ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA APLIKOVANÉ ELEKTRONIKY A TELEKOMUNIKACÍ

DIPLOMOVÁ PRÁCE

Návrh bezpečného systému pro řízení lisu chmele

Bc. Lukáš Martínek **2018**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš MARTÍNEK**
Osobní číslo:	**E16N0076P**
Studijní program:	**N2612 Elektrotechnika a informatika**
Studijní obor:	**Dopravní elektroinženýrství a autoelektronika**
Název tématu:	**Návrh bezpečného systému pro řízení lisu chmele**
Zadávající katedra:	**Katedra aplikované elektroniky a telekomunikací**

Zásady pro vypracování:

Úkolem práce je návrh elektronického systému pro automatizované řízení lisu chmele s ohledem na požadavky bezpečnosti dle příslušných norem.

1. Prostudujte a vyberte vhodné normy vztahující se k návrhu bezpečných systémů v dané oblasti.
2. Vytvořte specifikaci pro řídicí systém a proveďte rizikovou analýzu.
3. Sestavte koncept řídicího systému a navrhněte vhodné bezpečnostní funkce.
4. Zhodnoďte vliv bezpečnostních funkcí s ohledem na snížení rizika.

Rozsah grafických prací:	**podle doporučení vedoucího**
Rozsah kvalifikační práce:	**40 - 60 stran**
Forma zpracování diplomové práce:	**tištěná/elektronická**

Seznam odborné literatury:

Student si vhodnou literaturu vyhledá v dostupných pramenech podle doporučení vedoucího práce.

Vedoucí diplomové práce:	**Ing. Luděk Elis** Regionální inovační centrum elektrotechniky
Datum zadání diplomové práce:	**10. října 2017**
Termín odevzdání diplomové práce:	**24. května 2018**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Dr. Ing. Vjačeslav Georgiev
vedoucí katedry

V Plzni dne 10. října 2017

Abstrakt

Předkládaná diplomová práce je zaměřena na návrh bezpečného systému pro řízení lisu chmele s ohledem na požadavky dle příslušných norem. Text této diplomové práce je rozdělen do tří částí. V první části jsou uvedeny normy používané při návrhu systému nebo zařízení související s bezpečností. V další části je popsána bezpečnostní norma, podle které bude probíhat návrh elektronického systému pro lis chmele, tedy ČSN EN 62061. Třetí část popisuje současný stav zařízení pro lisování chmele a návrh elektronického řídicího systému souvisejícího s bezpečností pro toto zařízení.

Klíčová slova

Bezpečnost, ČSN EN 62061, elektronický řídicí systém, lis chmelu, norma

Abstract

This diploma thesis is focused on the design of a safe hops press system with respect to the requirements of the relevant standards. The text of this diploma thesis is divided into three parts. In the first part, the standards used in designing the system or the safety related devices are mentioned. The next part describes the safety standard according to which the design of the electronic system for hop production, i.e. ČSN EN 62061, will be carried out. The third part describes the current state of the hops pressing plant and the design of the electronic safety management system for this equipment.

Key words

Safety, ČSN EN 62061, electronic control system, hops pressure, standard

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této diplomové práce, je legální.

.....

podpis

V Plzni dne 14.5.2018 Bc. Lukáš Martínek

Poděkování

Tímto bych rád poděkoval vedoucímu diplomové práce Ing. Luďku Elisovi za cenné profesionální rady, připomínky a metodické vedení práce.

Obsah

Úvod

Cílem této diplomové práce je návrh bezpečného systému pro řízení lisu chmele podle příslušných norem.

V první části jsou uvedeny nejčastěji zmiňované a používané normy pro návrh systémů souvisejících s bezpečností, především ČSN EN 61508, ČSN EN ISO 13849 a ČSN EN 62061. Dále je zde popsáno, jak se bezpečností normy pro strojní zařízení rozdělují.

Druhá část této práce podrobněji popisuje bezpečnostní normu ČSN EN 62061 podle které bude probíhat návrh elektronického systému pro řízení lisu chmele. Jsou zde uvedeny definice důležitých pojmů a postup návrhu podle této normy. Velkou částí této kapitoly je popis stanovení úrovně integrity bezpečnosti (SIL), proces výpočtu intenzit poruch a určení podílu bezpečných poruch (SFF).

Poslední část této práce obsahuje podrobný popis postupu návrhu celého řídícího systému souvisejícího s bezpečností (SRECS). Navržený systém je rozdělen do čtyř subsystémů, které jsou následně podrobně popsány a analyzovány z hlediska intenzit poruch a podílu bezpečných poruch. Na konci této kapitoly je ověření, zda celý systém splňuje požadavky dané normou a je tedy vhodný jako bezpečný systém pro řízení lisu chmele.

Seznam symbolů a zkratek

SIL ..... Úroveň integrity bezpečnosti (Safety Integrity Level)

PLr ..... Performance Level

SILCL ..... Dosažitelná mez (SIL Claim Limit)

SRECS ..... Elektrický řídicí systém související s bezpečností (Safety – Related Electrical Control System)

SRCF ..... Řídicí funkce související s bezpečností (Safety – Related Control Function)

MTTF ..... Střední doba do poruchy (Mean Time To Failure)

PFH_D ..... Pravděpodobnost nebezpečné poruchy za hodinu (Probability of dangerous Failure per Hour)

T_1 ..... Interval kontrolní zkoušky nebo doba života (Check interval)

β ..... Citlivost na společné poruchy (Sensitivity to common failure)

λ ..... Intenzita poruch (Intensity of failures)

λ_S ..... Intenzita bezpečných poruch (Intensity of safety failures)

λ_D ..... Intenzita nebezpečných poruch (Intensity of dangerous failures)

λ_{DD} ..... Intenzita nebezpečných detekovatelných poruch (Intensity of dangerous detectable failures)

1 Normy zabývající se funkční bezpečností strojů

Problematika bezpečnosti strojů a zařízení není jednoduchá. Kompletní postup pro návrh bezpečného stroje zahrnuje mnoho úkonů a norem. Bezpečnost strojních zařízení je v moderní společnosti nejdůležitější částí každého systému, kde nějaká jeho součást vykonává mechanický pohyb. Jde o sadu opatření pro zamezení kontaktu stroje a jakékoliv části lidského těla během tohoto pohybu.

Jedná se o ekvivalent bezpečnosti elektrických zařízení, kde je potřeba chránit lidskou obsluhu proti nebezpečí úrazu elektrickým proudem. Požadavky na zajištění bezpečnosti proti elektrickému proudu jsou brány jako velmi důležité ale u mechanických pohybů strojů se dlouho a často zanedbávaly. Mohou však způsobit stejně závažná zranění.

Zajištění bezpečnosti strojních zařízení je složitý proces a je potřeba se jí zabývat už při návrhu aplikace a pokud možno ji co nejlépe zahrnout hned od počátku samotné konstrukce strojů. Rizika, která nelze minimalizovat prvky konstrukce stroje, je nutné ošetřit. Zbytkové riziko je pak potřeba uvést na strojích pomocí štítků a detailně i v dokumentaci.

Vývoj zařízení a strojů z hlediska bezpečnosti není dnes problematika jen dvou nejznámějších norem ČSN EN ISO 13849 a ČSN EN 62061, ale je potřeba se řídit velice širokou škálou standardů a norem. Dokonce některé z těchto norem mohou být při výrobě více závazné než tyto velice známé normy.

1.1 Rozdělení bezpečnostních norem

Z norem vytvářených CEN/CENELEC, které jsou zaměřené na základní bezpečnostní požadavky za účelem dosažení jednotnosti s evropskou legislativou v oblasti strojních zařízení, se normy dělí do třech základních skupin.

1.1.1 A-normy (Základní bezpečnostní normy)

Tyto normy poskytují základní pojmy a ustanovení pro projektování, konstrukci a obecná pravidla, která by mohla být aplikována na všechny stroje. Patří sem například EN ISO 14121 (Bezpečnost strojních zařízení – zásady pro posouzení a identifikaci rizika), nebo ČSN EN 61508 (Funkční bezpečnost elektrických, elektronických a programovatelných elektrických systémů souvisejících s bezpečností).

1.1.2 B-normy (Skupinové bezpečnostní normy)

Normy skupinové se zabývají pouze jedním bezpečnostním aspektem nebo jedním typem bezpečnostního zařízení. Zaměřují se na bezpečnostní požadavky nebo bezpečnostní zařízení a lze je použít na široké škále strojů.

Mezi tyto normy se řadí normy typu B1 pro speciální bezpečnostní požadavky, jako jsou teplota povrchu, hluk, elektrická bezpečnost strojů, požadavky na řídicí systém a podobně. Dále pak normy typu B2 pro bezpečnostní zařízení, kterým je například dvouruční ovládání.

Do kategorie B-norem patří ČSN EN ISO 13849 (Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů) a ČSN EN 62061 (Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných řídicích systémů souvisejících s bezpečností), ale také například EN 60204-1 (Bezpečnost strojních zařízení) nebo IEC 61496-1 (Elektrická snímací ochranná zařízení).

1.1.3 C-normy (Speciální bezpečnostní normy)

C-normy určují detailní bezpečnostní požadavky pro každý jednotlivý stroj nebo skupinu strojů a obsahují bezpečnostní požadavky na stroje speciální nebo konstrukční skupinu strojů. Obvykle se jedná o zařízení, které pracuje ve velmi náročných podmínkách (hygienické prostředí, výbušné prostředí, prostředí s radiací apod.) nebo o stroje speciální s atypickou strukturou konstrukce. Patří sem například norma ČSN EN ISO 10218 (Roboty pro výrobní prostředí – Požadavky na bezpečnost).

Z výše uvedeného textu je zřejmé, že čím "vyšší" skupina, tím detailnější informace norma pro konstrukci daného stroje obsahuje. Ovšem platí, že daný stroj musí splňovat nejen detailní požadavky z norem typu B a C, které mají přednost, ale současně nesmí být v úplném rozporu s příslušnými normami typu A [1].

1.2 Základní informace o ČSN EN 61508, ČSN EN ISO 13849 a ČSN EN 62061

Tyto tři normy jsou nejznámější a zároveň nejpoužívanější při řešení bezpečnosti strojních zařízení a vším, co s tím souvisí. Proto budou v této kapitole popsány podrobněji.

1.2.1 Norma ČSN EN 61508

Norma ČSN EN 61508 je obecný dokument, který je určený pro jakékoliv odvětví průmyslu a pokrývá celý životní cyklus bezpečnosti systémů obsahujících elektrické, elektronické, programovatelné elektronické součásti využívané pro zajištění bezpečnostních funkcí. Obsahuje celkem sedm částí. První tři části jsou normativní, zbylé čtyři části jsou pouze informativní. Jsou zde také příklady použití [2].

1.2.2 Porovnání norem ČSN EN ISO 13849 a ČSN EN 62061

Obě tyto normy definují požadavky na návrh a následné provedení bezpečnostních částí řídicího systému. Norma ČSN EN 62061 využívá numerický postup pro určení rizika a výsledkem je hodnota SIL (úroveň integrity bezpečnosti). Tato norma je především zaměřena na elektrické a elektronické řešení bezpečnosti strojů. Norma ČSN EN ISO 13849 pro určení úrovně bezpečnosti používá rizikové grafy. Výsledkem je PLr (Performance Level). Tato norma zahrnuje možnost použití i mechanických, pneumatických a hydraulických prvků.

Jak už bylo uvedeno v úvodu, pro mojí aplikaci byla zvolena norma ČSN EN 62061. Proto bude dále detailněji popsána a bezpečný systém pro lisování chmele bude navržen podle ní [3].

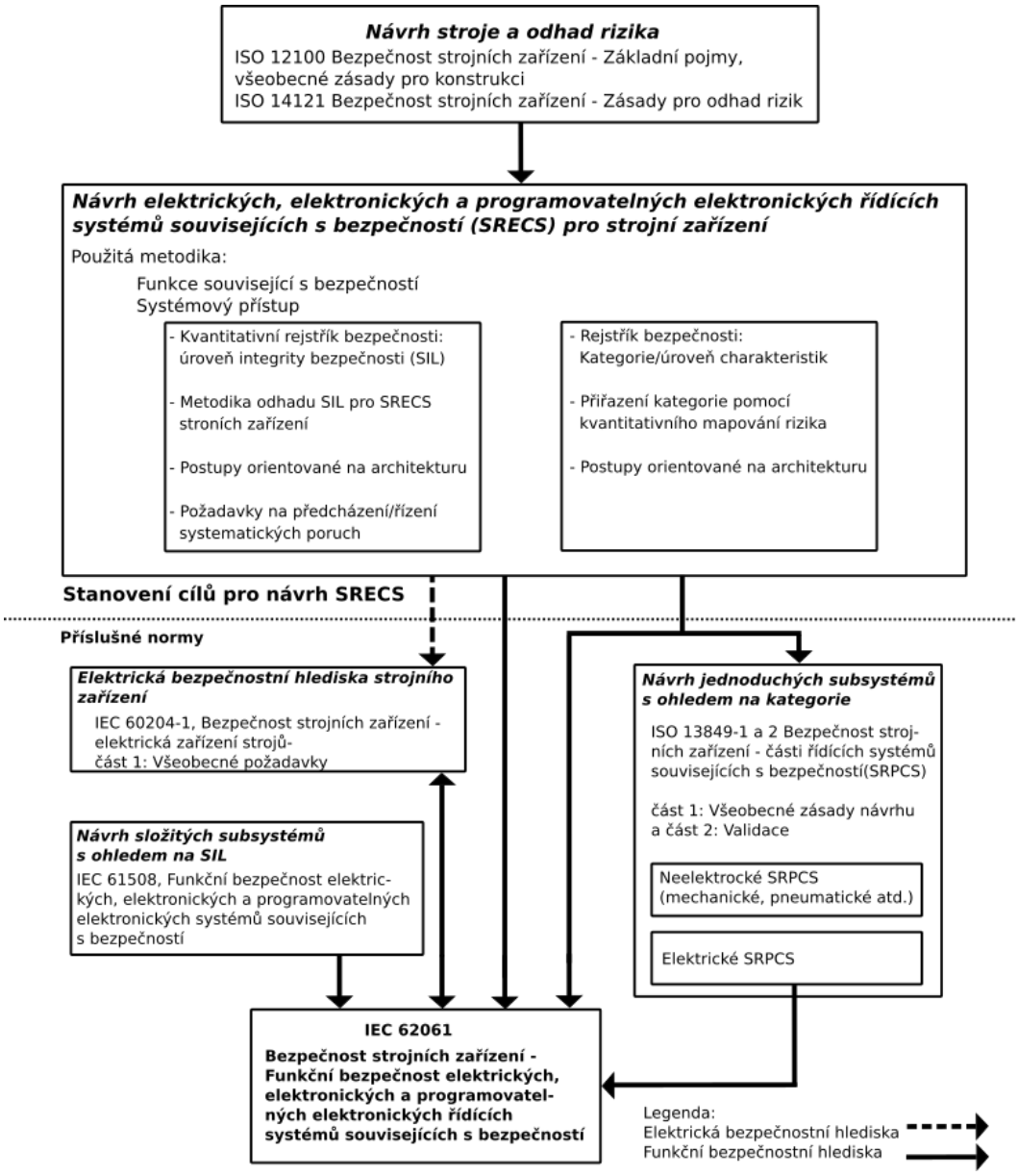
1.3 ČSN EN 62061

Jelikož je stále více zaváděna automatizace a objem výroby se neustále zvyšuje, snižuje se fyzická námaha obsluhy. Proto mají elektrické nebo elektronické řídicí systémy související s bezpečností (SRECS) stále důležitější úlohu. Je to z důvodu dosažení celkové bezpečnosti strojního zařízení. Ovšem i vlastní SRECS stále více využívá složité elektronické prostředky.

Tato norma je určena jak pro konstruktéry strojních zařízení, tak pro výrobce řídicích systémů, nebo montážní pracoviště a ostatní pracovníky, kteří jsou součástí týmu při specifikaci, návrhu a validaci SRECS. Určuje požadavky a postupy pro dosažení požadované funkce zařízení či stroje. ČSN EN 62061 patří do skupiny norem pro strojní zařízení v rámci IEC 61508 a je určena pro zjednodušení specifikace funkce řídicího systému vztahujícího se k bezpečnosti s ohledem na nezanedbatelná nebezpečí vztahující se ke stroji. Jedná se o rámcovou normu pro strojní zařízení, která se týká funkční bezpečnosti SRECS strojů a zaměřuje se pouze na ta hlediska životního cyklu, která se týkají určení bezpečnostních požadavků na základě validace bezpečnosti.

Existuje velké množství strojů, kde byl použit nějaký SRECS, jako součást bezpečnostních opatření pro snížení rizika. Nejčastějším řešením je použití ochranného krytu s využitím blokování, který při otevření pro přístup do nebezpečného prostoru stroje zajistí, aby řídicí systém nějakým způsobem zamezil nebezpečnou funkci stroje. Elektrický řídicí systém přispívá také v automatizaci pro zaručení správné funkce stroje.

Tato norma je určena pro použití v rámci soustavného snižování rizika popisovaného v ISO 12100-1 a v souvislosti hodnocení rizika podle ISO 14121. Na Obr. 1 je znázorněna souvislost této normy a ostatních souvisejících norem [4].



Obr. 1 Vztah mezi ČSN EN 62061 a dalšími příslušnými normami [4]

1.3.1 Důležité termíny a definice z normy ČSN EN 62061

- **Strojní zařízení (stroj)** – celek sestavený z částí nebo součástí strojů z nichž je alespoň jedna pohyblivá, s příslušnými pohonnými zařízeními a vzájemně spojenými za účelem přesně stanoveného používání
- **Řídicí systém stroje** – systém, který reaguje na vstupy z ostatních prvků stroje a generuje výstupy tak, aby se stroj choval určeným způsobem
- **Elektrický řídicí systém související s bezpečností (SRECS) –** elektrický řídicí systém, jehož porucha může vést k okamžitému nárůstu rizik
- **Subsystém –** entita vrcholové úrovně konstrukční architektury SRECS, kde porucha jednoho subsystému má za následek poruchu řídicí funkce související s bezpečností
- **Funkční bezpečnost –** část celkové bezpečnosti stroje a řídicího systému stroje závislá na fungování SRECS
- **Nebezpečí –** potenciální zdroj fyzického zranění nebo poškození zdraví
- **Riziko –** kombinace pravděpodobnosti výskytu škody a závažnosti této škody
- **Bezpečnostní funkce –** funkce stroje, jejíž porucha může vést k okamžitému zvýšení rizika
- **Řídicí funkce související s bezpečností (SRCF) –** řídicí funkce realizovaná v rámci SRECS s předepsanou hladinou integrity určená pro zachování bezpečnostní podmínky stroje nebo pro zabránění okamžitému zvýšení rizika
- **Diagnostická funkce SRECS –** funkce určená pro detekci poruchových stavů uvnitř SRECS a pro vyvolání předepsané výstupní informace nebo činnosti při detekci poruchového stavu
- **Úroveň integrity bezpečnosti (SIL) –** diskrétní úroveň (jedna ze tří možných) pro stanovení požadavků integrity bezpečnostních řídicích funkcí souvisejících s bezpečností, které mají být přiřazeny k SRECS, kde úroveň integrity bezpečnosti tři má nejvyšší úroveň integrity bezpečnosti a úroveň jedna nejnižší
- **Dosažitelná mez (SILCL) –** maximální SIL, kterou lze pro subsystém SRECS uplatňovat s ohledem na omezení architektury a systematickou integritu bezpečnosti
- **Pravděpodobnost nebezpečné poruchy za hodinu PFH_D –** střední pravděpodobnost nebezpečné poruchy za 1 hodinu
- **Funkční blok –** nejmenší prvek SRCF, jehož porucha může vést k poruše SRCF
- **Střední doba do poruchy MTTF –** očekávaná střední doba do poruchy

- **Architektura –** specifické uspořádání hardwarových a softwarových prvků SRECS
- **Nebezpečná porucha –** porucha SRECS, subsystému nebo prvku subsystému, která je schopna způsobit nebezpečný stav nebo stav, v němž není schopen plnit svou funkci
- **Bezpečná porucha –** porucha SRECS, subsystému nebo prvku subsystému, která není schopna způsobit nebezpečí
- **Odolnost proti vadám –** schopnost SRECS, subsystému nebo prvku subsystému pokračovat v plnění požadované funkce i za přítomnosti vad nebo chyb [4]

2 Postup návrhu dle ČSN EN 62061

Norma ČSN EN 62061 určuje požadavky a doporučení na návrh elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností (SRECS), které jsou určeny pro stroje. Je platná jak pro řídicí systémy použité jednotlivě, tak i v kombinaci pro zajištění bezpečného řízení stroje. Tato norma se týká pouze požadavků na funkční bezpečnost týkající se snížení rizika poranění nebo poškození zdraví osob v bezprostřední blízkosti stroje.

