VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV VÝROBNÍCH STROJŮ,
SYSTÉMŮ A ROBOTIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF PRODUCTION MACHNES, SYSTEMS
ANDROBOTICS

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
AUTOR

JAKUB KOTEN

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. JIŘÍ ZAHÁLKA

BRNO 2014

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav výrobních strojů, systémů a robotiky
Akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

student(ka): Jakub Koten

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

obor: **Strojní inženýrství (2301R016)**

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 26.11.2013

L.S.

doc. Ing. Petr Blecha, Ph.D.	prof. RNDr. Miroslav Doupovec, CSc., dr. h. c.
Ředitel ústavu	Děkan fakulty

ABSTRAKT

KOTEN Jakub: Zhodnocení současných technologií v zajišťování funkční bezpečnosti strojních zařízení

Tato bakalářská práce se zabývá zhodnocením současných technologií v zajišťování funkční bezpečnosti strojních zařízení. První část práce je věnována technickým normám, které se vztahují k této problematice. Jsou zde vysvětleny nejpoužívanější pojmy vyskytující se v těchto normách a popis základních principů k návrhu a zajištění funkční bezpečnosti strojních zařízení. V druhé části jsou představeny prvky zajišťující funkční bezpečnost. Jsou to prvky vstupní, které monitorují zařízení a jeho okolí. Logické prvky, které podle stanovených podmínek vyhodnocují vstupy a posílají výstupním prvkům podněty k reakci. Dále následuje kapitola, která na příkladu ukazuje návrh a ověření úrovně vlastností a úroveň integrity bezpečnosti.

Klíčová slova: funkční bezpečnost, vstupní prvky funkční bezpečnosti, logické prvky funkční bezpečnosti, výstupní prvky funkční bezpečnosti, úroveň vlastností, úroveň integrity bezpečnosti

ABSTRACT

KOTEN Jakub: Evaluation of present technologies in ensuring functional safety of machinery.

This bachelor's thesis deals with the evaluation of present technologies in ensuring functional safety of machinery. The first part devotes to the technical standards, which are related to this issue. It explains the most common terms occurring in these standards and the description of the basic principles for the design and ensuring the functional safety of machinery. The second part presents the elements ensuring functional safety. These are the input elements that monitor a device and its surroundings. Logical elements which, under specified conditions assess inputs and send output elements impulses to respond. Then there is the chapter showing on the example the design and verification of the performance level and safety integrity level.

Keywords: functional safety, input elements of functional safety, logical elements of functional safety, output elements of functional safety, performance level, safety integrity level

BIBLIOGRAFICKÁ CITACE

KOTEN, J. *Zhodnocení současných technologií v zajišťování funkční bezpečnosti strojních zařízení.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2014. 49 s. Vedoucí bakalářské práce Ing. Jiří Zahálka.

ČESTNÉ PROHLÁŠENÍ

Tímto prohlašuji, že předkládanou bakalářskou práci jsem vypracoval samostatně, s využitím uvedené literatury a podkladů, na základě konzultací a pod vedením vedoucího bakalářské práce.

V Brně dne 15.5.2014

……
Podpis

PODĚKOVÁNÍ

Chtěl bych poděkovat panu Ing. Jiřímu Zahálkovi za odborné vedení, za pomoc a rady při zpracování této práce.

OBSAH

1 ÚVOD

Již v historii, při počátku používání jednoduchých strojních zařízení, vznikaly první pracovní úrazy a škody na majetku. Jelikož práce na těchto strojích byla spíše ojedinělou záležitostí, nebyla tato problematika až na jednoduché školení obsluhy brána v potaz. Nejhorší byla situace po objevení parního stroje, kdy nastalo velké rozšíření strojních zařízení. Obsluha těchto strojů se považovala za velmi levnou pracovní sílu, takže ani obrovský nárůst, a to i vážných úrazů a usmrcení, nedonutil zaměstnavatele zabývat se touto problematikou více do hloubky. Jednodušší bylo zaměstnat dalšího dělníka. To se začalo měnit až s příchodem odborů, které začaly hájit práva dělníků a vymáhaly ze zaměstnavatelů odškodnění za způsobená poranění. Prvními zařízeními byly mechanické zábrany, které měly zabránit rizikům znemožněním přístupu do nebezpečných míst. Po dalším vývoji se objevily už bezpečnostní obvody, které detekují vstup a dokážou na něj vhodně reagovat. Nejnovějším řešením funkční bezpečnosti je použití bezpečnostních programovatelných logických automatů, jejichž hlavní výhodou je, že zpracovávají bezpečnostní funkce a zároveň řídí proces stroje.

Funkční bezpečnost má za úkol udělat strojní zařízení do jisté míry (která se definuje podle níže specifikovaných pravidel) bezpečný, to se ale nikdy nepovede úplně. Každé zařízení skrývá nějaké riziko, které má být při nemožnosti jeho odstranění minimalizováno na přijatelnou hodnotu. Teoretické určení rizik, návrh a kontrola funkční bezpečnosti jsou definovány v technických normách, které jsou zmíněny v první částí této práce, jsou zde vysvětleny základní pojmy a principy. Další část je věnována samotným členům funkční bezpečnosti. Jedná se o prvky vstupní, logické a výstupní. V další části jsou tyto poznatky uplatněny a na příkladu je zde vysvětleno stanovení a ověření úrovně vlastností a úrovně integrity bezpečnosti.

2 Normy používané v oblasti funkční bezpečnosti

2.1 ČSN EN ISO 13849 [2]

Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů

Norma má dvě části:
Část 1: Všeobecné zásady pro konstrukci
Část 2: Ověřování platnosti

Tato norma nahrazuje starou normu ČSN EN 954 - 1 a především se zabývá způsoby hodnocení bezpečnostních systémů. Jsou zde definovány úrovně vlastností PL (performance level), které jsou odvozeny od schopnosti bezpečnostních systémů vykonávat bezpečností funkci a to tak, že jsou uvedeny pravděpodobností výskytu poruchy za časový úsek (hodinu). Tyto úrovně vlastností by měly být určeny už při navrhování stroje a to určením těchto parametrů: MTTFd pro jednotlivé součásti, diagnostickým pokrytím (DC), poruchami se společnou příčinou (CCF), struktury a chování bezpečnostních funkcí v podmínce závady, systematických poruch bezpečnostního softwaru, schopnosti vykonávat bezpečností funkci v očekávaných podmínkách prostředí. Když už známe tuto úroveň vlastností, podle ní konstruktér navrhne strukturu bezpečnostního obvodu.

Určení střední doby do nebezpečné poruchy $MTTF_d$ znamená spočítat pravděpodobnost nebezpečného selhání zařízení za čas. Tyto hodnoty se určí pro jednotlivé komponenty vstupující do funkční bezpečnosti (jsou udávané výrobcem), aby se dala definovat $MTTF_d$ celého zařízení. Elektronické komponenty se v tomto ohledu určují lehce, vychází se ze statistických metod. U elektromechanických dílů musí zohlednit počet cyklů sepnutí, což vyjadřuje parametr B_{10d}. Na zřetel se také musí brát selhání, ke kterým dochází vlivem poruch se stejnou příčinou.

2.1.1 Vysvětlení nejpoužívanějších pojmů normy [2], [8]

Úroveň vlastností (PL) – při daných podmínkách určuje schopnost bezpečnostních částí ovládacích systémů k vykonávání bezpečnostní funkce

Požadovaná úroveň vlastností (PLr) – taková úroveň vlastností, při níž je dosaženo u každé bezpečnostní funkce požadovaného snížení rizika

Kategorie – základní parametr k dosažení určité úrovně vlastností

Střední doba do nebezpečné poruchy ($MTTF_d$) – doba, která se očekává do vzniku nebezpečné poruchy

Porucha se společnou příčinnou (CCF) – všechny poruchy různých objektů, které vznikly z jedné události, kde tyto poruchy nejsou vzájemným způsobem důsledkem každé z nich

Průměrné diagnostické pokrytí (DC_{avg}) – podíl intenzity poruch detekovaných nebezpečných poruch a intenzity poruch všech nebezpečných poruch

2.1.2 Určení úrovně vlastností [2]

Určuje se dle pravděpodobnosti výskytu nebezpečné poruchy, viz Tab.1 Určení úrovní vlastností.

PL - Úroveň vlastností	Průměrná pravděpodobnost nebezpečné poruchy za hodinu [1/h]
a	≥ 10 až < 10^{-4}
b	≥ 3 × 10^{-6} až < 10^{-5}
c	≥ 10^{-6} až < 3 × 10^{-6}
d	≥ 10^{-7} až < 10^{-6}
e	≥ 10^{-8} až < 10^{-7}

Tab.1 Určení úrovní vlastností

2.1.3 Výpočet střední doby do nebezpečné poruchy [2]

Tato hodnota se používá pro každý kanál zvlášť a je definována ve třech úrovních.

Doba	Rozsah doby
Krátká	3 roky ≤ $MTTF_d$ < 10 roků
Střední	10 roků ≤ $MTTF_d$ < 30 roků
Dlouhá	30 roků ≤ $MTTF_d$ < 100 roků

Tab.2 Určení Střední doby nebezpečné poruchy kanálu

$$MTTF_d = \frac{B10_d}{0{,}1 \times n_{op}}$$

Rovnice 1

2.1.4 Určení diagnostického pokrytí [2]

Jsou definovány čtyři úrovně pokrytí, které se určují analýzou možných vad a jejich následků tzv. FMEA procesu.

Označení	Rozsah
Žádné	DC < 60%
Nízké	60 % ≤ DC < 90 %
Střední	90 % ≤ DC < 99 %
Vysoké	99 % ≤ DC

Tab.3 Určení diagnostického pokrytí

Průměrné diagnostické pokrytí se řídí následujícím vztahem

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

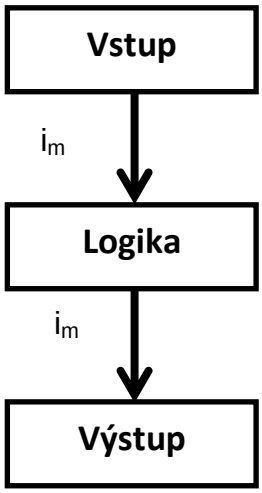
Rovnice 2

2.1.5 Struktury systému [2], [5]

Každá struktura systému se znázorňuje jako bezpečnostní blokové schéma. Je to základní parametr, kterým se určuje úroveň vlastností. Struktury se dělí do pěti bezpečnostních kategorií od B, která je nejnižší, poté 1, 2, 3 a 4, dvoukanálová struktura s diagnostikou, která je nejvyšší.

