České vysoké učení technické v Praze
Fakulta elektrotechnická

DIPLOMOVÁ PRÁCE

Bezpečnost strojů a opatření ke snížení rizik

Praha, 2011 **Autor: Bc. Josef Necid**

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

V Praze dne _____ _____

podpis

Poděkování

Děkuji vedoucímu práce Ing. Pavlu Burgetovi PhD., Ing. Ondřeji Nývltovi a společnosti B&R za cenné rady při řešení zadaných úkolů. Samozřejmě děkuji rodině, přátelům a kolegům za komplexní podporu během celého studia.

Abstrakt

Tato práce pojednává o bezpečnosti strojních zařízení. V práci jsou definovány nejdůležitější pojmy bezpečnosti strojů definované v normě ČSN EN 61508, využití této normy a popis jednotlivých kroků pro její splnění. Dále je uvedena krátká specifikace s bezpečnostního protokolu openSAFETY. Praktickou částí práce je riziková analýza, návrh a realizace bezpečnostních opatření pro dvě rozdílné strojní zařízení. Jedním ze zařízení je model Žonglér, stroj Katedry řídicí techniky Fakulty elektrotechnické ČVUT v Praze a druhým zařízením je CNC pálicí a vrtací stroj společnosti Vanad 2000 a.s. Práce dále obsahuje případovou studii na zabezpečení visuté lanové dráhy.

Abstract

This thesis deals with machine safety. There are specified basic terms of machine safety, which are defined in the ČSN EN 61508 standard. There is a short specification of an openSAFETY protokol too. Practical part of this thesis is a risk analysis, design and realization of safety equipments for two different machines. First machine is the Juggler model and the second is a CNC machine for burning and boring, which was developed by Vanad 2000 a.s. company. This thesis include the case study for cableway safety.

vložit originální zadáníííííííííííííííííí !!!!!

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých značek

B_{10}	$[-]$	statistické 10% rozhraní pro elektrickou životnost udávanou výrobcem
C	$[1/h]$	počet sepnutí za hodinu
β	[-]	citlivost na jednotlivé poruchy
λ	$[1/h]$	intenzita nebezpečných poruch
λ_D	$[1/h]$	intenzita detekovatelných nebezpečných poruch
λ_U	$[1/h]$	intenzita nedetekovatelných nebezpečných poruch
$MCTF$	$[1/h]$	střední počet cyklů do poruchy (Mean Cycles Time to Failure)
$MTTF$	$[1/h]$	střední čas do poruchy (Mean Time To Failure)
$MTTR$	$[h]$	střední doba do zotavení systému (Mean Time To Repair)
PFD	$[h]$	průměrná pravděpodobnost poruchy při vyžádání (Propability of Failure on Demand)
T_1	$[h]$	četnost testování systému v hodinách

Seznam použitých zkratek

ALARP	As Low As Reasonably Practicable (nejnižší rozumně proveditelný)
E/E/EPS	Elektrický/elektronický/elektronický programovatelný systém
SD	openSAFETY Domain
MN	POWERLINK managing node
MooN	Výběr M prvků z N
PL	Performance level (úroveň vlastností)
PLC	Programmable logic controller (programovatelná logická řídicí jednotka)
SCM	Safety Configuration Manager
SIF	Safety Integrity Function (bezpečnostní integrovaná funkce)
SIL	Safety Integrity Level (úroveň integrity bezpečnosti)
SIS	Safety Integrated System (bezpečnostní integrovaný systém)
SN	openSAFETY Node

Kapitola 1

Úvod

Bezpečnost strojních zařízení je, zejména v poslední době, velice diskutovanou záležitostí ve strojním průmyslu. Na každém zařízení, nejen stojním, lze definovat velké množství typů bezpečností (požární, elektrickou atp.), které musí výrobce zařízení bezpodmínečně dodržet. Různými druhy bezpečností se zabývá velké množství mezinárodních i českých závazných, které každé strojní zařízení musí splňovat. Tato množina závazných norem, je dále doplněna některými nezávaznými, avšak doporučenými normami.

Zaměřením této práce je jeden z druhů bezpečnosti, tzv. **fukční bezpečnost**. Tento pojem se začal vyskytovat v souvislosti s normou **ČSN EN 954-1: 1998** *Bezpečnost strojních zařízení - Bezpečnostní části řídicích systémů*. Jak již název funkční bezpečnost napovídá, jedná se o postupy, návody a požadavky na funkce a parametry bezpečnostního systému při výskytu nežádoucí události, vznikající nesprávnou funkcí zařízení.

V dnešní době se zmíněnou formou bezpečnosti zabývají minimálně normy ČSN EN ISO 13849 - *Bezpečnost strojních zařízení*, ČSN EN 62061 - *Bezpečnost strojních zařízení- Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídících systémů souvisejících s bezpečností* a ČSN EN 61508 - *Funkční bezpečnost elektrických/elektronických/progamovatelných elektronických systémů související s bezpečností*. Pro potřeby této práce se jako nejvhodnější jeví norma ČSN EN 61508 zejména pro svojí obecnost a pokrytí obou dalších zmíněných norem. V praxi se spíše používá norma ČSN EN 13849, ovšem použití postupu dle ČSN EN 61508 je složitější ale také správné.

Uvedené normy řeší požadavky na návrh a funkci bezpečnostního systému, navrženého pro zabránění nežádoucím událostem. Tyto nežádoucí události lze identifikovat několika rozličnými způsoby, danými konstrukcí zařízení, dobou od uvedení do provozu a dalšími faktory.

Cílem této práce je analyzovat postupy používané k odstranění a minimalizaci rizik v praxi, a pomocí těchto postupů najít nežádoucí události a aplikovat (teoreticky i prakticky) bezpečnostní opatření na vybraná strojní zařízení tak, aby byly kompatibilní s uvedenými normami.

Praktickou částí této práce je aplikace teoretických poznatků analýzy rizik, zabezpečení zařízení a návrh bezpečnostního integrovaného systému pro výukový model Žonglér, jeho popis a realizaci. Další částí je analýza rizik strojů společnosti Vanad 2000 s.r.o. a návrh bezpečnostních opatření zamezující výskytu těchto rizik včetně doporučených hardwarových prvků. Práce obsahuje i případovou studii na zabezpečení modelové visuté sedačkové lanové dráhy.

Kapitola 2

Postupy pro odstranění rizik

Cílem této kapitoly je seznámení se s jednotlivými normami používanými k zajištění zejména funkční bezpečnosti strojů, s metodami z těchto norem vyplývajících, způsoby hodnocení rizik a postupy pro jejich odstranění. Jsou zde také zmíněny normy závazné pro bezpečnost lanových drah a jejich srovnání s normou EN 61508. Poslední částí je stručné seznámení s bezpečnostním protokolem openSAFETY.

2.1 Právní předpisy

Pro nově vyráběné strojní zařízení platí Zákon č. 22/1997 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů, doplněný ještě Nařízením č. 176/2008 Sb. o technických požadavcích na strojní zařízení. Tyto dva legislativní prvky popisují požadavky jak na nově vyráběná strojní zařízení, tak i na již používaná zařízení. Tyto předpisy jsou pro výrobce strojů z právního hlediska závazné a jejich stručnou specifikaci lze najít v [26].

2.2 Normy zabývající se funkční bezpečností

Jak je uvedeno již v úvodu, první normou, která definovala pojem funkční bezpečnosti byla norma **ČSN EN 954-1: 1998**, jenž byla nahrazena dnes platnou normou ČSN ISO 13849. Tuto normu zpravidla využívá výrobce strojů a strojních zařízení. Bezpečností strojních zařízení se zabývají ještě normy ČSN/IEC EN 61508 a ČSN/IEC EN 61061.

Normy EN 62061 a ISO 13849 jsou určeny k zajištění bezpečnosti strojních zařízení, zatímco EN 61508 je obecná norma pro návrh a realizaci funkční bezpečnosti pro jakékoliv zařízení. Použití jakékoliv z uvedených norem a splnění požadavků jedné z těchto norem zajišťuje základní požadavky bezpečnosti. Pro další potřeby práce byla pro svoji obecnost zvolena norma EN 61508.

2.2.1 Norma ČSN EN 61508

Norma ČSN EN 61508 - Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností, je nejkomplexnější a nejobecnější normou zabývající se bezpečností strojů z pohledu funkční bezpečnosti. Je složena ze sedmi částí, pro dokonalé pokrytí všech aspektů náležících správnému návrhu, realizaci a testování funkčních bezpečnostních systémů.

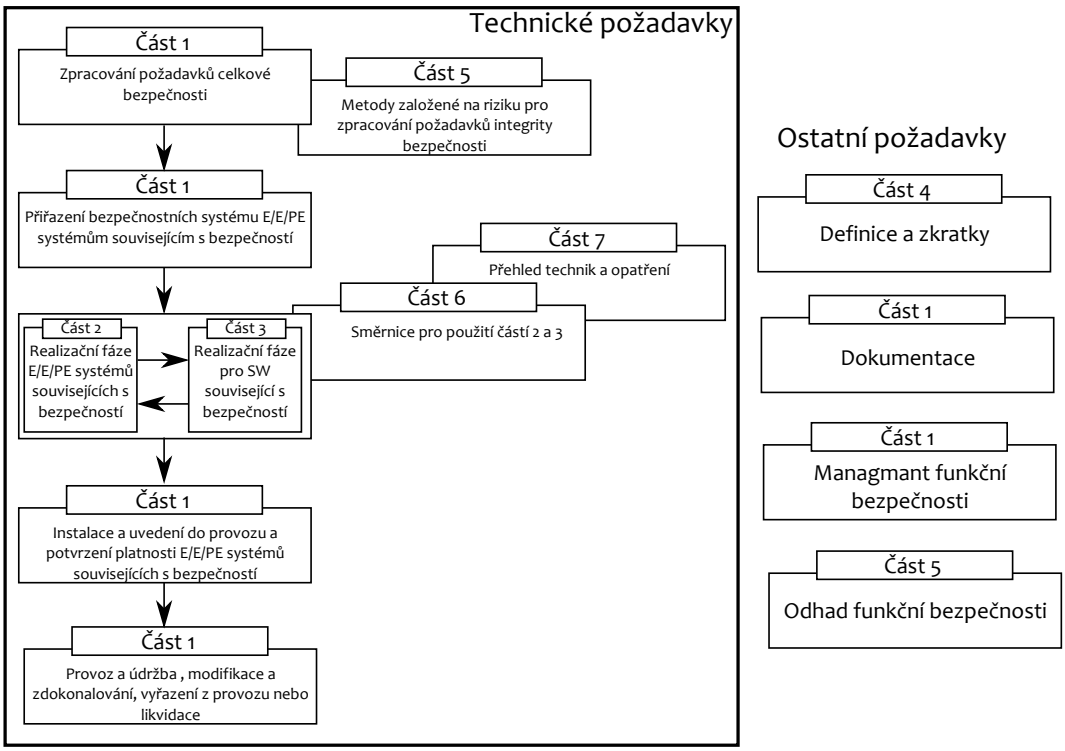
Část	Název části
Část 1	Všeobecné požadavky
Část 2	Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností
Část 3	Požadavky na software
Část 4	Definice a zkratky
Část 5	Příklady metod určování integrity bezpečnosti
Část 6	Metodické pokyny pro použití ČSN EN 61508-2 a ČSN EN 61508-3
Část 7	Přehled technik a opatření

Tabulka 2.1: Části normy ČSN EN 61508

V tabulce 2.1 jsou uvedeny jednotlivé části normy a jejich podíl na návrhu a realizaci bezpečnostního systému ilustruje obrázek 2.1. V následujících částech jsou rozebrány důležité pojmy a postupy nezbytné pro plné pochopení dalších kapitol této práce bez nutnosti studia celé normy. Tyto části ovšem nelze obecně využít pro návrh a shodu s normou ČSN EN 61508

2.2.1.1 Definice nejdůležitějších pojmů použitých normou

Definice vychází z části 4 normy.



Obrázek 2.1: Celková struktura normy

- **bezpečnostní funkce** je konkrétní realizace opatření pro zajištění bezpečnosti systému.
- **funkční bezpečnost** je bezpečnost týkající se řízených zařízení a systémů jejich řízení. Funkční bezpečnost je závislá na správném fungování E/E/PE systémů souvisejících s bezpečností a systémech založených na jiných principech.
- **integrita bezpečnosti** je pravděpodobnost spolehlivě plnit bezpečnostní funkce
- **riziko** je kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození
- **úroveň integrity bezpečnosti** (SIL) je jedna ze čtyř hodnot přiřazena integritě bezpečnosti. SIL 4 značí nejvyšší úroveň bezpečnosti.
- **životní cyklus bezpečnosti** udává veškeré činnosti spojené s řešením bezpečnosti od konceptu až po likvidaci bezpečnostního zařízení.

2.2.1.2 Výběr nejdůležitějších ustanovení a metod normy ČSN EN 61508

2.2.1.2.1 Životní cyklus celkové bezpečnosti zahrnuje všechny činnosti od návrhu, přes realizaci a údržbu bezpečnostního systému, až po jeho vyřazení z provozu.

Životní cyklus celkové bezpečnosti ilustruje obrázek 2.2.

2.2.1.2.2 Stručný popis jednotlivých fází životního cyklu

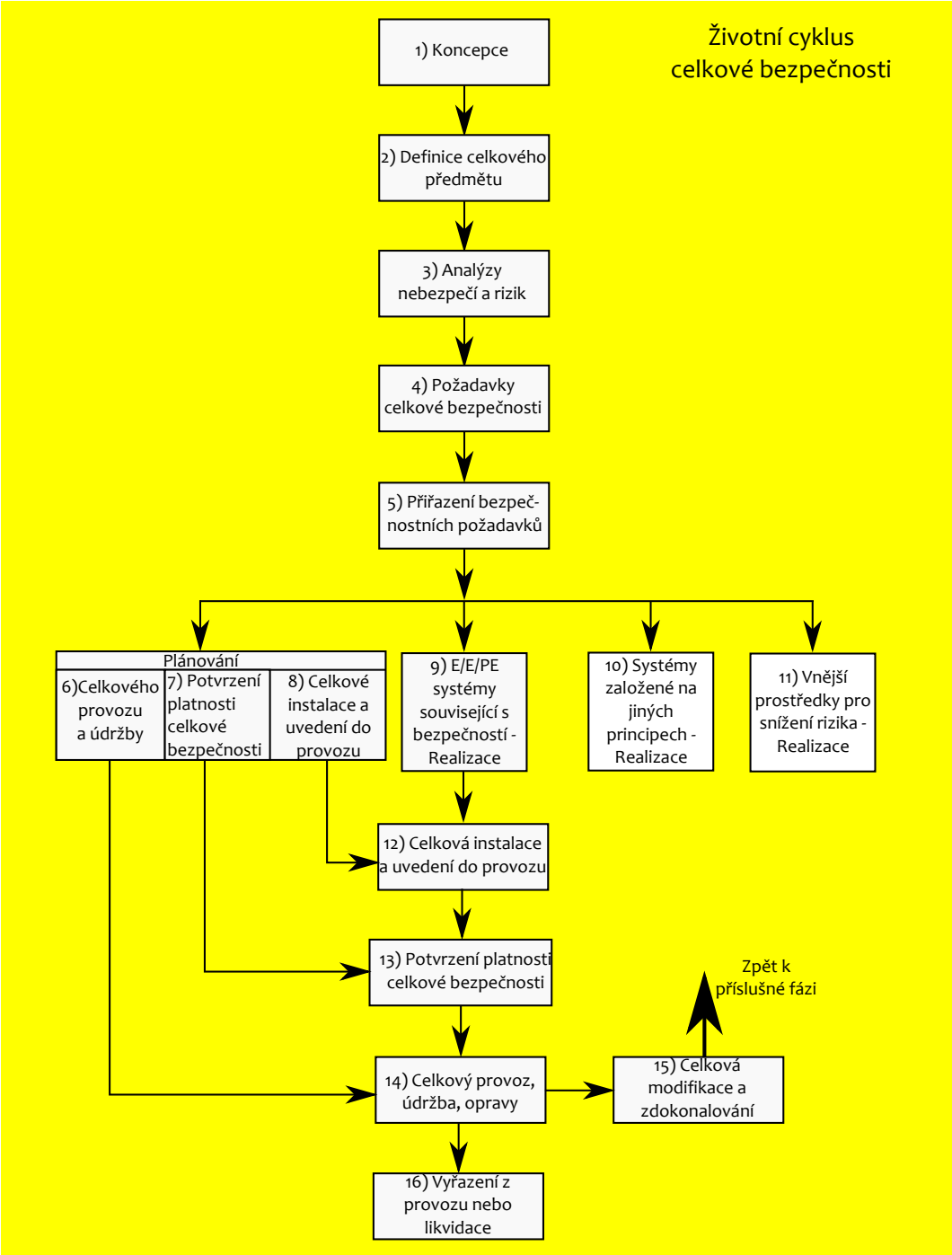
Koncepce je první částí ŽC a v jejím průběhu je nutné pochopit funkce a principy zařízení určeného pro návrh bezpečnosti. Je nutné zajistit co nejkomplexnější analýzy podmínek provozu a prostředí, ve kterém se provoz zařízení předpokládá.

Definice celkového předmětu je požadavek na stanovení předmětu, určeného pro analýzu rizik. Nutností je specifikovat vnější události a možné příčiny vzniku rizika.

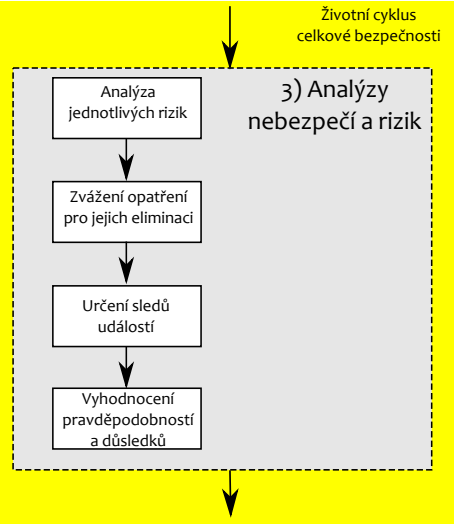
Analýzy nebezpečí rizik mají za úkol identifikovat všechna možná myslitelná rizika, která se mohou na zařízení vyskytnout vlivem selhání obsluhy, nesprávného použití nebo poruchy zařízení a určení sledu událostí, které mohou tato rizika vyvolat. Riziková analýza musí být vždy, pro každé zařízení aktuální, tzn. že v případě, kdy se provedou změny na zařízení v době po rizikové analýze, je nutné provést dodatečnou analýzu. Tato analýza probíhá pomocí kvalitativních nebo kvantitativních metod analýzy rizik. Ty jsou popsány v části 5 normy. Použití kvalitativních nebo kvantitativních metod závisí na každé jednotlivé aplikaci zvlášť, zejména na dostupnosti přesných statistických dat. Správná analýza rizik zvažuje okolnosti a pravděpodobnosti výskytu jednotlivých rizik, požadavky na snížení rizik a očekávané četnosti jednotlivých poruch. Sled jednotlivých částí ukazuje obrázek 2.3.

Požadavky celkové bezpečnosti jsou prostředky snížení každého jednotlivého rizika z předchozího kroku. Tyto celkové požadavky popisují jednotlivé bezpečnostní funkce systému pro dosažení požadované funkční bezpečnosti navržené pro každou nežádoucí událost plynoucí z analýzy rizik. Pro každou bezpečnostní funkci je nutné stanovit požadovanou úroveň integrity bezpečnosti a zjištění i požadavků na celkovou integritu bezpečnosti zařízení.

Přiřazení bezpečnostních požadavků má za úkol přiřadit bezpečnostní požadavky navrhovaným bezpečnostním systémům a přiřazení úrovně integrity



Obrázek 2.2: Životní cyklus celkové bezpečnosti



Obrázek 2.3: Vývojový diagram analýzy rizik

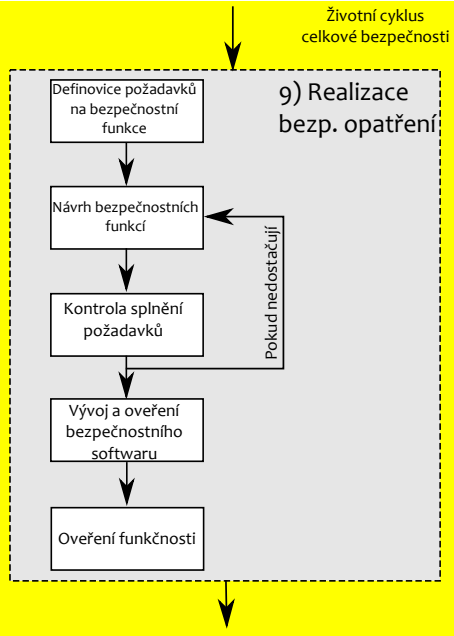
bezpečnosti jednotlivým bezpečnostním funkcím. Každá bezpečnostní funkce musí být pak přiřazena bezpečnostnímu systému tak, aby bylo dosaženo požadovaného snížení rizik.

