

ZÁPADOČESKÁ UNIVERZITA V PLZNI

---

Fakulta elektrotechnická  
Katedra elektroniky a informačních technologií

## DIPLOMOVÁ PRÁCE

Zvýšení spolehlivosti elektronických systémů architekturou jejich  
propojování

Autor práce: **Bc. Matěj Zeman**  
Vedoucí práce: **Ing. Ivo Veřtát, Ph.D.**

---

2022

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta elektrotechnická  
Akademický rok: 2022/2023

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Bc. Matěj ZEMAN**  
Osobní číslo: **E20N0056P**  
Studijní program: **N0714A060013 Elektronika a informační technologie**  
Specializace: **Elektronika**  
Téma práce: **Zvýšení spolehlivosti elektronických systémů architekturou jejich propojování**  
Zadávající katedra: **Katedra elektroniky a informačních technologií**

## Zásady pro vypracování

1. Popište problematiku zajištění spolehlivosti obecného elektronického systému, kde je potřeba procesorem obsluhovat různé senzory na společné sběrnici.
2. Navrhněte způsob propojení několika vývojových desek mikrokontrolérů a senzorů s cílem zvýšit spolehlivost a realizujte praktickou ukázkou takového elektronického systému.
3. Demonstrujte schopnost navrženého elektronického systému vypořádat se s poruchami mikrokontrolérů i senzorů se zachováním co největší funkcionality.


Rozsah diplomové práce: **40 – 60**  
Rozsah grafických prací: **dle doporučení vedoucího**  
Forma zpracování diplomové práce: **elektronická**

Seznam doporučené literatury:

1. VOBORNÍK, A., VEŘTÁT, I., LINHART, R. Experimental electric power system for small satellites with independent supply channels. In International Conference on Applied Electronics (AE 2018) : /proceedings/. Pilsen: University of West Bohemia, 2018. s. 155-161. ISBN: 978-80-261-0721-7 , ISSN: 1803-7232.
2. GANSSELE, J. A Designer's Guide to Watchdog Timers. Accessible online – <https://www.digikey.com/en/articles/a-designers-guide-to-watchdog-timers>

Vedoucí diplomové práce: **Ing. Ivo Veřtát, Ph.D.**  
Katedra elektroniky a informačních technologií

Datum zadání diplomové práce: **7. října 2022**  
Termín odevzdání diplomové práce: **26. května 2023**



L.S.

---

**Prof. Ing. Zdeněk Peroutka, Ph.D.**  
děkan



---

**Doc. Ing. Jiří Hammerbauer, Ph.D.**  
vedoucí katedry

## **Abstrakt**

Návrh spolehlivých zařízení pro náročná prostředí, zejména pro kosmické mise, obnáší zdoluhavý proces vývoje a testování, kdy ke konci vývoje mohou být použité součástky nedostupné nebo zastaralé. Předkládaná práce realizuje návrh elektronického systému se zvýšenou spolehlivostí za použití běžně dostupných součástek. Návrh se skládá z desky propojující části systému rozhraním, které umožňuje odpojení selhaných částí. K této desce jsou připojeny jednotlivé desky mikrokontrolerů a senzorů. Navrhované řešení přináší zlevnění, zrychlení a zvýšení spolehlivosti vývoje.

## **Klíčová slova**

Spolehlivost, spolehlivá zařízení, náročná prostředí, kosmické mise, propojení mikrokontrolerů, modulární systém, redundantní systém, studená redundance, teplá redundance, mikrokontroler, FMEA

## **Abstract**

The design of reliable devices for harsh environments, particularly for space missions, involves a long process of development and testing, during which the components used may become unavailable or outdated when reaching the end of the development cycle. The presented work proposes an electronic system that enhances reliability while using commonly available components. The design consists of a board that connects different parts of the system through an interface, which allows to disconnect faulty components. Individual microcontroller and sensor boards are connected to this board. The proposed solution brings cost reduction, acceleration, and increased reliability to the development process.

## **Key Words**

Reliability, reliable devices, harsh environments, space missions, microcontroller interconnection, modular system, redundant system, cold redundancy, warm redundancy, microcontroller, FMEA

## **Poděkování**

Tímto bych rád poděkoval vedoucímu diplomové práce Ing. Ivo Veřtátovi, Ph.D, za cenné profesionální rady, připomínky a metodické vedení práce.

# Obsah

Úvod.....	- 1 -
1 Vliv radiace na elektronický systém.....	- 2 -
1.1 Total Ionizing Dose.....	- 2 -
1.2 Single Event Effects.....	- 4 -
1.2.1 Single-Event Transients.....	- 4 -
1.2.2 Single-Event Upsets.....	- 6 -
1.2.3 Single-Event Functional Interrupts.....	- 9 -
1.2.4 Single-Event Latch-up.....	- 10 -
1.2.5 Single-Event Burn-out.....	- 12 -
1.2.6 Single-Event Gate Rupture.....	- 12 -
2 Ochrana elektronického systému vůči vlivům radiace.....	- 13 -
2.1 Fyzická radiační ochrana.....	- 13 -
2.1.1 Technologie Epi-bulk.....	- 13 -
2.1.2 Technologie Silicon on Insulator.....	- 14 -
2.2 Logická radiační ochrana.....	- 14 -
2.2.1 Redundantní systém.....	- 15 -
2.2.1 TMR.....	- 16 -
2.2.2 WDT.....	- 17 -
2.3 Softwarová radiační ochrana.....	- 18 -
3 Způsob vyhodnocování spolehlivosti elektronického systému.....	- 19 -
3.1 Příklad implementace Design FMEA.....	- 20 -
3.1.1 Sepsání jednotlivých komponentů k analýze ze schématu.....	- 20 -
3.1.2 Přiřazení možných poruch ke každému komponentu.....	- 21 -
3.1.3 Přiřazení důsledků ke každé z poruch.....	- 22 -
3.1.4 Vyhodnocení závažnosti, pravděpodobnosti, detekce poruchy.....	- 23 -
3.1.5 Výpočet RPN.....	- 26 -
4 Návrh systému.....	- 28 -
5 Elektrické schéma.....	- 30 -
5.1 Historie změn.....	- 32 -

5.2	Blok napájení.....	- 34 -
5.3	Blok zpoždění.....	- 38 -
5.4	Blok regulátoru napětí.....	- 39 -
5.5	Blok Mikrokontroleru .....	- 40 -
5.6	Blok I2C periferie.....	- 43 -
6	Návrh DPS.....	- 44 -
7	Demonstrační program .....	- 47 -
7.1	Init .....	- 48 -
7.2	Master-Slave.....	- 48 -
7.3	Init_Master .....	- 48 -
7.4	I2C_Diag .....	- 49 -
7.5	I2C_assign.....	- 50 -
7.6	Main_Master .....	- 50 -
7.7	Init_Slave .....	- 50 -
7.8	Main_Slave.....	- 50 -
8	Výsledky měření.....	- 51 -
8.1	Reakční doba zkratu mikrokontroleru.....	- 51 -
8.2	Reakční doba zkratu I2C periferie .....	- 52 -
8.3	Porucha na I2C konektoru.....	- 52 -
8.4	Ochrana podpětí .....	- 53 -
9	FMEA .....	- 54 -
9.1	Výpočet poruchovosti rezistorů .....	- 55 -
9.2	Výpočet poruchovosti bočníku.....	- 56 -
9.3	Výpočet poruchovosti kondenzátorů.....	- 57 -
9.4	Výpočet poruchovosti integrovaných obvodů s počtem tranzistorů < 1000 .....	- 58 -
9.5	Výpočet poruchovosti univerzálních diod.....	- 59 -
9.6	Výpočet poruchovosti výkonových integrovaných obvodů.....	- 60 -
9.7	Výpočet poruchovosti mikrokontrolerů .....	- 61 -
9.8	Výpočet poruchovosti MOS tranzistorů.....	- 62 -
9.9	Vyhodnocení výsledků FMEA.....	- 63 -
10	Současný stav a doporučení dalšího vývoje .....	- 64 -
10.1	Hardware .....	- 64 -



10.2	Software.....	- 65 -
	Zhodnocení a závěr.....	- 67 -
	Literatura.....	- 68 -

## Seznam symbolů a zkratek

Značka	Popisek	Jednotka
<i>BJT</i>	Bipolar Junction Transistor (bipolární tranzistor)	
<i>BOM</i>	Bill of materials (seznam součástek)	
<i>CAN</i>	Controller Area Network	
<i>CMOS</i>	Complementary Metal–Oxide–Semiconductor	
<i>DPS</i>	Deska Plošných Spojů	
<i>ECC</i>	Error-Correcting Code (kód pro opravu chyb)	
<i>EDAC</i>	Error Detection And Correction (detekce chyby a následná oprava)	
<i>FET</i>	Field-Effect Transistor	
<i>FMEA</i>	Failure Mode and Effect Analysis (analýza možného výskytu a vlivu poruch)	
<i>FRAM</i>	Ferroelectric Random Access Memory	
<i>GPIO</i>	General Purpose Input and Output (univerzální vstupní/výstupní pin)	
<i>MLC</i>	Multi-level Cell (Buňka uchovávající dva bity)	
<i>MOSFET</i>	Metal Oxide Semiconductor Field Effect Transistor	
<i>MRAM</i>	Magnetoresistive Random-Access Memory	
<i>MTBF</i>	Mean Time Between Failures (střední doba mezi poruchami)	[h]
<i>NFET</i>	N-channel FET	
<i>NMI</i>	Non-Maskable Interrupt (nemaskovatelné přerušení)	
<i>PFET</i>	P-channel FET	
<i>RPN</i>	Risk Priority Number (rizikové číslo)	
<i>SEB</i>	Single-Event Burn-out	
<i>SEE</i>	Single-Event Effects	
<i>SEFI</i>	Single-Event Functional Interrupts	
<i>SEGR</i>	Single-Event Gate Rupture	
<i>SEL</i>	Single-Event Latch-up	
<i>SET</i>	Single-Event Transients	
<i>SEU</i>	Single-Event Upsets	
<i>SLC</i>	Single-Level Cell (Buňka uchovávající jeden bit)	
<i>SOI</i>	Silicon On Insulator	
<i>SRAM</i>	Static Random Access Memory	
<i>TLC</i>	Triple-level Cell (Buňka uchovávající tři bity)	
<i>TMR</i>	Triple modular redundancy (trojitá redundance modulů)	
<i>WDT</i>	Watchdog timer (Hlídací časovač)	
$\lambda$	Poruchovost zařízení	$\left[ \frac{\text{Poruch}}{10^6 \text{h}} \right]$
$\tau$	Časová konstanta	[s]

## Úvod

Návrh spolehlivých zařízení pro náročná prostředí, zejména pro kosmické mise, obnáší zdoluhavý proces vývoje a testování. Na druhou stranu životní cyklus moderních mikrokontrolerů a senzorů je velice rychlý. Může se tak stát, že v době dokončení návrhu nejsou již některé z použitých součástek dostupné, anebo jsou součástky svými parametry zastaralé. Taková situace značně zpomaluje inovaci a zvyšuje finanční náklady.

Pro snížení nákladů a zvýšení rychlosti vývoje malých výzkumných satelitů je nezbytné používat běžné komerční součástky. Radiační odolnost běžných součástek závisí na mnoha faktorech a pro zjištění jejich spolehlivosti v kosmickém prostředí je nevhodnější testování radiační odolnosti. Zkušební testy součástek jsou však časově i finančně náročné, proto není možné je provádět pro každou použitou součástku a opakovaně pro každou novou generaci.

Existují vývojové a zkušební desky, které jsou svým rozložením pinů často kompatibilní po řadu generací. Tyto desky samy o sobě nemusí být odolné vůči radiaci, ale spolehlivost by mohla být zvýšena systémem zapojení, jako je redundantní systém nebo trojitá redundance modulů.

Navrhované řešení přináší zlevnění, zrychlení a zvýšení spolehlivosti vývoje. Sestává se z desky propojující části systému rozhraním, které umožňuje odpojení selhaných částí. Na tuto desku se postupně připojují jednotlivé desky mikrokontrolerů a senzorů. Tímto způsobem je možné rychle testovat nové generace součástek v malých satelitech, aniž by bylo nutné složitě upravovat layout desek.

Návrh upřednostňuje využití součástek, které mají delší životnost na trhu. Jelikož je deska navržena pro použití v řadě generací satelitů, je možné dosáhnout vyváženého poměru mezi náklady na testování a zajištění vysoké radiační spolehlivosti.

V budoucnosti by takovýto přístup mohl přispět k rozvoji kosmických misí a dalších aplikací vyžadujících spolehlivé zařízení v extrémních podmínkách.

## 1 Vliv radiace na elektronický systém

Zařízení operující ve vesmírném prostředí jsou vystavena náročným mechanickým, teplotním a radiačním podmínkám. [1] Obsah této kapitoly je zaměřen na mechanismy působení kosmického záření na elektronický systém a možné způsoby radiačních ochranných zařízení.

### 1.1 Total Ionizing Dose

Jevy spojené s TID, česky celkovou ionizační dávkou, nastávají v případě vystavení zařízení obsahujícího dielektrikum po dostatečně dlouhou dobu ionizujícímu záření. [1]

Při interakci ionizujícího záření s dielektrickým materiálem jsou v materiálu generovány páry elektronů a děr. Dielektrika jsou materiály s velmi nízkou elektrickou vodivostí. Pokud je dielektrikum vystaveno ionizujícímu záření, pohyb vzniklých elektronů a obzvláště děr uvnitř materiálu je tedy velmi malý. [1]

Není-li přítomné elektrické pole, nosiče náboje uvnitř materiálu postupně rekombinují. Pokud je přítomné elektrické pole, elektrony budou přitahovány k vyššímu potenciálu a díry, vzhledem k jejich velice nízké mobilitě, zůstanou uvnitř materiálu. Z důvodu přibývajících uvězněných děr uvnitř dielektrika získá materiál vystavený ionizujícímu záření postupem času kladný náboj. [1]

Jelikož ionizující záření nabíjí dielektrikum elektrickým nábojem, citlivost zařízení na TID závisí na celkovém objemu dielektrika, jeho umístění, intenzitě přítomného elektrického pole a okolní teplotě. [1, 2]

U CMOS tranzistorů vystavených radiaci vznikají defekty uvnitř oxidové izolační vrstvy, ve kterých mají díry opět nižší mobilitu a v defektech se tak hromadí. Důsledkem je pak posun prahového napětí sepnutí tranzistoru  $U_{GS}$ . [2]

S postupnou miniaturizací součástek, která přináší nižší operační napětí a tenčí vrstvy dielektrik je vliv TID snižován, ale stále není eliminován. Tabulka 1.1 ukazuje přehled radiační odolnosti CMOS součástek za použití rozdílných technologií výroby.

Tabulka 1.1 - Radiační odolnost CMOS součástek v závislosti na použité technologii výroby. [2]

Použitá technologie výroby	TID před selháním
> 1 $\mu\text{m}$	< 30 krad, v některých případech i < 3 krad
< 1 $\mu\text{m}$	< 100 krad
< 180 nm	> 100 krad (i při vyšší intenzitě radiace)
< 90 nm	~ 300 krad

Celková radiační odolnost součástky dále záleží na intenzitě radiace, které je součástka vystavena. Příkladem může být D-A konvertor DAC121S101QML-SP, který při dávce radiace nad 50 rad/s selže při celkové radiační dávce 30 krad, zatímco při dávce nižší jak 0.01 rad/s přežije součástka i přes 100 krad. Důvodem zvýšené radiační odolnosti při nízkých dávkách radiace je Self-annealing effect, což je efekt zapříčiňující částečné uzdravování defektů uvnitř oxidu tranzistoru v důsledku rekombinace. [2]

Bipolární technologie je ze své podstaty napříč použitými technologiemi výroby vůči TID málo odolná. Oxid používaný jako izolant u většiny bipolárních tranzistorů byl vyvinut pro optimalizaci výkonu součástky a z hlediska radiační odolnosti nemá dobré vlastnosti. Očekávaná TID před selháním u bipolární technologie je mezi 1 až 100 krad a celková radiační odolnost je obzvláště citlivá na řadu faktorů při výrobě. [2]

## 1.2 Single Event Effects

Pojem SEE označuje následky dopadu jednoho iontu s vysokou energií na elektronický systém. Na rozdíl od TID efektu, který se projeví až po delší době vystavení systému radiaci, se jedná o děj v rámci nanosekund. [1]

Podle následků lze SEE dle [1] dále dělit na:

- SET (Single-Event Transients)
- SEU (Single-Event Upsets)
- SEFI (Single-Event Functional Interrupts)
- SEL (Single-Event Latch-up)
- SEB (Single-Event Burn-out)
- SEGR (Single-Event Gate Rupture)

Pro pochopení příčiny SEE je potřeba porozumět mechanismům možného odvedení vzniklého náboje uvnitř polovodiče zasaženého iontem.

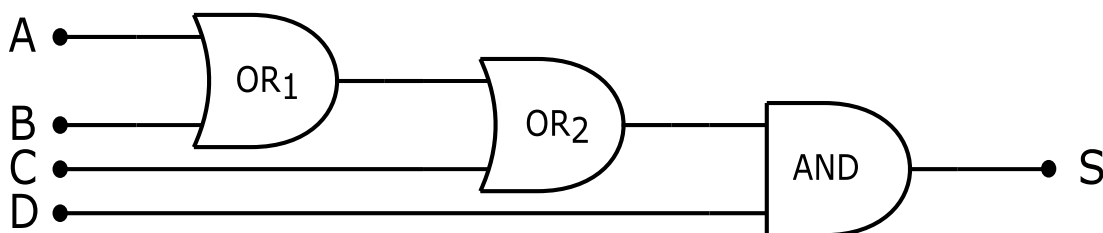
Ionty při průniku polovodičem ve své cestě vytváří shluky elektronů a děr. Bez přítomnosti vnějšího elektrického pole zůstanou nosiče blízko sebe, tudíž většina z nich rychle rekombinuje. Na kovových přívodech součástky se vlivem difúze může dostat malá část náboje, ta ovšem nemá dostatečnou energii pro ovlivnění elektronického systému. [1]

Pokud je přítomné elektrické pole, což je právě případem PN přechodu polovodičových součástek, vzniklé díry budou přitahovány k nejnižšímu potenciálu a elektrony k nejvyššímu potenciálu. Vzniklá separace elektronů a děr brání rekombinaci a z průniku iontu tedy v polovodiči zůstane velký náboj. Uvolnění náboje zapříčiní na přívodech součástky proudový impulz. V důsledku kapacity na výstupu elektronického systému vznikne z proudového impulzu impulz napěťový. Tyto impulzy pak mohou zapříčinit jeden ze zmíněných SEE. [1]

### 1.2.1 Single-Event Transients

SET značí jev, kdy důsledkem průchodu iontu součástkou dojde k napěťovému výkyvu na výstupu analogového obvodu, dočasné změně výstupní hodnoty logického obvodu, případně dočasné změně hodnoty uvnitř logického obvodu.

Jako příklad je uveden obvod tvořený dvěma OR a jedním AND členem zapojenými v sérii - Obr. 1.1. Uvažujme situaci, kdy vstupy obvodu A, B, C jsou ve stavu logická 0 a vstup D ve stavu logická 1. [1]



Obr. 1.1 – schéma logického obvodu tvořeného dvěma OR členy a jedním AND členem.  
Překresleno dle předlohy [1].

Pokud jeden z výstupních tranzistorů členu  $OR_1$  bude zasažen iontem, může na jeho výstupu dojít k napěťovému pulzu. Pokud tento napěťový pulz bude dosahovat dostatečně vysokého napětí a trvat po dostatečně dlouhou dobu, ovlivní výstup členu  $OR_2$ , na kterém se krátce objeví hodnota logická 1. V dalším kroku řetězce bude výstup členu  $OR_2$  společně se vstupem D vyhodnocen členem AND na výstupu celého systému S jako logická 1. [1]

Aby SET zapříčinil chybu, musí zásah iontu a následný způsobený napěťový pulz splnit několik kritérií:

- Pulz musí dosahovat dostatečně vysokého napětí a trvat po dostatečně dlouhou dobu, aby ovlivnil ostatní členy. Reálné logické členy mají omezenou šířku frekvenčního pásma a příliš krátké pulzy budou vyfiltrovány z důsledku fyzikálních vlastností členu. Nepřekoná-li pulz napětí pro rozlišení logické úrovně, taktéž nemůže ovlivnit další členy řetězce. V anglické literatuře se nesplnění tohoto kritéria označuje *Electrical masking*. [1]
- Následující člen řetězce, případně paměťová buňka, musí být schopen zachytit vzniklý pulz. Vznikne-li pulz na vstupu synchronního obvodu mimo citlivostní časové okno, nijak se neprojeví na výstupu. Takový případ je označován jako *Temporal masking*. [1]
- Iont musí zasáhnout citlivý člen. Pokud změna výstupu zasaženého členu nezmění výstup systému, nejedná se o citlivý člen. Takový případ je označován jako *Logical masking*. [1]

SET jevy můžou nastat i v analogovém obvodu. Příkladem mohou být napěťové pulzy na výstupu napěťového zesilovače. [1]

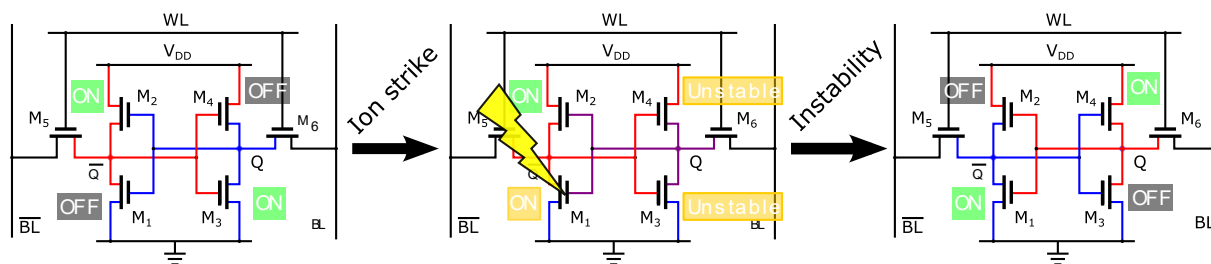
### 1.2.2 Single-Event Upsets

SEU označují korupci informace v důsledku zásahu iontem. Informace může být obsažena v jedné či více paměťových buňkách. K tomuto efektu typicky dochází, pokud iont zasáhne přímo paměťovou buňku, případně její blízké okolí, kdy zanechaný náboj naruší stav buňky. [1]

SEU může také nastat následkem SET, vznikne-li SET na periférii paměti během operace zápisu. Mechanismy SEU se odvíjejí od použité technologie paměťových buňek. [1]

Na Obr. 1.2 je naznačen případ SEU pro paměťovou buňku SRAM.

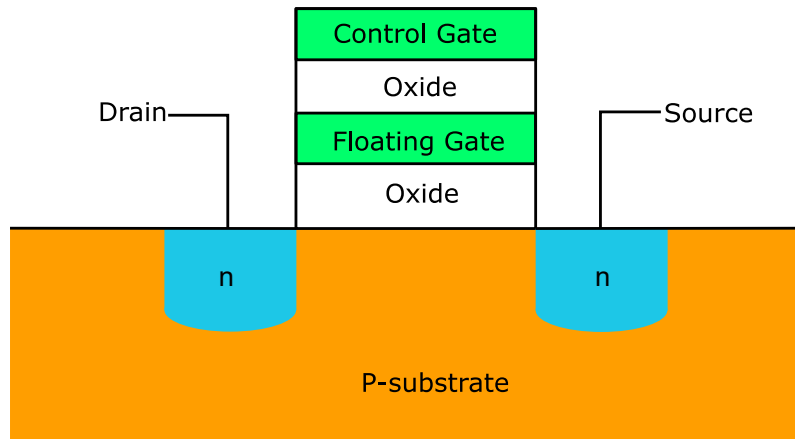
- První schéma reprezentuje SRAM buňku v ustáleném stavu. Červeně zvýrazněné vodiče mají vyšší potenciál a modře zvýrazněné vodiče nižší potenciál. Tranzistory  $M_2$  a  $M_3$  jsou tedy sepnuté a tranzistory  $M_1$  a  $M_4$  vypnuté. [1]
- Prostřední schéma představuje stav buňky při zasažení jednoho z vypnutých tranzistorů, v tomto případě  $M_4$ , iontem. Tranzistor je v důsledku nashromážděného náboje vzniklým proudovým pulzem sepnut. Sepnutí vyvolá na výstupu Q neznámé napětí v rozmezí mezi  $V_{DD}$  a zemí. Jelikož je Q vstupem invertoru tvořeného tranzistory  $M_1$  a  $M_2$ , výstup  $\overline{Q}$  nastane také nestabilní a působí kladnou zpětnou vazbou na vstup invertoru tvořeného tranzistory  $M_3$  a  $M_4$ . [1]
- Dva nestabilní invertory tvořící paměťovou buňku se mohou ustálit pouze ve dvou stavech. Buď se výstupy vrátí zpět do původního stavu, nebo jak je znázorněno na posledním schématu, se ustálí v opačném stavu. V případě ustálení buňky v opačném stavu nastává SEU a dochází ke korupci informace. [1]



Obr. 1.2 – příklad korupce dat (SEU) jedné paměťové buňky SRAM v důsledku zásahu iontu. Překresleno dle předlohy [1].