2.1 Riziková analýza

V první části návrhu funkcí pro snížení rizika je třeba zhodnotit stávající nebezpečí a provést rizikovou analýzu. Výsledkem této analýzy by měl nebo měly být faktory nebezpečnosti stroje. U jednoduchých systémů postačí metody jako je brainstorming nebo kontrolní seznam. U rozsáhlejších systémů je potřeba týmové spolupráce pro určení potenciálních zdrojů nebezpečí.

Účelem rizikové analýzy je určit, jestli je riziko, které je spjaté s vykonáváním dané činnosti, přijatelné nebo ne. Skládá se z několika kroků, jako jsou identifikace zdrojů rizika, seznam různých nebezpečných scénářů, odhad četností výskytu a následků těchto scénářů a hodnocení rizika, většinou porovnáním s určenými kritérii. Riziko lze hodnotit ve třech stupních:

- Zanedbatelné riziko
- Únosné riziko
- Neakceptovatelné riziko.

2.2 Specifikace požadavků na řídicí funkce související s bezpečností (SRCF)

Specifikace každé SRCF se musí skládat ze dvou částí. Specifikace funkčních požadavků a specifikace požadavků na integritu bezpečnosti. Aby mohly být tyto požadavky splněny, je potřeba využít následujících informací:

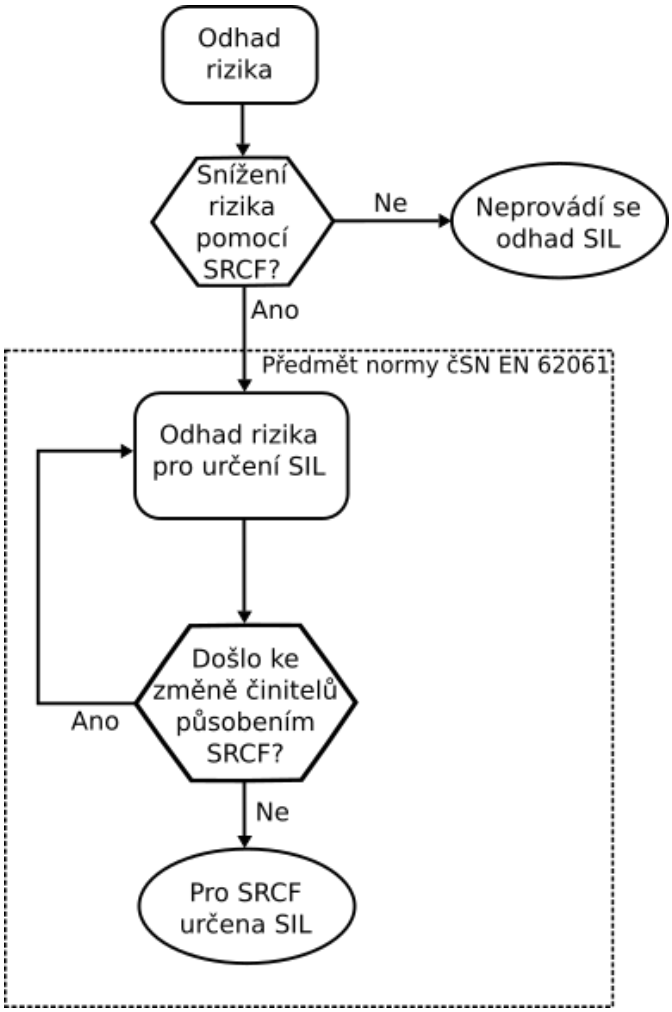
- výsledky rizikové analýzy stroje včetně všech bezpečnostních funkcí pro každé konkrétní nebezpečí
- pracovní charakteristiky stroje – pracovní režim, cykly, časové odezvy, prostředí.

2.2.1 Specifikace funkčních požadavků SRCF

Specifikace funkčních požadavků na SRCF popisuje všechny podrobnosti, které přicházejí v úvahu. Těmito požadavky jsou například pracovní režimy stroje, časové odezvy, popis každé SRCF, popis pracovního prostředí nebo počet provozních cyklů.

2.2.2 Specifikace požadované integrity bezpečnosti SRCF

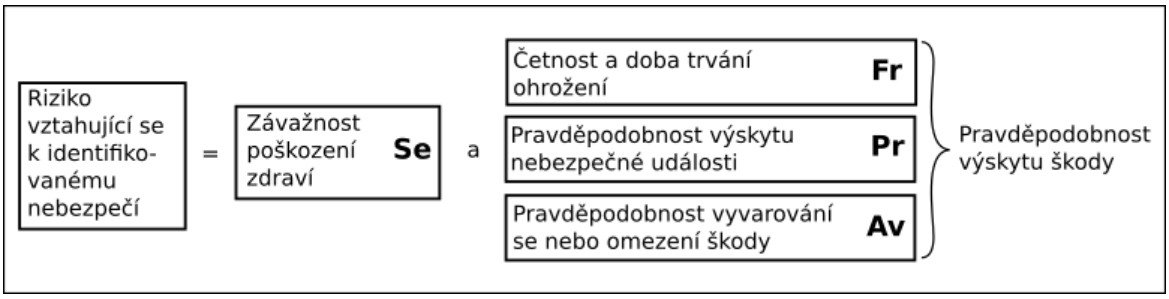
Pro řídicí funkce související s bezpečností SRECS by měli být požadavky integrity bezpečnosti určeny samostatně pro každé nebezpečí. Na Obr. 2 je ukázán příklad provedení hodnocení rizika při konkrétním nebezpečí, které se používá při odhadu požadavku na SIL pro funkce SRECS. Na konci tohoto procesu se odhadnutá SIL rovná požadované SIL pro řídicí funkce související s bezpečností.



Obr. 2 Sled činností při určování SIL [4]

2.2.3 Odhad rizika a přiřazení SIL

Je potřeba provést odhad rizika pro každé nebezpečí určením prvků rizika. Tyto prvky jsou znázorněny na Obr. 3.



Obr. 3 Prvky rizika [4]

Odhady těchto prvků rizika by měly být založeny na nejnepříznivějších podmínkách pro řídicí funkce související s bezpečností (SRCF). Ovšem pokud např. přichází v úvahu zranění s trvalými následky s mnohem nižší pravděpodobností než zranění s přechodnými následky, měly by být obě tyto situace posuzovány separátně.

2.2.3.1 Závažnost (Se)

Závažnost poškození zdraví se dá odhadnout dle zranění jako:

- zranění s přechodnými následky
- zranění s trvalými následky
- zranění smrtelné.

Je nutné zvolit příslušnou hodnotu závažnosti z Tab. 1 dle důsledků zranění, kde:

4 znamená smrtelné zranění, nebo zranění s trvalými následky, takže bude velmi obtížné pokračovat po uzdravení ve stejné práci, pokud to bude vůbec možné

3 znamená těžká zranění s trvalými následky, takovými, že po uzdravení bude možné pokračovat ve stejné práci. Může také zahrnovat závažná těžká zranění bez trvalých následků, jako jsou zlomené končetiny

2 znamená zranění s přechodnými následky, včetně závažných tržných ran, bodných ran a těžkých pohmožděnin, které vyžadují ošetření praktickým lékařem

1 znamená lehká zranění včetně škrábanců a lehkých pohmožděnin, které vyžadují ošetření na první pomoci [4].

Tab. 1 Třída závažnosti [4]

Následky	Závažnost (Se)
Trvalé: smrt, ztráta oka nebo paže	4
Trvalé: zlomená končetina, ztráta prstů	3
Přechodné: vyžadující ošetření praktickým lékařem	2
Přechodné: vyžadující ošetření na první pomoci	1

2.2.3.2 Četnost a doba ohrožení (Fr)

Pro určení úrovně ohrožení je třeba brát na zřetel dva základní předpoklady: Potřebu přístupu do nebezpečné zóny při všech režimech užití a povahu přístupu. Podle těchto dvou kritérií by mělo být možné odhadnout střední interval mezi ohroženími, a tak i střední četnost přístupu.

Také by mělo být možné předvídat dobu trvání ohrožení, která je delší než 10 minut. Pokud je doba trvání ohrožení kratší než 10 minut, může být hodnota snížena na nejbližší nižší úroveň. Ovšem to neplatí, pokud je četnost ohrožení menší či rovna jedné hodině. V takovém případě by se hodnota snižovat nikdy neměla. Jednotlivé četnosti a doby ohrožení jsou uvedeny v Tab. 2 [4].

Tab. 2 Třídy četnosti a doby trvání ohrožení (Fr) [4]

Četnost ohrožení	Četnost a doba trvání odrožení (Fr) pro t > 10 min
≤ 1 h	5
> 1 h až ≤ 1 den	5
> 1 den až ≤ 2 týdny	4
> 2 týdny až ≤ 1 rok	3
> 1 rok	2

2.2.3.3 Pravděpodobnost výskytu nebezpečné události (Pr)

Pravděpodobnost výskytu škody by se měla odhadovat nezávisle na ostatních prvcích Fr a Av. Jak už bylo řečeno, měl by být u každého parametru uvažován nejnepříznivější odhad, aby nebyla přidělena jiná SIL, než je potřeba. Tato pravděpodobnost může být odhadnuta při dodržení dvou základních kritérií. Prvním je předvídatelnost chování částí stroje souvisejících s nebezpečím při různých režimech použití. Druhým kritériem jsou předepsané nebo předvídatelné charakteristiky vzájemného působení osob a částí strojů. Zda působí na obsluhu

stres, nebo jestli bylo poskytnuto dostatek informací týkajících se nebezpečí. Jednotlivé třídy pravděpodobnosti jsou uvedeny v Tab. 3 [4].

Tab. 3 Třída pravděpodobnosti [4]

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

2.2.3.4 Pravděpodobnost vyvarování se nebo omezení škody (Av)

Tato pravděpodobnost může být odhadnuta z konstrukce stroje a jeho aplikace. To může pomoci předcházet nebo omezit škody vyplívající z nebezpečí. Těmi hledisky jsou:

- náhlý, rychlý nebo pomalý výskyt nebezpečné události
- možnost úniku z nebezpečné zóny
- povaha součástí nebo systému
- možnost rozpoznat nebezpečí.

Příslušný řádek pro pravděpodobnost vyvarování se nebo omezení škody (Av) je třeba zvolit z Tab. 4 [4].

Tab. 4 Třída pravděpodobnosti vyvarování se nebo omezení škody (Av) [4]

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

2.2.3.5 Třída pravděpodobnosti škody (Cl)

Pro každé konkrétní nebezpečí a každý stupeň závažnosti škody se v Tab. 5 sečtou body od prvků Fr, Pr a Av a jejich součet bude uveden ve sloupci Cl [4].

Tab. 5 Prvky použité pro určení třídy pravděpodobnosti škody (Cl) [4]

Číslo	Nebezpečí	Se	Fr	Pr	Av	Cl
1						
2						
3						
4						

2.2.3.6 Konečné určení SIL bezpečnostní funkce

V Tab. 6 určuje průsečík řádku závažnosti (Se) a sloupce (Cl) požadovanou SIL. Černá oblast tabulky značí přiřazenou SIL jako hodnotu pro danou SRCF. Světle šedá oblast je určena pro použití jiných opatření (OM). Pokud vyjde průsečík do bílé oblasti, není nutné zavádět žádné bezpečnostní funkce [4].

Tab. 6 Matice určení SIL [4]

Závažnost (Se)	Třída (Cl)				
	3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2
1				(OM)	SIL1

Pro normu ČSN EN 62061 se musí hodnota SIL převést na pravděpodobnost nebezpečných poruch za hodinu. Přepočet je uveden v Tab. 7.

Tab. 7 Hladina integrity bezpečnosti – cílové míry poruch pro SRCF [4]

Hladina integrity bezpečnosti	Pravděpodobnost nebezpečné poruchy za hodinu (PFH_D)
3	$\geq 10^{-8}$ až $< 10^{-7}$
2	$\geq 10^{-7}$ až $< 10^{-6}$
1	$\geq 10^{-6}$ až $< 10^{-5}$

2.3 Požadavky na elektrický řídicí systém související s bezpečností (SRECS)

Elektrický řídicí systém související s bezpečností musí být vybrán nebo navržen tak, aby mohl vyhovět jak specifikaci funkčních požadavků, tak i požadavkům na integritu bezpečnosti SRCF. Návrh SRECS, včetně veškeré hardwarové i softwarové architektury, ovládacích prvků, čidel nebo programovatelné elektroniky, musí splňovat požadavky:

- požadavky na integritu bezpečnosti
- požadavky na systematickou integritu bezpečnosti
- požadavky na chování SRECS při detekci poruchového stavu
- požadavky na návrh a vývoj softwaru souvisejícího s bezpečností.

Požadavky na integritu bezpečnosti byly popsány v předchozích kapitolách a návrh a vývoj softwaru není obsahem této práce. Proto jsou dále detailněji popsány pouze požadavky

na systematickou integritu bezpečnosti a na chování SRECS při detekci poruchového stavu.

Návrh dále musí počítat s lidskými schopnostmi včetně používání, které je logicky předvídatelné a musí vyhovovat také z hlediska činností operátorů nebo ostatních osob, které by na SRECS mohly působit. Všechna rozhraní pro obsluhu musí být pro uživatele vhodná a přizpůsobena pravděpodobné úrovni výcviku obsluhy, zvláště tam, kde obsluhu může zajišťovat osoba laická [4].

2.3.1 Požadavky na chování SRECS při detekci poruchového stavu

Pokud je v kterémkoliv subsystému, který má odolnost proti vadám hardwaru větší než nula, zjištěn nebezpečný poruchový stav, musí se vykonat předepsané funkce reagující na tento poruchový stav. Odolnost proti vadám hardwaru N znamená, že N + 1 poruchových stavů by mohlo způsobit ztrátu SRCF. Může být dovoleno odpojení poškozené části subsystému, ale provoz stroje musí být i nadále bezpečný, zatímco probíhá oprava porušené části. Tato oprava však musí být provedena během předem odhadnuté doby, která byla použita při výpočtu pravděpodobnosti náhodné poruchy hardwaru. Pokud se tak nestane, musí být spuštěna druhá funkce, aby se udržel bezpečný stav stroje.

Pokud má subsystém nulovou odolnost proti vadám hardwaru a je zde tedy nutné využít diagnostických funkcí pro dosažení požadované pravděpodobnosti nebezpečných náhodných poruch hardwaru, musí být detekce poruchového stavu a daná reakce na tento poruchový stav provedena ještě předtím, než se nebezpečná situace vůbec může objevit [4].

2.3.2 Požadavky na řízení systematických poruch

a) **Odpojení od zdroje** – SRECS musí být navržen tak, aby při ztrátě elektrického napájení byl dosažen a udržován bezpečný stav stroje
b) **Přechodné poruchy** – SRECS musí mít opatření proti řízení účinků přechodných poruch některých subsystémů jako je kolísání napětí. Jedná se o krátkodobé přerušení, nebo poklesy napětí. Tyto poruchy nesmí mít vliv na bezpečnost systému. Dále pak účinky elektromagnetického rušení vnějšího prostředí taktéž nesmí vést k nebezpečí [4].

2.4 Možnosti realizace subsystémů

Cílem normy ČSN EN 62061 je realizace takových subsystémů, které budou plnit všechny bezpečnostní požadavky a uvažuje dva postupy řešení:

a) Volba zařízení, které dostatečně plní požadavky tohoto subsystému. To znamená, že musí plnit bezpečnostní požadavky každého přiřazeného funkčního bloku a požadavky této normy.
b) Návrh a vývoj subsystému kombinací prvků funkčních bloků, včetně jejich uspořádání a vzájemného působení [4].

2.4.1 Požadavky na realizaci subsystémů

Pro každý subsystém musí být známo několik následujících informací:

a) funkční specifikace těch funkcí a rozhraní subsystémů, které mohou být použity pro SRCF
b) předpokládané intenzity poruch deklarované ve všech režimech, které by mohly způsobit nebezpečnou poruchu SRECS
c) omezení subsystému vlivem:
    - podmínek prostředí a provozních podmínek, které by měly být sledovány tak, aby byla udržena platnost předpokládaných intenzit poruch způsobených náhodnou poruchou hardwaru
    - doby života subsystému, která by neměla být překročena tak, aby byla udržena platnost předpokládaných intenzit poruch způsobených náhodnou poruchou hardwaru
d) požadavky na zkoušky a údržbu
e) diagnostické pokrytí a interval diagnostické zkoušky
f) všechny doplňující informace, které jsou potřebné pro odvození střední doby do obnovy po zjištění poruchového stavu diagnostikou
g) SILCL (dosažitelná mez SIL) v závislosti na omezení architektury nebo:
    - všechny informace, které jsou potřebné pro odvození podílu bezpečných poruch (SFF) subsystému použitého v SERCS
    - odolnost proti vadám hardwaru subsystému
h) všechna aplikační omezení subsystému, které by měly být sledovány z důvodu předcházení systematickým poruchám
i) nejvyšší úroveň integrity bezpečnosti, kterou lze pro SRCF uplatňovat v subsystému založenou na:

- opatřeních a postupech použitých pro zabránění proniknutí systematických vad ve fázi návrhu a realizace subsystému hardwaru a softwaru
- konstrukčních opatřeních, které zajistí, aby subsystém byl odolný vůči systematickým vadám

j) všechny informace, které jsou vyžadovány pro identifikaci konfigurace hardwaru a softwaru subsystému tak, aby byl umožněn management konfigurace SRECS [4].

2.4.2 Návrh a vývoj subsystémů

Nejdůležitějším cílem na návrh subsystému je splnění všech bezpečnostních požadavků přiřazených funkčních bloků. Dalším cílem je vytvořit takovou architekturu spolupracujících prvků subsystému, aby plnily jak funkční požadavky, tak požadavky na integritu bezpečnosti všech bloků přiřazených v subsystému. Subsystém musí splňovat následující požadavky:

a) požadavky na integritu bezpečnosti hardwaru zahrnující:
   - omezení architektury na integritu bezpečnosti hardwaru
   - požadavky týkající se pravděpodobnosti nebezpečných náhodných poruch hardwaru

b) požadavky na systematickou integritu bezpečnosti zahrnující:
   - požadavky na předcházení poruchám a požadavky na řízení systematických poruch
   - prokázání skutečnosti, že zařízení je „ověřeno v provozu“

c) požadavky na chování subsystému týkající se detekce poruchového stavu včetně reakce na tyto poruchové stavy [4].

