$

Bezpečnostní relé

Hodnota PFH_d je volena z katalogu firmy Siemens [16].

$PFH_d = 1 \times 10^{-8}$

$DC_2 = 99\%$

<u>Výpočet $MTTF_d$</u>

$$MTTF_{d2} = \frac{1}{8760 \times PFH_d} = 11\ 415\ roků$$

Stykače

$B_{10d3} = B_{10d4} = 1\ 369\ 863\ cyklů$

$h_{op} = 8\ h\ za\ den$ h

$d_{op} = 252$ dnů za rok

$t_{cyklu} = 14\ 400\ s\ na\ cyklus$

$DC_3 = DC_4 = 0\%$

<u>Výpočet $MTTF_d$</u>

$$n_{op3} = n_{op4} = \frac{d_{op} \times h_{op} \times 3600 s/h}{t_{cyklu}} = \frac{252 \times 8 \times 3600}{14\ 400} = 504\ cyklů/rok$$

$$T_{10d3} = T_{10d4} = \frac{B_{10d3}}{n_{op3}} = \frac{1\ 369\ 863}{504} = 2\ 718\ roků$$

$$MTTF_{d3} = \frac{B_{10d3}}{0{,}1 \times n_{op3}} = \frac{1\ 369\ 863}{0{,}1 \times 504} = 27\ 179{,}8\ roků$$

$MTTF_{d3} = MTTF_{d4}$

Výpočet $MTTF_d$ pro 1. kanál

$$\frac{1}{MTTF_d} = \sum_{i=1}^{n} \frac{1}{MTTF_{di}}$$

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \frac{1}{MTTF_{d3}}$$

$$MTFF_{d1k} = \frac{1}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \frac{1}{MTTF_{d3}}} = \frac{1}{\frac{1}{9\,920{,}6} + \frac{1}{11\,415} + \frac{1}{27\,179{,}8}}$$

$$= 4\,440{,}6\ rok\text{ů}$$

Výpočet $MTTF_d$ pro 2. kanál

Jelikož máme stykač v kanálu 1 je stejný jak stykač v kanálu 2, pak předpokládáme, že:

$$MTTF_{d1k} = MTFF_{d2k}$$

Výpočet $MTTF_d$ pro celou funkci

$$MTTF_d = \frac{2}{3}\left[MTTF_{d1k} + MTTF_{d2k} - \frac{1}{\frac{1}{MTTF_{d1k}} + \frac{1}{MTTF_{d2k}}}\right]$$

$$= \frac{2}{3}\left[4\,440{,}6 + 4\,440{,}6 - \frac{1}{\frac{1}{4\,440{,}6} + \frac{1}{4\,440{,}6}}\right] = 4\,440{,}6\ rok\text{ů}$$

Odhad průměrného diagnostického pokrytí

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \frac{DC_3}{MTTF_{d3}} + \frac{DC_4}{MTTF_{d4}}}{\frac{1}{MTTF_{d3}} + \frac{1}{MTTF_{d2}} + \frac{1}{MTTF_3} + \frac{1}{MTTF_4}}$$

$$= \frac{\frac{0{,}9}{9\,920{,}6} + \frac{0{,}99}{11\,415} + \frac{0}{27\,719{,}8} + \frac{0}{27\,719{,}8}}{\frac{1}{9\,920{,}6} + \frac{1}{11\,415} + \frac{1}{27\,719{,}8} + \frac{1}{27\,719{,}8}} = 0.681 = 68{,}1\%$$

Ověření úrovně vlastností PL podle tab.2

PL=d

4.2 STANOVENÍ SIL PRO BEZPEČNOSTNÍ FUNKCI NOUZOVÉHO ZASTAVENÍ

Stanovení požadované úrovně SIL

Následky Se trvalé, hrozí smrt nebo ztráta končetin. (Se = 4)

Četnost ohrožení Fr, více než jednou za den. (Fr = 4)

Pravděpodobnost výskytu, pravděpodobná. (Pr = 4)

Pravděpodobnost vyvarování se, možná za určitých podmínek. (Av = 3)