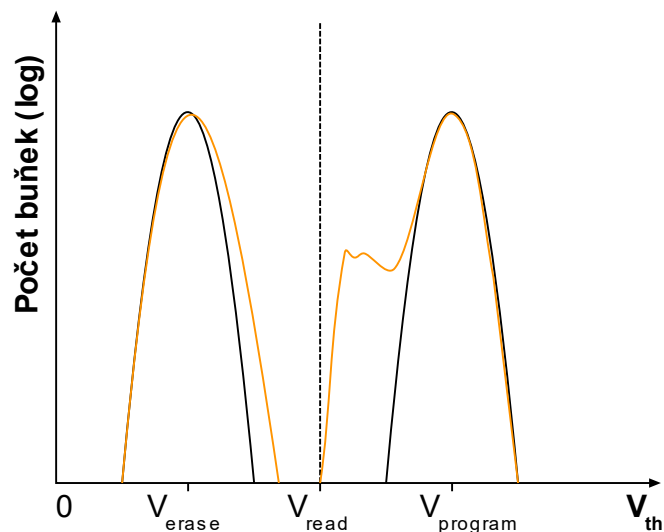


Paměti typu Flash mohou taktěž trpět efektem SEU. Flash paměťové buňky jsou tvořeny tranzistorem s plovoucím hradlem – floating-gate MOSFET. Informace je do buňky zapisována pomocí elektronů přivedených, případně odvedených z plovoucího hradla. Úroveň potenciálu plovoucího hradla určená přítomnými elektrony ovlivňuje prahové napětí sepnutí tranzistoru  $U_{GS}$ , čehož se využívá k vyčtení uložené informace. [1]



Obr. 1.3 – Průřez Flash paměťové buňky s floating-gate MOSFET strukturou. Překresleno dle předlohy [3].

Flash paměť obsahující data bude mít rozložení potenciálu jednotlivých prahových napětí tranzistorů odpovídající černému průběhu na Obr. 1.4.

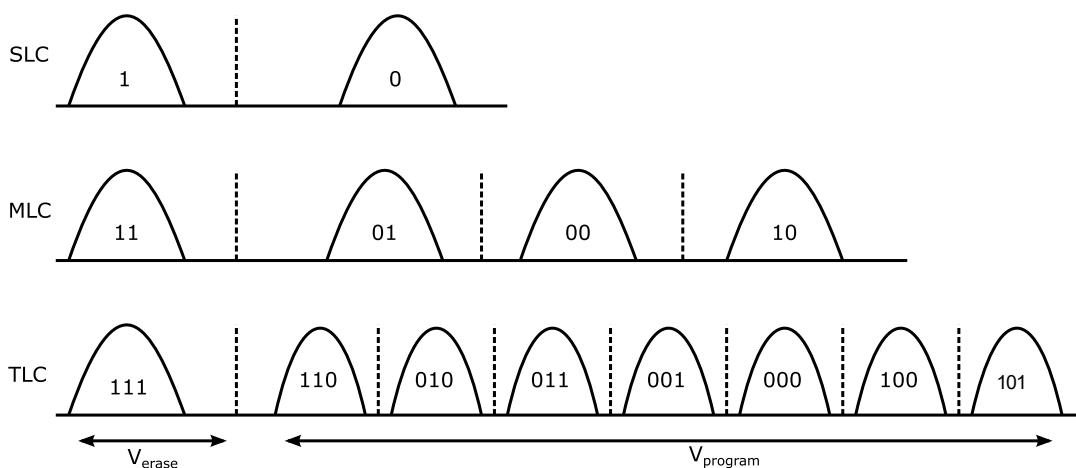


Obr. 1.4 – Rozložení prahového napětí paměťových buněk před zásahem iontem (černá) a po zásahu iontem (oranžová). Překresleno dle předlohy [1].

V důsledku zasažení paměťové buňky iontem bude prahové napětí zasažených tranzistorů posunuto ke střednímu napětí  $V_{read}$ , což se na rozložení napětí projeví jako oranžový průběh.

Přesáhne-li prahové napětí buňky hranici  $V_{read}$ , bude informace uvnitř buňky v případě přečtení buňky vyhodnocena špatně, dochází ke korupci dat a nastane tedy SEU. [1]

Paměťové buňky uchovávající jeden bit informace jsou nazývány SLC – Single Level Cell. Paměťová buňka může uchovávat i více bitů, kdy v případě MLC jsou v jedné paměťové buňce uloženy 2 bity a v případě TLC dokonce 3 bity. SEU u takových buněk představuje o to častější a závažnější problém. [3]



Obr. 1.5 - Rozložení prahového napětí paměťových buněk SLC, MLC a TLC. Překresleno dle předlohy [3].

Mechanismus způsobující SEU u Flash paměti není doposud prokázán, ale jako nejpravděpodobnější důvody [1] uvádí:

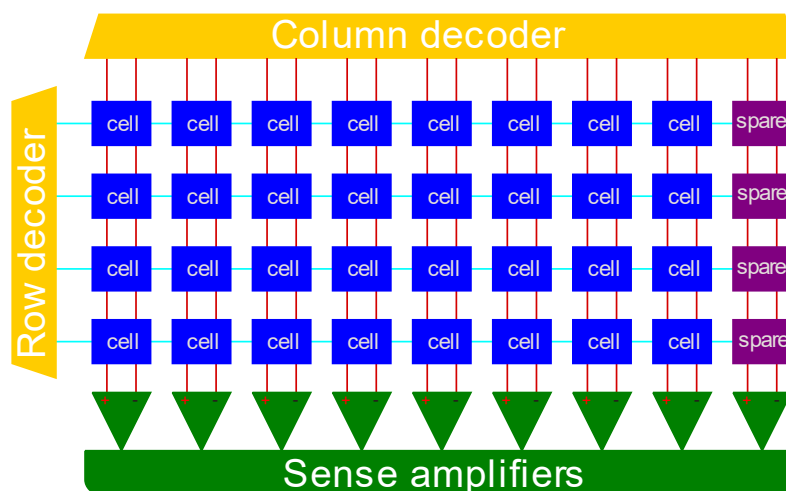
- Zásahem iontu dojde k vytvoření dočasné vodivé cesty v izolačním oxidu plovoucího hradla tranzistoru, což umožní odvedení náboje.
- Elektrony obsažené v plovoucím hradle tranzistoru jsou zásahem iontu excitovány, což jim dodá dostatečnou energii, aby mohli principem tunelování opustit bázi.
- Zásahem iontu se v okolí hradla zachytí pozitivní náboj.

Některé technologie paměti jsou vůči SEU z fyzikálního hlediska odolné. Na rozdíl od uvedených typů paměti totiž nevyužívají pro uchování informace elektrický náboj. Mezi takové paměti patří například FRAM, či MRAM. U těchto paměti je slabým článkem z hlediska odolnosti při zásahu iontem periferie obsluhující paměťové buňky, tradičně realizovány CMOS technologií. [1, 4]

### 1.2.3 Single-Event Functional Interrupts

Pokud iont zásahem paměťových periférií zapříčiní SET či SEU v kritickém místě, mohou se tyto obvody dostat do stavu, kdy nemohou dále vykonávat jejich určenou funkci. Takový případ je nazýván SEFI. Následky SEFI se liší napříč zařízeními, neboť jsou velmi závislé na designu daného zařízení.

Pro příklad je uvedeno následující zjednodušené schéma paměťového bloku:



Obr. 1.6 – Zjednodušené schéma paměťového bloku obsahujícího čtyři 8bit slova a jeden sloupec. Překresleno dle předlohy [1].

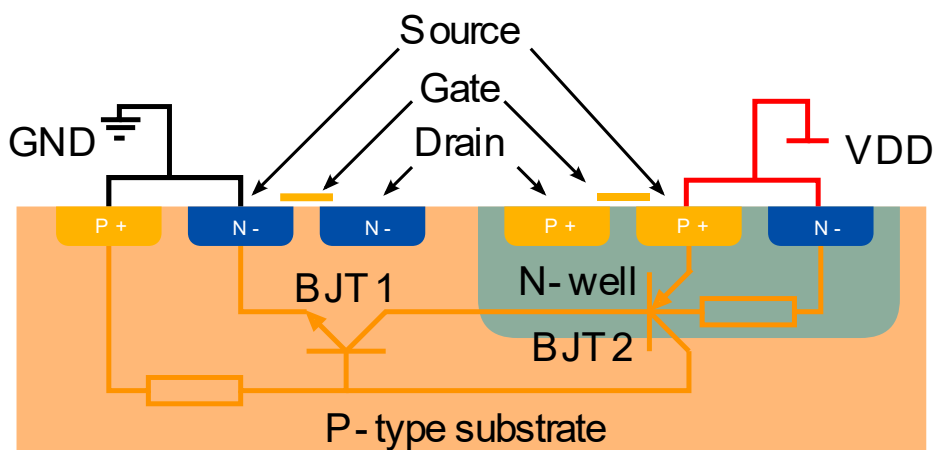
Přestože účelem paměťového bloku na Obr. 1.6 je uchovat pouze čtyři 8bit slova, je běžným zvykem výrobců realizovat blok s přidáním sloupců (případně i řádků, což je v ukázce vynecháno). Využití těchto redundantních sloupců nastává při výrobě. Pokud se při testování výrobku odhalí vadný sloupec paměti, což není neobvyklé, výrobce může na místo vadného sloupce přiřadit jeden z redundantních, čímž je paměť zachráněna od následné likvidace. [1]

Přiřazování redundantních sloupců je v propojovací matrixě buněk realizováno například nastavitelnými pojistkami a antipojistkami, které mohou být nastavitelné elektronicky či laserem. Některé zřízení mají ovšem možnost programového přiřazování, pro které je vyhrazena vnitřní energeticky nezávislá paměť (oddělena od běžně používané paměti). Při každém zapnutí zařízení se informace z této vnitřní paměti nahraje do registrů řídicích obvodů pro sestavení požadovaného propojení matrixě zbytku paměti. [1]

Pokud dojde k SEU právě v jednom z těchto registrů, dojde k relokaci jednoho z redundantních sloupců. Data obsažená v originálním sloupci budou tudíž nahrazena náhodnými daty z redundantního sloupce a při každém adresování tohoto bloku paměti budou přečtena chybná data. [1]

### 1.2.4 Single-Event Latch-up

SEL nastává v případě, že průletem iontu a následným depozitem náboje je uvnitř součástky umožněno vytvoření parazitní PNPN struktury (tyristor). Tím se vytvoří soběstačná vodivá cesta mezi přívody na různých potenciálech. Polovodičem pak mohou protékat vysoké proudy bez možnosti říditelnosti.



Obr. 1.7 – Průřez typické CMOS struktury se schématickým znázorněním parazitních součástek. Překresleno dle předlohy [1].

Obr. 1.7 představuje typické uspořádání N a P typů polovodiče pro vytvoření CMOS struktury – v tomto případě realizované na polovodičovém substrátu typu P. Z uspořádání vzniknou dva parazitní bipolární tranzistory – BJT: u NFET vznikne NPN tranzistor BJT<sub>1</sub> mezi source (jakožto emitor), vrstvou N-well (jakožto kolektor) a substrátem typu P (jakožto báze). Druhý PNP tranzistor BJT<sub>2</sub> u PFET mezi source (jakožto emitor), substrátem typu P (jakožto kolektor) a vrstvou N-well (jakožto báze). Báze parazitického BJT<sub>1</sub> je vodivě spojena s elektrodou na potenciálu GND, ale vzhledem k relativně vysokému odporu substrátu a přechodu křemíku s elektrodou, má toto spojení velký odpor. To samé může být řečeno o bázi BJT<sub>2</sub> spojené s VDD. [1]

Pokud iont zasáhne vrstvu N-well, zanechané elektrony budou přitahovány k N+ elektrodě s potenciálem VDD a díry rekombinují s majoritními nosiči ve vrstvě N-well. Pokud zásah iontu zanechá dostatek elektronů, jejich pohybem skrz vrstvu N-well, která má kvůli slabé dotaci vysoký odpor, vznikne napěťový úbytek. Bude-li úbytek dostatečný, začne u PFET source emitovat díry skrz vrstvu N-well do substrátu typu P, neboli PNP tranzistor sepne. Emitované díry putují P substrátem k P+ elektrodě s potenciálem GND. Bude-li děr dostatečné množství, jejich pohyb P substrátem způsobí díky vysokému odporu P substrátu napěťový nárůst a source NFET začne emitovat elektrony skrz P substrát do vrstvy N-well

a dále do N<sup>+</sup> elektrody na potenciálu VDD. Nyní už každý z parazitních bipolárních tranzistorů dodává minoritní nosiče do báze toho druhého. Tím vzniká kladná zpětná vazba, která dovoluje tok proudu z elektrody s potenciálem VDD do elektrody s potenciálem GND, a to naprosto mimo hradlo MOS tranzistorů. To má za následek, že proud způsobený tímto jevem nemůže být řízen napětím přivedeným na hradlo MOS tranzistorů. Vypnout parazitické bipolární tranzistory je pak možné pouze dostatečným snížením (nebo přímo vypnutím) napájecího napětí VDD. [1]

Pravděpodobnost vzniku SEL se zvětšuje s nárůstem teploty součástky a energie iontu. [1]

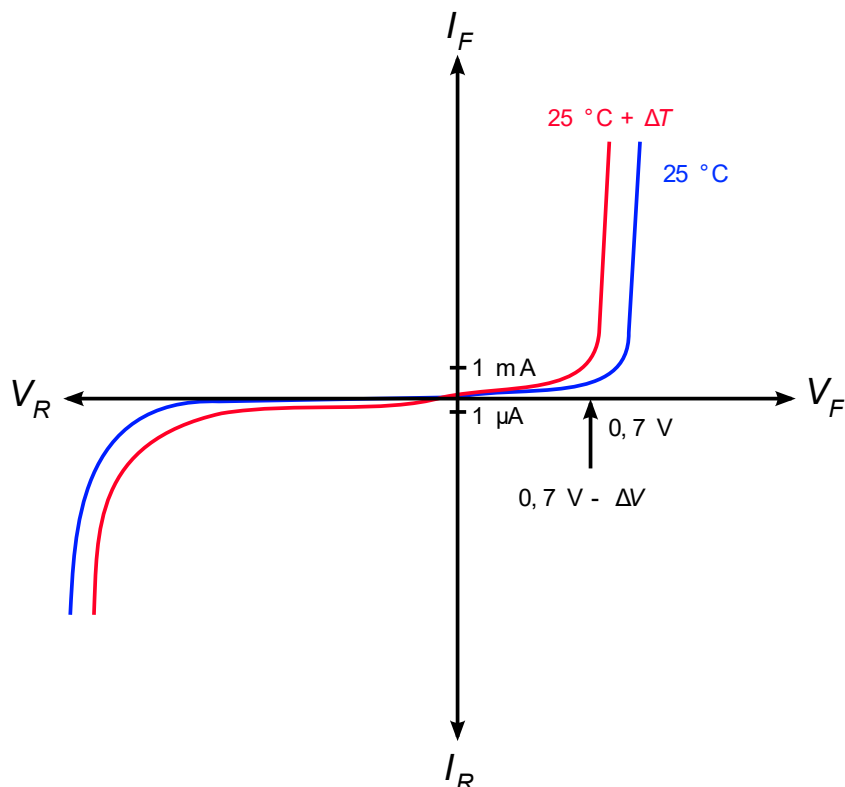
Součástky je do jisté míry možno chránit externě. Do série s napájením může být vložena proudová pojistka, která při nadměrném proudu přeruší napájecí napětí. Jelikož ale v důsledku SEL mohou nastat proudy různých velikostí, pojistka nemusí vždy zareagovat. [1]

Je ovšem možné vytvořit součástky technologií, která možnost SEL minimalizuje. Příkladem může být technologie SOI, která neobsahuje PNP strukturu nutnou pro vznik SEL. Za použití této technologie je každý tranzistor od sebe oddělený vrstvou oxidu. Další možností je použití Epi-bulk technologie za účelem snížení odporu substrátu. Tyto technologie jsou dále probírány v kapitole 2.1 - Fyzická radiační ochrana.

Jevy typu SEL představují vážnou poruchu, která může vyústit až ke zničení součástky teplotním namáháním. [1]

### 1.2.5 Single-Event Burn-out

SEB nastává, pokud iont zasáhne PN přechod s přivedeným vysokým závěrným napětím. U výkonových diod nosiče vzniklé zásahem iontu (a následně i minoritní nosiče generované lavinovým efektem) lokálně zvýší teplotu polovodiče, což zapříčiní drastické zvýšení závěrného parazitního proudu diody. Zvýšený závěrný proud generuje další teplo, čímž je uzavřena kladná zpětná vazba. Výsledek může vyústit až ke zničení součástky teplotním namáháním, či v lepším případě zvýšeným závěrným proudem. [1]



Obr. 1.8 – Příklad vlivu zvýšené teploty  $\Delta T$  na velikost prahového napětí a závěrného proudu PN přechodu

### 1.2.6 Single-Event Gate Rupture

SEGR značí jev, kdy je dopadem iontu s vysokou energií trvale narušena vrstva oxidu sloužící jako izolant hradla tranzistoru. Takový jev způsobí navýšení svodového proudu, které může vést až k selhání součástky. [1]

## 2 Ochrana elektronického systému vůči vlivům radiace

Pro zařízení operující ve ztížených radiačních podmínkách představují TID a SEE, jejichž princip vzniku byl představen v kapitole 1, vážný problém. Právě proto je tato kapitola zaměřena na mechanismy ochrany vůči způsobeným chybám.

Obvodu se zvýšenou odolností vůči radiaci lze dosáhnout řešením softwarovým, hardwarovým, či použitím radiačně odolné technologie. Pro dosažení obvodu schopného spolehlivého provozu ve vesmírných podmínkách je vhodné zmíněné způsoby kombinovat.

### 2.1 Fyzická radiační ochrana

Principem fyzické radiační ochrany je zabránění vzniku SEE, případně jevům spojeným s TID. Běžně užívaná CMOS technologie je velmi náchylná na SEL i SEU jevy. Existují ovšem radiačně mnohem odolnější technologie výroby, mezi které patří například CMOS vyrobené za použití Epitaxial (Epi-bulk) technologie, nebo technologie Silicon on Insulator (SOI). [5]

Zvýšit odolnost zařízení vůči radiaci je možné i stíněním. V praxi ovšem řešení často naráží na nesplnitelné požadavky z hlediska váhy materiálů stínění s vysokým atomovým číslem. [6]

#### 2.1.1 Technologie Epi-bulk

Technologie Epi-bulk spočívá v růstu tenké krystalické vrstvy na substrátu formou Epitaxe. Taková vrstva může být ze stejného materiálu jako substrát, ale použity mohou být i materiály jiné. Mnoho zařízení vyžaduje strukturu vrstev různě dopovaného polovodiče, případně různých typů polovodiče. Tomu je tak hlavně ve výkonové elektronice, kdy se tato technologie ukazuje jako nejlepší řešení. [5, 7]

V kapitole 1.2.4 byl představen princip SEL, ve kterém hraje zásadní roli vysoký odpor substrátu. Za použití Epi-bulk technologie je možné vyrobit CMOS s vysoce dopovaným substrátem (tedy s nízkým odporem) a Epitaxí vytvořenou nízce dopovanou vrstvou nad ní (s vysokým odporem) pro samotnou strukturu součástky. Tímto způsobem je možné značně omezit výskyt SEL. [5, 7]

### 2.1.2 Technologie Silicon on Insulator

S příchodem SOI technologie bylo možné docílit při stejném napětí o 30 % rychlejších obvodů s až třetinovou spotřebou oproti běžné technologii výroby. Při použití nižších napětí je možné dosáhnout ještě lepších výsledků.

Těchto výsledků dosahuje SOI technologie snížením parazitní kapacity PN přechodu a kompletnímu oddělení jednotlivých tranzistorů dielektrikem (oxidem křemičitým). Dielektrickým oddělením tranzistorů tato technologie taktéž docílila vysoké odolnosti vůči SEE. [5]

Princip této technologie přináší i značné nevýhody. Izolační vrstva působí jako tepelný izolátor vůči substrátu a snižuje schopnost odvodu tepla z čipu. Teploty čipu pak mohou dosahovat vysokých hodnot, což ovlivní i výstupní voltampérové charakteristiky dané součástky. [8]

Izolační vrstva činí SOI technologii také méně odolnou vůči TID. [2]

## 2.2 Logická radiační ochrana

Logická radiační ochrana zajišťuje zachování funkčnosti systému při poruše. Zvýšení radiační ochrany lze docílit i za použití běžných součástek, a to použitím vhodného systému propojení (Redundantní systém, TMR), softwarových ochran (ECC) či použitím WDT, které by mohlo být zařazeno do obou ze zmíněných kategorií.



### 2.2.1 Redundantní systém

Redundantní systém zařizuje převzetí kontroly záložním systémem v případě selhání hlavního systému. Systém tedy musí vyhodnotit selhání hlavního systému a následně přepnout na systém záložní. Blokové schéma na Obr. 2.1 ukazuje příklad redundantního řídicího systému. Redundantní systém může být dle [9] rozdělen na tři druhy:

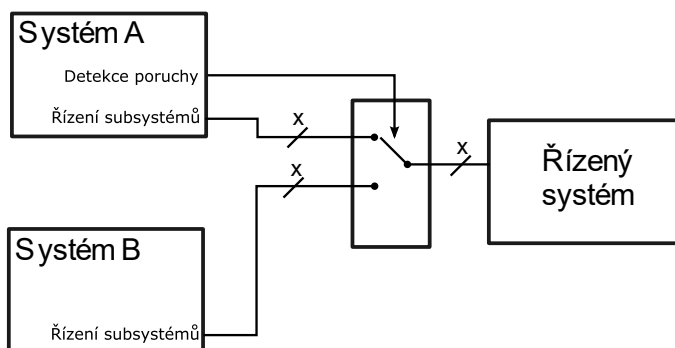
- horký (hot redundant)
- teplý (warm redundant)
- studený (cold redundant)

Při studené redundanci je záložní systém vypnutý, což v případě poruchy rozšiřuje časové okno bez kontroly systému. Záložní systém ale není při běžném provozu zařízení zatěžován, a tudíž se pravděpodobnost jeho poruchy před selháním hlavního systému blíží k nule. Studenou redundanci lze využít pro méně kritické aplikace, kdy ztráta kontroly nad systémem je po krátkou dobu přípustná. [9]

Systém s horkou redundancí v případě poruchy nesmí ztratit kontrolu nad řízeným systémem. Oba řídicí systémy po celou dobu provozu vykonávají stejnou funkci a jsou tedy i stejně zatěžovány. Horká redundance se využívá pro kritické aplikace, kde je ztráta říditelnosti nepřijatelná. Implementace je často mnohem složitější. [9]

Posledním způsobem je teplá redundance, kdy záložní systém je zapnutý, ale nevykonává stejnou funkci jako hlavní systém. Teplá redundance má oproti studené rychlejší reakci na poruchu, a tedy užší okno bez řízení systému. Záložní systém bude oproti hlavnímu systému méně namáhaný a je možné ho využít pro pokročilou diagnostiku. [9]

Při využití záložního systému u mikrokontrolerů je vhodným způsobem vyhodnocení poruchy WDT.