2.4.3 Omezení architektury na integritu bezpečnosti hardwaru subsystémů

Nejvyšší úroveň integrity hardwaru, kterou je možné pro danou SRCF v souvislosti s integritou bezpečnosti hardwaru uplatňovat, je omezena odolností proti vadám hardwaru a podílem bezpečných poruch subsystémů, které SRCF realizují. Předepsaná nejvyšší úroveň integrity bezpečnosti, kterou lze pro SRCF uplatňovat při respektování odolnosti proti vadám hardwaru a podílu bezpečných poruch, je uvedena v Tab. 8. Toto omezení architektury musí být uplatňováno v každém subsystému a musí na ně brán ohled, přičemž:

a) Odolnost proti vadám hardwaru N znamená, že N + 1 poruchových stavů by mohlo způsobit ztrátu SRCF. Nerespektují se zde další opatření, která by mohla účinky poruchových stavů řídit, jako je diagnostika.
b) Pokud jedna vada vede přímo ke vzniku následných vad, považují se tyto vady za vadu jednu.
c) Při určování odolnosti proti vadám hardwaru mohou být určité poruchové stavy vyloučeny, a to ze předpokladu, že pravděpodobnost jejich vzniku je ve vztahu k požadavkům integrity bezpečnosti subsystému velmi malá [4].

Tab. 8 Omezení architektury na subsystém [4]

Podíl bezpečných poruch	Odolnost proti vadám hardwaru		
	0	1	2
< 60 %	není povoleno	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIl2	SIL3	SIL3
≥ 99 %	SIL3	SIL3	SIL3

2.4.4 Požadavky na pravděpodobnost náhodných poruch hardwaru subsystému

Hodnota pravděpodobnosti nebezpečné náhodné poruchy hardwaru musí být menší nebo se rovnat cílové hodnotě předepsané při specifikaci bezpečnostních požadavků na daný subsystém. Proto musí být odhadnuta pravděpodobnost nebezpečné poruchy každého subsystému a musí respektovat:

a) architekturu subsystému ve vztahu k funkčním blokům
b) intenzitu poruch každého prvku subsystému, které by mohly způsobit nebezpečnou poruchu systému a jsou zjištěny diagnostickými zkouškami
c) intenzitu poruch každého prvku subsystému, které by mohly způsobit nebezpečnou poruchu systému, které nejsou zjištěny diagnostickými zkouškami
d) citlivost systému na společné poruchy
e) diagnostické pokrytí při provádění diagnostických testů
f) doby oprav poruchových stavů

Pokud je v subsystému prvek, který má pravděpodobnost poruch udávanou v závislosti na počtu provozních cyklů, musí se tyto hodnoty přepočítat na předepsaný počet pracovních cyklů dané SFRC v závislosti na čase. U subsystémů s větší, než nulovou

odolností proti vadám hardwaru musí být diagnostický interval nastaven tak, aby byla možnost splnit požadavky na pravděpodobnost náhodných poruch hardwaru [4].

2.4.5 Postup odhadu nebezpečné náhodné poruchy hardwaru subsystému

Zjednodušený postup odhadu pravděpodobnosti nebezpečné náhodné poruchy hardwaru subsystému je použitelný pro několik základních architektur a uvádí vzorce, které jsou použitelné buď pro jednoduché nebo složité prvky subsystému. Tyto vzorce představují zjednodušenou analýzu spolehlivosti a slouží pro odhady v souvislosti s bezpečností. Základním předpokladem použití těchto vzorců je podmínka:

$$1 \gg \lambda \cdot T_1$$

T_1 je interval kontrolní zkoušky nebo doba života a λ je intenzita poruch. Intenzitu poruch λ lze spočítat:

$$\lambda = {}^{1}/_{MTTF}$$

MTTF je střední doba do poruchy. Další možností je vypočítat intenzitu poruch λ jako součet λ_S (intenzita bezpečných poruch) a λ_D (intenzita nebezpečných poruch), tedy:

$$\lambda = \lambda_S + \lambda_D$$

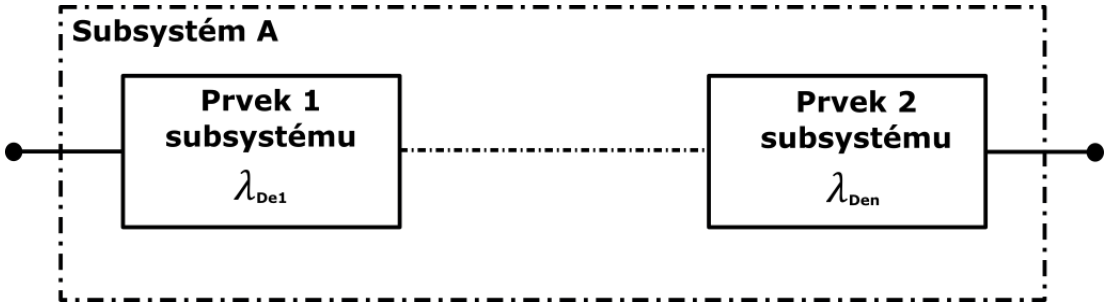
Dalšími parametry nutnými pro výpočet intenzity poruch různých částí systému je T_1, což je interval kontrolní zkoušky nebo doba života (podle toho, co je kratší doba) a citlivost na společné poruchy β.

Norma ČSN EN 62061 rozlišuje několik základních architektur, z nichž byly využity a popsány v této diplomové práci pouze tyto dvě:

a) Základní architektura subsystému A

Architektura subsystému A má nulovou odolnost proti vadám a neobsahuje diagnostickou funkci. Tedy každá nebezpečná porucha kteréhokoliv prvku způsobí poruchu bezpečnostní funkce SRCF. Pravděpodobnost nebezpečné poruchy u architektury A je součtem pravděpodobností nebezpečných poruch všech prvků subsystému:

$$\lambda_{DssA} = \lambda_{De1} + \cdots + \lambda_{Den}$$

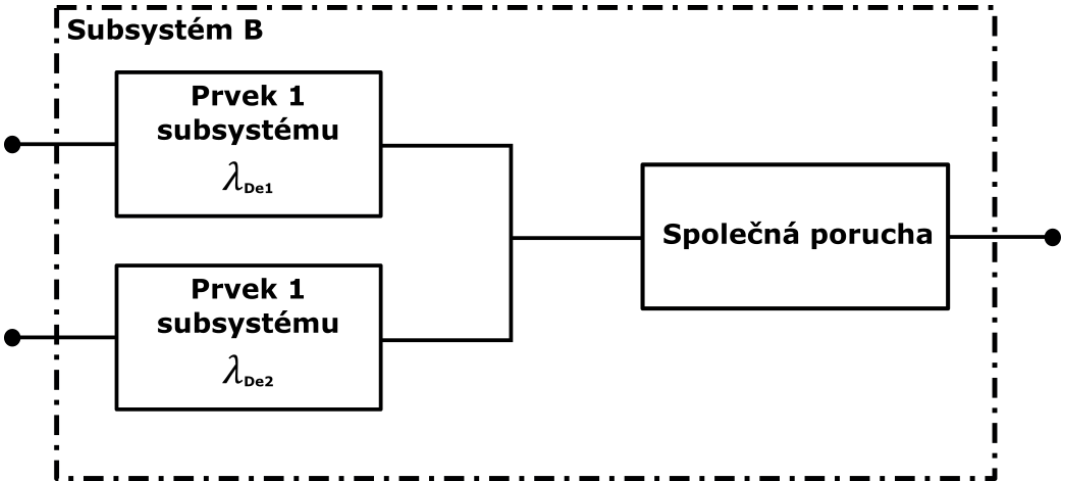


Obr. 4 Logické znázornění subsystému A [4]

b) Základní architektura subsystému B

Tato základní architektura také neobsahuje diagnostickou funkci, ovšem má odolnost proti jedné vadě hardwaru, a tak jednotlivá porucha kteréhokoliv prvku subsystému nezpůsobí ztrátu SRCF. Muselo by dojít k poruše více než jednoho prvku, aby nastala porucha SRCF. Pravděpodobnost nebezpečné poruchy u architektury B je dána vzorcem:

$$\lambda_{DssB} = (1-\beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$$



Obr. 5 Logické znázornění subsystému B [4]

2.5 Realizace diagnostických funkcí

Diagnostické funkce jsou nutné pro splnění požadavků na omezení architektury a pravděpodobnosti nebezpečné náhodné poruchy hardwaru. Musí jimi být vybaven každý subsystém. Diagnostické funkce se považují za funkce samostatné a mohou mít odlišnou strukturu od SRCF. Mohou být plněny třemi různými způsoby:

- stejným subsystémem vyžadujícím diagnostiku

- jiným subsystémem SRECS
- subsystémy SRECS, které nevykonávají SRCF

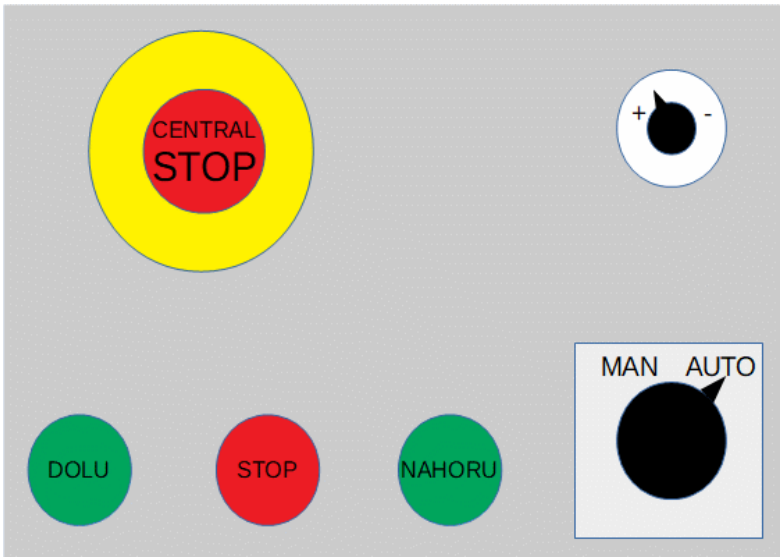
I diagnostické funkce musí vyhovovat požadavkům na předcházení systematickým poruchám a požadavkům na řízení systematických poruch. Také je třeba aby byly započteny do pravděpodobnosti při odhadu nebezpečné poruchy SRCF [4].

3 Návrh řídicího systému

V této kapitole bude popsán návrh automatického systému pro řízení lisu chmele dle postupů normy ČSN EN 62061, jejíž obecná struktura je popsána v předchozí kapitole.

3.1 Současný stav lisu

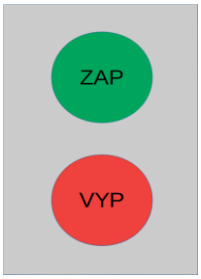
Čerstvě usušený chmel je potřeba slisovat do pytlů (hranolů). K tomu slouží lis chmele. Jedná se o jednoduchý lis poháněný asynchronním elektromotorem. Tento elektromotor je k lisu připojen pomocí řetězu a řetězových kol. Pohyb lisu je ovládán z jednoduchého panelu pomocí tlačítek, jehož rozvržení je na Obr. 6. Na panelu jsou čtyři tlačítka, jeden přepínač a otočný potenciometr. Jedno z tlačítek je „CENTAL STOP“, které v případě nebezpečí odpojí celý stroj od přívodu energie. Zbylá tři tlačítka slouží pro pohyb lisu, směrem dolů, nahoru a pro zastavení lisu. Dvoupolohový přepínač je zde pro změnu mezi tzv. manuálním a automatickým režimem. V manuálním režimu je potřeba pro pohyb lisu tlačítko držet, po jeho uvolnění se lis zastaví. Automatický režim využívá proudového relé, které po sepnutí tlačítka pro chod lisu směrem dolů slouží jako přídržný kontakt. Při zatížení lisu naroste proud tímto relé, které sepne. Sepnutím tohoto relé dojde k rozepnutí stykače pro chod dolů, a naopak k sepnutí druhého stykače, který slouží pro chod lisu nahoru. Lisovací tlak je tedy závislý na velikosti proudu, při kterém sepne kontakt proudového relé. Tento proud je nastavitelný pomocí otočného potenciometru na předním panelu.



Obr. 6 Přední ovládací panel

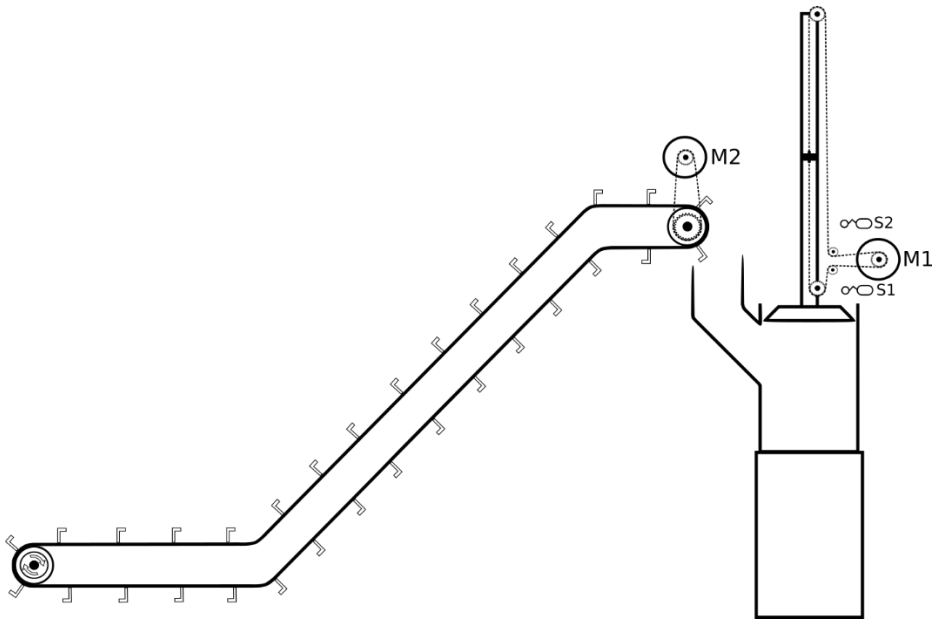
3.1.1 Ovládání dopravníku

Pro plnění lisu chmelem slouží kapsový dopravník. Ten je ovládaný dvěma tlačítky podle Obr. 7 umístěnými vedle hlavního panelu přímo na lisu. Jedná se o tlačítka „ZAP“ a „VYP“. Pro rozběh nebo zastavení dopravníku stačí jedno z tlačítek stlačit jen na krátký okamžik. Tyto dvě tlačítka ovládají stykač. Jelikož je kapsový dopravník součástí sušárny chmele, je tento stykač umístěn v hlavním rozvaděči celé sušárny. Při stisknutí tlačítka „ZAP“ se sepne přídržný kontakt stykače, který drží stykač sepnutý až do doby, kdy je tlačítkem „VYP“ rozepnut a tím se dopravník zastaví.



Obr. 7 Tlačítka pro ovládání dopravníku chmele

Lis pracuje v tzv. pracovním cyklu. Tento cyklus slouží pro výrobu finálního produktu ze sušeného chmelu, kterým je pytlový hranol o rozměrech 60x60x120 centimetrů a hmotností 50 až 55 kilogramů. Pracovní cyklus tedy zahrnuje několikanásobné nasypání a slisování, tak aby byl finální produkt v požadované kvalitě. Celá sestava lisu chmele a pásového dopravníku je ukázána na Obr. 8.



Obr. 8 Schematický nákres sestavy lisu a pásového dopravníku

3.1.2 Lisovací cyklus

Do lisu se vloží prázdný pytel, který je přímo určen pro použití v tomto typu lisu chmele. Poté se tlačítkem „ZAP“ rozběhne kapsový dopravník, který dopravuje chmel ze sušárny přímo do lisu. Když je hladina chmele v lisu na správné úrovni, tak se dopravník zastaví tlačítkem „VYP“. Před prvním spuštěním lisu je potřeba se ujistit, zda je přepínač v poloze „AUTO“. Samotný lis se uvede do pohybu stisknutím tlačítka „DOLŮ“. Jelikož je aktivován automatický režim, tak proudové relé po dosažení nastaveného proudu, který odpovídá lisovacímu tlaku, obrátí směr chodu lisu, který se vrátí do výchozí horní polohy. V ten moment se opět spustí celý cyklus znovu. Výjimkou je slisování po posledním nasypání, kdy je potřeba aby lis nevyjel zpět nahoru, ale zůstal v dolní pozici. Proto probíhá poslední slisování v manuálním režimu a je tedy potřeba držet tlačítko „DOLU“ až do doby, kdy je chmel v lisu stlačen. Je to z důvodu výměny pytle, kdy je potřeba pytel zajistit třemi jehlicemi, které se zapichují hned pod beran lisu. Z přední strany se dávají dvě jehlice, z boku jedna. Poté, co jsou všechny jehlice na svém místě, přepne se přepínač opět na automatický režim a stisknutím „NAHORU“ lis vyjede nahoru. Pytel se poté vytáhne bokem a vloží se pytel prázdný a celý cyklus se opakuje. Celý cyklus se opakuje 7-krát až 10-krát, aby měl hranol požadované rozměry i váhu.

3.2 Funkce s automatickým systémem

Funkce lisu se zařízením pro automatickou činnost by se prakticky neměla lišit oproti funkci při využití lidské obsluhy, která pomocí tlačítek lis ovládá. Pro snímání výšky hladiny chmele v lisu musí být přidáno optické čidlo, které po dosažení nastavené hladiny sepne. Dále bude lis doplněn o koncový spínač, který bude informovat o poloze beranu lisu. Poslední informací, nutnou pro funkci systému, dává proudové relé. To má dvě skupiny přepínacích kontaktů. Jedna skupina je již využita, ovšem druhá je volná a na té první nezávislá. Proto bude tato druhá skupina kontaktů využita pro automatický systém.

Motor lisu byl při manuální obsluze spínán pomocí stykačů, jedním pro každý směr. Požadavkem provozovatele bylo, aby tyto stykače byly zachovány a byla tak i nadále možná manuální obsluha. Stykače tedy budou zachovány, ale nebudou už spínány tlačítky, ale pomocí několika relé. Pomocí relé bude spínán i kapsový dopravník, kde budou relé sloužit také jako náhrada tlačítek.

S použitím automatického systému pro lisování chmele se celý cyklus po nasazení nového pytle spustí stisknutím tlačítka „START“. Po stisknutí tohoto tlačítka se zkontroluje,

zda je beran lisu v horní poloze a optické čidlo volné. Pokud ano, tak je zapnut pásový dopravník. Ten začne plnit lis chmelem až do doby, kdy je zakryt optický senzor, umístěný na straně lisu. Zakrytý senzor dá signál do řídicího zařízení, a to zastaví plnění lisu. Když se dopravník zastaví, je sepnut lis směrem dolu. Jede dolů až do té doby, kdy sepne proudové relé. To dá informaci o sepnutí řídicí jednotce, která zastaví lis směrem dolů a uvede ho do pohybu směrem zpět nahoru. Když lis vyjede do horní koncové polohy, která je kontrolována koncovým spínačem, opět se zapne pásový dopravník a cyklus se opakuje.