Plánování se skládá ze tří částí. Plánování celkového provozu údržby musí definovat požadavky na údržbu celého systému pro zachování dané úrovně integrity bezpečnosti. Plánování potvrzení platnosti celkové bezpečnosti zase definuje požadavky na metody, techniky a osoby, jež mají potvrdit dosažené úrovně bezpečnosti pro jednotlivé režimy provozu. Z plánování celkové instalace pak vychází povinnost sestavení plánů instalace E/E/PE bezpečnostních systémů a požadavky pro jejich uvedení do provozu.

Realizace E/E/PES se opět skládá z několika kroků. Sekvenci těchto kroků ukazuje diagram 2.4.

Definice požadavků na bezpečnostní funkce slouží k zařazení možných rizik, pro zjištění jeho závažnosti. K tomu je určeno několik metod a způsobů. Jedním z nich je koncepce **ALARP**, která dělí rizika do tří skupin. skupin.

- Nebezpečné riziko, které musí být bezpodmínečně odstraněno
- Přípustné riziko, jehož existence je vzhledem k jeho povaze přijatelná
- Riziko ALARP, které je mezi nepřijatelným a přípustným rizikem. Udává povinnost snížit riziko do té míry, do která je v rozumné míře investic proveditelná. Riziko této



Obrázek 2.4: Vývojový diagram realizace bezpečnostních opatření

kategorie, které je eliminováno nejvyšší rozumnou investicí do zabezpečení může v této kategorii zůstat při splnění bezpečnostních požadavků.

Kategorie jednotlivých rizik je určena z tzv. matice rizik. Pro každé riziko se odhadne četnost jeho výskytu a jeho očekávaný následek. Z kombinací četností a následků se poté utvoří již zmíněná matice rizik (tabulka 2.2), která určí i tzv. třídu rizika z rozmezí I - IV. Zařazení jednotlivých rizik do kategorií četností a následků záleží ve velké míře na osobě, která zařazení provádí.

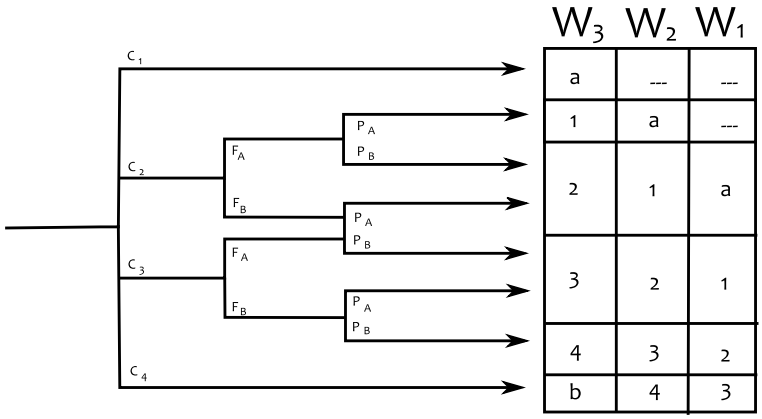
- Třída I obsahuje nepřípustné riziko
- Třída II je riziko z kategorie ALARP jehož snížení je neproveditelné nebo ekonomicky velice nevýhodné
- Třída III je riziko z kategorie ALARP přípustné v případě že by náklady na jeho další snížení přesáhly zlepšení
- Třída IV obsahuje riziko, jehož existence je přípustná

Použití matice rizik se v dalších částech práce vztahuje hlavně k návrhu bezpečnostních opatření založených na jiných technických principech než funkčním zabezpečení.

Četnost/Následek	Neuvěřitelná	Nepravděp.	Málo častá	Příležit.	Pravděp.	Častá
Katastrofální	IV	III	II	I	I	I
Kritický	IV	III	III	II	I	I
Nepodstatný	IV	IV	III	III	II	I
Zanedbatelný	IV	IV	IV	III	III	II

Tabulka 2.2: Matice rizik

Pro rizika, u nichž se předpokládá jejich ošetření pomocí funkčního bezpečnostního prvku je nutné znát požadavky na **úroveň integrity bezpečnosti**. K určení SIL lze použít dva typy metod. Kvantitativní, které lze použít v případě, že máme o daném zařízení velké množství vypovídajících informací. V našem případě se jako výhodnější jeví využít jednu z kvalitativních metod využívající tzv. diagramu rizika, viz obrázek 2.5.



Obrázek 2.5: Diagram rizika

Diagram rizika uvažuje pro přisouzení požadované SIL úrovně tyto parametry:

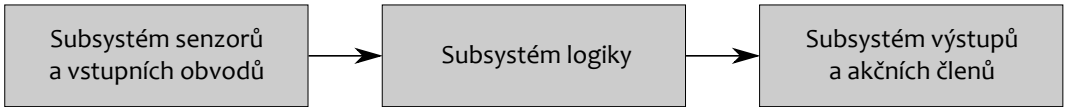
- **Následek (C)** dělený do kategorií 1 (malé zranění) až 4 (smrt velkého počtu lidí)
- **Doba vystavení v nebezpečné oblasti (F)** s kategoriemi A (vzácné vystavení) a B (časté až trvalé vystavení v nebezpečné oblasti)
- **Možnost vyhnutí se nebezpečné události (P)** s kategorií A (možné vyhnutí se za určitých podmínek nebezpečné události) a kategorií B (nemožnost vyhnutí se události)
- **Pravděpodobnost výskytu (W)** s kategoriemi 1 (velmi malá pravděpodobnost) až 3 (velká pravděpodobnost výskytu nežádoucích jevů).

Každému riziku určenému pro stanovení požadované úrovně integrity bezpečnosti se na základě parametrů vynesených do diagramu rizika stanoví požadovaná úroveň integrity bezpečnosti v rozsahu SIL 1 - SIL 4, popřípadě konstatování, že toto nebezpečí nepotřebuje žádné (—) nebo speciální požadavky (a). Pro velice závažná rizika může být nutné použít více E/E/PES (b).

V kroku *návrh bezpečnostních opatření* je zapotřebí definovat bezpečnostní funkce, které mají za úkol eliminovat jednotlivá rizika a zvolit hardwarové prvky pro realizaci těchto rizik. Při tomto kroku je nutné věnovat zvýšenou pozornost části 2 normy EN 61508.

Pro *kontrolu splnění požadavků* na úroveň zabezpečení systému lze použít například parametr PFD, který udává pravděpodobnost, že bezpečnostní systém v případě jeho vyžádání selže.

Celková úroveň zabezpečení systému se skládá ze tří částí (subsystémů) spolu sériově spojených. Tyto subsystémy ilustruje obrázek 2.6.



Obrázek 2.6: Diagram rizika

Každý subsystém je charakterizován svojí hodnotou PFD_i odpovídající jednotlivým hodnotám prvků subsystému a celková hodnota PFD pro celý systém je potom dána jako

$$\sum_i PFD_i. \tag{2.1}$$

Výsledná hodnota PFD se zařadí do jedné ze čtyř kategorií pro úrovně SIL podle tabulky 2.3.

SIL	Rozsah PFD
4	$< 10^{-4}$
3	$< 10^{-4},\ 10^{-3})$
2	$< 10^{-3},\ 10^{-2})$
1	$< 10^{-2},\ 10^{-1})$

Tabulka 2.3: Vazba mezi úrovněmi SIL a hodnotou PFD

Pro výpočet PFD je nutné zjistit intenzitu poruch λ.

$$\lambda = \frac{0.1C}{B_{10}} \tag{2.2}$$

Pro dvoukanálové funkce platí výpočet

$$\lambda = (1-\beta)^2 \lambda_1 \lambda_2 T_1 + \beta \frac{\lambda_1 \lambda_2}{2} \tag{2.3}$$

Kde λ_1 a λ_2 jsou intenzity poruch jednotlivých kanálů. Poruchy se dělí na detekovatelné λ_D a nedetekovatelné λ_U. Zjistíme si velikost t_{CE}

$$t_{CE} = \frac{\lambda_D}{\lambda} \frac{T_1 + MTTR}{2} + \frac{\lambda_U MTTR}{\lambda} \tag{2.4}$$

a následně potom hodnotu PFD

$$PFD = 1 - e^{-\lambda t_{CE}} \approx \lambda t_{CE} \tag{2.5}$$

Z tabulky 2.3 se určí dosažená hodnota SIL a porovná se s požadovanou hodnotou z prvního kroku. V případě nedosažení požadované SIL úrovně, viz Kapitola 3.1.4.1.1, je nutné zvážit navržená opatření, popřípadě doplnit tato opatření tak, aby k dosažení požadované úrovně mohlo dojít(například vícekanálovou funkcí).

Vývoj bezpečnostního softwaru zpravidla probíhá v jednoúčelovém vývojovém prostředí dodaném se zvoleným hardwarovým funkčním řídicím prvkem. Norma EN 61508 definuje možné programovací jazyky pro různou dosažitelnou úroveň SIL. Je kladen důraz na co největší jednoduchost a transparentnost bezpečnostního programu a proto mezi doporučené programovací jazyky patří například žebříčkový diagram, ze kterého je jasně patrný tok informací a použití co nejjednodušších datových struktur.

Ověření funkčnosti bezpečnostních funkcí je posledním krokem před uvedením zařízení do provozu. Úkolem tohoto kroku je v co nejširší míře dokázat funkčnost jednotlivých navržených bezpečnostních funkcí a v případě jakýchkoliv nesrovnalostí se vrátit k příslušnému předchozímu kroku.

Realizace systémů založených na jiných technických principech se hodí v případě, když nelze pomocí E/E/PE systémů efektivně omezit vznik jednotlivých rizik. Tyto jsou pak omezeny jiným systémem tak, aby bylo dosaženo požadovaných výsledků na vznik rizika. Do této části mohou patřit zejména pasivní bezpečnostní prvky, které narozdíl od funkčních bezpečnostních prvků mají za úkol zabránit vzniku jednotlivých rizik.

Realizace vnějších prostředků pro snížení rizika má za úkol dosažení splnění požadavků bezpečnostních funkcí a integrity bezpečnosti pomocí vnějších prostředků.

Celková instalace a uvedení do provozu a uvádění zařízení do provozu se řídí příslušným plánem z kroku plánování.

Potvrzení platnosti celkové bezpečnosti se řídí požadavky z části plánování potvrzení celkové bezpečnosti. Při neshodě mezi požadovanou celkovou bezpečností a skutečnou bezpečností je nutné zajistit změny bezpečnostních prvků, funkcí a systémů tak, aby vyhovovaly jednotlivým požadavkům.

Celkový provoz, údržba a opravy specifikuje nutná opatření definovaná části plánování pro zajištění požadovaných vlastností bezpečnostního systému.

Celková modifikace a zdokonalování systému má za úkol zlepšovat funkční bezpečnost během provozu zařízení modifikací požadavků a bezpečnostních funkcí. Žádost o modifikaci je nutné posoudit ze všech bezpečnostních ohledů a v případě pozitivních výsledků se teprve může přistoupit k modifikaci funkce.

Vyřazení z provozu nebo likvidace je konečným prvkem celého životního cyklu. Úkolem je zajistit funkční bezpečnost v požadované míře i po vyřazení zařízení z provozu a při jeho likvidaci. Pro zajištění dopadů vyřazení zařízení z provozu je nutné provést analýzu nebezpečí a rizik pro zajištění požadované funkční bezpečnosti. V případě zjištění nemožnosti dosažení požadavků na bezpečnost stroje, musí se od vyřazení z provozu upustit po dobu, než se nalezne řešení tyto požadavky plnící.

2.2.2 Další normy zabývající se funkční bezpečností

Jak je uvedeno výše, normami pro návrh a realizaci funkční bezpečnosti strojů jsou ČSN EN 62061 a ISO 13849. Použití normy ISO 13849 pro zabezpečení robotického zařízení je demonstrováno v [26] a EN 62061 je prakticky aplikace EN 61508 do strojní oblasti.

2.2.2.1 Srovnání EN 61508, EN 62061 a ISO 13849

Normy EN 61508 a 62061 používají pro určení požadavků a vlastností zabezpečovacích funkcí jednu ze čtyř hodnot úrovně integrity bezpečnosti (SIL), ISO 13849 používá k

PL	SIL
a	Neodpovídá
b	1
c	1
d	2
e	3

Tabulka 2.4: Odpovídající úrovně PL a SIL

témuž účelu tzv. performance level (PL, úroveň vlastností), která definuje pět hodnot (a-e). Odpovídající transformace mezi PL a SIL ukazuje tabulka 2.4. ISO 13849 je určená pro strojní zařízení, tedy neuvažuje možnost vzniku rizika majícího katastrofické následky (SIL 4) a nejvyšší úroveň bezpečnosti PL e odpovídá hodnotě SIL 3.

Norma ISO 13849 navíc definuje základní požadavky na realizaci typických bezpečnostních funkcí pro strojní zařízení, například zastavení stroje, jenž byla použita jako podklad při návrhu sekvence činností pro nouzové zastavení strojů v následující kapitole.

2.2.2.2 Bezpečnost lanových drah

Lanové dráhy jsou speciálním případem zařízení, na které se vztahují zvláštní bezpečnostní požadavky. Požadavky vycházejí ze základních prvků normy EN 61508 ale jsou definovány celou množinou norem určených přímo pro lanové dráhy.

Do množiny norem **bezpečnostní požadavky na osobní lanové dráhy** spadá:

- ČSN EN 12397 - Provoz
- ČSN EN 12408 - Zabezpečování kvality
- ČSN EN 12930 - Výpočty
- ČSN EN 13223 - Poháněcí a další mechanická zařízení
- ČSN EN 13243 - Elektrická zařízení mimo poháněcí zařízení
- ČSN EN 333570 - Elektrická zařízení lanových drah a vleků

Pro potřeby studie v kapitole 3.3 jsou nejdůležitější EN 13223 a EN 13243, které definují požadavky na poháněcí a další elektrická a mechanická zařízení. Pro jednotlivé typy la-

AK	SIL
1	0
2	1
3	2
4	3

Tabulka 2.5: Odpovídající úrovně AK a SIL

nových drah jsou normami přesně definovány jednotlivé bezpečnostní prvky, bezpečnostní funkce a umístění zabezpečovacích prvků, přesně definované v kapitole 3.3.

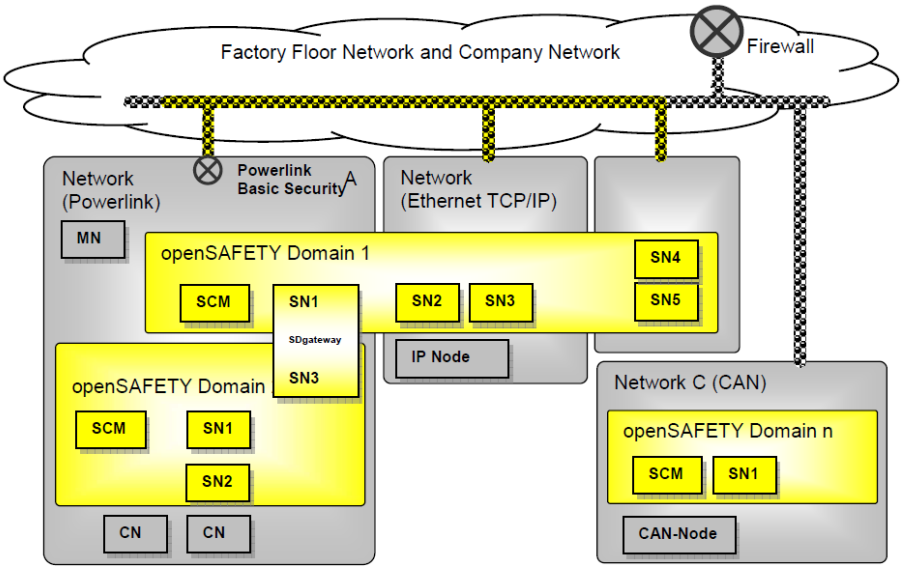
Jednotlivé bezpečnostní funkce lanových drah jsou zařazeny do čtyř tříd. K zařazení bezpečnostních funkcí lze použít například diagramu rizika, který je podobný obrázku 2.5, jenž je použitý v normě EN 61508. Více v příloze A normy EN 13243. Vazbu mezi kategoriemi AK a SIL ukazuje tabulka 2.5. Norma EN 13243 nařizuje pro všechny prvky z kategorie AK 3 a vyšší použít redundantní řešení připojení bezpečnostních prvků s rozpoznáním poruchy. Tohoto požadavku bude využito v následující kapitole zejména pro návrhy funkce nouzového zastavení.

2.3 Protokol openSAFETY

Vývoj bezpečnostních komunikačních protokolů odstartovala až norma ČSN EN 61508, která umožňuje použití programovatelných systémů pro řešení bezpečnosti strojů. Programovatelné systémy tak začaly nahrazovat původní bezpečnostní prvky, například bezpečnostní relé, jejichž jednou zvolené funkce byly v případě potřeby složitě modifikovatelné. Vývojem a aplikací nových forem bezpečnostních komponent se tak snížily finanční náklady na zabezpečení strojů, při zachování nebo rostoucí úrovni zabezpečení. Toto bylo hlavním podmětem společnosti EPSG (European Powerlink Standardization Group) pro vytvoření nového otevřeného bezpečného komunikačního protokolu nazvaného openSAFETY, založeného na klasické ethernetové komunikaci. Kompletní popis protokolu obsahuje [8].

Základní vlastnosti openSAFETY protokolu:

- Protokol openSAFETY je autonomní protokol, nezávislý na použité komunikační sběrnici, na kterou nejsou kladeny žádné bezpečnostní požadavky. Tento protokol je



Obrázek 2.7: Použití openSAFETY nad několika protokoly

vložen do standardního komunikačního protokolu, například POWERLINKU tak, aby standardní data a bezpečnostní data mohla využívat tutéž síť.

- Vychází z klasické komunikace producer/consumer kdy producer odesílá data opatřená adresou, consumer přijímá tato data.
- openSAFETY je kompatibilní s normou EN 61508 a umožňuje dosáhnout úrovně zabezpečení až SIL 3.
- Díky flexibilnímu tvoření rámců je použitelný pro mnoho rozličných aplikací. Velikost jednotlivých rámců je závislá na požadované velikosti datové výměny.
- Podporuje až 1023 openSAFETY Domains s až 1023 openSAFETY Nodes pro každou doménu

Na obrázku 2.7 je vidět integrace openSAFETY při využití několika rozličných fyzických vrstev.

2.3.1 Logické uspořádání a základní prvky sítě

Jak již bylo řečeno, openSAFETY protokol není závislý na fyzické komunikační vrstvě a ochrana před nežádoucím přístupem na síť je závislá na ochraně komunikační vrstvy.

2.3.1.1 openSAFETY Node (SN)

Je zařízení pro vykonávání bezpečnostní funkce určené:

- Logickou adresou, unikátní uvnitř SD s rozsahem 1-1023. Tato adresa je definována programátorem pomocí programátorského nástroje. Duplicitní adresa uvnitř SD je detekována při startu komunikace.
- Fyzickou adresou, která je unikátní v celé síti. Duplicitní adresa je opět detekována při startu komunikace.

2.3.1.2 openSAFETY Domain (SD)

Je adresový prostor až pro 1023 openSAFETY Nodes. Jednotlivé SN uvnitř SD mohou komunikovat přímo mezi sebou a každá doména je identifikována pomocí své unikátní adresy v rozsahu 1-1023 definované programátorem. Každá doména může obsahovat SNs z několika rozdílných fyzických vrstev

2.3.1.3 openSAFETY Gateway (SDG)

Je zařízení, jenž umožňuje komunikaci mezi dvěma SN, přičemž se každý se nachází v jiné SD

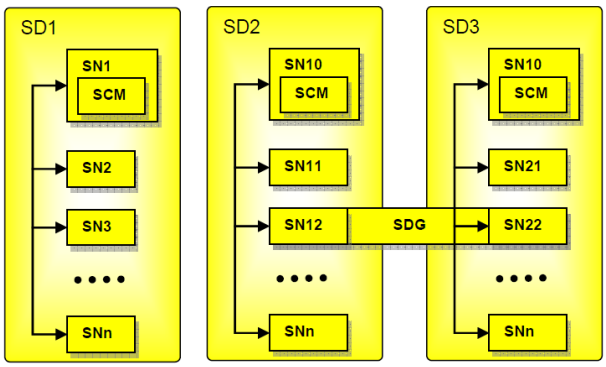
2.3.1.4 openSAFETY Configuration Manager (SCM)

Je služba zodpovědná za řízení openSAFETY. Každá doména s alespoň jedním SN musí obsahovat SCM. SCM je zodpovědný za přiřazení a kontroly unikátních adres jednotlivých SNs, kontroly adres SD, vysílání a vyhodnocování kontrolních signálů detekujících selhání jednotlivých SN.