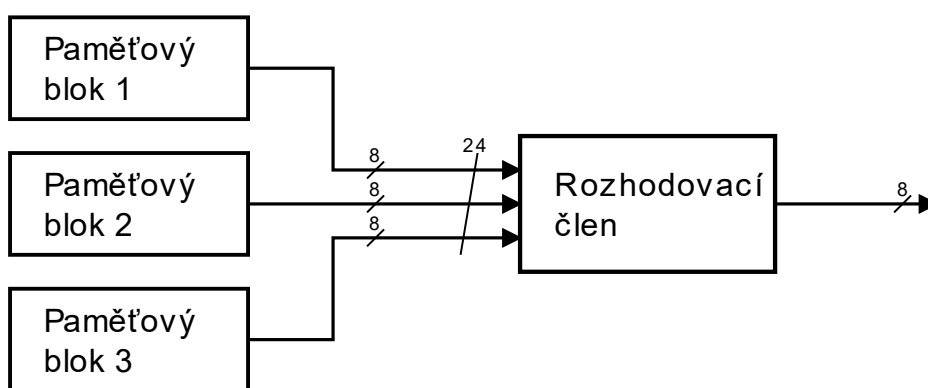


Obr. 2.1 – Blokové schéma principu redundantního systému

### 2.2.1 TMR

Triple Modular Redundancy, česky trojitá redundance modulů, je jednou z možných implementací horké redundance a často používaný způsob ochrany vůči SEU. Mechanismus této ochrany spočívá v použití třech stejných modulů plnících identickou funkci a rozhodovacího členu. Příkladem může být použití třech identických bloků paměti na Obr. 2.2. Na výstupu rozhodovacího členu jsou majoritní data ze třech pamětí. Pokud v důsledku SEU jsou data jedné z pamětí poškozena, data na výstupu nebudou ovlivněna a je možné poškozená data v daném bloku následně opravit. [10]

Šance výskytu SEU na dvou pamětech zároveň je minimální a TMR tedy značně zvyšuje spolehlivost. Stále je ovšem možný vznik chyby v rozhodovacím členu, která by měla vlivem následné distribuce katastrofální následky. Je tedy vhodné pro rozhodovací člen použít radiačně odolnou technologii výroby. Hlavní nevýhoda TMR spočívá již v principu, a to potřeba velké redundance (v případě paměti dvakrát větší než užitečná data). [10]



Obr. 2.2 – Blokový diagram TMR implementace paměťové buňky.  
Překresleno dle předlohy [10].

### 2.2.2 WDT

Watchdog timer, česky hlídací čítač, je poslední záchranou v případě chyby kódu procesoru. Jedná se o hardwarový prvek, který hlídá průběh programu a v případě chyby vyvolá tvrdý reset. Chyba může být způsobena programem samotným, ale také v důsledku SEE. [11]

WDT musí být naprosto nezávislý na procesoru, jelikož se procesor může ocitnout v jakémkoliv stavu a stále nesmí narušit WDT. Po prvotním nastavení při startu programu by tedy WDT již nemělo být možné přeprogramovat. [11]

Některé WDT používají namísto resetu nemaskovatelné přerušení. Myšlenkou je, že část kódu vyvolaná přerušením zaznamená informace potřebné pro následnou analýzu chyby. Problém nastane, pokud procesor nebude vlivem chyby na NMI reagovat. Příkladem takové chyby může být narušené číslo ukazatele zásobníku. Mnoho procesorů v takovém případě nepřejde k procesu vyvolání přerušení. Mít k dispozici informace o procesu před chybou kódu je ovšem velice užitečné. V praxi se tedy může použít WDT, který vyšle NMI a spustí časovač, který po uplynutí přednastavené doby vyvolá tvrdý reset. Zareaguje-li procesor na NMI, má tedy dost času pro uložení potřebných informací před resetem. [11]

Pokud procesor ovládá potencionálně nebezpečný hardware, je velice důležité, aby WDT nezávisle na procesoru uvedl systém v případě chyby do bezpečného stavu. [11]

Moderní embedded systémy mají velice sofistikované periferie. V některých případech mohou být dokonce složitější než samotný procesor. Při chybě může dojít ke stavu, kdy se periférii odešle náhodný sled dat. Procesor pak nemusí být schopen uvést periférii opět do původního stavu. V takovém případě tuto funkci musí opět zařídit resetovací sekvence WDT. [11]

### 2.3 Softwarová radiační ochrana

Formou softwarové radiační ochrany je ECC – Error correcting code, česky kód pro opravu chyb. Kódovaná data umožňují detekci a opravu chyb v paměti způsobených ať už SEE nebo TID. Princip ochrany spočívá v přidání redundantních bitů. [3]

Nejjednodušším způsobem detekce chyby je přidání paritního bitu. Slovo je rozšířeno o jeden bit tak, aby součet všech bitů byl lichý (nebo sudý). V případě korupce jednoho bitu lze detekovat chybu, jelikož součet bitů bude sudý (případně lichý). Nelze však určit pozici chyby, a tudíž chybu není možné opravit. [3]

Pro opravu jedné chyby lze využít Hammingův kód, který využívá několika paritních bitů. Počet potřebných bitů vzhledem k datovým bitům lze vypočítat rovnicí:

$$2^p \geq d + p + 1, \quad (2.1)$$

kde  $d$  je počet datových bitů a  $p$  je počet paritních bitů. Pro 4 datové bity je tedy potřeba 3 paritních bitů. Paritní bity jsou v kódovém slovu rozmístěny na mocninách čísla 2 (1,2,4,8...). Zbytek pozic je vyplněn datovými bity. Pozice čísel je převedena do binární soustavy a výsledné pokrytí je určeno logickou operací AND mezi pozicí paritních a datových bitů. [3]

Tabulka 2.1 - Hammingův kód pokrytí

Pozice bitu – decimální		7	6	5	4	3	2	1
Pozice bitu - binární		111	110	101	100	011	010	001
Paritní / datový bit		Datový 4	Datový 3	Datový 2	Paritní 3	Datový 1	Paritní 2	Paritní 1
Pokrytí paritního bitu	p1	x		x		x		x
	p2	x	x			x	x	
	p3	x	x	x	x			

Následně je vypočítána sudá parita pro každý z paritních bitů. V případě dat 1100 budou sečteny datové bity na pozicích 1, 2 a 4. Výsledek (01) je lichý a paritní bit p1 tedy bude 1. Celé kódované slovo pak bude 1100001. V případě korupce jednoho bitu je možné vypočítat pomocí parit pozici chyby a slovo opravit. V případě dvou chyb Hammingův kód chybu detekuje, ale neopraví. [3]

Pro opravu vícebitových chyb může být Hammingův kód rozšířen, nebo mohou být použity cyklické BCH (Bose–Chaudhuri–Hocquenghem) kódy. [3]

### 3 Způsob vyhodnocování spolehlivosti elektronického systému

Velice účinným nástrojem pro definici, identifikaci a eliminaci známých či potenciálních poruch systému, je FMEA – Failure Mode and Effect Analysis, česky: analýza poruch a jejich důsledků. FMEA byla vytvořena americkou armádou v roce 1940 a dále zdokonalena NASA v průběhu mise Apollo. Její implementace je detailně popsána v knize D. Stamatis, Failure Mode and Effect Analysis [12].

FMEA je velice flexibilním nástrojem. Dle úrovně implementace se dále dělí na: System, Design, Process, Service a Machine FMEA. Pro vývoj nového elektronického zařízení je vhodná Design FMEA, která je hojně využívána v automobilovém průmyslu, letectví, zdravotnictví, ale i běžné výrobě. FMEA je často využívána pro vyhodnocení bezpečnosti systému, ale jednoduchou úpravou vyhodnocovacích tabulek je možné hodnotit spolehlivost systému. [12]

Na začátek je vhodné upřesnit několik pojmů, které jsou při implementaci často zaměňovány:

- Failure mode – Porucha – Způsob, jakým může zařízení selhat.
- Failure effect – Důsledek poruchy – Změna chování systému v důsledku poruchy.
- Cause of failure – Příčina vzniku poruchy.
- RPN – Rizikové číslo – Přiřazuje chybě číslo v závislosti na kritičnosti poruchy.

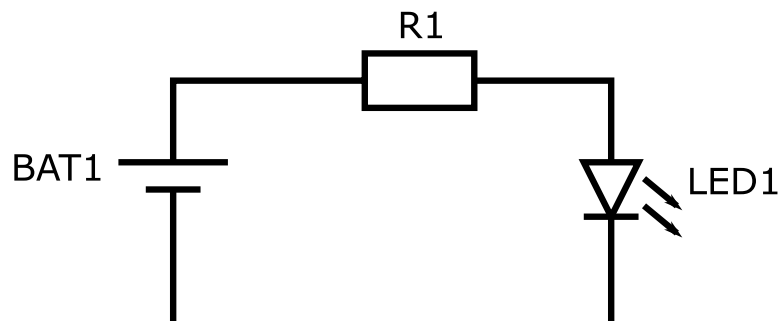
Správně implementovaná FMEA by měla dle [12] splnit následující body:

- Identifikace známých a potenciálních poruch
- Identifikace příčin a následků každé z poruch
- Prioritizace identifikovaných poruch v závislosti na závažnosti, pravděpodobnosti a detekci – RPN.
- Analýza poruch s RPN nad určenou kritickou mez a doporučení kroků ke zmírnění důsledků.

FMEA může být implementována v jakémkoliv stádiu vývoje produktu, včetně již produktů v sériové výrobě. Pro docílení největšího zrychlení procesu je však nutné implementovat FMEA již v prvotních fázích vývoje. FMEA může v takovém případě sloužit zároveň jako dokumentace vývoje produktu.

### 3.1 Příklad implementace Design FMEA

Příklad implementace FMEA procesu je představen na jednoduchém obvodu obsahujícím pouze tři součástky: Bateriový článek, rezistor a LED.



Obr. 3.1 - Jednoduché schéma pro ukázkou FMEA

#### 3.1.1 Sepsání jednotlivých komponentů k analýze ze schématu

Prvním krokem Design FMEA je sepsání prvků pro další analýzu. U elektronického zařízení bude seznam vycházet z BOM. U komplexních schémat je vhodné třídit komponenty do skupin podle bloků schématu. [12]

Tabulka 3.1 - Příklad FMEA – krok 1

Blok schématu	Komponent
Hlavní blok	R1
Hlavní blok	LED1
Hlavní blok	BAT1

### 3.1.2 Přiřazení možných poruch ke každému komponentu

U každého z komponentů může dojít k poruše různými způsoby. Druhým krokem je sepsání všech poruch, které mohou u komponentu nastat. Při tomto kroku je vhodné pro pokrytí širokého spektra příčin poruch uspořádat brainstorming lidí s různými zaměřenými.  
[12]

Tabulka 3.2 – Příklad FMEA – krok 2

Blok schématu	Komponent	Porucha
Hlavní blok	R1	Zkrat
Hlavní blok	R1	Rozpojený obvod
Hlavní blok	LED1	Zkrat
Hlavní blok	LED1	Rozpojený obvod
Hlavní blok	BAT1	Vybití akumulátoru
Hlavní blok	BAT1	Zkrat
Hlavní blok	BAT1	Rozpojený obvod

### 3.1.3 Přiřazení důsledků ke každé z poruch

Každá porucha může ovlivnit elektronický systém rozdílným způsobem. Pro zjištění důsledků na celý systém je vhodné využívat simulací, testů či předchozích zkušeností. [12]

Tabulka 3.3 - Příklad FMEA - krok 3

Blok schématu	Komponent	Porucha	Důsledek
Hlavní blok	R1	Zkrat	Diodou poteče vysoký proud – dojde k trvalému poškození. Baterie se začne zahřívat. Dioda nebude svítit.
Hlavní blok	R1	Rozpojený obvod	Dioda nebude svítit.
Hlavní blok	LED1	Zkrat	Dioda nebude svítit, obvod se bude dále vybíjet.
Hlavní blok	LED1	Rozpojený obvod	Dioda nebude svítit.
Hlavní blok	BAT1	Vybití akumulátoru	Dioda nebude svítit.
Hlavní blok	BAT1	Zkrat	Baterie se začne zahřívat.
Hlavní blok	BAT1	Rozpojený obvod	Dioda nebude svítit.



### 3.1.4 Vyhodnocení závažnosti, pravděpodobnosti, detekce poruchy

Pro vyhodnocení závažnosti, pravděpodobnosti, detekci poruch a radiační odolnosti součástky je potřeba vytvořit několik vyhodnocovacích tabulek.

Tabulky mohou být přizpůsobeny pro potřeby daného odvětví či zařízení - Tabulka 3.4 byla vytvořena pro vyhodnocení spolehlivosti zařízení, namísto častějšího vyhodnocování bezpečnosti zařízení. Tabulka 3.6 byla vytvořena pro vyhodnocení diagnostiky chyby a Tabulka 3.7 byla přidána pro zohlednění radiační odolnosti součástky. Aby mezi sebou mohly být porovnávány verze elektronického systému či podobné elektronické systémy, je třeba využívat pro FMEA stejných vyhodnocovacích tabulek.

Hodnotu závažnosti a detekce poruchy lze pomocí vytvořených tabulek vyhodnotit studováním schématu, případně přistoupením k simulaci a měření.

Radiační odolnost je možné v některých případech zjistit od výrobce součástek, nebo lze přistoupit k testu radiační odolnosti.

Vyhodnocení pravděpodobnosti poruchy lze docílit testováním součástek, využitím databáze nebo výpočtem.

Testování součástek vyžaduje specializované vybavení nejen pro samotný test, ale i pro následné zkoumání příčiny selhání. Vzhledem k časové a finanční náročnosti se k testování přistupuje pouze v nutných případech.

Existuje řada databází spolehlivosti součástek, tvořené z testů, případně dlouhodobého sběru dat o poruchovosti komponentů. Databáze jsou často zaměřeny na specifický segment elektronických systémů. Přístup ke zmíněným databázím je ovšem placený.

Poslední možností je výpočet spolehlivosti. Norma MIL-HDBK-217F [13], blízce spjatá s prvotním zavedením FMEA, poskytuje širokou řadu vzorců pro výpočet spolehlivosti komponentů.

Tabulka 3.4 - FMEA tabulka pro vyhodnocení závažnosti poruchy.

<b>Závažnost poruchy</b>	<b>Definice</b>	<b>Přiřazené číslo</b>
Velmi vysoká	Porucha způsobí katastrofické následky, které mohou poškodit přidružené systémy	10, 9
Vysoká	Porucha učiní zařízení zcela nefunkční	8,7
Střední	Porucha učiní část zařízení zcela nefunkční	6,5
Středně nízká	Porucha učiní redundantní část zařízení nefunkční, či omezí funkčnost části zařízení	4
Nízká	Porucha může snížit spolehlivost části zařízení	3, 2
Zanedbatelná	Porucha neovlivní činnost zařízení	1

Tabulka 3.5 - FMEA tabulka pro vyhodnocení pravděpodobnosti poruchy.

<b>Pravděpodobnost poruchy</b>	<b>Definice</b>	<b>Přiřazené číslo</b>
Velmi vysoká	Porucha je nevyhnutelná	10, 9
Vysoká	Často se vyskytující porucha	8,7
Střední	Občasná porucha	6,5,4
Nízká	Zřídka se vyskytující porucha	3,2
Nepravděpodobná	Porucha je velice nepravděpodobná	1

Tabulka 3.6 - FMEA tabulka pro vyhodnocení detekce poruchy.

<b>Detekce poruchy</b>	<b>Definice</b>	<b>Přiřazené číslo</b>
Měřením	Poruchu není možné detekovat automaticky a pro diagnostiku chyby je potřeba provést měření na desce.	3
Automatická pokročilá	Poruchu je možné detekovat pokročilou diagnostikou.	2
Automatická	Porucha je detekovaná automaticky, nebo porucha nemůže nijak ovlivnit chod systému	1

## ZPŮSOB VYHODNOCOVÁNÍ SPOLEHLIVOSTI ELEKTRONICKÉHO SYSTÉMU

Tabulka 3.7 - FMEA tabulka pro vyhodnocení radiační odolnosti součástky.

<b>Radiační odolnost součástky</b>	<b>Definice</b>	<b>Přiřazené číslo</b>
Špatná	Aktivní součástka se špatnou tolerancí vlivů radiace.	4
Běžná	Aktivní součástka s běžnou tolerancí vlivů radiace.	3
Dobrá	Aktivní součástka se zvýšenou ochranou proti vlivům radiace.	2
Vynikající	Pasivní součástka, nebo aktivní součástka s velmi vysokou ochranou proti vlivům radiace.	1

Tabulka 3.8 - Příklad FMEA – krok 4.

<b>Blok schématu</b>	<b>Komponent</b>	<b>Porucha</b>	<b>Důsledek</b>	<b>Závažnost</b>	<b>Pravděpodobnost</b>	<b>Detekce</b>
Hlavní blok	R1	Zkrat	Diodou poteče vysoký proud – dojde k trvalému poškození. Baterie se začne zahřívat. Dioda nebude svítit.	10	1	1
Hlavní blok	R1	Rozpojený obvod	Dioda nebude svítit.	7	2	1
Hlavní blok	LED1	Zkrat	Dioda nebude svítit, obvod se bude dále vybíjet.	8	3	1
Hlavní blok	LED1	Rozpojený obvod	Dioda nebude svítit.	7	2	1
Hlavní blok	BAT1	Vybití akumulátoru	Dioda nebude svítit.	7	10	1
Hlavní blok	BAT1	Zkrat	Baterie se začne zahřívat. Hrozí vznícení.	10	1	1
Hlavní blok	BAT1	Rozpojený obvod	Dioda nebude svítit.	7	3	1

### 3.1.5 Výpočet RPN

RPN – Risk Priority Number, česky Rizikové číslo slouží pro prioritizaci kritických poruch. RPN je dané součinem čísel přiřazených závažnosti, pravděpodobnosti, detekci poruchy a radiační odolnosti součástky.

$$RPN = Závažnost * Pravděpodobnost * Detekce * Radiační odolnost \quad (3.1)$$

Tabulka 3.9 - příklad FMEA – krok 5

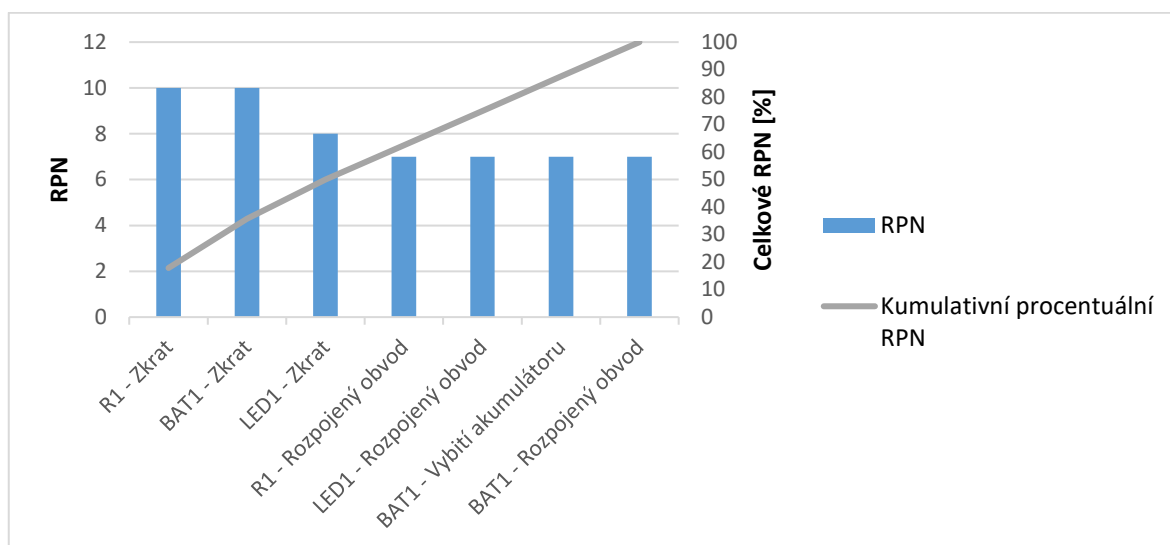
Blok schématu	Komponent	Porucha	Důsledek	Závažnost	Pravděpodobnost	Detekce	Radiační odolnost	RPN
Hlavní blok	R1	Zkrat	Diodou poteče vysoký proud – dojde k trvalému poškození. Baterie se začne zahřívat. Dioda nebude svítit.	10	1	1	1	10
Hlavní blok	R1	Rozpojený obvod	Dioda nebude svítit.	7	2	1	1	14
Hlavní blok	LED1	Zkrat	Dioda nebude svítit, obvod se bude dále vybíjet.	8	3	1	3	72
Hlavní blok	LED1	Rozpojený obvod	Dioda nebude svítit.	7	2	1	3	42
Hlavní blok	BAT1	Vybití akumulátoru	Dioda nebude svítit.	7	10	1	1	70
Hlavní blok	BAT1	Zkrat	Baterie se začne zahřívat. Hrozí vznícení.	10	1	1	1	10
Hlavní blok	BAT1	Rozpojený obvod	Dioda nebude svítit.	7	3	1	1	21

Dále lze vypočítat celkové RPN, kde:

$$Celkové RPN = \sum_{n=1}^{celkový\ počet\ poruch} RPN_n \quad (3.2)$$

Pro uvedený příklad by celkové RPN bylo 239. Výsledné celkové RPN je možné použít při vyhodnocování vlivu úprav schématu na celkovou spolehlivost elektronického systému, případně na porovnávání spolehlivosti podobných zařízení využívajících stejnou FMEA.

Dále lze poruchy pro přehlednost zobrazit formou Paretova diagramu, kdy nejkritičtější poruchy budou zobrazeny jako první.



Graf 3.1 - Příklad FMEA - Paretův diagram

Problémy jsou následně adresovány od nejkritičtějších, až po určenou hranici RPN, která bude záležet na dané aplikaci. Při každé modifikaci elektronického systému by se mělo vypočítat RPN a ujistit se, že změna nemá negativní vliv na celkové RPN. Cílem FMEA je vyvinout zařízení s co nejnižším celkovým RPN, kdy RPN každé z poruch je pod zvolenou hranicí.

## 4 Návrh systému

Vzhledem k zaměření systému na spolehlivost, spíše než bezpečnost, byl pro zvýšení spolehlivosti mikrokontrolerů vybrán princip studené, případně teplé redundance.

Namísto přepojení řídicích signálů mikrokontroleru multiplexorem v případě poruchy je blok mikrokontroleru oddělen od společných sběrnic a řídicích signálů až do potvrzení správné funkčnosti. Takový přístup umožňuje implementaci pokročilých módů. Příkladem může být využití mikrokontrolerů jako 2 výpočetních jader.

Správná funkčnost mikrokontroleru je vyhodnocena pomocí WDT. Mikrokontroler po potvrzení správné funkčnosti má možnost vypnout napájení druhého mikrokontroleru. V softwaru pak byla implementována funkce volby mezi studenou a teplou redundancí.