Kategorie B

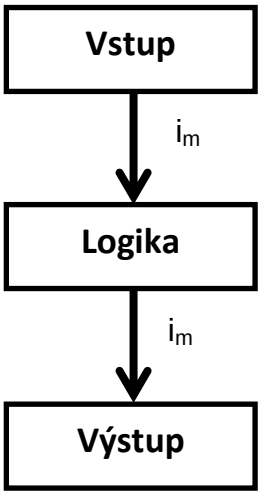
Je základní kategorií, kde porucha může vést k selhání bezpečnostní funkce.



Obr. 1 Schéma kategorie B

Kategorie 1

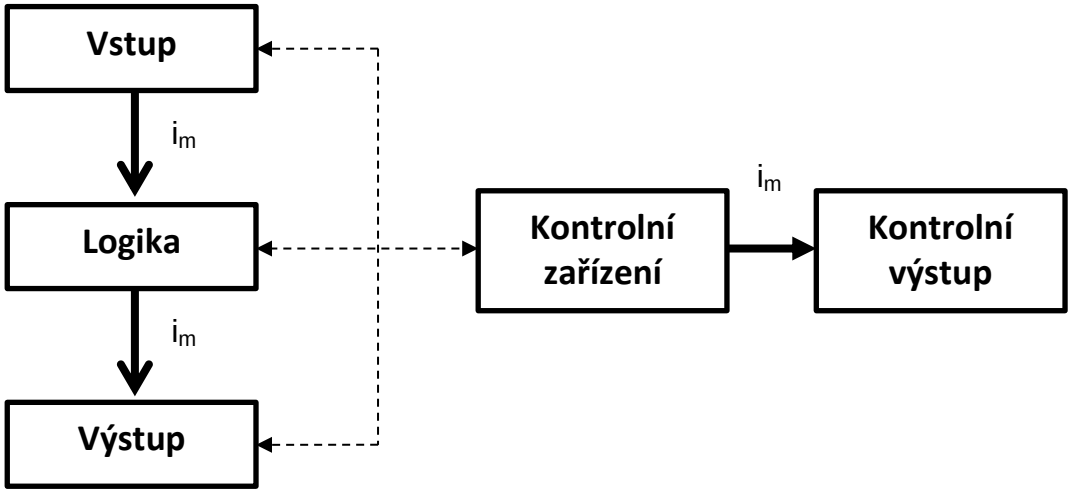
V této kategorii je pravděpodobnost selhání bezpečnostní funkce menší než základní kategorie B. $MTTF_d$ je zde tedy u každého kanálu delší než u předešlého případu.



Obr. 2 Schéma kategorie 1

Kategorie 2

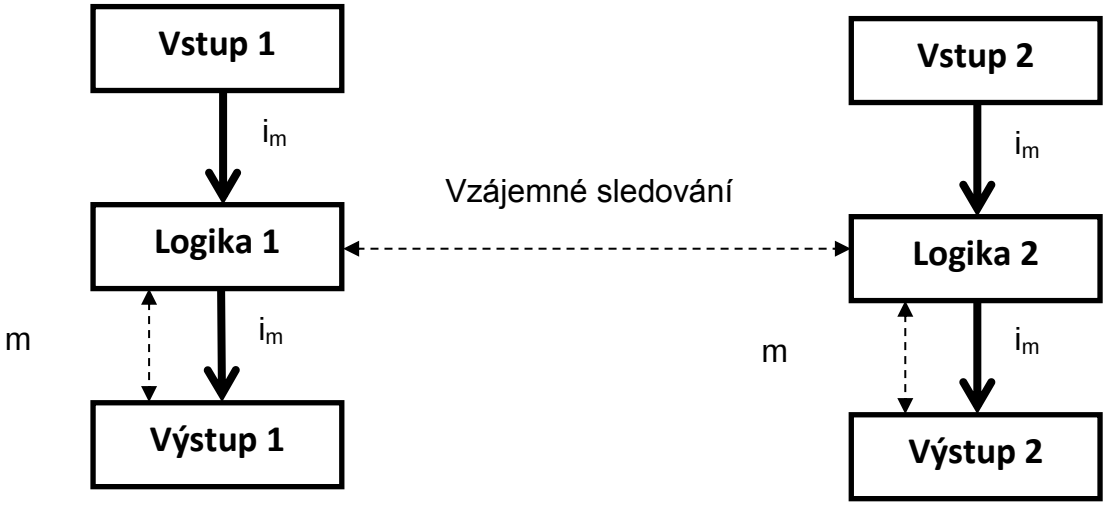
Zde sice může porucha způsobit selhání bezpečnostní funkce, to je ale při kontrole odhaleno.



Obr. 3 Schéma kategorie 2

Kategorie 3

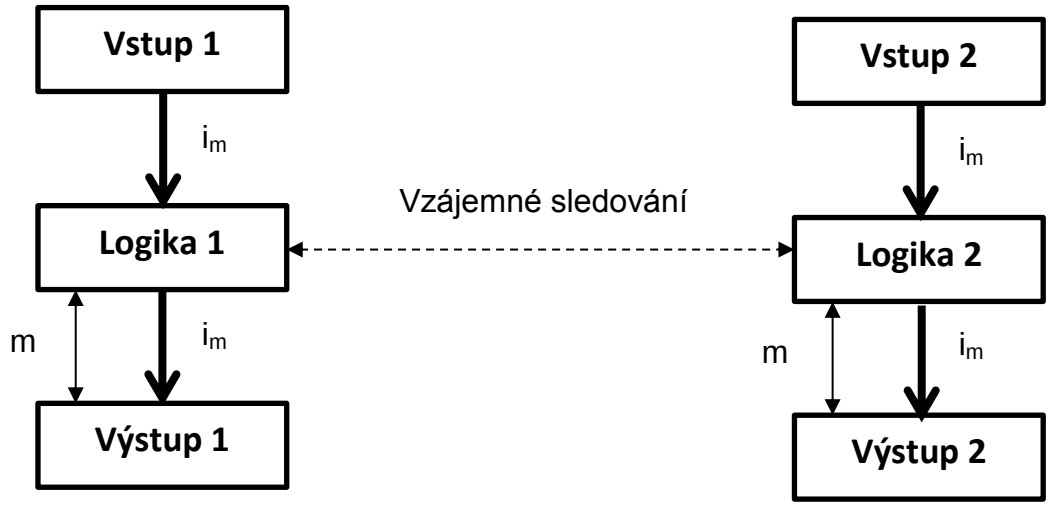
Detekce závad je u této kategorie navržena tak, aby jakákoliv závada v některé části nemohla způsobit ztrátu bezpečnostní funkce.



Obr. 4 Schéma kategorie 3

Kategorie 4

Tato kategorie nesmí dopustit ztrátu bezpečnostní funkce, tomu musí odpovídat návrh kategorie. Závady jsou zde detekovány při nebo před nejbližšími požadovanými bezpečnostními funkcemi.



Obr. 5 Schéma kategorie 4

2.2 Norma ČSN EN 62061 [4]

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

Tato norma se věnuje bezpečnosti strojních zařízení se zaměřením na funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností a je to česká verze evropské normy EN 62061:2005. Určuje požadavky a návrhy systémů, proto je důležitá pro konstruktéry strojních zařízení, výrobce řídicích systémů a ostatní osoby, které mají co do činění s vývojem, výrobou a validací těchto zařízení souvisejících s bezpečností. Řeší ale jen požadavky funkční bezpečnosti vzhledem k poranění nebo poškození zdraví osob pracujících přímo se strojem nebo pohybujících se v jeho těsné blízkosti. Nespadají sem problémy neelektrických systémů. Norma stanovuje postupy pro stanovení požadované integrity bezpečnosti pro každou řídicí funkci související s bezpečností. Dále návrh elektrických, elektronických a programovatelných řídicích systémů, který bude odpovídat daným řídicím bezpečnostním funkcím, začlenění těchto podsestav a validaci řídicích systémů souvisejících s bezpečností.

2.2.1 Vysvětlení nejpoužívanějších pojmů normy [4], [6]

Elektrické řídicí systémy - elektrické, elektronické a programovatelné elektronické řídicí systémy

SRECS – elektrické, elektronické a programovatelné elektronické řídicí systémy související s bezpečností

Architektura subsystému - je specifické uspořádání prvků v SRECS

Pravděpodobnost nebezpečné poruchy za hodinu (PFH_d) – střední pravděpodobnost nebezpečné poruchy za hodinu

Beta faktor (β) – Faktor chyb se společnou příčinou

Úroveň integrity bezpečnosti (SIL) - Diskrétní úroveň pro stanovení požadavků integrity bezpečnostních řídicích funkcí souvisejících s bezpečností. Úroveň integrity bezpečnosti tři má nejvyšší úroveň integrity bezpečnosti a úroveň jedna nejnižší

Dosažitelná mez úrovně integrity bezpečnosti (SILCL) - Maximální úroveň integrity bezpečnosti, kterou lze pro subsystém uplatňovat s ohledem na omezení architektury a systematickou integritu bezpečnosti

Řídicí systém stroje je systém, který vyhodnocuje vstupy a vhodně na ně reaguje výstupy. Jeho částí je elektrický řídicí systém, který zahrnuje všechny elektrické, elektronické a programovatelné elektronické části řídicího systému, které jsou použity pro řízení stroje.

Řídicí funkce je funkce uvnitř řídicího systému, která přijímá vstupní informace, zpracovává je a případně vyvolá podnět k výstupním členům. Řídicí funkce související s bezpečností SRCF je opět funkce, která po zpracování vstupních informací zajišťuje danou funkční bezpečnost stroje.

Diagnostická funkce SRECS je taková funkce, která detekuje poruchy bezpečnostního systému. Integrita bezpečnosti vyjadřuje pravděpodobnost, že bezpečnostní systémy budou pracovat správně.

Úroveň integrity bezpečnosti SIL může nabývat hodnot 1 - 3, kdy hodnota SIL 3 značí nejvyšší úroveň bezpečnosti a hodnota SIL 1 nejnižší. Dosažitelná mez SIL znamená největší hodnotu SIL, kterou lze za daných podmínek zaručit.

Systematickou integritou bezpečnosti se rozumí odolnost systému proti systematickým poruchám v nebezpečném režimu. Prováděním automatických diagnostických testů, tzv. diagnostické pokrytí, se snižuje výskyt nebezpečných hardwarových poruch.