Třída CL = Fr + Pr + Av = 4 + 4 + 3 = 11

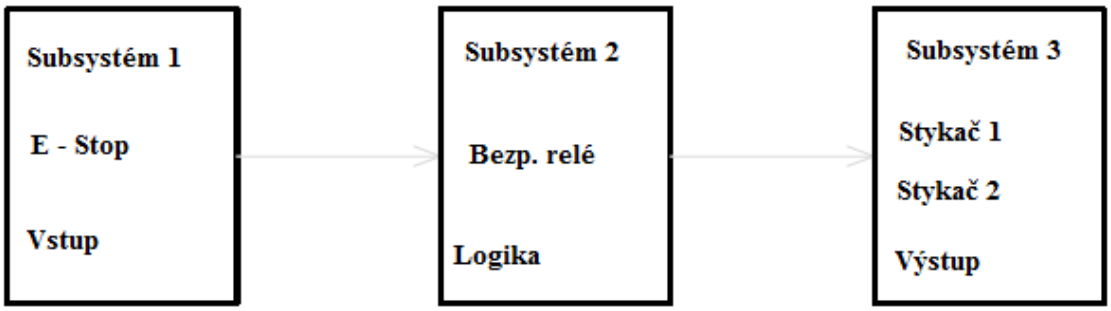
Hodnoty voleny podle normy ČSN EN 62061 [4].

Tab. 3 Stanovení SIL

Závažnost (Se)	Třída (Cl)				
	3-4	8-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Z tab. 3 nám vychází požadovaná úroveň SIL CL 3.

Funkční blok bezpečnostní funkce



Obr. 22 Funkční blok

Výběr součástí subsystému

Vstup – Tlačítko nouzového zastavení od firmy Siemens.

Logika – Bezpečnostní relé od firmy Siemens, typ EM138 4/8 F-DI.

Výstup – Dva stejné stykače od firmy Siemens, typ Contactor 3RT.

Tab. 4 Součásti subsystému

Součást	Počet operací B_{10}	Počet operací B_{10d}	PFH_d
Tlačítko E - Stop	100 000	500 000	
Bezp. relé			1×10^{-8}
Stykač 1,2	1 000 000	1 369 863	

Hodnoty voleny z katalogu Siemens [16].

Diagnostická funkce

Vstup – architektura C

Logika – architektura C

Výstup – architektura B

Subsystém 1

Počet operací za hodinu uvažujeme 0,25.

C = 0,25

$$\lambda_{Estop} = 0{,}1 \times \frac{C}{B_{10d}} = 0{,}1 \times \frac{0{,}25}{500\,000} = 5 \times 10^{-8}$$

Hodnota DC volena z katalogu Siemens. [16]

$$\lambda_{Ss1} = \lambda_{Estop}(1 - DC_1) = 5 \times 10^{-8} \times (1 - 0{,}9) = 5 \times 10^{-9}$$

$$PFH_{DSs1} = \lambda_{Ss1} \times 1h = 5 \times 10^{-9}$$

Subsytém 2

$PFH_{dSs2} = 1 \times 10^{-8}$

Subsystém 3

$$\lambda_{Stykač1} = 0{,}1 \times \frac{C}{B_{10d}} = 0{,}1 \times \frac{0{,}25}{1\,369\,863} = 1{,}825 \times 10^{-8}$$

$$\lambda_{Stykač2} = 0{,}1 \times \frac{C}{B_{10d}} = 0{,}1 \times \frac{0{,}25}{1\,369\,863} = 1{,}825 \times 10^{-8}$$

$$T_1 = \frac{B_{10d}}{C} = \frac{1\,369\,863}{0{,}25} = 5\,479\,452$$

Citlivost na společné poruchy $\beta = 0{,}1$ volena podle normy ČSN EN 62061.

$$\lambda_{Ss3} = (1-\beta)^2 \times \lambda_{Stykač1} \times \lambda_{Stykač2} \times T_1 + \beta \times \frac{(\lambda_{Stykač1} + \lambda_{Stykač2})}{2}$$
$$= (1-0{,}1)^2 \times 1{,}825 \times 10^{-8} \times 1{,}825 \times 10^{-8} \times 5\,479\,452 + 0{,}1 \times \frac{(1{,}825 \times 10^{-8} + 1{,}825 \times 10^{-8})}{2} = 2{,}698 \times 10^{-18}$$

$$PFH_{DSs3} = \lambda_{Ss3} \times 1h = 2{,}698 \times 10^{-18}$$

Celková hodnota PFH_D

$$PFH_D = PFH_{DSs1} + PFH_{DSs2} + PFH_{DSs3} = 5 \times 10^{-9} + 1 \times 10^{-8} + 2{,}698 \times 10^{-18} = 1{,}5 \times 10^{-8}$$

Z této hodnoty PFH_D vyplývá úroveň integrity SIL 3 dle normy ČSN EN 62061.