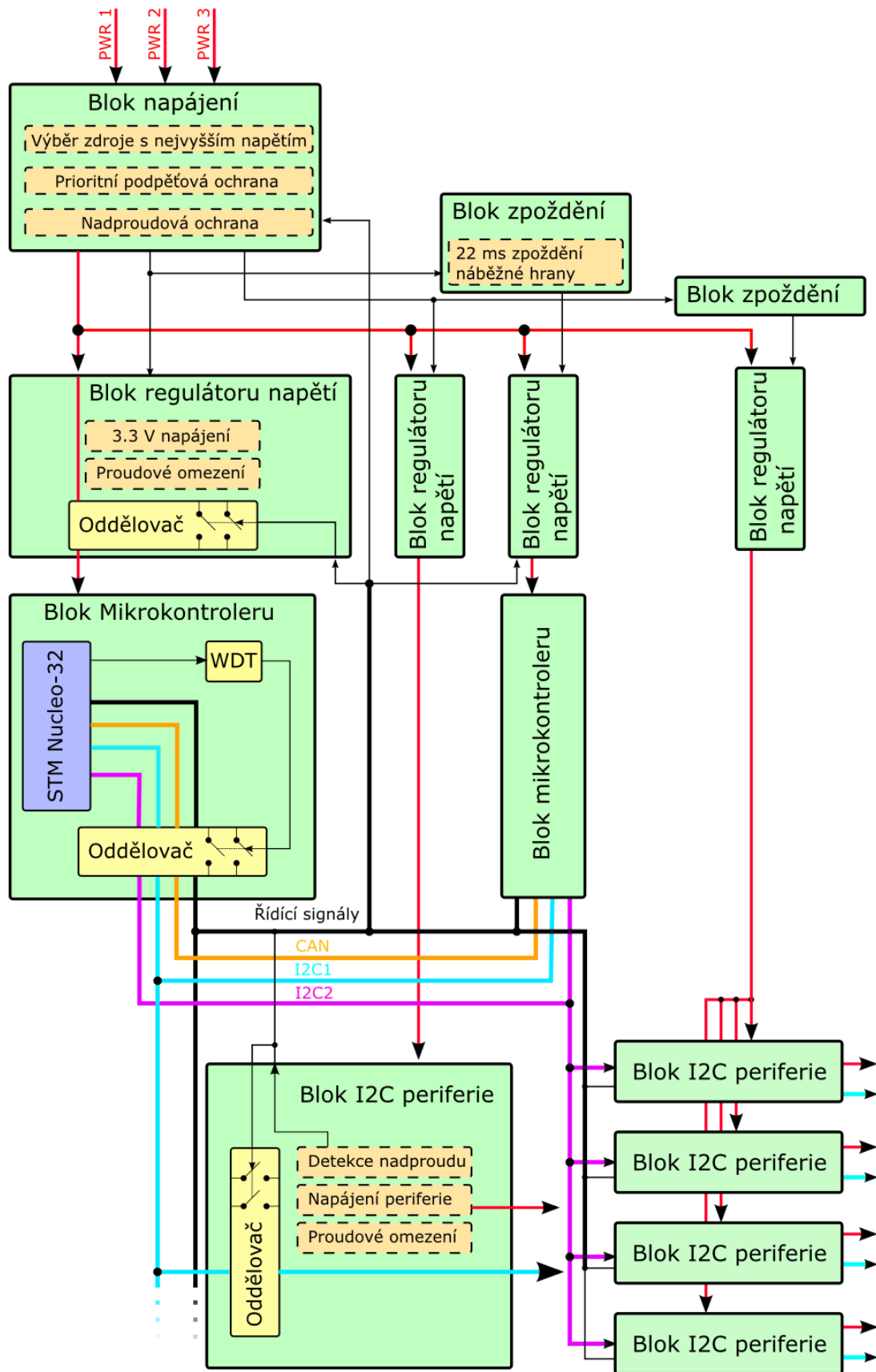
Systém je navržený pro STM desky Nucleo-32, které mají jednotnou velikost a rozložení pinů. Pro demonstraci systému byly vybrány mikrokontrolery STM32 Nucleo\_G431KB, které mají hardwarovou implementaci softwarové radiační ochrany – ECC pro Flash paměť a kontrolou paritních bitů pro prvních 16 kB SRAM. U vybraných mikrokontrolerů je tak možné docílit zvýšené radiační ochrany.

Periferie je možné k desce připojit pomocí I2C sběrnice. Každá z periférií má vlastní blok, který při poruše odpojí napájení a rozhraní I2C periferie. K desce je možné připojit 8 periférií rozložených mezi dvě I2C sběrnice. Na Obr. 4.1 je zobrazené zjednodušené schéma funkcí a propojení jednotlivých bloků.

Pro výběr součástek byly upřednostňovány součástky z napájecího zdroje a společného řešení ochran na satelitu PilsenCUBE [6], u kterých byla ověřena radiační odolnost na kobaltovém zářiči.

Výsledná navržená deska má za cíl poskytnout standardizovaný systém propojení se zvýšenou spolehlivostí. Díky standardizaci zapojení a použitých součástek je možné značně snížit poměr ceny testování a výsledné spolehlivosti systému. Tím může být u levných CubeSat satelitů docíleno vysoké spolehlivosti za použití běžných komponentů.

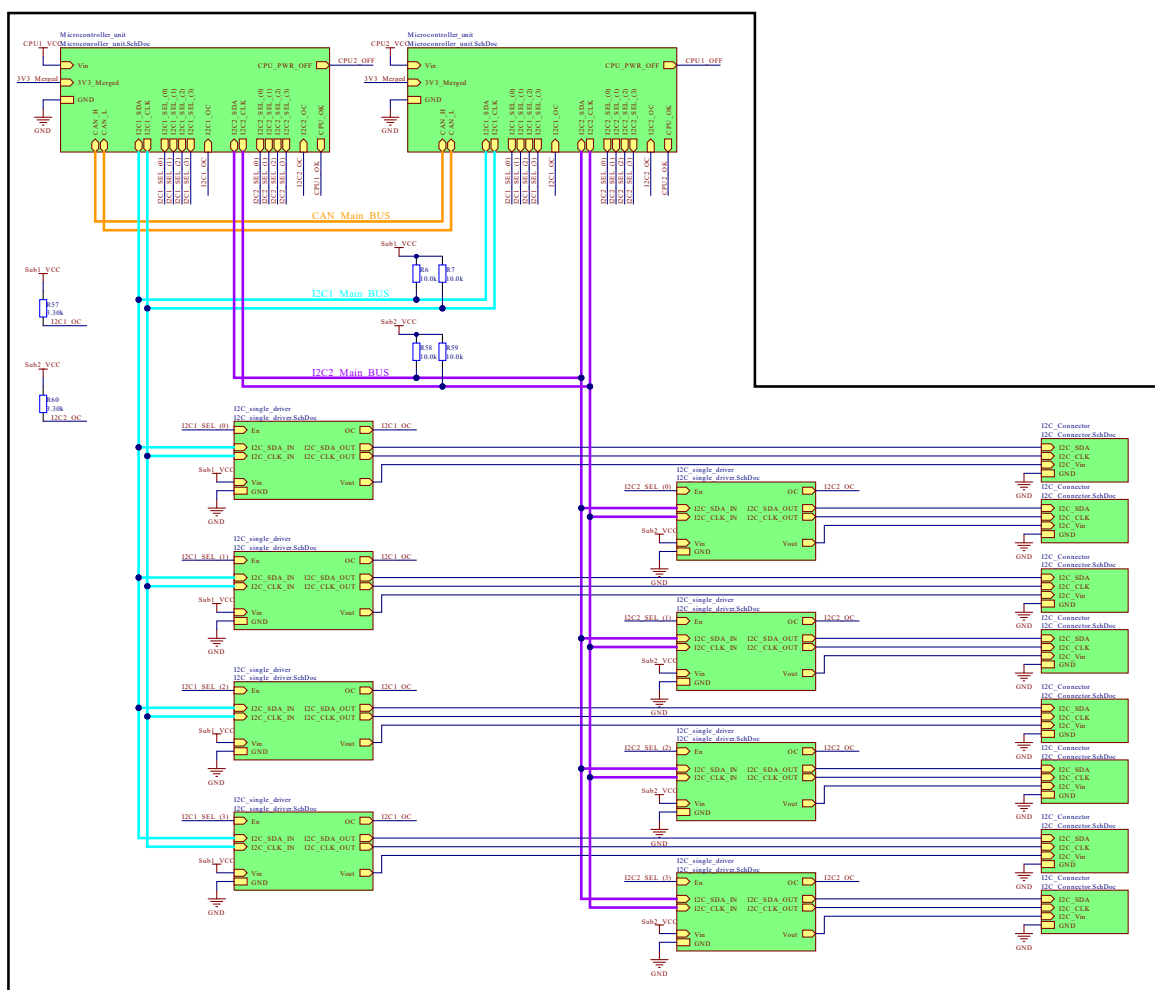
Navrhované řešení přináší zlevnění, zrychlení a zvýšení spolehlivosti vývoje.



Obr. 4.1 – Schéma funkcí elektronického systému

## 5 Elektrické schéma

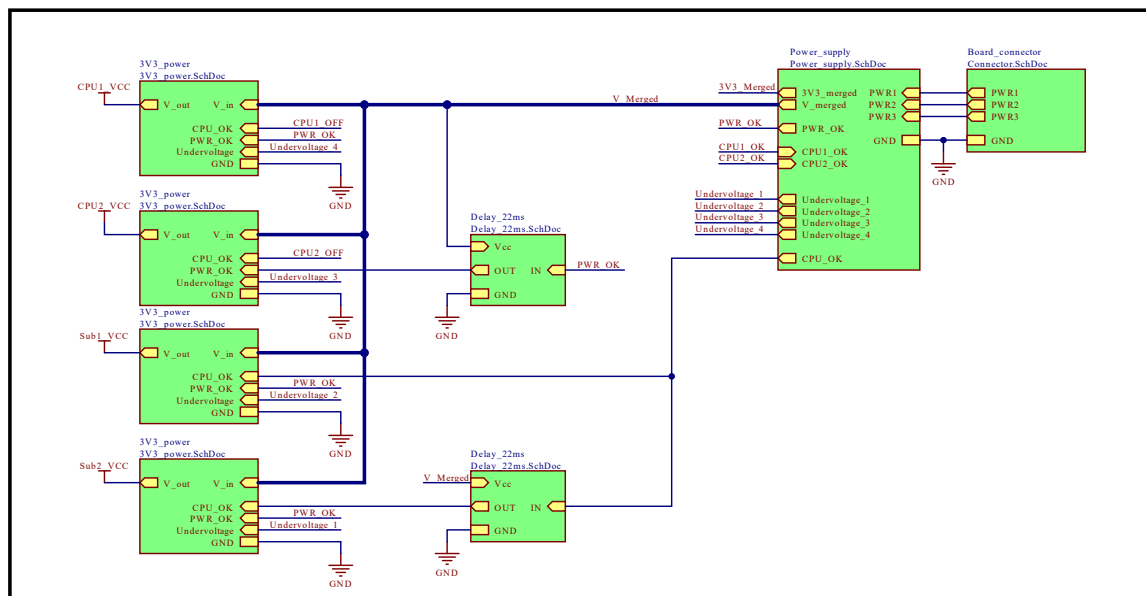
Předkládaný návrh elektronického systému umožňuje propojení dvou vývojových desek mikrokontrolerů STM32 s osmi I2C periferiemi při zachování co největší funkcionality systému v případě poruchy. Systém je schopný provozu v režimu studené a teplé redundance. Řada zapojení byla převzata nebo inspirována ze zdroje [6]. Návrh elektronického systému byl realizován v programu Altium. Soubory projektu jsou dostupné v elektronické příloze. Blokové schéma se skládá ze dvou částí.



Obr. 5.1 - Blokové schéma elektronického systému – část 1

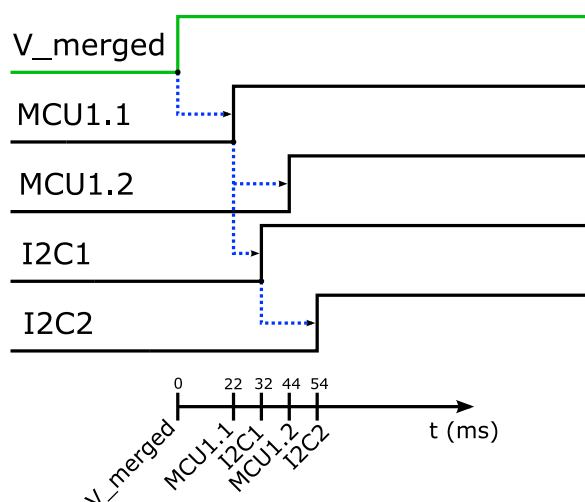
První blokového schéma obsahuje dva bloky mikrokontrolerů vzájemně propojených komunikačním rozhraním CAN. Každý z mikrokontrolerů má přístup ke sběrnicím I2C1 a I2C2 pro komunikaci s periferiemi, kdy přiřazení přístupu na I2C sběrnice je dané softwarovou implementací. Každá ze sběrnic I2C je rozdělena na 4 větve, pro celkovou podporu až osmi I2C periferií. Selhání jakékoliv z periferií vyřadí pouze ovlivněnou periferii. Stejně tak selhání mikrokontrolerů zapříčiní jeho odpojení od zbytku systému.



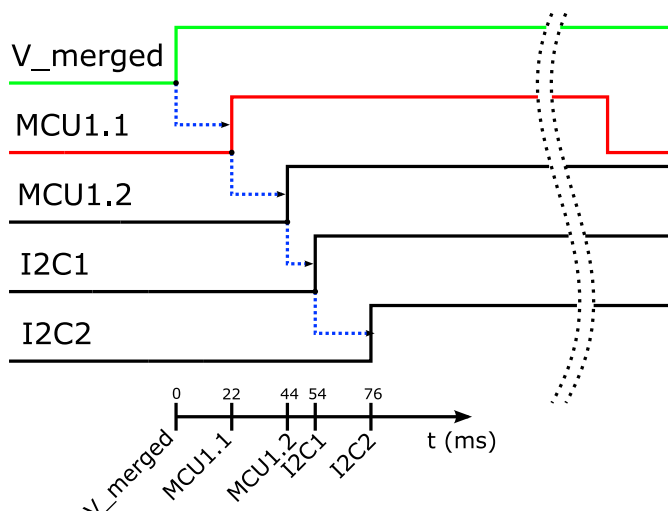


Obr. 5.2 - Blokové schéma elektronického systému – část 2

Druhá část blokového schéma poskytuje napájení pro celý systém. Pořadí zapínání systémů je zobrazeno na Obr. 5.3 a v případě poruchy MCU1.1 pak na Obr. 5.4. Zpoždřovací bloky umožňují rozložení proudových rázů při zapínání zařízení a poskytují MCU 1.1 časovou výhodu využívanou softwarem pro zavedení Master – Slave architektury mezi mikrokontrolery. Skupiny periférií I2C1 a I2C2 jsou napájeny až po potvrzení správné funkčnosti jednoho z mikrokontrolerů. Napájecí obvod dále zajišťuje proudové omezení pro každý z napájených systémů, celkovou nadproudovou ochranu a prioritní podpěťovou ochranu, kdy v případě podpětí budou systémy vypnuty v pořadí: I2C2, I2C1, Slave MCU a Master MCU.



Obr. 5.3 – Sekvence zapínání při běžném provozu



Obr. 5.4 – Sekvence zapínání při poruše na MCU1.1

## 5.1 Historie změn

Elektrické schéma bylo popisováno v nejnovější verzi. Pro kontext s výsledky měření byla přiložena tabulka historie změn.

Tabulka 5.1 - Historie změn verzí schématu

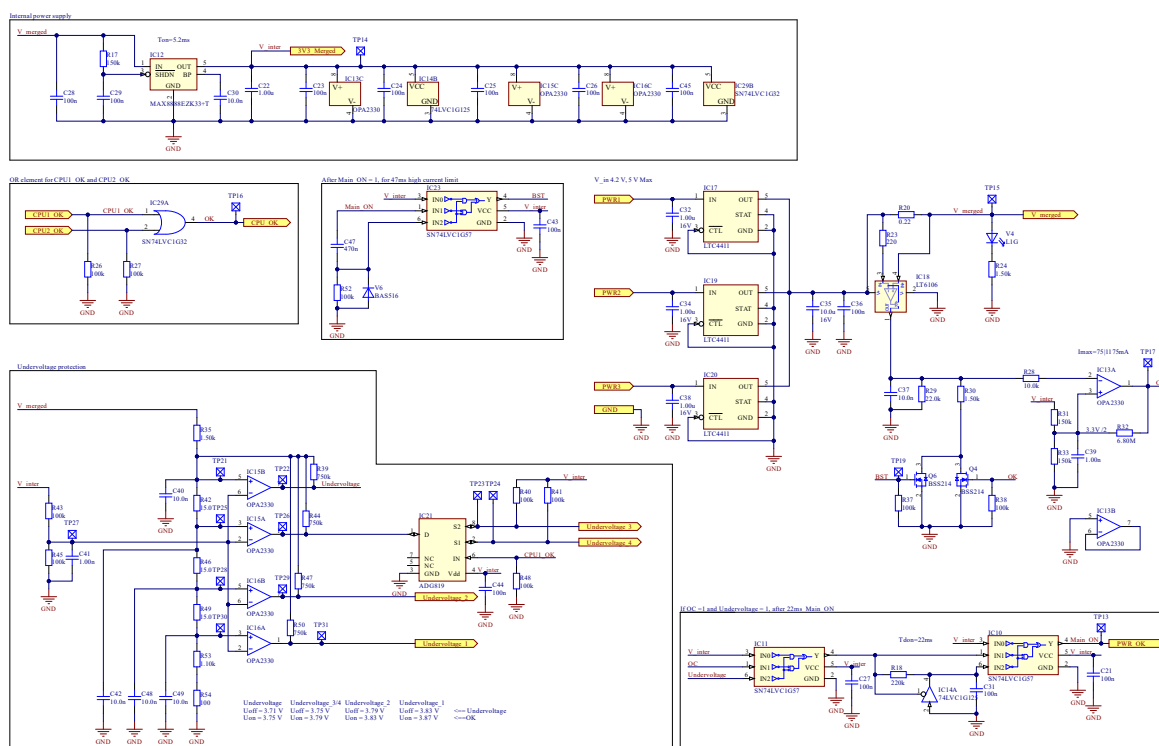
Verze schématu	Součástka/y	Akce	Komentář
V1	-	-	První verze schématu
V1.1	R57,R60	Pull down -> Pull up	Chyba ve schématu
V1.1	R57,R60	100k ohm -> 3k3 ohm	Mikrokontroler v průběhu resetu částečně přizemní některé z pinů. Při vysoké hodnotě pull-up rezistorů dojde k triggrování I2Cx_OC.
V1.1	IC2, R2, R3	Pin 8 - VCC -> IC1 pin 1	Pokus o přizpůsobení I2C opakovače pro nepodporovanou funkci - hot swap.
V1.1	Microcontroller unit	Port Vcc_merged přidán	Pro analogové spínače v bloku mikrokontroleru je pro správnou funkčnost při vypnutém napájení bloku potřeba stále přítomné napájení.
V1.1	U1, U2, U3, U4	Port 14 VIN -> V_Merged	Pro analogové spínače v bloku mikrokontroleru je pro správnou funkčnost při vypnutém napájení bloku potřeba stále přítomné napájení.
V1.1	Microcontroller unit	Port CPU_PWR_OFF přidán	Port pro funkci vypínání napájení druhého procesoru.
V1.1	R62	10k ohm rezistor přidán	Pull-up rezistor pro nový port CPU_PWR_OFF.
V1.1	3V3_power.1, 3V3_power.2	Port_CPU_OK přepojen na CPU_PWR_OFF	Mikrokontrolery nevyužitý port byl použit pro funkci vypínání napájení druhého mikrokontroleru.
V1.1	IC21	Výstupy S2 a S1 prohozeny	Chyba ve schématu - funkční diagram datasheetu neodpovídá pravdivostní tabulce.
V1.1	Delay_22ms.2	Pin Vcc připojen na V_Merged	Se změnou zapojení bloku 3V3_Power je nutné přepojení

Tabulka 5.1 - Historie změn verzí schématu

Verze schématu	Součástka/y	Akce	Komentář
V1.1	Delay_22ms.3	Pin Vcc připojen na V_Merged	Se změnou zapojení bloku 3V3_Power je nutné přepojení
V1.1	IC27, IC28	Pin 1, 8 - připojeno na VIN	Chyba ve schématu, label byl umístěn mimo net.
V1.1	IC26	Pin 5 Vcc -> V_in	Zjednodušení zapojení bez změny funkcionality.
V1.1	3V3_power	Port Vcc odebrán	Již nepoužívaný port.
V1.2	IC2, IC27, IC28	Změna za PCA9511AD	Záměna za I2C buffer podporující hot-swap.
V1.2	C4, 56, C58	Odebráno	PCA9511AD potřebuje pouze jeden filtrační kondenzátor.
V1.2	Power supply	Port 3V3_Merged přidán	Stálé napětí potřebné pro analogové spínače v bloku mikrokontroleru musí být stabilizováno
V1.2	Microcontroller unit	Port Vcc_merged přejmenován a na 3V3_Merged	Stálé napětí potřebné pro analogové spínače v bloku mikrokontroleru musí být stabilizováno
V1.2	Motherboard_Top	Port 3V3_Merged připojen na signál 3V3 Merged	Stálé napětí potřebné pro analogové spínače v bloku mikrokontroleru musí být stabilizováno
V1.3	IC23, C47, R52, V6	funkce BST 1 a BST 2 sjednocena	Zjednodušení zapojení, které činí systém odolný vůči zkratovanému napájení MCU1.1 při zapnutí.
V1.3	Microcontroller unit	port High_I1_ms odebrán	Již nepoužívaný port.
V1.3	IC13B,R19,R21, R22,C33,R25,Q1,Q2	OR element tvořený z OZ nahrazen za hradlo	Zjednodušení zapojení, stejná funkcionality, vyšší spolehlivost, menší footprint zapojení.
V1.3	IC22,R21,C33	Přidána funkce zpoždění zapnutí výstupů - 10ms	Přidána funkce zvyšuje spolehlivost systému a umožňuje optimalizaci rozvodu napájení.
V1.3	Delay_22 ms	Odebráno zpoždění pro napájení I2C1	Zjednodušení zapojení. Funkci zpoždění obstarává obvod mikrokontroleru, který připojí mikrokontroler až 10ms po potvrzení funkčnosti.
V1.3	Q3,Q7,R34	Odebráno	Zjednodušení zapojení. Možné falešné spínání podpěťové ochrany při zapnutí je přípustné, jelikož spínání bude filtrované zpožděvacím členem IC23.
V1.3	R29	2k2 ohm na 1k5 ohm	Zvýšení maximálního limitu proudové ochrany. Při zkratu periferie mohlo dojít k sepnutí ochrany.

## 5.2 Blok napájení

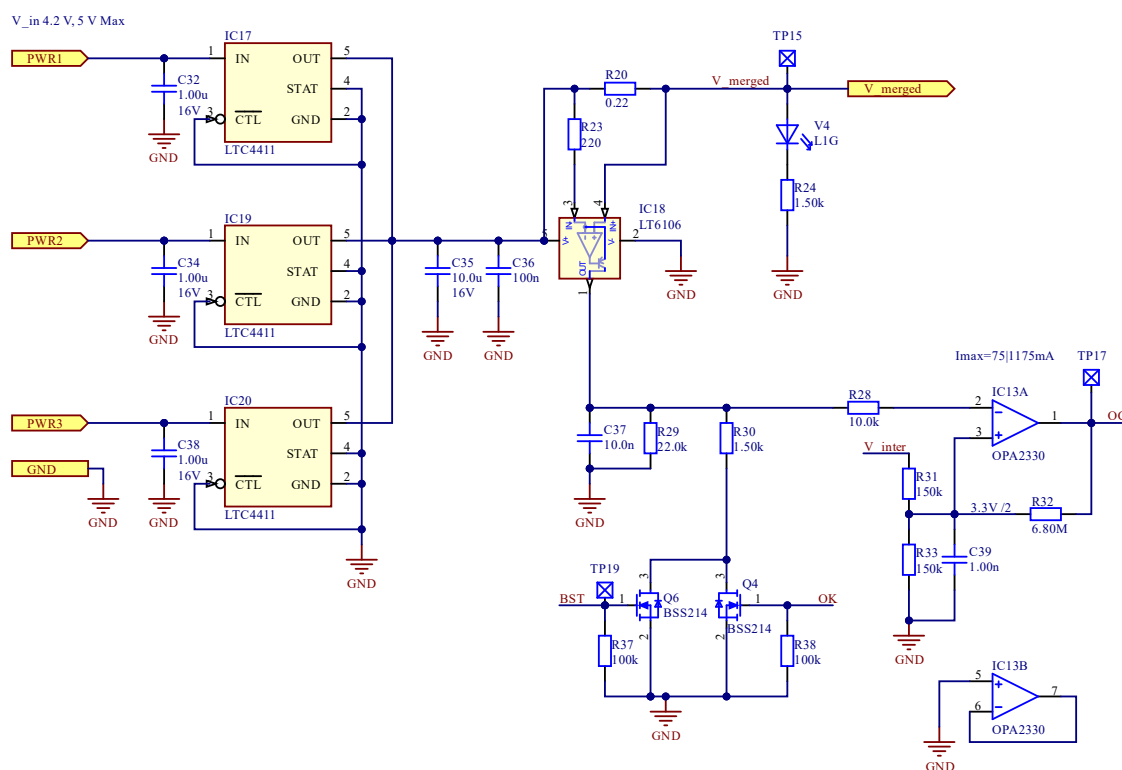
Napájení desky je možné třemi přívody na konektoru H1 : PWR1, PWR2 a PWR3. Pomocí ideálních diod IC17, IC19 a IC20 je napětí sjednoceno do V\_Merged, kdy proud je odebírán ze vstupu s největším napětím. Ideální diody plní funkci konvenční usměrňovací diody s takřka nulovým úbytkem – zabraňují toku proudu zpět do vstupů s nižším napětím. Při výpadku napájení s paralelním zapojením ideálních diod dojde k přepojení na jeden ze záložních zdrojů bez přerušení napájení zbytku systému. Systém není v tomto případě odolný vůči připojení závěrného napětí, či napětí většího jak 5 V. Napětí V\_merged je přivedeno na vstupy bloků 3V3\_Power, které napětí stabilizují a poskytují proudové omezení pro zbytek částí systému.



