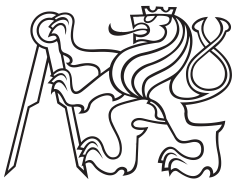
Diplomová práce



České
vysoké
učení technické
v Praze

F3

Fakulta elektrotechnická
Katedra radioelektroniky

Bezpečná akustická výstražná signalizace

Safety Acoustic Warning System

Jakub Rösler

Školitel: doc. Ing. Petr Skalický, CSc.
Obor: Vysokofrekvenční a digitální technika
Praha 2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Rösler** Jméno: **Jakub** Osobní číslo: **434936**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra radioelektroniky**

Studijní program: **Otevřené elektronické systémy**

Studijní obor: **Vysokofrekvenční a digitální technika**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Bezpečná akustická výstražná signalizace

Název diplomové práce anglicky:

Safety Acoustic Warning System

Pokyny pro vypracování:

Navrhněte a realizujte bezpečné datově ovládané výstražné zvukové zařízení ve smyslu ČSN 34 2600, splňující požadavky technické specifikace SŽDC TS 1/2018-Z (Výstražné zařízení pro přechod kolejí) a ČSN EN 50129. Datová komunikace bude plnit požadavky pro přenosový systém kategorie 1 ČSN EN 50 159. Zvukové výstražné zařízení bude připojeno dvojicí datových linek podle standardu RS485 s poloduplexním provozem a napájecím napětím 48 V/50 Hz. Architektura řešení je specifikována 2oo2, tj. dva galvanicky oddělené mikroprocesorové systémy se vzájemnou kontrolou a s bezpečným komparátorem. Použijte mikroprocesory s lock-step strukturou. Každá větev systému 2oo2 musí být napájena samostatným galvanicky odděleným zdrojem napětí. Součástí diplomové práce bude i rozbor bezpečnosti komparátoru. Software bude vypracován jazyku C podle standardu MISRA. Specifikované maximální rozměry zařízení jsou 18*12*12 cm. Zařízení otestujte v požadovaném teplotním rozsahu, tj. -40°C až 70°C.

Seznam doporučené literatury:

[1] Cortex-M4 Procesor – ARM [online]. ARM Ltd. [cit. 2016.04.15]. Dostupné z: https://www.arm.com/products/processors/cortex-m/cortex-m4-processor.php
[2] MISRA-C:2004: MIRA Limited, 2004, 2008, Edition 2 reprinted July 2008, ISBN 978-0-9524156-4-0
[3] Skalický,Petr.: Přístrojové aplikace mikropočítačů.Praha: Vydavatelství ČVUT 2004, skripta

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. Ing. Petr Skalický, CSc., katedra radioelektroniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **20.09.2019** Termín odevzdání diplomové práce: **22.05.2020**

Platnost zadání diplomové práce: **19.02.2021**

doc. Ing. Petr Skalický, CSc. podpis vedoucí(ho) práce	doc. Ing. Josef Dobeš, CSc. podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

. Datum převzetí zadání

Podpis studenta

Poděkování

Rád bych na tomto místě poděkoval Ing. Josefu Martincovi, Ing. Martinu Liptajovi, Ph.D. a dalším pracovníkům Závodu Technika společnosti AŽD Praha s. r. o. za cenné rady při návrhu zařízení a doc. Ing. Petru Skalickému, CSc. za odborné vedení práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Abstrakt

Tato diplomová práce se zabývá vývojem akustické části datově ovládaného výstražného zabezpečení pro přechod kolejí (VZPK). Zařízení je navrženo tak, aby splňovalo podmínky norem pro drážní zařízení, z nichž vyplývají požadavky na bezpečnost komunikace, vnitřního zpracování dat a kontrolu výstupu. Tyto požadavky vedou na uspořádání 2oo2 (two-out-of-two), ve kterém je informace ze dvou oddělených datových linek zpracovávána ve dvou nezávislých větvích, které se obě podílejí na generování výstupního signálu. Výstupy z obou větví jsou bezpečně sloučeny a výsledný signál je přiveden do elektroakustického měniče (EAM). Proud přiváděný do EAM je monitorován dvěma snímacími obvody a v obou větvích nezávisle vyhodnocován.

Klíčová slova: Přechod kolejí, bezpečnost, signalizace pro nevidomé, drážní zařízení

Školitel: doc. Ing. Petr Skalický, CSc.

Abstract

This diploma thesis deals with the development of an acoustic part of a data-controlled rail crossing warning system. The device is designed to meet the standards for railway applications, which state requirements for safety-related communication, internal data processing and output monitoring. These requirements lead to a 2oo2 (two-out-of-two) architecture, where the data from two independent data lines are processed by two independent branches, which both participate on the output signal generation. Signals from the both branches are safely combined and used for electroacoustic transducer excitation. The current to the transducer is monitored by two separate circuits and evaluated independently by both branches.

Keywords: Railway crossing, safety, signalling for visually impaired, railway applications

Title translation: Safety Acoustic Warning System

Obsah

Obrázky

Tabulky

Kapitola 1
Úvod

1.1 Použité zkratky

2oo2	Two-out-of-two
ASN	Akustická signalizace pro nevidomé - navrhované zařízení
Bd	Baud, jednotka modulační rychlosti (zde rovná přenosové rychlosti [bit/s])
BCH	Bose–Chaudhuri–Hocquenghem (autoři BCH kódů)
BI	Bezpečnostně irelevantní, nevztahující se k bezpečnosti
BR	Bezpečnostně relevantní, vztahující se k bezpečnosti
DMA	Direct memory access - přímý přístup do paměti
EAM	Elektro-akustický měnič
EEPROM	Electrically Erasable Programmable Read-Only Memory
GF(n)	Galoisovo těleso o n prvcích
GPIO	General Purpose Input/Output
LSb/LSB	Least significant bit/byte - nejméně signifikantní bit/byte
MSb/MSB	Most significant bit/byte - nejvíce signifikantní bit/byte
NS	Nadřízená stanice
PS	Podřízená stanice
RS	Reed-Solomon (autoři RS kódů)
USART	Universal Synchronous/Asynchronous Receiver and Transmitter
VZPK	Výstražné zařízení pro přechod kolejí

1.2 Účel zařízení

V železničních stanicích s poloostrovními nástupišti je třeba v souladu s příslušnými požadavky Technických specifikací pro interoperabilitu (TSI) [1] zabezpečit centrální přechod přes koleje optickou i akustickou signalizací. Použití klasických výstražníků pro železniční přejezdy není mj. z důvodu jejich rozměrů vhodné. Proto Správa železniční dopravní cesty, s. o. (SŽDC, dnes Správa železnic, s. o.) vydala technickou specifikaci [2], která určuje požadavky na systém VZPK, sestávající se z optické a akustické části. Tato práce se zabývá pouze návrhem akustické části (označované jako ASN), která

bude součástí kompletního systému VZPK firmy AŽD Praha s. r. o. (dále jen zadavatel). Řídicí povely jsou generovány ovládacím zařízením (nadřízenou stanicí) na základě informací ze staničního zabezpečovacího zařízení a požadavků z vysílačky povelů nevidomého. Signál VOLNO se zjednodušeně řečeno vydává po dobu dvou minut od přijetí povelu z vysílačky povelů, pokud přes přechod není dovolena jízda vlaku. Signál STŮJ se vydává vždy, když je přes přechod dovolena jízda vlaku.

Navrhované zařízení bude přímo povelované z nadřízené stanice, komunikace bude řešena dle firemního standardu zadavatele - protokolu LEUNET [14], blíže popsaného v kapitole 2.1.

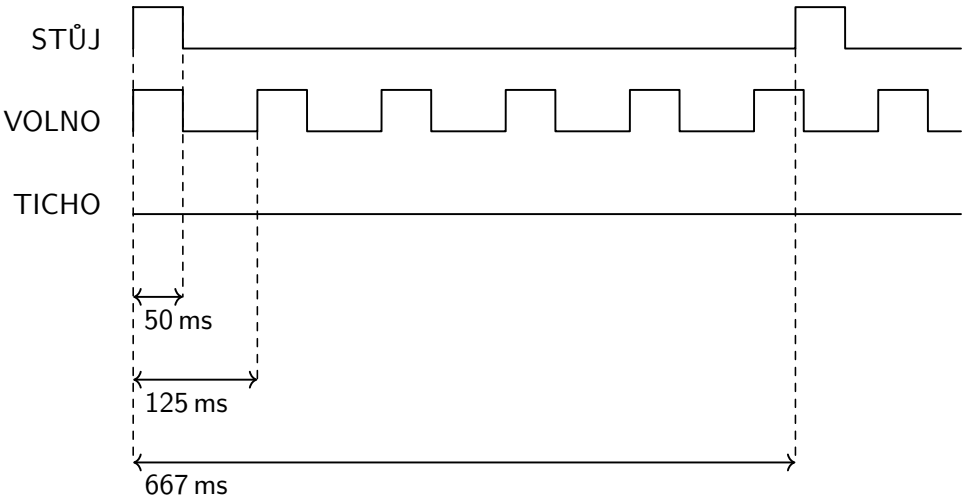
Technická specifikace [2] dále požaduje, aby jedna porucha nezpůsobila nevydávání signálu STŮJ nebo VOLNO. Toho bude docíleno umístěním dvou zařízení na jednom stožáru. Požadované střídání zdrojů zvuku v takovém případě zajistí nadřízená stanice.

1.3 Vydávané signály

Akustické signály pro přechody pro chodce upravuje §14 vyhlášky ministerstva dopravy č. 294/2015 Sb. [3]. Podle ní má zařízení vydávat následující signály:

- STŮJ s kmitočtem 1,5 Hz
- VOLNO s kmitočtem 8 Hz

Pro účely návrhu se uvažuje dále signál označený jako TICHO, kdy zařízení nevydává žádný zvuk. Nosná frekvence zvukového signálu musí být pro přejezdové zabezpečovací zařízení, kam spadá i VZPK, v rozmezí 900 . . . 1100 Hz. Střída signálu není vyhláškou přesně určena, požaduje pouze krátký tón. Délka tónu byla stanovena na 50 ms pro STŮJ i VOLNO. Požadovaná intenzita zvuku je 60. . . 80 dB ve vzdálenosti 7 m [4].



Obrázek 1.1: Časování modulační obálky generovaných zvukových signálů

1.4 Obvodová koncepce

Soubor požadavků na železniční zabezpečovací zařízení, mezi něž navrhované zařízení spadá, shrnuje norma [5], která obsahuje i odkazy na další závazné normy. Mezi ně patří i bezpečnost při poruše (fail-safe), což znamená, že jedna porucha musí být detekována a nesmí způsobit nebezpečí. Jednotlivá nebezpečí a poruchy k nim vedoucí jsou blíže popsány v kapitole 4. Tento požadavek výrazně formuje celkovou koncepci zařízení. Norma [6] uvažuje tři způsoby zajištění bezpečnosti při poruše:

1. **Složená** - Každá funkce vztahující se k bezpečnosti musí být prováděna alespoň dvěma nezávislými jednotkami. Chyba v jedné z nich musí být detekována a negována druhou jednotkou.

2. **Reaktivní** - Funkce vztahující se k bezpečnosti může být prováděna pouze jednou jednotkou, pokud je jakýkoliv nebezpečný poruchový stav rychle detekován a negován.

3. **Inherentní** - Funkce vztahující se k bezpečnosti smí být prováděna jednou jednotkou za předpokladu, že žádné hodnověrné druhy poruch nejsou nebezpečné.

Navrhované zařízení má být datově ovládané po sériové lince. Řešení z diskrétních součástek, které by umožnilo zajištění inherentní bezpečnosti celého zařízení, nepřipadá vzhledem ke složitosti v úvahu, zbývají mikrokontroléry a hradlová pole. Norma [8] klade takové požadavky na zabezpečení komunikace (blíže viz kapitolu 2.1), jejichž splnění by bylo v hradlovém poli poměrně komplikované, obzvláště s uvážením, že nelze použít hotová řešení bez zhodnocení jejich bezpečnosti. Jako vhodné se tedy jeví použití mikrokontrolérů a tím pádem složené bezpečnosti, tedy systém označovaný jako 2oo2 (two-out-out-two). Vyhodnocení přijatých zpráv bude prováděno nezávisle ve dvou větvích; komunikační linka bude rovněž řešena jako dvojitá, přičemž každý procesor bude komunikovat po jedné větvi, vyhodnocení přijatých zpráv z každé větve ovšem bude probíhat nezávisle v obou větvích.

Protože výstupem mají být akustické signály z jednoho zdroje zvuku, je třeba výstupy z těchto větví bezpečným způsobem sloučit a takto sloučeným signálem budit EAM. Pro slučování připadají v úvahu dvě možnosti: komparátor s inherentní bezpečností nebo komparátor obyčejný, jehož bezpečnost bude zajištěna reaktivně. Kvůli tomu, že o poruše budiče nebo EAM musí být předána informace nadřízené stanici (nedetekované nevyžádané ticho je považováno za nebezpečné), musí existovat zpětná vazba o správné funkci EAM. Té je možné využít i k zajištění reaktivní bezpečnosti komparátoru, což oproti inherentní variantě vede na jednodušší hardwarový návrh. Tato možnost tedy bude dále sledována.

V souladu s požadavkem na nezávislost větví plynoucím z [6] bude zařízení rozděleno do šesti galvanicky oddělených sekcí:

- **Vnější napájecí** - spojena s napájecí linkou

- **Vnější A** - spojena s komunikační linkou A
- **Vnější B** - spojena s komunikační linkou B
- **Vnitřní A** - obvody spojené s mikrokontrolérem ve větvi A
- **Vnitřní B** - obvody spojené s mikrokontrolérem ve větvi B
- **Vnitřní C** - obvody komparátoru, budiče a snímání proudu

Linky označené jako vnější jsou galvanicky spojené s vodiči vedoucími mimo zařízení a musejí být odděleny od vnitřních obvodů izolační bariérou 4 kV [5]. Dále platí, že mezi jakýmikoliv vnitřními i vnějšími sekcemi navzájem musí být izolační hladina 500 V.

Těmto požadavkům je uzpůsoben napájecí zdroj (viz kapitolu 3.10) i celý zbytek zařízení. Komunikace mezi jednotlivými sekcemi bude opticky oddělena.

1.5 Softwarová koncepce

Požadavky na software specifikuje norma [9]. Podstatné jsou zejména nároky na programovací jazyk a proces vzniku softwaru.

Vhodným programovacím jazykem pro mikrokontroléry je jazyk C; norma [9] v příloze D54 ovšem klade řadu omezení, například zakazuje nepodmíněné skoky nebo vícenásobné vstupy a výstupy cyklů. Standard MISRA C [10], vyvinutý původně pro automobilový průmysl, definuje detailní požadavky na kód, který vyhovuje normě [9].

V systému 2oo2 je dále požadováno, aby program pro každou větev byl vytvořen jiným programátorem. Pro účely této práce nebude tento požadavek splněn, pro budoucí schvalování bude ovšem třeba nechat napsat software pro jednu z větví jiným programátorem.

Kapitola 2
Teoretická část

Tato kapitola se zabývá rozborem výchozích předpokladů před zahájením návrhu. Protože dokumentace k použitému komunikačnímu protokolu LEUNET není veřejně dostupná, jsou zde rozebrány jeho základní principy, zásadní pro následnou implementaci.

Dále je zde popsána teorie Reed-Solomonových kódů, použitých nejen pro zabezpečení komunikace v síti LEUNET, ale i v dalších částech návrhu.