Na obrázku 2.8 jsou vidět možnosti komunikace uvnitř domény a mezi dvěma doménami pomocí prvku openSAFETY Gateway.

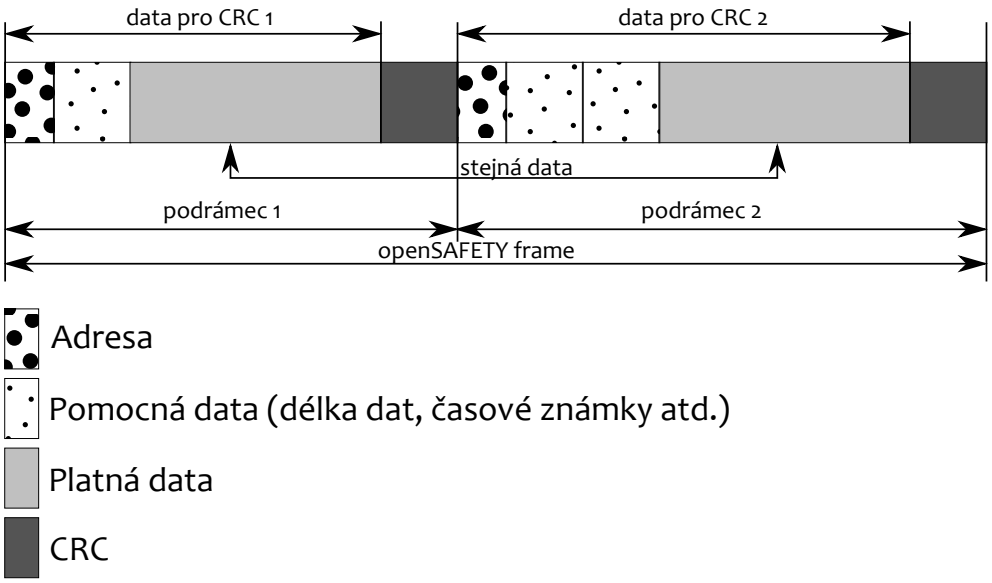
2.3.2 openSAFETY frame

Platná data přenášená pomocí openSAFETY protokolu jsou zabalena v jednom rámci (frame), který se skládá ze dvou podrámců. Každý z podrámců obsahuje, kromě platných dat také informace o jejich délce, adrese zařízení pro které jsou určena atp. Pomocí jednoho rámce lze přenést až 254 bytů dat, přičemž data v obou podrámcích jsou shodná,



Obrázek 2.8: Možná topologie openSAFETY

chráněná proti chybě pomocí CRC kódování v délce 8 pro platná data do velikosti 8 bytů a v délce 16 pro data větší než 8 bytů. Toto kódování zajišťuje Hammingovu vzdálenost nejméně 4 pro oba podrámce. Strukturu openSAFETY rámce ukazuje obrázek



Obrázek 2.9: Struktura openSAFETY rámce

2.9. Je vidět, že data obsažená v části pro CRC budou pro oba podrámce rozličná, z důvodu jiného celkového počtu bytů, zpracovávaného pomocí CRC.

Kapitola 3

Riziková analýza strojů

V této části je na dvou zcela rozdílných strojních zařízeních demonstrována praktická ukázka rizikové analýzy. Prvním strojem je výukový model Žonglér, umístěný na Katedře řídicí techniky Fakulty elektrotechnické ČVUT v Praze, a druhým zařízením je stroj používaný pro tepelné řezání kovů. Výrobcem tohoto stroje je společnost Vanad 2000 a.s. se sídlem v Golčově Jeníkově. Pro uvedené stroje je zpracována riziková analýza a proveden návrh bezpečnostních opatření. Pro model Žonglér jsou navržená opatření i realizována, pro stroje Vanad jsou závěry rizikové analýzy doporučeny výrobci k realizaci. V poslední části kapitoly je provedena studie na zabezpečení lanové dráhy.

3.1 Riziková analýza pro model Žonglér

Model Žonglér je výukové a demonstrační zařízení vyvinuté na Katedře řídicí techniky. Jedná se o pětiosé zařízení, řízené pomocí PLC, realizující funkci žongování s až pěti kulečníkovými koulemi. Model je primárně umístěn v místnosti KNE: L909 (Strojovna) a je určen jako zařízení pro nácvik řízení a synchronizace rychlých servopohonů v praxi. Model je připraven k použití ve výuce přes vzdálenou laboratoř Lablink. Dalším použitím modelu je reprezentace školních projektů a spolupráce školy s průmyslem, v tomto případě s firmou B&R. Model byl k vidění na veletrhu Ampér 2010, 2011 a veletrhu SPS/IPC/DRIVES 2010 v Norimberku. Na všech těchto akcích získal Žonglér velký ohlas. Při přípravě na veletrhy model prošel výraznou rekonstrukcí, přičemž modernizací prošly i původní bezpečnostní systémy. Pro nový model tak bylo nutné provést znovu rizikovou analýzu a realizaci zabezpečení celého systému.

3.1.1 Stav modelu před analýzou

Pro co nejrobustnější rizikovou analýzu je nutné uvažovat stroj s žádným, nebo co nejmenším počtem bezpečnostních prvků. Pro model Žonglér jsou bezpečnostními prvky pouze snímače přehřátí motorů, jejichž hodnoty jsou analyzovány v měniči Acopos.

Riziková analýza se vztahuje pouze k normálnímu provozu stroje, t.j. žonglování s až pěti koulemi, vývoj a ladění uživatelského programu. Pod tento pojem rozhodně nespadá jakákoliv manipulace se strojem. Jakákoliv manipulace se strojem může probíhat pouze za dozoru bezpečnostního technika a pouze kvalifikovanou osobou.

3.1.2 Specifikace normy ČSN EN 61508 pro zařazení jednotlivých rizik

Přesná specifikace pojmů Četnost a Následek je normou ČSN EN 61508 ponechána k určení podle každé aplikace zvlášť. Je tedy nutné tyto pojmy přesně specifikovat. Konkrétní hodnoty pro parametr následek jsou uvedeny v tabulce 3.1.

Následek	Specifikace
Katastrofální	Smrt, těžké ublížení na zdraví s trvalými následky, velké materiální škody
Kritický	Ublížení na zdraví, středně velké materiální škody
Nepodstatný	Malé až zanedbatelné materiální škody
Zanedbatelný	Bez materiálních škod, zastavení provozu stroje

Tabulka 3.1: Specifikace pro zařazení rizik z hlediska následku

Pro parametr četnost jsou zvolené hodnoty uvedeny v tabulce 3.2.

Četnost	Perioda opakování rizika
Častá	< měsíc
Pravděpodobná	< 182 dní (půl roku)
Příležitostná	< rok
Málo častá	< 10 let
Nepravděpodobná	< 100 let
Neuvěřitelná	> 100 let

Tabulka 3.2: Specifikace pro zařazení rizik z hlediska četnosti

3.1.3 Identifikovaná rizika modelu

Provedená analýza bezpečnostních rizik modelu odhalila události, které mohou vést k nebezpečné situaci. Výčet těchto událostí, jejich pravděpodobná příčina i důsledek je uveden v tabulce 3.3.

č.	Příčina	Riziko	Důsledek
1	Selhání koncových spínačů	Nezabrždění motorů	Poškození konstrukce
2	Chyba v řídicím programu	Vypadnutí koule	Poškození okolí
3	Chyba v řídicím programu	Vylétnutí koule	Poškození okolí, úraz
4	Chyba v řídicím programu	Srážka horiz. os	Poškození konstr., motorů
5	Selhání obsluhy	Nechtěné spuštění	Poškození konstr. a okolí, úraz
6	Selhání obsluhy	Narušení prac. prostoru	Poškození konstr. a okolí, úraz
7	Poškození elektroinstalace	Zkrat	Úraz, požár, poškození el. z.
8	Vysoké vibrace	Pád konstrukce	Poškození konstr. a okolí, úraz
9	Normální provoz	Zahřátí motorů	Popálení

Tabulka 3.3: Výčet rizik modelu

Pro jednotlivá rizika je nutné zvolit způsob jejich ošetření. Pro použití SIS připadají v úvahu pouze rizika č. 1 - nezastavení jednoho či více motorů, č. 5 - nechtěné spuštění a č. 6 - narušení pracovního prostoru. Zbylá rizika, vyjma rizika č. 4 - srážka horizontálních os, jsou určeny k zabezpečení pomocí pasivních bezpečnostních prvků. Zabezpečení proti riziku č. 4 nespadá ani pod jeden z uvedených způsobů zabezpečení a proto je uveden zvlášť.

3.1.4 Zamezení vzniku nebo omezení následků rizik

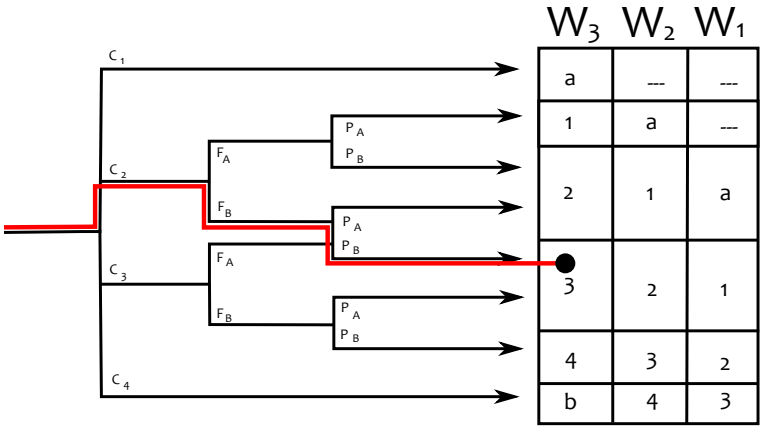
Dle normy EN 61508 je nutné každé závažné riziko, jenž může vzniknout na strojním zařízení, ošetřit pomocí prvků funkční bezpečnosti nebo pomocí systému založených na jiných principech. Tyto systémy jsou v následujících částech souhrně označeny jako pasivní bezpečnostní prvky. Jelikož už při začátku celé rizikové analýzy byla představa o budoucím ošetření některých rizik, jsou z výčtu rizik oddělena ta, jenž budou ošetřena pomocí prvků funkční bezpečnosti, tedy pomocí bezpečnostního integrovaného systému.

3.1.4.1 Návrh SIS a jeho analýza

Pro rizika č. 1, 5, 6 je nutné stanovit požadovanou úroveň **SIL**, určující minimální bezpečnostní požadavky, kterou musí SIF, ošetřující toto riziko splňovat. Toto ohodnocení provedeme i pro přídavnou funkci **nouzové zastavení stroje**, která přímo nevyplývá z analýzy rizik. Pro stanovení úrovně slouží např. postup využívající **diagramu rizika** a ohodnocení jeho prvků pomocí rizikových parametrů C,F,P a W. Klasifikace parametrů je analogická s přílohou **D** v [16], část 5, doplněná ještě o zahrnutí způsobené materiální škody (C_1 pro zanedbatelné škody až po C_4 pro nedozírné materiální škody). Jako příklad je uvedeno určení SIL úrovně pro nežádoucí událost č. **6 - narušení pracovního prostoru**. Uvedenému riziku náleží toto ohodnocení:

- C_2 - Může být způsobeno zranění s trvalými následky, popřípadě smrt osoby
- F_B - Trvalý výskyt osob v nebezpečné oblasti
- P_B - Této události nelze prakticky zabránit a hraje zde velkou roli faktor selhání člověka
- W_3 - Pravděpodobnost, že dojde k této události, je vysoká

Takto definované ohodnocení rizika je poté zaznačeno do diagramu rizika (viz obrázek 3.1) a je z něj jasně patrný výsledek požadované SIL úrovně zabezpečení. V našem případě je výsledkem **SIL 3**.



Obrázek 3.1: Diagram rizika pro narušení pracovního prostoru

Analogicky toto ohodnocení provedeme pro další rizika a funkci Nouzové zastavení stroje. Přehled ohodnocení a výsledné požadované úrovně SIL jsou vidět v tabulce 3.4.

č.	Riziko	C	F	P	W	SIL
-	Nouzové zastavení stroje	C_2	F_B	P_A	W_2	1
1	Nezabrždění motorů	C_2	F_B	P_A	W_3	2
5	Nechtěné spuštění	C_2	F_B	P_B	W_3	3
6	Narušení pracovního prostoru	C_2	F_B	P_B	W_3	3

Tabulka 3.4: Přehled výsledného určení SIL úrovně

3.1.4.1.1 Návrh, analýza a realizace bezpečnostních funkcí je část, kdy bezpečnostním funkcím navrhneme jejich teoretickou realizaci včetně zvolení vhodného hardwaru. Pro takto navržené funkce provedeme zpětnou kontrolu splnění bezpečnostních požadavků. Jako testovací periodu zvolíme jednu z hodnot, definovanou normou EN 61508, v tomto případě budeme uvažovat $T_1 = 4380h$, tedy každého půl roku.

Jako hlavní bezpečnostní prvek je vhodné použít bezpečnostní PLC včetně příslušných modulů bezpečných vstupů a výstupů, jejichž výrobce zajišťuje dodržení požadavků normy EN 61508.

Byly zvoleny komponenty společnosti B&R. Jako bezpečnostní PLC je zvoleno PLC SafeLogic X20SL8000 s dosaženou úrovní SIL 3 s hodnotou $PFD = 10^{-5}$.

Analýza bude probíhat pomocí vztahů (2.2) až (2.5). Hodnotu $MTTR$ parametru zvolíme dle EN 61508 typicky jako $MTTR = 8h$ a počet detekovatelných poruch odhadneme na 50%. Hodnota udávající periodu testování T_1 je zvolena jako jednou za půl roku, tedy $4380h$. Parametr β má odhadnutou hodnotu 0.5.

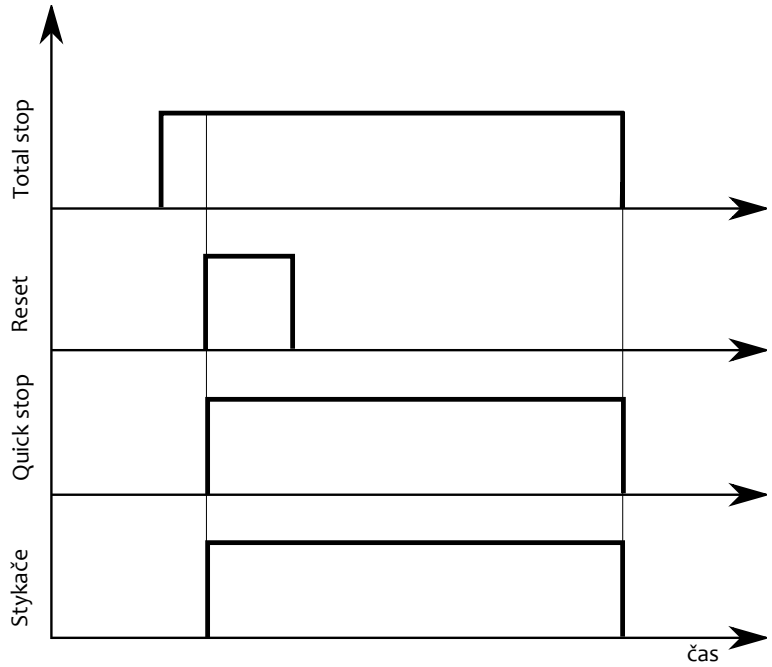
Veškeré bezpečnostní funkce jsou navrženy na model negativní logiky, kdy funkce nebo signál v klidovém stavu mají hodnotu log. 1. Například funkce pro zastavení stroje se stává aktivní při hodnotě tlačítka Total stop = log. 0.

Nouzové zastavení stroje je funkce, jejíž vyvolání způsobí neodkladné uvedení stroje do klidu. V případě modelu Žonglér stačí (vzhledem k dalším opatření uvedeným dále) pokud bude možné stroj kdykoliv během jeho chodu nuceně vypnout pomocí bezpečnostního tlačítka.

Ovlivněné riziko: Žádné, obecná bezpečnostní funkce.

Požadavky: Stroj se zastaví po stisknutí tlačítka Total stop na rozvaděči a následným signálem Quick stop (stroj zastaví při Quick stop = log. 0) do měniče Accopos, který způsobí okamžité zastavení motorů, přičemž je nutné i odpojení měničě od silového napájení. Následné odblokování tlačítka Total stop je nutné potvrdit tlačítkem Reset.

Vývojový diagram je vidět na obrázku 3.2.

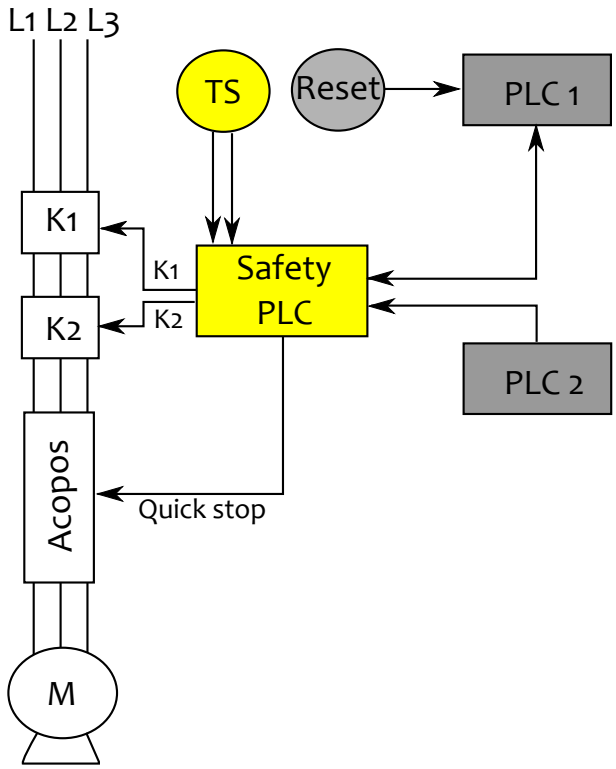


Obrázek 3.2: Vývojový diagram zastavení stroje

Navrhovaná realizace:

- *Tlačítko Total Stop* jako rozpínací kontakt (Moeller M22-K01, viz [23]), umístěný na dveřích rozvaděče stroje. Pomocí dvoukanálového vedení je připojeno k vstupům bezpečnostního PLC.
- *Stykače* o nominálním proudu 12 A jsou umístěny v rozvaděči. Jsou použity 2 stykače v sérii jako redundance (Moeller X Start DIL M12 a Schneider TeSys LP1K12, viz [24] a [29]) a jejich ovládání je řešeno pomocí výstupů bezpečnostního PLC.
- *Tlačítko Reset* obsahuje spínací kontakt a podsvícení (Moeller M22-K10 a M22-LED, viz [23]). Je umístěno na dveřích rozvaděče a slouží k potvrzení deaktivace tlačítka Total stop a pro umožnění spuštění uživatelského programu po otevření dveří (viz dále). Nutnost stisknutí tlačítka Reset je signalizována vizualizací a blikáním tlačítka. Toto je řízeno z řídicího programu běžícího v řídicím PLC.