Obr. 5.5 - Schéma bloku napájení

Proud odebraný celkovým zařízením je měřen pomocí bočnicku R20. Operační zesilovač IC18 se zápornou zpětnou vazbou drží mezi diferenciálními vstupy virtuální nulové napětí a výslednou vzniklou smyčkou dodává na svém výstupu proud:

$$I_{sens} = \frac{I_{R_{20}} * R_{20}}{R_{23}} = I_{R_{20}} * 10^{-3} A \quad (5.1)$$



Obr. 5.6 – Schéma bloku napájení – nadproudová ochrana

Dodávaný proud vytváří napětí na rezistoru R29, které je porovnáváno operačním zesilovačem IC13A. Při překročení napětí invertovaného vstupu operačního zesilovače hodnoty určené děličem R31 a R33 s hysterezním offsetem R32 výstup operačního zesilovače OC přejde do logické 0 a všechny bloky napájení 3V3\_Power budou vypnuty. Vzhledem k vypnutí napájení při nadproudové ochraně může být vypočten pouze horní limit proudové ochrany  $I_{R_{20\_OC\_H}}$ :

$$I_{sens\_H} * R_{29} = V_{inter} * \frac{R_{33}}{(R_{31} // R_{32}) + R_{33}} \quad (5.2)$$

$$I_{R_{20\_OC\_H}} = \frac{V_{inter} * \frac{R_{33}}{(R_{31} // R_{32}) + R_{33}}}{10^{-3} * R_{29}} \quad (5.3)$$

$$I_{R_{20\_OC\_H}} = 75,8 \text{ mA} \quad (5.4)$$

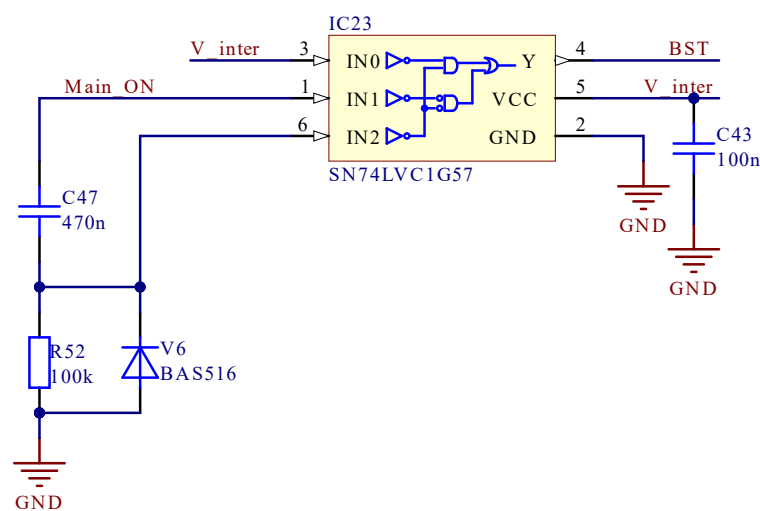
V případě signálů OK či BST ve stavu logická 1 dojde k připojení rezistoru R30 paralelně k rezistoru R29. Výsledkem je zvýšení limitu proudové ochrany:

$$I_{R_{20-OC-H}} = \frac{V_{inter} * \frac{R_{33}}{(R_{31} // R_{32}) + R_{33}}}{10^{-3} * (R_{29} // R_{30})} \quad (5.5)$$

$$I_{R_{20-OC-H}} = 1187,8 \text{ mA} \quad (5.6)$$

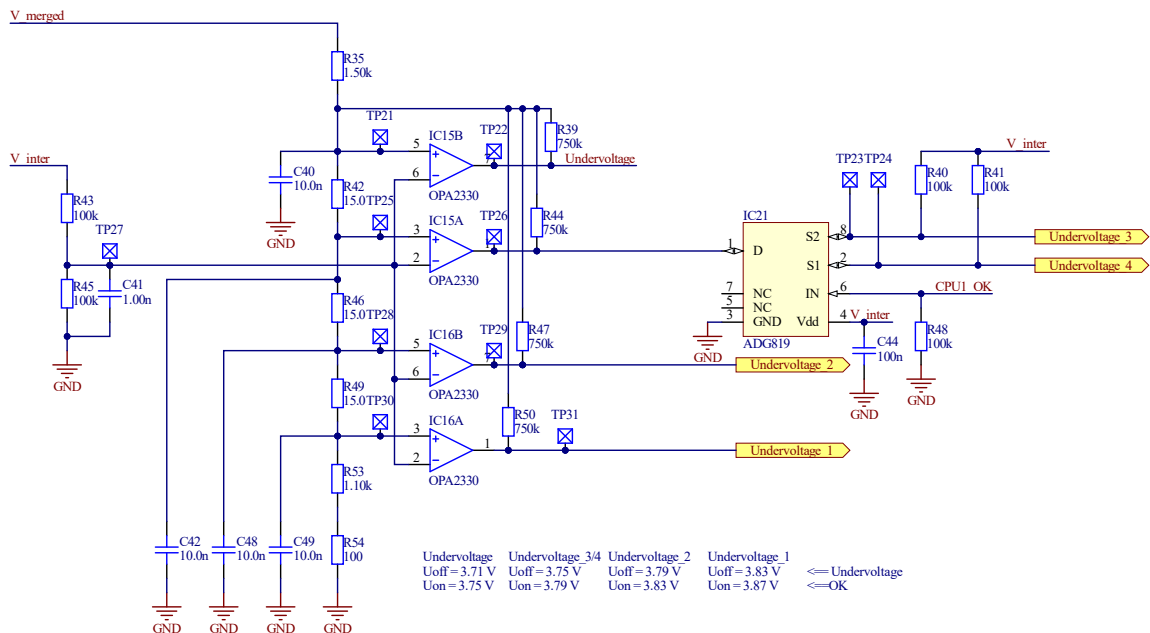
Signál BST je aktivní po dobu 47 ms při zapínání napájení systému. Tuto funkci zařizuje multifunkční hradlo IC23. Při nastavení vstupu IN0 do logické 1 hradlo plní na vstupech IN1 a IN2 funkci násobení. Při změně signálu Main\_ON ze stavu logická 0 na logickou 1 dojde mezi odporem R52 a kapacitou C47 k přechodovému jevu prvního řádu. Napětí na vstupu IN2 (rezistoru R52) pak bude přibližně po dobu nabíjení kondenzátoru  $\tau_{BST2}$  ve stavu logická 1 a stejně tak výstup hradla BST. Vstupy multifunkčního hradla mají integrovaný Schmittův klopný obvod. Dioda V6 zajišťuje rychlé vybití kondenzátoru v případě stavu logická 0 signálu Main\_ON. Účelem funkce BST je dočasné zvýšení proudového limitu při zapínání mikrokontroleru, které by mohlo při překročení spodního limitu proudové ochrany zapříčinit oscilaci systému. To obzvláště platí pro případ poruchy MCU1.1 – zkrat napájení, kdy by nedošlo k zapnutí MCU1.2, který napájení vadného mikrokontroleru následně vypne.

$$\tau_{BST} = R_{52} * C_{47} = 47 \text{ ms} \quad (5.7)$$



Obr. 5.7 - Schéma bloku napájení – funkce BST

Signál OK nastaví hodnotu proudové ochrany do horní meze v případě, že alespoň jeden z mikrokontrolerů je připojený a správně fungující. Funkce je realizována OR hradlem IC29, kde vstupem je potvrzení správně funkčnosti mikrokontrolerů CPU1\_OK a CPU2\_OK.



Obr. 5.8 - Schéma bloku napájení – podpěťová ochrana

Ochrana proti podpětí je realizována pomocí čtyř komparátorů. Nejvyšší vstupní napětí ze zdrojů PWR 1-3 je přivedeno signálem V\_merged přes řadu odporových děličů na neinvertované vstupy operačních zesilovačů, kde je porovnáváno s konstantním napětím na invertovaných vstupech. Při vypnutí části systému odebírající proud ze zdroje dojde k navýšení napětí v závislosti na vnitřním odporu zdroje a odporu přívodů. Z toho důvodu musí mít každý z komparátorů hysterezi realizovanou slabou kladnou zpětnou vazbou. Vzhledem ke dvěma použitým mikrokontrolerům je potřeba vyhodnocovat prioritu vypnutí v závislosti na aktuálním Master procesoru. MCU1.1 má časovou výhodu při zapnutí oproti MCU1.2, tudíž je při správné funkčnosti Master. Potvrzení správné funkčnosti MCU1.1 – CPU1\_OK je přivedeno na vstup multiplexoru IC21 a při podpětí je prvně vypnut MCU1.2 – Slave. V případě poruchy se stane Master MCU1.2 a jako první bude vypnut MCU1.1.

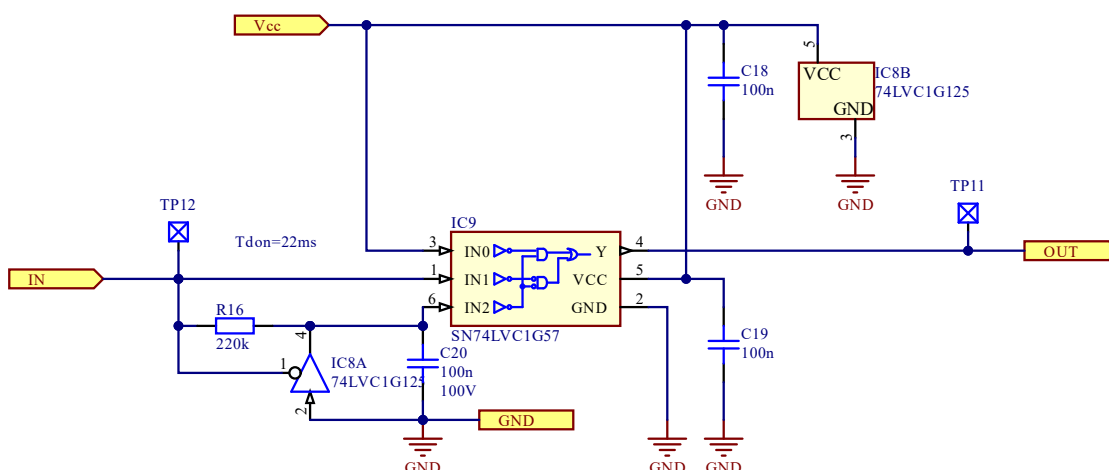
Při splnění podmínek podpět'ové a nadproudové ochrany po dobu 22 ms je signál potřebný pro zapnutí dalších systémů – PWR\_OK přiveden do stavu logická 1. Zapojení obvodu je shodné s blokem zpoždění.

Všechny integrované obvody obsažené v bloku napájení jsou napájeny 3,3V napětím ze stabilizátoru IC12.

### 5.3 Blok zpoždění

Blok zpoždění zajišťuje postupné zapínání procesorů a periférií, což rozděljuje proudové rázy vzniklé nabíjením kondenzátorů. Dále je časová výhoda mikrokontroleru MCU 1.1 využita programem pro zavedení Master – Slave hierarchie u procesorů s jednotným kódem. Obvod se skládá z multifunkčního hradla IC9 nastaveného do funkce násobení vstupů IN1 a IN2. Při změně stavu vstupu IN z logická 0 na logická 1 dojde u odporu R16 a kondenzátoru C20 k přechodovému jevu prvního řádu. Napětí na vstupu IN2 pak bude po odeznění přechodového jevu  $\tau$  ve stavu logická 1, a tudíž i výstup AND hradla. Buffer IC8 zajišťuje aktivní vybíjení kondenzátoru při vstupu IN ve stavu logická 0 a v případě stavu logická 1 je jeho výstup ve stavu vysoké impedance.

$$\tau = R_{16} * C_{20} = 22 \text{ ms} \quad (5.8)$$

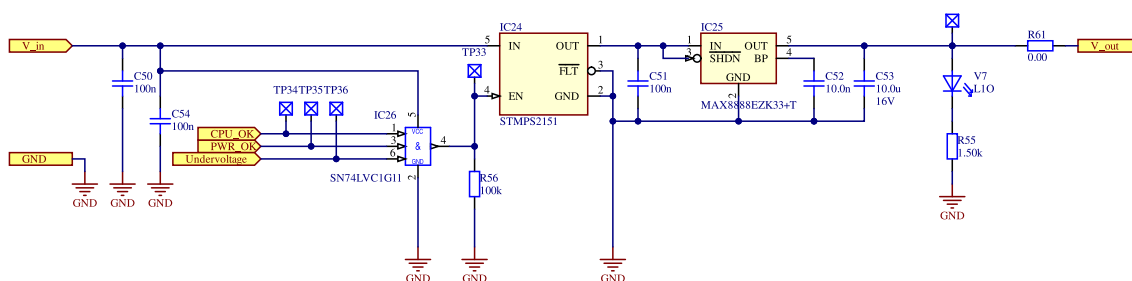


Obr. 5.9 – Schéma bloku zpoždění 22 ms



## 5.4 Blok regulátoru napětí

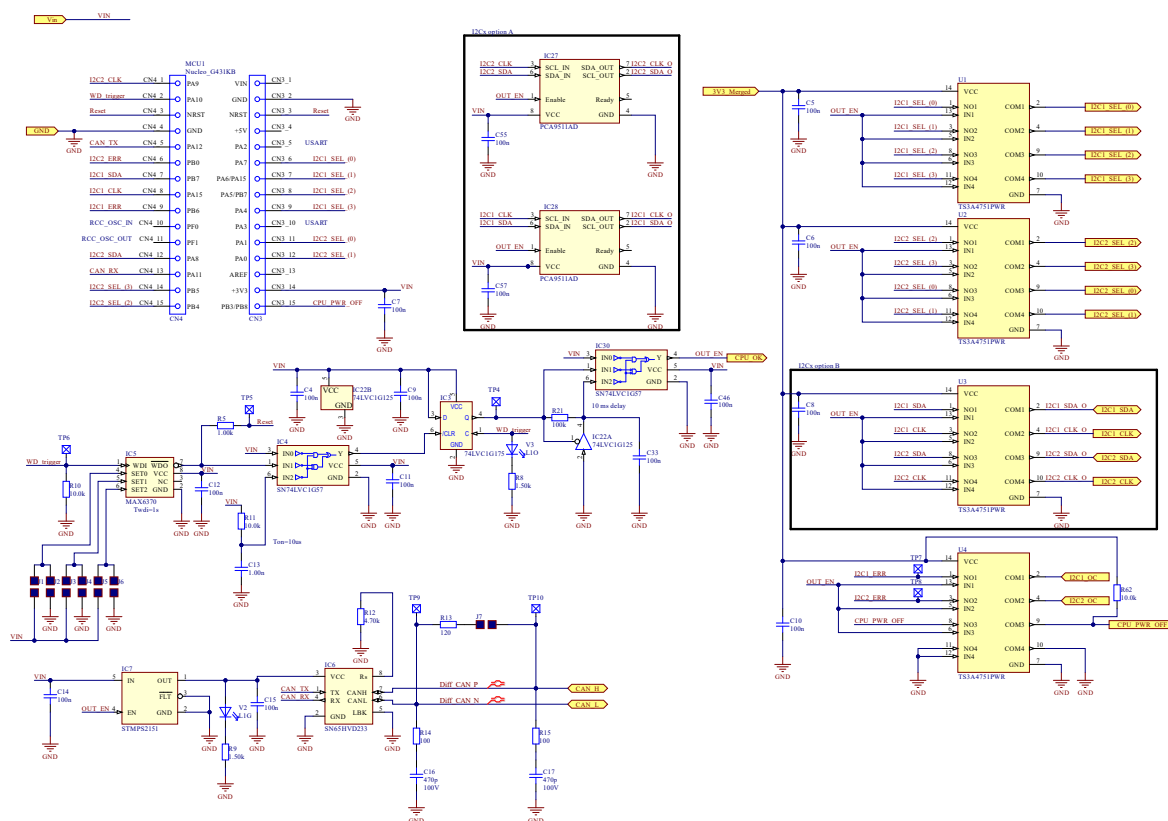
Navržený systém obsahuje čtyři bloky regulátoru napětí poskytující 3.3 V napětí pro mikrokontrolery a periferie. Pro zapnutí bloku musí být všechny z řídicích signálů na vstupu AND hradla IC26 ve stavu logická 1. První vstup je u I2C periferií využit pro potvrzení přítomnosti a správné funkčnosti alespoň jednoho z mikrokontrolerů. U mikrokontrolerů je vstup využit k vypnutí napájení Slave mikrokontroleru. Druhý vstup je využit pro nadproudovou ochranu a třetí pro vypnutí napájení v případě podpětí. IC24 spíná přivedené nestabilizované napětí na 3,3V stabilizátor IC25 a zároveň poskytuje proudové omezení bloku na 500 mA.



Obr. 5.10 - Blok regulátoru napětí

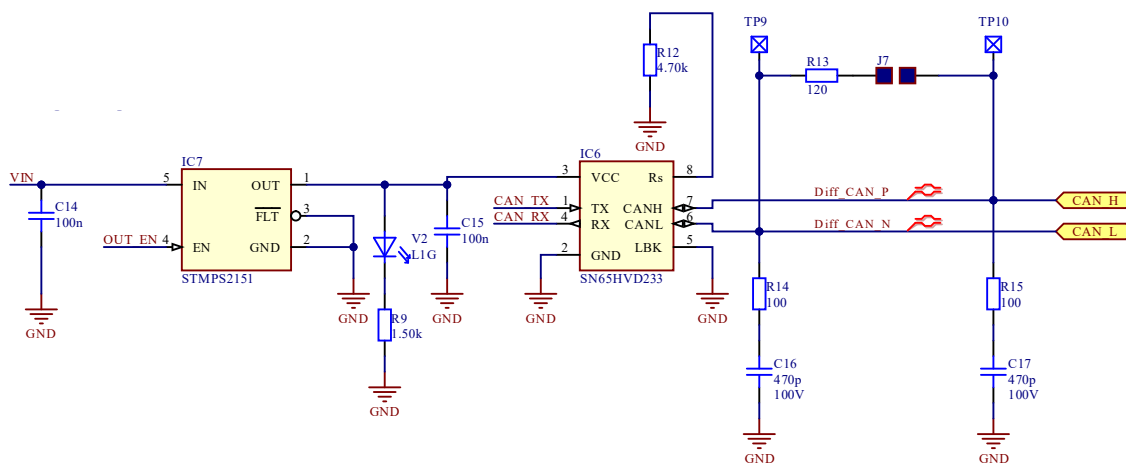
## 5.5 Blok Mikrokontroleru

Pro demonstraci systému byla vybrána dvojice mikrokontrolerů STM32G431KB, jelikož obsahují 128 kB Flash paměť s podporou ECC a 22 kB SRAM paměť s hardwarovou kontrolou parity pro prvních 16 kB. U mikrokontrolerů tak může být docílena zvýšená odolnost vůči TID a SEE. Mikrokontrolery jsou k ukázkové desce připojeny pomocí patice, což umožňuje adaptaci různých mikrokontrolerů bez modifikace desky, či snadnou výměnu při poruše.



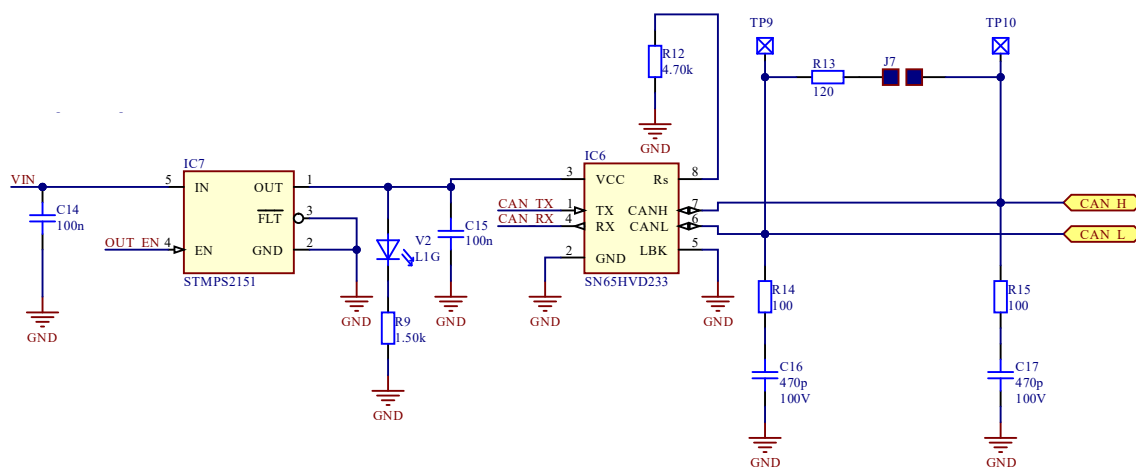
Obr. 5.11 - Schéma bloku mikrokontroleru

Blok vyhodnocuje správnou funkčnost mikrokontroleru pomocí WDT a v případě poruchy mikrokontroler resetuje. Signál  $\overline{WD0}$  změnou stavu z logické 0 na logickou 1 resetuje WDT - IC5 a výstup  $\overline{WD0}$  zůstane ve stavu logická 1. Výstup WDT je dále přiveden na asynchronní negovaný reset klopného obvodu IC3, který svým výstupem připojuje mikrokontroler ke zbytku systému. Zapnutí periférií je zpožděno zapojením IC22A, IC30, R21, C33 (zapojení shodné s blokem zpoždění) o 10 ms od sepnutí klopného obvodu, čímž je zajištěno, že mikrokontroler bude připojen až po dokončení inicializace GPIO. Zpoždění je zároveň využito pro rozložení proudových rázů při zapínání napájení periférií. Hradlo IC4 zajišťuje reset klopného obvodu při zapnutí napájení mikrokontroleru. V případě poruchy dojde po překročení časového limitu nastaveného propojkami J1 - J6 na výstupu WDT k pulzu, který resetuje mikrokontroler.



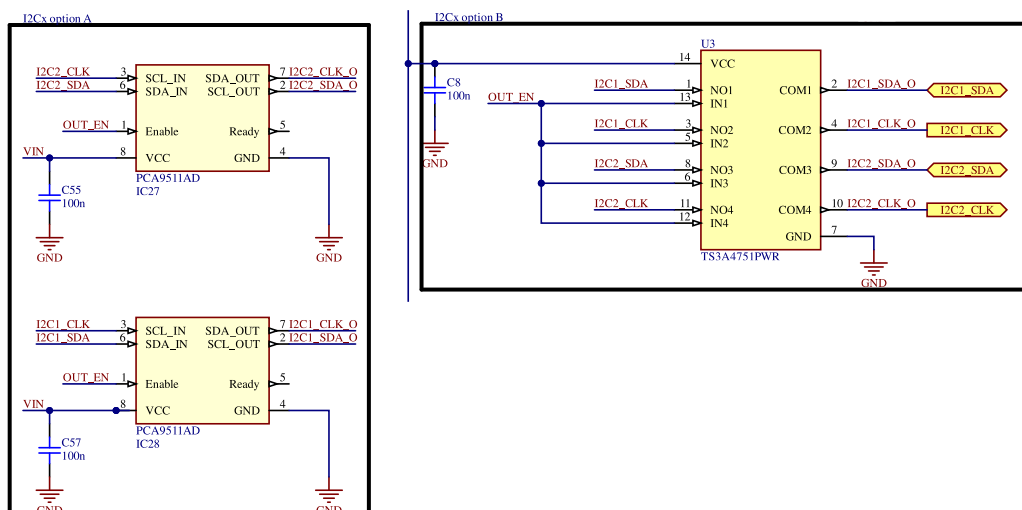
Obr. 5.12 - Schéma bloku mikrokontroleru – WDT

Komunikaci mezi mikrokontrolery zařizuje IC6 pomocí rozhraní CAN. Při poruše mikrokontroleru je napájení IC6 odpojeno spínačem IC7 a výstupy IC6 přejdou do stavu vysoké impedance.