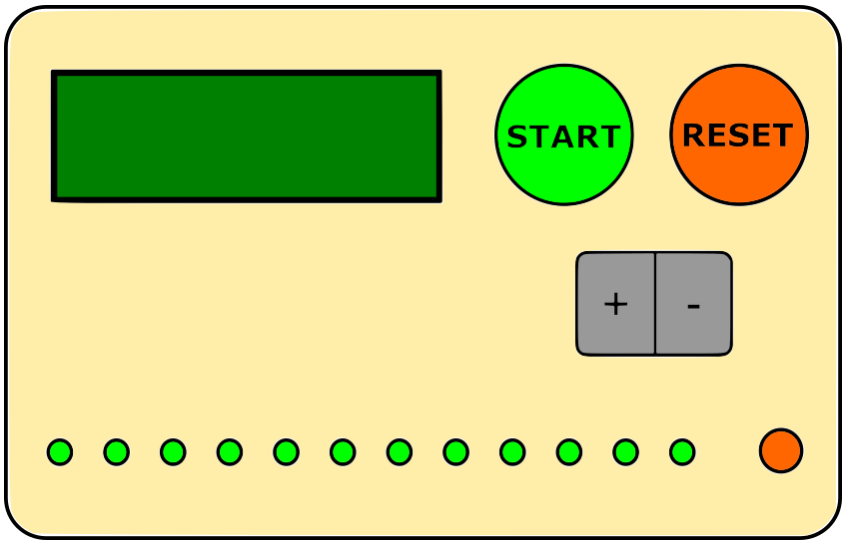
Jediný rozdíl v tomto cyklu je, pokud se jedná o poslední plnění pytle. Zapne se dopravník po naplnění lisu a poté co je lis dostatečně naplněn, sepne se lis směrem dolů. V těchto úkonech není oproti předešlým cyklům žádný rozdíl. Rozdíl je až v tom, že po sepnutí proudového relé v dolní poloze lisu se stroj pouze zastaví a beran lisu v této poloze zůstane. Poté se dveře lisu otevřou, speciálními jehlicemi se pytel zajistí. Když je pytel v lisu zajištěn jehlicemi, stiskne se druhé tlačítko na panelu - „RESET“ pro návrat lisu do výchozí polohy. Stávající pytel se vyjme a nahradí novým. Dveře lisu se uzavřou a stisknutím tlačítka „START“ se spustí cyklus pro další pytel.

3.2.1 Detailní popis zařízení

Pro ovládání bude systém vybaven několika tlačítky. Pro spuštění lisovacího cyklu, pro přerušení cyklu a pro nastavení příslušného počtu lisovacích cyklů.

Zařízení samozřejmě bude mít i vizualizační a ovládací prvky. Nejdůležitějším zobrazovacím prvkem bude displej, kde se budou zobrazovat prakticky všechny zásadní informace o stavu lisu, lisovaného hranolu nebo také nastavený počet lisování. Dalším vizualizačním prvkem je skupina zelených luminiscenčních diod. Těch bude dvanáct. To je nejvyšší možný nastavitelný počet lisování při jednom cyklu, tedy dvanáct. Jednotlivé led diody se budou rozsvěcet s každým průběhem lisovacího cyklu. Pokud tedy bude např. hotovo pět lisovacích cyklů, bude svíti prvních pět led diod. Na panelu bude kromě těchto zelených diod také jedna dioda oranžová. Ta bude mít upozorňovací význam a bude vizualizovat to, že je cyklus už hotov nebo byl přerušen. Posledním vizualizačním prvkem je piezoelektrický reproduktor, který bude fungovat jako upozornění pro obsluhu, že lisovací cyklus je již hotový. Celý řídicí panel je ukázán na Obr. 9.

Systém bude obsahovat kromě výše uvedených funkčních a vizualizačních prvků také jeden prvek jen informativní, který nebude mít na chod zařízení sebemenší vliv. Tím prvkem je digitální čidlo teploty. To bude měřit teplotu uvnitř rozvaděče se všemi prvky a tuto teplotu zobrazovat na displeji.



Obr. 9 Ovládací panel automatického systému

3.3 Riziková analýza

Přestože je lis chmele a jeho řízení považován za jednoduchý systém, bude k němu pro fázi detekce rizik přihlíženo jako k zařízení složitějšímu. Stávající nebezpečí budou určeny za pomoci dvou odborníků, kteří se specializují mino jiné i na zpracování chmele.

Při zjišťování rizik lisu a pásového dopravníku bylo k těmto zařízením přistupováno jako k sestavě. I když se jedná o dva stroje, budou řízeny jedním řídicím systémem a z hlediska bezpečnosti je k něm nutné přistupovat jako k celku.

3.3.1 Bezpečnostní funkce

Na základě rizikové analýzy byla určena jediná bezpečnostní funkce:

- ***při otevřených dveřích se nesmí beran lisu pohybovat.***

Tato funkce musí platit jak při začátku cyklu, kdy může dojít ke špatnému dovření dveří, tak v průběhu lisovacího cyklu. Jedinou výjimkou je poslední lisovací cyklus, kdy je potřeba, aby lis vyjel do horní polohy při otevřených dveřích, aby byla umožněna výměna pytle.

3.4 Specifikace funkčních požadavků SRCF

Pro lis chmele byla stanovena jediná bezpečnostní funkce a to, že se při otevřených dveřích nesmí beran lisu pohybovat. Jelikož je právě pohybující se beran lisu nejnebezpečnější částí stroje a může způsobit značná zranění, je potřeba, aby se zastavil v co nejkratším čase. Motor, který lisem pohybuje, je vybaven stejnosměrnou brzdou, a proto pro zastavení postačí odpojení napájecího napětí motoru.

Je tedy potřeba snímat polohu dveří lisu. Výstup snímače následně vyhodnotit logickou částí obvodu tak, aby se lis při otevření dveří téměř okamžitě zastavil.

Napětí je k motoru připínáno pomocí stykačů. Součástí zadání byl požadavek, aby stykače i nadále zůstaly a bylo možné lis ovládat i manuálně, ovšem do návrhu SRECS nebudou zahrnuty. V rámci SRCF bude tedy motor ovládán skupinou relé.

3.5 Přiřazení SIL bezpečnostní funkci

Dalším krokem je přiřazení úrovně integrity bezpečnosti (SIL) pro každou bezpečnostní funkci. Jelikož bylo zjištěno jediné riziko, pro které je potřeba vytvořit bezpečnostní funkci, bude SIL přiřazována jen této jediné bezpečnostní funkci.

3.5.1 Závažnost (Se)

Určení závažnosti i ostatních parametrů návrhu SIL bylo určeno z předchozí zkušenosti se zařízením pro lisování chmele včetně jeho obsluhy.

Nejnebezpečnější částí lisu chmele je jednoznačně ta část, která se pohybuje, tedy beran lisu. Pokud budou dveře lisu otevřeny, je poměrně jednoduché strčit ruku na nesprávné místo. Lis, který má vůči stavbě lidského těla velkou sílu, může danou část těla buď velmi silně pohmoždit nebo dokonce zlomit. Na druhou stranu tento pohyb není tak nebezpečný, aby byla způsobena ztráta končetiny, nebo dokonce usmrcení. Proto volím třídu závažnosti (Se) 3.

3.5.2 Četnost a doba ohrožení (Fr)

Dle zkušenosti s obsluhou a činností zařízení pro lisování chmele byla určena četnost a doba trvání ohrožení.

Obsluha lisu musí být v blízkosti lisu téměř po celou dobu jeho používání. Vytvoření

jednoho slisovaného pytle chmele trvá průměrně 15 minut, a to je tedy četnost ohrožení. Samotný pohyb části lisu se děje několikrát během lisovacího cyklu, vždy mezi jednotlivými nasypáními chmele. Jednotlivý pohyb pak netrvá déle než minutu. Doba trvání ohrožení je tedy vždy menší než 10 minut. Z Tab. 2 tedy vyplývá, že třída četnosti a doby trvání ohrožení (Fr) pro lis chmelu je 5.

3.5.3 Pravděpodobnost výskytu nebezpečné události (Pr)

V normě ČSN EN 62061 je uvedeno, že pravděpodobnost vzniku nebezpečné události „Velmi vysoká“ by měla být zvolena při respektování omezení při normální výrobě a pokud jsou uvažovány nejnepříznivější podmínky. A pokud by měla být zvolena nižší hladina pravděpodobnosti, musí existovat důvody, které příznivě na tuto pravděpodobnost působí.

Pro určení byly uvažovány pouze dvě polehčující okolnosti. Jednou je to, že pohybující se části lisu jsou po většinu procesu chráněny alespoň nasazeným pytlem a druhá že místo, kterým se k pohybující časti lisu při běžné obsluze dostat je poměrně malé a není jednoduché umístit do tohoto místa jakoukoliv část těla. Proto byla zvolena pravděpodobnost výskytu jako „Možná“, tedy třída 3.

3.5.4 Pravděpodobnost vyvarování se nebo omezení škody (Av)

Lis chmele je stroj, který má okolo sebe poměrně velké volné prostranství a možnost úniku tedy není problémem. Nebezpečí hrozí, když by nebyla vrata lisu úplně zavřena a při jeho spuštění by se tlakem lisu mohla otevřít a způsobit nějakou škodu, jak na materiálu, tak i na lidském zdraví. Ostatní případná nebezpečí jsou lehce rozpoznatelná a pro byla zvolena pravděpodobnost vyvarování se nebo omezení škody jako „Možné za určitých podmínek“, tedy třída 3.

3.5.5 Konečné určení SIL

Pro případ lisu chmele je Se = 3 a Cl = 11 jak je ukázáno v Tab. 9. Pro bezpečnostní funkci SRCF je tedy z Tab. 6 přiřazena hodnota SIL 2. Hladině integrity bezpečnosti SIL2 odpovídá dle Tab. 7 pro normu ČSN EN 62061 pravděpodobnost nebezpečné náhodné poruchy za hodinu v rozmezí 10^{-7} až < 10^{-6}.

Tab. 9 Prvky použité pro určení třídy pravděpodobnosti škody (Cl)

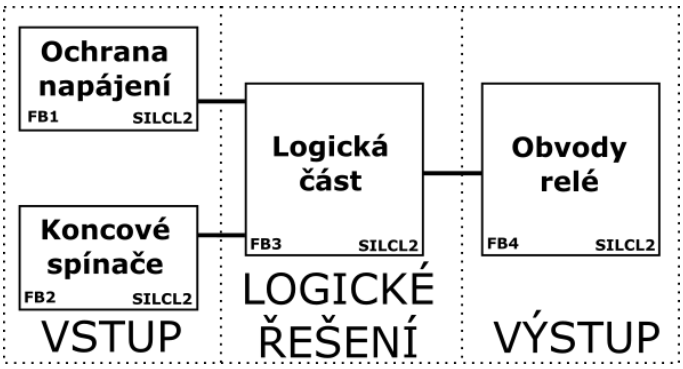
Číslo	Nebezpečí	Se	Fr	Pr	Av	Cl
1	*při otevřených dveřích se nesmí beran lisu pohybovat*	3	5	3	3	11

3.6 Dekomponování SRCF

Norma ČSN EN 62061 určuje metodiku, ve které jsou požadavky integrity bezpečnosti řídicích funkcí souvisejících s bezpečností a funkční požadavky dekomponovány na bloky vykonávající dílčí funkce. Toto rozdělení je důležité pro začlenění struktury funkční bezpečnosti do oblasti strojních zařízení. Na Obr. 10 je ukázána základní dekompozice systému, která je použita pro každou úroveň začleňování návrhu SRECS při pozdější instalaci stroje. Celý systém je rozdělen do tří základních subsystémů. Tyto subsystémy se pak dále skládají z jednotlivých prvků subsystému. V mém případě se systém skládá ze čtyř subsystémů. Kromě výše uvedených, je zde navíc subsystém zajišťující kontrolu napájecího napětí, jak je vidět z Obr. 11.

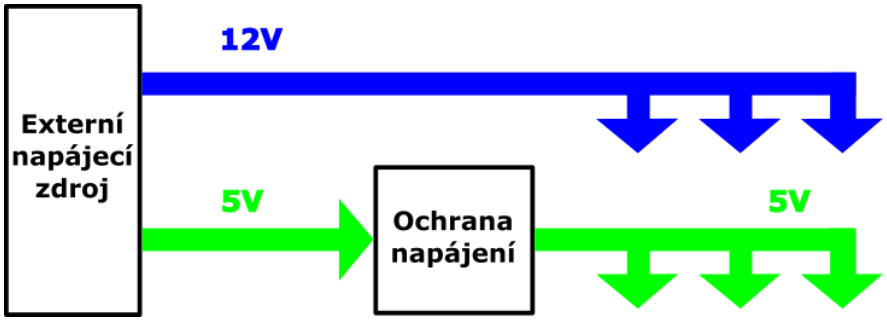
Obr. 10 Dekompozice funkcí SRECS

Bezpečnostní požadavky na každý funkční blok jsou odvozeny ze specifikace samotné bezpečnostní funkce. Přičemž prvek, nebo prvky každého funkčního bloku musí mít alespoň stejnou hodnotu SIL jako je hodnota celé SRCF. Jelikož má bezpečnostní funkce zastavení beranu lisu při otevřených dveří SIL 2, musí mít každý funkční blok systému minimálně hodnotu SIL 2.



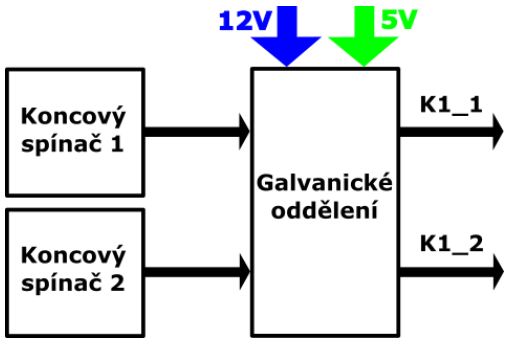
Obr. 11 Dekompozice systému do funkčních bloků

Funkční blok ochrany napájení slouží pro omezení přepětí. Do tohoto bloku budou vstupovat dvě úrovně napájení z dvou oddělených spínaných průmyslových zdrojů. Úrovně napětí budou 5 V pro napájení mikroprocesoru a 12 V pro koncové spínače a relé. Země těchto dvou úrovní budou také vedeny separátně. Jak je vidět na Obr. 12, napětí 12 V tímto blokem pouze prochází, protože jeho výpadek ani přepětí nevyvolají nebezpečnou událost. Úroveň napětí 5 V zde bude ochráněna proti přepětí, tak aby nedošlo k poškození mikroprocesoru. Podpětí této úrovně není nebezpečné, a proto v tomto bloku není řešeno.



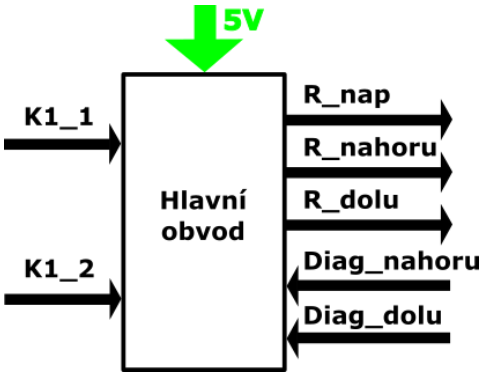
Obr. 12 Blokové schéma subsystému pro ochranu napájecího napětí

Blok koncových spínačů slouží pro galvanické oddělení signálu mezi koncovými spínači a samotným mikroprocesorem. Oddělení je nutné hlavně kvůli tomu, že koncové spínače budou připojeny na napětí 12 V a mikroprocesor má maximální vstupní napětí na A/D převodník 5,5 V. Dalším důvodem je, že po oddělení 12 V napájecí větve nebude možné, aby do mikroprocesoru pronikaly rušivé proudy. Blokové schéma je na Obr. 13.



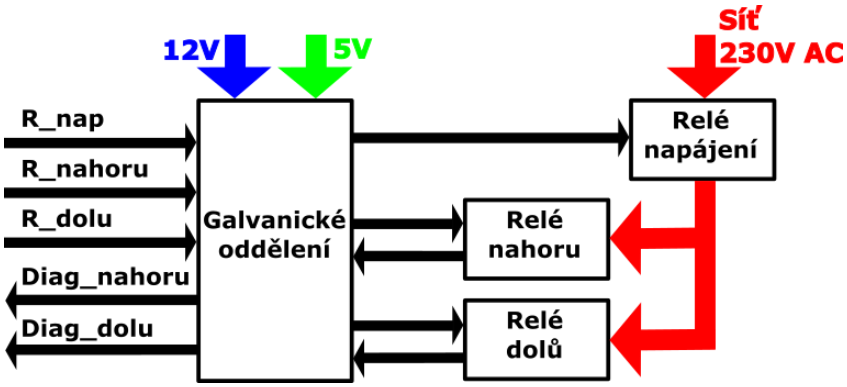
Obr. 13 Blokové schéma subsystému vstupních obvodů

Dalším funkčním blokem je mikroprocesor. Ten bude v rámci funkčního bloku obklopen jen několika pull-down rezistory, blokovacími a filtračním kondenzátorem, jednoduchým programovacím konektorem a resetovacím tlačítkem. Samotný mikroprocesor bude nejdůležitějším, a i nejsložitějším prvkem celého SRECS. Vstupní a výstupní signály tohoto bloku jsou uvedeny na Obr. 14.



Obr. 14 Blokové schéma subsystému hlavní obvod

Posledním blokem jsou obvody obsahující několik relé. Ty budou sloužit jak pro ovládání lisu nahoru a dolů, tak pro vykonávání bezpečnostní funkce, tedy odpojení od napájecího napětí. Pro účel odpojení od napájecího napětí 230 V bude v tomto bloku samostatně určené relé, jak je patrné z Obr. 15. Relé pro ovládání pohybu lisu budou vybaveny další skupinou kontaktů pro zavedení diagnostické funkce.



Obr. 15 Blokové schéma subsystému výstupních obvodů (relé)

3.7 Popis jednotlivých subsystémů SRECS

V této kapitole budou popsány veškeré subsystémy systému souvisejícího s bezpečností. Součástí budou i veškeré požadavky na tyto subsystémy jak z hlediska omezení architektury, tak i z cílové míry nebezpečných poruch.

3.7.1 Subsystém – Ochrana napájení

Tento subsystém, jak už název napovídá, slouží pro kontrolu napájecího napětí, a tedy pro ochranu následně připojených dalších součástí systému, které jsou citlivé na velikost napájecího napětí. Tento subsystém musí mít s ohledem na bezpečnost tyto vlastnosti:

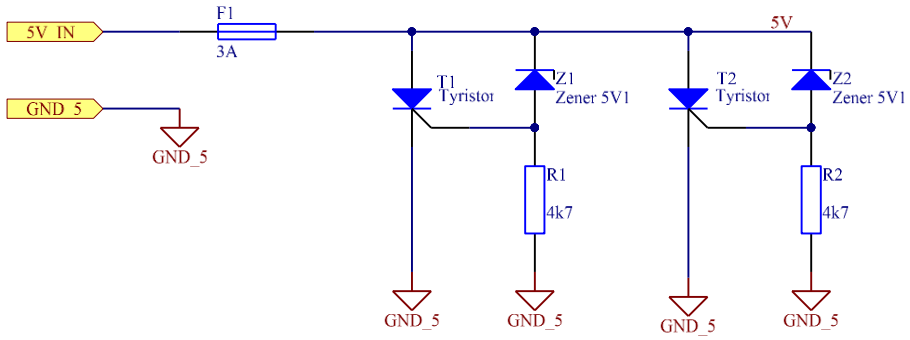
- Architektura subsystému **typ A**
- Odolnost proti vadám hardwaru **0**
- Podíl bezpečných poruch **90 % až 99 %**
- Úroveň integrity bezpečnosti **SIL 2**

3.7.1.1 Funkce

Jak už bylo napsána v předchozím odstavci, tento subsystém slouží pro kontrolu napájecího napětí. Konkrétně jen větve s napětím 5 V.