2.1 Protokol LEUNET

Norma [8] rozděluje přenosové systémy do tří kategorií:

- Kategorie 1 - Uzavřený přenosový systém
- Kategorie 2 - Otevřený přenosový systém
- Kategorie 3 - Otevřený přenosový systém, který může být vystaven neautorizovanému přístupu se škodlivým úmyslem

Tato práce se zabývá pouze návrhem podřízené stanice v systému kategorie 1. Aby se předešlo nutnosti navrhovat i nadřízenou stanici a z důvodu unifikace v rámci firemního portfolia, byl zvolen pro přenos dat protokol LEUNET [14], používaný ve firemním řešení traťové části systému ETCS (European Train Control System - jednotný evropský vlakový zabezpečovač). Název vychází ze zkratky LEU - Lineside Electronic Unit. Tento protokol vyhovuje nejen pro systémy kategorie 1, ale i kategorie 2. Účelem této kapitoly je popsat části protokolu LEUNET relevantní pro aplikaci v navrhovaném zařízení.

Komunikační protokol je tvořen čtyřmi vrstvami, jejichž porovnání s referenčním ISO/OSI modelem znázorňuje tabulka 2.1.

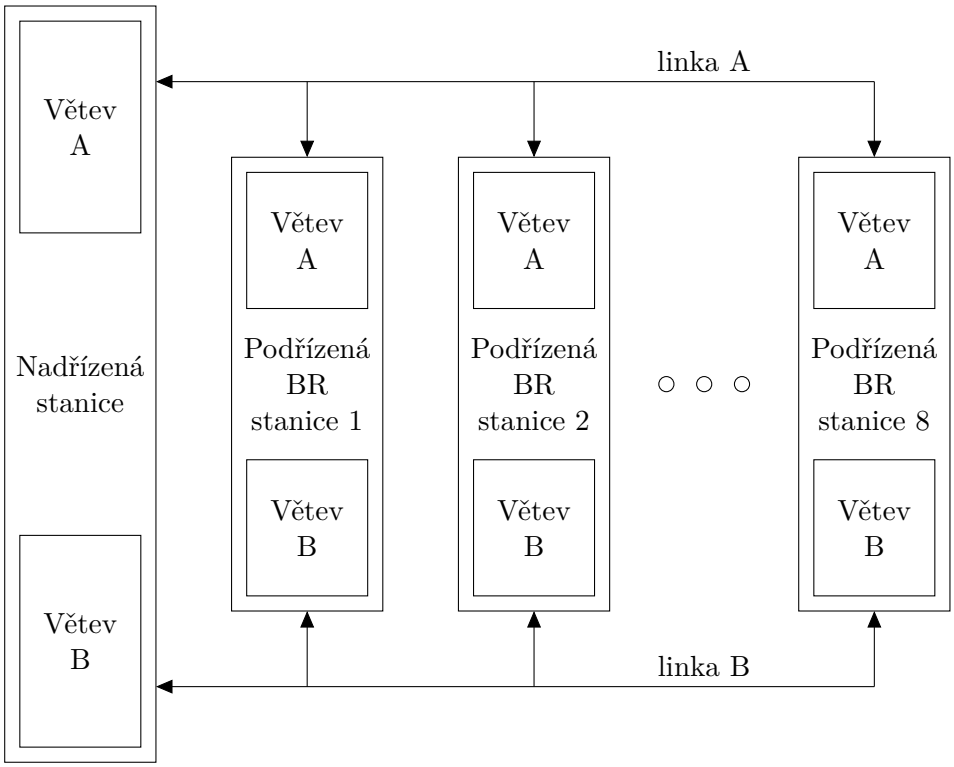
2.1.1 Fyzická vrstva

Síť LEUNET je tvořena jednou nadřízenou stanicí (NS) a až 8 BR podřízenými stanicemi (PS). Topologie sítě je znázorněna na obrázku 2.1. Každá stanice je dvouvětvovým zařízením pracujícím v režimu 2oo2, přičemž každá z větví je připojena k jedné z linek A a B, což jsou poloduplexní sběrnice RS-485.

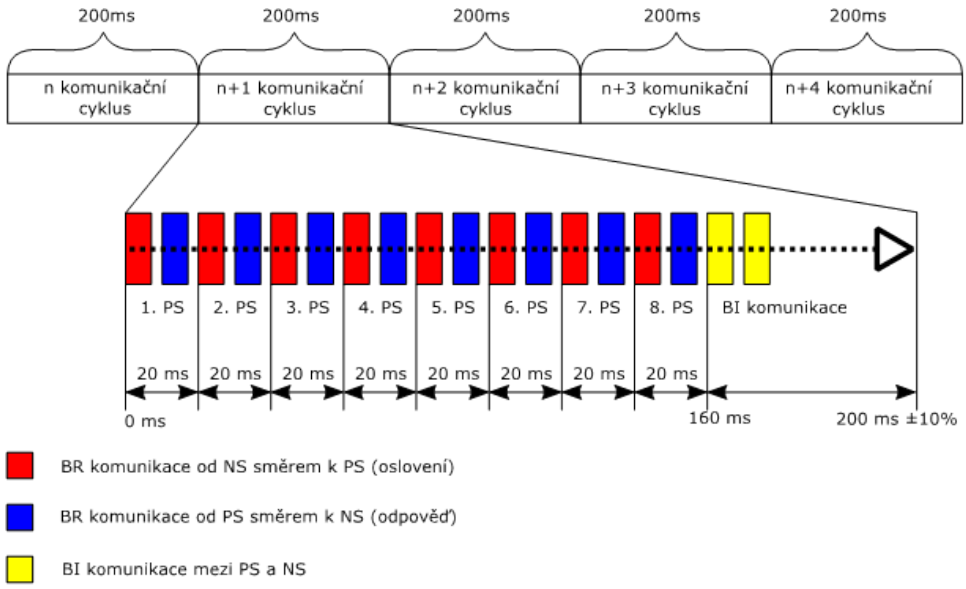
#	ISO/OSI	LEUNET
7	Aplikační	Aplikační
6	Prezentační	Relační
5	Relační	
4	Transportní	Přenosová
3	Síťová	
2	Spojová	
1	Fyzická	Fyzická

Tabulka 2.1: Porovnání síťových vrstev protokolu LEUNET s referenčním modelem ISO/OSI

Přenášené znaky jsou jedenáctibitové, tvořené START bitem (log. 0), 8 bity dat v pořadí od nejméně signifikantního, WAKE-UP bitem a STOP bitem (log. 1). WAKE-UP bit je v log. 1 pouze u bytu adresy vysílaného nadřízenou stanicí, jinak je v log. 0. Rychlost přenosu je stanovena na 115 200 Bd.



Obrázek 2.1: Topologie sítě LEUNET. BI stanice se v sítích, do nichž bude řešené zařízení připojováno, nebudou vyskytovat, proto nejsou zobrazeny, přestože protokol LEUNET s nimi obecně počítá.



Obrázek 2.2: Znázornění komunikace v síti LEUNET, převzato z [14]

2.1.2 Přenosová vrstva

Komunikace v síti LEUNET je založena na přenosu tzv. datagramů (neboli paketů), tedy určitého počtu bytů s danou strukturou. Datagram je tvořen čtyřbytovou hlavičkou a tělem. Přenosová vrstva kontroluje hlavičku přijatého datagramu a je-li korektní a přijata ve stanoveném časovém intervalu (tzv. synchrookně, viz níže), zajišťuje příjem těla, které následně předává relační vrstvě. Odpověď od relační vrstvy doplňuje hlavičkou a předává fyzické vrstvě. Nejsou-li k dispozici data od relační vrstvy, vysílá synchronizační datagram ISP (ISN v případě NS), tvořený pouze hlavičkou.

Výměna datagramů probíhá periodicky s periodou $200\,\text{ms} \pm 10\,\%$, synchronně v obou větvích s povolenou odchylkou 10 ms. Během periody jsou postupně obsluhovány jednotlivé podřízené stanice tak, že NS vyšle BR datagram s adresou určené PS a tato s odstupem času $T3 \geq 100\,\text{ms}$ odpoví. Posledních 40 ms komunikačního cyklu je vyhrazeno pro BI komunikaci. Časové rozvržení komunikace je znázorněno na obrázku 2.2.

Formát hlavičky

Hlavička je tvořena vždy čtyřmi byty s následující strukturou

1. **Adresa** - Adresa podřízené stanice, pro niž je datagram určen, resp. která jej vytvořila. Adresy jsou voleny tak, aby jejich vzájemná Hammingova vzdálenost byla alespoň 2.
2. **Délka** – Počet bytů těla datagramu.
3. **Příznaky** – Určují typ datagramu.
4. **Zabezpečení** – Viz kapitolu 2.2.2.

Stavový automat přenosové vrstvy

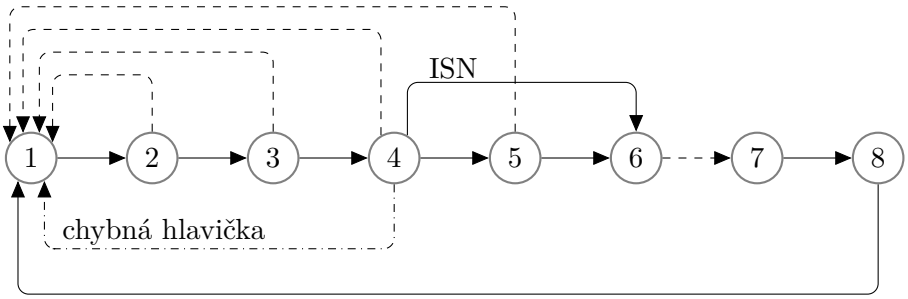
Přenosová vrstva se chová jako konečný stavový automat s níže uvedenými stavy a definovanými přechody mezi nimi. Stavové automaty jednotlivých větví jsou vzájemně nezávislé. Po zapnutí se nachází automat ve stavu 1. Ve stavech 2 - 5 je příjem každého následujícího bytu očekáván po dobu $T1 = 120\,\mu s$. Pokud do vypršení této doby nepřijde, přechází automat do stavu 1.

1. **Stav očekávání příjmu** – V tomto stavu je očekáván příjem bytu adresy shodného s adresou této stanice. Při jeho přijetí přechází automat do stavu 2.
2. **Stav očekávání délky** – Je očekáván byte s významem délky. Po jeho příjmu přechází automat do stavu 3.
3. **Stav očekávání příznaků** – Je očekáván byte příznaků. Po jeho příjmu přechází automat do stavu 4.
4. **Stav očekávání zabezpečení hlavičky přenosové vrstvy** – Je očekáván byte zabezpečení. Po jeho přijetí je proveden test integrity (neporušenosti) hlavičky, dále se kontroluje přípustnost délky datagramu a příznakových bytů. Je-li příznak synchronizačního bytu aktivní, pak se v případě, že se relační vrstva nachází v jiném stavu než WAIT I1 kontroluje, zda byla hlavička přijata v časovém intervalu $\langle 200k - 20; 200k + 20\rangle$[ms], $k \in \mathbb{N}$ od příjetí poslední akceptované hlavičky (tzv. synchrookno) a pokud ne, přechází stavový automat přenosové vrstvy do stavu 1. Je-li výsledek všech uvedených kontrol kladný, přechází automat do stavu 5, nebo 6 v případě přijetí ISN.
5. **Stav přijímání těla datagramu** – Dochází k přijímání bytů těla datagramu až do počtu uvedného v hlavičce. Po jejich přijetí ve stanoveném čase přejde automat do stavu 6.
6. **Stav přepínání směru** – Trvá dobu $T3 \geq 100\,\mu s$, po jejímž uplynutí dojde k přepnutí směru na lince a automat přechází do stavu 7.
7. **Stav vysílání odpovědi** – Je vysílán předem připravený datagram odpovědi. Následně přechází automat do stavu 8.
8. **Stav ukončení vysílání** – V paměti vyhrazené pro odpověď jsou předchozí data nahrazena datagramem ISP a automat přechází do stavu 1.

Grafické znázornění stavového automatu je na obrázku 2.3.

2.1.3 Relační vrstva

Relační vrstva umožňuje bezpečný přenos BR dat pomocí navázané relace a dále nezabezpečený přenos BI dat. Relace zajišťuje kontroly účastníků a přenášených datagramů podle doporučení normy [8] pro systémy kategorie 2.



Obrázek 2.3: Stavový automat přenosové vrstvy. Plná čára značí úspěšné přijetí/vyslání příslušných bytů, čárkovaná vypršení časového limitu nebo chybu fyzické vrstvy, čerchovaná negativní výsledek kontrol.

Typy a formát přenášených datagramů

Relační vrstva rozlišuje dva druhy datagramů, podle toho, zda přenášejí bezpečnostně relevantní data.

Bezpečnostně irelevantní datagramy slouží především k přenosu diagnostických informací. Jejich tělo sestává z bytu určujícího typ, několika bytů dat a jednoho bytu zabezpečení. Formát BI datagramů závisí na implementaci a je popsán v kapitole 3.4.5. Specifickým BI datagramem je datagram I0, který má příznak synchronizačního datagramu (a je tedy vysílán v synchrookně) a slouží k ukončení relace. Jeho dva datové byty specifikují důvod ukončení.

Bezpečnostně relevantních datagramů je 6 typů označených I1...I6, přičemž liché vysílá nadřízená stanice a sudé podřízená:

1. **I1** - Požadavek navázání spojení s PS.
2. **I2** - Odezva na požadavek spojení
3. **I3** - Potvrzení navázaného spojení z NS
4. **I4** - Potvrzení navázaného spojení z PS
5. **I5** - Přenos uživatelských dat od NS
6. **I6** - Přenos uživatelských dat od PS

Relace se navazuje postupným úspěšným přenosem datagramů I1...I4., přičemž vytváření následujícího datagramu je podmíněno úspěšným vyhodnocením datagramu předchozího. Dokud tedy stanice ještě nestihla vyhodnotit přijatý datagram a vytvořit nový, vysílá synchronizační datagramy ISN resp. ISP. Navázání relace zahajuje vždy nadřízená stanice vysláním datagramu I1, podřízená stanice považuje relaci za navázanou po přijetí I3, nadřízená po přijetí I4. Následně si stanice vyměňují datagramy I5 a I6 bez ohledu na korektní přijetí datagramu od protistrany, dokud nedojde k ukončení relace přenosem datagramu I0 nebo z důvodu nepřípustné chybovosti (viz níže).

BR datagramy obsahují kromě bezpečných dat rovněž celou řadu dalších informací ("bezpečnostních atributů") zajišťujících bezpečnost podle doporučení normy [8]. Ty jsou přenášeny buď přímo, nebo jako součást skrytých informací zahrnutých do výpočtu zabezpečení.