Obr. 5.13 - Schéma bloku mikrokontroleru – CAN

Komunikace mikrokontroleru s periferiemi je realizována pomocí I2C sběrnice. Připojení mikrokontroleru ke sběrnicím je ve verzi desky 1.3 možné dvěma způsoby. Prvním způsobem (varianta A) jsou I2C opakovače IC27 a IC28, druhým (varianta B) je řada analogových spínačů U3. Při osazování desky musí být osazena pouze jedna z možností. Varianta A zabírá při implementaci na DPS více místa a integrované obvody jsou dražší. U varianty B musí program zajistit přerušení komunikace na I2C sběrnicích při připojení mikrokontroleru ke zbytku systému. Obě varianty se ovšem osvědčily jako spolehlivé.

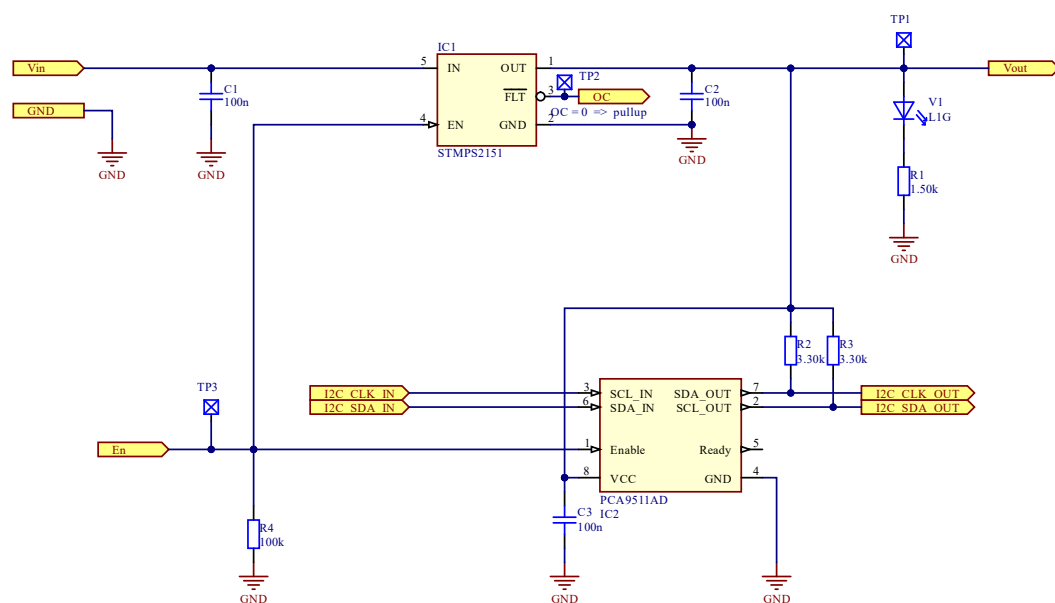


Obr. 5.14 - Schéma bloku mikrokontroleru – I2C

Zbytek řídicích I/O mikrokontroleru je k systému připojeno pomocí analogové řady spínačů, obdobně jako variantě B připojení I2C komunikace.

## 5.6 Blok I2C periferie

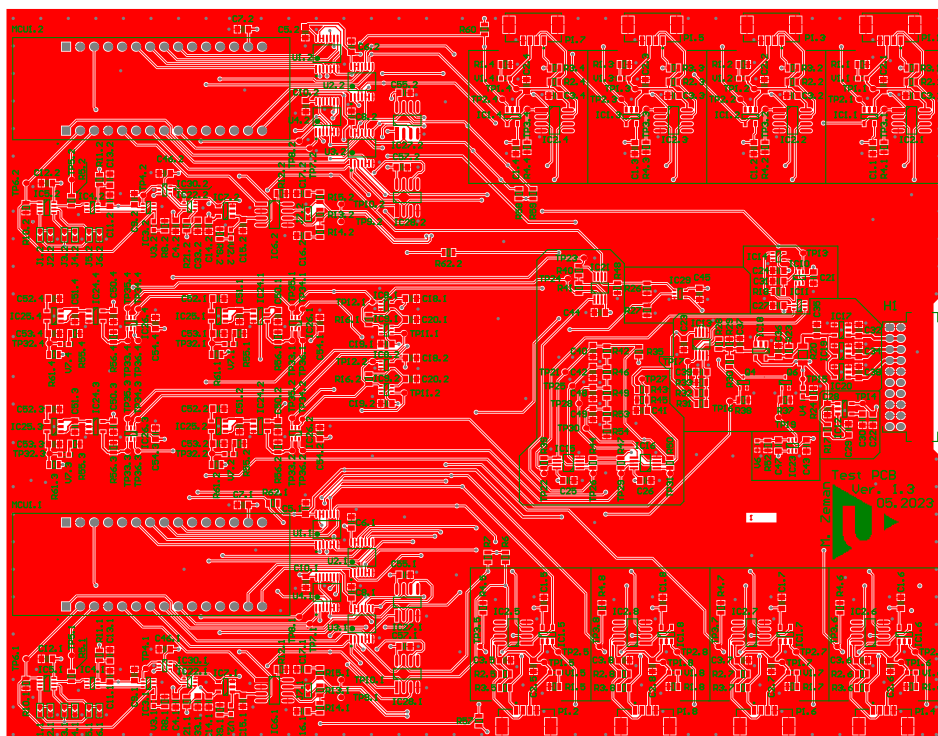
Pro dosažení maximálního zachování funkčnosti systému při selhání některé z periférií musí být každá periferie připojena k systému pomocí vlastního bloku I2C periferie. Blok poskytuje po přivedení logické 1 na vstup En periferii napájení 3.3 V s proudovým omezením 500 mA pomocí spínače IC1. Signály pro I2C komunikaci jsou k periferii přivedeny přes I2C opakovač IC2, který disponuje funkcí hot-swap – připojení periferie ke společné I2C sběrnici dojde až v případě, že signály SCL a SDA na obou stranách I2C opakovače jsou ve stavu logická 1. I2C opakovač použitý v předchozích verzích desky bez této funkce při připojení I2C periferie s poruchou na signálu SLC blokoval komunikaci na společné sběrnici až do resetu napájení.



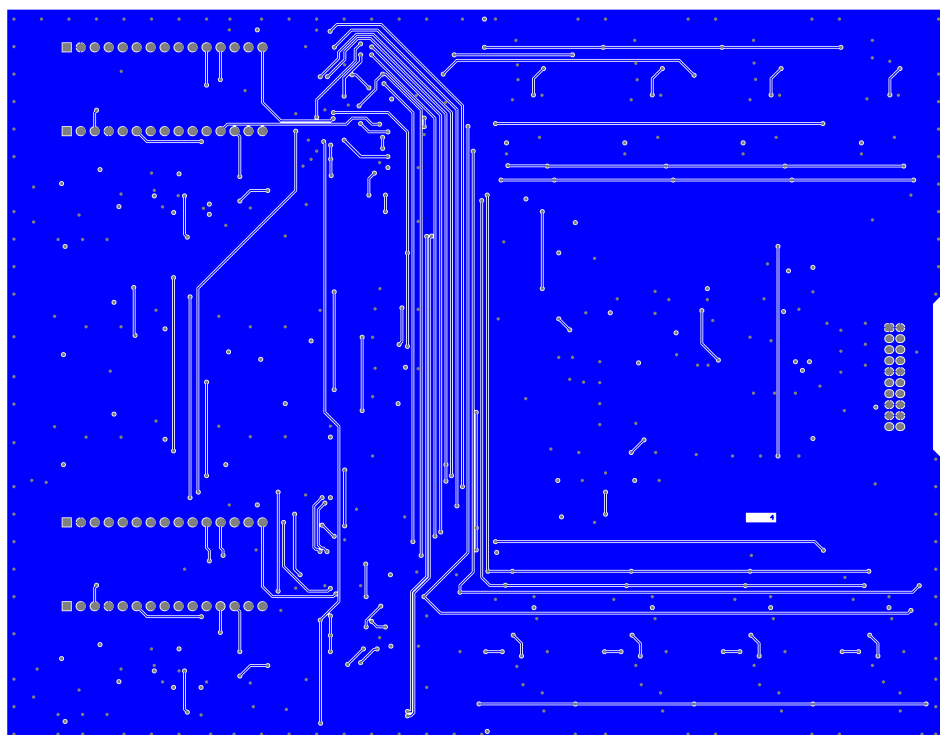
Obr. 5.15 - Schéma bloku I2C periferie

## 6 Návrh DPS

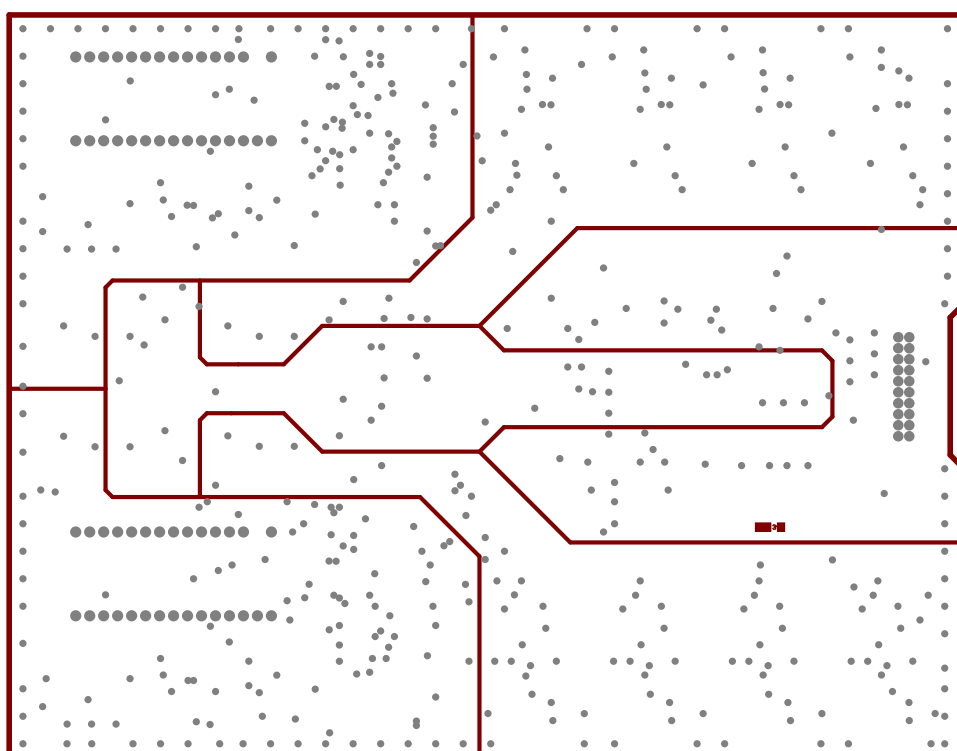
Návrh desky plošných spojů byl proveden v programu Altium. Soubory projektu jsou dostupné v elektronické příloze. Navržená testovací DPS se skládá ze čtyř vrstev, kdy prostřední vrstvy jsou použity pro zemnicí a napájecí plochu. Součástky byly za účelem snadného testování a modifikací desky rozloženy pouze na horní vrstvu DPS. Předložený návrh desky je ve verzi 1.3.



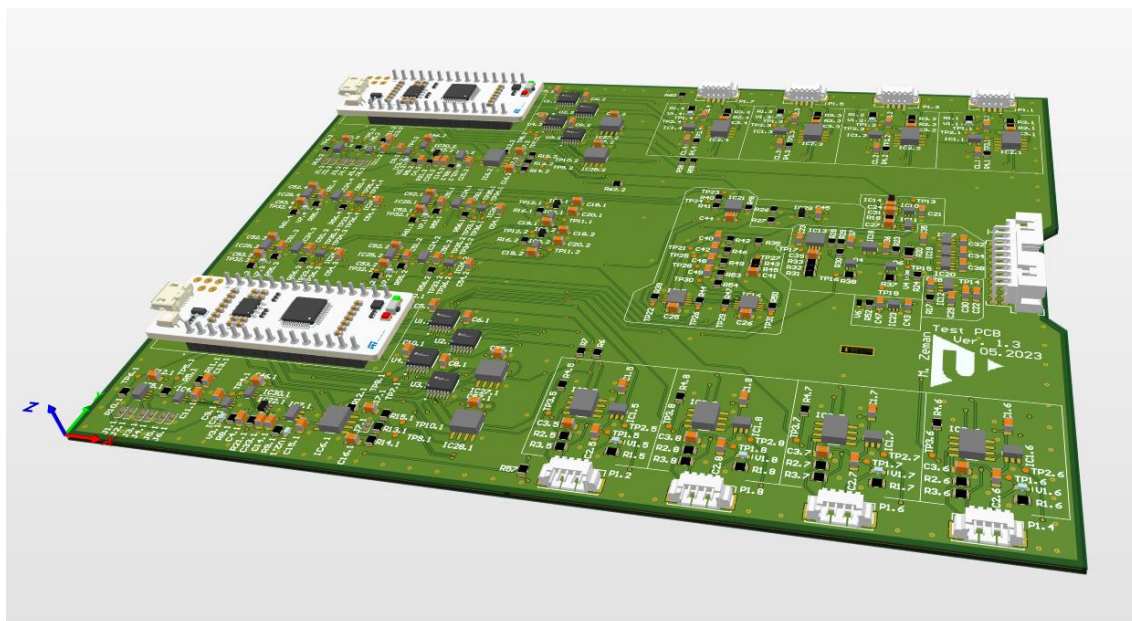
Obr. 6.1 TOP vrstva desky V1.3 včetně popisků



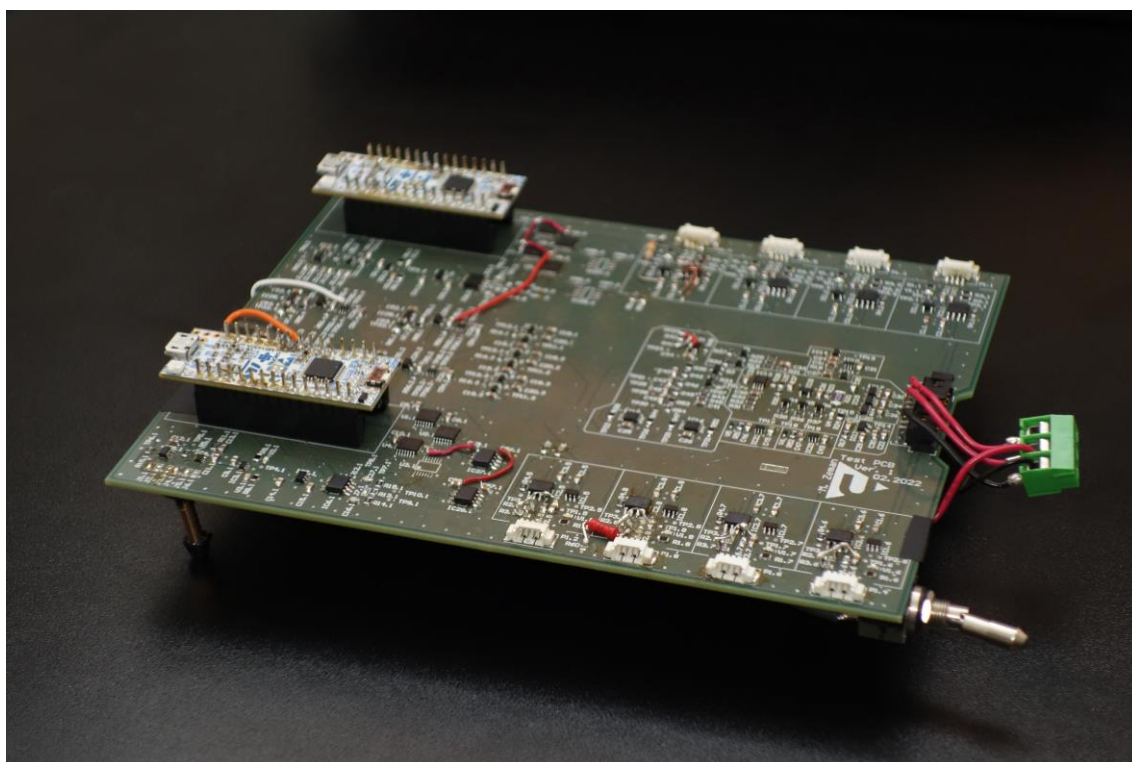
Obr. 6.2 - BOT vrstva desky V1.3



Obr. 6.3 - Vnitřní vrstva napájení desky V1.3



Obr. 6.4 - 3D model desky V1.3

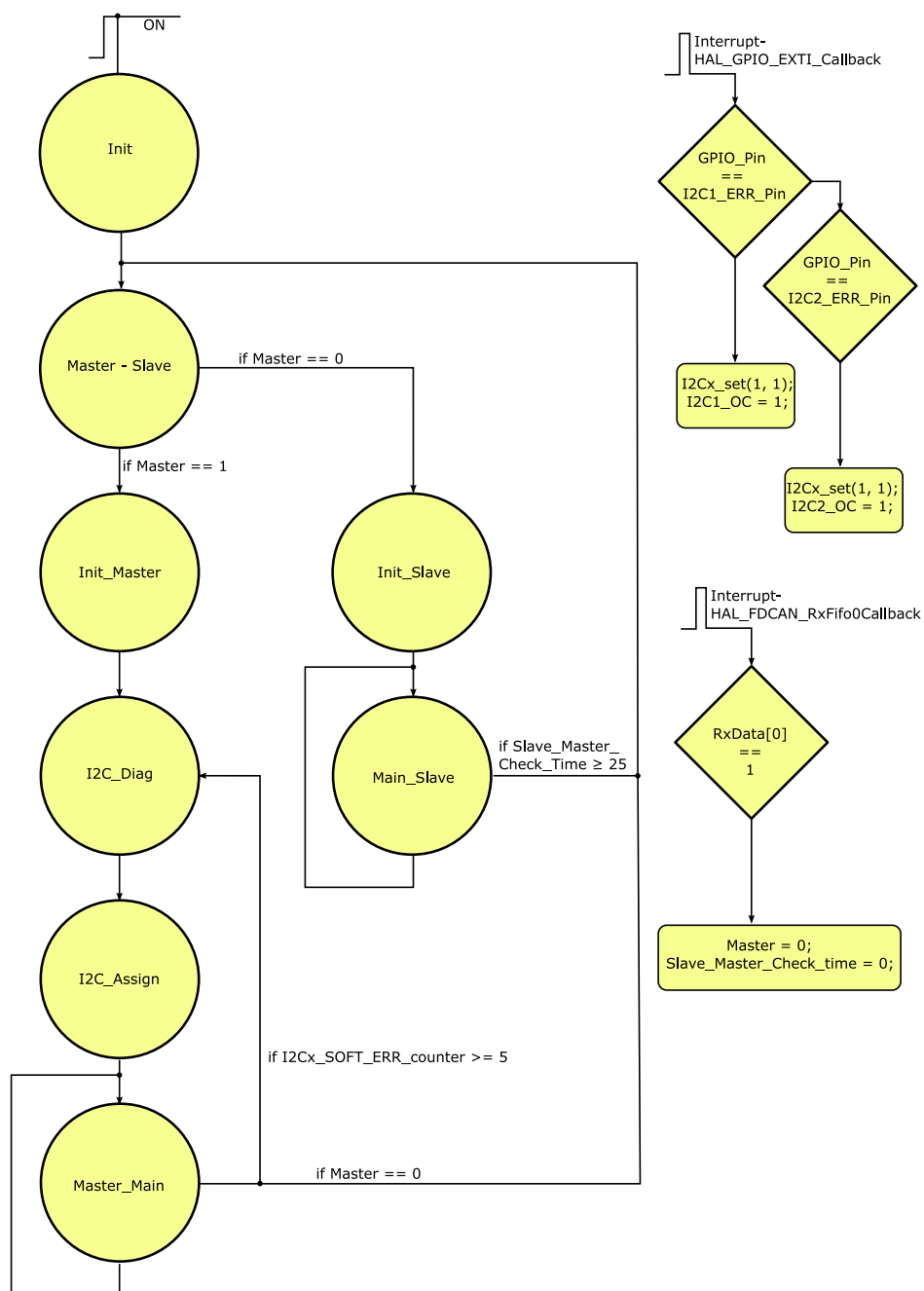


Obr. 6.5 - Vyrobená deska V1 s úpravami pro měření dalších verzí



## 7 Demonstrační program

Program pro demonstraci systému byl napsán v embedded vývojovém prostředí STM32CubeIDEm, které poskytuje řadu pokročilých funkcí pro pohodlné nastavení mikrokontroleru. Program je dostupný v elektronické příloze. Struktura programu je tvořena stavovým automatem, kdy každý ze stavů vyvolává příslušné funkce.



Obr. 7.1 - Blokový diagram programu

## 7.1 Init

Stav Init inicializuje potřebné periferie pro rozdělení Master-Slave hierarchie mezi mikrokontrolery. Inicializovány jsou následující periferie:

- CAN – pro posílání a příjem hlavičky obsahující informaci o Master MCU
- Čítač &tim2 s přerušením – pro časování
- Pin GPIO obsluhující WDT
- USART pro komunikaci s terminálem počítače

Veškeré ostatní GPIO jsou inicializovány jako analog input, což optimalizuje spotřebu a vylučuje kolizi řídicích signálů mezi mikrokontrolery. Mikrokontroler čeká ve stavu Init po dobu 1500 ms na příjem CAN zprávy obsahující informaci o přítomném Master procesoru. V případě příjmu zprávy mikrokontroler přeskočí čekání a nastaví svůj příznak Master na hodnotu 0. Dále mikrokontroler pokračuje do stavu Master-Slave.

## 7.2 Master-Slave

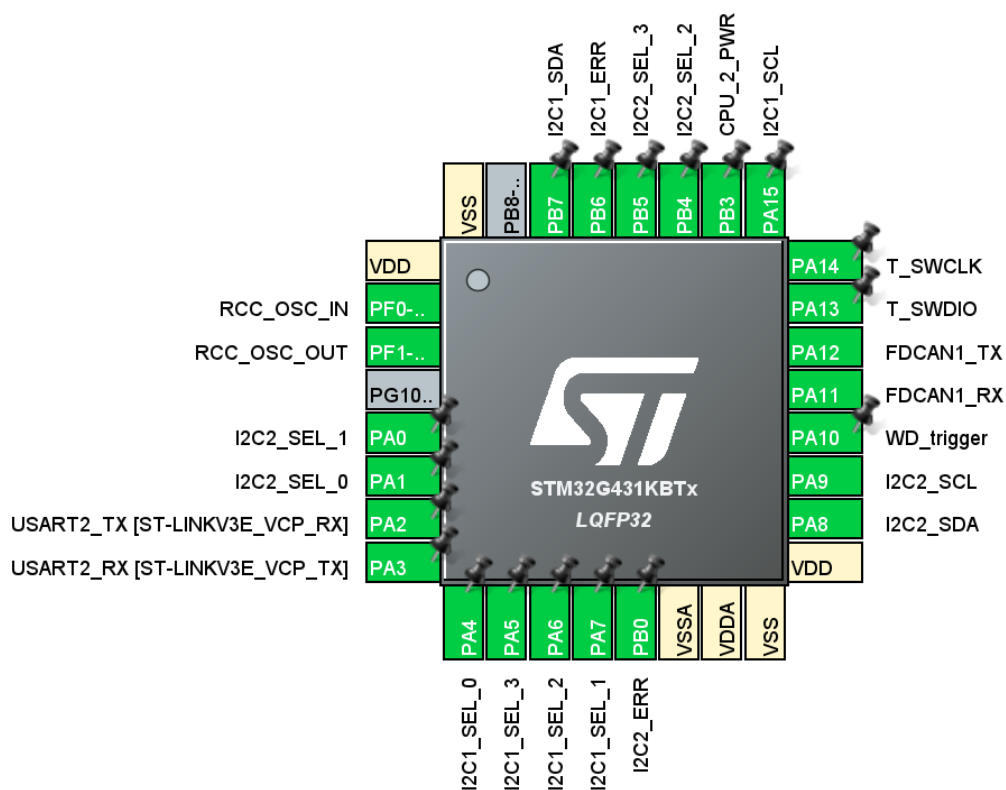
Pro rozdělení Mater-Slave hierarchie využívá MCU1.1 časovou výhodu 22 ms při zapnutí. Do stavu Master-Slave se dostane jako první a odešle hlavičku s příznakem přítomného Master mikrokontroleru přes rozhraní CAN, čímž je hierarchie Master-Slave rozdělena s použitím stejného programu na obou mikrokontrolerech.