ZÁVĚR

Účelem téhle bakalářské práce bylo seznámení s problematikou funkční bezpečnosti. Nezbytným základem pro tuto práci bylo mít představu co to vlastně funkční bezpečnost je a co všechno zahrnuje.

Po seznámení se základními pravidly a principy funkční bezpečnosti jsem mohl začít s další částí bakalářské práce, kde jsem vycházel zejména ze zákonů a nařízení týkající se funkční bezpečnosti. Po seznámení se s normami ČSN EN 62061, ČSN EN 13849-1 A ČSN EN 61508-1 jsem mohl pokračovat v jejich stručném popisu. Nejdůležitější částí bylo porozumění výpočtů ke stanovení úrovně vlastností a úrovně integrity. Po pochopení a nastudování těchto výpočtů jsem se mohl vrhnout na popsání postupů k jejich stanovení.

Abych se mohl vrhnout na rešerši prvků užívaných v oblasti funkční bezpečnosti, bylo zapotřebí pročtení spousty katalogů a brožur od různých firem, které sloužily pro seznámení s jednotlivými prvky a s jejich funkcemi. Pro popis a charakterizace jsem vybíral prvky, které se používají nejčastěji a o kterých si můžeme říci, že jsou charakteristickými pro danou skupinu, ať už to jsou vstupní, logické nebo výstupní prvky.

Důležité také bylo ukázat si výpočty, které jsem teoreticky popsal jedné z předchozích kapitol, na praktickém příkladu. Za příklad byla vybrána jednoduchá bezpečnostní funkce nouzového zastavení. Použité prvky v téhle bezpečnostní funkci jsou tlačítko nouzového zastavení, bezpečnostní relé a dva stejné stykače, které v případě poruchy nebo stlačení tlačítka nouzového zastavení odpojí zařízení od zdroje. Z výpočtů nám vyšlo, že daná bezpečnostní funkce splňuje předem určenou úroveň vlastností a úroveň integrity, což znamená, že byly voleny správné prvky a funkce splňuje podmínky k zařazení do provozu.

POUŽITÉ INFORMAČNÍ ZDROJE

1. **AUTOMA.** Funční bezpečnost bez kompromisů. [Online] 2011. [Citace: 21. duben 2014.] http://www.odbornecasopisy.cz/res/pdf/42958.pdf.

2. **SCHNEIDER ELECTRIC.** Schneider Electric CZ. *Bezpečnostní příručka pro strojní zařízení.* [Online] 2010. [Citace: 25. duben 2014.] http://www.schneider-electric.cz/sites/czech-republic/cz/reseni/oem/strojni-bezpecnost/bezpecnostni-prirucka.page.

3. **Česká republika.** Zákon č. 22/1997 Sb. *Zákon o technických požadavích na výrobky.* 1997.

4. **ČSN EN ISO 62061.** *Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných řídicích systémů souvisejících s bezpečností.* Praha : Český normalizační institut, 2005. Třídící znak 33 2208.

5. **ČSN EN ISO 13849-1.** *Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Všeobecné zásady pro konstrukci.* Praha : Český normalizační institut, 2008. Třídící znak 83 3205.

6. **AUTOMA.** Úvod do funkční bezpečnosti I: norma ČSN EN 61508. [Online] 2004. [Citace: 10. květen 2014.] http://www.odbornecasopisy.cz/uvod-do-funkcni-bezpecnosti-i:-norma-csn-en-61508-32520.html.

7. **ČSN EN ISO 61508-1.** *Funkční bezpečnost elektrických/elektronickcýh/programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky.* Praha : Český normalizační institut, 2010. Třídícíí znak 83 3303.

8. **AUTOMA.** Bezpečnostní prvky pro strojní zařízení Eaton. [Online] 2011. [Citace: 2. květen 2014.] http://www.odbornecasopisy.cz/res/pdf/41724.pdf.