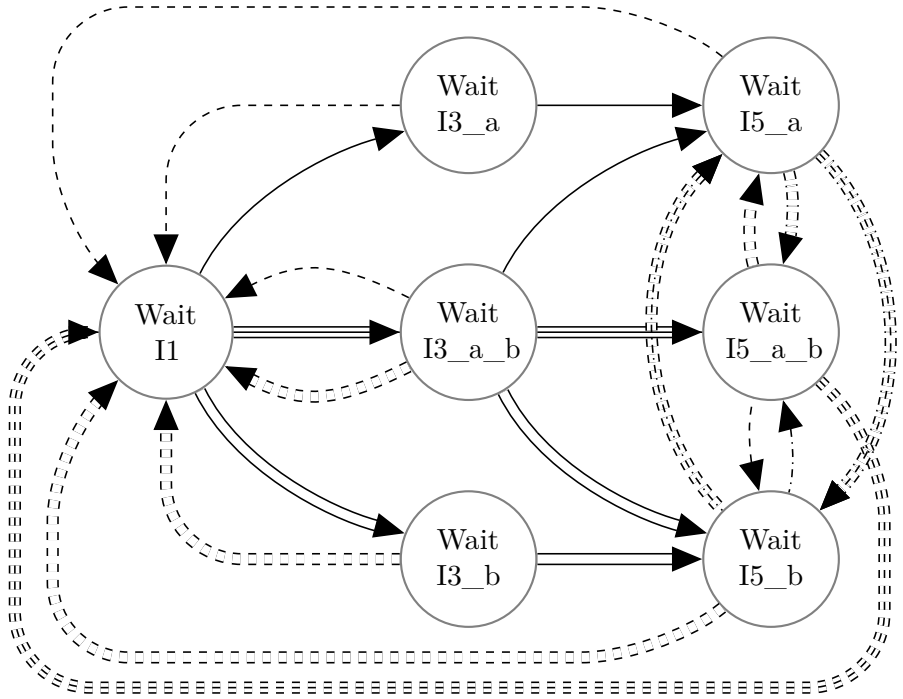
Poměrový čítač chyb

Chybovosti jednotlivých linek jsou sledovány pomocí čítačů chyb ERCa a ERCb. Obecně platí, že při přijetí korektního datagramu I5 příslušnou linkou se hodnota čítače snižuje o P (není-li nulová), při přijetí nekorektního nebo žádného datagramu I5 se zvyšuje o N. Přesáhne-li hodnota čítače hranici M, nastaví se na $M + V$ a datagramy této linky nejsou předávány k dalšímu zpracování aplikační vrstvě (tzv. stav neakceptovatelné chybovosti), dokud hodnota opět nepodklesne pod M. Přejdou-li obě linky do stavu neakceptovatelné chybovosti, dojde k ukončení relace. Čítač je inicializován vždy po navázání spojení na hodnotu $M - 2N$. Konkrétní hodnoty P, M, N a V zde nejsou uvedeny z důvodu neveřejnosti úplného znění protokolu.

Stavový automat relační vrstvy

Relační vrstvu lze rovněž popsat konečným stavovým automatem, který ovšem narozdíl od automatu přenosové vrstvy přísluší celé stanici. K přechodům dochází vždy jednou za komunikační cyklus 200 ms poté, co se zkontrolují přijaté datagramy (nebo se zjistí jejich nepřijetí). Časové prodlevy jsou tedy udávány v násobcích délky programové smyčky, která činí 200 ms. Výchozím stavem je stav Wait I1.

- **Wait I1** – Obě větve očekávají datagram I1. Jeho přijetí v alespoň jedné větvi vede na vytvoření datagramu I2 a automat přechází do stavu Wait I3_a_b (přijetí v obou větvích), nebo Wait I3_a (přijetí pouze ve větvi A), nebo Wait I3_b (přijetí pouze ve větvi B).
- **Wait I3_a_b** – Obě větve očekávají datagram I3. Jeho přijetí alespoň jednou větví vede na vytvoření datagramu I4, nastavení příslušného poměrového čítače (čítačů) chybovosti na hodnotu $M - 2N$ a přechod do stavu Wait I5_a_b, resp. Wait I5_a, resp. Wait I5_b. Příjem nekorektního datagramu způsobí ignorování pozdějšího korektního datagramu z dané linky. Nepřijme-li ani jedna větev korektní datagram během 3 po sobě jdoucích komunikačních cyklů, přijmou-li obě větve datagram nekorektní nebo alespoň jedna z větví přijme datagram I0, stanice vytvoří datagram I0 a přejde do stavu Wait I1.
- **Wait I3_a** – Větev A očekávává datagram I3. Jeho přijetí touto větví vede na vytvoření datagramu I4, nastavení poměrového čítače chybovosti větve A na hodnotu $M - 2N$ a přechod do stavu Wait I5_a. Nepřijme-li větev A korektní datagram během 3 po sobě jdoucích programových cyklů, přijme-li datagram nekorektní, přijme-li pouze linka B korektní datagram nebo alespoň jedna z větví přijme datagram I0, stanice vytvoří datagram I0 a přejde do stavu Wait I1.
- **Wait I3_b** – Analogicky k předchozímu.
- **Wait I5_a_b** – Obě větve očekávají přijetí datagramu I5. Datagram I6 je vytvářen v každém cyklu bez ohledu na přijetí I5. Každé úspěšné přijetí



Obrázek 2.4: Stavový automat relační vrstvy. Plná čára značí úspěšné přijetí příslušných datagramů, čárkovaná vypršení časového limitu přijetí I3 nebo překročení tolerované chybovosti, čerchovaná podkročení tolerované chybovosti. Jednoduchá čára se vztahuje k lince A, dvojitá k lince B, trojitá k oběma současně. Přijetí datagramu I0 vede vždy na přechod do stavu Wait I1 (není zakresleno).

datagramu I5 znamená dekrementaci příslušného poměrového čítače chyb o P, neúspěšné přijetí inkrementaci o N. Překročení tolerované meze chybovosti M čítačem větve A vede na přechod do stavu Wait I5_b, překročení čítačem větve B na přechod do stavu Wait I5_a. Dojde-li současně k překročení meze v obou větvích nebo přijde-li datagram I0, stanice vytvoří datagram I0 a přejde do stavu Wait I1.

- **Wait I5_a** – Pouze korektní datagramy z větve A jsou předávány aplikační vrstvě. Datagram I6 je vytvářen v každém cyklu bez ohledu na přijetí I5. Úspěšné přijetí datagramu I5 některou z větví znamená dekrementaci příslušného poměrového čítače chyb o P, neúspěšné přijetí inkrementaci o N v případě větve A nebo nastavení na hodnotu $M + V$ u větve B. Podkročení tolerované meze chyb čítačem větve B znamená přechod do stavu Wait I5_a_b s výjimkou situace, kdy v témže cyklu dojde k jejímu překročení ve větvi A, čímž automat přejde do stavu Wait I5_b. Dojde-li k překročení tolerované meze ve větvi A (a čítač větve B je nad ní) nebo přijde-li datagram I0, stanice vytvoří datagram I0 a přejde do stavu Wait I1.

- **Wait I5_b** – Analogicky k předchozímu.

2.2 Reed-Solomonovy kódy

Protokol LEUNET využívá pro zajištění integrity přenášených dat Reed-Solomonovy (RS) kódy. Tyto kódy jsou rovněž použity pro kontrolu bezpečnostní značky a konfiguračních dat zapsaných v externí paměti EEPROM, kontrolu programové paměti procesoru a zabezpečení příčné komunikace.

2.2.1 Teorie

Základní myšlenka RS kódů v užším smyslu je následující: Mějme zprávu $\boldsymbol{z} = \{z_1, z_2, \dots z_k\}$ o k symbolech z konečného tělesa $\mathcal{A} = \mathrm{GF}(2^q)$. Dále uvažme sadu různých hodnot $\{\alpha_i\}_{i=1}^{n}$, $\alpha_i \in \mathcal{A}$, prosté zobrazení $\mathcal{Z} : \mathcal{A}^k \to \mathcal{A}^k$, které jednoznačně přiřadí zprávě koeficienty polynomu

$$p(x) = p_{k-1}x^{k-1} + p_{k-2}x^{k-2} + \ldots + p_1 x + p_0, \tag{2.1}$$

tedy

$$\mathcal{Z}(\boldsymbol{z}) = \{p_i\}_{i=0}^{k-1} \tag{2.2}$$

a $n \in \mathbb{N}$ takové, že $k < n \leq 2^q$. Typicky se volí $\mathcal{Z}$ takové, že přiřadí zprávě přímo koeficienty polynomu ($p_{i-1} = z_i$), nebo hodnoty polynomu v po dvou různých bodech $\{\alpha_i\}_{i=1}^{k}$ ($p(\alpha_i) = z_i$). Kódové slovo $C(\boldsymbol{z})$ má pak délku n a je tvořeno hodnotami polynomu p v bodech $\{\alpha_i\}_{i=1}^{n}$.

$$C(\boldsymbol{z}) = \left(p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_n)\right). \tag{2.3}$$

Předpokládejme, že příjemce přijal toto kódové slovo s t chybnými symboly. Přitom ale ví, že přijatá zpráva je tvořena hodnotami polynomu stupně nejvýše k, tedy jestliže

$$t < n - k, \tag{2.4}$$

pak příjemce jistě přijal alespoň k správných symbolů, které jednoznačně určují onen polynom. Neexistuje tak jiný polynom $p'(x)$, který by procházel jak těmi k korektně přijatými symboly, tak těmi t chybnými. Za podmínky (2.4) je tedy příjemce schopen s jistotou detekovat příjem chybného kódového slova [16].

Alternativní způsob tvorby kódového slova vycházející z BCH kódů spočívá v tom, že odesílatel rovněž přiřadí zprávě koeficienty polynomu $f(x)$ stupně nejvýše k (ať už některým z výše uvedených způsobů, nebo jiným), místo hodnot tohoto polynomu ale vyšle koeficienty jiného polynomu $s(x)$, který je s tímto svázán vztahem

$$s(x) = f(x) \cdot g(x), \tag{2.5}$$

kde $g(x)$ je takzvaný generační polynom stupně $l = n - k$ známý oběma stranám ve tvaru

$$g(x) = x^l + g_{l-1}x^{l-1} + \ldots + g_1 x + g_0 = (x - \beta^c) \cdot (x - \beta^{c+1}) \cdot \ldots \cdot (x - \beta^{c+l-1}), \tag{2.6}$$

kde β je nějaký generátor grupy $\{\mathcal{A} \setminus \{0\}, \cdot, 1\}$ a $c \in \mathcal{A} \setminus \{0\}$.

Použití po sobě jdoucích mocnin generátoru garantuje minimální hammingovskou vzdálenost dvou platných kódových slov rovnu $l + 1$. [18]

Aby byl kód systematický, lze výše uvedený postup dále upravit vhodnou volbou zobrazení $\mathcal{Z}$ následovně: Uvažme polynom

$$a(x) = a_{n-1}x^{n-1} + \ldots + a_{n-k}x^{n-k} \tag{2.7}$$

s koeficienty $a_{i+n-k} = z_{k-i}$, $i = 1 \ldots k$. Podle věty o dělení polynomů lze najít jednoznačné polynomy $f(x)$ a $r(x)$ stupňů nejvýše $n - 1 - l$ resp. l tak, že

$$a(x) = f(x) \cdot g(x) + r(x). \tag{2.8}$$

Polynom $a(x) - r(x)$ je dělitelný polynomem $g(x)$, lze tedy psát

$$s(x) = f(x) \cdot g(x) = a(x) - r(x) \tag{2.9}$$

v souladu s (2.5), přičemž existuje jednoznačné $\mathcal{Z}$ podle (2.2). V případě $c = 1$ lze dokázat, že tento způsob kódování je ekvivalentní původní definici, přičemž $\{\alpha_i\}_{i=1}^{n} = \{\beta^{i-1}\}_{i=1}^{n}$. [17]. V tomto návrhu jsou využity systematické RS kódy v širším slova smyslu, kdy $c > 1$.

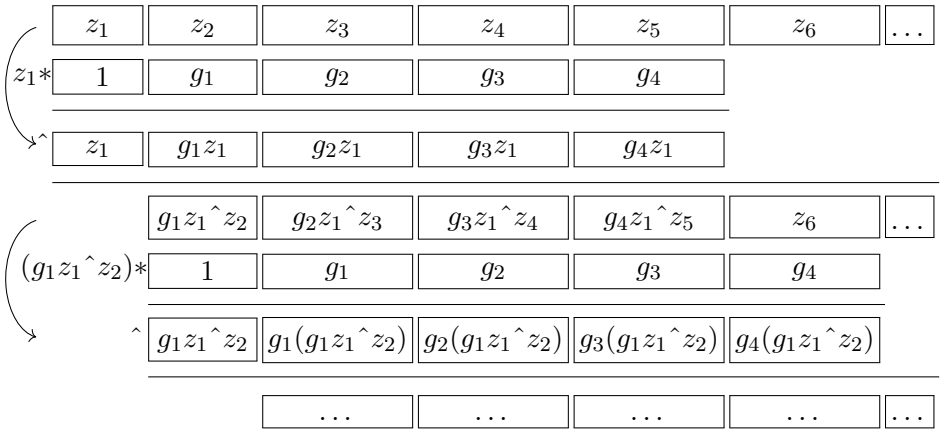
2.2.2 Implementace

Algoritmus generování a kontroly RS kódů je založen na klasickém schématu dělení polynomů (obr. 2.5). K tomu jsou potřeba dvě operace na GF(2^q): sčítání, které se v tělesech tohoto typu redukuje na výhradní součet (dále jen XOR, značený ^) a součin modulo generátor tělesa (značený *). Druhou jmenovanou operaci není z bezpečnostních důvodů vhodné implementovat přímo, místo toho jsou součástí programu tabulky hodnot součinů jednotlivých koeficientů polynomů s čísly 0 až 2^q. Tím je zaručeno, že každý účastník komunikace umí generovat pouze jemu příslušející kódy a chybou programu nemůže snadno vytvořit platný cizí kód.

Vstupem algoritmu je posloupnost $(z_1, z_2, \ldots, z_k)$, výstupem $(r_1, r_2, \ldots, r_{n-k})$ taková, že $g(x)$ bezezbytku dělí $z_1x^{n-1} + z_2x^{n-2} + \cdots + z_kx^{n-k} + r_1x^{n-k-1} + \ldots + r_{n-k-1}x + r_{n-k}$. Díky linearitě a cykličnosti kódu není nutné počítat vždy kód pro celou zprávu najednou, ale je možné aplikovat algoritmus zvlášť na jednotlivé části zprávy. V takovém případě je výsledek výpočtu předchozí části přičten k prvním k členům části navazující.

Byty zabezpečení komunikace v síti LEUNET jsou po získání kódu celé zprávy invertovány a přidány ke zprávě. Smyslem inverze je vyloučit předání neúplné zprávy (neinvertované mezivýsledky nejsou platným kódovým slovem) a minimalizovat pravděpodobnost selhání kontroly chyb na přijímací straně. Ta využívá stejný algoritmus pro výpočet zbytku po dělení. Přípustným výsledkem ale díky zmíněné inverzi není nulová hodnota, která může snadno vzniknout chybou, ale konkrétní nenulová sada koeficientů odpovídající zbytku po dělení polynomu $(2^q - 1)x^{n-k-1} + \ldots + (2^q - 1)x + (2^q - 1)$ polynomem $g(x)$.

Byty zabezpečení jsou v této práci označovány též jako CRC - Cyclic Redundancy Check, protože kód je cyklický. Je třeba mít na paměti, že



Obrázek 2.5: Schéma dělení polynomů v GF(256). Obdélníky představují jednotlivé byty.

se ale nejedná o kód nad GF(2), na kterýžto význam bývá označení CRC často zužováno. V následujících podkapitolách jsou uvedeny podrobnosti k jednotlivým kódům použitým při návrhu.