Master dále pokračuje do stavu Init\_Master, Slave pak do stavu Init\_Slave

## 7.3 Init\_Master

Ve stavu Init\_Master mikrokontroler inicializuje I2C sběrnice a zbytek řídicích GPIO. Všechny řídicí GPIO jsou inicializovány jako výstupy s otevřeným kolektorem, aby případná kolize řídicích signálů nezpůsobila zkratové proudy.

Pokud je uživatelská proměnná Slave\_mode nastavena do stavu 0, vypne Master napájení Slave mikrokontroleru a systém pracuje v režimu studené redundance. V případě Slave\_mode nastaveného do stavu 1 bude Slave mikrokontroler ponechán zapnutý a jedná o systém s teplou redundancí. Po provedení inicializace mikrokontroler pokračuje do stavu I2C\_Diag.



Obr. 7.2 - Pinout mikrokontroleru

## 7.4 I2C\_Diag

Funkce I2C\_Diag rozpozná stav na všech I2C větvích, kdy stav může být: připojená periferie, nepřipojená či nefunkční periferie a zkrat napájení.

Master mikrokontroler nejprve čeká po dobu 100ms, aby se dokončila případná inicializace Slave mikrokontroleru, která by mohla zapříčinit kolize na řídicích signálech a poté přejde k diagnostice I2C periferií.

Diagnostika je realizována pomocí funkce I2Cx\_diag(x), kde parametr x volí diagnostiku mezi I2C1 a I2C2. Funkce vypne všechny větve I2Cx sběrnice, postupně zapne každou větev zvlášť a hledá zařízení připojené ke sběrnici. Při zkratu napájení blok periferie vyvolá signálem I2Cx\_OC přerušení, které vypne všechny periferie dané sběrnice a nastaví příznak zkratu. Po dokončení diagnostiky dojde k zapnutí pouze těch větví, kde bylo nalezeno zařízení. Program obsahuje uživatelskou proměnnou I2C\_mode, kterou lze zapnout paměť zkratovaných periferií. V případě zkratu na I2C větvi při aktivní paměti zkratovaných periferií bude větev vyřazena z diagnostiky až do resetu mikrokontroleru.

## 7.5 I2C\_assign

Ve stavu I2C\_assign mikrokontroler inicializuje I2C periferie, nastaví příznaky přítomnosti na sběrnici a pokračuje do stavu Main\_Master.

## 7.6 Main\_Master

Stav Main\_Master zařizuje obsluhu přítomných periférií, periodické odesílání CAN hlavičky pro udržení Master titulu a periodické obsluze WDT. Stav odkazuje sám na sebe, čímž tvoří nekonečnou smyčku, ze které se mikrokontroler může dostat pouze dvěma způsoby:

- Mikrokontroler obdrží CAN zprávu s hlavičkou značící přítomnost Master mikrokontroleru – mikrokontroler pak přejde opět do stavu Master-Slave.
- Došlo k chybě na I2C sběrnici a je potřeba znovu provést diagnostiku – mikrokontroler přejde do stavu I2C\_Diag. Tento případ může nastat dvěma způsoby. Prvním je zkrat napájení na konektoru periferie, což vyvolá přerušení, které vypne všechny periferie na dané sběrnici a nastaví příznak potřebné diagnostiky. Druhým je, že čítač chyb komunikace na sběrnici I2Cx\_SOFT\_ERR\_counter překročí hranici 5 chyb za 100 vteřin.

## 7.7 Init\_Slave

Inicializace Slave mikrokontroleru se v ukázkovém programu shoduje s inicializací při zapnutí napájení.

## 7.8 Main\_Slave

Mikrokontroler ve stavu Main\_Slave čeká na výpadek komunikace po sběrnici CAN po dobu delší jak 5 vteřin. V takovém případě si nastaví příznak Master = 1 a přejde do stavu Master\_Slave.

## 8 Výsledky měření

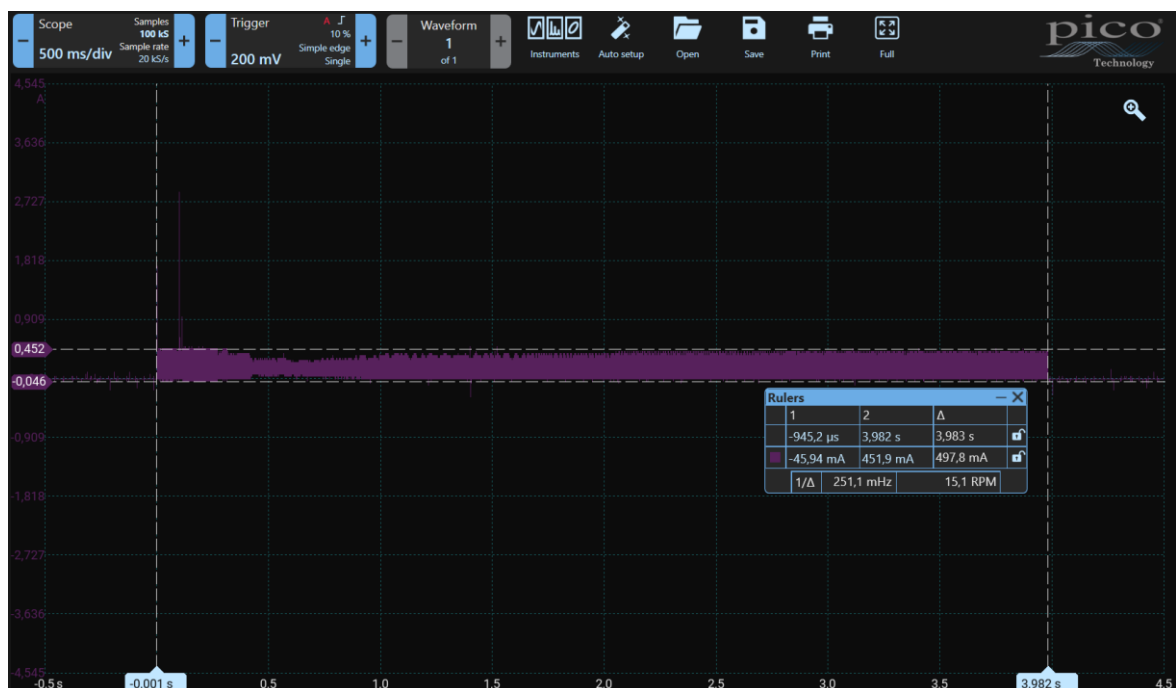
Z důvodu časové a finanční náročnosti spojené s výrobou nových verzí desky byly části DPS ve verzi 1 v průběhu vývoje pro účely testování upravovány. Dokumentace testů včetně postupu měření a dalších provedených testů je dostupná v elektronické příloze.

### 8.1 Reakční doba zkratu mikrokontroleru

V případě poruchy mikrokontroleru převezme řízení systémů Slave mikrokontroler. Test byl proveden zkratováním napájení Master mikrokontroleru a reakční doba byla změřena dobou trvání zkratového proudu. Verze desky pro účel měření odpovídala verzi 1.2.

Změřená reakční doba činí 3,98 s při Slave mikrokontroleru v teplém redundantním módu. Reakční doba je dána programem mikrokontroleru a může být optimalizací řádově snížena. Časové prodlevy byly v použité verzi programu při měření nastaveny pro jednodušší debugging.

Slave mikrokontroler převzal řízení systému a funkcionality byla plně zachována.



Obr. 8.1 - Reakční doba zkratu mikrokontroleru

## 8.2 Reakční doba zkratu I2C periferie

V případě zkratu I2C periferie bude od sběrnice daná periferie okamžitě odpojena. Reakční doba byla měřena dobou zkratového proudu na periférii. Verze desky pro účel měření odpovídala verzi 1.2.

Změřená reakční doba činí 858  $\mu$ s.

System byl schopný zachovat maximální funkcionalitu na I2C sběrnici.



Obr. 8.2 - Reakční doba zkratu I2C periferie

## 8.3 Porucha na I2C konektoru

Měření otestovalo schopnost systému ustát nestandardní stavy na I2C konektoru. Verze desky pro účel měření odpovídala verzi 1.2. Otestovaný byly stavy:

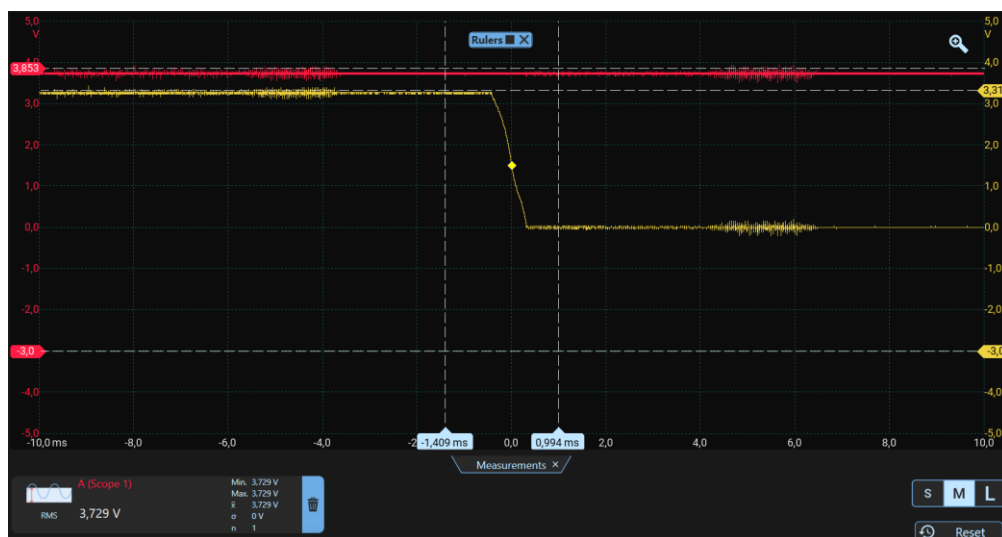
- Zkrat napájení
- Zkrat signálů CLK a SDA k napájení
- Zkrat signálů CLK a SDA k zemi

System byl schopný rozpoznat a zaznamenat zkrat napájení. Stav při zkratovaných signálech I2C komunikace je shodný s nepřipojeným zařízením. Komunikace na dalších I2C větvích nebyla ovlivněna a systém byl schopný plné funkčnosti při všech kombinacích stavu na výstupu I2C konektoru.

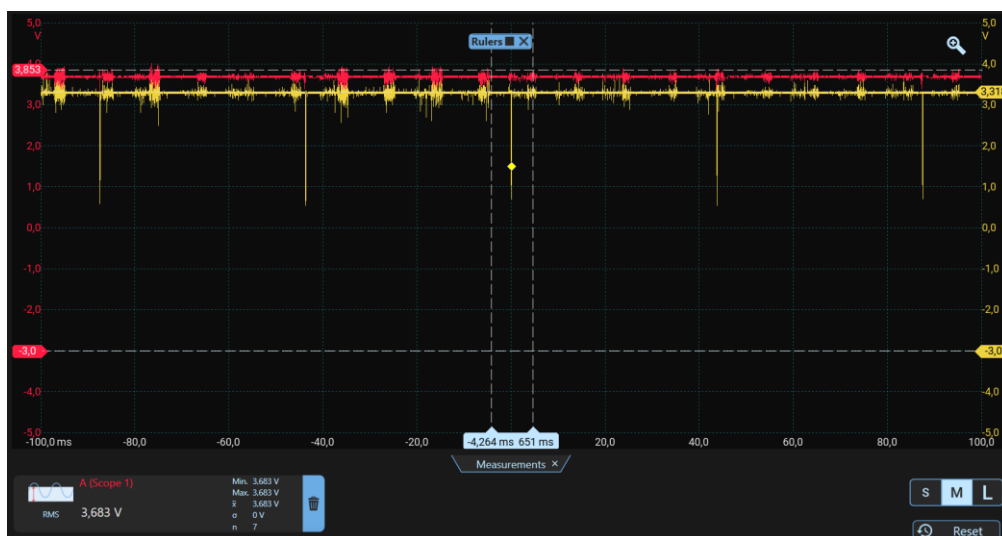
## 8.4 Ochrana podpětí

Ochrana podpětí byla otestována postupným snižováním napětí napájecího zdroje. Verze desky pro účel měření odpovídala verzi 1.1. Systém vypnul periferie v očekávaném pořadí, včetně případu poruchy mikrokontroleru MCU1.1, kdy se mění priorita vypínání. Spínané napětí se lišilo přibližně o 0.02 V od simulace.

Při spínání podpěťové ochrany s nejvyšší prioritou (při mezním podpětí) docházelo k oscilaci, což naznačuje nedostatečnou hysterezi. Vzhledem k měření v domácích podmínkách za použití dlouhých přívodních kabelů, spoje pomocí krokodýlových spojek a levného laboratorního zdroje je možné, že oscilace není zapříčiněna samotným obvodem.



Obr. 8.3 - Prioritní podpěťová ochrana – správná funkčnost



Obr. 8.4 - Prioritní podpěťová ochrana – oscilace

## 9 FMEA

V kapitole 3.1.4 byla vytvořena čtveřice tabulek pro vyhodnocení celkové kritičnosti poruchy. Hodnoty závažnosti a detekce poruchy součástek byly vyhodnoceny za pomoci schématu, radiační odolnost pak byla odhadnuta z datasheetu součástek. K vyhodnocení pravděpodobnosti poruchy byly použity vzorce pro výpočet poruchovosti z normy MIL-HDBK-217F [13].



## 9.1 Výpočet poruchovosti rezistorů

Všechny rezistory (s výjimkou bočniců) použité při návrhu jsou typu tlustovrstvé SMD.

Pravděpodobnost poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = \lambda_b * \pi_R * \pi_Q * \pi_E \left( \frac{Poruch}{10^6 h} \right), \quad (9.1)$$

kde  $\lambda_b$  značí základní poruchovost součástky,  $\pi_R$  je faktor odporu součástky,  $\pi_Q$  je faktor kvality součástky a  $\pi_E$  je faktor prostředí. Pro výpočet základní poruchovosti součástky byla použita rovnice:

$$\lambda_b = 3,25 * 10^{-4} * e^{\left(\frac{T+273}{343}\right)^3} e^{S * \left(\frac{T+273}{343}\right)} \left( \frac{Poruch}{10^6 h} \right), \quad (9.2)$$

kde  $T$  značí maximální provozní teplotu a  $S$  značí poměr provozního a jmenovitého výkonu součástky. Předpokládaná maximální provozní teplota pro LEO mise by dle [14] neměla překročit 60 °C. Poměr provozního a jmenovitého napětí je u většiny rezistorů pod hodnotou  $S = 0,1$ . Po dosazení do rovnice (9.2) je výsledná základní poruchovost součástky:

$$\lambda_b = 0,00092 \left( \frac{Poruch}{10^6 h} \right) \quad (9.3)$$

Pro odpory do 1 M $\Omega$  může být použit koeficient  $\pi_R = 1,1$ , koeficient kvality může být za předpokladu dostatečné kvality součástek zanedbán. Koeficient prostředí by mohl být zvolen pro zařízení bez propulzního systému v orbitu Země – 0,20. V takovém případě ale není bráno v potaz prostředí při vzestupu rakety do orbitu, které odpovídá koeficientu 28. Koeficient prostředí byl tedy ve výpočtu pravděpodobnosti zanedbán a prostředí je zohledněno v FMEA radiační odolností součástky.

Výsledná poruchovost součástky je pak:

$$\lambda_p = 0,001045 \left( \frac{Poruch}{10^6 h} \right) \quad (9.4)$$

Dále může být určen střední čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 956937799 h \quad (9.5)$$

Přibližný čas mezi poruchami je pro použité rezistory tedy 109167 let a pravděpodobnost poruchy je možné vyhodnotit jako 1 – nepravděpodobná. Pravděpodobnost poruchy pro rozpojený obvod je zvýšena na 2 – nízká z důvodů možného selhání pájeného spojení v důsledku vibrací, teplotní roztažnosti či nesprávného zapájení součástky.

## 9.2 Výpočet poruchovosti bočníku

Bočník použitý při návrhu je typu metal element SMD.

Pro daný typ rezistoru norma [13] neuvádí, pro výpočet tedy byly použity rovnice výkonového tlustovrstvého rezistor.

$$\lambda_p = \lambda_b * \pi_R * \pi_Q * \pi_E \left( \frac{Poruch}{10^6 h} \right), \quad (9.6)$$

kde  $\lambda_b$  značí základní poruchovost součástky,  $\pi_R$  je faktor odporu součástky,  $\pi_Q$  je faktor kvality součástky a  $\pi_E$  je faktor prostředí. Pro výpočet základní poruchovosti součástky byla použita rovnice:

$$\lambda_b = 7,33 * 10^{-3} * e^{0,202 * \left( \frac{T+273}{298} \right)^{2,6}} * e^{\left( \frac{S}{1,45 * \left( \frac{T+273}{273} \right)^{0,89}} \right)^{1,3}} \left( \frac{Poruch}{10^6 h} \right), \quad (9.7)$$

kde  $T$  značí maximální provozní teplotu a  $S$  značí poměr provozního a jmenovitého výkonu součástky. Předpokládaná maximální teplota pro LEO mise by dle [14] neměla překročit 60 °C. Poměr provozního a jmenovitého proudu nepřesáhne dlouhodobě  $S = 0,3$ . Základní poruchovost je pak:

$$\lambda_b = 0,011 \left( \frac{Poruch}{10^6 h} \right) \quad (9.8)$$

Koeficient odporu je pro bočník  $\pi_R = 1$ .

Koeficienty kvality a prostředí byly pro výpočet zanedbány.

Výsledná poruchovost součástky pak zůstává:

$$\lambda_p = 0,011 \left( \frac{Poruch}{10^6 h} \right) \quad (9.9)$$

Dále může být určen střední čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 9090909 h \quad (9.10)$$

Přibližný čas mezi poruchou je pro použité bočníky tedy 1037 let a pravděpodobnost poruchy je možné vyhodnotit jako 2 – nepravděpodobná. Pravděpodobnost poruchy pro rozpojený obvod byla vzhledem k velkým pájeným plochám ponechána beze změny.

### 9.3 Výpočet poruchovosti kondenzátorů

Všechny kondenzátory použité při návrhu jsou typu SMD keramické.

Pravděpodobnosti poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = \lambda_b * \pi_{CV} * \pi_Q * \pi_E \left( \frac{Poruch}{10^6 h} \right), \quad (9.11)$$

kde  $\lambda_b$  značí základní poruchovost součástky,  $\pi_{CV}$  je faktor kapacity součástky,  $\pi_Q$  je faktor kvality součástky a  $\pi_E$  je faktor prostředí. Pro výpočet základní poruchovosti součástky byla použita rovnice:

$$\lambda_b = 3 * 10^{-4} * \left[ \left( \frac{S}{0.3} \right)^3 + 1 \right] * e^{\left( \frac{T+273}{358} \right)} \left( \frac{Poruch}{10^6 h} \right), \quad (9.12)$$

kde  $T$  značí maximální provozní teplotu a  $S$  značí poměr provozního a jmenovitého napětí součástky. Předpokládaná maximální teplota pro LEO mise by dle [14] neměla překročit 60 °C. Největší poměr provozního a jmenovitého napětí dosahuje v zapojení 0,206, tudíž zvolený koeficient  $S = 0,2$ . Dosazení do rovnice (9.12 vychází základní poruchovost:

$$\lambda_b = 0,000986 \left( \frac{Poruch}{10^6 h} \right) \quad (9.13)$$

Pro kondenzátory do 100 nF může být použit koeficient  $\pi_{CV} = 1,45$  získaný výpočtem následující rovnice:

$$\pi_{CV} = 0,41 * (C * 10^{12})^{0,11} \quad (9.14)$$

Koeficient kvality může být za předpokladu dostatečné kvality součástek zanedbán. Koeficient prostředí byl při výpočtu zanedbán. Výsledná poruchovost součástky je pak:

$$\lambda_p = 0,00143 \left( \frac{Poruch}{10^6 h} \right) \quad (9.15)$$

Dále může být určen střední čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 699300699 h \quad (9.16)$$

Přibližný čas mezi poruchami je pro použité kondenzátory je tedy 79776 let a pravděpodobnost poruchy je možné vyhodnotit jako 1 – nepravděpodobná. Pravděpodobnost poruchy rozpojený obvod je zvýšena na 2 – nízká z důvodů možného selhání pájeného spojení v důsledku vibrací, teplotní roztažnosti či nesprávného zapájení součástky.

#### 9.4 Výpočet poruchovosti integrovaných obvodů s počtem tranzistorů < 1000

Integrované obvody s menším počtem tranzistorů zahrnují CAN vysílače/přijímače, I2C opakovače a jednoduchá hradla. Do této kategorie nejsou zařazeny integrované obvody s vysokým výstupním proudem.

Pravděpodobnosti poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = (C_1 * \pi_T + C_2 * \pi_E) * \pi_Q * \pi_L \left( \frac{Poruch}{10^6 h} \right), \quad (9.17)$$

kde  $C_1$  značí základní poruchovost součástky,  $\pi_T$  je faktor maximální teploty čipu,  $C_2$  značí základní poruchovost pouzdra,  $\pi_E$  je faktor prostředí,  $\pi_Q$  je faktor kvality součástky a  $\pi_L$  je faktor konvenčnosti součástky.

Základní poruchovost pro součástky s počtem tranzistorů do 1000 odpovídá  $C_1 = 0,02$  (poruchovost zahrnuje bipolární i MOS tranzistory).

Maximální teplota čipu pro logické obvody bude vzhledem k minimálnímu výstupnímu zatížení velice blízká ambientní teplotě. Předpokládaná maximální teplota pro LEO mise by dle [14] neměla překročit 60 °C, což odpovídá faktoru  $\pi_T = 0,42$ .

Počet vývodů pouzdra plnicích logickou funkcí je u všech jednoduchých obvodů menší než 10, což odpovídá poruchovosti  $C_2 = 0,0020$ .

Faktory  $\pi_E$  a  $\pi_Q$  byly při výpočtu opět zanedbány. Faktor  $\pi_L = 1$ , jelikož každá z použitých součástek byla uvedena na trh před více jak dvěma lety.

Výsledná poruchovost součástky je pak:

$$\lambda_p = 0,0104 \left( \frac{Poruch}{10^6 h} \right) \quad (9.18)$$

Dále může být určen střední čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 96153846 h \quad (9.19)$$

Přibližný čas mezi poruchami pro použité jednoduché logické obvody je tedy 10 969 let a pravděpodobnost poruchy je možné vyhodnotit jako 2 - nízka.

## 9.5 Výpočet poruchovosti univerzálních diod

Pravděpodobnosti poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = \lambda_b * \pi_T * \pi_S * \pi_C * \pi_Q * \pi_E \left( \frac{Poruch}{10^6 h} \right), \quad (9.20)$$

kde  $\lambda_b$  značí základní poruchovost součástky,  $\pi_T$  je faktor teploty PN přechodu,  $\pi_S$  je faktor poměr operačního a maximálního závěrného napětí,  $\pi_C$  je faktor konstrukce součástky,  $\pi_Q$  je faktor kvality součástky a  $\pi_E$  je faktor prostředí.

Udávaná základní poruchovost pro univerzální diody  $\lambda_b = 0,0038$ .

Vzhledem k nízkým konstantním proudům bude teplota PN přechodu blízká okolní teplotě. Předpokládaná maximální teplota pro LEO mise by dle [14] neměla překročit 60 °C, což odpovídá faktoru  $\pi_T = 3$ .

Poměr operačního a maximálního závěrného napětí nikdy nepřesáhne  $S=0,054$ , což odpovídá  $\pi_S = 0,054$ .

Konstrukční faktor pro SMD diody odpovídá  $\pi_T = 1$ .

Faktory  $\pi_E$  a  $\pi_Q$  byly při výpočtu zanedbány.