2.2.2 Plán funkční bezpečnosti [4], [5]

Tento plán musí být sestaven dle normy pro každý bezpečnostní systém. Jeho základem je specifikace požadavků na funkční bezpečnost, specifikace funkčních požadavků a integrity bezpečnosti řídicí funkce související s bezpečností. Dále návrh, vývoj a specifikace požadavků na chování elektronických řídicích systémů souvisejících s bezpečností při poruchovém stavu a jejich systematickou integritu bezpečnosti. Nesmí chybět dokumentace realizace jednotlivých podsystémů, vznik diagnostických funkcí, vstup hardwarových prvků do bezpečnostního systému a vývoj softwaru. Tento plán také musí obsahovat informace o kontrole a zkouškách systému, validaci a počítat se také musí s úpravami systému. Za toto musí zodpovídat určené osoby. Všechna tato data musejí být zaznamenána a uchována.

2.2.3 Požadavky na řídicí funkce související s bezpečností [4], [5]

Každá tato funkce, která je použita, musí mít přesně specifikované funkční požadavky. Mezi ně patří pracovní prostředí to, co se od této funkce očekává z hlediska bezpečnosti, v jakých stavech stroje bude funkce pracovat a v jakých nikoliv, s tím souvisí i četnost spuštění funkce. Definovaná musí být komunikace této funkce s ostatními funkcemi stroje například zastavení stroje v nebezpečné situaci nebo v poruchovém stavu, kdy je potřeba zajistit opravu nebo údržbu stroje.

2.2.4 Elektrický řídicí systém související s bezpečností [4], [5]

Řídicí systém musí být navržen tak, aby splnil požadavky funkční bezpečnosti a integrity bezpečnosti, které jsou uvedeny ve specifikaci bezpečnostních požadavků. Systém by měl předcházet poruchám. Když se tak nestane, musí adekvátně zareagovat. S tím je spjat návrh a následný vývoj softwaru souvisejícího s bezpečností. Hardwarová architektura, která obsahuje senzory a ovládací prvky, musí splňovat požadavky na integritu bezpečnosti. Správnou volbou a uspořádáním těchto prvků se musí předcházet systematickým poruchám hardwaru. Důležitá je komunikace mezi řídicí funkcí související s bezpečností a řídicím systémem, jestliže funkce dá pokyn k zastavení stroje při nějaké nebezpečné situaci, nesmí řídicí systém uvést stroj do pohybu dříve než je porucha odstraněna.

2.2.5 Návrh elektrického řídicího systému souvisejícího s bezpečností [4], [5], [6]

Při návrhu tohoto systému se musí postupovat po daných krocích, prvním z nich je, jak už bylo zmiňováno výše, určení požadavků na každou bezpečnostní funkci. Poté je nutný rozklad každé řídicí funkce související s bezpečností do funkčních bloků a vytvoření první verze architektury elektrického řídicího systému. Bezpečnostní požadavky každého funkčního bloku musejí být podrobně popsány a přiřazeny do subsystémů. Poté přichází fáze ověřování, při které odhalíme případné nedostatky a odstraníme je. Následuje volba buď typizovaného subsystému a nebo návrh a vývoj subsystému na míru. V každém případě poté dojde k realizaci diagnostických funkcí, určení dosažitelných SIL pro danou architekturu. Architektura musí být zdokumentována a nakonec přichází konečná realizace navrženého elektrického řídicího systému souvisejícího s bezpečností.

2.2.6 Postup návrhu a vývoje subsystému [4], [5], [6]

Zde musíme opět začít rozkladem. Ten vede ke struktuře prvků, která plně respektuje funkční požadavky funkčního bloku. Důležitá je dokumentace architektury subsystému, kde se bude nalézat podrobný popis požadavků integrity bezpečnosti a funkční bezpečnosti každého prvku subsystému, případně i prvku funkčního bloku. Poté přichází stejně jako výše buď volba zařízení pro prvky subsystému, nebo návrh a vývoj prvků subsystému. Když už tyto prvky subsystému máme, musejí se začlenit do celého subsystému, při dodržení zásad pro předcházení systematických poruch. Přichází testování subsystému, kde se zjistí mez maximální integrity bezpečnosti subsystému. Celý proces musí být samozřejmě zdokumentován.

2.2.7 Úrovně integrity bezpečnosti [4], [5], [6]

Čím lepší bezpečnostní systém chceme, tím méně poruch se u něj musí vyskytovat. Mírou četnosti výskytu těchto nebezpečných poruch je integrita bezpečnosti systému, která je definována jako pravděpodobnost bezpečnostního systému, jeho plnění požadované funkce během určené doby a za určitých podmínek. Norma definuje tři úrovně integrity bezpečnosti SIL, SIL 1 až SIL 3 na integritu bezpečnosti bezpečnostních funkcí elektrických, elektronických a programovatelných systémů souvisejících s bezpečností. SIL 3 značí nejvyšší úroveň integrity bezpečnosti a SIL 1 nejnižší. Pravděpodobnost výskytu poruchy a k němu přiřazenou hodnotu SIL můžeme vidět v tabulce níže. Jak je vidět, není tam nikde 0, to znamená, že neexistuje nulové riziko, takže nelze dosáhnout absolutní bezpečnosti. Při schválení a prohlášení systému za bezpečný musí proběhnout nezávislé řízení, kterým je systém posouzen.

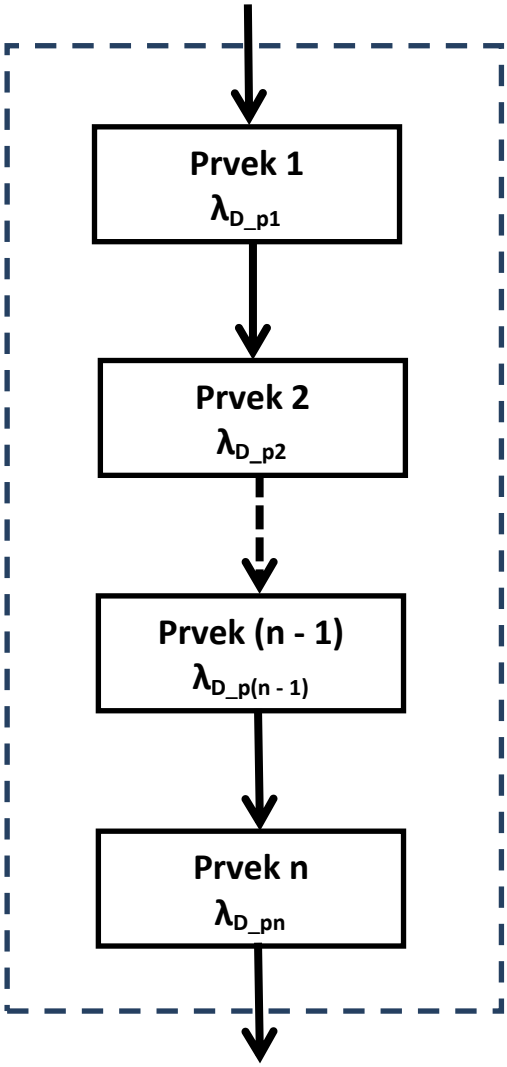
SIL	Pravděpodobnost výskytu poruchy za hodinu provozu
1	10^{-6} až $<10^{-5}$
2	10^{-7} až $<10^{-6}$
3	10^{-8} až $<10^{-7}$

Tab. 4 Určení SIL

2.2.8 **Architektury subsystémů** [4], [5]

Základní architektura subsystému A

Architektura(subsystém) A nemá žádné diagnostické funkce a jeho odolnost proti poruše je nulová.



Obr. 6 Logické uspořádání subsystému A

$$\lambda_{D\_ssA} = \lambda_{D\_p1} + \lambda_{D\_p2} + \cdots + \lambda_{D_{p(n-1)}} + \lambda_{D\_pn}$$

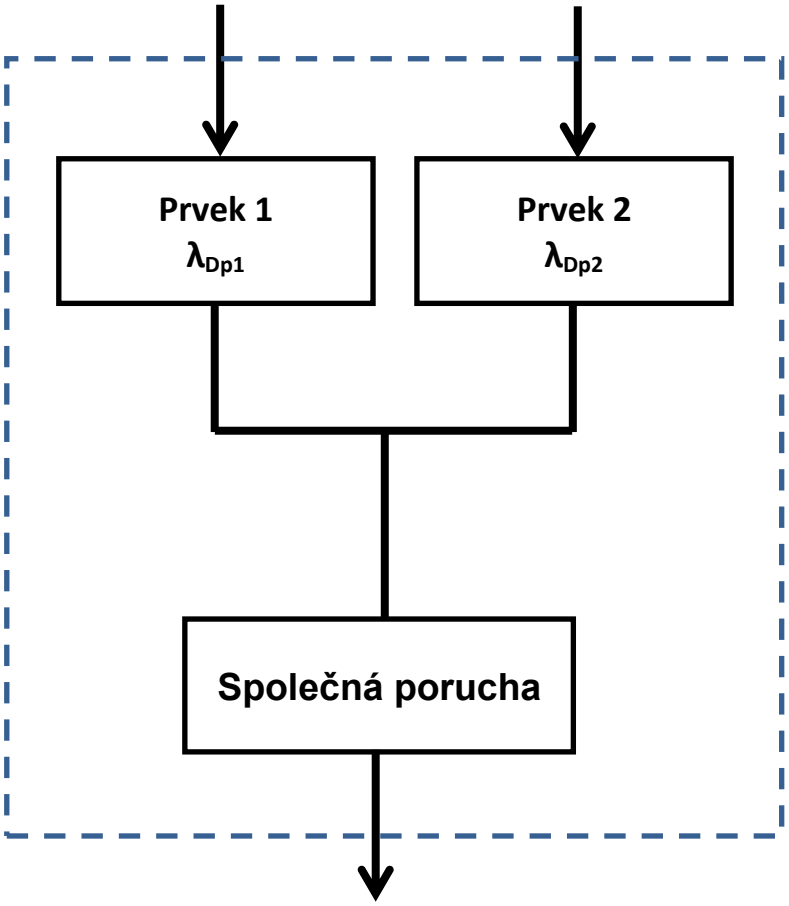
Rovnice 3

$$PFH_{D\_ssA} = \lambda_{D\_ssA} \times 1h$$

Rovnice 4

Základní architektura subsystému B

Architektura B pořád nemá žádné diagnostické funkce, ale už obsahuje odolnost proti jedné poruše. Interval kontrolní zkoušky nebo životnosti T_1 určíme z výpočtu nebo použijeme hodnotu poskytovanou výrobcem.