Zabezpečení hlavičky

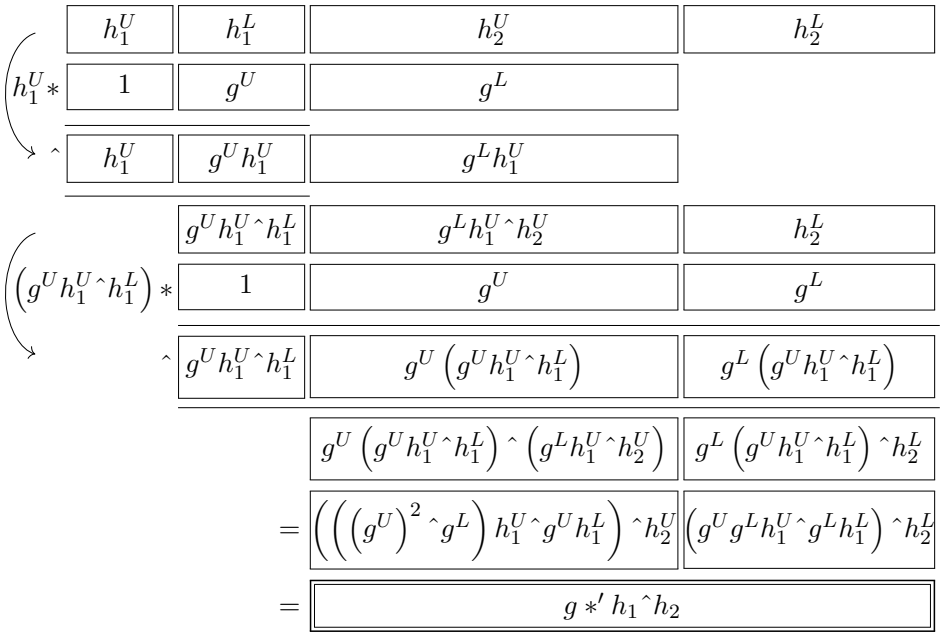
Tři byty dat hlavičky jsou zabezpečeny jedním redundantním bytem. Díky malé délce datové části je možné použít těleso GF(16), díky čemuž jeden byte (dva nibbly) zabezpečení dokáže s jistotou odhalit chybu až dvou libovolných nibblů. Použité polynomy se liší u zpráv vysílaných nadřízenou a podřízenou stanicí i mezi jednotlivými větvemi.

Přestože výpočty v GF(16) by měly z definice probíhat po nibblech, lze dva po sobě jdoucí kroky sloučit do jednoho a operovat po bytech. Tento postup je znázorněn na obrázku 2.6. Místo násobení pak vystupuje operace $*'$, která je pro každé použité g a každou hodnotu bytu hlavičky h_i tabelována. Každá stanice má implementovány pouze polynomy, které generuje nebo kontroluje.

Při generování i kontrole je vždy první byte bitově invertován. Tím je zajištěno, že hlavička tvořená samými nulami není přijata jako správná.

Zabezpečení těl BI datagramů

Všechny BI datagramy, lhostejno které stanice či větve, jsou zabezpečeny jedním redundantním bytem. Všechny do výpočtu vstupující byty jsou interpretovány reverzně, tedy nejvíce signifikantní bit jako nejméně signifikantní, druhý nejvíce signifikantní jako druhý nejméně signifikantní atd. Implementovaná tabulka násobení už tuto reverzaci zohledňuje, samotný výpočet tedy probíhá standardně.



Obrázek 2.6: Schéma dělení polynomů v GF(16). Jednoduché obdélníky představují jednotlivé nibbly, dvojité byty. Dolní index značí pořadí bytu, horní je U pro horní polovinu a L pro dolní.

Zabezpečení těl BR datagramů

Těla BR datagramů jsou zabezpečena polynomy čtvrtého stupně v GF(256). Pořadí bitů je přímé. Každá větev každého typu stanice má implementován právě jeden generační polynom označený písmenem - D a E pro nadřízenou stanici, větve A resp. B a X a Y pro podřízenou stanici, větve A resp. B. Kromě toho má implementovány dvojice kontrolních polynomů kódů ostatních stanic a větví. Každý generační polynom čtvrtého stupně je roven součinu dvojice kontrolních polynomů. Přitom kořeny kontrolních polynomů jsou unikátní. Díky tomuto přístupu, kdy součin v daném tělese není přímo implementován, je prakticky vyloučeno, aby stanice vytvořila platný kód příslušející jiné stanici. 8 bytů zabezpečení na konci každého BR datagramu je tvořeno kontrolními součty v pořadí D, E resp. X, Y.

Zabezpečení programové paměti a příčné komunikace

Pro účely kontroly paměti FLASH a zabezpečení příčné komunikace má každá větev implementovány dvě dvojice kontrolních polynomů prvního stupně, které jsou rozkladem polynomů generačních, dle tabulky 2.2b. Každá větev disponuje generační tabulkou pouze jednoho z těchto polynomů.

Toho se využívá pro zabezpečení příčné komunikace mezi větvemi. Každá větev je schopna přidat na konec každé odesílané příčné zprávy dva byty zabezpečení, nemůže ale žádným způsobem generovat kontrolní byty zpráv, které přijímá.

	Polynom
generující	$x^3 + 221x^2 + 178x + 117$
kontrolní 8-bit	$x + 128$
kontrolní 16-bit	$x^2 + 93x + 19$

(a) : Polynomy zabezpečení externí paměti

	Větev A	Větev B
generující	$x^2 + 157x + 38$	$x^2 + 156x + 117$
kontrolní 1	$x + 29$	$x + 116$
kontrolní 2	$x + 128$	$x + 232$

(b) : Polynomy zabezpečení příčné komunikace a paměti FLASH. Generující polynom pro větev A je implementován pouze ve větvi B a naopak.

Tabulka 2.2: Vybrané polynomy použité RS kódy

Stejné polynomy jsou využity i pro kontrolu paměti FLASH, viz kapitolu 3.7.2.

Těleso GF(256) je generováno polynomem $x^8 + x^4 + x^3 + x^2 + 1$.

Zabezpečení externí EEPROM

Pro zabezpečení dat v paměti EEPROM, uspořádaných do bloků po 50 bytech, slouží 3 byty kontrolního součtu s generačním polynomem podle tabulky 2.2a. Kontrola probíhá pomocí polynomů prvního a druhého stupně. První 3 byty jsou při generování bitově invertovány, při kontrole je toto zohledněno v kontrolní konstantě, s níž je porovnáván výsledek.

Kapitola 3
Návrh

Návrh zařízení respektuje principy shrnuté v úvodu. Jeho srdcem je dvojice mikrokontrolérů z rodiny STM32F302, konkrétně STM32F302CCT7 [19] [20].

Tento 32bitový mikrokontrolér disponuje 256 kB programové paměti typu FLASH, 40 kB operační paměti SRAM a celou řadou periferií, které umožňují nezatěžovat jádro operacemi, které je vhodnější řešit hardwarově. Prezentovaný návrh se snaží v maximální míře využít možností periferií, což vede k determinističtějšímu chování systému (neuplatní se latence přerušení apod.) ve srovnání se softwarově orientovaným návrhem. Nevýhodou tohoto přístupu je fixace na konkrétní typ procesoru a horší přenositelnost návrhu na jinou platformu.

Výběr konkrétního typu byl proveden na základě požadovaných periferií (viz následující kapitolu), zkušeností s danou platformou a unifikace v rámci portfolia zadavatele.

3.1 Využití periferií

Přiřazení hardwarových periferií jednotlivým funkcím je shrnuto v následujících podkapitolách.

3.1.1 Časovače

Tabulka 3.1 znázorňuje využití hardwarových časovačů procesoru. Pro snazší orientaci jsou časovačům označeným dle výrobce pořadovým číslem (první sloupeček) přiděleny názvy podle funkce (alias). Tyto názvy jsou pak pomocí příkazů preprocesoru definovány i pro účely programu, což umožňuje snadno měnit využití jednotlivých periferií během vývoje.

Přidělení úloh jednotlivým časovačům je ovlivněno jejich specifickými funkcionalitami a dostupností vstupních a výstupních signálů jako alternativních funkcí vývodů procesoru. Časovač TIM1 jako jediný může pracovat v módu, kdy jeho vstupní hodinový signál je hradlován okénkovým komparátorem (analogovým watchdogem - AWD) připojeným na výstup AD převodníku, což je nezbytné pro kontrolu proudu do EAM (viz kapitolu 3.8.5). Časovač TIM2 (TIMC - časovač výstupní nosné) umí ze dvou capture/compare (CC) kanálů spouštět jeden kanál přímého přístupu do paměti, čehož se využívá

#	Alias	Délka tiku [us]	Maximální hodnota	Mód	Popis
1	-	1	50[1]	↗	Čítač analogových chyb
2	TIMC	$\frac{1}{36}$	36 000	↗↘	Výstupní frekvence 1 kHz
3	TIMS	100	2 000	↗	Programová smyčka
4	TIMV	100	1 200[1]	↗	Výpadky napájení
16	TIMR	1	200[4]	↗	Přepnutí směru aj.
17	TIMM	500	1 334 /[2] 250	↗	Modulace výstupu
	TIMI	$\frac{1}{72}$ /[3] $\frac{8192}{9}$	65535	↗	Inicializace poř. čísla relace
SysTick		$\frac{1}{9}$	9 000 000	↘	Využit v poměrových čítačích chyb

[1] Určeno přerušením při dosažení hodnoty CC registru, ne přes ARR
[2] Uvedené hodnoty platí při generování signálů STŮJ resp. VOLNO.
[3] Stanice A resp. B
[4] Tento časovač je využíván pro více účelů, uvedená hodnota odpovídá nejčastějšímu použití pro časový interval mezi příjmem datagramu a vysíláním připravené odpovědi (přepnutí směru).

Tabulka 3.1: Využití hardwarových časovačů

pro přepínání AWD. Díky tomu není pro generování a kontrolu nosné výstupního signálu třeba využívat přerušení procesoru, které by jinak muselo být voláno každých 500 µs. Časovač TIM4 (TIMV) slouží pro monitorování napájecího napětí (viz kapitolu 3.12), neboť může být resetován externím signálem. Rozdělení ostatních časovačů není kritické, z důvodu efektivního využití hardwarových prostředků sdílí TIMM a TIMI jeden hardwarový časovač TIM17. Činnost časovače TIMI, pomocí něhož se získává náhodné číslo pro inicializaci pořadového čísla relace, je ukončena při navázání první relace. Teprve poté může být TIM17 využit jako časovač TIMM modulující výstupní signály podle obr. 1.1.

Od hodnoty časovače TIMS se odvíjí časování programové smyčky. TIMR je určen přednostně k zajištění prodlevy při přepínání směru na vnější komunikační lince, je ale použit i pro některé další funkce.

Speciální postavení má časovač SysTick, který je nastaven tak, aby každou sekundu inkrementoval proměnnou `seconds`. Hodnota čítače SysTick a proměnné `seconds` tak dohromady jednoznačně určují čas od spuštění zařízení. Ten slouží jednak pro účely diagnostiky, jednak je od něj odvozena dekrementační hodnota poměrových čítačů analogových chyb (viz kapitolu 3.8.6).

3.1.2 Sběrnice

Použitý mikrokontrolér disponuje třemi periferiemi sériového rozhraní USART. USART2 ovšem sdílí vývody pouzdra a kanály přímého přístupu do paměti s časovačem TIM2, proto pro použití připadají v úvahu pouze USART1 a USART3. USART1 je konfigurován v plně duplexním módu a použit pro

příčnou komunikaci s rychlostí 115 200 Bd. Ve větvi A má nastavenu bitovou inverzi pro příjem i vysílání. Tím se snižuje pravděpodobnost nechtěné záměny vlastních a sousedních dat. USART3 slouží pro vnější komunikaci v síti, je tedy nastaven na poloduplexní provoz s aktivním výstupem Driver Enable (DE) pro řízení směru provozu na lince.

Externí EEPROM je připojena sběrnicí I^2C.

Využití sběrnic shrnuje tabulka 3.2.

Sběrnice	Popis	Duplex
USART1	Příčná komunikace	Full
USART3	Vnější komunikace	Half
I2C1	Externí EEPROM	-

Tabulka 3.2: Využití sběrnic procesoru

3.1.3 Přímý přístup do paměti (DMA)

Každé přerušení procesoru je spojené s určitou časovou ztrátou, způsobenou ukládáním kontextu do zásobníku a po skončení přerušení jeho vybavením. Přímý přístup do paměti umožňuje provádět jednoduché přepisování periferních registrů do operační paměti a naopak a tím šetřit čas procesoru, neboť tento není tak často přerušován.

Použitý procesor je vybaven dvěma periferiemi DMA, s různým počtem kanálů, které jsou spouštěny různými hardwarovými událostmi. DMA2 není využita. Kanály DMA1 jsou naopak využity až na jeden zcela, viz tabulku 3.3. Kanály jedné DMA sdílí prostředky a jejich obsluha při nahromadění více požadavků probíhá postupně dle nastavené priority, v případě rovnosti pak od nejnižšího čísla kanálu k nejvyššímu.

#	Kanál	Priorita	Spouštěč	Směr[1]	Popis
1	1	0	TIM2_CH3	M→P	Nulování čítače analogových chyb
	2	0	USART3_TX	M→P	Vnější komunikace Tx
	3	0	USART3_RX	P→M	Vnější komunikace Rx
	4	0	USART1_TX	M→P	Příčná komunikace Tx
	5	0	USART1_RX	P→M	Příčná komunikace Rx
	7	3	TIM2_CH2 TIM2_CH4	M→P	Přepínání analogových watchdogů

[1] M→P - z paměti do registru periferie; P→M - z registru periferie do paměti

Tabulka 3.3: Využití kanálů přímého přístupu do paměti

3.2 Struktura programu

Průběh inicializace a hlavní programové smyčky znázorňuje obrázek 3.1.

3.2.1 Inicializace

Při zapnutí provádí zařízení sérii úkonů pro kontrolu správné funkce a nastavení potřebných hodnot. Chyba při provádění operací označených * vyvolá nevratnou bezpečnou reakci.

- **Inicializace hodin a GPIO**
- **Čekání na dostatečné napájecí napětí** - Dokud nebude na vstupu PA8 logická nula značící, že vstupní střídavé napájecí napětí přesáhlo hodnotu nastavenou pomocí Zenerovy diody (viz kapitolu 3.12), procesor čeká.
- **Inicializace čítače TIMV a sběrnice I^2C**
- **Kontrola bezpečnostní značky** (viz kapitolu 3.5.1) *
- **Čtení a zápis pořadového čísla spuštění** (viz kapitolu 3.5.3) *
- **Načtení konfigurace** (viz kapitolu 3.5.2) *
- **Inicializace časovačů TIMI a TIMR**
- **Inicializace příčného USARTu**
- **Výměna počátečního bytu** - Počáteční byte slouží k potvrzení, že se sousední větev spustila. Větev A vysílá každých 50 ms byte 0x8B. Větev B čeká na přijetí tohoto bytu a následně vyšle rovněž byte 0x8B větvi A. Když obě stanice přijmou inicializační byte od souseda, pokračují dále. Přijetí jiné hodnoty vyvolá nevratnou bezpečnou reakci. (viz též obrázek 3.2) *
- **Inicializace časovače sysTick**
- **Výměna a kontrola verzí software a otisku konfigurace** - atributy v obou větvích musí být shodné. (viz též obrázek 3.3) *
- **Kontrola paměti FLASH** - všech bloků (viz kapitolu 3.7.2). *
- **Inicializace vnějšího USARTu**
- **Inicializace čítače TIMC**
- **Inicializace analogových kontrol** (viz kapitolu 3.8.5)
- **Povolení přerušení** - vnější USART, analogové kontroly, synchronizační linka
- **Spuštění čítače TIMS**
- **Rozsvícení zelené LED**

3.2.2 Hlavní smyčka

Délka hlavní programové smyčky je shodná s periodou komunikace s nadřízenou stanicí. Při přijetí synchronizačního datagramu s platnou hlavičkou (pouze je-li přijat v synchrookně, s výjimkou stavu Wait I1) jednou z větví se nastaví synchronizační čítač TIMS na hodnotu 1800 odpovídající času smyčky 180 ms a příčným USARTem je vyslán BREAK. Tím se synchronizuje i druhá větev, která datagram nepřijala, nebo přijala později (podrobnosti v kapitole 3.4.2).