Velikost napětí je snímána pomocí Zenerovi diody s prahovým napětím 5,1 V. Po překročení této úrovně se dioda stane propustnou a sepne tyristor. Tyristor tím způsobí zkrat, dojde k přepájení tavné pojistky o jmenovitém proudu 3 A a tím k odpojení 5 V napájení. Pro omezení maximálního procházejícího proudu Zenerovo diodou je obvod doplněn rezistorem o velikosti 4,7 kΩ. Tím je proud omezen přibližně na 1 mA při 5,1 V.

Pro splnění vlastností subsystému v souvislosti s bezpečností je nutné ochranný zkratovací obvod zdvojit, jak je vidět na Obr. 16.



Obr. 16 Schéma zapojení subsystému pro ochranu napájení

3.7.1.2 Výpočty

Jelikož musí SRECS i každý její subsystém mít úroveň integrity bezpečnosti alespoň SIL 2, neboli pravděpodobnost nebezpečných poruch za hodinu v rozmezí 10^{-7} až 10^{-6}, bude v této kapitole provedeno ověření těchto podmínek pro tento subsystém. Další podmínkou, kterou je nutné ověřit, je podíl bezpečných poruch, který musí být při nulové odolnosti proti vadám hardwaru v rozmezí 90 % až ≤ 99 %.

a) Intenzita poruch součástek subsystému PFH_D

Prvním krokem výpočtu celkové intenzity poruch subsystému je určit intenzitu poruch každé součástky. Tyto hodnoty jsou v Tab. 10.

Tab. 10 PFH_D všech součástek subsystému na kontrolu napájení

Součástka	$PFH_D \cdot 10^{-9}$
Konektor	4
Pojistka	10
Odpor	0,5
Zenerova dioda	2
Tyristor	5

Z těchto hodnot je následně dopočtena celková hodnota PFH_D subsystému. V tomto případě se jedná o součet intenzit poruch všech součástek, jelikož se jedná o architekturu typu A a porucha jakékoliv prvku může způsobit poruchu. Výsledná intenzita poruch je vypočtena v Tab. 11.

Tab. 11 Výsledné PFH_D subsystému na kontrolu napájení

Použité součásti	$PFH_D \cdot 10^{-9}$	Počet	Suma
Konektor	4	1	4
Pojistka	10	1	10
Odpor	0,5	2	1
Zenerova dioda	2	2	4
Tyristor	5	2	10
CELKEM	**$29 \cdot 10^{-9}$**		

Výsledná intenzita poruch subsystému z Tab. 11 je tedy **$29 \cdot 10^{-9}$** a s rezervou se vejde do rozmezí 10^{-7} až 10^{-6}. Tedy splňuje podmínku na úroveň integrity tohoto subsystému.

b) Podíl bezpečných poruch subsystému (SFF)

Pro výpočet podílu bezpečných poruch bylo využito intenzit poruch uvedených v Tab. 10 a přílohy D normy ČSN EN 62061. Tato příloha rozděluje intenzity poruch pro každou jednotlivou součást a určuje možné poruchové režimy dané součástky. Každý poruchový režim má určitou váhu danou procentuálním podílem z celkové intenzity poruch součástky. Poté, co je určena intenzita poruch každého poruchového

režimu, musí být rozhodnuto, zda se jedná o poruchu bezpečnou nebo nebezpečnou. Dalším aspektem je, zda poruchu lze detekovat, či nikoliv. Vypočítá se podle vzorce:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \cdot 100\ [\%]$$

- λ_S je intenzita bezpečných poruch
- λ_{DD} je intenzita nebezpečných detekovatelných poruch
- λ_D je intenzita nebezpečných poruch
- $\sum \lambda_S + \sum \lambda_D$ je celková intenzita poruch

Pro splnění požadavku na podíl bezpečných poruch musí být výsledek tohoto vzorce v rozmezí 90 % až ≤ 99 %. Celá tabulka výpočtu SFF tohoto subsystému je v příloze A1. Jejím výsledkem je SFF = 96,55 % a subsystém tedy splňuje i požadavek na podíl bezpečných poruch.

3.7.2 Subsystém – Vstupní obvody

Tento jednoduchý subsystém slouží pro galvanické oddělení koncových spínačů umístěných na dveřích a vstupu mikrokontroleru. Do koncových spínačů vede napětí 12 V, zatímco mikroprocesor má napájecí napětí 5 V. Subsystém musí splňovat tato požadavky:

- Architektura subsystému **typ B**
- Odolnost proti vadám hardwaru **1**
- Podíl bezpečných poruch **60 % až 90 %**
- Úroveň integrity bezpečnosti **SIL 2**

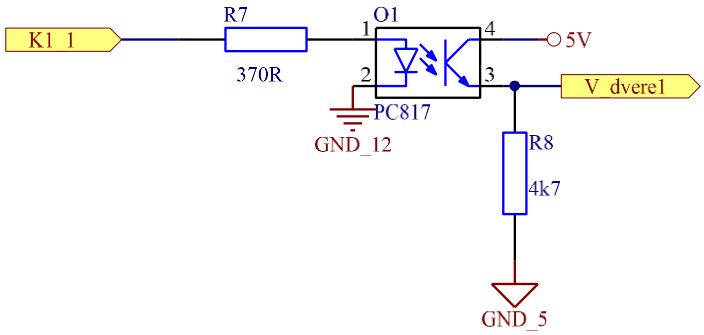
3.7.2.1 Funkce

Galvanické oddělení je zde provedeno pomocí optočlenu s tranzistorem a odporů pro správné nastavení vstupního i výstupního proudu.

Na vstup optočlenu je přivedeno napětí 12 V a hodnota maximálního vstupního proudu je 50 mA. Tento proud je pomocí rezistoru o hodnotě 370 **Ω** omezen na 32 mA, aby zde byla

určitá rezerva. Výstup z optočlenu je na 5 V potenciálu a výstupní proud může mít maximální hodnotu také 50 mA. Pro omezení tohoto proudu je zde rezistor o hodnotě 4700 Ω, který slouží i jako pull-down rezistor vstupního pinu mikroprocesoru. Výstupní proud je tedy velice malý a má přibližnou velikost 1 mA.

Jedná se o dvoukanálový subsystém, protože u mechanických spínacích prvků, jakým jsou koncové spínače, se dá předpokládat možná porucha. Dalším významem použití dvou paralelních kanálů je možnost diagnostiky. Na rozdíl od relé není u koncových spínačů jednoduchá možnost diagnostiky pomocí další skupiny kontaktů. Jako diagnostika zde tedy slouží druhý kanál a následné porovnávání obou výstupních signálů tohoto subsystému. Schéma zapojení jednoho řetězce subsystému vstupních obvodů je na Obr. 17.



Obr. 17 Schéma zapojení subsystému vstupních obvodů

3.7.2.2 Výpočty

Oproti subsystému pro ochranu napájecího napětí má tento subsystém základní typ architektury B, a tedy dva paralelní kanály. Stačí tedy, když podíl bezpečných poruch bude v intervalu 60 % až 90 %. Pravděpodobnost nebezpečných poruch za hodinu zůstává v rozmezí 10^{-7} až 10^{-6}, tedy SIL 2.

a) Intenzita poruch součástek subsystému (PFH_D)

V Tab. 12 jsou uvedeny intenzity poruch všech součástech využitých v tomto subsystému.

Tab. 12 PFH_D všech součástek subsystému vstupních obvodů

Součástka	$PFH_D \cdot 10^{-9}$
Konektor	4
Optočlen	14
Odpor	0,5
Koncový spínač	2

Výpočet výsledné intenzity poruch součástek se v případě tohoto subsystému bude skládat ze dvou kroků. Nejprve bude vypočtena intenzita poruch jedné větve, poté bude využit vzorec uvedený v 2.4.5 pro dopočtení celkové intenzity poruch celého subsystému.

V prvním kroku bude postup shodný s předchozím subsystémem a intenzita poruch jednoho kanálu bude součtem všech použitých součástek v řetězci. Výsledek je $21{,}1 \cdot 10^{-9}$ poruch za hodinu a je uveden v Tab. 13.

Tab. 13 PFH_D jednoho kanálu subsystému vstupních obvodů

Použité součásti	$PFH_D \cdot 10^{-9}$	Počet	Suma
Konektor	4	1	4
Optočlen	14	1	14
Odpor	0,5	2	1
Koncový spínač	2	1	2
CELKEM (1 kanál)	**$21 \cdot 10^{-9}$**		

V dalším kroku se z toho mezivýsledku vypočítá výsledná intenzita poruch za hodinu celého subsystému. Základní vzorec je:

$$\lambda_{DssB} = (1-\beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2,$$

kde λ_{De1} a λ_{De2} jsou intenzity poruch jednotlivých kanálů subsystému. Jelikož jsou v tomto případě oba kanály shodné, bude $\lambda_{De1} = \lambda_{De2} = 21{,}1 \cdot 10^{-9}$. β(citlivost na společné poruchy) byla určena z přílohy F normy ČSN EN 62061 a její velikost je 0,05. Poslední potřebnou hodnotou, pro výpočet vzorce je interval kontrolní zkoušky T_1, který byl zvolen jeden rok, tedy 8760 hodin. Vzorec po dosazení vypadá takto:

$$\lambda_{DssB} = (1-0{,}05)^2 \cdot 21{,}1 \cdot 10^{-9} \cdot 21{,}1 \cdot 10^{-9} \cdot 8760 + 0{,}05 \cdot (21{,}1 \cdot 10^{-9} + 21{,}1 \cdot 10^{-9})/2$$

$$\boldsymbol{\lambda_{DssB} = 1{,}05 \cdot 10^{-9}}$$

Výsledná intenzita poruch za hodinu subsystému vstupních obvodů má hodnotu **$1{,}05 \cdot 10^{-9}$**, tedy s velkou rezervou splňuje dané požadavky.

b) Podíl bezpečných poruch subsystému (SFF)

Subsystém vstupních obvodů má odolnost proti vadám hardwaru 1, a proto postačí, když podíl bezpečných poruch bude v intervalu 60 % až ≤ 90 %. Tabulka s výpočtem podílu bezpečných poruch tohoto subsystému je umístěna v příloze A2 a výsledná hodnota SFF je 72,86 %. Subsystém splňuje požadavek na podíl bezpečných poruch.

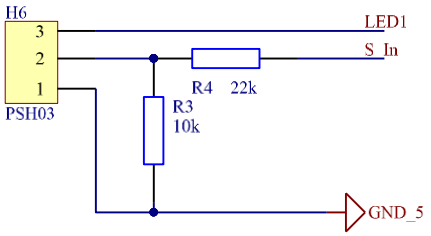
3.7.3 Subsystém – Hlavní obvod

Tento subsystém je hlavní částí řídicího systému souvisejícího s bezpečností. Obsahuje mikroprocesor, který celý automatický systém řídí. Dále pak několik pull-down rezistorů, filtrační a blokovací kondenzátory, resetovací tlačítko a programátor mikroprocesoru. Tento subsystém musí splňovat tato kritéria:

- Architektura subsystému **typ A**
- Odolnost proti vadám hardwaru **0**
- Podíl bezpečných poruch **90 % až 99 %**
- Úroveň integrity bezpečnosti **SIL 2**

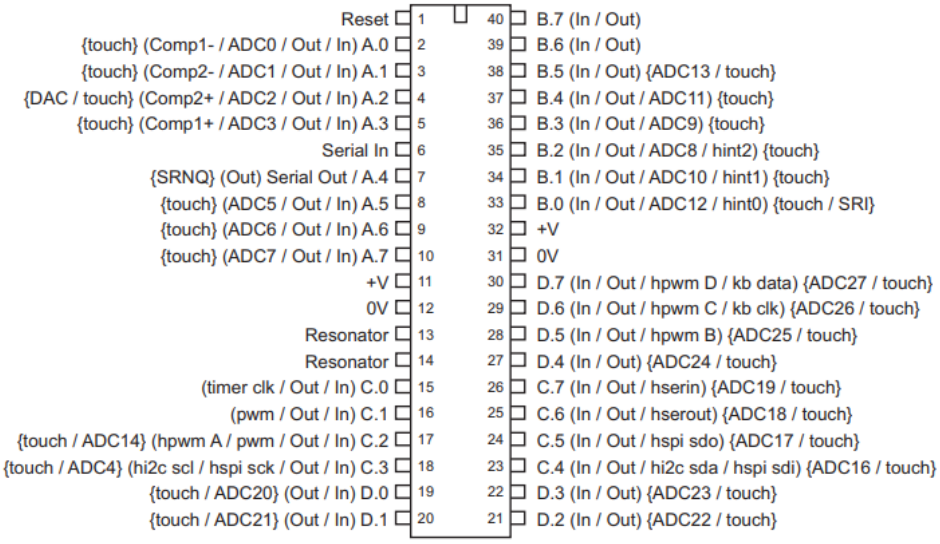
3.7.3.1 Funkce

Jelikož tento subsystém obsahuje mikroprocesor PICAXE 40x2, je „mozkem“ celého SRECS. Mikroprocesor PICAXE 40x2 je čip firmy Microchip s označením PIC18F45K22, který je následně upraven společností PICAXE tak aby bylo jeho programování co nejjednodušší a nebylo potřeba zakupovat složitý programátor. Pro nahrání i ladění programu postačí tří žilový kabel a dva rezistory. Zapojení programovacího konektoru je ukázáno na Obr. 18.



Obr. 18 Zapojení programovacího konektoru

Tento mikroprocesor byl zvolen nejen kvůli jednoduchosti programování, ale i díky jeho nízké ceně, která je přibližně 200 Kč. Další dobrou vlastností je široký rozsah napájecího napětí - 3 až 5,5. Možnost využití všech jeho pinů je na Obr. 19. Z tohoto obrázku je patrné, že většina pinů umožňuje více funkcí. Pro řízení lisu chmele nebyly všechny využity. Byly využity jen funkce analogově-digitálního převodníku (ADC) a funkce výstupu (Out). Dalších funkcí nebylo pro SRECS potřeba využít a byly použity u ostatních funkcí systému, které s bezpečností nesouvisí a ani ji neovlivňují.



Obr. 19 Funkce pinů PICAXE 40x2 [10]

Kromě mikroprocesoru obsahuje tento subsystém několik blokovacích a filtračních kondenzátorů, již zmíněný programovací konektor a několik konektorů pro připojení dalších subsystémů. Celkové schéma zapojení včetně funkcí, které nesouvisí s bezpečností, je v příloze B.

3.7.3.2 Výpočty

Tento subsystém musí splňovat stejný požadavek na maximální intenzitu poruch součástek i na podíl bezpečných poruch, jako subsystém pro ochranu vstupního napětí. Musí tedy platit, že úroveň integrity bezpečnosti je alespoň SIL2, tedy pravděpodobnost nebezpečných poruch za hodinu musí být v rozmezí 10^{-7} až 10^{-6} a podíl bezpečných poruch hardwaru v intervalu 90 % až 99 %.

a) Intenzita poruch součástek subsystému (PFH_D)

Hodnoty intenzit poruch všech součástek tohoto subsystému jsou uvedeny v Tab. 14

Tab. 14 PFH_D všech součástek subsystému hlavní obvod

Součástka	$PFH_D \cdot 10^{-9}$
Konektor	4
Mikroprocesor	9
Kondenzátor	5

Stejně jako v případě výpočtu u subsystému pro ochranu napájecího napětí, se pouze sečtou intenzity všech součástek využitých v tomto subsystému. Výsledná intenzita poruch neboli pravděpodobnost nebezpečných poruch za hodinu, je zobrazena v Tab. 15.

Tab. 15 PFH_D subsystému hlavní obvod

Použité součásti	$PFH_D \cdot 10^{-9}$	Počet	Suma
Konektor	4	3	12
Mikroprocesor	9	1	9
Kondenzátor	5	3	15
CELKEM	**$36 \cdot 10^{-9}$**		

Výsledná intenzita poruch tohoto subsystému je podle Tab. 15 rovna $36 \cdot 10^{-9}$ poruch za hodinu a je tety v daných mezích pro SIL 2.

b) Podíl bezpečných poruch subsystému (SFF)

Jelikož má tento subsystém nulovou odolnost proti vadám hardwaru a úroveň integrity bezpečnosti SIL 2, z Tab. 8 vyplývá požadavek na podíl bezpečných poruch v intervalu 90 % až 99 %.

Tabulka, kde jsou uvedeny všech prvky výpočtu podílu bezpečných poruch tohoto subsystému, je v příloze A3. Dle této tabulky je výsledný podíl bezpečných poruch roven 95 % a je tedy v předepsaném intervalu.

3.7.4 Subsystém – Výstupní obvody s relé

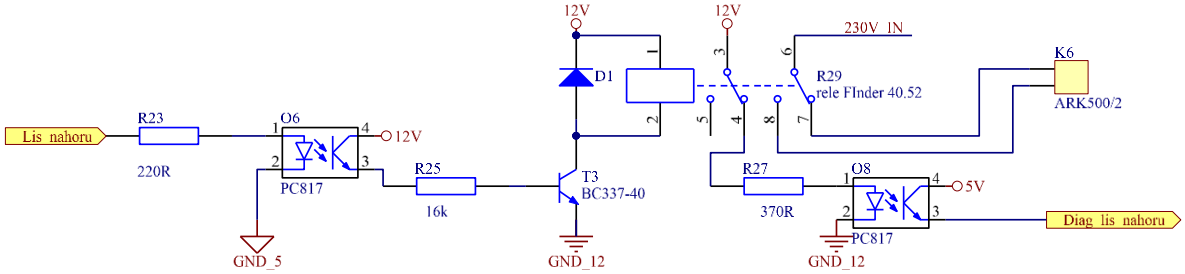
Tento subsystém je poslední částí SRECS. Jeho nejdůležitější součástí jsou relé pro následné spínání stykačů. Dále obsahuje relé, které při možném vzniku nebezpečné situace odpojí vstupní napětí 230 V pro relé a lis se tek nemůže dát do pohybu. Tento subsystém musí splňovat tyto podmínky:

- Architektura subsystému **typ A**
- Odolnost proti vadám hardwaru **0**
- Podíl bezpečných poruch **90 % až 99 %**
- Úroveň integrity bezpečnosti **SIL 2**

3.7.4.1 Funkce

Jak už bylo řečeno v předchozím odstavci, tento subsystém obsahuje relé pro ovládání pohybu lisu. Jedná se o dvě relé, jedno pro směr nahoru a druhé pro směr dolů. Typ těchto relé je takový, aby splňoval požadavky na bezpečnost. To se týká zejména kontaktů relé, které musí umožnovat využití diagnostické funkce. Obě relé tedy mají dvoje přepínací kontakty, ovšem ne zcela nezávislé. Kontakty jsou navzájem elektricky izolovány, ale mechanicky spojeny. Díky této vlastnosti se nemůže např. stát, že silové kontakty relé zůstanou v sepnutém stavu a diagnostické kontakty budou rozepnuty. Pokud by tento případ mohl nastat, diagnostická funkce by postrádala význam. Tato situace ovšem u těchto speciálních relé nastat nemůže.