Schéma zapojení komponent pro zastavení stroje je vidět na obrázku 3.3 a vývojový diagram na obrázku 3.2



Obrázek 3.3: Principiální schéma výměny signálů pro zastavení stroje

Parametry jednotlivých prvků jsou uvedeny v tabulce 3.5. Výpočet hodnoty PFD z pro tlačítko Total stop:

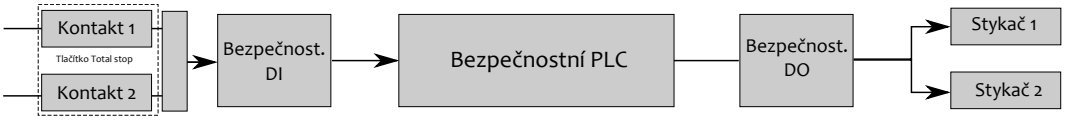
$$
\begin{aligned}
\lambda_{s1} &= \lambda_{s2} = \frac{0.1C}{B_{10}} = \\
&= \frac{0.1}{4380 \times 5 \times 10^5} = 4.56 \times 10^{-10} h^{-1} \\
\lambda_{s1s2} &= (1-\beta)^2 \lambda_1 \lambda_2 T_1 + \beta \frac{\lambda_1 \lambda_2}{2} = \\
&= (1-0.5)^2 \times (4.56 \times 10^{-11})^2 \times 4380 + 0.5 \frac{(4.56 \times 10^{-11})^2}{2} = \\
&= 2.77 \times 10^{-18} h \\
t_{CE} &= \frac{\lambda_D}{\lambda} \frac{T_1 + MTTR}{2} + \frac{\lambda_U MTTR}{\lambda} = \\
&= 0,5 \frac{4388}{2} + 0.5 \times 4 = 1101 h \\
PFD_{s1s2} &\approx \lambda t_{CE} = 2.50 \times 10^{-15} h
\end{aligned}
$$

Logické zapojení (subsystémy vstupů, logiky a výstupů) odpovídající obrázku 3.3 ukazuje obrázek 3.4.

Pro výpočet celkové hodnoty PFD podle 2.1 je nutné sečíst dílčí hodnoty. Výsledná

Prvek	Subsystém	B_{10}	C	λ	t_{CE}	PFD
Kontakt 1 Kontakt 2	Vstupní	5×10^5	$\frac{1}{4380}\,h^{-1}$	$4.56 \times 10^{-11} h^{-1}$	$1101h$	$2.50 \times 10^{-15} h$
Karta vstupů	Vstupní	-	-	-	-	$1 \times 10^{-5} h$
Bezp. PLC	Logika	-	-	-	-	$1 \times 10^{-5} h$
Karta výstupů	Výstupní	-	-	-	-	$1 \times 10^{-5} h$
Stykač 1 (Moell.) Stykač 2 (Schne.)	Výstupní	1×10^5 3×10^5	$\frac{1}{12}\,h^{-1}$	$2.53 \times 10^{-12} h^{-1}$	$1101h$	$2.79 \times 10^{-9} h$

Tabulka 3.5: Parametry navrhovaných prvků



Obrázek 3.4: Navrhované logické znázornění prvků pro funkci Total stop

hodnota PFD_{k1k2} při dvoukanálovém přivedení je podle rovnice (2.4) rovna $PFD_{k1k2} = 2.50 \times 10^{-15} h$. Tato hodnota je velmi malá a je dána velkou životností jednotlivých kontaktů a malou očekávanou periodou spínání C, kdy uvažujeme použití pouze jednou za půl roku.

Celkovou hodnotu PFD_{s1s2} pro oba stykače můžeme brát stejně jako v předchozím případě, pak tedy $PFD_{s1s2} = 2.79 \times 10^{-9} h$.

Celková hodnota $PFD = 3 \times 10^{-5} h$ pro součet PFD bezpečnostních prvků hodnot vstupů, logiky a výstupů. Hodnoty kontaktů a stykačů jsou natolik malé, že se na celkové hodnotě neprojeví. Zabezpečení tak dosahuje úrovně SIL 3 a to je nadmíru dostačující zabezpečení oproti požadované hodnotě SIL 1.

Funkce nouzového zabezpečení může být realizována pomocí výše navržených komponent.

Funkce zastavení při překročení limitu způsobí zastavení všech motorů bez odpojení stykačů od napájení.

Ovlivněné riziko: Riziko č. 1, nezabrždění motorů.

Požadavky: Při překročení maximální hranice pro bezpečnou polohu jakéhokoliv motoru je zapotřebí zastavit všechny motory v co nejkratším limitu. Pro tento účel je ideální použít softwarový limit osy, který zajistí zastavení motorů při jejím překročení. Navíc je

vhodné tento limit jistit pomocí vhodného koncového senzoru připojeného do měniče (vstup Limit)a pro případ selhání je nutná instalace tlumiče, který zajistí nepoškození motorů a kostry stroje. Tento tlumič způsobí postupné zpomalování motoru a k jeho případnému kontaktu s konstrukcí tak dojde v minimální rychlosti.

Navrhovaná realizace:

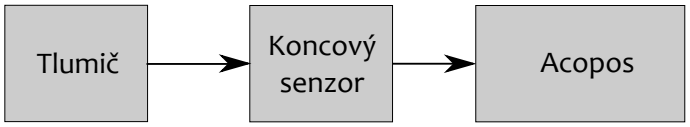
- *Koncový senzor* jako spínací kontakt, navržen Balluff BNS 819, parametry viz [2]
- *Tlumič* jako ochranný prvek konstrukce, navržen Bibus SCS33, parametry viz [1]
- Jako *logický subsystém* je použit přímo měnič Acopos 1022, viz [5]

Parametry jednotlivých prvků jsou uvedeny v tabulce 3.6. Všimněte si zejména PFD hodnoty tlumiče. Tato její malá hodnota je dána tím, že tlumič se aktivuje teprve v případě, že selže koncový senzor a tak i přes malou životnost tlumiče je pravděpodobnost jeho selhání velice malá.

Prvek	Subsystém	B_{10}	C	λ	t_{CE}	PFD
KS Balluf	Vstupní	1×10^5	$\frac{5}{4380}\,h^{-1}$	$1.14 \times 10^{-9}h^{-1}$	1101	$1.25 \times 10^{-6}h$
Tlumič Bibus	Vstupní	1×10^3	1.14×10^{-9}	$1.14 \times 10^{-12}h^{-1}$	$1101h$	$1.25 \times 10^{-9}h$
Acopos 1022	Logika	-	-	-	-	$1 \times 10^{-3}h$

Tabulka 3.6: Parametry navrhovaných prvků

Navrhované logické znázornění ukazuje obrázek 3.5.



Obrázek 3.5: Logické znázornění prvků pro funkci Zastavení na limitu

Celková hodnota $PFD = 1 \times 10^{-3}h$ je dána součtem všech tří uvedených hodnot PFD a dosahuje úrovně pro zabezpečení SIL 2.

Funkce zastavení motorů při překročení maximální možné polohy motorů může být realizována pomocí tohoto navrženého opatření.

Funkce zamezení nechtěného spuštění a reakce na narušení pracovního prostoru nedovolí spustit stroj při otevřeném pracovním prostoru a v případě narušení pracovního prostoru stroj zastaví.

Ovlivněné riziko: Rizika č. 5, 6 nechtěné spuštění resp. narušení pracovního prostoru

Požadavky:

Nechtěným spuštěním modelu se rozumí jeho uvedení do provozu v momentě, kdy je možnost kolize pohyblivých částí stroje s obsluhou nebo jinou osobou, která se může nacházet v pracovním prostoru modelu (t.j. ve vnitřní části ochranné konstrukce). Narušení pracovního prostoru je situace, kdy je stroj v běhu, ovšem jsou otevřeny ochranné dveře. Pro zamezení těmto událostem je doporučeno omezení přístupu do pracovního prostoru modelu pouze z jeho přední části pomocí otevíratelného plexiskla (dveří) s detekcí otevření pomocí koncového spínače. Při otevření dveří je nutné zamezit ve spuštění stroje odebráním signálu Enable měničům. Pro tento úkol je ideální požít opět bezpečnostní PLC. Uzavření dveří je nutné potvrdit tlačítkem RESET. Po tomto potvrzení bude možno model uvést do chodu.

Navrhovaná realizace:

- *Senzor otevření* jako koncový kontakt pro polohu dveří zavřeno, navržen Balluf BNS 819.
- *Plexisklo* z tvrzeného materiálu s tloušťkou 4 mm.

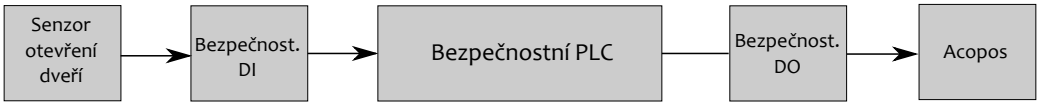
Parametry jednotlivých prvků jsou uvedeny v tabulce 3.7.

Prvek	Subsystém	B_{10}	C	λ	t_{CE}	PFD
Koncový senzor	Vstupní	1×10^5	$\frac{5}{4380}\,h^{-1}$	$1.14 \times 10^{-9} h^{-1}$	$1101h$	$1.25 \times 10^{-6} h$
Karta vstupů	Vstupní	-	-	-	-	$1 \times 10^{-5} h$
Bezp. PLC	Logika	-	-	-	-	$1 \times 10^{-5} h$
Karta výstupů	Výstupní	-	-	-	-	$1 \times 10^{-5} h$
Acopos	Výstupní	-	-	-	-	$1 \times 10^{-3} h$

Tabulka 3.7: Parametry navrhovaných prvků

Navrhované logické znázornění ukazuje obrázek 3.6.

Celková hodnota PFD je ovlivněna maximální úrovní zabezpečení pro spojení prvků Acopos s bezpečnostním PLC (jako celkem včetně DI a DO). Toto spojení zajišťuje dosažení bezpečnostní úrovně maximálně SIL 2 (viz [5]), tedy přibližné hodnoty $PFD =$



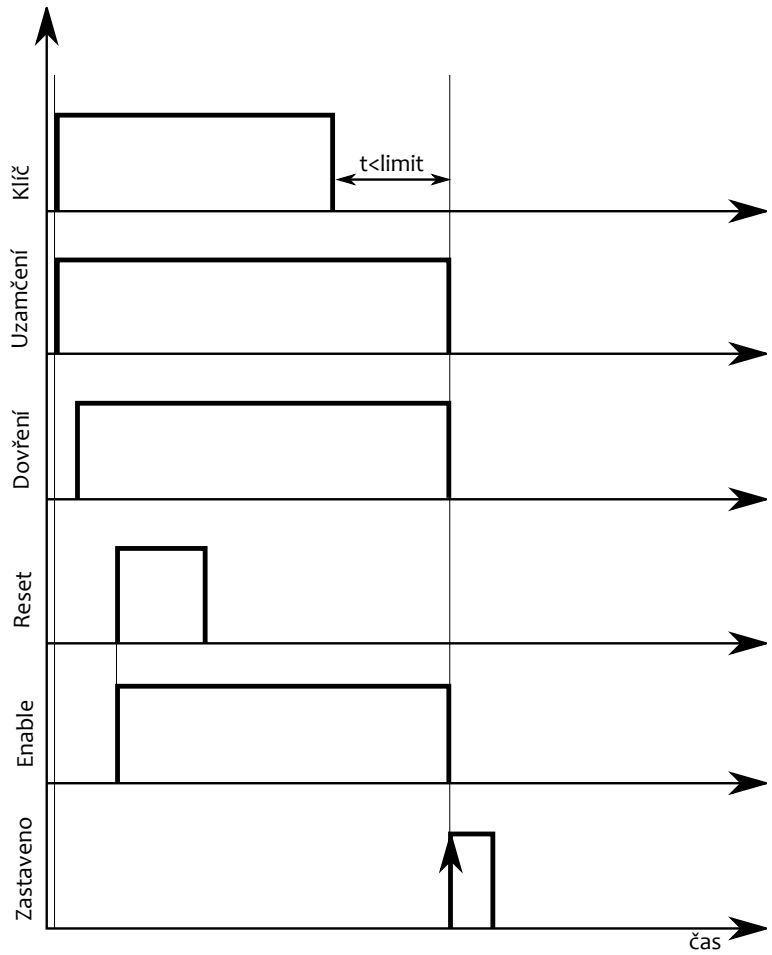
Obrázek 3.6: Logické znázornění prvků pro funkci Zamezení nechtěného spuštění

$1 \times 10^{-3}h$. Při součtu s hodnotou pro senzor zůstává požadovaná dosažená bezpečnostní úroveň stále na hodnotě SIL 2. Požadovaná hodnota zabezpečení pro tuto funkci je ovšem SIL 3, proto je nutné zvážit další postup. Jednou z možností by byla výměna měničů Acopos za Acopos multi, který ve spojení s bezpečnosntím PLC již umožňuje dosažení hodnoty SIL 3. Tato verze je ovšem velice nákladná a je vhodné zvolit jiné řešení. Tímto řešením by byla výměna koncového senzoru za zámek ovládaný klíčem s identifikací jeho dovření a potvrzením dovření tlačítkem Reset. Toto řešení již nepatří mezi klasické funkční zabezpečení, ale přísluší do kapitoly pro návrh pasivních zabezpečení, ale protože je pro jeho realizaci vhodné použít bezpečnostní PLC, je uvedeno v této části práce. Vliv realizace tohoto opatření na snížení rizika je patrný z tabulky 3.8.

Uzamčení pracovního prostoru je opatření, které zamezí vnik osob do pracovního prostoru stroje při jeho běhu zamčením dveří.

Požadavky: Dveře se uzamykají pomocí zamykatelného tlačítka Klíč. Potvrzené uzamčení a dovření dveří pomocí tlačítka RESET povolí přes bezpečnostní PLC spustit stroj signálem Enable pro Acopos. Při odemčení dveří v případě, že stroj je v běhu, předá bezpečnostní PLC signál řídicímu programu, který má za úkol v co nejkratším čase ukončit běh programu v příhodné části cyklu a potvrdit to bezpečnostnímu PLC signálem Zastaveno, a teprve po zastavení stroje je odebrán měniči signál Enable a jsou odemknuty dveře stroje. V případě, že se tak nestane do určitého časového limitu, dojde k řízenému zastavení stroje pomocí odebrání signálu Enable bez ohledu na část cyklu, ve kterém se stroj nachází. Uvedená časová prodleva byla zvolena vzhledem k vlastnostem uživatelského programu na 3s, jelikož délka jednoho cyklu při žonglování se čtyřmi koulemi je menší než 1.5s a program tak má minimálně dvě možnosti na ukončení běhu. Doba doběhu při zastavování je řádu desetin sekundy a interval 3s je tak dostatečný.

Vývojový diagram je vidět na obrázku 3.7.



Obrázek 3.7: Vývojový diagram pro uzamčení pracovního prostoru

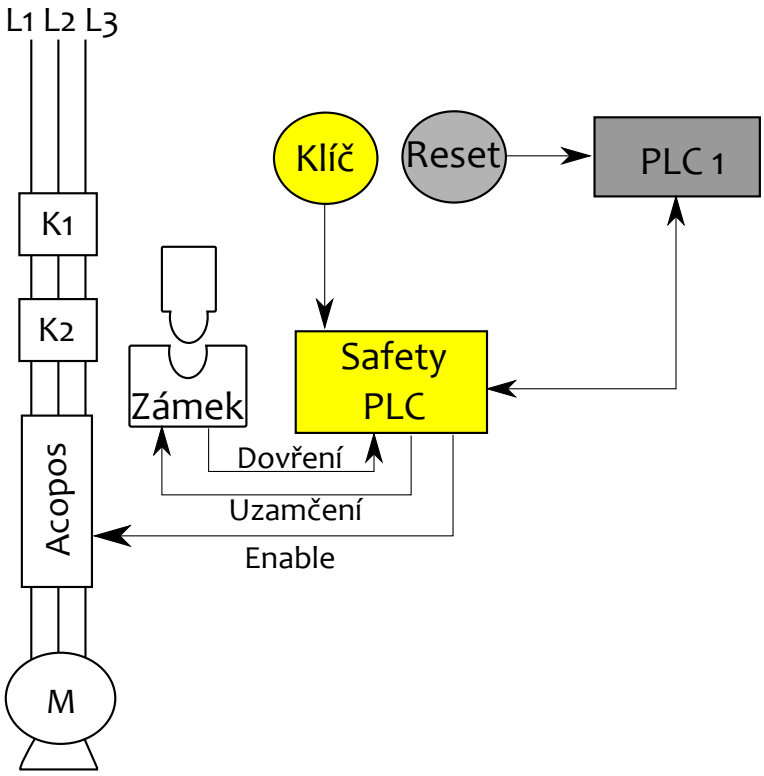
Navrhovaná realizace:

- *Zámek pracovního prostoru* umožňuje uzamknout pracovní prostor a kontrolovat správné uzavření dveří, Moeller AT0-11-24DMT-ZBZ/X, viz [22]
- *Tlačítko Klíč* slouží pro uzamčení pracovního prostoru pomocí zamykatelného tlačítka se spínacím kontaktem totožným s tlačítkem Reset

Schéma zapojení je vidět na obrázku 3.8

3.1.4.2 Návrh pasivních bezpečnostních prvků

Pasivní zabezpečení budou použita pro rizika z tabulky 3.3, která nelze odstranit pomocí SIS (kromě události č. 1, řešené pomocí SIS a události č. 4, řešené speciálním



Obrázek 3.8: Principiální schéma výměny signálů pro uzamčení pracovního prostoru

zabezpečovacím algoritmem, viz dále).

3.1.4.2.1 Rozdělení rizik z hlediska přípustnosti Určování rozdělení zbylých rizik z hlediska přípustnosti je prováděno podle principu založeného na kombinaci četností a následků definovaných v výše. Každému riziku přiřadíme očekávanou hodnotu z množin **Četnost** a **Následek** definovaných v tabulkách 3.2 a 3.1. Poté dosadíme riziko do odpovídající pozice v matici (tabulce) obsahující v horizontální rovině míru četnosti a ve vertikální rovině míru závažnosti (následku) rizika.

Četnost/Následek	Neuvěřitelná	Nepravděp.	Málo častá	Příležit.	Pravděp.	Častá
Katastrofální		8		3		
Kritický		7,5,6	4	9		
Nepodstatný						
Zanedbatelný					2	

Tabulka 3.8: Matice rizik

Při pohledu na tabulku 3.8 vidíme, že téměř všechna rizika, která mohou vzniknout, jsou z tříd I-III a musíme je bezpodmínečně(8, 9) nebo s přijatelnými investicemi v duchu principu ALARP odstranit. V tabulce 3.9 je uveden návrh na odstranění (resp. snížení) rizik na přijatelnou úroveň pomocí pasivních (preventivních) opatření.

č.	Riziko	Pasivní opatření	Snížení
2	Vypadnutí koule	Snížení dopadové desky pod rám konstrukce	Následku
3	Vylétnutí koule	Ochranné plexisklo	Následku
4	Srážka horizontálních motorů	Predikční algoritmus	Následku
5	Nechtěné spuštění	Zámek prac. prostoru	Četnosti
6	Narušení prac. prostoru	Zámek prac. prostoru	Četnosti
7	Zkrat	Pospojování, uzemnění	Četnosti
8	Pád konstrukce	Stabilizace základny, připevnění ke zdi	Četnosti
9	Zahřátí motoru	Ochranná mříž	Následku

Tabulka 3.9: Navrhované pasivní bezpečnostní opatření

Po provedení těchto preventivních opatření se výrazně změnila matice rizik. Její nová podoba je uvedena v tabulce 3.10.

Četnost/následek	Neuvěřitelná	Nepravděp.	Málo častá	Příležit.	Pravděp.	Častá
Katastrofální	3,8	8				
Kritický	5,6,7	4,9				
Nepodstatný						
Zanedbatelný	2					

Tabulka 3.10: Nová matice rizik

Z tabulky 3.10 je vidět, že po provedení preventivních bezpečnostních opatření se výrazně snížily možnosti vzniku nežádoucích událostí, popřípadě závažnost jejich následků. Všimněme si zvláště rizik č. 5 a 6, která se díky preventivnímu opatření v podobě zámku dostala do míst obecně přípustného rizika a není potřeba tak již realizovat řešení pomocí koncového spínače. Rizika č. 3, 8, 9, se nacházejí v zóně **ALARP** a jejich odstranění by bylo dále finančně velice nákladné. Ostatní rizika se nacházejí v mezích přípustného rizika a jejich ošetření je tak dostačující.

3.1.4.3 Opatření zamezující srážce horizontálních os

Existence rizika č. 4 je dána možným sdílením pracovního prostoru horizontálních hřídelí a tedy i možností jejich kolize. Ke srážce může dojít v případě, že vertikální motory jsou v pohybu v k sobě opačných směrech a zároveň jsou obě hřídele horizontálních motorů vytočeny o více než +38° od základní pozice (pozice, kdy inkrementální čidlo natočení motoru udává údaj 0°).

Bezpečnostní opatření je možno realizovat pomocí dalšího přidaného PLC připojeného na použitou komunikační sběrnici Ethernet POWERLINK, například **PLC X20 1485** společnosti B&R, a jeho komunikací s bezpečnostním PLC. V tomto přidaném PLC pak bude naprogramovaný, v co nejrychlejším možném PLC cyklu ($400\mu s$ pro uvedené PLC), algoritmus, který bude číst data z komunikační sběrnice udávající polohu, rychlost a zrychlení jak horizontálních, tak vertikálních motorů. Z takto zjištěných dat může použitím predikčního algoritmu (např. Kalmanova filtru) předpovídat budoucí stav systému, tedy i možnou kolizi hřídelí horizontálního motoru.