Po přetečení časovače TIMS, kdy končí synchronizační okno, je v čase 3 ms zahájena kontrola přijatého datagramu. Nekorektní datagram je zahozen. V čase 4 ms vyšle každá stanice paket příčné komunikace #1 s významem podle tabulky 3.5. Je-li hodnota prvního bytu nejvýše 0xF0, následuje bezprostředně příčná komunikace #2 obsahující tělo přijatého datagramu.

Okamžitě po jejím skončení je zahájena kontrola cizího datagramu. Je-li datagram od souseda nekorektní, nebo se liší od vlastního korektně přijatého datagramu, provede program nevratnou bezpečnou reakci.

Po skončení kontrol je volána funkce `sessionLayerStateMachine`, která zajišťuje přechod stavového automatu relační vrstvy a zpracování dat z přijatého datagramu, podrobnosti jsou uvedeny v kapitole 3.4.3.

Následuje časové okno pro zpracování BI komunikace, viz kapitolu 3.4.5.

V čase 50 ms je inicializována synchronizace časovačů TIMC. Na větvi A je synchronizační výstup (TIM2_CC1_ETR) nastaven na logickou úroveň 1. Při nejbližší spodní úvrati časovače TIMC spadne tento výstup do log. 0, čímž je jednak přímo resetován časovač TIMC ve větvi B (externím resetem na vstupu TIM2_CC1_ETR) a jednak je generováno přerušení, které nastaví čítač TIMM na hodnotu fáze přijatou v datagramu I5 (modulo 125 resp. 667; pokud má být výstup ve stavu TICHO, je TIMM deaktivován) a případně upraví stav výstupu (viz obr. 3.13).

Harmonizace odpovědí je založena na datech příčné komunikace #3, která začíná v čase 100 ms. Její strukturu zachycuje tabulka 3.6. Data pro odpověď se liší pro jednotlivé typy datagramů. Pro I0 se jedná o důvod zrušení relace, pro I2 hodnota pořadového čísla relací, při vytváření ostatních typů datagramů jsou tyto byty nulové.

Následuje sestavení odpovědi a v čase 120 ms výměna bytů zabezpečení (příčná komunikace #4; jen pokud má být nějaká odpověď vytvořena). Přijaté zabezpečovací byty jsou přidány k vytvářenému datagramu a jeho integrita je kontrolována.

Posledním úkonem v programové smyčce je kontrola programové paměti, popsaná blíže v kapitole 3.7.2.

V čase 160 ms začíná synchronizační okno, kdy procesor očekává příjem datagramu.

Časové údaje příčných výměn informací shrnuje tabulka 3.4.

#	Hodnota `TIMS->CNT`			Stručný popis
	odkdy je očekávána	kdy je vysílána	dokdy je očekávána	
1	30	40	200	Informace o přijetí datagramu
2	ihned	ihned		Tělo datagramu od souseda
3	1000	1010	1100	Data pro tvorbu odpovědi
4	1190	1200	1300	Výměna CRC odpovědi
5	1490	1500	1600	Kontrola FLASH

Tabulka 3.4: Přehled časových údajů příčné komunikace

Byte	Hodnota	Význam
1	≤0xF0	Délka těla korektně přijatého datagramu
	0xFC	Přijat nekorektní datagram
	0xFE	Přijat datagram ISN
	0xFF	Nepřijat žádný datagram
	jiná	Rezerva
2...5		Hodnota čítače sebekontroly
6...7		Zabezpečení

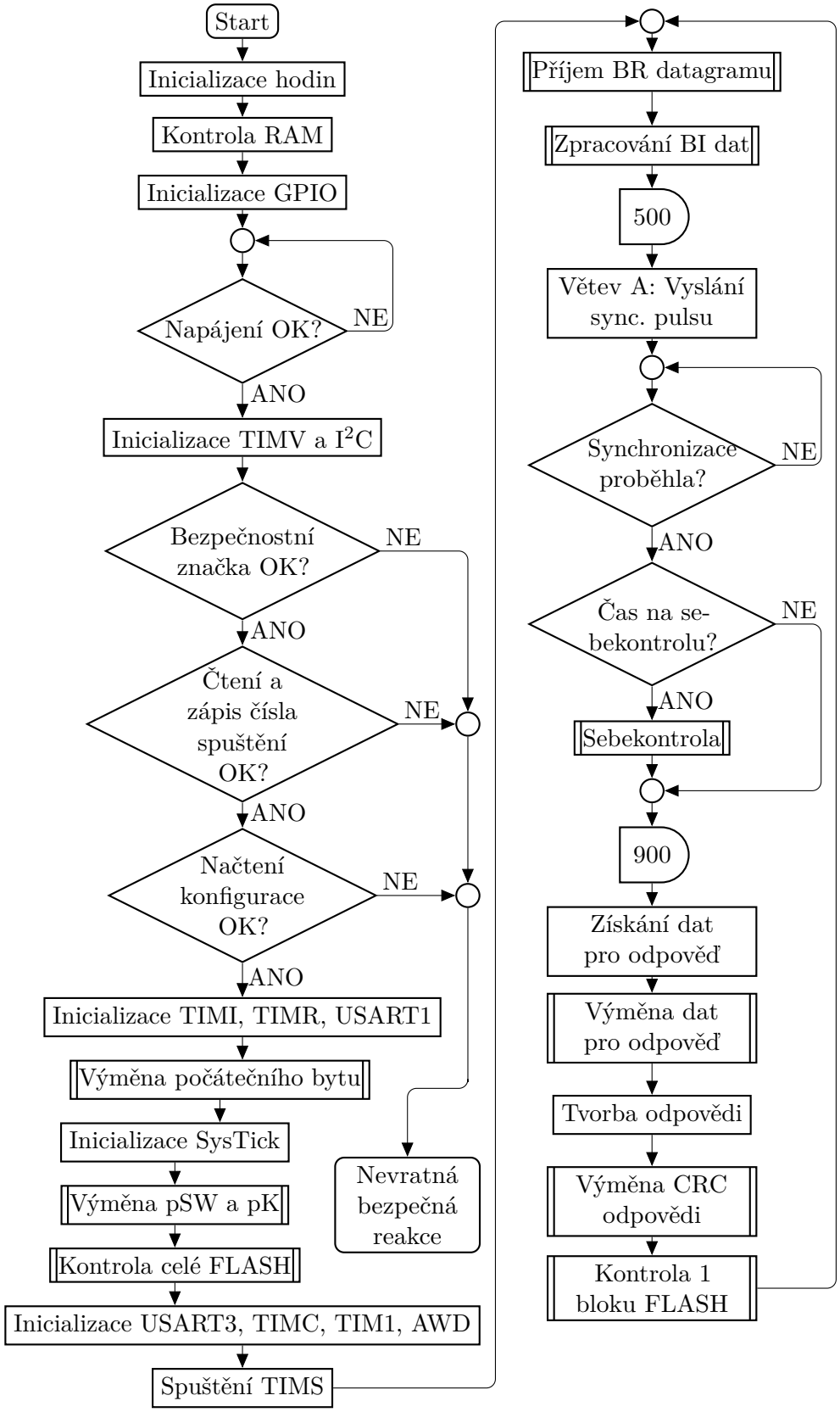
Tabulka 3.5: Příčná komunikace #1

Byte	Význam
1	Stav stavového automatu relační vrstvy
2	Typ datagramu odpovědi
3...6	Data pro odpověď
7...8	Zabezpečení

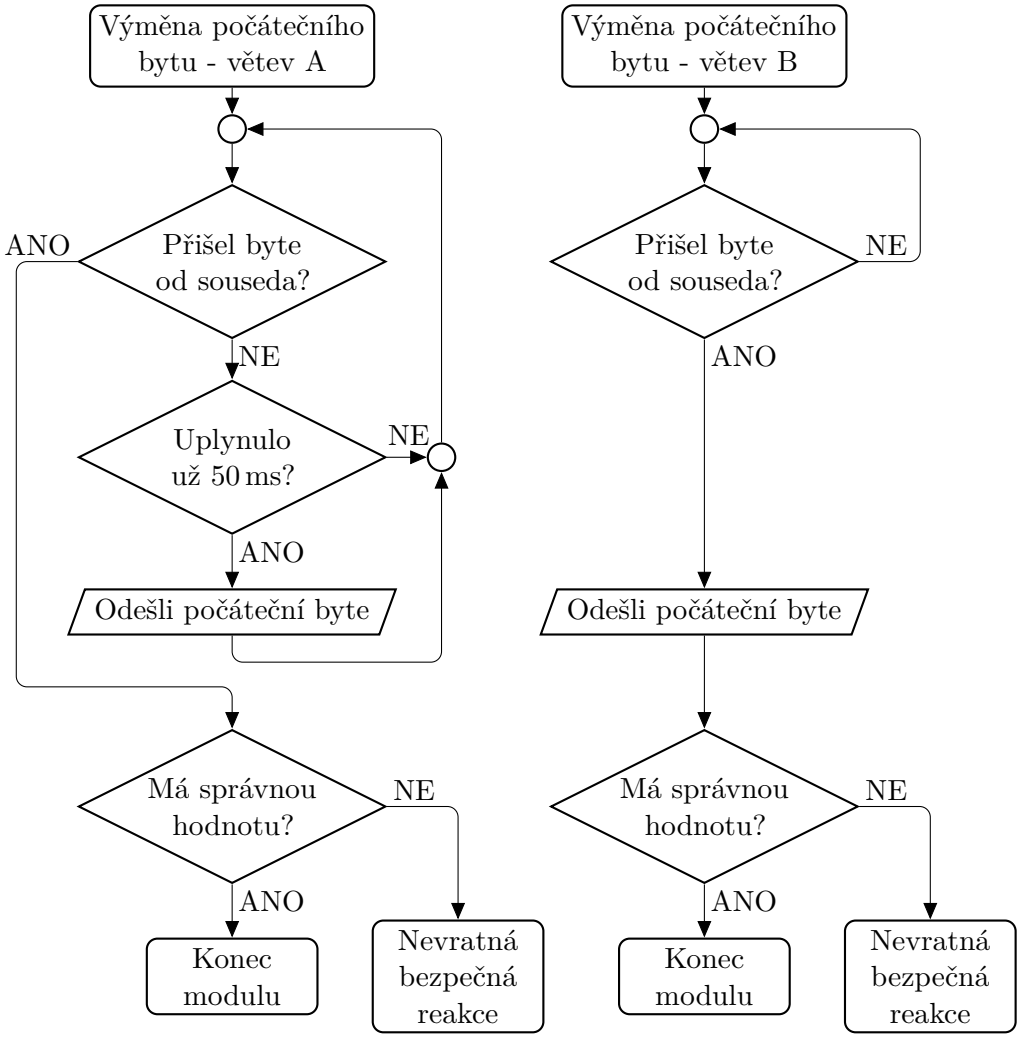
Tabulka 3.6: Příčná komunikace #3

3.3 Vývojové diagramy

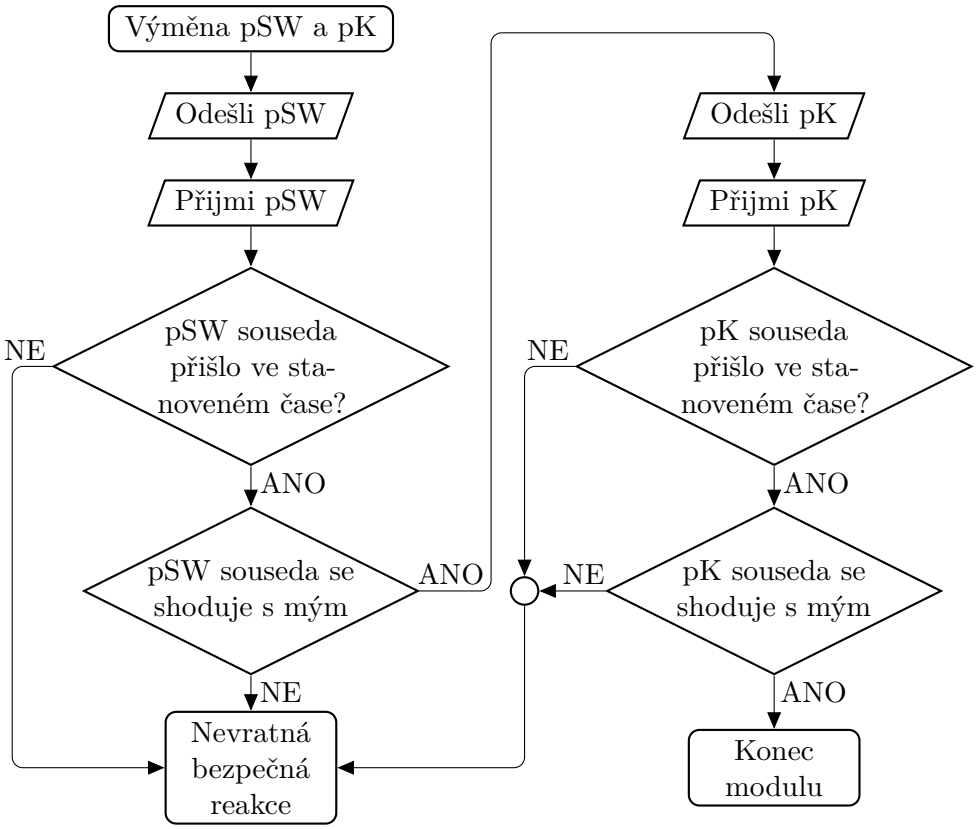
Hlavní programová smyčka, významné funkce a přerušení jsou znázorněny vývojovými diagramy. Kromě běžně používaných symbolů se v nich vyskytuje ještě blok ve tvaru písmene D (z anglického delay). Číslo v něm uvedené odpovídá hodnotě časovače TIMS, do jejíhož dosažení program čeká. Pokud není navázaná komunikace, může v libovolné části smyčky dojít k příchodu synchronizačního datagramu a tím nastavení `TIMS->CNT` na hodnotu 1800. V takovém případě program přeskočí všechny následující úkony a začne pracovat od začátku smyčky. Tato skutečnost není v diagramech pro přehlednost znázorněna.