Obr. 7 Logické uspořádání subsystému B

$$\lambda_{D\_ssB} = (1-\beta)^2 \times \lambda_{D_{p1}} \times \lambda_{D_{p2}} \times T_1 + \beta \times \frac{(\lambda_{D_{p1}} + \lambda_{Dp2})}{2}$$

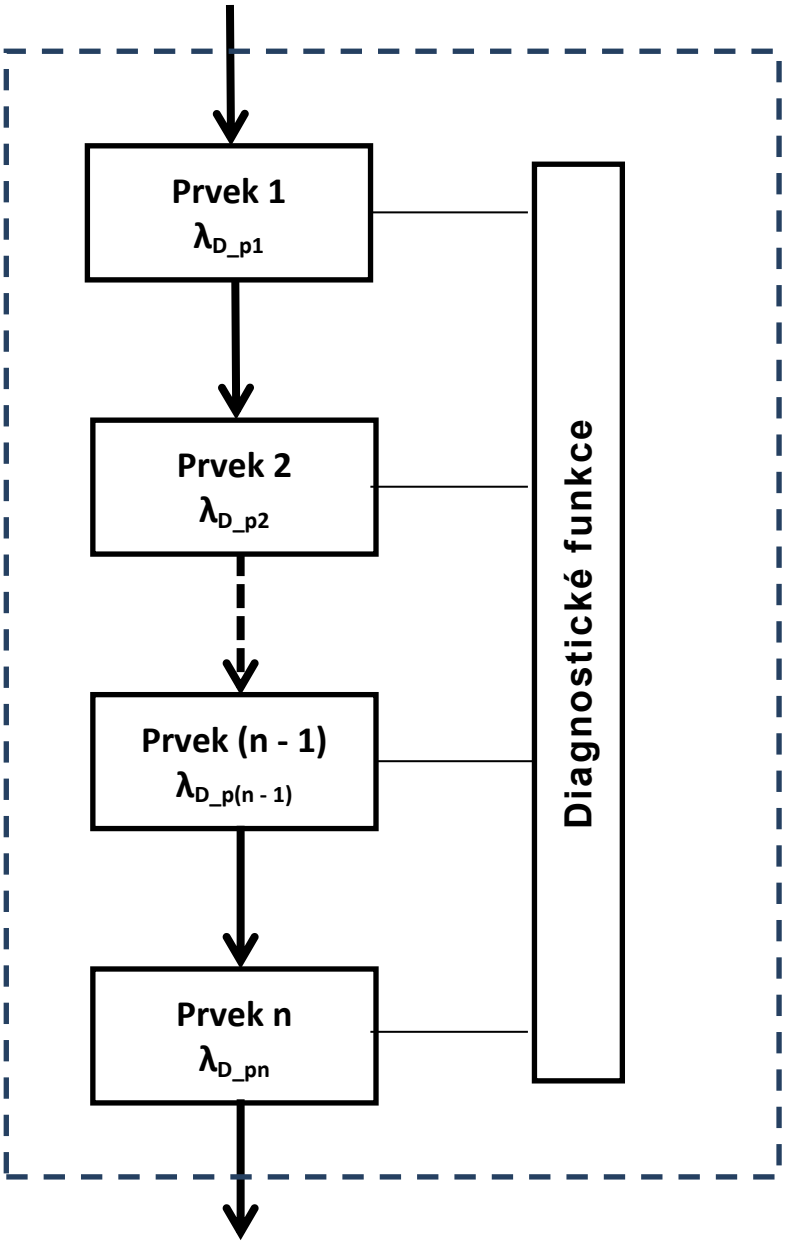
Rovnice 5

$$PFH_{D\_ssB} = \lambda_{D\_ssB} \times 1h$$

Rovnice 6

Základní architektura subsystému C

Subsystém C obsahuje diagnostickou funkci, ale má nulovou odolnost proti poruše. Diagnostické pokrytí DC nabývá hodnot dle efektivity diagnostické funkce.



Obr. 8 Logické uspořádání subsystému C

$$\lambda_{D\_ssC} = \lambda_{D\_p1}(1 - DC_1) + \lambda_{D\_p2}(1 - DC_2) + \cdots + \lambda_{D\_pn}(1 - DC_n)$$

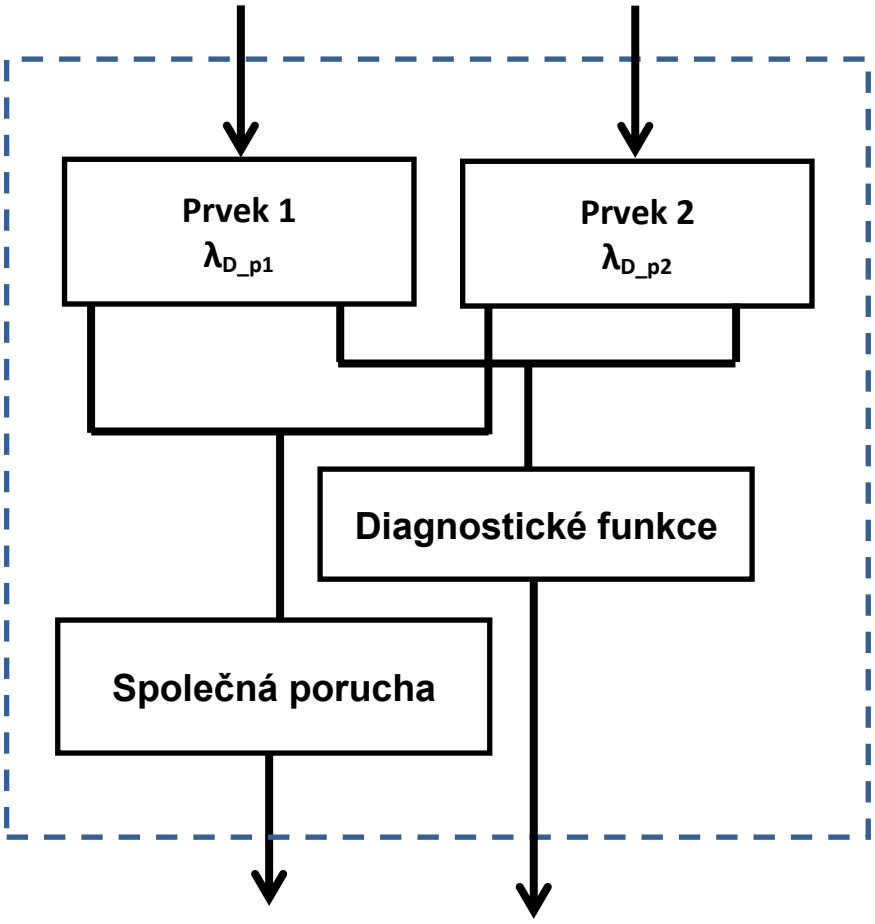
Rovnice 7

$$PFH_{D\_ssC} = \lambda_{D\_ssC} \times 1h$$

Rovnice 8

Základní architektura subsystému D

Subsystém D obsahuje diagnostickou funkci a má odolnost proti jedné poruše.



Obr. 9 Logické uspořádání subsystému D

$$\lambda_{D\_ssD} = (1-\beta)^2 \left[\left({\lambda^2}_{D\_p1} \times 2 \times DC \right) \times \frac{T_2}{2} + ({\lambda^2}_{D_{p2}} \times (1-DC)) \times T_1 \right] + \beta \times \lambda_{D\_p2}$$

Rovnice 9

$$PFH_{D\_ssD} = \lambda_{D\_ssD} \times 1h$$

Rovnice 10

2.3 Norma ČSN EN 61508 [3]

Řada těchto norem má sedm částí. Obecně se zabývají funkční bezpečností elektrických, elektronických nebo programovatelných elektronických systémů souvisejících s bezpečností. První čtyři díly normy jsou normativní a další tři jsou informativní, to znamená, že poskytují informace o tom, jak používat první čtyři díly normy.

Elektrické a elektronické prvky jsou stále velmi používané ve spojení s bezpečnostními funkcemi, avšak začínají být nahrazovány ve složitějších případech programovatelnými elektronickými systémy, které nabízejí více možností. Tyto normy také popisují technický přístup k řešení funkční bezpečnosti pomocí těchto systémů tak, aby mohl být bezpečnostní systém navržen přesně pro potřeby dané situace. Bezpečnostní systémy nejsou závislé na řídicím systému, takže při jeho výpadku nebo nesprávné funkci je bezpečnost neohrožena. Bezpečnost je zde rozdělena na primární bezpečnost, funkční bezpečnost a nepřímou bezpečnost. Tyto pojmy jsou vysvětleny níže. Podle této normy musejí být všechna rizika řízeného zařízení zkoumána a zaevidována. Jestliže se zjistí, že je nějaké riziko nepřijatelné, musí nastat opatření, aby bylo riziko odstraněno nebo zmenšeno na přípustnou hodnotu.

Rozdělení normy:
Část 1: Všeobecné požadavky
Část 2: Požadavky na elektrické, elektronické a programovatelné elektronické systémy související s bezpečností
Část 3: Požadavky na software
Část 4: Definice a zkratky
Část 5: Příklady metod určování úrovní integrity bezpečnosti
Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3
Část 7: Přehled technik a opatření

2.3.1 Vysvětlení nejpoužívanějších pojmů normy [3]

Riziko – kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození

Přípustné riziko – takové riziko, které je za daných podmínek a souvislostí přijatelné

Zbytkové riziko – riziko, které stále zbývá i po přijetí ochranných opatření

Bezpečnost – odstranění nepřijatelného rizika

Primární bezpečnost – uvažuje rizika, která můžou vzniknout přímo strojním zařízením

Nepřímá bezpečnost – není přímo ohroženo zdraví osob a jsou to vedlejší důsledky nesprávné funkce strojního zařízení

Funkční bezpečnost – bezpečnost řízeného procesu, která je ovládána elektrickými, elektronickými a programovatelnými systémy souvisejícími s bezpečností nebo jinými bezpečnostními systémy

Chyba – znamená, že zařízení není schopno vykonávat požadovanou funkci

Nebezpečná chyba – taková chyba, která zbavuje bezpečnostní systém některých jeho funkcí a uvádí strojní zařízení do nebezpečí

Bezpečná chyba – tato chyba není tolik závažná a nesmí ohrozit funkci bezpečnostního systému

Integrita bezpečnosti – je pravděpodobnost, se kterou systém související s bezpečností plní svoji bezpečnostní funkci za daných podmínek a po určitý časový úsek

Integrita bezpečnosti hardwaru – část integrity bezpečnosti, která souvisí s poruchami hardwaru

Integrita bezpečnosti softwaru – vyjadřuje pravděpodobnost, s níž software plní svoji funkci v elektrických, elektronických a programovatelných systémech souvisejících s bezpečností za daných podmínek a po určitý časový úsek