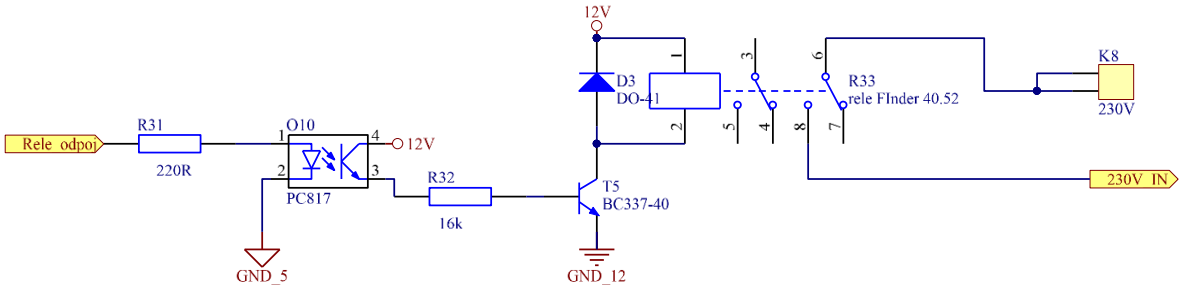
Každé relé je spínáno z jednoho výstupního pinu mikroprocesoru. Mezi výstupní pin a relé je ovšem ještě zařazen optočlen a bipolární tranzistor, který relé fyzicky spíná. K relé je pro omezení proudových špiček zapojena antiparalelně dioda. Celé zapojení je na Obr. 20.



Obr. 20 Schéma zapojení jednoho relé pro ovládání lisu

Pro diagnostickou funkci bylo využito druhé skupiny přepínacích kontaktů relé. Jelikož je pravděpodobnost poruchy mnohem větší pro rozpojení obvodu kterékoliv součástky, byl pro diagnostiku použit rozpínací kontakt relé. Na tento kontakt je přes rezistor připojen optočlen pro galvanické oddělení a poté je tento signál přiveden na vstupní pin mikrokontroleru, kde může být porovnán s ostatními signály.

Poslední podsestavou tohoto subsystému je relé, které může odpojit vstupní napětí pro ovládací relé a zamezit tak pohybu lisu, pokud mikrokontroler vyhodnotí možný nebezpečný stav. Schéma je na Obr. 21.



Obr. 21 Schéma zapojení relé pro odpojení vstupního napětí pro ovládací relé

3.7.4.2 Výpočty

Subsystém výstupních obvodů (relé) má stejný požadavek na vlastnosti jako subsystém ochrany napájení i subsystém hlavní obvod. Úroveň integrity bezpečnosti se musí rovnat alespoň SIL 2 a podíl bezpečných poruch hardwaru v rozmezí 90 % až 99 %.

a) Intenzita poruch součástek subsystému (PFH_D)

Tab. 16 PFH_D všech součástek subsystému výstupních obvodů (relé)

Součástka	$PFH_D \cdot 10^{-9}$
Konektor	4
Relé	156
Dioda	1
Odpor	0,5
Bip. tranzistor	5
Optočlen	14

Intenzity poruch všech součástek použitých v tomto subsystému jsou uvedeny v Tab. 16.

Výpočet se provádí stejně jako u předchozího subsystému a výsledná intenzita poruch za hodinu je součtem všech intenzit poruch součástek subsystému. Výsledek je v Tab. 17.

Tab. 17 PFH_D subsystému výstupních obvodů (relé)

Použité součásti	$PFH_D \cdot 10^{-9}$	Počet	Suma
Konektor	4	6	24
Relé	156	3	468
Dioda	1	3	3
Odpor	0,5	10	5
Bip. tranzistor	5	3	15
Optočlen	14	5	70
CELKEM	**$585 \cdot 10^{-9}$**		

Výsledná intenzita poruch tohoto subsystému je podle Tab. 17 rovna $585 \cdot 10^{-9}$ poruch za hodinu. Je tety v daných mezích pro SIL 2.

b) Podíl bezpečných poruch subsystému (SFF)

I tento subsystém má odolnost proti vadám hardwaru 0 a úroveň integrity bezpečnosti SIL 2 a tudíž pro něj platí, že hodnota bezpečných poruch musí být v intervalu 90 % až 99 %.

Všechny prvky výpočtu podílu bezpečných poruch pro tento subsystém jsou v příloze A4. Podíl bezpečných poruch tohoto subsystému je 95,67 % a tedy splňuje požadavek SFF.

3.8 Intenzita poruch součástek celého SRECS

Jako každý subsystém musí splňovat požadavky na úroveň integrity bezpečnosti, tak i celý systém musí splňovat toto kritérium. Interval pro splnění předepsané úrovně integrity SIL2 je 10^{-7} až 10^{-6}. V Tab. 18 jsou uvedeny PFH_D všech subsystému SRECF v jednotkách FIT, tedy 10^{-9}.

Tab. 18 Celkové PFH_D všech subsystémů

Subsystém	Základní typ	$PFH_D \cdot 10^{-9}$
Ochrana napájení	A	29
Vstupní obvody	B	1,05
Hlavní obvod	A	36
Výstupní obvody (relé)	A	585
CELKEM	**$651{,}05 \cdot 10^{-9}$**	

Z výše uvedené tabulky je zřejmé, že hodnota je 651,05 FIT, tedy $651{,}05 \cdot 10^{-9}$. Po převedení je hodnota intenzit poruch za hodinu $6{,}5105 \cdot 10^{-7}$ a tedy splňuje parametry pro **splnění SIL 2**.

Závěr

Cílem této práce byl návrh automatického systému pro ovládání lisu chmele s ohledem na bezpečnost. V první části této diplomové práce byly vybrány a porovnány normy, které se nejvíce hodí pro návrh řídících systémů pro strojní zařízení včetně bezpečnostních požadavků. Norma ČSN EN 61508 je obecnou normou pro návrh řídích elektronických systémů a zabývá se především elektronickými zařízeními a pro návrh řídícího systému pro strojní zařízení není tedy příliš vhodná. Vhodnější jsou normy ČSN EN ISO 13849 a ČSN EN 62061. První zmíněná norma se však především zaobírá návrhem bezpečných systémů jiných než elektrických či elektronických, zejména mechanickými, hydraulickými a pneumatickými. Jelikož je řídící systém pro lis chmele systémem elektronickým, nehodí se tuto normu použít. Norma ČSN EN 62061 je přímo podle názvu určena pro strojní zařízení a použitelná je pro elektronické, elektrické nebo programovatelné systémy. Porovnáním a vhodným výběrem těchto norem byl splněn první bod zadání této diplomové práce a následný návrh bezpečného systému pro řízení lisu chmele postupoval podle poslední zmíněné normy, tedy **ČSN EN 62061**.

V další kapitole této práce byl obecně popsán postup návrhu systému podle ČSN EN 62061 včetně důležitých vlastností a požadavků na bezpečný systém. Dále byly v této kapitole uvedeny všechny potřebné informace pro návrh konkrétního elektronického systému, který splňuje dané bezpečnostní požadavky včetně procesu odhadu rizika, určení integrity bezpečnosti pro dané riziko a procesu vývoje řídícího systému a funkcí souvisejících s bezpečností pro konkrétní riziko.

Třetí kapitola je zaměřena na konkrétní návrh bezpečnostního systému pro řízení lisu chmele. Nejprve byla provedena riziková analýza, která odhalila nezanedbatelné riziko spočívající v možnosti zranění obsluhy pohybujícím se beranem lisu. Pro omezení tohoto rizika byla navržena bezpečnostní funkce „**při otevřených dveřích se nesmí beran lisu pohybovat**“. V dalším kroku byla bezpečnostní funkci přiřazena úroveň integrity bezpečnosti neboli SIL. Po zhodnocení všech aspektů rizika dle normy ČSN EN 62061 byla stanovena úroveň integrity bezpečnosti **SIL 2.** Následně byla navržena specifikace řídícího systému a jeho rozčlenění do subsystémů. Rozdělením vznikly celkem čtyři subsystémy, pro které byly následně provedeny výpočty intenzit poruch za hodinu a podílu bezpečných poruch. Jedná se o subsystémy: **kontrola napájení, vstupní obvody, hlavní obvod a výstupní obvody (relé)**. Po vypočtení uvedených dvou parametrů pro každý subsystém byla provedena kontrola, zda

každý ze subsystémů i celý systém splňuje požadavky na maximální možnou intenzitu poruch a podíl bezpečných poruch, aby byl tak splněn požadavek úrovně integrity bezpečnosti SIL 2. Dovolená hodnota intenzit poruch pro SIL 2 je v rozmezí 10^{-7} až 10^{-6}. Celková intenzita poruch za hodinu celého systému vyšla $6{,}5105 \cdot 10^{-7}$ a systém tedy **splňuje SIL2.**

Díky zavedení bezpečnostní funkce do řídícího systému pro lis chmelu byla většinová část rizika pro tento stroj eliminována a stroj tak lze považovat za **bezpečný**. V návaznosti na tuto diplomovou práci by mohl být tento systém uveden do praxe, aby mohly být využity jeho dobré vlastnosti z hlediska bezpečnosti, protože lidské zdraví je to nejdůležitější.

Seznam literatury a informačních zdrojů

[1] Bezpečnost strojů - 1. díl: úvod, normy, posouzení rizika. *Automatizace.hw.cz* [online]. c1997-2014, 2015 [cit. 2018-04-16]. Dostupné z: https://automatizace.hw.cz//bezpecnost-stroju/bezpecnost-stroju-1-dil-normy-rizika.html

[2] ČSN EN 61508-1. *Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností: Část 1: Všeobecné požadavky*. Ed. 2. Praha: Český normalizační institut, 2005.

[3] Bezpečnost strojů - 2. díl: PL vs. SIL. *Automatizace.hw.cz* [online]. c1997-2014, 2015 [cit. 2018-04-16]. Dostupné z: https://automatizace.hw.cz/bezpecnost-stroju/bezpecnost-stroju-2-dil-pl-vs-sil.html

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

[5] ČSN EN ISO 13849-1. *Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů: Část 1: Obecné zásady pro konstrukci*. Praha: Úřad pro technickou normalizaci, 2017.

[6] Bezpečnost strojů a strojních zařízení. *Asociace pracovníků tlakových zařízení* [online]. 17. 2. 2017 [cit. 2018-04-25]. Dostupné z: http://atz.cz/?p=493

[7] ČSN EN 61508-5. *Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností: Část 5: Příklady metod určování úrovní integrity bezpečnosti*. Ed. 2. Praha: Český normalizační institut, 2005.

[8] Funkční bezpečnost. *TÜV SÜD Czech* [online]. 2018 [cit. 2018-05-01]. Dostupné z: https:// www.tuv-sud.cz/cz-cz/ odvetvi/ automobilovy- prumysl/ dodavatele- pro-automobilovy-prumysl/funkcni-bezpecnost

[9] *Safety Integrated: Náhled do norem* [online]. 18.6.2009 [cit. 2018-05-01]. Dostupné z: http://stest1.etnetera.cz/ad/current/content/data_files/reseni/safety_integrated/prezentace/prez_tia-si-uvod-normy_2009-09_cz.pdf

[10] *PICAXE* [online]. [cit. 2018-05-01]. Dostupné z: http://www.picaxe.com/

Přílohy

Příloha A – Podíl bezpečných poruch hardwaru SRECS

A1. SFF subsystému pro ochranu napájecího napětí

subsystém	*součástka*	*označení ve schematu*	*druh poruchy*	*procenta*	*detekovatelnost*	*bezpečnost*	*FIT*	*% FIT*	*bezpečný FIT*	*nebezpečný nedetekovatelný FIT*	*nebezpečný detekovatelný FIT*	***SFF***
Ochranné obvody napájení	konektor 5V	H1	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	**96,55%**
			Zkrat libovolného vodiče s neživou částí	10	NE	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	pojistka 3A	F1	Nedojde k přetavení	10	NE	NE	10	1	0	1	0	
			Přerušený obvod	90	NE	ANO	10	9	9	0	0	
	Rezistor	R1	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	ANO	0,5	0,05	0,05	0	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R2	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	ANO	0,5	0,05	0,05	0	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Zenerova dioda 5V1	Z1	Přerušený obvod	50	NE	ANO	2	1	1	0	0	
			Zkrat	50	NE	ANO	2	1	1	0	0	
	Zenerova dioda 5V1	Z2	Přerušený obvod	50	NE	ANO	2	1	1	0	0	
			Zkrat	50	NE	ANO	2	1	1	0	0	
	Tyristor TIC116M	T1	Rozpojený kontakt kteréhokoliv spoje	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi dvěma libovolnými spoji	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi všemi spoji	25	NE	ANO	5	1,25	1,25	0	0	
			Změna charakteristik	25	NE	ANO	5	1,25	1,25	0	0	
	Tyristor TIC116M	T2	Rozpojený kontakt kteréhokoliv spoje	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi dvěma libovolnými spoji	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi všemi spoji	25	NE	ANO	5	1,25	1,25	0	0	
			Změna charakteristik	25	NE	ANO	5	1,25	1,25	0	0	

A2. SFF subsystému vstupních obvodů

subsystém	*součástka*	*označení ve schematu*	*druh poruchy*	*procenta*	*detekovatelnost*	*bezpečnost*	*FIT*	*% FIT*	*bezpečný FIT*	*nebezpečný nedetekovatelný FIT*	*nebezpečný detekovatelný FIT*	*SFF*
Vstupní obvody - koncové spínače	Koncový spínač	K1_1	Kontakty nelkze rozepnout	50	ANO	NE	2	1	0	0	1	72,86%
			Kontakty nelkze szepnout	50	ANO	ANO	2	1	1	0	0	
	Koncový spínač	K1_2	Kontakty nelkze rozepnout	50	ANO	NE	2	1	0	0	1	
			Kontakty nelkze szepnout	50	ANO	ANO	2	1	1	0	0	
	Konektor ARK500/2	K1	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	
			Zkrat libovolného vodiče s neživou částí	10	NE	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	Konektor ARK500/2	K2	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	
			Zkrat libovolného vodiče s neživou částí	10	NE	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	Rezistor	R7	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	NE	0,5	0,05	0	0,05	0	
	Rezistor	R8	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	ANO	0,5	0,05	0,05	0	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R9	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	NE	0,5	0,05	0	0,05	0	
	Rezistor	R10	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	ANO	0,5	0,05	0,05	0	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Optočlen PC817	O1	Rozpojený obvod jednotlivého spoje	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	NE	NE	14	4,2	0	4,2	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	
	Optočlen PC817	O2	Rozpojený obvod jednotlivého spoje	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	NE	NE	14	4,2	0	4,2	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	

A3. SFF subsystému – hlavní obvod

subsystém	součástka	označení ve schematu	druh poruchy	procenta	detekovatelnost	bezpečnost	FIT	% FIT	bezpečný FIT	nebezpečný nedetekovatelný FIT	nebezpečný detekovatelný FIT	SFF
Hlavní obvod	Konektor napájení	H5	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	95,00%
			Zkrat libovolného vodiče s neživou částí	10	NE	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	Konektor sig. relé	H4	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	
			Zkrat libovolného vodiče s neživou částí	10	ANO	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	ANO	ANO	4	3,2	3,2	0	0	
	Konektor diagnostiky	H3	Zkrat mezi libovolnými dvěma sousedními spoji	10	ANO	NE	4	0,4	0	0	0,4	
			Zkrat libovolného vodiče s neživou částí	10	ANO	NE	4	0,4	0	0	0,4	
			Rozpojený obvod libovolného spoje konektoru	80	ANO	NE	4	3,2	0	0	3,2	
	Kondenzátor 470uF	C1	Rozpojený obvod	40	NE	ANO	5	2	2	0	0	
			Zkrat	40	NE	ANO	5	2	2	0	0	
			Náhodná změna parametrů	20	NE	ANO	5	1	1	0	0	
	Kondenzátor 100nF	C2	Rozpojený obvod	40	NE	ANO	5	2	2	0	0	
			Zkrat	40	NE	ANO	5	2	2	0	0	
			Náhodná změna parametrů	20	NE	ANO	5	1	1	0	0	
	Kondenzátor 10nF	C3	Rozpojený obvod	40	NE	ANO	5	2	2	0	0	
			Zkrat	40	NE	ANO	5	2	2	0	0	
			Náhodná změna parametrů	20	NE	ANO	5	1	1	0	0	
	Mikroprocesor PICAXE 40x2	U1	Rozpojený obvod kteréhokoliv vývodu	20	NE	ANO	9	1,8	1,8	0	0	
			Zkrat mezi dvěma libovolnými vývody	20	NE	NE	9	1,8	0	1,8	0	
			Uváznutí v jednom stavu	20	ANO	NE	9	1,8	0	0	1,8	
			Parazitní kmity na vývodech	20	NE	ANO	9	1,8	1,8	0	0	
			Změna hodnot - referenčního napětí	20	NE	ANO	9	1,8	1,8	0	0	

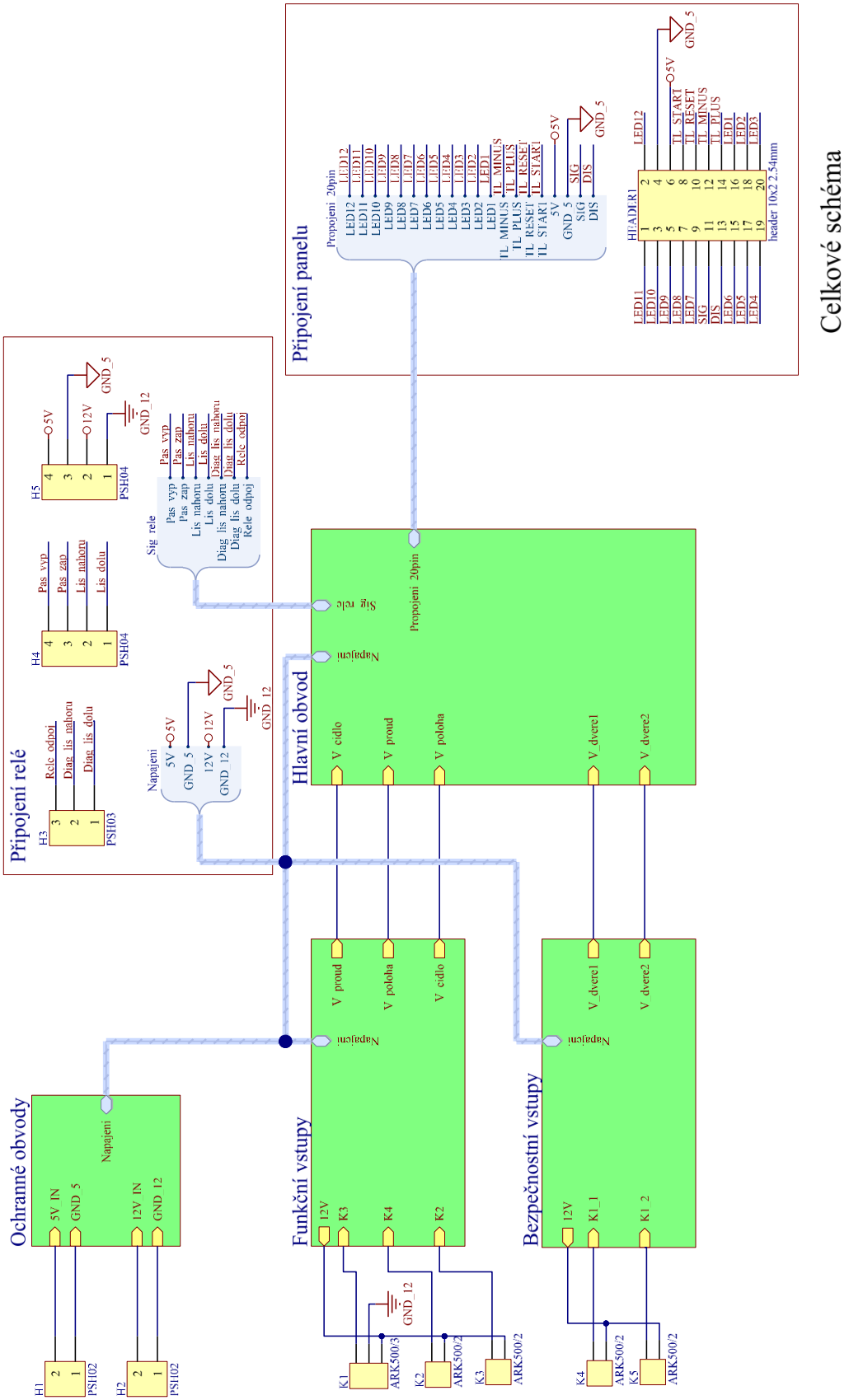
A4. SFF subsystému výstupních obvodů (relé)