9. **EATON.** Bezpečnostní prvky pro strojní zařízení. [Online] 2010. [Citace: 20. duben 2014.] http://www.eatonelektrotechnika.cz/pdf/tiskoviny_pdf_385.pdf.

10. **EATON.** Bezpečnostní relé ESR. *Eaton elektrotechnika.* [Online] 2010. [Citace: 6. květen 2014.] http://www.eatonelektrotechnika.cz/produkty-prumyslove_instalace-ovladani_signalizace-bezpecnostni_rele_esr.

11. **SIEMENS.** *Frézování a soustružení s řídicím systémem Sinumerik: CNC řešení pro Vaši dílnu.* [s.l.] : Siemens.

12. **KLOCOVÁ, Eva.** Sinumerik slaví půlstoletí. *MM Průmyslové spektrum.* [Online] 2010. [Citace: 4. květen 2014.] http://www.mmspektrum.com/clanek/sinumerik-slavi-pulstoleti.html. ISSN 1212-2572.

13. **HEIDENHAIN.** *iTNC530.* [s.l.] : Heidenhain, 2011.

14. **HEIDENHAIN.** MANUALplus 620 - The Contouring Control for CNC and Cycle Lathes. [Online] 2009. [Citace: 6. květen 2014.] http://pdf.directindustry.com/pdf/dr-johannes-heidenhain-gmbh/manualplus-620-the-contouring-control-cnc-cycle-lathes/155-166854.html.

15. **ELEKTRO.** Výkonové stykače DIL. [Online] 2009. [Citace: 6. květen 2014.] http://www.odbornecasopisy.cz/res/pdf/38514.pdf.

16. **SIEMENS.** [Online] [Citace: 10. květen 2014.] https://mall.industry.siemens.com/registration/login.aspx?ret=https%3a%2f%2fmall.industry.siemens.com%2fspice%2fsid%2findex.html%3flang%3den.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

B_{10d}	[-]	Průměrný počet provozních cyklů dosažených před tím, než 10% vzorků selže za nebezpečného stavu
C	[-]	Pracovní cyklus
CAD	[-]	Computer Aided Manufacturing – Počítačem podporovaná výroba
CAM	[-]	Computer Aided Design – Počítačem podporované navrhování
CCF	[-]	Common Cause Failure – Selhání se společnou příčinou
CE	[-]	Dokládá, že výrobek byl posouzen před uvedením na trh a splňuje legislativní požadavky Evropské unie
DC	[-]	Diagnostic Coverage – Diagnostické pokrytí
d_{op}	[-]	Střední doba provozu ve dnech za rok
E/E/PE	[-]	Electrical/Electronic/Programable Electronic Systém – Elektrický/elektronický/programovatelný elektronický systém
EU	[-]	Evropská unie
EUC	[-]	Equipment under Control – Řízené zařízení
h_{op}	[-]	Střední doba provozu v hodinách za den
HSE	[-]	The Health and Safety Executive – Úřad pro bezpečnost a ochranu zdraví
IEC	[-]	International Electrotechnical Commision – Mezinárodní elektrotechnická komise
$MTTF_d$	[rok]	Mean Time to Dangerous Failure – Střední doba do nebezpečného selhání
n_{op}	[-]	Střední počet činností za rok
PFH_d	[-]	Probability of Dangerous Failure – Pravděpodobnost nebezpečných selhání
PL	[-]	Performance level – Úroveň vlastností
PLC	[-]	Programmable Logic Controller – Programovatelný logický automat
PLr	[-]	Performance level required – Požadovaná úroveň vlastností
SIL	[-]	Safety Integrity Level – Úroveň integrity bezpečnosti
SRECS	[-]	Safety-Related Electrical Control System – Elektrický řídicí systém související s bezpečností
SRP/CS	[-]	Safety-Related Part of a Control System – Část kontrolní systému související s bezpčností
T_1	[-]	Interval kontrolní zkoušky nebo životnost – podle toho, který interval je kratší

T_{10d}	[rok]	Střední doba do které 10% součástí selže
T_2	[-]	Diagnostický zkušební interval
t_{cyklu}	[s]	Střední doba mezi začátkem dvou po sobě následujících cyklů
λ_d	[-]	Míra nebezpečných poruch
λ_{DssD}	[-]	Pravděpodobnost nebezpečné poruchy
β	[-]	Faktor poruch se společnou příčinou