Řízené zařízení – je takový stroj, který se používá pro spojité i nespojité výrobní činnosti

Systém řízení – tento systém reaguje na vstupní signály od obsluhy a výrobního procesu vytvářením výstupů

Systém související s bezpečností – zastřešuje bezpečnostní funkce potřebné pro dosažení dané bezpečnosti a přitom musí dodržet jistou integritu bezpečnosti dané bezpečnostní funkce

Programovatelný elektronický systém – slouží k řízení a je složen i z několika programovatelných elektronických zařízení

2.3.2 Životní cyklus bezpečnosti [3], [5], [6]

Aby se zajistila a udržovala celková bezpečnost strojních zařízení, musí se dodržet patřičný postup. Prvním krokem je zpracování koncepce, kam patří systémová analýza řízeného zařízení, rešerše příslušné legislativy a standardizace. Definice oblasti použití, vzhledem k prostředí s čím souvisí stanovení rozsahu analýzy nebezpečí a rizik. Tam se identifikuje nebezpečí, nebezpečné události a sledy událostí, které vedou k nebezpečí ve všech režimech provozu. Dále se musí určit požadavky na funkční bezpečnost, integritu bezpečnosti a opatření pro snížení rizik. Po zpracování a vyhodnocení těchto informací se elektrickým, elektronickým nebo programovatelným řídicím systémům přidělí bezpečnostní funkce, u které se určí hodnota SIL. Musí být provedena celková dokumentace provozu, údržby a také instalace s uvedením do provozu. Měla by se také prověřit jiná opatření, která by mohla přispět ke snížení rizika, případně blíže specifikovat a realizovat. Po celkové instalaci a uvedení do provozu se musí provést potvrzení platnosti celkové bezpečnosti. Během provozu probíhá údržba, opravy a případné modifikace.

2.3.3 Rizika [3], [5], [6]

Další důležitá věc, která je předmětem této normy, jsou rizika. Je zde řešena vyváženost mezi opatřeními zajišťujícími bezpečnost a riziky spojenými s řízeným zařízením. Rizika je potřeba analyzovat ve třech krocích a to určení, analýza a ocenění rizika. Určení nebezpečí znamená, že se musí zmapovat všechny možné potenciální zdroje nebezpečí, a to jak při běžném provozu, tak i při nouzovém stavu a při poruše. Při analýze rizik se určují příčiny a následky zjištěného rizika. Ta může být kvalitativní nebo kvantitativní. U kvalitativní je riziko spočteno jako kombinace jeho pravděpodobnosti a následků. Při kvantitativní metodě je pravděpodobnost určována jako hodnota jejích následků a riziko je spočteno vzájemným vynásobením. U ocenění rizika porovnáváme hodnoty rizika z analýzy nebezpečí a ta musí být menší než přípustná rizika. Při všech takovýchto analýzách je normou doporučeno brát v úvahu lidský faktor, což je ovšem velmi složité. Zvolení přípustnosti rizika je velmi složitá otázka, jde o to rozhodnout jestli je nějaké riziko přípustné nebo už ne. Je zde už vkládán subjektivní pohled na věc.

2.4 Norma ČSN EN 61511 [7], [9]

Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů

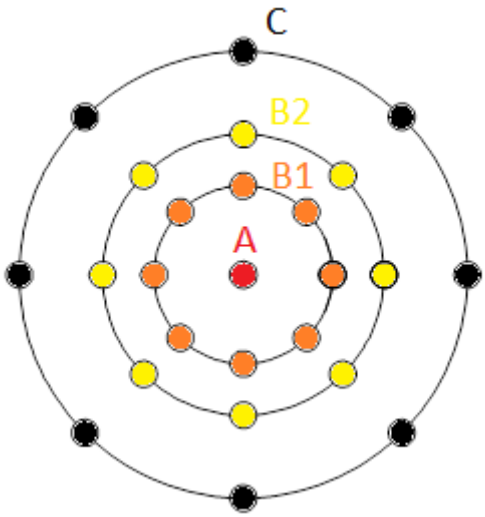
Tato technická norma se rozděluje na 3 části.
Část 1: Požadavky na systémy hardwaru a softwaru, struktura, definice
Část 2: Metodický pokyn pro používání IEC 61511-1
Část 3: Pokyn pro stanovení požadované úrovně integrity bezpečnosti

Principy zmiňované ve všech částech této normy jsou použitelné pro bezpečnostní systémy používané v procesní výrobě na rozdíl od normy ČSN EN 61508, která se touto problematikou zabývá obecně.

Jsou zde definovány tři fáze životního cyklu bezpečnostního přístrojového systému. Je to fáze analýzy, realizace a údržby. Fáze analýzy je prvním krokem cyklu funkční bezpečnosti. Určují a posuzují se zde všechna možná rizika, která slouží k návrhu požadavků na bezpečnostní systém. Následuje fáze realizace, kde se podle požadované úrovně integrity bezpečnosti a úrovně vlastností sestavuje hardwarová a softwarová podoba bezpečnostního systému. Poslední fází je už samotný provoz a údržba. Nejdůležitější specifikace této normy říká, že bezpečnostní technika musí být nezávislá na řídicí technice. Tím se zabrání možným systematickým chybám.

2.5 Evropské normy [5]

Evropské normy pro bezpečnost strojních zařízení jsou uspořádány podle tohoto schématu.



Obr. 10 Schéma uspořádání evropských norem

Normy typu A – základní bezpečnostní normy

Pro všechny strojní zařízení určují tyto normy základní pravidla, konstrukční principy a terminologii.

Normy typu B – obecné bezpečnostní normy

Tyto normy se ještě dále dělí na normy B1 a B2. Všechny se zabývají bezpečností jednoho prvku, který lze použít v mnoha strojních zařízeních.

Normy typu B1 se zabývají konkrétními bezpečnostními faktory jako je bezpečná vzdálenost, teplota, hluk.

Normy typu B2 se už zabývají konkrétními bezpečnostními prvky například kryty, blokovacími zařízeními nebo obouručním zařízením.

Normy typu C – bezpečnostní normy strojních zařízení

Tyto normy už zpracovávají bezpečnostní požadavky na konkrétní strojní zařízení.

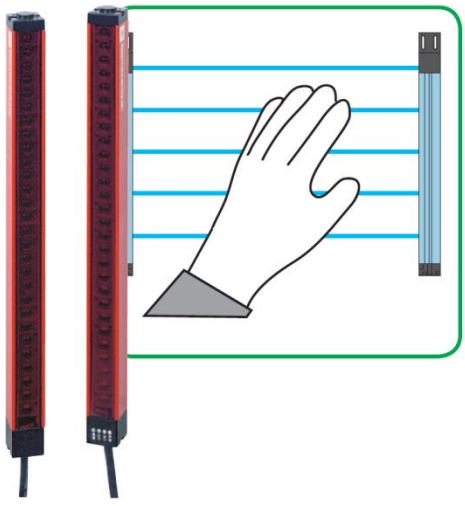
3 Prvky používané v oblasti funkční bezpečnosti

3.1 Vstupní prvky

Tato zařízení jsou prvním elementem funkční bezpečnosti, jejich úkolem je sledovat a přijímat informace, a to jak od jednotlivých částí strojních zařízení, tak od obsluhy a okolí. První skupinou jsou prvky ke snímání přítomnosti osob, tam patři světelné bariéry, 2D optický scanner nebo nově používaná technologie založená na 3D kamerovém systému. Dále blokovací zařízení, obouruční ovládání, potvrzovací spínače, tlačítka nouzového zastavení a koncové spínače.

3.1.1 **Světelné bariéry** [5], [6]

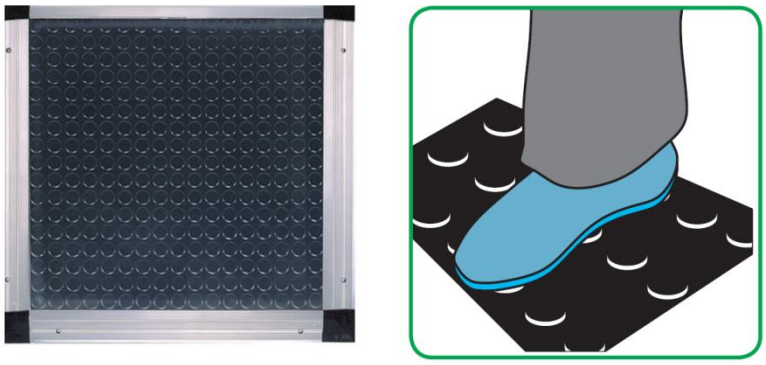
Tento prvek funkční bezpečnosti může do jisté míry nahrazovat funkci fyzických bariér (překážek) před nějakým nebezpečím a to tak, že při přerušení paprsku, který ohraničuje oblast, je pohyb stroje zastaven. Chrání tak zdraví osob, které se pohybují okolo těchto míst skrývajících nějaká rizika. Zároveň ale neznemožňují přístup na tato místa v dobu, kdy stroj nepracuje a musí se třeba seřizovat, opravovat nebo jen měnit nástroje a vyráběné dílce. To samozřejmě snižuje čas těchto operací. Tyto světelné bariéry se používají například okolo svařovacích robotů, laserovacích stanic, obráběcích center nebo při manipulaci s materiálem. Podle použití těchto bariér se musí správně zvolit jejich rozlišení. To bývá do 14 mm pro detekci prstů, do 30 mm pro detekci ruky a rozlišení větší než 30 mm.



Obr. 11 Světelné bariéry [5]

3.1.2 Bezpečnostní nášlapné rohože pro detekci osob [5], [6]

Tyto rohože se taktéž instalují okolo nebezpečné zóny jako světelné bariéry, tyto dva bezpečnostní prvky lze také zkombinovat. Funkce je zajištěna citlivostí na tlak.V případě nášlapu na tuto rohož je vyslán signál a nebezpečný pohyb stroje je zastaven. Dají se použít i na místech kde není pro jiné bezpečnostní prvky místo, mohou pracovat i v silně znečištěném prostředí, což je jedna z jejich velkých výhod.