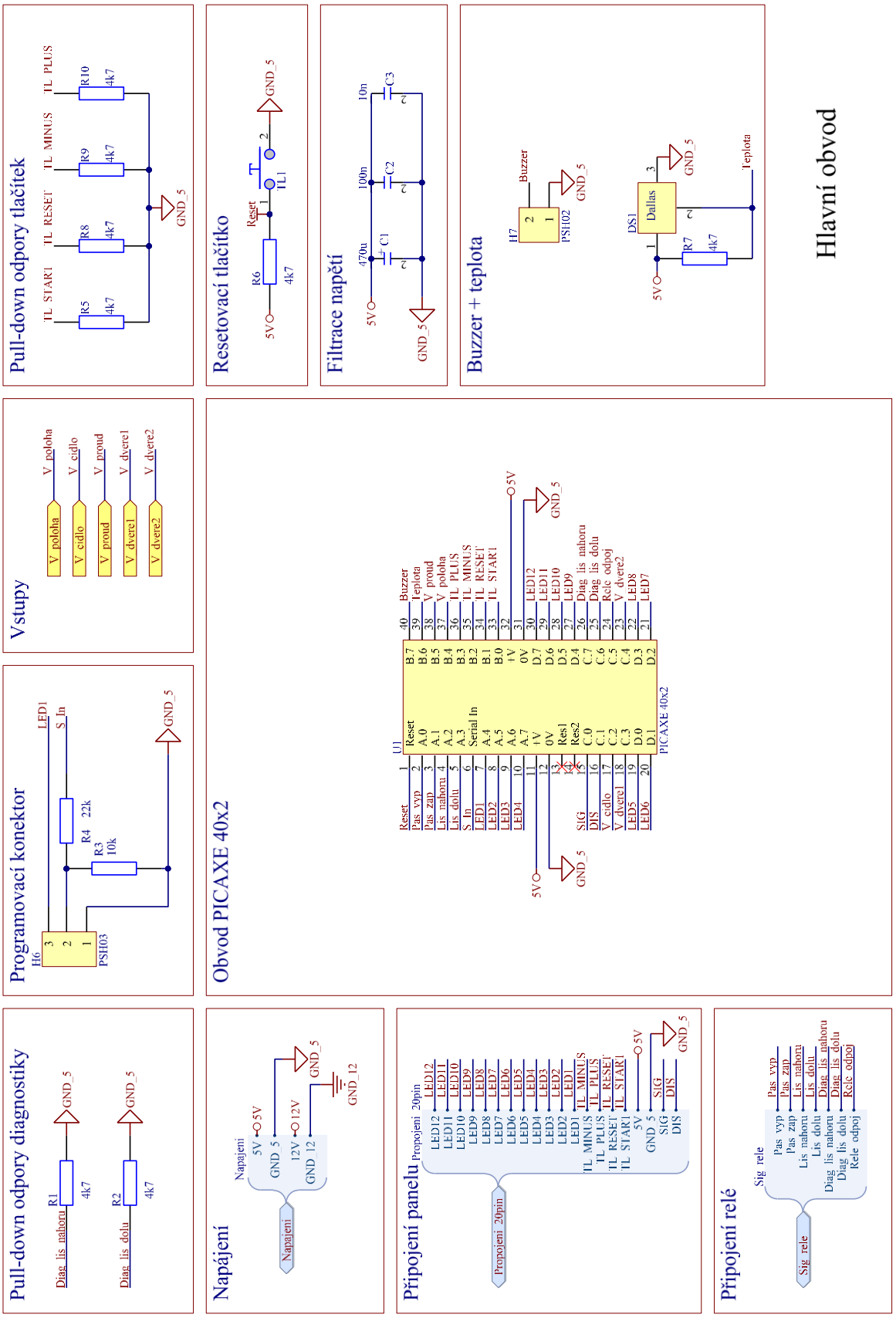
subsystém	součástka	označení ve schematu	druh poruchy	procenta	detekovatelnost	bezpečnost	FIT	% FIT	bezpečný FIT	nebezpečný nedetekovatelný FIT	nebezpečný detekovatelný FIT	SFF
Výstupní obvody - relé	Konektor napájení	H8	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	95,67%
			Zkrat libovolného vodiče s neživou částí	10	NE	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	Konektor sig. relé	H9	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	
			Zkrat libovolného vodiče s neživou částí	10	ANO	ANO	4	0,4	0,4	0	0	
			Rozpojený obvod libovolného spoje konektoru	80	ANO	ANO	4	3,2	3,2	0	0	
	Konektor diagnostiky	H10	Zkrat mezi libovolnými dvěma sousedními spoji	10	ANO	NE	4	0,4	0	0	0,4	
			Zkrat libovolného vodiče s neživou částí	10	ANO	NE	4	0,4	0	0	0,4	
			Rozpojený obvod libovolného spoje konektoru	80	ANO	NE	4	3,2	0	0	3,2	
	Optočlen PC817	O6	Rozpojený obvod jednotlivého spoje	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	NE	NE	14	4,2	0	4,2	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	
	Optočlen PC817	O8	Rozpojený obvod jednotlivého spoje	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	NE	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	NE	NE	14	4,2	0	4,2	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	
	Optočlen PC817	O7	Rozpojený obvod jednotlivého spoje	30	ANO	NE	14	4,2	0	0	4,2	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	ANO	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	ANO	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	
	Optočlen PC817	O9	Rozpojený obvod jednotlivého spoje	30	ANO	NE	14	4,2	0	0	4,2	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	ANO	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	ANO	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	
	Optočlen PC817	O10	Rozpojený obvod jednotlivého spoje	30	ANO	NE	14	4,2	0	0	4,2	
			Zkrat mezi dvěma libovolnými vstupními spoji	30	ANO	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěla libovolnými výstupními spoji	30	ANO	ANO	14	4,2	4,2	0	0	
			Zkrat mezi dvěma libovolnými spoji vstupu a výstupu	10	NE	NE	14	1,4	0	1,4	0	
	Rezistor	R23	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R24	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R25	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R26	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R27	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R28	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R31	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	
	Rezistor	R32	Přerušený obvod	80	NE	ANO	0,5	0,4	0,4	0	0	
			Zkrat	10	NE	NE	0,5	0,05	0	0,05	0	
			Náhodná změna parametrů	10	NE	ANO	0,5	0,05	0,05	0	0	

subsystém	součástka	označení ve schematu	druh poruchy	procenta	detekovatelnost	bezpečnost	FIT	% FIT	bezpečný FIT	nebezpečný nedetekovatelný FIT	nebezpečný detekovatelný FIT	SFF
Výstupní obvody - relé	Dioda u relé	D1	Přerušený obvod	50	NE	ANO	1	0,5	0,5	0	0	95,67%
			Zkrat	50	NE	ANO	1	0,5	0,5	0	0	
	Dioda u relé	D2	Přerušený obvod	50	NE	ANO	1	0,5	0,5	0	0	
			Zkrat	50	NE	ANO	1	0,5	0,5	0	0	
	Dioda u relé	D3	Přerušený obvod	50	NE	ANO	1	0,5	0,5	0	0	
			Zkrat	50	NE	ANO	1	0,5	0,5	0	0	
	Relé	R29	Všechny kontakty zůstávají v zapnuté poloze, je-li cívka bez napětí	30	ANO	NE	156	46,8	0	0	46,8	
			Všechny kontakty zůstávají ve vypnuté poloze, je-li cívka pod napětím	30	ANO	ANO	156	46,8	46,8	0	0	
			Kontakty nelze rozepnout	10	ANO	NE	156	15,6	0	0	15,6	
			Kontkty nelze sepnout	10	ANO	ANO	156	15,6	15,6	0	0	
			Sloučasný zkrat mezi třemi kontakty přepínacího spínače	10	ANO	NE	156	15,6	0	0	15,6	
			Současné zapnutí zapínacího a vypínacího kontaktu	10	NE	ANO	156	15,6	15,6	0	0	
	Relé	R30	Všechny kontakty zůstávají v zapnuté poloze, je-li cívka bez napětí	30	ANO	NE	156	46,8	0	0	46,8	
			Všechny kontakty zůstávají ve vypnuté poloze, je-li cívka pod napětím	30	ANO	ANO	156	46,8	46,8	0	0	
			Kontakty nelze rozepnout	10	ANO	NE	156	15,6	0	0	15,6	
			Kontkty nelze sepnout	10	ANO	ANO	156	15,6	15,6	0	0	
			Sloučasný zkrat mezi třemi kontakty přepínacího spínače	10	ANO	NE	156	15,6	0	0	15,6	
			Současné zapnutí zapínacího a vypínacího kontaktu	10	NE	ANO	156	15,6	15,6	0	0	
	Relé	R33	Všechny kontakty zůstávají v zapnuté poloze, je-li cívka bez napětí	30	NE	ANO	156	46,8	46,8	0	0	
			Všechny kontakty zůstávají ve vypnuté poloze, je-li cívka pod napětím	30	NE	ANO	156	46,8	46,8	0	0	
			Kontakty nelze rozepnout	10	NE	ANO	156	15,6	15,6	0	0	
			Kontkty nelze sepnout	10	NE	ANO	156	15,6	15,6	0	0	
			Sloučasný zkrat mezi třemi kontakty přepínacího spínače	10	NE	ANO	156	15,6	15,6	0	0	
			Současné zapnutí zapínacího a vypínacího kontaktu	10	NE	ANO	156	15,6	15,6	0	0	
	Bipolární tranzistor BC337	T3	Rozpojený kontakt kteréhokoliv spoje	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi dvěma libovolnými spoji	25	NE	NE	5	1,25	0	1,25	0	
			Zkrat mezi všemi spoji	25	NE	NE	5	1,25	0	1,25	0	
			Změna charakteristik	25	NE	ANO	5	1,25	1,25	0	0	
	Bipolární tranzistor BC337	T4	Rozpojený kontakt kteréhokoliv spoje	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi dvěma libovolnými spoji	25	NE	NE	5	1,25	0	1,25	0	
			Zkrat mezi všemi spoji	25	NE	NE	5	1,25	0	1,25	0	
			Změna charakteristik	25	NE	ANO	5	1,25	1,25	0	0	
	Bipolární tranzistor BC337	T5	Rozpojený kontakt kteréhokoliv spoje	25	NE	ANO	5	1,25	1,25	0	0	
			Zkrat mezi dvěma libovolnými spoji	25	NE	NE	5	1,25	0	1,25	0	
			Zkrat mezi všemi spoji	25	NE	NE	5	1,25	0	1,25	0	
			Změna charakteristik	25	NE	ANO	5	1,25	1,25	0	0	
	Konektor ARK500/3	K6	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	NE	4	0,4	0	0,4	0	
			Zkrat libovolného vodiče s neživou částí	10	NE	NE	4	0,4	0	0,4	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	Konektor ARK500/3	K7	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	NE	4	0,4	0	0,4	0	
			Zkrat libovolného vodiče s neživou částí	10	NE	NE	4	0,4	0	0,4	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	
	Konektor ARK500/2	K8	Zkrat mezi libovolnými dvěma sousedními spoji	10	NE	ANO	4	0,4	0,4	0	0	
			Zkrat libovolného vodiče s neživou částí	10	NE	NE	4	0,4	0	0,4	0	
			Rozpojený obvod libovolného spoje konektoru	80	NE	ANO	4	3,2	3,2	0	0	

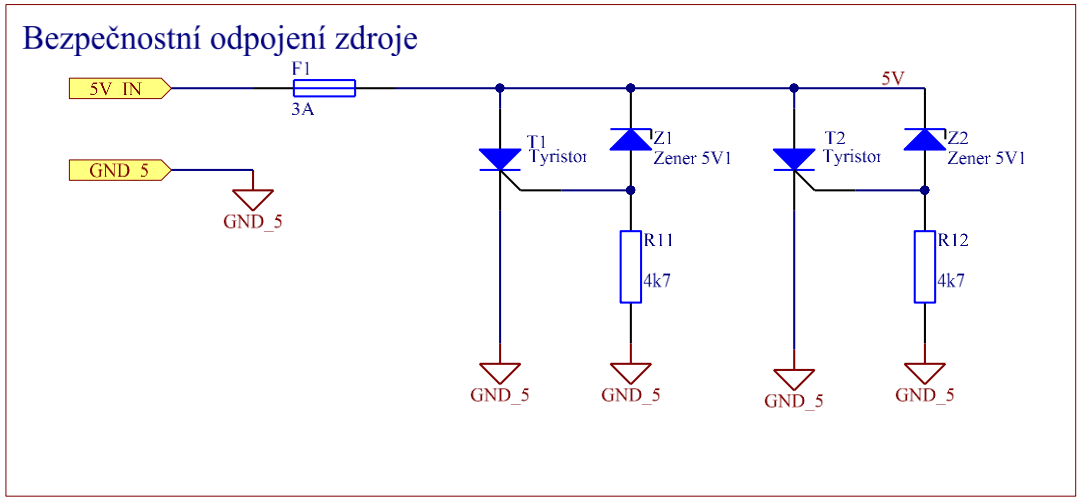
Příloha B –Schéma zapojení

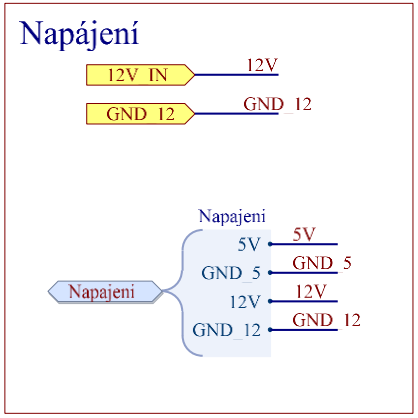
B1. Schéma zapojení řídícího systému

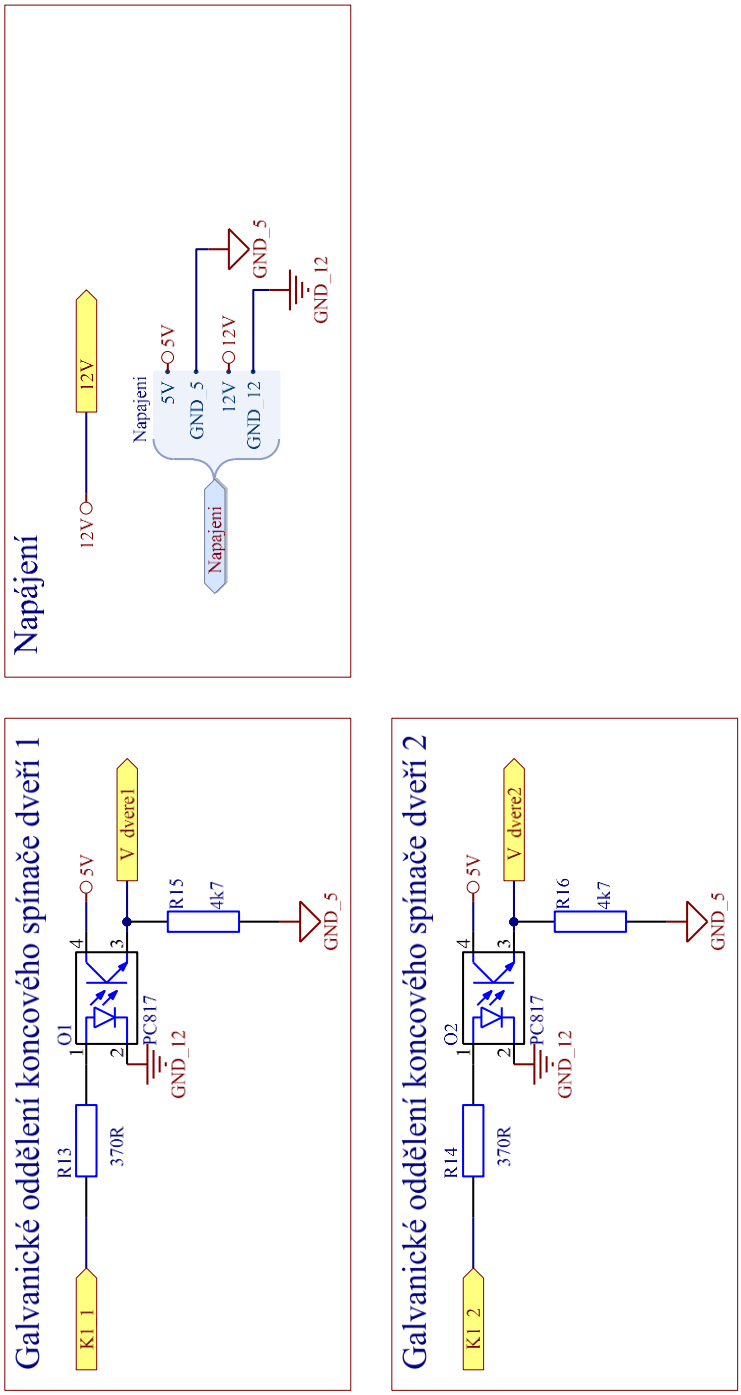



Pull-down odpory tlačítek
TL_START
TL_RESET
TL_MINUS
TL_PLUS
R5 4k7
R8 4k7
R9 4k7
R10 4k7
GND_5
Resetovací tlačítko
Reset
R6 4k7
TL1
5V
GND_5
Filtrace napětí
470u
C1
100n
C2
10n
C3
5V
GND_5
Buzzer + teplota
H7
Buzzer
PSH02
DS1
Dallas
R7 4k7
Teplota
Vstupy
V_poloha
V_cidlo
V_proud
V_dvere1
V_dvere2
Programovací konektor
H6
PSH03
LED1
S_In
R4 22k
R3 10k
Obvod PICAXE 40x2
U1
PICAXE 40x2
Reset
Pas_vyp
Pas_zap
Lis_nahoru
Lis_dolu
S_In
LED1
LED2
LED3
LED4
LED5
LED6
LED7
LED8
LED9
LED10
LED11
LED12
Buzzer
Teplota
V_proud
V_poloha
TL_PLUS
TL_MINUS
TL_RESET
TL_START
Serial In
Res1
Res2
SIG
DIS
V_cidlo
V_dvere1
V_dvere2
Diag_lis_nahoru
Diag_lis_dolu
Rele_odpoj
Pull-down odpory diagnostiky
Diag_lis_nahoru
Diag_lis_dolu
R1 4k7
R2 4k7
Napájení
Napajeni
5V
12V
GND_5
GND_12
Připojení panelu
Propojeni_20pin
Připojení relé
Sig_rele
Pas_vyp
Pas_zap
Lis_nahoru
Lis_dolu
Diag_lis_nahoru
Diag_lis_dolu
Rele_odpoj
Hlavní obvod