V případě, že bude detekována možná kolize hřídelí, predikční algoritmus, opět pomocí sběrnice, předá signál **STOP** algoritmu v bezpečnostním PLC, které bude adekvátně reagovat a zamezí tak srážce držáků a z toho plynoucímu poškození stroje, podrobný popis, viz [20].

Jak již bylo uvedeno, ošetření této události nelze obecně zařadit mezi již zmíněné typy bezpečnostních opatření. Je to důsledek použití predikčního algoritmu v pomocném PLC, kterému nelze triviální metodou určit spolehlivost jeho výsledků (spolehlivost samotného PLC je **SIL 2**) a zajistit tak dosažení určitého maxima pravděpodobnosti selhání. Jsme schopni pouze použitím tohoto algoritmu s jistotou říci, že se pravděpodobnost srážky držáků výrazně sníží.

3.1.5 Použité funkční bezpečnostní prvky a bezpečnostní program

Mezi tyto zařízení spadá již zmíněné bezpečnostní PLC a moduly zajišťující zpracování vstupních a výstupních signálů. Jedním z požadavků na funkční bezpečnostní prvky bylo využití bezpečnostního standardu openSAFETY. Tento požadavek splňují komponenty společnosti B&R.

3.1.5.1 Bezpečnostní PLC

Bezpečnost zařízení zajišťovaná bezpečnostním PLC je zcela autonomní systém, který zaručuje dodržení zásad bezpečnosti bez ohledu na stav řízeného systému. To umožňuje zajistit bezpečnost zařízení i při selhání hlavního řídicího PLC.

Bezpečnostní PLC je hlavním výkonným prvkem pro realizaci bezpečnostních funkcí. Jeho hlavní výhodou oproti bezpečnostním relé je možnost naprogramování a modifikace programu na míru každé aplikaci, při použití téměř totožného hardwarového vybavení. Přidání bezpečnostní funkce, nebo úprava aktuální funkce je tak možná bez nutného zasahování do hardwaru stroje, což přináší výrazné finanční úspory. Pro komunikaci využívá bezpečnostní PLC standardní komunikační sběrnici a protokol openSAFETY. OpenSAFETY zajišťuje, že je bezpečnostní systém plně distribuovaný a veškerá komunikace probíhá po komunikační síti, pro tento model je tou sítí Ethernet POWERLINK. V nabídce bezpečnostních PLC společnosti B&R je několik řešení, pro různé náročnosti bezpečnostního systému. Pro zabezpečení tohoto modelu byl po konzultaci s technickou podporou B&R zvolen jako dostačující základní model bezpečnostního PLC, SafeLogic X20SL 8000, zobrazený na obrázku 3.9(a).

3.1.5.2 Požadavky na bezpečnostní vstupy a výstupy

Návrh modulů pro zpracování bezpečnostních vstupů/výstupů vychází z tabulky 3.11.

č.	Signál	Typ
1	Total stop kanál 1	Vstup
2	Total stop kanál 2	Vstup
3	Klíč	Vstup
4	Dovření dveří	Vstup
5	Uzamčení dveří	Výstup
6	Stykač K1	Výstup
7	Stykač K2	Výstup
8	Enable	Výstup
9	Quick stop	Výstup

Tabulka 3.11: Seznam signálů určených ke zpracování bezpečnostním PLC

Jako **Modul bezpečnostních vstupů** byl zvolen typ X20SI 4100 znázorněný na obrázku 3.9(b).

Jako **Modul bezpečnostních výstupů** byl zvolen typ X20SO 4110, v počtu 2 kusů, zobrazený na obrázku 3.9(c).

(a) Modul X20SL 8000 (b) Modul X20SI 4100 (c) Modul X20SO 4110

Obrázek 3.9: Bezpečnostní moduly řady X20Sxxxxx

Parametry použitých bezpečnostních modulů

Parametr	**X20SL 8000**	**X20SI 4100**	**X20SO 4110**
Komunikace	POWERLINK V2	X2X link	X2X link
Počet vstupů	0	4 bezpečnostní	0
Počet výstupů	0	4 pulsní	4 bezpečnostní
Spotřeba	5.1W	1.25W + 0.32W BUS	1.3W + 0.25W BUS
Max. délka cyklu	—	800μs	800μs
ČSN EN 61508	ano	ano	ano
ČSN EN 61061	ano	ano	ano
ISO 13849	ano	ano	ano
Krytí	IP20	IP20	IP20

Tabulka 3.12: Základní parametry použitých bezpečnostních modulů

3.1.5.3 Bezpečnostní program

Bezpečnostní program je vykonáván v bezpečnostním PLC. Program je implementován pomocí žebříčkového (ladder) diagramu. K vývoji slouží nezávislý vývojový program SafeDESIGNER, určený výhradně pro vývoj algoritmů pro bezpečnostní PLC za využití knihovny PLCopen.

Základem bezpečnostního programu je zpracování bezp. vstupů a provedení akčního zásahu na výstupech. Globální proměnné slouží ke čtení/zápisu na I/O (bezpečnostní vstupy, výstupy, komunikace s dalšími prvky na síti) a každá globální proměnná musí

být některému I/O přiřazena. Globální proměnné jsou doplněny lokálními proměnnými, které pomáhají sestrojení bezpečnostních funkcí.

Celkový bezpečnostní program zpravidla obsahuje dvě skupiny proměnných, podle jejich určení:

- **SAFE (bezpečná) proměnná** je používaná pro zajištění běhu bezpečnostního algoritmu. Je to zpravidla binární proměnná, jejichž spojením se realizují samotné bezpečnostní funkce. Použití SAFE proměnné je vázáno pouze ve spojení s jinou SAFE proměnnou a její mapování na fyzický vstup/výstup je omezeno pouze na bezpečnostní HW prvky. Její deklarace probíhá spojením řetězce "SAFE"se zvoleným datovým typem, např.: SAFEBOOL.

- Ostatní proměnné (nonSAFE) jsou určeny pro podpůrné funkce programu, monitorování běhu programu, komunikaci s dalšími hardwarovými prvky, například pro předávání diagnostických zpráv PLCOpen modulů. Tyto proměnné nejsou určeny pro realizaci bezpečnostních funkcí a jejich zapojení společně s SAFE proměnnou je vyhodnoceno chybou při kompilaci programu. Deklarace probíhá klasickým způsobem zvolením datového typu proměnné, např.: BOOL.

Signály typu SAFE lze pomocí konvertoru převést na klasické signály bez omezení bezpečnostních funkcí programu. Opačná konverze je také možná, ale nejsou potom zaručeny požadované hodnoty bezpečnosti, což je dáno rozdílným fyzickým uložením SAFE a nonSAFE proměnných, kdy uložení SAFE proměnných je lépe chráněno proti nepříznivým vlivům.

Jak je již zmíněno, pomocí nonSAFE proměnných lze komunikovat některé signály pomocí komunikační sítě s prvky na síti POWERLINK. Pro prvek na síti, např. řídicí PLC, se definují počty a typy signálů, které se v SafeDESIGNERU tak i ve vývojovém prostředí Automation studio zobrazují jako I/O signály a je možné je číst/zapisovat pomocí namapování proměnných na tyto signály. Příkladem použití komunikace signálů je jejich užití pro vizualizaci stavu bezpečnostního programu, popřípadě může obsluha pomocí vizualizace provést potvrzení vzniklých bezpečnostních akčních zásahů, nebo k samotnému aktivování bezpečnostní funkce. Například vstupy Reset, resp. Activate funkce pro zastavení stroje, popsané v následujícím odstavci.

3.1.5.3.1 Knihovna PLCopen poskytuje mimo jiné i standardizované funkční bloky pro programování bezpečnostních algoritmů v bezpečnostním PLC, pro vyhod-

nocování a správné řízení akčních členů, senzorů a řízené zablokování funkce ochranných členů. Více o PLCopen v [3].

Některé standardizované bloky a jejich krátký popis:

- `SF_Antivalent` - nerovnost dvou signálů
- `SF_Equivalent` - rovnost dvou signálů
- `SF_EmergencyStop` - nouzové zastavení
- `SF_TwoHandControl` - obouruční řízení stroje

V bezpečnostním programu pro model Žonglér bylo využito pouze bloku `SF_EmergencyStop`, například pro realizaci bezpečnostní funkce Total stop s nutností použití tlačítka Reset po aktivaci funkce ale stal se i základem funkce pro zamykání dveří. Blok `SF_EmergencyStop` je uveden na obrázku 3.10.

Vstup Activate slouží k zapnutí dané funkce, S_EStopIn je signál od vstupního bezpečnostního prvku (Total stop tlačítko), vstupy S_StartReset a S_AutoReset nastavují možnosti resetování (nastavení log 1 na výstup) funkce po jejím aktivování a vstup Reset slouží k ručnímu resetování. Výstup Ready značí, že je funkce v pořádku a zapnuta, S_EStopOut je akční zásah funkce (výstup), Error je signál o chybě a DiagCode obsahuje diagnostickou zprávu. Celý blok je nutné použít ve smyslu negativní logiky, tzn. požadavek na zastavení stroje je při hodnotě S_EStopOut = log. 0. Případné použití předpony S_ u názvu vstupů/výstupů funkce slouží k jednoduchému rozlišení skupiny signálů (SAFE, nonSAFE) připojitelných k danému vstupu/výstupu.

Mimo funkční bloky knihovny PLCopen lze pro implementaci bezpečnostních funkcí využít velké množství dalších bloků, jako časovače, RS klopné obvody pro SAFE i nonSAFE signály.

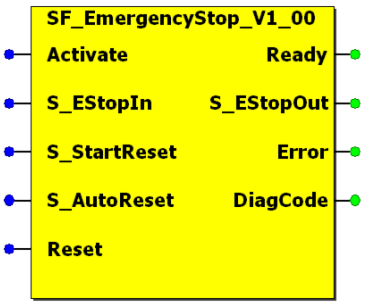
Funkci bloku ilustruje obrázek 3.11.

Bezpečnostní PLC umožňuje, kromě přiřazování signálů na jednotlivé bezpečnostní vstupy/výstupy, také komunikaci s dalšími prvky na síti, pomocí sběrnice POWERLINK a umožnění těmto prvkům čtení některých vnitřních proměnných.

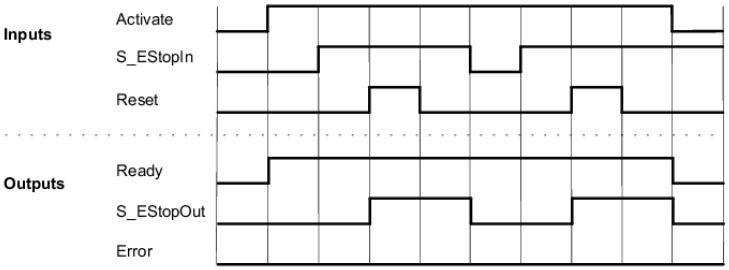
Stručný návod na práci s prostředím SafeDESIGNER je v příloze A.

3.1.5.4 Dosažené reakční časy

Vývojové prostředí SafeDESIGNER umožňuje výpočet reakční doby při zpracování vstupního bezpečnostního požadavku bezpečnostním programem. Pro model Žonglér je tato doba důležitá ve dvou případech:



Obrázek 3.10: Zobrazení bloku SF_EmergencyStop v prostředí SafeDESIGNER



Obrázek 3.11: Diagram funkce bloku SF_EmergencyStop

1. Reakce signálu Uzamčení na uzamčení pracovního prostoru klíčem, doba zpoždění uzamčení t_k

2. Reakce signálu Quick stop na nouzové zastavení přístroje tlačítkem Total stop, doba zpoždění t_{ts}

Programem vypočtená nejhorší reakční doba byla $67.5ms$. Pro oba dva případy bylo pomocí funkce trace v hlavním vývojovém prostředí Automation Studio naměřeno devět hodnot. Z těchto hodnot, uvedených v tabulce 3.13 je vidět, že při průměrných reakčních časech $t_k = 20.2ms$ respektive $t_{ts} = 14.2ms$, což je s dostatečnou rezervou od vypočítaného času pro nejhorší reakční dobu.

3.2 Riziková analýza pro stroje Vanad

Stroje společnosti Vanad slouží k CNC vypalování výrobků z plechu. Pro pálení se používají technologie autogenu, laseru či plazmy. Stroje jsou dostupné v několika veli-

č. měření	t_k $[ms]$	t_{ts} $[ms]$
1	13	13.9
2	14.1	14.1
3	22.2	14.2
4	22	14.2
5	21.9	13.9
6	22.2	18
7	22.1	13.9
8	22	13.8
9	22.1	12
Průměr	20.2	14.2

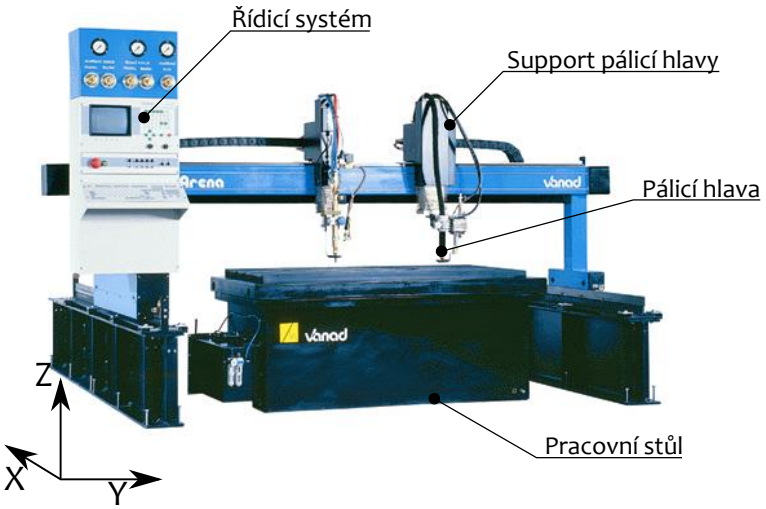
Tabulka 3.13: Naměřené reakční časy

kostech a typech.

Jakákoliv technologie vypalování sebou nese velká úskalí z pohledu skloubení kvality výsledného řezu a dodržení požadavků na bezpečnost stroje, zejména z důvodů manipulace s otevřeným ohněm, hořlavými plyny a vysokými teplotami při pálení. Vzhledem k odletující strusce může docházet k jejímu usazování na plechu a následnému nucenému odstranění při běhu programu. Tyto všechny faktory jsou hlavními zdroji možných rizik a nebezpečí.

3.2.1 Popis stroje a jeho funkce

Stroj (platí pro všechny modely strojů Vanad) je CNC zařízení s několika motory pro horizontální a vertikální posuv a pro řízení polohy hořáku nad materiálem. Řízení motorů je prováděno pomocí pohonů Accopos a řízeno pomocí PLC od společnosti B&R. Stroj při své práci provádí horizontální pohyb v osách x a y nad rovinou stolu a pomocí zpětné vazby pohyb hořákem v ose z. Samotný pohyb je řízen pomocí příkazů pro CNC program z řídicího PLC. Rychlosti pohybu tohoto stroje jsou relativně malé, dosahují hodnot do 20 m za minutu. Pro správnou identifikaci rizik posloužila návštěva ve společnosti Vanad v Golčově Jeníkově, kde byla za asistence technologa firmy konzultována jednotlivá rizika. Pro lepší pochopení souvislostí jednotlivých rizik při běžném provozu byla provedena návštěva zákaznického provozu společnosti ve městě Horka.



Obrázek 3.12: Stroj Vanad Aréna

3.2.2 Stav stroje před analýzou

Veškerý následující obsah uvažuje stroj bez jakýchkoliv, ať již softwarových nebo hardwarových bezpečnostních opatření mimo opatření neoddělitelná od správného vykonávání uživatelského programu.

3.2.3 Specifikace normy ČSN EN 61508 pro zařazení rizik

Stejně jako v případě modelu Žonglér je nutné pro stroje Vanad přesně specifikovat hodnoty četností a následků pro jednotlivé kategorie. Specifikace hodnot následků je uvedená v tabulce 3.14, kde pro přesnější zařazení používáme narozdíl od specifikací pro model Žonglér 5 kategorií.

A podobně pro četnost, jejíž specifikované hodnoty jsou uvedeny v tabulce 3.15. Pro srovnání různých četností viz tabulka 3.2 pro model Žonglér. Tabulky se liší zejména díky rozdílné odhadované frekvenci vzniku nebezpečných událostí, kde pro stroje Vanad jsou tyto četnosti větší (perioda vzniku jednotlivých rizik je menší).

3.2.4 Identifikace jednotlivých rizik

S technologem firmy byla konzultována jednotlivá rizika, jejich možný vznik a frekvence výskytu, vyplývající z povahy a funkce stroje. Identifikovaná rizika jsou uvedena v tabulce 3.16, kde z důvodu přehlednosti uvádím i odhadované četnosti a následky jejich

Následek	Specifikace
Katastrofální	Smrt, zničení zařízení
Kritický	Těžké ublížení na zdraví (trvalé následky), velké materiální škody
Vážný	Úraz bez trvalých následků s dlouhou pracovní neschopností nebo střední materiální škody na zařízení
Nepodstatný	Úraz bez trvalých následků s malou nebo žádnou pracovní neschopností, malé až zanedbatelné materiální škody
Zanedbatelný	Velmi lehký úraz (pohmožděniny, odřeniny), bez materiálních škod, zastavení provozu stroje

Tabulka 3.14: Specifikace pro zařazení rizik z hlediska následku

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

Tabulka 3.15: Specifikace pro zařazení rizik z hlediska četnosti

vzniku jak z hlediska zdravotní újmy tak možných materiálních škod na zařízení či jeho bezprostředním okolí, včetně slovního popisu následků.

Četnost	ID	Událost	Následek	Popis následků
2	1	Pád obsluhy či jiné osoby (zakopnutí atd.)	2-5	Typicky zlomeniny nebo vyražené zuby, ale i možnost kontaktu s plamenem
2	2	Opomenutí nasazení ochranných brýlí a chrániců sluchu	2	Trvalé poškození zraku či sluchu
2	3	Opomenutí nasazení ochranného oděvu (rukavice, oděv)	4-5	Popáleniny od odletující strusky
5	4.1 4.2	Přetržení lana, které ovládá "slave"jednotky	4 4	Trvalý úraz při zásahu obsluhy lanem Vážné poškození stroje přetrženým lanem či vzájemným nárazem hořáků
2	5	Náraz jiného zařízení do pojezdů řezacího stroje (při chodu/mimo chod) nebo pád plechu na stroj	2	Vážné poškození stroje
3	6	Odražení paprsku laserového ukazovátka	5	Dočasné poškození zraku
4	7	Najetí se spuštěným hořákem nad součásti stroje	2	Vážné poškození stroje, požár
5	8.1 8.2 8.3	Únik kyslíku (Prasknutí hadic etc.)	2 3-4 5	Požár, popáleniny, poškození stroje, zplodiny Poškození sluchu Přerušení provozu/zastavení stroje
5	9.1 9.2 9.3	Únik hořlavých plynů (Prasknutí hadic etc.)	2 3-4 5	Požár, výbuch, poškození stroje, popáleniny, otrava zplodinami Poškození sluchu, přiotrávení plynem Přerušení provozu
5	10	Únik stlačeného vzduchu (prasklá hadice)	3-4	Možný úraz - poškození sluchu; Zastavení stroje
4	11	Neoprávněné či nechtěné spuštění hořáku	2-3	Trvalý úraz či vážné popáleniny, poškození stoje či požár
5	12	Srážka strojů při konfiguraci více strojů na jednom stole	3	Poškození stroje

Pokračování na další stránce

Pokračování z předchozí stránky

Četnost	ID	Událost	Následek	Popis následků
4-5	13	Sražení obsluhy strojem	3-4	Trvalé poškození zdraví
5	14	Zkrat	1	Smrt či popáleniny
4	15	Probití (především při dotyku hořáku), neukostřený materiál	1	Smrt či popáleniny
4	16	Namotání nebo zachycení rotátorem	2-3	Může vést k velmi vážným úrazům
4	17	Zachycení obsluhy mezi stůl a koleje	3	Typicky nejhůře zlomenina
4	18	Kontakt části těla s plamenem	2-3	Trvalý úraz či vážné popáleniny
4	19	Pády či zaseknutí předmětu v pojezdu stroje	5	Zastavení stroje z důvodu přetížení motorů
2	20	Manipulace s plechem a s výpalky	2	Možnost vážného úrazu
5	21	Opomenutí vypnutí vrtání	4	Mírné poškození stroje či lehčí úraz
3	22	Náraz hořáku o překážku (vrtání, autogen)	3	Poškození supportu stroje
1-2	23.1	Masivně odlétávající struska	4-5	Pokud dojde k opomenutí nasazení ochranného oděvu pak hrozí popáleniny
	23.2		5	Lehké poškození stroje, či kabelů (propálení) nebo drobný požár v případě, že nebylo dodržení čištění a struska zapálí zbytky vazelíny či prachu
3-4	24	Náraz strojem do překážky (ne hořákem)	4	Zastavení stroje či nejhůře lehké poškození

Pokračování na další stránce

Pokračování z předchozí stránky

Četnost	ID	Událost	Následek	Popis následků
2	25	Při pálení hliníku plasmou - výbušný prach v kombinaci se železným prachem	2	Poškození stroje, otrava obsluhy
1	26	Při pálení plasmou - jedovatý plyn (ozón)	2	Trvalé poškození zdraví v případě nepoužití odsávání
1	27	Při pálení nerezi plasmou - jedovaté plyny	2	Trvalé poškození zdraví v případě nepoužití odsávání
2	28	Ovlivnění kardiostimulátoru	1	Vážné poškození zdraví, smrt

Tabulka 3.16: Identifikovaná rizika strojů Vanad

Četnost/Následek	Neuvěřitelná	Nepravděp.	Málo častá	Příležit.	Pravděp.	Častá
Katastrofální		14, 23.1, 23.2	15, 23.1		28	
Kritický		8.1, 9.1, 23.1	7, 11, 16, 18; 23.1		1, 2, 4, 20, 25	26, 27
Vážný		8.2, 9.2, 10, 12, 13	11, 13, 16, 17, 18	22	1	
Nepodstatný		4.1, 4.2, 8.2, 9.2, 10, 13, 21	13, 24	24	1, 3	
Zanedbatelný		8.3, 9.3	19	6	1,3	

Tabulka 3.17: Matice rizik pro stroje Vanad

Z důvodu větší složitosti než u modelu Žonglér je v tabulce upuštěno od odhadování příčin rizika, neboť v mnoha případech je hranice rizika a jeho příčiny velice nejasná, nebo dokonce vůbec žádná. Nelze tedy rozlišit, jestli daná událost je příčina rizika nebo již riziko samotné.