Obr. 12 Bezpečnostní nášlapné rohože [5]

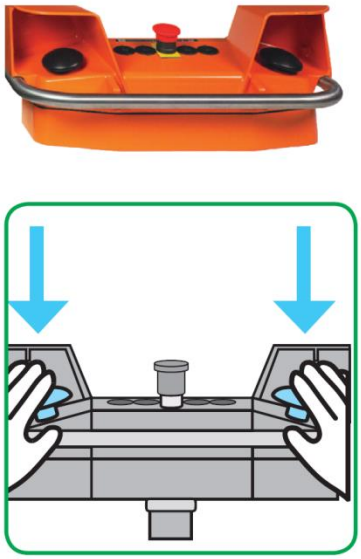
3.1.3 Blokovací zařízení ochranných krytů [5], [6]

Ochranné kryty chrání obsluhu stroje před pohyblivými částmi stroje, které by mohly způsobit říznutí, stlačení, vtažení a další poranění osob pracujících se strojními zařízeními, dále před dotknutím části stroje, kterou prochází elektrický proud. Také chrání před odletujícími třískami a hlukem. To byly ochranné kryty vnější, které oddělují okolí od pracovní části stroje. Vnitřní ochranné kryty oddělují pracovní část stroje od pohyblivých mechanizmů tak, aby se stroj nepoškodil.

Blokovací zařízení ochranných krytů může být bez přidržení, což je mechanický nebo elektrický přístroj, který sleduje polohu krytu a v případě, že je kryt otevřený, nedovolí spuštění stroje a nebo stroj zastaví, když je při provozu kryt někým otevřen. Blokovací zařízení s přidržovačem je také mechanický nebo elektrický přístroj, který se používá u strojů s vysokou setrvačností, kde je možné otevřít kryt, až když je nebezpečný pohyb zastaven. K tomu se používá zpožďovací obvod ale jen v případě, kdy se doba zastavení nebezpečného pohybu nemění. V opačném případě, když se doba zastavení mění, musí být použita detekce nulové rychlosti.

3.1.4 Obouruční ovládání [5], [6]

Tento vstupní prvek obsahuje dva ovladače, které jsou umístěny tak, aby je musel pracovník stisknout oběma rukama, a to musí učinit současně. K dalšímu opakování cyklu stroje musí pracovník ovladače uvolnit a opět stisknout. Tím je zaručena poloha pracovníka mimo nebezpečnou oblast. Používá se u obsluhy strojních lisů a raznic, kde by bylo veliké riziko úrazu rukou při manipulaci se strojem v chodu. Na ochranu dalších pracovníků by musela být použita další zařízení jako jsou například světelné bariéry nebo nášlapné rohože, které jsou zmiňovány výše.



Obr. 13 Obouruční ovládání [5]

3.1.5 Potvrzovací spínače [5], [6]

Tyto spínače se používají v prostorách, které jsou pro pracovníky nebezpečné, ve většině případů pro seřizování stroje a nářadí nebo pro údržbu. Spínač má tři polohy. První je uvolněná, když spínač není stisknut a stroj stojí. Druhá, středová poloha, která po stlačení tlačítka uvádí stroj do pohybu, ale jsou zpomaleny posuny stroje tak, aby nebyly pro pracovníka nebezpečné. Tlačítko musí být po celou dobu pohybu jednou rukou stlačeno. Je-li tlačítko přemáčknuto do třetí polohy, je všechen pohyb stroje ihned zastaven.

3.1.6 Nouzové zastavení [5], [6]

Nouzové zastavení je základní nutná součást každého stroje, která ochrání v nebezpečných situacích obsluhu, okolí, samotný stroj i zpracovávaný materiál okamžitým zastavením pohybu stroje. Tyto situace mohou nastat poruchou stroje, špatným nastavením, jinými vlastnostmi materiálu, než byly očekávány nebo jinou chybou lidského faktoru.

Nouzové zastavení může proběhnout dvěma způsoby, okamžitým odpojením přívodu energie do ovládací části stroje, tzv. neřízené zastavení. Druhá možnost je řízené zastavení, kdy je energie přiváděna do ovládací části stroje, aby mohlo proběhnout zastavení stroje, poté je přívod energie odpojen. Opětovné sepnutí kontaktů a tím i možné zapnutí je možné až po resetování nouzového tlačítka. To může být možné pootočením tlačítka, tahem nebo pomocí klíče. Tlačítka musejí být odolná proti nepříznivým vlivům svého okolí jako jsou prach, voda, vibrace nebo velký rozsah teplot.

3.1.7 Mechanické polohové spínače [5], [6]

Jinak nazvané bezpečnostní koncové spínače se používají k omezení pracovního prostoru stroje. Je zde možné použít pouze jeden polohový spínač, který má rozpínací kontakty. Tyto kontakty se rozepnou v krajní poloze. Při použití dvou spínačů má jeden také rozpínací kontakty a druhý má spínání kontaktů s vratnou pružinou.

3.2 Logické prvky [5], [6]

Slouží ke zpracování signálů z bezpečnostních prvků (většinou jsou to informace o poloze a stavu sledovaného zařízení), tedy vstupních zařízení, a to vydáváním bezpečnostních výstupních signálů. Tyto prvky se nazývají logické. Jejich volba a použití jsou závislé na požadavcích na množství zpracovaných bezpečnostních vstupů, složitosti bezpečnostních funkcí, nákladech nebo vzdálenosti, na kterou je potřeba posílat bezpečnostní signály a data.

Jednou z možností logického prvku je použití bezpečnostního relé a nebo jiné neúplné elektroniky, těmito zařízeními se dají zabezpečit úrovně vlastností až do úrovně „e“ a úroveň integrity bezpečnosti „3“.

Úplné elektronické systémy tzv. programovatelné opět mohou zaručit úroveň integrity „3“, ale zaručují o stupeň nižší úroveň vlastností. Možná je také kombinace těchto metod, a to jak mezi sebou, tak s nějakým neelektrickým prvkem, nejčastěji hydraulickým.

Bezpečnostní relé má na rozdíl od obyčejného relé samostatné kontaktní páry pro pracovní i klidové kontakty. Ty jsou odloženy odděleně v komorách kvůli izolaci různých napětí.

Dalším logickým prvkem je programovatelný logický automat (PLC), což je vlastně průmyslový počítač. PLC pracuje cyklicky podle vytvořeného programu, který je vytvořen podle dané aplikace a dá se kdykoliv v celé době životnosti bez menších problémů přeprogramovat nebo jen doladit. V řádu milisekund PLC ověří všechny vstupy, podle programu je vyhodnotí a pošle výstupní informace výstupním prvkům. Poté se program opět opakuje. Je opatřen v dnešní době hlavně digitálními vstupy a výstupy, ale je možné pracovat i se spojitými signály pomocí analogových vstupů a výstupů. Podle konstrukce jsou tyto automaty rozděleny na dvě skupiny: kompaktní systém a modulární systém. Kompaktní systém obsahuje všechny své části (procesor, vstupy, výstupy, nástroje komunikace, zdroj) v jednom modulu, jeho nevýhoda je omezení případného rozšíření systému. Naopak modulární systém má své jednotlivé části umístěny v jednotlivých modulech, které až spojené dohromady tvoří modulární systém programovatelného logického automatu. Jeho výhoda je možnost mnohem většího rozšíření oproti kompaktnímu systému.

Pomocí řídicích jednotek pohonů lze mít pod kontrolou jednoduché pohony s jedním motorem, ale i složitější koordinované víceosé pohony. Opět je zde možnost řízení analogově nebo digitálně. V nebezpečné situaci dá řídicí jednotka pokyn k zastavení nebezpečného pohybu.

Bezpečnostní řídicí systémy jsou systémy sloužící k automatizaci strojních zařízení a zároveň jsou použity jako bezpečnostní prvek. To samozřejmě snižuje náklady.

3.3 Výstupní prvky

Výstupní prvky, které můžeme taktéž pojmenovat slovem aktuátory, jsou opačná zařízení k vstupním prvkům. Zpracovanou informaci dostanou z logického prvku a převádějí ji na výstup, ten je buď silový nebo ovládací. Takovými zařízeními může být například ventil, stykač nebo relé. Tyto prvky mají pod kontrolou přívod energie, tu mohou omezit a nebo úplně odstřihnout. Dalšími jsou servo - pohony a frekvenční měniče.

3.3.1 **Stykače** [5], [6]

Spojují nebo rozpojují elektrický obvod v závislosti na potřebě, a to tak, že ovládací elektrický proud zapříčiní přitažení kotvy elektromagnetu nebo změní polohu trvalého magnetu. Může se tak stát bez zatížení nebo i při něm. Stykač má dvě polohy z toho je jedna nestálá, ta musí být udržována nějakou vnější silou. Pokud však tato síla přestane působit, stykač se vrátí do jeho stálé polohy. Dají se používat i pro velmi časté spínání (ve stovkách až tisících za hodinu).

Právě podle funkce stykače můžeme použít buď stykač zapínací, u kterého se hlavní kontakty zapínají tahem elektromagnetu, nebo vypínací. Další dělení je podle druhu elektrického proudu (střídavý proud, stejnosměrný proud). Nejdůležitějšími částmi stykačů jsou hlavní a pomocné kontakty. Hlavní kontakty, aby mohly být spínané malými silami, jsou kvůli tření ploché palcové nebo můstkové. Pomocné kontakty jsou opět buď zapínací – pracovní, nebo rozpínací – klidové.

3.3.2 **Relé** [5], [6]

Je elektromechanická součástka, která obsahuje elektromagnet a kontakty, které jsou zapínací a vypínací. Dělíme je na ty, které jsou ovládané stejnosměrným proudem, a ty, které jsou ovládané proudem střídavým. Princip je v podstatě stejný jako u stykačů - ovládací elektrický proud zapříčiní přitažení kotvy elektromagnetu nebo změní polohu trvalého magnetu. Potom nastane sepnutí spínacích kontaktů a rozepnutí vypínacích kontaktů.

4 Příklad postupu stanovení úrovně vlastností a úrovně integrity bezpečnosti

Stanovíme PL a SIL na strojním zařízení (obráběcí centrum), které je vybaveno bezpečnostním krytem. Při otevření tohoto krytu musí nastat zastavení stroje tak, aby se minimalizovalo riziko zranění obsluhy stroje. Postup je následovný: definice SIL CL a PLr tak, aby stroj splňoval požadavky na bezpečnostní funkci spojenou s bezpečnostním krytem, návrh řešení a jeho ověření.

4.1 Určení požadované úrovně integrity bezpečnosti

4.1.1 Závažnost poranění [2], [4]

Základem je odhalit a pojmenovat následky, které mohou nastat poraněním obsluhy.

V našem případě mohou nastat i těžká zranění s trvalými následky (komplikované zlomeniny a amputace prstů), proto volím hodnotu Se = 3, dle Tab. 5 doporučených klasifikací uvedené níže.