Výsledná poruchovost součástky je pak:

$$\lambda_p = 0,000615 \left( \frac{Poruch}{10^6 h} \right) \quad (9.21)$$

Dále může být určen průměrný čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 1626016260 h \quad (9.22)$$

Přibližný čas mezi poruchami je pro použité diody tedy 185 495 let a pravděpodobnost poruchy je možné vyhodnotit jako 1 – nepravděpodobná.

## 9.6 Výpočet poruchovosti výkonových integrovaných obvodů

Výkonové integrované obvody zahrnují v navrhovaném systému ideální diody, LDO stabilizátory a elektronické spínače napájení. Zmíněné obvody obsahují malý počet tranzistorů, ale vzhledem ke zvýšenému výstupnímu proudu jsou více namáhány, což se negativně projeví na celkové spolehlivosti.

Pravděpodobnosti poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = (C_1 * \pi_T + C_2 * \pi_E) * \pi_Q * \pi_L \left( \frac{Poruch}{10^6 h} \right), \quad (9.23)$$

kde  $C_1$  značí základní poruchovost součástky,  $\pi_T$  je faktor maximální teploty čipu,  $C_2$  značí základní poruchovost pouzdra,  $\pi_E$  je faktor prostředí,  $\pi_Q$  je faktor kvality součástky a  $\pi_L$  je faktor konvenčnosti součástky.

Základní poruchovost pro součástky s počtem tranzistorů do 300 v kombinaci digitální a lineární operace odpovídá  $C_1 = 0,02$  (poruchovost zahrnuje bipolární i MOS tranzistory).

Maximální teplota čipu pro obvody napájení může být vzhledem k výstupnímu zatížení značně vyšší než ambientní teplota. Pro výpočet byla zvolena teplota 90 °C, což odpovídá faktoru  $\pi_T = 7$ .

Počet vývodů pouzdra plnících logickou funkci je u všech jednoduchých obvodů menší než 5, což odpovídá poruchovosti  $C_2 = 0,0019$ .

Faktory  $\pi_E$  a  $\pi_Q$  mohou být opět zanedbány. Faktor  $\pi_L = 1$ , jelikož každá z použitých součástek byla uvedena na trh před více jak dvěma lety.

Výsledná poruchovost součástky je pak:

$$\lambda_p = 0,1419 \left( \frac{Poruch}{10^6 h} \right) \quad (9.24)$$

Dále může být určen střední čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 7047216 h \quad (9.25)$$

Přibližný čas mezi poruchami pro použité výkonové integrované obvody je tedy 803 let a pravděpodobnost poruchy je možné vyhodnotit jako 3 - nízká.

## 9.7 Výpočet poruchovosti mikrokontrolerů

Pravděpodobnosti poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = \lambda_{BD} * \pi_{MFG} * \pi_T * \pi_{CD} + \lambda_{BP} * \pi_E * \pi_Q * \pi_{PT} + \lambda_{EOS} \left( \frac{Poruch}{10^6 h} \right), \quad (9.26)$$

kde  $\lambda_{BD}$  značí základní poruchovost čipu součástky,  $\pi_{MFG}$  je faktor procesu výroby,  $\pi_T$  je faktor teploty čipu,  $\pi_{CD}$  je faktor složitosti čipu,  $\lambda_{BP}$  značí základní poruchovost pouzdra součástky,  $\pi_E$  je faktor prostředí,  $\pi_Q$  je faktor kvality,  $\pi_{PT}$  je faktor provedení pouzdra součástky a  $\lambda_{EOS}$  značí ESD odolnost.

Udávaný koeficient základní poruchovosti pro mikrokontroler  $\lambda_{BD} = 0,24$ .

Firma STMicroelectronics je na seznamu kvalifikovaných výrobců [15], a tudíž může být použit faktor  $\pi_{MFG} = 0,55$ .

Maximální povolená teplota čipu mikrokontroleru je 125 °C. To je ovšem velice extrémní případ. Pro výpočet bude jako stropní teplota čipu použita hodnota 100 °C. Při použité CMOS technologii je pak faktor  $\pi_T = 1,3$ .

Velkosti čipu by neměla vzhledem k velikosti pouzdra překročit 25 mm<sup>2</sup> a odhadovaná použitá technologie výroby je 60 nm.  $\pi_{CD}$  je pak možné vypočítat rovnicí:

$$\pi_{CD} = \left[ \left( \frac{A}{0.21} \right) * \left( \frac{2}{X_s} \right)^2 * 0.64 \right] + 0.36 \left( \frac{Poruch}{10^6 h} \right), \quad (9.27)$$

kde A je velikost čipu v cm<sup>2</sup> a X<sub>s</sub> je použitá technologie výroby v μm. Po dosazení vychází faktor složitosti čipu  $\pi_{CD} = 0,61$ .

Základní poruchovost pouzdra  $\lambda_{BP}$  udává rovnice:

$$\lambda_{BP} = 0,0022 + (1,75 * 10^{-5} * NP) \left( \frac{Poruch}{10^6 h} \right), \quad (9.28)$$

kde NP značí počet pinů pouzdra, což je u zvoleného mikrokontroler 32. Po dosazení do rovnice vychází  $\lambda_{BP} = 0,00275 \left( \frac{Poruch}{10^6 h} \right)$ .

Faktory  $\pi_E$  a  $\pi_Q$  byly při výpočtu zanedbány.

Faktor  $\pi_{PT}$  není pro pouzdro LQFP uvedený. Nejbližší uvedené pouzdro je PGA s faktorem  $\pi_{PT} = 2,2$ , u kterého je možné z důvodů menší pružnosti pinů očekávat oproti LQFP nižší spolehlivost. Pro výpočet LQFP byl odhadnut faktor  $\pi_{PT} = 2$ .

Při předpokladu ESD odolnosti v rozmezí 0-1000 V je koeficient  $\lambda_{EOS} = 0,065$ .

Po dosazení všech faktorů do výpočtu vychází celková poruchovost:

$$\lambda_p = 0,4165 \left( \frac{Poruch}{10^6 h} \right) \quad (9.29)$$

Dále může být určen střední čas mezi poruchami:

$$MTBF = \frac{1}{\lambda_p} = 2400960 h \quad (9.30)$$

Přibližný čas mezi poruchami je pro použité mikrokontrolery tedy 274 let a pravděpodobnost poruchy je možné vyhodnotit jako 4 – občasná porucha.

## 9.8 Výpočet poruchovosti MOS tranzistorů

Pravděpodobnosti poruchy  $\lambda_p$  je možné dle normy [13] vypočítat rovnicí:

$$\lambda_p = \lambda_b * \pi_T * \pi_A * \pi_Q * \pi_E \left( \frac{Poruch}{10^6 h} \right), \quad (9.31)$$

kde  $\lambda_b$  značí základní poruchovost součástky,  $\pi_T$  je faktor teploty čipu,  $\pi_A$  je faktor aplikace součástky,  $\pi_Q$  je faktor kvality součástky a  $\pi_E$  je faktor prostředí.

Základní poruchovost pro MOS tranzistory je  $\lambda_b = 0,012 \left( \frac{Poruch}{10^6 h} \right)$ .

Teplota čipu bude vzhledem k minimálním proudům tekoucím tranzistory blízká ambientní teplotě. Předpokládaná maximální teplota pro LEO mise by dle [14] neměla překročit 60 °C, což udává faktor  $\pi_T = 2$ .

Tranzistor je využíván pro spínání malých proudů, proto byl použit aplikační faktor  $\pi_A = 0,7$ .

Koeficienty kvality a prostředí byly při výpočtu opět zanedbány.

Výsledná celková poruchovost je po dosazení faktorů:

$$\lambda_p = 0,0168 \left( \frac{Poruch}{10^6 h} \right) \quad (9.32)$$

Dále může být určen střední čas mezi poruchami:

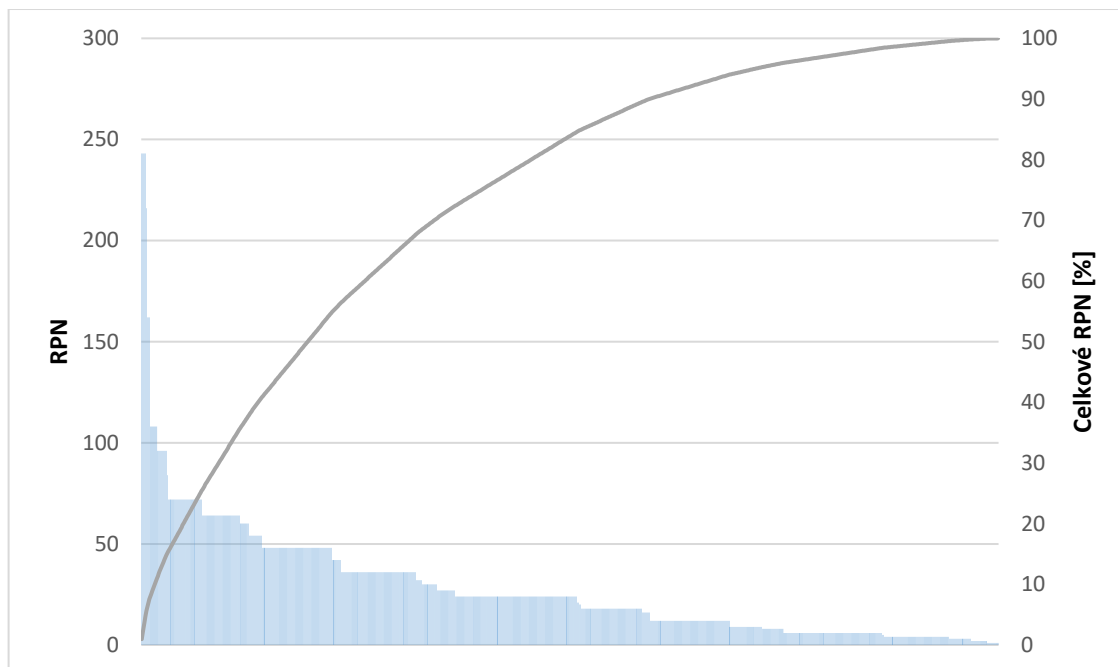
$$MTBF = \frac{1}{\lambda_p} = 59523809 h \quad (9.33)$$

Přibližný čas mezi poruchami je pro použité tranzistory tedy 6790 let a pravděpodobnost poruchy je možné vyhodnotit jako 2 – nízká.



## 9.9 Vyhodnocení výsledků FMEA

Vzhledem k vysokému počtu komponentů obsahuje FMEA velké množství možných poruch a důsledků. Pro desku ve verzi 1.3 přesahují data 900 poruch. Systém je tedy vhodné studovat pomocí Paretova diagramu.



Graf 9.1 - FMEA Peretův diagram pro desku V1.3, kde modré sloupce představují RPN hodnotu poruchy a šedá čára kumulativní procentuální RPN

Výsledky ukazují, že nejkritičtější poruchy systému souvisí s napájecími obvody. Nejvyšší kritické číslo 243 je přiřazeno poruchám LDO stabilizátorů, kdy v případě zkratu vstupu na výstup může dojít k poškození integrovaných obvodů daného subsystému. Příčinou poruchy může být přehřátí součástky, či SEGR. Použité integrované obvody LDO stabilizátorů mají ochranu proti přehřátí, kterou výpočet poruchovosti nezahrnuje. Výsledné kritické číslo je však vysoké z důvodu neověřené radiační odolnosti použitých stabilizátorů. Při poruše stabilizátoru IC12 nastane systém nefunkční, ale nedojde k poškození systému. Takový případ je označený druhým největším RPN číslem – 216 a je opět převážně způsobeno neznámou radiační odolností součástky.

Další závažnou poruchou s RPN číslem 162 může být zkrat vstupu a výstupu ideálních diod, což by mohlo zapříčinit tok proudu ze sloučeného napětí V\_Merged zpět do jednoho ze zdrojů s nižším napětím. Taková porucha je vzhledem k testované zvýšené odolnosti obvodů méně pravděpodobná, ale bylo by vhodné učinit zdroje takové poruše odolné.

Zbytek poruch buď způsobí pouze částečnou nefunkčnost systému, nebo jsou velmi nepravděpodobné.

## 10 Současný stav a doporučení dalšího vývoje

Vzhledem k omezenému času při návrhu zařízení byl vývoj zaměřen na hardwarové zvýšení spolehlivosti. Tato kapitola slouží jako přehled současných funkcí a doporučení možných způsobů dalšího vývoje hardwaru a softwaru.

### 10.1 Hardware

Navržený systém je možné napájet třemi zdroji pracujícími v režimu horké redundance, kdy systém bude napájený nejvyšším z přítomných napájecích napětí. Napájecí část dále poskytuje nadproudovou ochranu, prioritní podpět'ovou ochranu a řízení sekvence zapínání podsystémů. Každý z podsystémů má vlastní proudové omezení.

Podsystémy se skládají ze dvou bloků mikrokontrolerů a dvou skupin I2C periférií, kde každá I2C skupina obsahuje 4 větve pro celkovou podporu osmi I2C periférií.

Mikrokontrolery jsou až do potvrzení správné funkčnosti pomocí WDT odpojeny od zbytku systému. Mikrokontroler po potvrzení správné funkčnosti může odpojit napájení druhého mikrokontroleru, čímž je možné volit režim provozu mezi studenou a teplou redundancí. Při teplé redundanci je zavedena Master-Slave hierarchie.

Každá větev I2C periferie obsahuje napájení pro danou periferii, detekci nadproudu a proudové omezení. Připojení individuálních I2C periférií ke zbytku systému je řízeno Master mikrokontrolerem. Při zapojení identických I2C periférií na větve rozdílných I2C skupin je možné pro periferie dosáhnout horké redundance.

Funkcionalita systému může být dále rozšířena následujícími úpravami hardwaru:

- **Implementace integrovaného proudového a napět'ového měření**

Pro řízení spotřeby v případě provozu z bateriového zdroje je nutné měřit napětí zdroje a spotřebu systému. Přidáním bočníků pro měření proudu před LDO stabilizátor subsystémů je možné za použití ADC převodníku měřit napětí na bočníku úměrné proudu odebíraného daným subsystémem. Doporučené měření proudu: Celkový proud na větvi V\_merged, proudy napájecích bloků pro mikrokontrolery periferie

Doporučené měřené napětí: Napájecí napětí na vstupech hlavního konektoru PWR1-3

Pro měření celkových osmi napětí mohou být použity dva integrované obvody MCP3424. Jeden obvod umožňuje měření čtyř kanálů s diferenciálním

vstupem a v ukázkovém programu již byly vytvořeny funkce pro inicializaci obvodu a vyčítání napětí.

### - **Implementace integrované paměti**

Pro pokročilou diagnostiku je nutné uchovávat data o stavech systému před poruchou. Vzhledem k riziku poruchy Master procesoru je nejjednodušší možností uchovávat diagnostická data v paměti mimo procesor. Paměť může být připojena jako externí periferie, ale vzhledem k benefitům pokročilé diagnostiky je vhodné paměť integrovat přímo do systému. Paměť FRAM se dle výzkumu [4] jeví díky své zvýšené odolnosti vůči SEE a TID jako velice vhodným řešením.

## **10.2 Software**

Software v současné implementaci obsahuje pouze základní funkce pro obsluhu desky. Program využívá postupného spínání napájení podsystémů pro rozdělení Master-Slave hierarchie. Hierarchie je udržována odesíláním hlavičky s Master příznakem mezi mikroprocesory přes CAN rozhraní. Dále je implementována funkce volby provozu mikrokontrolerů mezi režimem teplé a studené redundance.

Program umožňuje rozpoznat stavy jednotlivých větví I2C periferií uložené v příslušných diagnostických polích. Rozpoznané stavy mohou být: připojené zařízení, nepřipojené nebo nefunkční zařízení a zkrat napájení. Uživatelskou proměnnou je možné zapnout paměť zkratu větví, kdy zkratované větve budou z diagnostiky až do resetu mikrokontroleru vyřazeny.

Funkcionalita systému může být značně rozšířena následujícími úpravami softwaru:

### - **Implementace pokročilé diagnostiky**

Při přidání integrované paměti, zmíněné v doporučených hardwarových změnách, je možné zavést pokročilou diagnostiku v závislosti na stavu systému před poruchou. Většina mikrokontrolerů již obsahuje integrovaný WDT. V kapitole 2.2.2 byl zmíněn mód, kdy WDT vyvolá nemaskované přerušení a následně uloží diagnostická data. Vnitřní WDT by bylo možné využít pro zmíněnou funkci při nastavení časování tak, aby vnitřní WDT vyvolal při poruše NMI s dostatečnou časovou rezervou před zareagováním externího WDT resetem. Implementace proudového měření napájecích bloků pro mikrokontrolery a periferie by umožnilo nastavení limitních operačních

proudových limitů pro každé z daných zařízení a opět zlepšilo diagnostiku systému.

### - **Implementace přístupu Slave mikrokontroleru na I2C sběrnice**

Slave mikrokontroler má fyzický přístup k I2C sběrnicím, ale nemůže je vzhledem k případné kolizi na sběrnici obsluhovat. Funkcí v programu lze přístup na sběrnici Slave mikrokontroleru dočasně přidělit. Slave mikrokontroler odešle žádost o přístup k periférii a Master v případě nečinnosti na sběrnici dočasně přiřadí přístup k dané I2C sběrnici Slave mikrokontroleru. Funkci lze implementovat na desce V1.3.

### - **Implementace záložního způsobu komunikace mezi mikrokontrolery**

V případě selhání CAN komunikace může být I2C použita jako záložní komunikace. I2C mikrokontroleru je možné inicializovat i jako Slave zařízení. MCU1.1 má oproti MCU1.2 22 ms časovou výhodu při zapnutí. Při neúspěšném rozdělení Master-Slave hierarchie přes CAN rozhraní může první z mikrokontrolerů odeslat hlavičku s příznakem přítomného Master mikrokontroleru přes I2C a zachovat tak hierarchii i komunikaci mezi mikrokontrolery. Vzhledem ke dvěma I2C sběrnicím je možné v případě potřeby docílit plně duplexní komunikace. Funkci lze implementovat na desce V1.3.

### - **Implementace módu pro zvýšený výpočetní výkon**

V případě potřeby je možné, vzhledem ke dvěma I2C sběrnicím, rozdělit přístup mikrokontrolerů na sběrnice. Master mikrokontroler by například obsluhoval sběrnici I2C1 a Slave mikrokontroler sběrnici I2C2. Při vhodném rozdělení periférií je tak možné využívat mikrokontrolery jako dvě jádra a potřebná společná data si vyměňovat přes rozhraní CAN. Funkci lze implementovat na desce V1.3.

## Zhodnocení a závěr

Náplní práce byl návrh systému propojení běžných mikrokontrolerů a senzorů s cílem zvýšení spolehlivosti celkového systému pro použití v náročných prostředích. Předkládaný návrh využívá redundance a odpojitelných částí systému. Zvýšení spolehlivosti bylo ověřeno měřeními a analýzou poruch a jejich důsledků. Měření dokazuje, že systém je odolný vůči poruchám na mikrokontrolerech i senzorech a zachovává si maximální funkčnost. FMEA ukázala, že nejkritičtější poruchy mohou vzniknout, i přes největší pravděpodobnost poruchy mikrokontroleru, pouze v napájecím obvodu systému. Vzhledem k možnosti využití systému pro více generací mikrokontrolerů a senzorů je možné několik kritických komponentů vybrat na základě testování radiační odolnosti a dosáhnout tak optimálního poměru výsledné ceny a spolehlivosti.

Řešení ukazuje velký potenciál rozšíření funkcionality dalším vývojem hardwaru a softwaru. Představuje tak atraktivní možnost vývoje systémů se zvýšenou spolehlivostí.

Navrhované řešení přináší zlevnění, zrychlení a zvýšení spolehlivosti vývoje.

## Literatura

- [1] BOSSER, Alexandre. SINGLE-EVENT EFFECTS OF SPACE AND ATMOSPHERIC RADIATION ON MEMORY COMPONENTS [online]. Finland, 2017 [cit. 2023-05-26]. Dostupné z: <https://jyx.jyu.fi/handle/123456789/56348>. Academic Dissertation for the Degree of Doctor of Philosophy. University of Jyväskylä.
- [2] BAUMANN, Robert a Kirby KRUCKMEYER. Radiation Handbook for Electronics [online]. Dallas, Texas: Texas Instruments Incorporated, 2020 [cit. 2023-05-26]. Dostupné z: <https://www.ti.com/applications/industrial/aerospace-defense/space/radiation-handbook-for-electronics.html>
- [3] REGULAPATI, Varsha. Error Correction Codes in NAND Flash Memory [online]. 2015 [cit. 2023-05-26]. Dostupné z: <https://repositories.lib.utexas.edu/handle/2152/33302>. Master of Science in Engineering. University of Texas at Austin.
- [4] Radiation Evaluation of Ferroelectric Random Access Memory Embedded in 180nm CMOS Technology. In: <https://www.ti.com> [online]. Dallas, Texas: Texas Instruments Incorporated, 2016 [cit. 2023-05-26]. Dostupné z: <https://www.ti.com/lit/wp/sboa154/sboa154.pdf>
- [5] TILLI, Markku, Teruaki MOTOOKA, Veli-Matti AIRAKSINEN, Sami FRANSSILA, Mervi PAULASTO-KRÖCKEL a Veikko LINDROOS. Handbook of Silicon Based MEMS Materials and Technologies: Second Edition [online]. William Andrew, 2015 [cit. 2023-05-26]. ISBN 978-0-323-29965-7. Dostupné z: <https://doi.org/10.1016/C2013-0-19270-7>
- [6] VOBORNÍK, Aleš, Ivo VEŘTÁT a Richard LINHART. Experimental Electric Power System for Small Satellites with Independent Supply Channels. In: Články / Articles (KAE) [online]. Západočeská univerzita v Plzni, 2018 [cit. 2023-05-26]. ISBN 978-80-261-0721-7. ISSN 1803-7232. Dostupné z: <http://hdl.handle.net/11025/35493>
- [7] FISHER, Graham, Michael SEACRIST a Robert STANDLEY. Silicon Crystal Growth and Wafer Technologies. Proceedings of the IEEE [online]. 2012, (100), 1454 - 1474 [cit. 2023-05-26]. ISSN 1558-2256. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/6178756>

- 
- [8] SINGH, Rahul Kr., Amit SAXENA a Mayur RASTOGI. SILICON ON INSULATOR TECHNOLOGY REVIEW. International Journal of Engineering Sciences & Emerging Technologies, [online]. 2011 [cit. 2023-05-26]. ISSN 2231-6604. Dostupné z: [https://www.researchgate.net/publication/263889224\\_SILICON\\_ON\\_INSULATOR\\_TECHNOLOGY\\_REVIEW](https://www.researchgate.net/publication/263889224_SILICON_ON_INSULATOR_TECHNOLOGY_REVIEW)
- [9] Cold vs. hot standby mission operation cost minimization for 1-out-of-N systems. ScienceDirect: European Journal of Operational Research [online]. 2014, (234) [cit. 2023-05-26]. Dostupné z: doi: <https://doi.org/10.1016/j.ejor.2013.10.051>
- [10] Research on EDAC Schemes for Memory in Space Applications. MDPI [online]. 2021 [cit. 2023-05-26]. Dostupné z: <https://doi.org/10.3390/electronics10050533>
- [11] GANSSLE, Jack. A Designer's Guide to Watchdog Timers. In: DigiKey [online]. Convergence Promotions, 2012 [cit. 2023-05-26]. Dostupné z: <https://www.digikey.com/en/articles/a-designers-guide-to-watchdog-timers>
- [12] STAMATIS, D. H. Failure Mode and Effect Analysis. Milwaukee, Wisconsin: ASQ Quality Press, 2003. ISBN 9780873895989.
- [13] MIL-HDBK-217F: Military Handbook – Reliability Prediction of Electronic Equipment. Washington: US Department of Defense, 1991.
- [14] REISS, Philip. New Methodologies for the Thermal Modelling of CubeSats. In: Proceedings of the Small Satellite Conference [online]. Technische Universitat Munchen, 2012 [cit. 2023-05-26]. Dostupné z: <https://digitalcommons.usu.edu/smallsat/2012/all2012/67/>
- [15] Qualified Suppliers List. In: Defense Logistics Agency [online]. 2023 [cit. 2023-05-26]. Dostupné z: <https://www.dla.mil/What-DLA-Offers/Consumable-Hardware/Qualified-Suppliers-List/>