Zvláštním druhem rizika, je riziko pádu obsluhy, či jiné osoby (číslo 1) . Toto riziko je natolik specifické, že nelze ošetřit klasickou metodou přiřazení hodnot četností a následků a ani mu nelze přímo nijak efektivně zabránit. Případu zakopnutí a následného pádu obsluhy do blízkosti stroje lze pouze preventivně předcházet, například udržováním čistoty na pracovišti, vymezením pracovního prostoru stroje atd.

3.2.5 Rozdělení rizik z hlediska přípustnosti

Vzhledem k velice obecným znalostem přesných principů vzniku nebezpečných událostí provedeme rozdělení do matice rizik pro všechna identifikovaná rizika pro hodnoty četností a následků z tabulky 3.16.

Stejně jako pro model Žonglér rozdělíme rizika do kategorií dle ČSN EN 61508-5 na nepřijatelné riziko, ALARP a přijatelné riziko. Z tabulky 3.18 vidíme, že stejně jako v případě modelu Žongléru se velké množství rizik nachází v třídách $I - III$ a je proto nutné navrhnout pro tato rizika bezpečnostní opatření, snižující jejich četnost nebo následek.

Nepřijatelné riziko	1, 2, 5,15, 20, 22, 23.1, 25, 27, 28
ALARP	1, 3, 7, 8.1, 8.2, 9.1, 9.2, 10,11, 12, 13, 14, 16, 17,18, 23.1, 23.2, 24
Přijatelné riziko	1, 3, 4.1, 4.2, 6, 8.2, 8.3, 9.2, 9.3, 10, 13, 19, 21

Tabulka 3.18: Rozdělení rizik do kategorií dle normy ČSN EN 61508-5

3.2.6 Zamezení vzniku nebo omezení následků rizik

Stejně jako pro předchozí zařízení, je nutné nalézt metody a způsoby pro snížení rizik. Tyto doporučené způsoby jsou uvedeny v tabulce 3.19.

Id	Ovlivněné riziko	Prostředek snížení rizika	Opratření primárně snižuje
I	1, 13, 16, 18, 21	Laserové či optické závory vymezující prostor okolo hořáku	Četnost i následek
II	17	Zabezpečení proti zachycení končetiny mezi vany a pojezdové dráhy - např. mříže	Četnost
III	14, 15	Pravidelná revize uzemnění a elektrické instalace stroje; při výměně dílů hlavy hořáků nutno preventivně vypnout plazmu	Četnost
IV	8.1, 9.1, 9.2, 9.3, 10	Detekce hořlavých, jedovatých a výbušných plynů (senzor), kontrola náhlého poklesu tlaku v hadicích, zapnutí odsávání ; kontrola poškození přívodních hadic	Četnost i následek
V	11	Zabezpečení (uzamknutí) ovládání (panelu atd.), když u něj obsluha není (pohybuje se u stroje) kartou, kódem a nechat funkční jen "total stop"(zvláště pro velké provozy) + opatření I	Četnost
VI	19	Zakrytí pojezdových drah	Četnost
VII	19	Rychlejší detekce přetěžování motorů	Následek
VIII	22	Stejná automatická detekce u autogenu jako u plazmy	Četnost
IX	7, 22	Blokace chodu plazmy/autogenu při posunu do pozice nad pojezdem; vymezení pracovního prostoru koncovými spínači; při odhlašování operátora (karta...) automatický stop	Četnost
X	23.1	Ochranný štít okolo trysky	Následek
XI	23.2	Důkladné zakrytí důležitých komponent stroje (kabeláže; hadice s plynem)	Následek
XII	28	Výstražné štítky a cedule zakazující vstup osobám s kardiostimulátorem	Četnost

Pokračování na další stránce

Pokračování z předchozí stránky

Id	Ovlivněné riziko	Prostředek snížení rizika	Opratření primárně snižuje
XIII	2, 3, 6, 8.2, 9.2, 10	Výstražné štítky a cedule přikazující nasazení ochr. pomůcek	Četnost i následek
XIV	20	Výstražný maják, siréna (údržba apod.) při manipulaci s materiálem; vhodná manipulace s materiálem	Četnost
XV	12	Laserové či ultrazvukové čidlo s měřením vzdálenosti na jednotlivých supportech	Četnost
XVI	24	Vymezení a vyznačení pracovního prostoru stroje a detekce senzory předmětu/osoby ve směru pohybu supportu	Četnost
XVII	4.1, 4.22	Pravidelná kontrola stavu lana; zakrytování lan; detekce přetržení	Četnost i následek
XVIII	2, 3	Postihy zaměstnanců za nedodržování povinné výbavy	Četnost
XIX	25, 26, 27	Automatické odsávání v případě pálení plazmou a detekce nebezpečné koncentrace jedovatých plynů	Následek
XX	5	Jasné vymezení a vyznačení pracovního prostoru	Četnost
XXI	16	Striktní dodržování pravidel o oděvu (dlouhé vlasy; volné části oděvu...) zamezující zachycení	Četnost

Tabulka 3.19: Navržená opatření pro snížení rizik strojů Vanad

Četnost/Následek	Neuvěřitelná	Nepravděp.	Málo častá	Příležit.	Pravděp.	Častá
Katastrofální	14	15, 28				
Kritický	18	7, 11, 16, 26, 27	2, 5, 20			
Vážný	17, 18	3, 8.1, 8.2, 9.1, 10, 11, 12, 13, 16, 17	3			
Nepodstatný	4.2, 13	3, 4.1, 4.2, 8.1, 8.2, 9.1, 9.2, 10, 21, 24, 25				
Zanedbatelný		4.1, 8.3, 9.3, 19, 22	22	6	23.1, 23.2	23.1, 23.2

Tabulka 3.20: Nová matice rizik

Nepřijatelné riziko	
ALARP	2, 3, 5, 8.1, 8.2, 9.1, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 23.1, 23.2, 28
Přijatelné riziko	3, 4.1, 4.2, 6, 8.1, 8.2, 8.3, 9.1, 9.2, 9.3, 13, 18, 21, 22, 24, 25

Tabulka 3.21: Očekávané rozdělení rizik po aplikaci bezp. opatření

Tyto bezpečnostní opatření mají zásadní vliv na snížení hodnot četností a/anebo následků u jednotlivých událostí. Opatření jsou obecně nezávazná, jelikož mnoha událostem lze předcházet více způsoby s různými finančními požadavky. Navíc jsou zde uvedena i opatření, jejichž vlivem se snižují četnosti a následky u přijatelných rizik provozu. Skutečná aplikace těchto nebo komplementárních opatření je poté úplně dobrovolná a podle normy nepotřebná.

Při uvažování použití uvedených opatření se nám výrazně změní matice rizik na tvar uvedený v tabulce 3.20, jelikož bezpečnostních opatření má vliv na snížení celkové závažnosti jednotlivých nežádoucích událostí.

Seznam rizik pro jednotlivé kategorie je vidět v tabulce 3.20.

Jak je názorně vidět, použitím uvedených bezpečnostních opatření se velká část nežádoucích událostí ocitla v části pro přijatelné riziko, popřípadě v části, kde je vyžadován princip ALARP, avšak žádná uvedená nežádoucí událost již není v části nepřijatelného rizika. Při předpokladu, že zabránění událostem náležícím v nové matici rizik části ALARP jsou na samé hranici finančních možností, je jejich setrvání v této části normou povolené a nemusí se nijak dále ošetřovat a v tomto případě je stroj vyhovující z pohledu normy ČSN EN 61508.

3.2.6.1 Návrh a analýza bezpečnostních funkcí pro stroje Vanad

Při návrhu vycházím z předpokladu, že rizika zařazená jako přijatelná z matice rizik před aplikováním bezpečnostních opatření není potřeba ošetřovat. V následující části se budu zabývat hlavně riziky z tříd pro nepřijatelné riziko a ALARP a rizika, jejichž dopady lze snížit například pasivními bezpečnostními prvky.

Rizika určená k ošetření pomocí SIF ukazuje tabulka 3.22.

Pro tato uvedená rizik zjistíme, stejně jako pro podobná rizika u modulu Žonglér požadavky na úroveň integrity zabezpečení, pomocí prostupu diagramem rizika z obrázku 2.3. Ostatní rizika je nutné ošetřit jinak, například pomocí pasivních bezpečnostních prvků, uvedených v tabulce 3.19.

Jednotlivá výsledná ohodnocení ukazuje tabulka 3.23. Relativně nízké požadavky na úroveň zabezpečení (maximální požadovaný SIL je 2) jsou dány hlavně pomalými pohyby stroje.

č.	Riziko
1	Pád obsluhy či jiné osoby
8	Únik kyslíku
9	Únik hořlavých plynů
10	Únik stlačeného vzduchu
12	Srážka strojů
13	Sražení obsluhy strojem
16	Namotání nebo zachycení rotujícími částmi
18	Kontakt těla s plamenem
22	Detekce kolize hořáku

Tabulka 3.22: Rizika pro ošetření pomocí SIF

č.	Riziko	C	F	P	W	SIL
-	Nouzové zastavení stroje	C_2	F_B	P_A	W_2	1
1	Pád obsluhy či jiné osoby	C_2	F_B	P_A	W_2	1
8	Únik kyslíku	C_2	F_B	P_A	W_2	1
9	Únik hořlavých plynů	C_2	F_B	P_A	W_2	1
10	Únik stlačeného vzduchu	C_1			W_2	—
12	Srážka strojů	C_2	F_B	P_A	W_2	2
13	Sražení obsluhy strojem	C_2	F_B	P_A	W_2	1
16	Namotání nebo zachycení rotujícími částmi	C_2	F_B	P_B	W_2	2
18	Kontakt těla s plamenem	C_2	F_B	P_B	W_2	2
22	Detekce kolize hořáku	C_2	F_B	P_B	W_2	1

Tabulka 3.23: Přehled výsledného určení SIL úrovně

3.2.6.2 Návrh SIS a jeho analýza

Protože bezpečnostní funkce pro stroje Vanad jsou mnohem komplexnější, mohou pokrýt hned několik rizik jedinou funkcí, proto nejsou jednotlivým rizikům přiřazeny funkce, jako v případě Žongléru, ale jednotlivým funkcím přiřazena rizika, která tyto funkce ovlivňují.

Jako logický bezpečnostní prostředek je ideální zvolit stejně jako pro model Žonglér bezpečnostní PLC společnosti B&R, využívající openSAFETY protokol ve spojení s vhodnými bezpečnostními prvky. Bezpečnostní PLC bude stejně jako u Žongléru přidělovat signály Enable a Quick stop použitým frekvenčním měničům Acopos.

Je nutné si stejně jako v předchozím případě zvolit některé parametry, tedy $T_1 = 4380h$, $MTTR = 8h$ a $\beta = 0.5$. Poměr $\frac{\lambda_D}{\lambda_U} = 1$.

3.2.6.2.1 Návrh a analýza bezpečnostních funkcí

Funkce nouzové zastavení stroje, stejně jako podobná funkce v případě Žongléru zastaví neprodleně stroj a odpojí měniče od napájení.

Ovlivněné riziko: Žádné, obecná bezpečnostní funkce.

Požadavky: Stroj se zastaví po stisknutí tlačítky Total stop umístěnými na operátorském panelu a na vhodných, snadno přístupných místech stroje. Signál Quick stop u měniče Accopos způsobí okamžité zastavení motorů, přičemž je nutné i odpojení měničě od silového napájení. Následné odblokování tlačítka Total stop je nutné potvrdit tlačítkem Reset ve vizualizaci. Vývojový diagram je vidět na obrázku 3.2. Diagram je totožný s odpovídajícím diagramem pro model Žonglér.

Navrhovaná realizace:

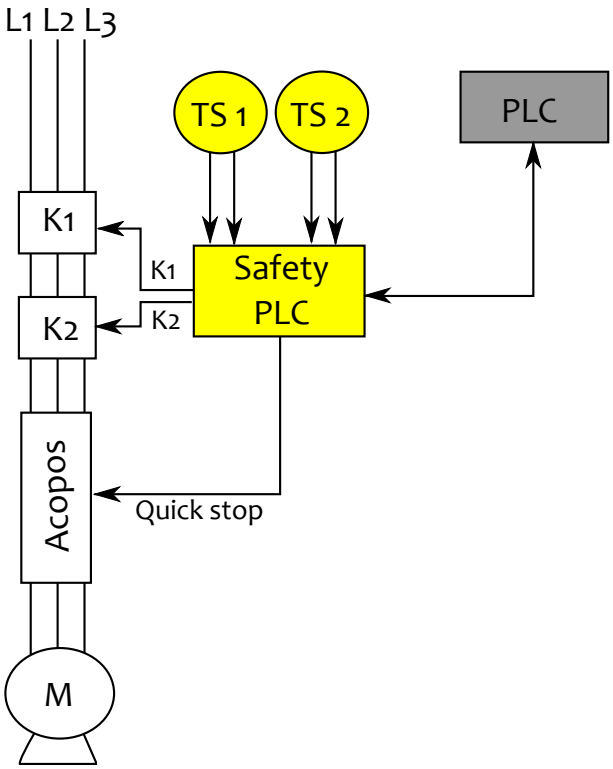
- *Tlačítko Total Stop* jako zdvojený rozpínací kontakt (Moeller M22-K01), umístěný na dveřích rozvaděče a vhodných pozicích na stroji. Pomocí vedení jsou připojeny dvoukanálově ke vstupům bezpečnostního PLC.

- *Stykače* o nominálním proudu 9 A jsou umístěny v rozvaděči. Jsou použity 2 stykače v sérii jako redundance stejně jako pro model Žonglér a jejich ovládání je řešeno pomocí výstupů bezpečnostního PLC. Použité stykače Moeller DILEM-10-G a Schneider LC1K09.

Schéma zapojení komponent pro zastavení stroje je vidět na obrázku 3.13.

Parametry jednotlivých prvků jsou uvedeny v tabulce 3.24.

Navrhované logické zapojení znázornění ukazuje obrázek 3.14.

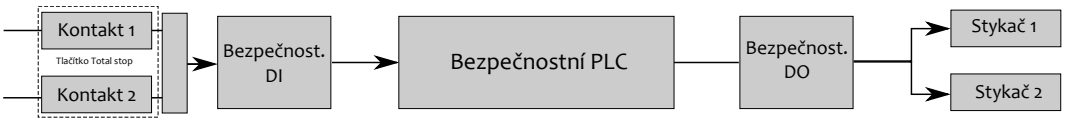


Obrázek 3.13: Principiální schéma výměny signálů pro zastavení stroje s dvěma tlačítky Total stop

Prvek	Subsystém	B_{10}	C	λ	t_{CE}	PFD
Kontakt 1 Kontakt 2	Vstupní	5×10^5	$\frac{1}{4380}\,h^{-1}$	$2.77 \times 10^{-18} h^{-1}$	$1101h$	$2.50 \times 10^{-15} h$
Karta vstupů	Vstupní	-	-	-	-	$1 \times 10^{-5} h$
Bezp. PLC	Logika	-	-	-	-	$1 \times 10^{-5} h$
Karta výstupů	Výstupní	-	-	-	-	$1 \times 10^{-5} h$
Stykač 1 (Moell.) Stykač 2 (Schne.)	Výstupní	2×10^4 3×10^5	$\frac{1}{12}\,h^{-1}$	$1.26 \times 10^{-10} h^{-1}$	$1101h$	$1.39 \times 10^{-7} h$

Tabulka 3.24: Parametry navrhovaných prvků

Pro výpočet celkové hodnoty PFD je nutné sečíst dílčí hodnoty. Výsledná hodnota PFD_{k1k2} při dvoukanálovém přivedení je podle rovnice 2.4 rovna $PFD_{k1k2} = 2.5 \times 10^{-15} h$. Tato hodnota je stejně jako u modelu Žonglér velice malá, protože protože očekávaná četnost spínání tlačítka Total stop je opět $C = \frac{1}{4380}\,h$. Celkovou hodnotu PFD_{s1s2} pro oba stykače můžeme brát stejně jako v předchozím případě, pak tedy $PFD_{s1s2} = 1.39 \times 10^{-7} h$.



Obrázek 3.14: Navrhované logické znázornění prvků pro funkci Total stop

Celková hodnota $PFD = 3.x10^{-5}h$ pro součet PFD bezpečnostních prvků. Ostatní hodnoty jsou natolik malé, že se na celkové hodnotě neprojeví. Navrhované dosahuje úrovně SIL 3 a to je dostačující při požadované hodnotě SIL 1.

Funkce nouzového zastavení může být realizována pomocí výše navržených komponent.

Zastavení stroje stejně jako v případě Žongléru zastaví stroj bez nutnosti vypínat měniče od napájení.

Ovlivněné riziko: Všechna uvedená

Požadavky:

Všechna rizika jsou natolik závažná, že je nutné neprodlené zastavení stroje v případě jejich vzniku. Není nutné v případě jejich vzniku však odpojovat motory od napájení, tím se liší od nouzového zastavení stroje. Jednotlivá rizika mohou mít hned několik příčin.

Navrhovaná realizace:

Navrhovaná realizace obsahuje i účel jednotlivých komponent, když to není zřejmé.

- *Optická závora* Leuze Solid-4E o výšce 1500 mm s roztečí paprsků 90 mm s konektorem M12 umístěná okolo celého stroje zabrání veškerým rizikům, které mohou vzniknout kontaktem stroje nebo paprsku s člověkem. Tato závora dosahuje zabezpečení na úrovni SIL 3, viz [21].

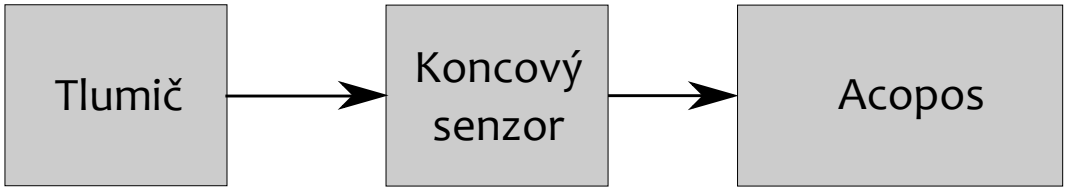
- *Snímač polohy trysky* například již osvědčený koncový spínač Balluff BNS 819 v obou horizontálních osách pohybu spolu s výkyvnou tryskou zajistí indikaci nárazu hořáku do strusky. Další senzor umožňuje rozeznat porušení minimální vzdálenosti mezi jednotlivými supporty stroje.