Následky zranění	Se
Smrtelné zranění nebo trvalé následky	4
Těžká zranění s trvalými následky	3
Zranění s přechodnými následky	2
Lehká zranění	1

Tab.5 Doporučené klasifikace následků zranění

4.1.2 Pravděpodobnost výskytu škody [2], [4]

Prvním faktorem ovlivňujícím pravděpodobnost výskytu škody je četnost a doba trvání ohrožení. Jelikož stroj bude pracovat v běžném provozu a celou jeho obsluhu bude provádět člověk, podle doporučeného třídění vyjde Fr = 5, viz Tab. 6.

Četnost ohrožení	Doba trvání > 10 min
≤ 1 za h	5
> 1 za h až ≤ 1 za den	5
> 1 za den až ≤ 1 za 2 týdny	4
> 1 za 2 týdny až ≤ 1 za rok	3
>1 za rok	2

Tab. 6 Četnost a doba trvání ohrožení

Druhým faktorem je pravděpodobnost výskytu nebezpečné události, kde se bere v potaz nebezpečné chování stroje i obsluhy. Pravděpodobnost výskytu nebezpečné události jsem v našem případě identifikoval jako „velmi vysokou“ s hodnotou Pr = 5, z důvodu možné práce nedostatečně kvalifikované nebo nezkušené obsluhy. Opět níže je Tab. 7 pravděpodobnosti výskytu nebezpečné události.

Pravděpodobnost výskytu	Pr
Velmi vysoká	5
Pravděpodobná	4
Možná	3
Výjimečná	2
Zanedbatelná	1

Tab. 7 Pravděpodobnosti výskytu nebezpečné události

Poslední proměnnou vstupující do této problematiky je pravděpodobnost vyvarování se nebo omezení škody. Zvolil jsem hodnotu Av = 3, kdy je za určitých podmínek možné škody omezit nebo se jich zcela vyvarovat.

Pravděpodobnost vyvarování se škody nebo omezení škody	Av
Nemožné	5
Možné za určitých podmínek	3
Pravděpodobné	1

Tab. 8 Pravděpodobnosti vyvarování se škody nebo omezení škody

Z těchto tří hodnot je vypočtena celková třída pravděpodobnosti výskytu škody.

$$Cl = Fr + Pr + Av$$

Rovnice 11

$$Cl = 5 + 5 + 3$$
$$Cl = 13$$

4.1.3 Vyhodnocení požadované úrovně integrity bezpečnosti [2], [4]

Z kombinace hodnot závažnosti poranění (u nás Se = 3) a třídy pravděpodobnosti výskytu škody (Cl = 13) určíme podle tabulky Tab. 9 hodnotu SIL = 2, což znamená, že elektronický řídicí systém spojený s bezpečností musí tuto bezpečnostní funkci zajistit v úrovni integrity bezpečnosti 2.

Se	**Cl**				
	3 – 4	***5 – 7***	***8 – 10***	***11 – 13***	***14 – 15***
4	*SIL 2*	*SIL 2*	*SIL 2*	*SIL 3*	*SIL 3*
3			*SIL 1*	*SIL 2*	*SIL 3*
2				*SIL 1*	*SIL 2*
1					*SIL 1*

Tab. 9 Stanovení SIL

4.2 Určení požadované úrovně vlastností

Analýzou rizika zranění dojdeme z grafu rizik k určení požadované úrovně vlastností.

4.2.1 Analýza rizika [4], [5]

Podobně jako u určování SIL je prvním krokem rozhodnutí o závažnosti možného poranění, v našem případě volím S_2, dle Tab. 10 určení závažnosti poranění.

Závažnost poranění	**S**
Lehké zranění	S_1
Těžké zranění nebo smrt	S_2

Tab. 10 Určení závažnosti poranění

Při definici četnosti a době vystavení jsem volil F_2, protože pojem časté vystavení nebezpečí je uváděn jako častěji než jednou za hodinu, což je náš případ. Viz Tab. 11 Četnost a doba vystavení nebezpečí.

Četnost a doba vystavení nebezpečí	**F**
Méně často nebo zřídka	F_1
Často nebo nepřetržitě	F_2

Tab. 11 Četnost a doba vystavení nebezpečí

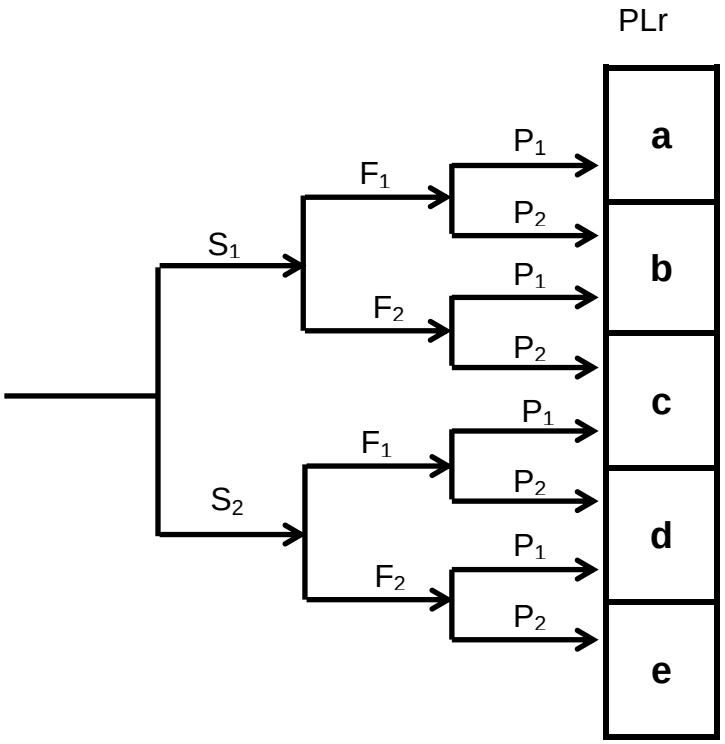
Posledním kritériem je možnost vyloučení nebezpečí. Z dvou možností je pro nás přijatelná volba P_1, reálná možnost, Tab. 12 Možnost vyloučení nebezpečí.

Možnost vyloučení nebezpečí	**P**
Reálná možnost	P_1
Žádná možnost	P_2

Tab. 12 Možnost vyloučení nebezpečí

4.2.2 Vyhodnocení požadované úrovně vlastností [4], [5]

Po zjištění těchto parametrů je z grafu rizik patrné, že požadovaná úroveň vlastností pro tuto bezpečnostní funkci je „d“.



Obr. 14 Graf rizik

4.3 Ověření SIL

Podmínky, které musí řídicí systém související s bezpečností splnit, jsou už známy, nyní je třeba ho navrhnout.

4.3.1 Návrh řešení [2], [4]

Snímání polohy ochranného krytu budou mít za úkol dva vstupní prvky, a to bezpečnostní polohové spínače LS – 02 2 N/C s $B_{10Dspín}$ = 20 000 000 cyklů, $B_{10spín}$ = 4 000 000 cyklů, 20% nebezpečných poruch a životností 20 let. Logickou analýzu bude obstarávat bezpečnostní relé ESR5 – NO – 21 – 24VAC – DC s $MTTF_d$ = 96 let, $PFH_D = 1{,}59 \times 10^{-9}$. Spínání bude prováděno dvěma stykači DILM170 s parametry $B_{10Dstyk}$ = 750 000 cyklů, B_{10styk} = 562 500 cyklů, 73% nebezpečných poruch a životností 20 let.

Další důležitý parametr je délka cyklu prováděného na strojním zařízení, v tomto případě je t_{cyklu} = 900 s, z toho vyplývá počet operací za hodinu c = 4.

4.3.2 Výpočet [2], [4]

Polohové spínače

Poruchovost prvku

$$\lambda_{espín} = 0{,}1 \times \frac{c}{B_{10spín}} = 0{,}1 \times \frac{4}{4\,000\,000} = 1 \times 10^{-7}$$

Rovnice 12

Míra nebezpečných poruch prvku

$$\lambda_{Dpspín} = \lambda_{espín} \times x = 1 \times 10^{-7} \times 0{,}2 = 2 \times 10^{-8}$$

Rovnice 13

Míra nebezpečných poruch subsystému

Subsystém spínačů je zapojen v architektuře B, kde podle kapitoly 2.2.8. počítám míru nebezpečných poruch subsystému podle **Rovnice 5** a **Rovnice 6**

$$\lambda_{D\_ssBspín} = (1-0{,}1)^2 \times 2 \times 10^{-8} \times 2 \times 10^{-8} \times 175\,200 + 0{,}1 \times \frac{(2 \times 10^{-8} + 2 \times 10^{-8})}{2}$$

$$\lambda_{D\_ssBspín} = 5{,}67 \times 10^{-11} + 2 \times 10^{-9} = 2{,}06 \times 10^{-9}$$

kde $T_{12} = min\left(životnost, \frac{B_{10D}}{c}\right) = \min\left(175\,200h, \frac{20\,000\,000}{4}\right) = 175\,200h$

Pravděpodobnost nebezpečné poruchy za hodinu

$$PFH_{D_{ssBspín}} = \lambda_{D\_ssBspín} * 1h = 2{,}06 \times 10^{-9}$$

Stykače

Poruchovost prvku – použita rovnice 12

$$\lambda_{estyk} = 0{,}1 \times \frac{c}{B_{10styk}} = 0{,}1 \times \frac{4}{562\,000} = 7{,}12 \times 10^{-7}$$

Míra nebezpečných poruch prvku – použita rovnice 13

$$\lambda_{Dpstyk} = \propto_{estyk} \times x = 7{,}12 \times 10^{-7} \times 0{,}73 = 5{,}20 \times 10^{-7}$$

Míra nebezpečných poruch subsystému

Subsystém stykačů je opět zapojen v architektuře B, kde podle kapitoly 2.2.8. počítám míru nebezpečných poruch subsystému podle **Rovnice 5** a **Rovnice 6**

$$\lambda_{D\_ssBstyk} = (1 - 0{,}1)^2 \times 5{,}20 \times 10^{-7} \times 5{,}20 \times 10^{-7} \times 175\,200 + 0{,}1 \times \frac{(5{,}20 \times 10^{-7} + 5{,}20 \times 10^{-7})}{2}$$

$$\lambda_{D\_ssBstyk} = 3{,}83 \times 10^{-8} + 5{,}20 \times 10^{-8} = 9{,}03 \times 10^{-8}$$

kde $T_{34} = min\left(\check{z}ivotnost, \frac{B_{10D}}{c}\right) = \min\left(175\,200h, \frac{175200}{4}\right) = 175\,200h$

Pravděpodobnost nebezpečné poruchy za hodinu

$$PFH_{D_{ssBstyk}} = \lambda_{D\_ssBstyk} * 1h = 9{,}03 \times 10^{-8}$$

4.3.3 Vyhodnocení SIL [2], [4]

Celková pravděpodobnost nebezpečné poruchy řídícího systému spojeného s bezpečností je součtem jednotlivých pravděpodobností všech tří subsystémů.

$$PFH_{D_{celková}} = PFH_{D_{ssBspín}} + PFH_D + PFH_{D_{ssBstyk}}$$

$$PFH_{D_{celková}} = 2{,}06 \times 10^{-9} + 1{,}59 \times 10^{-9} + 9{,}03 \times 10^{-8}$$

$$PFH_{D_{celková}} = 9{,}40 \times 10^{-8}$$

Tato hodnota odpovídá dle Tab. 4 SIL 3. Požadovaná úroveň integrity bezpečnosti má hodnotu SIL 2, tudíž jsem vytvořil systém s vyšší úrovní integrity bezpečnosti.