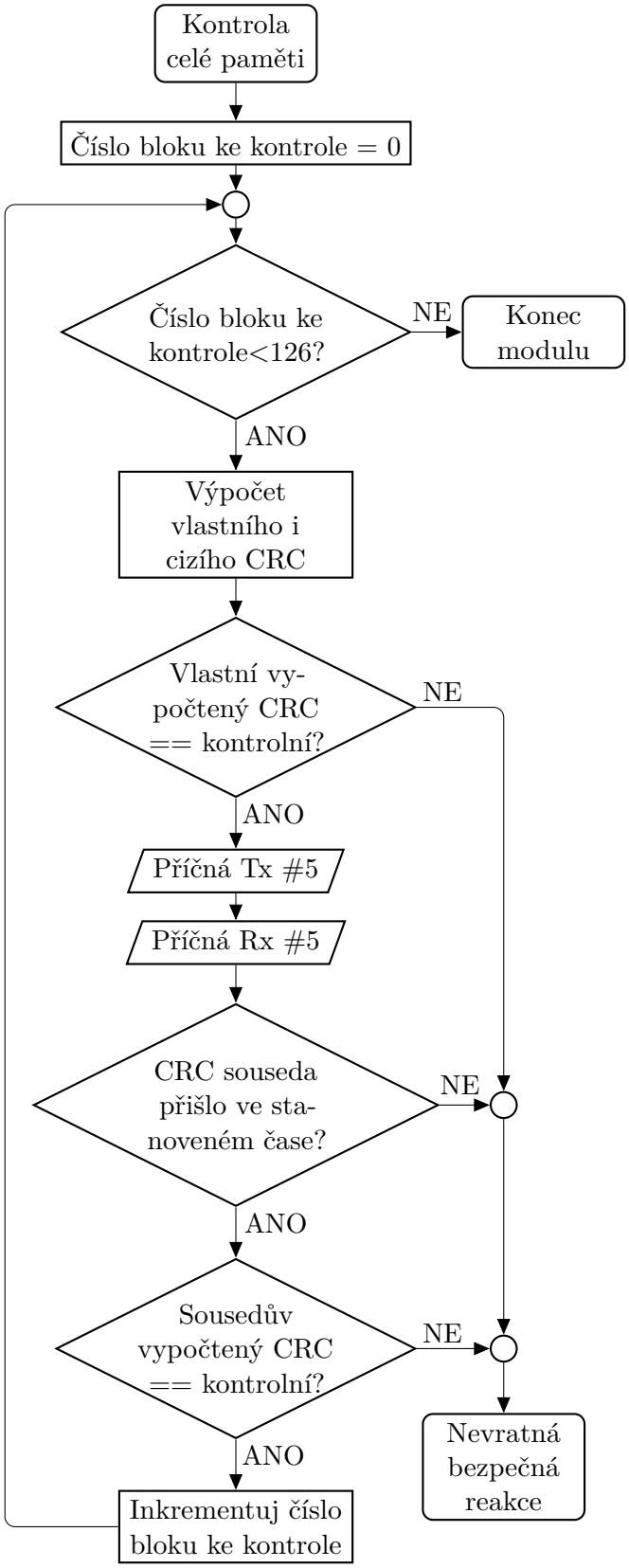
Obrázek 3.1: Vývojový diagram hlavní smyčky programu



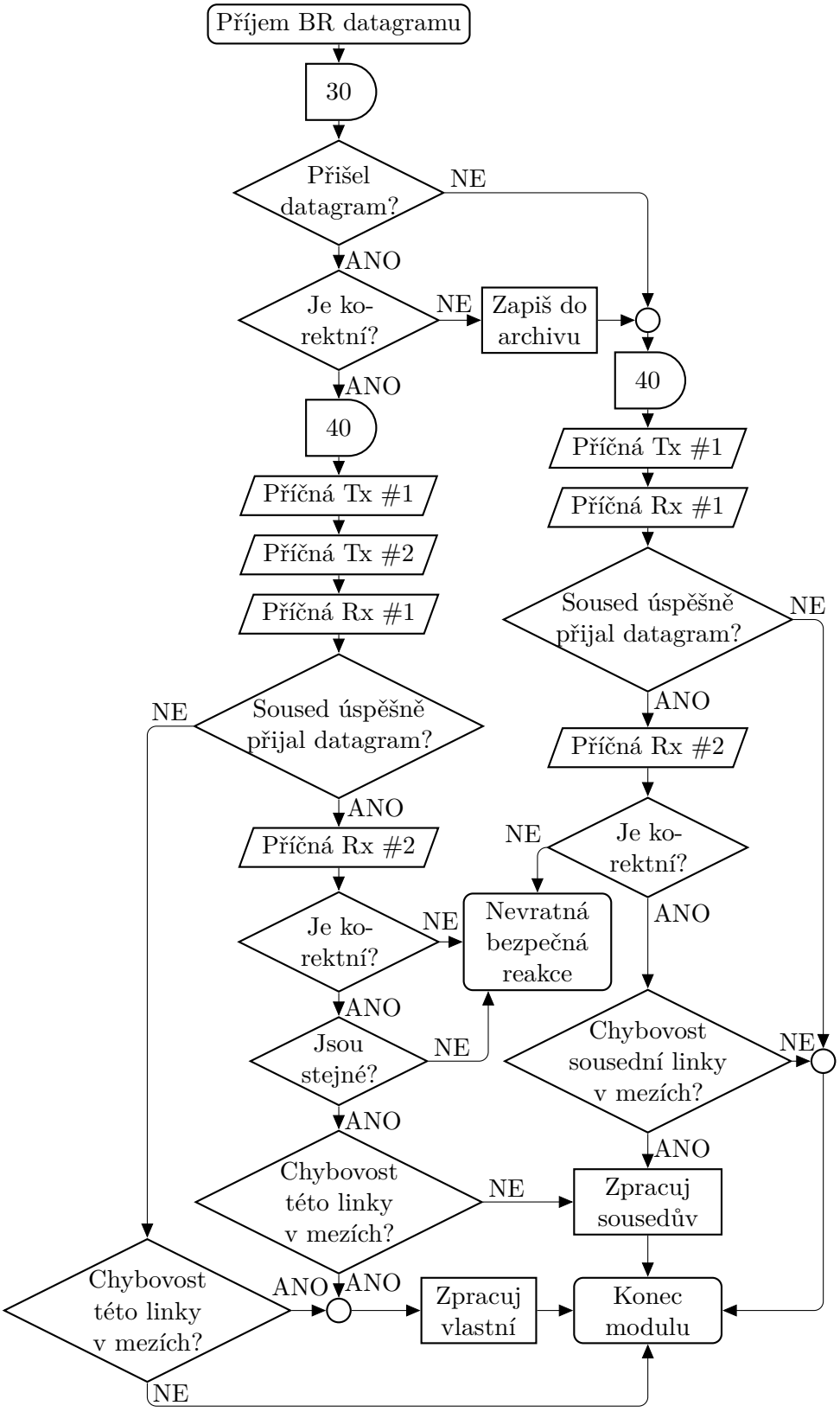
Obrázek 3.2: Vývojový diagram výměny počátečního bytu



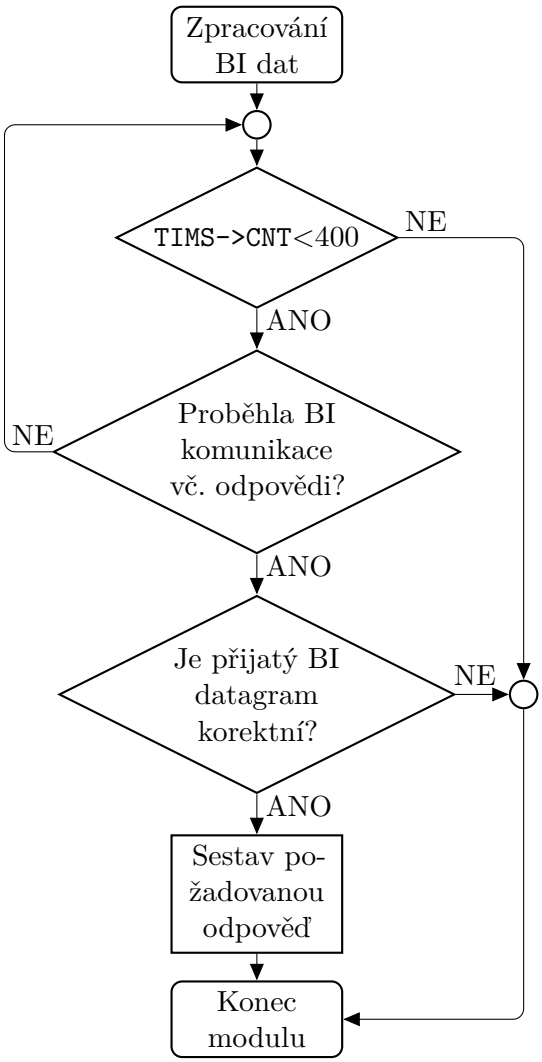
Obrázek 3.3: Vývojový diagram výměny verze software (pSW) a otisku konfigurace (pK)



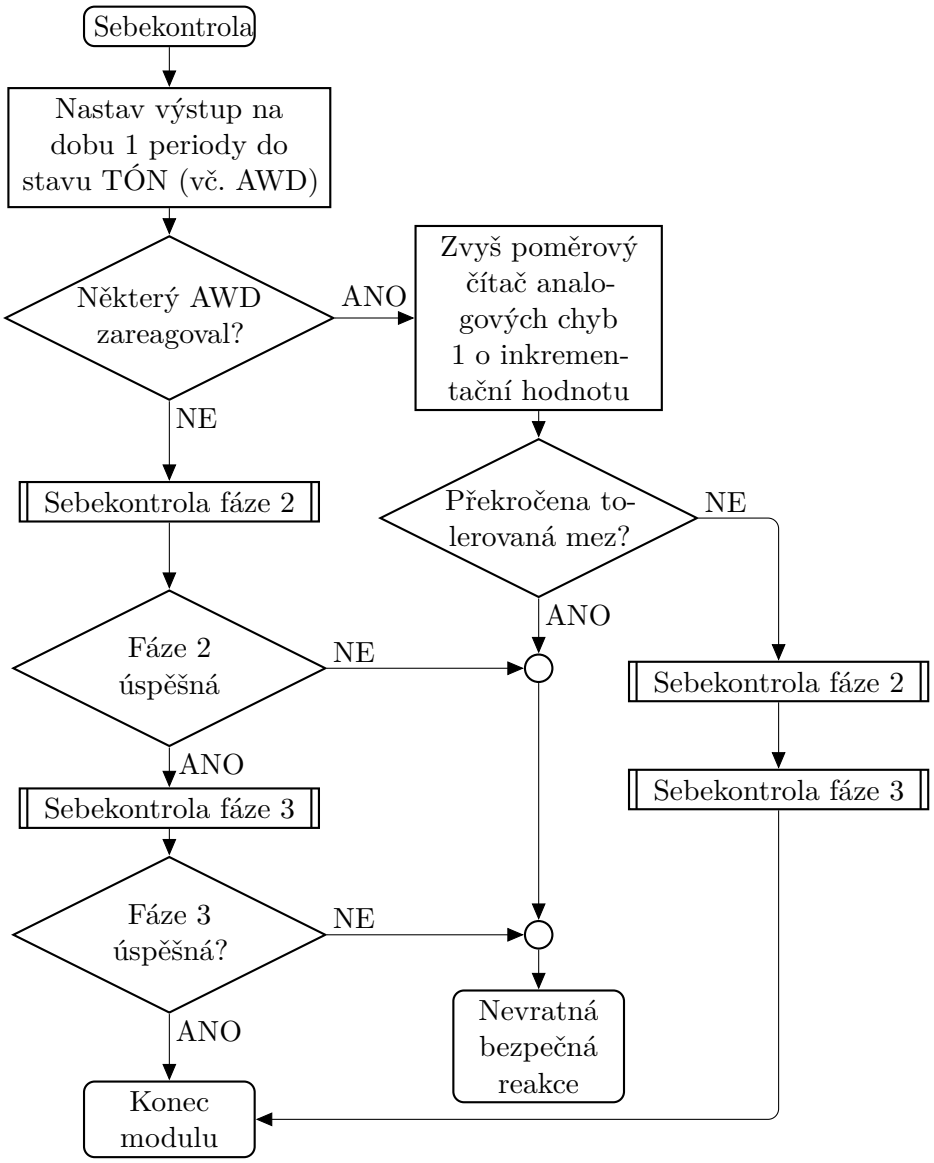
Obrázek 3.4: Vývojový diagram kontroly celé paměti



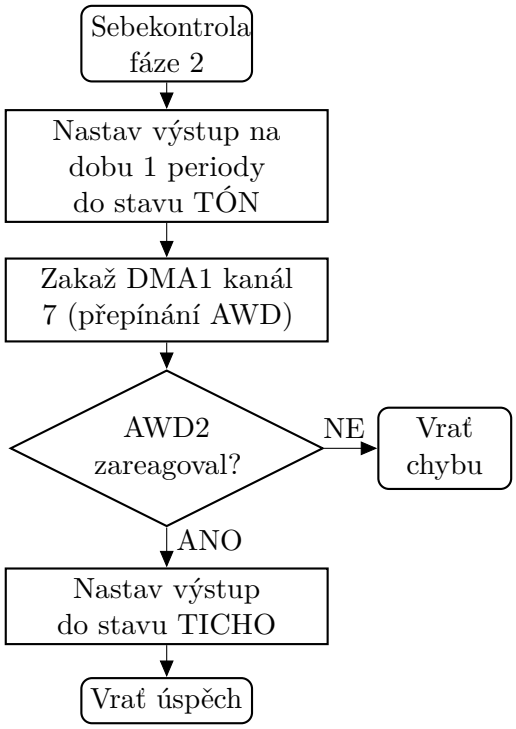
Obrázek 3.5: Vývojový diagram přijetí a kontroly datagramu



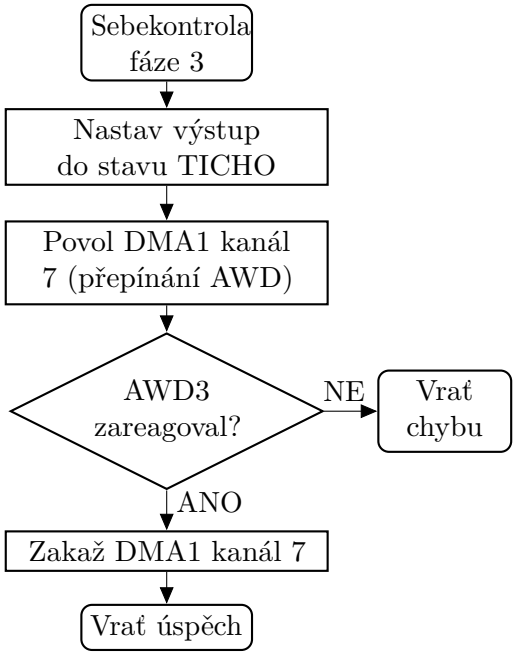
Obrázek 3.6: Vývojový diagram zpracování BI komunikace