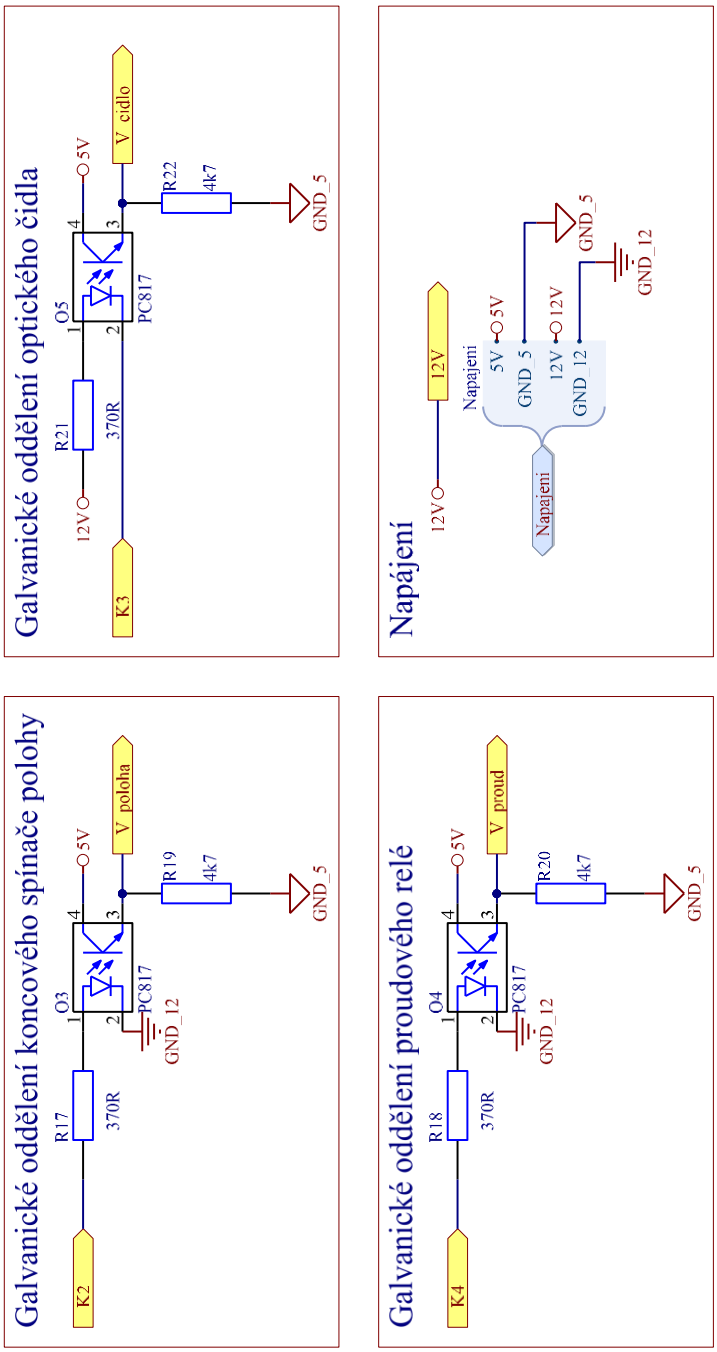
Ochranné obvody napájení





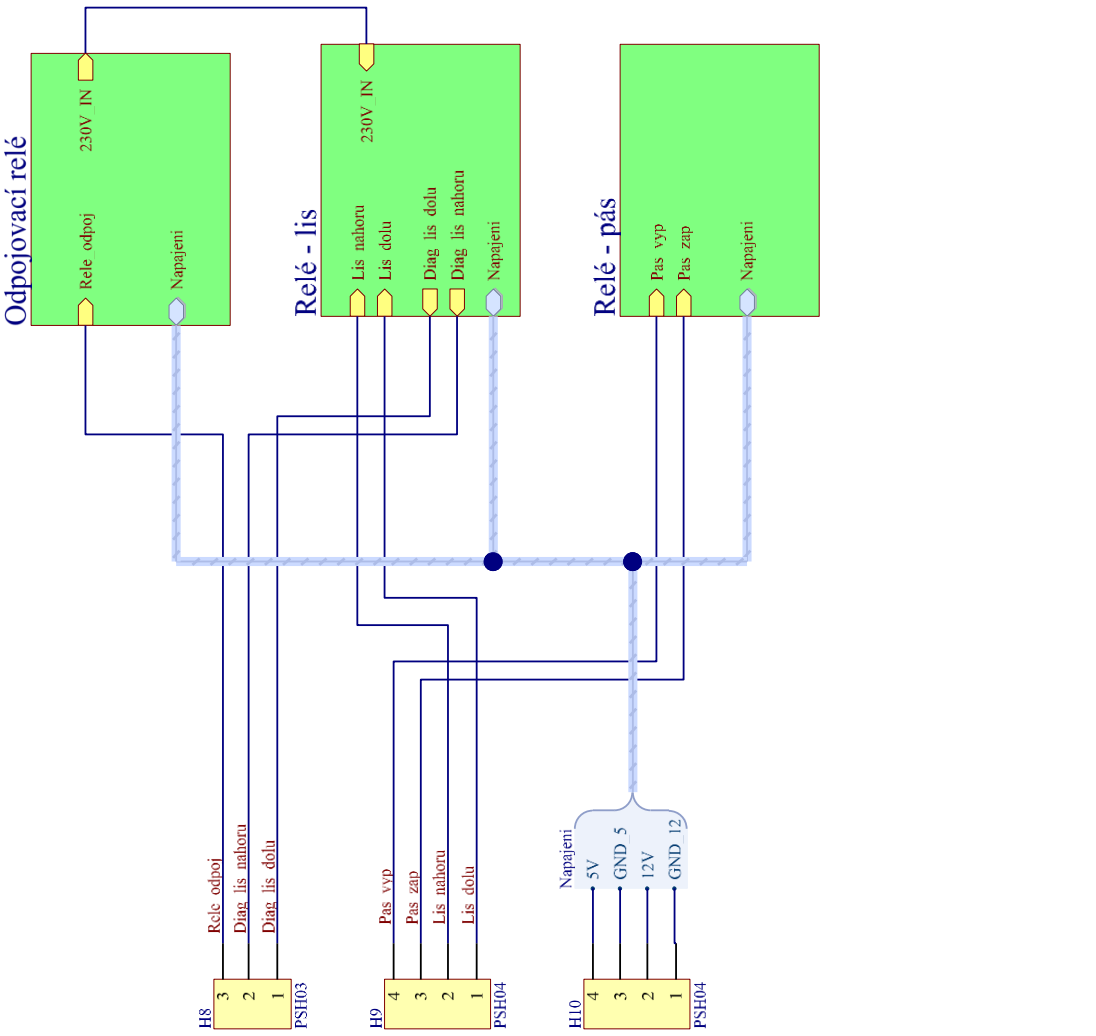


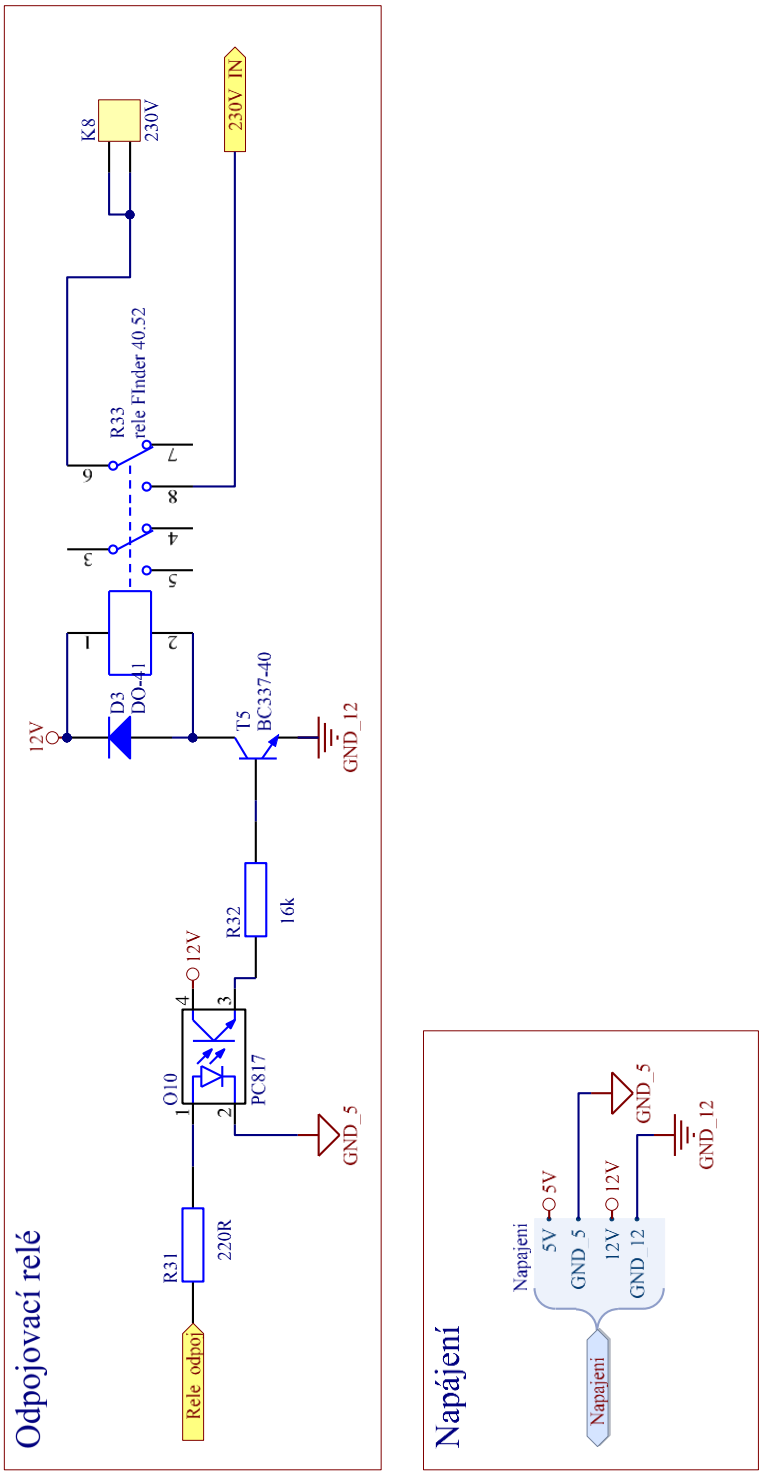
Vstupní obvody - koncové spínače

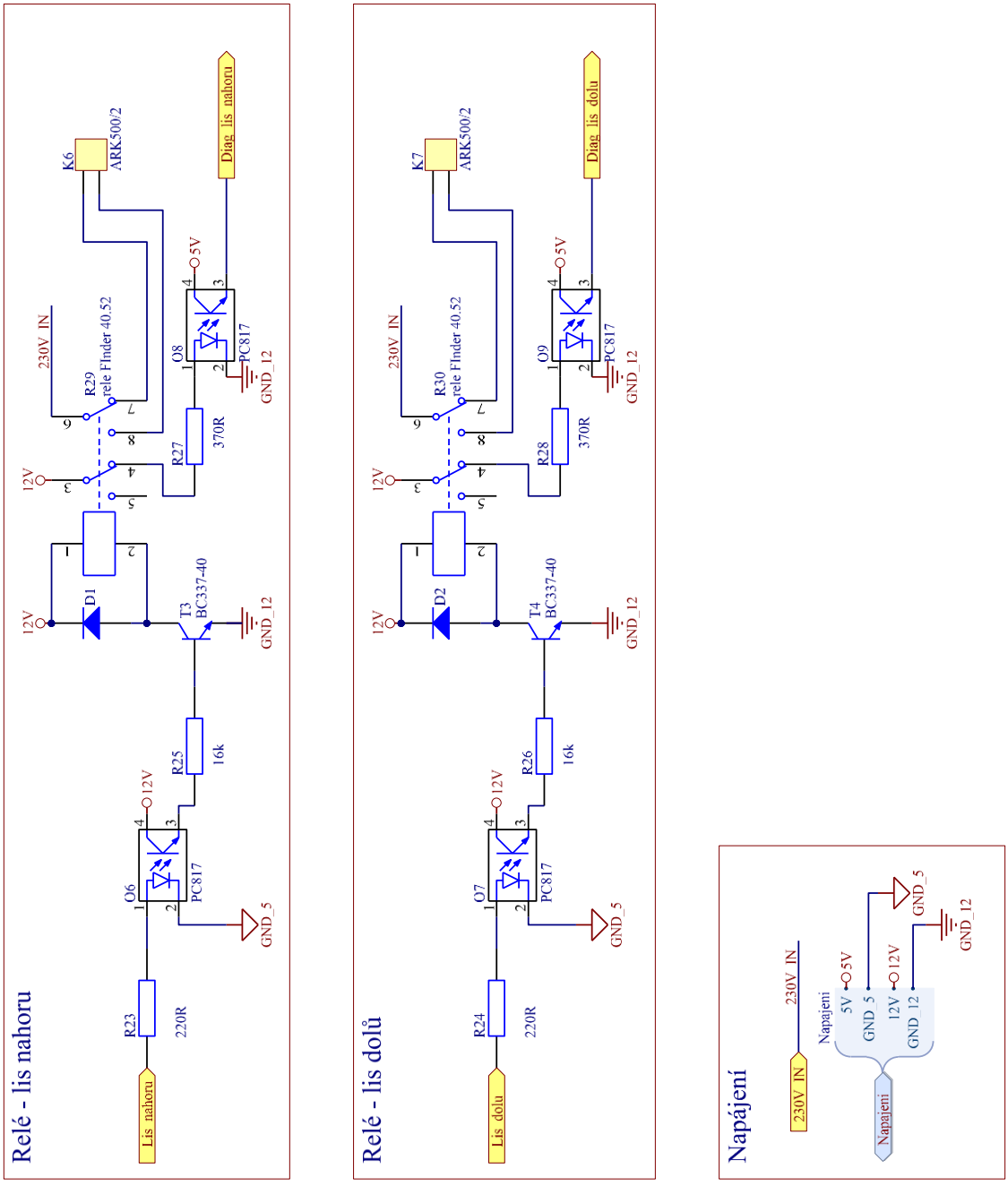


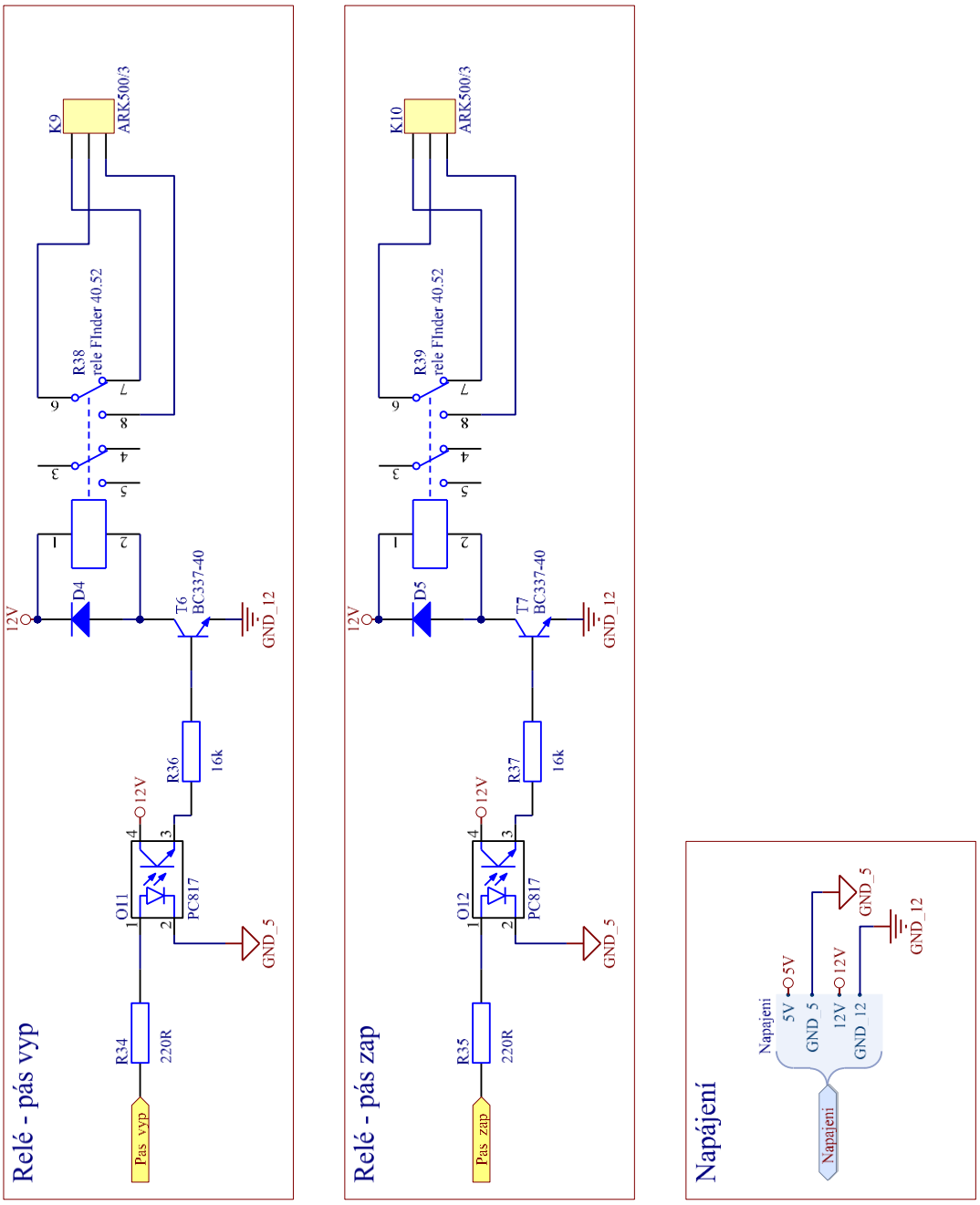
Vstupní obvody - čidlo + p.relé

B2. Schéma zapojení obvodů relé




Relé - odpojovací
Odpojovací relé
Napájení
Rele_odpoj
R31
220R
Q10
PC817
R32
16k
T5
BC337-40
D3
DO-41
K8
230V
230V_IN
R33
rele Finder 40.52
12V
GND_5
GND_12
Napajeni
5V
GND_5
12V
GND_12


Relé - lis
Relé - lis nahoru
Lis nahoru
R23
220R
Q6
PC817
R25
16k
T3
BC337-40
D1
K6
ARK500/2
R29
rele FInder 40.52
230V_IN
R27
370R
Q8
PC817
Diag_lis_nahoru
GND_12
GND_5
5V
12V
Relé - lis dolů
Lis dolu
R24
220R
Q7
PC817
R26
16k
T4
BC337-40
D2
K7
ARK500/2
R30
rele FInder 40.52
R28
370R
Q9
PC817
Diag_lis_dolu
Napájení
230V_IN
Napajeni
5V
GND_5
12V
GND_12


Relé - pás
Relé - pás vyp
K9
ARK500/3
R38
rele FInder 40.52
12V
D4
T6
BC337-40
GND_12
R36
16k
O11
PC817
R34
220R
Pas_vyp
GND_5
Relé - pás zap
K10
ARK500/3
R39
rele FInder 40.52
D5
T7
BC337-40
R37
16k
O12
PC817
R35
220R
Pas_zap
Napájení
Napajeni
5V
GND_5
12V
GND_12

B3. Schéma zapojení ovládacího panelu