4.4 Ověření PL [4], [5]

4.4.1 Výpočet [4], [5]

Dle ČSN EN ISO 13849 je použito zapojení v kategorii 3, zmiňované v kapitole 2.1.5.

Střední počet operací za rok

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cyklu}}$$

Rovnice 14

$$n_{op} = \frac{220 \times 8 \times 3600}{900} = 7040\ op/rok$$

Střední doba do nebezpečné poruchy – vypočítaná dle **Rovnice 1**

$$MTTF_{dspín} = \frac{B_{10dspín}}{0{,}1 \times n_{op}} = \frac{20\,000\,000}{0{,}1 \times 7040} = 28409{,}09\ let$$

$$MTTF_{dstyk} = \frac{B_{10dstyk}}{0{,}1 \times n_{op}} = \frac{750\,000}{0{,}1 \times 7040} = 1065{,}34\ let$$

$$\frac{1}{MTTF_{dcelková}} = \frac{1}{MTTF_{dspín}} + \frac{1}{MTTF_{d}} + \frac{1}{MTTF_{dstyk}}$$

Rovnice 15

$$\frac{1}{MTTF_{dcelková}} = \frac{1}{28409{,}09} + \frac{1}{96} + \frac{1}{1065{,}34}$$

$$MTTF_{dcelková} = 87{,}79\ let$$

$MTTF_{dcelková} = 87{,}79let$ je dleTab. 2 „dlouhá“ doba do nebezpečné poruchy

Průměrné diagnostické pokrytí

Vyjádřeno **Rovnicí 2**

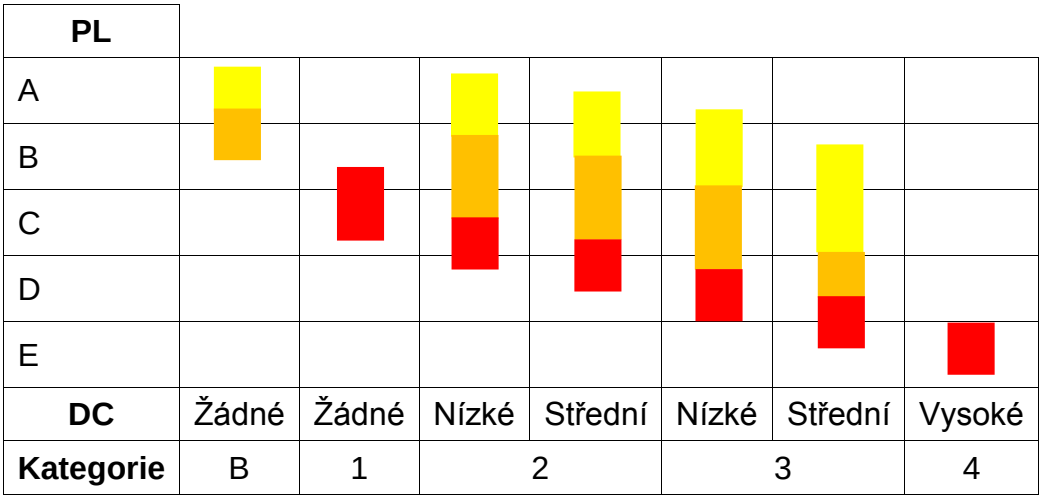
$$DC_{avg} = \frac{\frac{DC_{spín}}{MTTF_{dspín}} + \frac{DC}{MTTF_{d}} + \frac{DC_{styk}}{MTTF_{dstyk}}}{\frac{1}{MTTF_{dspín}} + \frac{1}{MTTF_{d}} + \frac{1}{MTTF_{dstyk}}}$$

$$DC_{avg} = \frac{\frac{0{,}99}{28409{,}09} + \frac{0{,}99}{96} + \frac{0}{1065{,}34}}{\frac{1}{28409{,}09} + \frac{1}{96} + \frac{1}{1065{,}34}}$$

$DC_{avg} = 0{,}91$
$DC_{avg} = 0{,}91$ odpovídá průměrnému diagnostickému pokrytí „střednímu“ dle Tab. 3.

4.4.2 Vyhodnocení PL [4], [5]

Z grafu níže pomocí zjištěného „středního“ diagnostického pokrytí, „dlouhé“ doby do nebezpečné poruchy a použití kategorie 3 vyčteme pro náš případ úroveň vlastností na přelomu „d“ a „e“, což je vyhovující, protože požadovaná úroveň vlastností je „d“.



Legenda grafu:

- $MTTF_d$ je dlouhá
- $MTTF_d$ je střední
- $MTTF_d$ je krátká

Obr. 15 Určení PL

Závěr

Tato bakalářská práce se zabývá zhodnocením současných technologií v zajišťování funkční bezpečnosti strojních zařízení. Toto téma spadá do několika technických norem, které jsou v první části práce zpracovány. Jedná se o technickou normu ČSN EN ISO 13849-1 Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů, která se zabývá hodnocením bezpečnostních systémů. Pro tyto účely jsou zde definovány pojmy: úroveň vlastností, požadovaná úroveň vlastností, střední doba do nebezpečné poruchy a diagnostické pokrytí. Dalším bodem jsou struktury systému, podle kterých jsou zapojeny prvky funkční bezpečnosti. Tyto struktury jsou rozděleny do pěti kategorií. Základní je kategorie B, u které může vlivem poruchy dojít ke ztrátě bezpečnostní funkce, naopak nejbezpečnější je kategorie 4.

V normě ČSN EN 62061 Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností jsou nejdůležitějšími pojmy dosažitelná mez úrovně integrity bezpečnosti a úroveň integrity bezpečnosti, které nabývají hodnot 1 – 3, kde 1 je nejnižší a 3 nejvyšší úroveň. Jsou zde definovány jednotlivé architektury subsystémů, od základní architektury subsystému A, která nemá žádné diagnostické funkce, tudíž je jeho odolnost proti poruše nulová až po architekturu D, která díky diagnostické funkci dokáže odolat poruše.

Ve zkratce jsou ještě zmíněny normy ČSN EN 61508 Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností a ČSN EN 61511 Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů.

V druhé části jsou zmíněny konkrétní prvky používané v oblasti funkční bezpečnosti. Mezi zmíněné vstupní prvky patří světelné bariéry, bezpečnostní nášlapné rohože pro detekci osob, obouruční ovládání, tlačítka nouzového zastavení nebo polohové spínače. Logické prvky, které zpracovávají signály ze vstupních prvků, mohou mít podobu bezpečnostního relé, bezpečnostního řídicího systému nebo programovatelného logického automatu. Na konci řetězce funkční bezpečnosti jsou výstupní prvky, které jsou zmíněny na konci této kapitoly.

Konec práce je věnován příkladu zhotovení jedné bezpečnostní funkce, na kterém jsou použity definice a prvky z prvních dvou částí práce. Na obráběcím centru po otevření bezpečnostního krytu musí dojít k zastavení nebezpečného pohybu. Byla určena požadovaná úroveň integrity bezpečnosti, která byla po návrhu řešení ověřena, a bylo zjištěno, že bezpečnostní systém zajišťuje vyšší úroveň integrity bezpečnosti, než bylo požadováno, což je v pořádku. Obdobně byla vyšetřena úroveň vlastností s opět tedy s kladným výsledkem. Návrh řešení tedy splňuje podmínky zadání.

Seznam použitých symbolů a zkratek

Označení	Legenda	rozměr
PL	úroveň vlastností	
PLr	požadovaná úroveň vlastností	
$MTTF_d$	střední doba do nebezpečné poruchy	roky
B_{10d}	počet cyklů do 10% nebezpečných selhání součástí	
n_{op}	průměrný počet operací za rok	op/rok
CCF	porucha se společnou příčinou	
DC	diagnostické pokrytí	
DC_{avg}	průměrné diagnostické pokrytí	
T_{10d}	doba provozu	h/rok
h_{op}	střední doba provozu	h/rok
d_{op}	střední doba provozu	dny/rok
t_{cyklu}	střední doba mezi začátkem dvou po sobě následujících cyklů součástí	s/cykl
PFH_d	pravděpodobnost nebezpečné poruchy za hodinu	
C	průměrný počet cyklů za hodinu	
β	beta faktor	
SIL	úroveň integrity bezpečnosti	
SILCL	dosažitelná mez úrovně integrity bezpečnosti	
T_n	interval diagnostické zkoušky	
Se	následky zranění	
Cl	pravděpodobnost výskytu škody	
Fr	četnost a doba trvání ohrožení	
Pr	pravděpodobnost výskytu nebezpečné události	
Av	pravděpodobnost vyvarování se nebo omezení škody	

S	závažnost poranění	
F	četnost a doba vystavení nebezpečí	
P	možnost vyloučení nebezpečí	
λ_e	poruchovost prvku	
λ_{Dp}	míra nebezpečných poruch prvku	
λ_D	míra nebezpečných poruch subsystému	

Seznam použitých zdrojů

[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 13849-1: 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

[5] Bezpečnostní příručka pro strojní zařízení - Schneider Electric CZ, s. r. o., 08-2010 (dostupný z: http://www.schneider-electric.cz/sites/czech republic/cz/reseni/oem/strojni-bezpecnost/bezpecnostni-prirucka.page)

[6] Bezpečnostní prvky pro strojní zařízení Eaton (dostupný z: http://www.eatonelektrotechnika.cz/produkty-prumyslove_instalace-ovladani_signalizace-bezpecnostni_rele_esr?view=tiskoviny&view_id=385)

[7] ČSN EN 61511-x: Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů. [s.l.]: ÚNMZ

[8] ČSN EN ISO 13849-1 – co se nezmění [online]. Časopis AUTOMA [cit. 2014-05-03]. Dostupné z: http://www.odbornecasopisy.cz/csn-en-iso-13849-1-–-co-se-nezmeni-44464.html

Seznam obrázků, schémat a grafů

Seznam tabulek