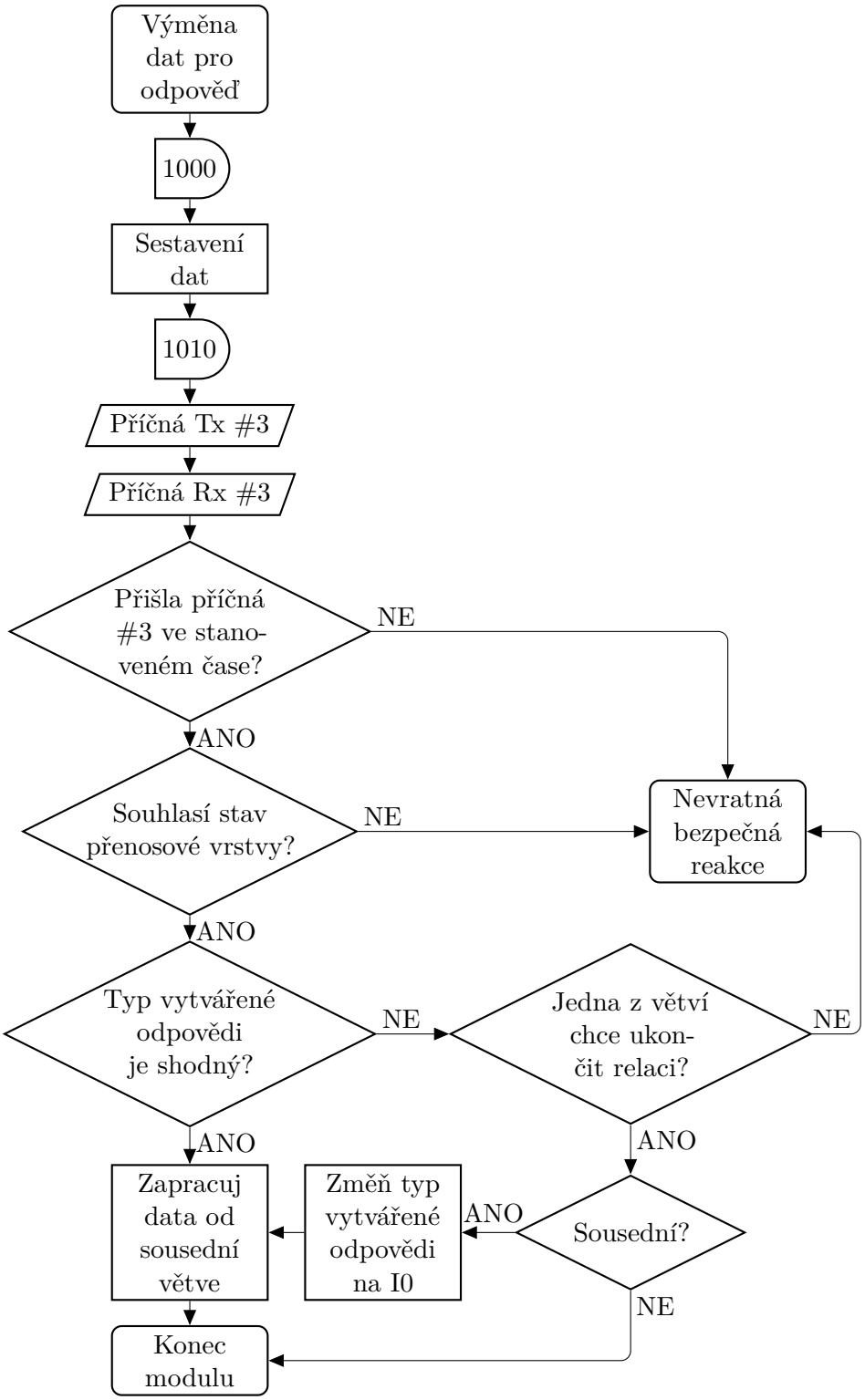
Obrázek 3.7: Vývojový diagram sebekontroly



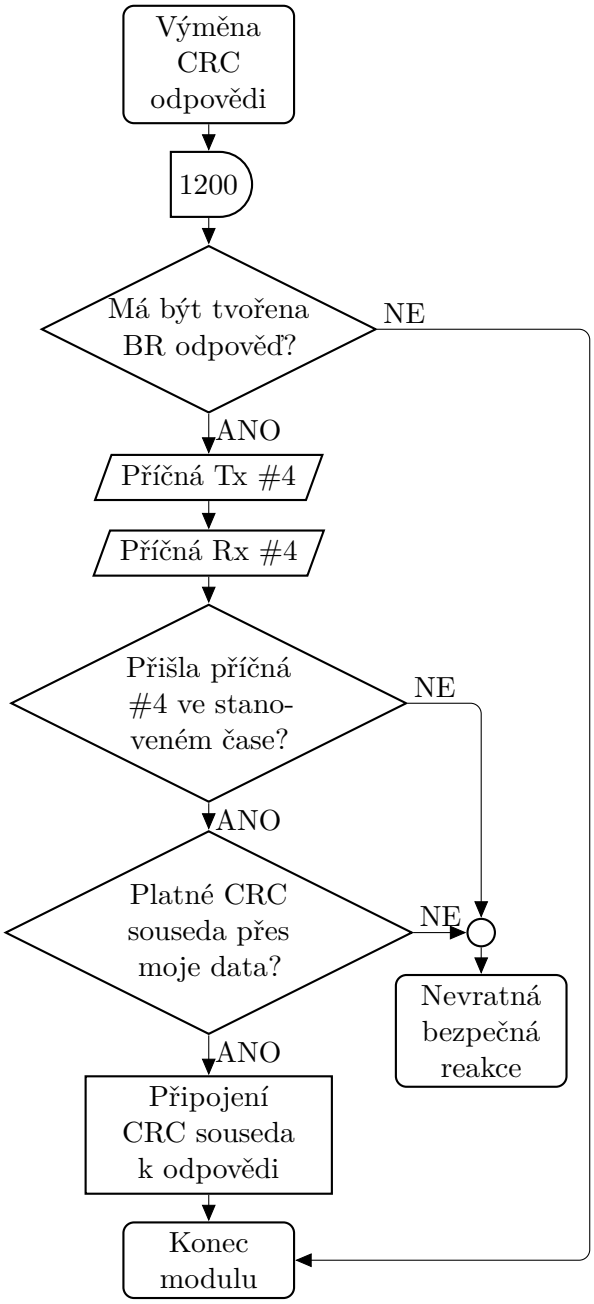
Obrázek 3.8: Vývojový diagram fáze 2 sebekontroly



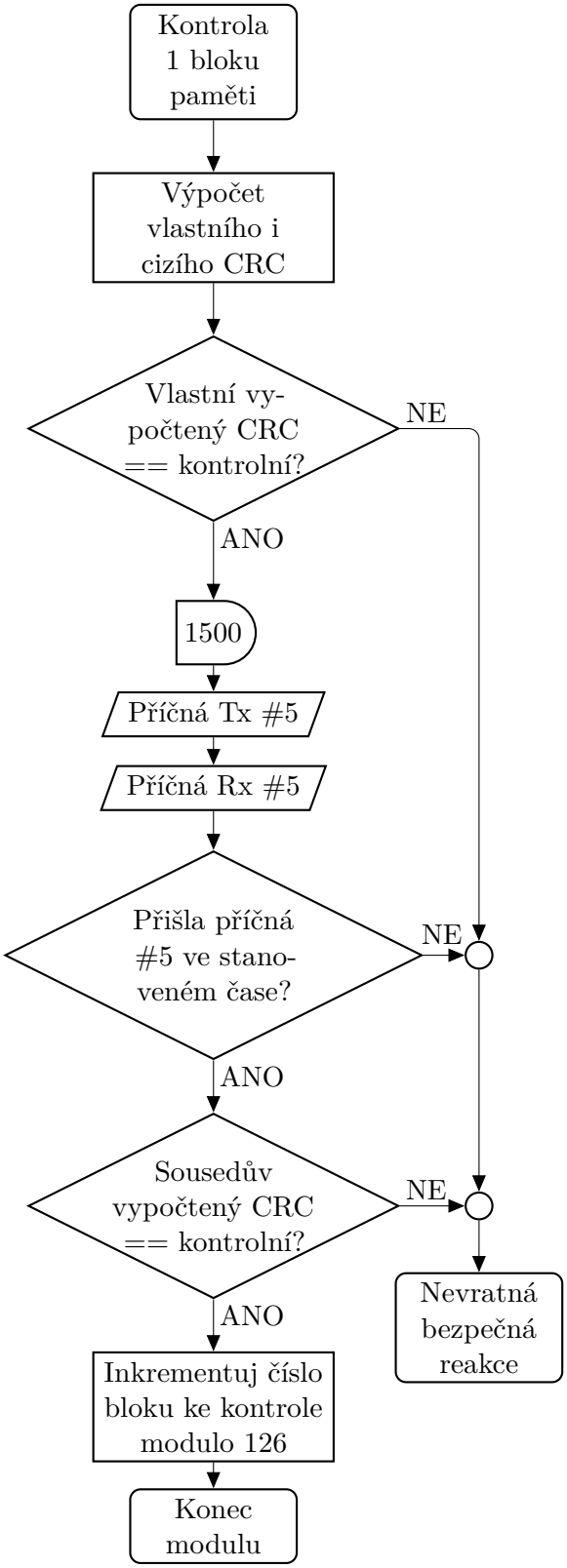
Obrázek 3.9: Vývojový diagram fáze 3 sebekontroly



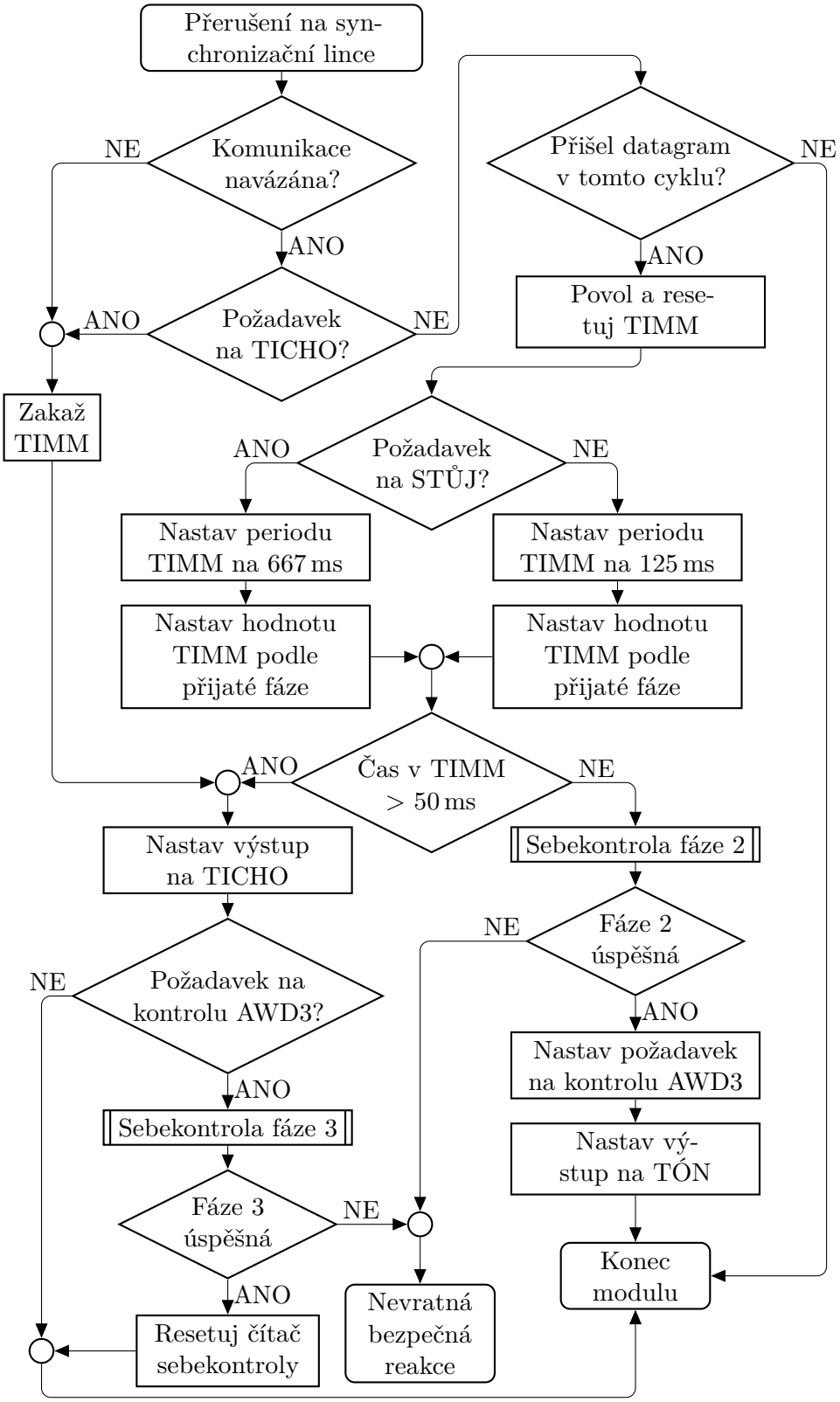
Obrázek 3.10: Vývojový diagram výměny dat pro odpověď



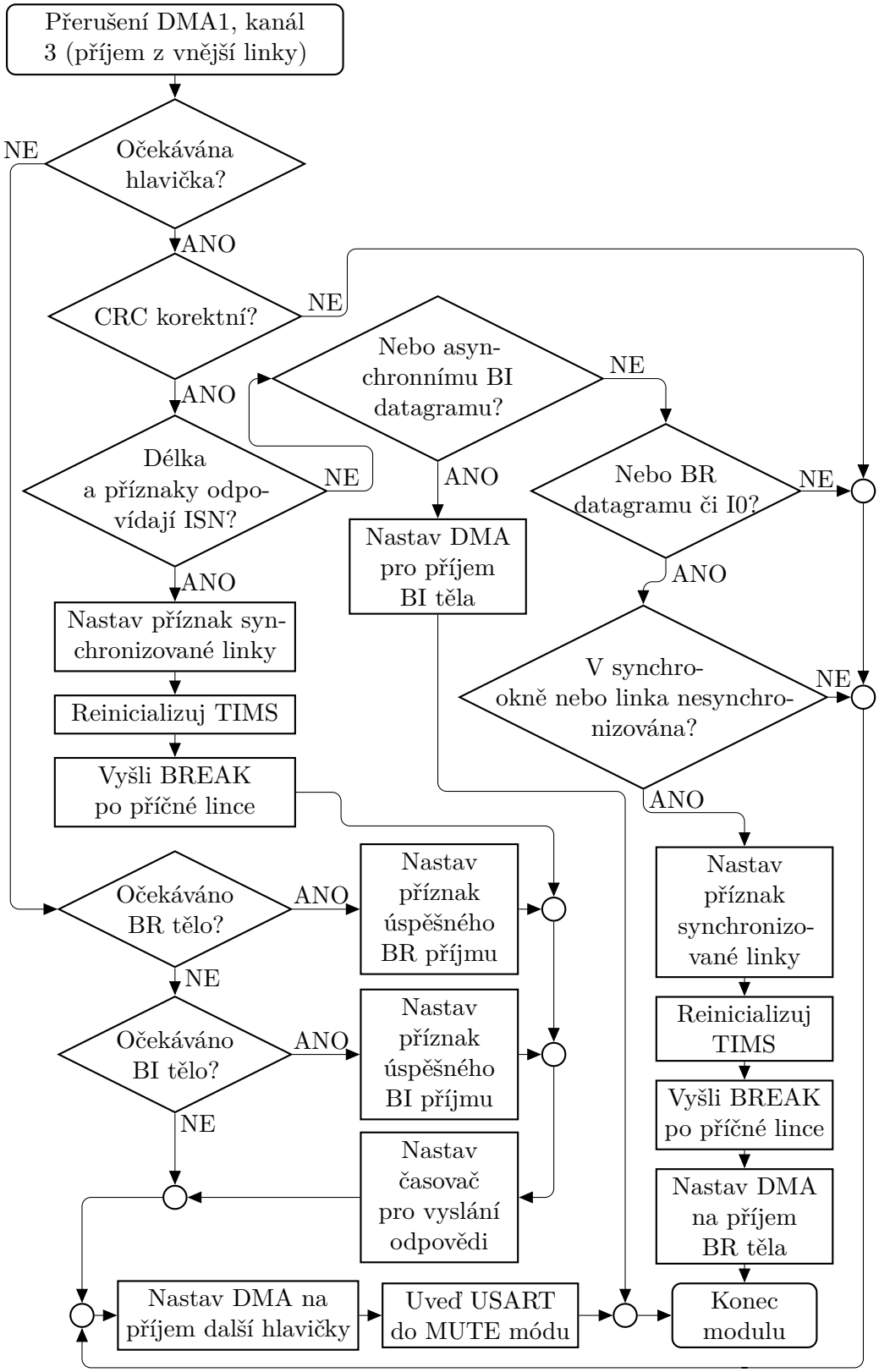
Obrázek 3.11: Vývojový diagram výměny CRC odpovědi