- *Senzor výbušných plynů* Dräger PIL 7000 s řídicí jednotkou Dräger REGARD-1 umožňuje detekci až 10 plynů. Jednotka má výstupní relé, které bude připojeno na vstup bezpečnostního PLC. Senzor dosahuje parametrů zabezpečení SIL 2.

Parametry jednotlivých prvků jsou uvedeny v tabulce 3.25.

Prvek	Subsystém	B_{10}	C	λ	t_{CE}	PFD
Koncový senzor	Vstupní	1×10^5	$\frac{500}{4380}\,h^{-1}$	$6.84 \times 10^{-8}h^{-1}$	$1101h$	$7.54 \times 10^{-5}h$
Detekce plynů	Vstupní	-	-	-	-	$1 \times 10^{-3}h$
Optická závora	Vstupní	-	-	-	-	$1 \times 10^{-4}h$
Karta vstupů	Vstupní	-	-	-	-	$1 \times 10^{-5}h$
Bezp. PLC	Logika	-	-	-	-	$1 \times 10^{-5}h$
Karta výstupů	Výstupní	-	-	-	-	$1 \times 10^{-5}h$
Acopos	Výstupní	-	-	-	-	$1 \times 10^{-3}h$

Tabulka 3.25: Parametry navrhovaných prvků



Obrázek 3.15: Logické znázornění prvků pro zastavení stroje

Navrhované logické znázornění ukazuje obrázek 3.15.

Celková hodnota PFD je opět ovlivněna maximální úrovní zabezpečení pro spojení prvků Acopos s bezpečnostním PLC. Toto spojení zajišťuje dosažení bezpečnostní úrovně maximálně SIL 2, tedy přibližné hodnoty $PFD = 1 \times 10^{-3}h$. Při součtu s hodnotou pro senzor hořlavých plynů zůstává požadovaná dosažená bezpečnostní úroveň stále na hodnotě SIL 2. Stejné je to pro případ optické závory nebo koncových senzorů detekující výkyv hořáku nebo překročení minimální vzdálenosti mezi supporty stroje. Maximální dosažená úroveň zabezpečení je SIL 2, požadovaná nejvyšší úroveň je SIL 1. Tato funkce je tedy dostačující.

3.2.7 Použité funkční bezpečnostní prvky a bezpečnostní program

3.2.7.1 Bezpečnostní PLC

zvolíme stejně jako v případě modelu Žonglér typ X20SL8000 společnosti B&R.

3.2.7.1.1 Požadavky na bezpečnostní vstupy a výstupy Návrh modulů pro zpracování bezpečnostních vstupů/výstupů vychází z tabulky 3.26, kdy uvažujeme použití dvou tlačítek Total stop.

č.	Signál	Typ
1	Total stop 1 kanál 1	Vstup
2	Total stop 1 kanál 2	Vstup
3	Total stop 2 kanál 1	Vstup
4	Total stop 2 kanál 2	Vstup
5	Senzor min. vzdálesnosti supportů	Vstup
6	Senzor vyhnutí trysky osa x	Vstup
7	Senzor vyhnutí trysky osa y	Vstup
8	Optická závora	Vstup
9	Detektor plynů	Vstup
10	Stykač K1	Výstup
11	Stykač K2	Výstup
12	Enable	Výstup
13	Quick stop	Výstup

Tabulka 3.26: Seznam signálů určených ke zpracování bezpečnostním PLC

Jako **Modul bezpečnostních vstupů** byl zvolen typ X20SI 4100 v počtu dvou kusů. Protože optická závora disponuje konektorem M12, je nutné použít ještě jeden modul vstupů s přizpůsobeným konektorem, v tomto případě X67SC 4122 s osmi vstupy a čtyřmi výstupy. Tento modul je vhodný pro použití přímo na stroji, protože obsahuje krytí IP67.

Jako **Modul bezpečnostních výstupů** byl zvolen typ X20SO 4110.

Takto sestavený a vhodně naprogramovaný bezpečnostní systém by zajišťoval bezpečnost strojů Vanad dle normy EN 61508.

3.3 Případová studie bezpečnosti lanové dráhy

3.3.1 Modelová lanová dráha

Pro tuto studii uvažujme modelovou lanovou dráhu typu Oběžná visutá sedačková lanová dráha s pevných uchycením.

Lanová dráha disponuje těmito prostory:

- Strojovna ve které je umístěn hlavní rozvaděč
- Řídicí pult umožňující veškeré ovládání lanové dráhy
- Prostory stanic
- Podpěrné sloupy

Řídicí systém (myšleno včetně bezpečnostního) X20 společnosti B&R je analogicky distribuován v uvedených prostorech, při použití komunikační sběrnice Ehternet POWERLINK. Jako modelová konfigurace je uvažována strojovna, řídicí pult i hlavní hnací zařízení a bezpečnostní zařízení v dolní stanici lanovky.

Základní prvky lanové dráhy:

- Hlavní pohon - základní pohon
- Pomocný pohon - slouží jako dočasná záloha pro hlavní pohon
- Nouzový pohon - slouží pro evakuaci
- Lanové podpěry, 5x a otočná zařízení ve stanicích
- Provozní brzda - zajišťuje regulovatelné zpomalení, popřípadě klidový stav lanovky
- Bezpečnostní brzda - ovládaná hydraulicky

Norma EN 13223 definuje povinné bezpečnostní funkce uvedené v tabulce 3.27. Význam jednotlivých použitých zkratek v tabulce 3.27:

- ST = zablokování spuštění lanovky
- EZ = nouzové zastavení poháněcím motorem, při jehož použití dojde vlivem měniče k zastavení hnacích motorů. Po zastavení se aktivuje provozní brzda a motor je odpojen od napájení[1].

[1] Odpojení musí být redundantní, přičemž alespoň jedno musí být galvanické

č.	Činnost	Účinek	Kategorie	Řešení
1	Sledování skutečné rychlosti oproti nastavené	PB	AK1	PLC
2	Sledování minimální rychlosti	PB	AK1	PLC
3	Sledování směru jízdy	PB	AK2	PLC
4	Vypnutí při překročení rychlosti o 10%	PB	AK3	PLC
5	Vypnutí při překročení rychlosti o 20%	BB	AK3	PLC
6	Sledování zpomalování EB	PB	AK1	PLC
7	Sledování zpomalování PB	BB	AK1	PLC
8	Sledování zpomalování BB	PB	AK1	PLC
9	Sledování koncové polohy spojky	BB	AK3	Safety PLC
10	Změna druhu pohonů	BB	AK1	PLC
11	Sledování odbrždění polohy provozní brzdy	PB	AK1	Safety PLC
12	Sledování odbrždění polohy bezpečnostní brzdy	BB	AK1	Safety PLC
13	Sledování zabrždění polohy provozní brzdy	ST	AK1	PLC
14	Působení provozní brzdy při jízdě	PB	AK1	PLC
15	Působení bezpečnostní brzdy při jízdě	BB	AK1	PLC
16	Sledování kroutícího momentu	PB	AK1	PLC
17	Sledování přenosu síly motor-lanový kotouč	BB	AK1	PLC
18	Výpadek elektrického napájení nebo asymetrie v síti	PB	AK2	Safety PLC
19	Sledování proudového pole	PB	AK1	PLC
20	Sledování proudu do hlavního hnacího motoru	PB	AK1	PLC
21	Hydraulický přenos síly- sledování tlaku oleje	BB	AK1	PLC
22	Sledování včasného vystoupení cestujících	EB nebo PB	AK3	Safety PLC
23	Nouzový vypínač stop	EB, PB, BB	AK3	Safety PLC
24	Spínač údržby	BB	AK3	Safety PLC
25	Přerušení, zkrat sledovaných lan	EB, PB	AK3	PLC
26	Spínač ochrany motoru	PB, BB	AK1	PLC
27	Pojistky a jističe pro ochranu důležitých el. obvodů	PB	AK2	Safety PLC
28	Sledování polohy lana	EB, PB	AK3	Safety PLC

Tabulka 3.27: Požadované bezpečnostní funkce

- PB = nouzové zastavení provozní brzdou následuje poté, když to vyžaduje aktivace určité z funkcí v tabulce 3.27. Při použití PB musí být motory odpojeny od napájení
- BB = nouzové zastavení bezpečnostní brzdou následuje poté, je li aktivována určitá bezpečnostní funkce z tabulky 3.27, motory musí být opět bez napájení.
- AKx je označení bezpečnostní kategorie, určené z diagramu v příloze A, resp. z tabulky v příloze C normy EN 13243. Zabezpečení kategorie AK1 je možné zpracovávat samotným řídicím algoritmem, AK2 požaduje použití ověřených bezpečnostních prvků a u kategorie AK3 je nutné použít redundantní řešení.

Případy dalšího samočinného použití provozních a bezpečnostních brzd uvádí EN 13223. Při použití provozní, nebo bezpečnostní brzy musí byt okamžitě odpojeny pohony od napájení a současné použití obou těchto systémů je možné pouze v případě, že bude výsledné zpomalení maximálně 2.5 ms^{-2}.

Pro řešení jednotlivých bezpečnostních funkcí lze použít dva typy výpočetních logických jednotek, které ovládají společné výstupy jako logický součin obou hodnot.

Základní jednotkou je bezpečnostní PLC, které se stará o většinu binárních bezpečnostních signálů (typicky nouzové bezpečnostní tlačítko) a podle jejich hodnoty aktivuje požadovaný bezpečnostní účinek.

Druhou z jednotek je klasické řídicí PLC, které se stará o běh lanové dráhy jako celku. Díky možnosti využití analogových karet má za úkol měřit analogové hodnoty (typicky rychlost motorů) a v případě vážné odchylky aktivovat příslušné ochranné opatření. Obrázek 3.16[2] ukazuje možné rozdělení zpracování signálů různými výpočetními jednotkami. Neudává však požadavky na vstupy systému, jelikož některé ze signálů lze získat přímo, například měření kroutícího momentu lze číst z měniče a není tudíž potřeba žádný vstup.

3.3.1.1 Požadavky na řídicí systém z pohledu bezpečnosti

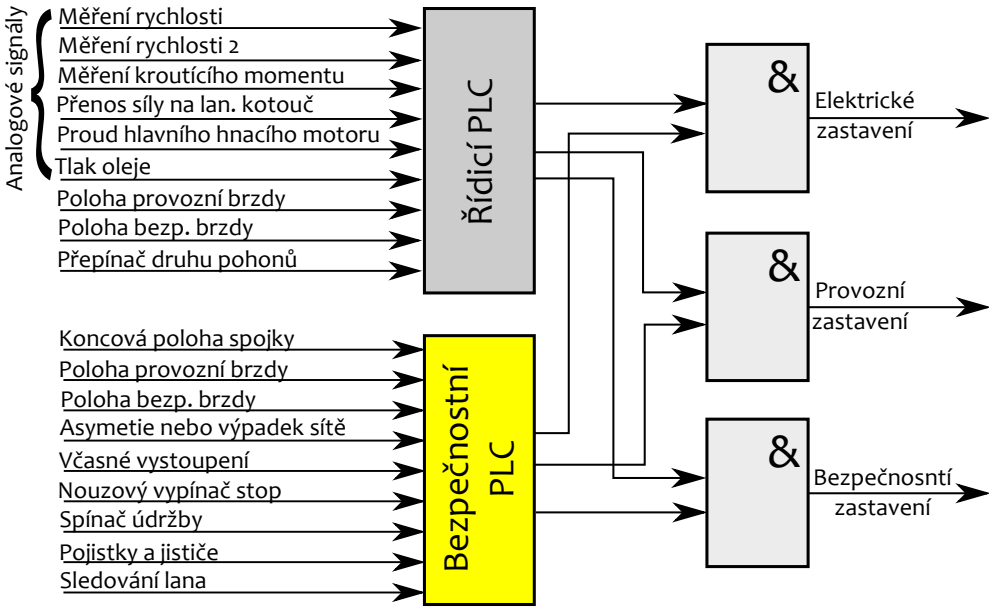
Tabulka 3.28[3] ukazuje požadavky na množství senzorů a celkový počet signálů od skupiny senzorů přivedených jako vstupy. Počty signály odpovídají požadavkům pro jednotlivé kategorie z tabulky 3.27. Pro sledování lana je redundance zajištěna sledováním lana na

[2] Je uvažována negativní logika, tzn. jednotlivé bezpečnostní opatření se aktivují při hodnotě log. 0 na odpovídajícím výstupu

[3] Sloupec Typ: AI - analogový vstup, DI - digitální vstup (přivedeny do řídicího PLC), SI- bezpečnostní vstup pro bezpečnostní PLC

Signál	Typ	Senzorů	Signálů	Umístění	Poznámka
Aktuální rychlost	AI	2	4	Strojovna	
Aktuální poloha spojky	AI	1	1	Strojovna	Přenos síly na lan. kotouč
Tlak oleje	AI	1	1	Strojovna	
Koncová poloha spojky	SI	1	2	Strojovna	
Poloha provozní brzdy	DI a SI	2	2	Strojovna	
Poloha bezpečnostní brzdy	DI a SI	2	2	Strojovna	
Problém v síti	SI	1	1	Strojovna	
Tlačítko nouzového zastavení	SI	3	6	Řídicí pult, stanice	Použito i pro nevystoupení ve stanicích
Přepínač druhů pohonů	DI	3	3	Řídicí pult	Třípolohový přepínač
Spínač údržby	SI	5	10	Strojovna, stanice, řídicí pult	
Stav pojistek a jističů	SI	1	1	Strojovna	
Sledování lana	SI	24	24	Sloupy, stanice	2x na každé straně sloupu

Tabulka 3.28: Množstevní požadavky na senzory a signály



Obrázek 3.16: Rozdělení zpracování signálů pro lanovou dráhu

č.	Typ modulu	Umístění	Počet vstupů	Poznámka
1	2x X20AI 4632	Strojovna	2x 4 analogové	
2	X20DI 4371	Strojovna	4 digitální	
3	X20DI 4371	Řídicí pult	4 digitální	
4	2x X20SI 4100	Strojovna	2x 4 bezpečnostní	
5	X20SI 4100	Řídicí pult	4 bezpečnostní	
6	2x X20SI 4100	Dolní stanice	2x 4 bezpečnostní	
7	2x X20SI 4100	Horní stanice	2x 4 bezpečnostní	
8	5x X67SC 4122	Sloupy	5x 8 bezpečnostních	Krytí IP67, každý sloup

Tabulka 3.29: Množstevní požadavky na bezpečnostní vstupy

dvou místech jedné strany lanové podpěry. Požadavky na počty a umístění senzorů pro jednotlivé signály definují normy EN 13223 a EN 13243.

Tabulka 3.29 ukazuje požadavky na počty karet pro vstupy signálů sloužících pro dosažení bezpečnosti. Počty/typy karet pro signály zpracovávané pomocí řídicího PLC ale nejsou konečné, z důvodu přivedení dalších signálů potřebných pro řízení a ovládání lanové dráhy.

Výstupní bezpečnostní signály jsou všechny pouze binární a jejich akční zásah probíhá ve strojovně. Tyto signály ukazuje je tabulka 3.30. Pro uvedených šest signálů stačí použít

dva kusy modulu X20SO 4110 v módu DIRECT pro řízení výstupů jak z bezpečnostního programu tak z řídicího PLC.

Signál	Počet výstupů	Ovlivněné zařízení
Napájení motorů	2	Stykače pro napájení měničů
Elektrické zastavení	1	Vstup Enable na měničích pohonů
Aktivace provozní brzdy	2	Vstup total stop měničů a provozní brzda
Aktivace bezpečnostní brzdy	1	Bezpečnostní brzda

Tabulka 3.30: Požadavky na bezpečnostní výstupy

3.3.1.2 Využití moderních řídicích prvků pro bezpečnost lanových drah

Normou EN 13223 je zmíněna nutnost odpojit při provozním, popřípadě bezpečném zastavení motory od napájení. Tato nutnost sebou nese ovšem i mnoho úskalí. Měniče, které se používají pro moderní řízení rychlosti pohybu lanových drah potřebují zpravidla několik desítek sekund k připravenosti provozu při připojení napájení. Tento čas se může projevit na kvalitě služby poskytované lanovkou. Řešením by bylo použít moderní řídicí jednotky motorů s implementovanými bezpečnostními funkcemi. Mezi tato moderní zařízení patří například Acopos multi SafeMC od společnosti B&R, který využívá bezpečnostní funkční bloky z již zmíněné knihovny PLCopen, které obsahují velké množství bezpečnostních funkcí, více viz [3]. Některé základní funkce řízení motorů měničem Acopos muli SafeMC:

- Safe Torque Off (SIL 3) - základní funkce pro okamžité zastavení motoru odebráním momentu
- Safely Limited Speed (SIL 2) - řízené zpomalování do dosažení nastaveného limitu
- Safe Direction (SIL 2) - funkce sleduje nastavený směr pohybu motoru
- Safe Stop 1 (SIL 3) - řízené zpomalování a při určitém rychlostním limitu pak odebrání momentu motoru jako v prvním případě
- Safe Stop 2 (SIL 3) - řízené zpomalování motoru až do nulové rychlosti

Díky uvedeným funkcím je vidět v porovnání s tabulkou 3.27 že pro velké množství bezpečnostních funkcí by bylo použití Acoposu multi SafeMC plně dostačující.

Kapitola 4

Závěr

Cílem práce bylo seznámení se s požadavky na funkční bezpečnost strojů definované v několika normách a tyto požadavky následně aplikovat na dvě rozdílná strojní zařízení. Jako výchozí byla zvolena nejobecnější norma ČSN EN 61508. Vzhledem ke svému rozsahu byla specifikována norma EN 61508 tak, aby byly všechny části praktické části práce plně srozumitelné bez nutnosti podrobné znalosti uvedené normy.

Požadavkem na realizaci jednotlivých bezpečnostních funkcí bylo využití protokolu openSAFETY. Princip protokolu, jeho kompatibilita s bezpečnostními normami a jeho základní parametry, včetně definovaného základního komunikačního rámce jsou popsány v teoretické části práce.

Byla provedena riziková analýza modelu Žonglér a CNC pálicího stroje, ze kterých vyplynuly možné bezpečnostní úskalí provozu těchto zařízení. Pro obě zařízení byla navržena bezpečnostní opatření odpovídající požadavkům na snížení rizik plynoucích z analýzy. Jako bezpečnostní funkční prvky byly zvoleny komponenty společnosti B&R. Jako bezpečnostní PLC byl zvolen SafeLogic X20SL8000 používající protokol openSAFETY, který řídí bezpečnostní vstupy a výstupy. Pro model Žonglér byly uvedené bezpečnostní funkce realizovány. Byl vyvinut algoritmus implementující požadované bezpečnostní funkce. Schopnost těchto funkcí zabránit odpovídajícím rizikům byla otestována a stroj úspěšně uveden do provozu, přičemž je kompatibilní s normou ČSN EN 61508. U CNC stroje byly výstupy rizikové analýzy a doporučené bezpečnostní opatření sděleny výrobci stroje, který nese zodpovědnost za jeho bezpečnost.

Poslední částí práce je případová studie pro zabezpečení visuté lanové dráhy. Pomocí příslušných norem jsou vyjmenovány bezpečnostní požadavky na funkce pro zajištění bezpečnosti provozu lanové dráhy. Zpracováním těchto požadavků vznikly potřebné specifikace a možnosti řešení zabezpečení modelové dráhy a byly navrženy doporučené

bezpečnostní hardwarové prvky pro realizaci požadovaných funkcí.

Tato práce ukazuje všechny zásadní kroky při zajišťování kompatibility stroje s normou EN 61508, včetně volby bezpečnostního zařízení a jeho parametrů při využití protokolu openSAFETY jako univerzálního protokolu pro zajištění funkční bezpečnosti.

Literatura

[1] Ace. *Main catalogue*, 2007.

[2] Balluff. *The mechanical line*. katalog.

[3] B&R Automation. *Help - Automation Studio 3.0.80*.

[4] B&R Automation. *Integrated Safety Technology User's Manual,v 1.20*.

[5] B&R Automation. *Acopos User's Manual,v 1.41*, 2009. online, http://www.br-automation.com.

[6] Burget, P. *Žonglování*. *Automa*, 7, 2010.

[7] Dräger. *Dräger PIR 7000*. online,

$http://www.draeger.com/CZ/cs/products/stationary\_gas\_detection/ex/gds\_pir\_7000.jsp$

.

[8] EPSG. *OpenSAFETY - Safety profile specification, v 1.1.3*, 2010.

[9] Český normalizační institut. *ČSN 33 3570 - Elektrická zařízení lanových drah a lyžařských vleků*, 1994.

[10] Český normalizační institut. *ČSN EN 62061 - Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů souvisejícíh s bezpečností*, 2004.

[11] Český normalizační institut. *ČSN EN 12397 - Bezpečnostní požadavky na osobní lanové dráhy - Provoz*, 2005.

[12] Český normalizační institut. *ČSN EN 12408 - Bezpečnostní požadavky na osobní lanové dráhy - Zabezpečování kvality*, 2005.

[13] Český normalizační institut. *ČSN EN 12930 - Bezpečnostní požadavky na osobní lanové dráhy - Výpočty*, 2005.

[14] Český normalizační institut. *ČSN EN 13223 - Bezpečnostní požadavky na osobní lanové dráhy - Poháněcí a další mechanická zařízení*, 2005.

[15] Český normalizační institut. *ČSN EN 13243 - Bezpečnostní požadavky na osobní lanové dráhy - Elektrická zařízení mimo poháněcí zařízení*, 2005.

[16] Český normalizační institut. *ČSN EN 61508 - Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností*, 2007.

[17] Český normalizační institut. *ČSN EN ISO 13849 - Bezpečnost strojních zařízení - Bezpečnosntí části ovládacích systémů*, 2007.

[18] Famfulík, J. a Míková, J. Příspěvek k analýze rizika modulu automatického vedení vlaku. *Perners Contact*, 2, 2009.

[19] Jaroš, P. *Dynamika rychlých servopohonů*, 2009.

[20] Kohout, T. *Model Žonglér pro vzdálenou výuku a řízení CNC stroje*, 2011.

[21] Leuze. *Safety lights curtains.* online,

$$http://www.leuze.de/products/las/slv/solid-4e/p\_01\_en.html$$

.

[22] Moeller. *AVA-131-1268.* montážní instrukce, katalog.

[23] Moeller. *HPL0211-2001/2002.* katalog.

[24] Moeller. *Stykače a relé*, 2007. katalog.

[25] Necid, J. a Nývlt, O. *Analýza rizik modelu Žonglér. Automa*, 2, 2011.

[26] Polák, P. *Bezpečnostní funkce pro Simatic S7*, 2009.

[27] Prudek, L. *Řízení rychlých servopohonů*, 2009.

[28] Rausand, M. *Preliminary hazard analyses.* výukové slidy, 2005.

[29] Sneider. *Motor control*, 2007. katalog.

[30] Valter, J. *Regulace*. online, ⟨http://valter.byl.cz⟩.

Příloha A

Praktická realizace bezpečnostních opatření

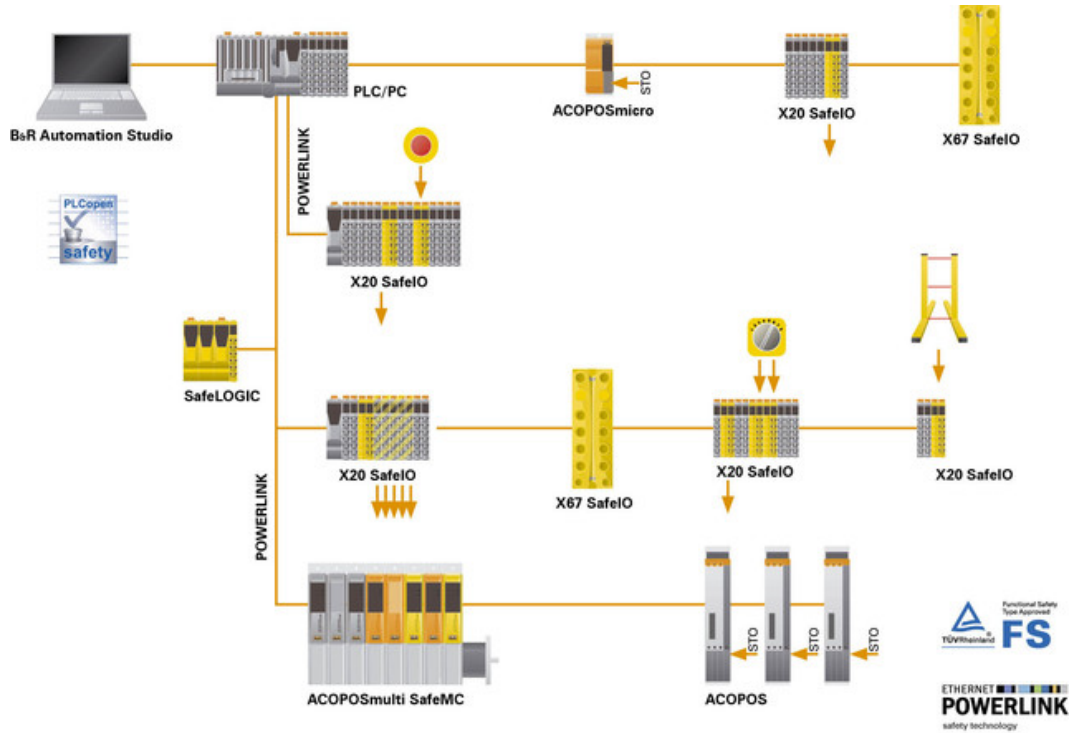
Tato příloha slouží jako pomůcka při vývoji a realizaci bezpečnostních opatření pomocí bezpečnostního protokolu openSAFETY. Jedná se pouze o jednoduchý návod pro zapojení a uvedení do provozu zařízení od společnosti B+R využívající openSAFETY protokol, jehož nezbytným doplňkem je Help vývojového prostředí Automation Studio 3.0 (AS Help, viz [3]).

V následujících odstavcích se předpokládá již hotová riziková analýza zařízení, určeného pro použití openSAFETY protokolu, včetně požadavků na bezpečnostní funkce a jejich realizaci podle normy ČSN EN 61508.

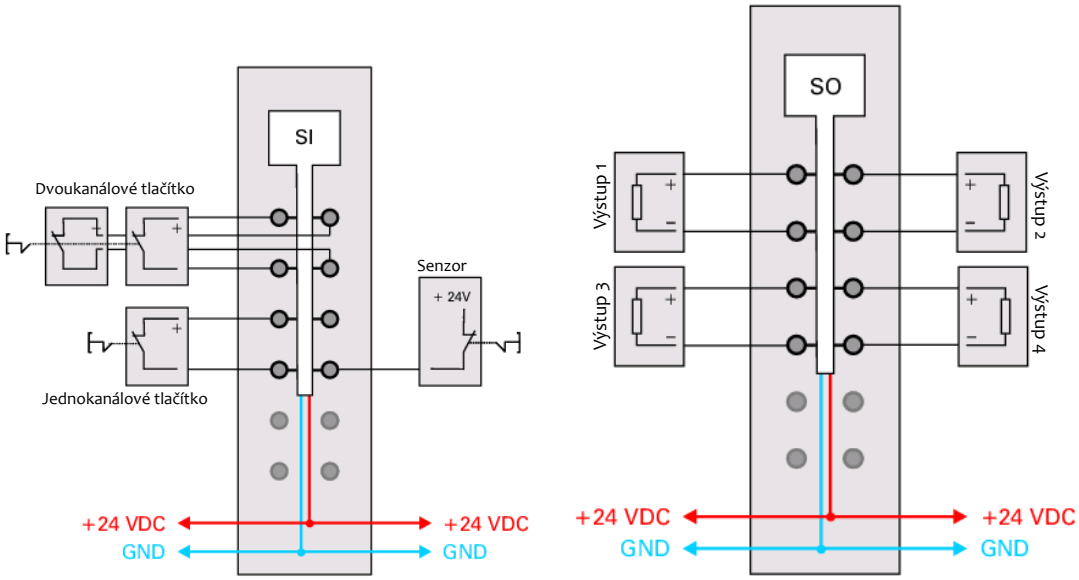
A.1 Zapojení jednotlivých komponent

Hlavním poznávacím znakem openSAFETY protokolu je využití hlavní komunikační sběrnice pro bezpečnostní účely a proto každá z bezpečnostních komponent musí být schopna komunikovat po sběrnici, jak je vidět na obrázku A.1.

Dalším krokem je připojení komponent k napájení a připojení jednotlivých vstupů a výstupů podle požadavků z výchozí rizikové analýzy. Způsoby pro jednotlivá připojení jsou uvedeny v **AS Help**. Na obrázku A.2(a) je vidět možné zapojení 3 vstupních prvků pro kartu bezpečnostních vstupů X20SI 4100. Možné zapojení bezpečnostních výstupů ukazuje obrázek A.2(b).



Obrázek A.1: Modelová topologie sítě při využití openSAFETY protokolu



(a) Zapojení X20SI 4100

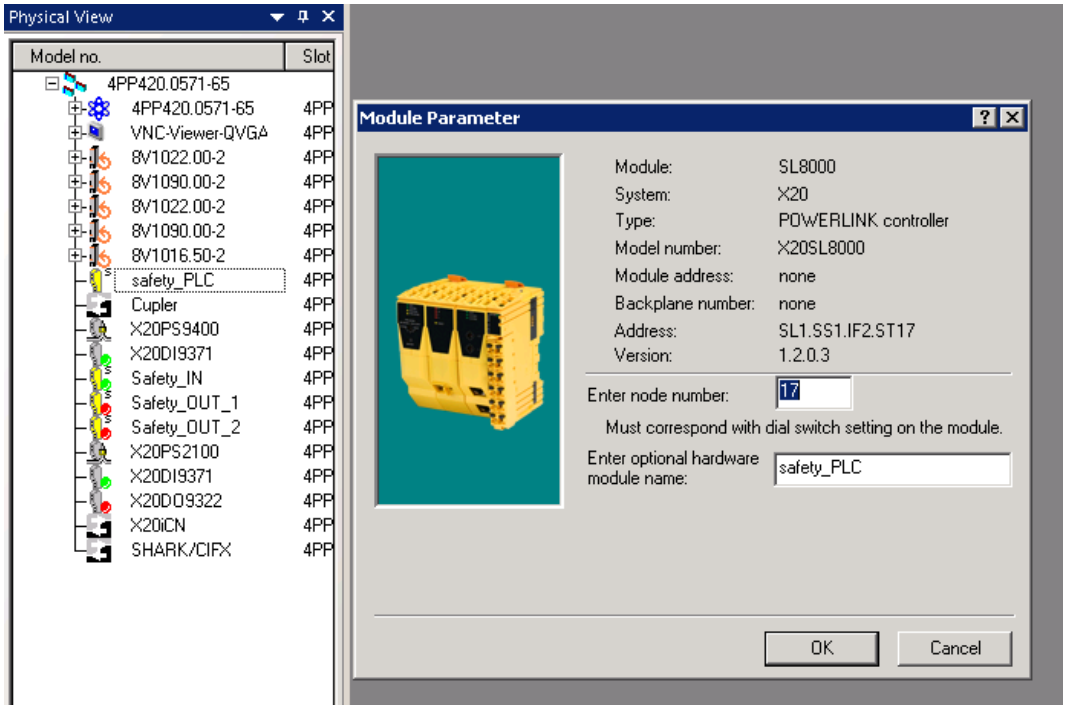
(b) Zapojení X20SO 4110

Obrázek A.2: Možnosti zapojení vstupních a výstupních karet

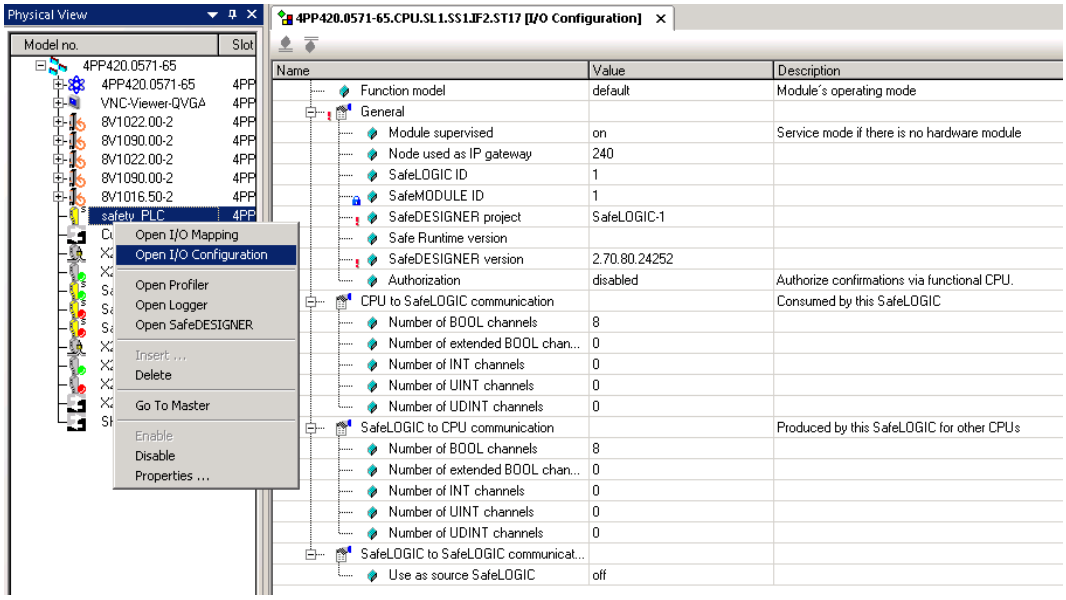
A.2 Vytvoření bezpečnostního programu

Vytvoření bezpečnostního programu se skládá z těchto kroků:

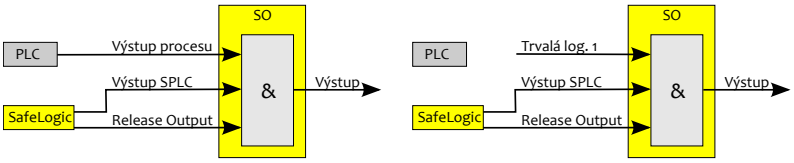
1. Otevření programu Automation Studio min. v. 3.0 (AS)
2. Založení nového projektu
3. Přidání hlavního CPU do HW konfigurace
4. Nastavení IP adresy komunikačního CPU
5. Vytvoření Compact Flash disku
6. Navázání spojení mezi AS a CPU
7. Vytvoření sběrnice POWERLINK (PL) v HW konfiguraci
8. Přidání zbývajících komponent na PL (Pro SAFETY komponenty platí, že nejprve je nutné přidat bezpečnosntí PLC SafeLogic a teprve poté lze přidat bezpečnostní I/O):
   Otevření PL> Pravé tlačítko> Insert> Vybrání komponenty z nabídky (např. SL8000)> Přiřazení PL adresy a zobrazovaného jména> Potvrzení, viz obrázek A.3
9. Definování názvu přiřazeného bezpečnostního programu a kontroly verze SafeDESIGNERU:
   Pravým tlačítkem na SL8xxx> Open I/O configuration, viz obrázek A.4
10. Určení ovládání bezpečnostních výstupů. Jelikož lze k bezpečnostním výstupům přistupovat z hlavního řídícího programu, mohou být zvoleny 2 základní typy spínání, a to **direct**, kdy je výsledná hodnota bezpečnostního výstupu podle obrázku A.5(a) nebo metoda **via SafeLOGIC**, kdy je hodnota totožná s výstupní hodnotou bezpečnostního programu podle obrázku A.5(b)
11. Transfer HW konfigurace do CPU
12. Otevřít SafeDESIGNER:
    Pravým tlačítkem na SL8xxx> Open SafeDESIGNER, viz obrázek A.6
13. Při prvním spuštění bude SD požadovat nastavení přístupových hesel pro různé úrovně, obrázek A.7



Obrázek A.3: Přidání safety komponenty na POWERLINK

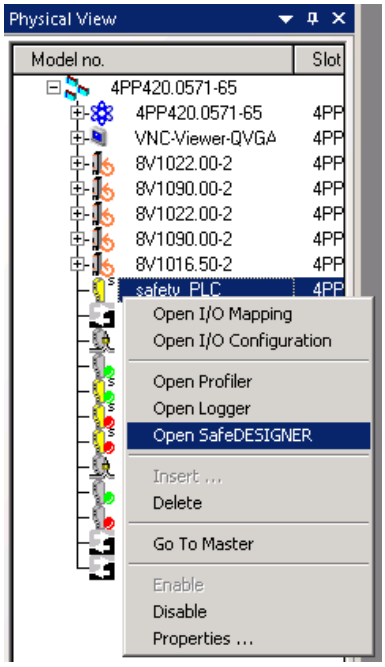


Obrázek A.4: Konfigurace Safety PLC

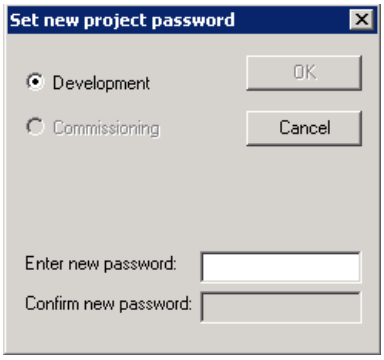


(a) Direct (b) via SafeLOGIC

Obrázek A.5: Způsoby řízení bezpečnostního výstupu



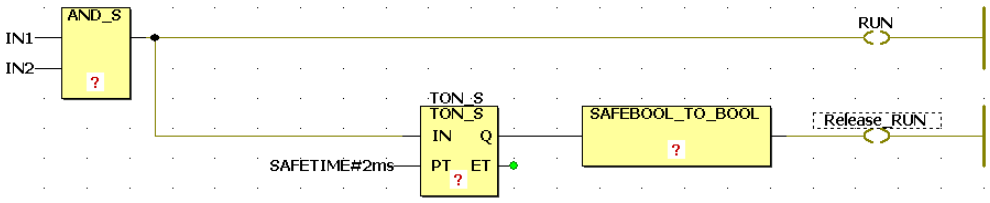
Obrázek A.6: Otevření SD z HW konfigurace



Obrázek A.7: První spuštění SD

14. Základní pokyny pro vytvoření jednoduchého bezpečnostního programu:

    - Vývoj bezpečnostního programu probíhá pomocí ladder diagramu podobně jako u klasického programu
    - K I/O lze přistupovat buď přes tlačítko Global variables, nebo je lze použít přetažením na pracovní plochu z HW stromu
    - Hodnota každého safety výstupu se na fyzický výstup přepíše až s náběžnou hranou odpovídajícího Release output. Tento postup například umožňuje nastavit hodnoty několika nezávislých bezp. výstupů v jeden moment zároveň.
    - Obrázek A.8 ukazuje jednoduchý bezpečnostní program pro základní obouruční ovládání stroje

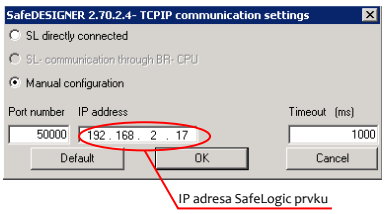


Obrázek A.8: Jednoduchý program SD

15. Kompilace programu stisknutím tlačítka "Compile"
16. Nastavení spojení *Online> TCPIP communication settings*

    - "SL directly conected"v případě, že je možnost se připojit na PL port přímo na SafeLogicku
    - "Manual configuration"kde se jako adresa IP vyplní adresa prvku SafeLogic na síti POWERLINK, viz obrázek A.9. Pro tento mód je připojení realizováno pomocí hlavního CPU, který má za úkol přeposílat data určená pro SL. Toho lze dosáhnout nastavením směrování v příkazovém řádku:
      route add [IP adresa PL sítě] mask [maska podsítě] [IP CPU], příklad *route add 192.168.2.0 mask 255.255.255.0 192.168.1.1*

17. Zmáčknutím tlačítka SafePLC dojde ke spojení s bezpečnostním PLC
18. Download (ideálně v DEBUG módu a SafePLC je zastavené)
19. Bezpečnostní aplikace je připravena k použití



Obrázek A.9: Připojení k SD

Při prvním spuštění se může vyskytnout na SL několik stavů, jejichž řešení pomocí přepínače na SL ukazuje tabulka A.1.

Stav	Signalizace	Řešení nastavením přepínače na
FW-ACK	svítí	SK-XCNG + Enter
MX-ACKN	bliká v sériích	Zvolit číslo dle počtu bliknutí (n pro počet >4) + Enter
FW-ACKN	bliká	FW-ACKN + Enter

Tabulka A.1: Řešení nejčastějších nastavení při prvním spuštění

Pro řešení dalších problémů plně dostačuje AS Help, kde jsou popsány jednotlivé stavy systému a nastíněna možnost jejich řešení.

Příloha B

Obsah přiloženého DVD

K této práci je přiloženo DVD s těmito adresáři:

- Žonglér - obsahuje projekt Žonglér včetně bezpečnostního programu
- Diplomová práce - obsahuje soubor s touto DP