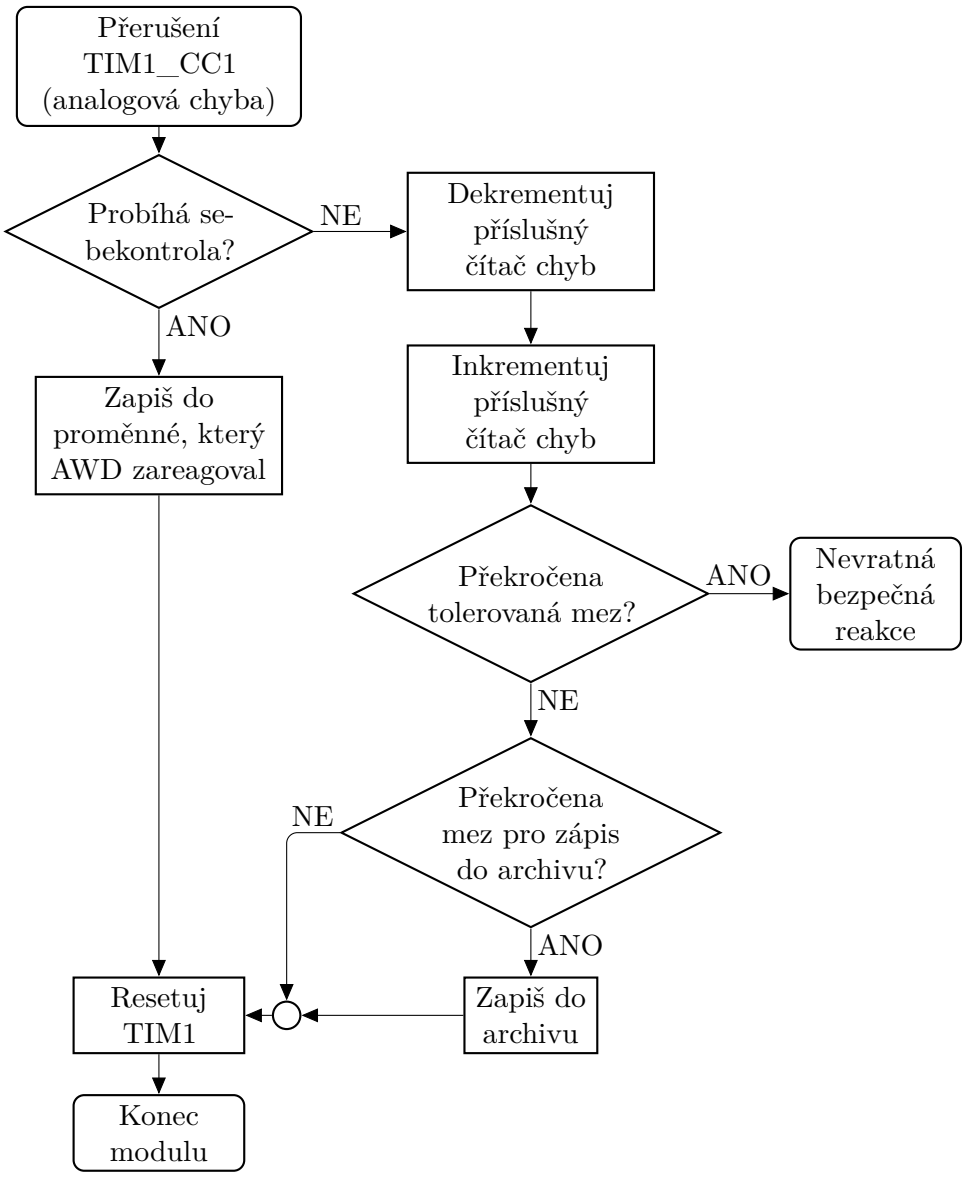
Obrázek 3.12: Vývojový diagram kontroly jednoho bloku paměti



Obrázek 3.13: Vývojový diagram synchronizačního přerušení



Obrázek 3.14: Vývojový diagram přerušení DMA1, kanál 3 (příjem z vnější linky)



Obrázek 3.15: Vývojový diagram přerušení TIM1_CC1 (analogová chyba)

3.4 Implementace komunikačního protokolu

3.4.1 Implementace fyzické vrstvy

Komunikaci s nadřízenou stanicí, označovanou dále jako vnější komunikace, zajišťuje v obou větvích periferie sériového rozhraní USART implementovaná v použitých procesorech, konkrétně USART3 s aktivním výstupem DE (Driver Enable) pro řízení směru na lince (log. 1, pokud podřízená stanice vysílá). Vnější linka musí být od procesoru galvanicky oddělena, proto jsou signály Rx, Tx a DE vedeny k budiči a od budiče linky RS485 přes optočleny. Budiče linek a jemu přislušné strany optočlenů jsou napájeny ze samostatných větví napájení. Signál DE je přiveden na spojené vstupy budiče DE a $\overline{\text{RE}}$, které určují, zda se budič chová jako vysílač či přijímač.

3.4.2 Implementace přenosové vrstvy

Při stavu 1 přenosové vrstvy se USART nachází v MUTE mode, což znamená, že zahazuje všechny přijaté byty, kromě těch s aktivním WAKE-UP bitem a hodnotou odpovídající přednastavené adrese. Je nastaven přímý přístup do paměti očekávající čtyři byty s cílem v poli `header[]`. Fyzická adresa je uložena v externí EEPROM a nahrána do registru `USART3->CR2` při spuštění zařízení. Ve chvíli, kdy USART přijme správnou adresu, vzbudí se a začne přijímat všechny byty s nulovým WAKE-UP bitem. Takto přijme právě čtyři byty odpovídající hlavičce. Pro příchod START bitu každého následujícího bytu platí časový limit 4 délky bitu od posledního STOP bitu nastavený v registru `USART3->RTOR`, což odpovídá času $T1 - \textit{délka bytu} + \textit{délka bitu}$. V případě vypršení tohoto časového limitu, nebo výskytu jiné chyby (Framing error - nepřišel STOP bit, Overrun error - předchozí byte nebyl vyzvednut z registru RDR přijímaných bytů nebo Noise error - trojice vzorků hodnot, které by měly odpovídat jednomu bitu, se neshoduje) je vyvoláno přerušení, které smaže dosud přijaté byty, znovu nastaví DMA na příjem hlavičky a uvede USART do MUTE mode (dále jen odmítnutí datagramu).

Po přijetí čtyř bytů hlavičky dochází nejprve ke kontrole bytu zabezpečení a následně ke kontrole přípustnosti příznaků a délky. Pokud některá z těchto kontrol neprojde nebo dojde k chybě fyzické vrstvy, je datagram odmítnut. Odmítnutí datagramu je zaznamenáno do archivu (viz kapitolu 3.6) s kódem podle tabulky 3.7. Podle přijatého bytu příznaků pak mohou nastat následující situace:

- Byl přijat datagram ISN. Je synchronizována programová smyčka (viz níže), USART uveden do MUTE mode a nastaven časovač TIMR na hodnotu $T3 = 200\,\mu\text{s}$, po jejímž uplynutí je vyvoláno přerušení, které nastaví DMA na vysílání odpovědi připravené v poli `reply[]`.

- Byl přijat asynchronní BI datagram. Nastaví se DMA pro příjem jeho těla do pole `bodyBI[]`.

Kód	Význam
0x1	BR datagram přišel mimo synchrookno
0x2	Délka nebo příznaky obsahují nepovolenou hodnotu
0x3	Nesprávné CRC hlavičky
0x12	USART3 - Framing error (nepřišel stop bit)
0x14	USART3 - Noise error (vzorkované hodnoty nejsou stejné)
0x18	USART3 - Overrun error (data nebyla vyzvednuta)
0x20	USART3 - Timeout error (nepřišel následující byte)
0x30	USART3 - Neznámé přerušení

Tabulka 3.7: Důvody odmítnutí datagramu přenosovou vrstvou

- Byl přijat synchronní BI nebo BR datagram. Je-li relační vrstva ve stavu jiném než WAIT I1, kontroluje se, zda je hodnota `TIMS->CNT` větší než 1600, jinak je datagram odmítnut. Programová smyčka je synchronizována, DMA nastaveno pro příjem těla do pole `body[]`.

Pokud přijatá hlavička nepatřila ISN, jsou přijímány byty těla. V případě výskytu některé z chyb (stejných jako při přijímání hlavičky), je datagram odmítnut. Přijetí všech bytů těla vyvolá přerušení a jsou provedeny stejné operace, jako při předchozím přijetí ISN s výjimkou synchronizace programové smyčky. Byl-li přijat asynchronní datagram, nastaví se jako zdroj DMA pole `replyBI[]`.

Ukončení vysílání odpovědi vyvolá přerušení, ve kterém se do pole `reply[]` zapíše datagram ISP, resp. do pole `replyBI[]` datagram I11 v případě asynchronní BI komunikace.

Synchronizace programové smyčky

Programové smyčky obou větví musí pracovat synchronně. Protože jsou vázány na komunikaci, která nemusí v obou větvích proběhnout přesně ve stejný čas (čas příjmu datagramů se může lišit až o 10 ms), je třeba programové smyčky obou větví synchronizovat pomocí příčné komunikace. Tím je zároveň správně nastaveno synchrookno, které musí být v obou větvích stejné, nastavené podle větve, která přijala synchronizační datagram první.

K synchronizaci je použit USART pro příčnou komunikaci. Ve stavu, kdy není navázána komunikace s nadřízenou stanicí, je nutné očekávat příchod synchronizačního datagramu kdykoliv, třeba i během probíhající příčné komunikace. Proto je k synchronizaci použit symbol BREAK, což je 13 po sobě jdoucích nulových bitů, vyslaný větví, která jako první přijala hlavičku synchronizačního datagramu. Jeho příjem druhou větví vyvolá vždy přerušení, neboť se jedná o frame error. V něm se kontroluje, že nulových bitů bylo právě 13 (a tedy se nejedná o chybu linky nebo výpadek napájení) a pokud ano, nastaví se `TIMS->CNT` na hodnotu 1801. Pokud větev už vyslala v daném cyklu BREAK, příchod BREAKu ze sousední větve je ignorován.

Pokud není navázána komunikace, nelze výše uvedený způsob synchronizace použít. Aby zůstaly smyčky přibližně synchronní i při delším výpadku

komunikace s NS, používá se k synchronizaci příčná komunikace #1. Ta by měla být inicializována při `TIMS->CNT==40`. Pokud ji některá z větví přijme při nižší hodnotě čítače, znamená to, že se oproti té druhé zpožďuje, a hodnota zmíněného časovače je zvýšena na 42.

3.4.3 Implementace relační vrstvy

Obě větve mají implementován kompletní stavový automat, shodnost stavů se kontroluje pomocí příčné komunikace. Po vyhodnocení korektnosti vlastního i sousedního datagramu je volána funkce `sessionLayerStateMachine`, která podle typu úspěšně přijatého datagramu a aktuálního stavu relační vrstvy tento stav aktualizuje. Dále vyhodnocuje podle stavu poměrových čítačů chybovostí linek, zda přijatý datagram smí být zpracován. Datagramy I1 a I3 jsou zpracovávány za účelem správného vytvoření I2 a I4, povely z datagramů I5 jsou předávány aplikační vrstvě. Při navázané relaci jsou I6 vytvářeny neustále bez ohledu na přijetí I5.

Náhodné číslo pro inicializaci pořadového čísla relace je získáváno pomocí časovačů TIMI (TIM17) obou větví. Při startu stanice je TIM17 inicializován jako časovač čítající vzhůru se vstupní frekvencí 72 MHz (větev A) resp. 1,1 kHz (větev B). Při příchodu prvního datagramu I1 je uložena hodnota obou časovačů, která pak tvoří vyšší dva (větev B) resp. nižší dva byty (větev A) tohoto bezpečnostního atributu a TIM17 je překonfigurován na modulační časovač (TIMM).

Má-li podřízená stanice zrušit relaci, odešle datagram I0 s důvodem zrušení relace podle tabulky 3.8.

3.4.4 Implementace aplikační vrstvy

Pro zabezpečení jednoho přechodu budou vždy aktivní právě dvě zařízení ASN, v rámci jedné stanice může být zabezpečeno více přechodů. Modulační křivky výstupních signálů všech zařízení musejí být alespoň přibližně ve fázi, aby se předešlo situaci, kdy souzvuk několika asynchronních signálů STŮJ by mohl být zaměněn za signál VOLNO. Proto nadřízená stanice obsahuje čítač modulo 83 375 (nejnižší společný násobek čísel 667 a 125), čítající každou milisekundu, jehož aktuální hodnotu odešle v každém datagramu I5. Toto číslo modulo 667 resp. 125 určuje fázi výstupního signálu a jeho dvojnásobek je při synchronizačním přerušení přepisován do registru `TIMM->CNT`.

Bezpečné povely, tvořící příslušnou část těla datagramu I5, jsou tvořeny jedním bytem určujícím výstupní signál a třemi byty fáze.

Při zpracování datagramu I5 je opětovně kontrolována jeho integrita a hodnoty jsou přepsány do dvou dvojic globálních proměnných, a to vždy přímo a bitově inverzně. V přerušení po synchronizačním impulsu, kdy se na základě přijatých povelů přepisují registry časovače TIMS, se kontroluje, zda výhradní součet komplementárních proměnných dává hodnotu 0xFF, resp 0xFFFFFF. Nesoulad vede na nevratnou bezpečnou reakci. Tímto postupem se minimalizuje riziko spojené s náhodným přepsáním paměti RAM z důvodu její chyby.

Kód (hex)	Důvod ukončení relace
0x100	Neplatné CRC datagramu I0
0x101	Neplatný typ synchronního BI datagramu
0x111	Nesprávná adresa
0x112	Verze protokolu LEUNET se neshodují
0x11C	Datagram I3 nepřišel po dobu 1 s
0x11D	Neplatné CRC D datagramu I1
0x11E	Neplatné CRC E datagramu I1
0x11F	I1 přijat, když nebyl očekáván
0x120	I3 přijat jinou větví než I1
0x131	Nenulový otisk konfigurace NS
0x13D	Neplatné CRC D datagramu I3
0x13E	Neplatné CRC E datagramu I3
0x13F	I3 přijat, když nebyl očekáván
0x1FF	Každá větev vykázala jinou chybu během autentizace
0x205	I5 nepřišel po dobu 1 s
0x21F	Přetekly poměrové čítače chybovosti linky
0x251	Neplatná časová značka datagramu I5
0x252	Neplatný povelový byte datagramu I5
0x253	I5 nemá očekávanou délku
0x25D	Neplatné CRC D datagramu I5
0x25E	Neplatné CRC E datagramu I5
0x25F	I5 přijat, když nebyl očekáván
0x2FF	Každá větev vykázala jinou chybu během přenosu BR dat

Tabulka 3.8: Důvody zrušení relace

Hodnoty signálového bytu jsou 0x00 pro TICHO, 0x7A pro STŮJ a 0xD7 pro VOLNO.

3.4.5 Bezpečnostně irelevantní komunikace

Protokol LEUNET umožňuje kromě přenosu zabezpečených povelů (BR komunikace) rovněž přenos informací bez vztahu k bezpečnosti, zejména pro diagnostické účely. Formát přenášených BI datagramů vychází z BI komunikace jednotek LEU [15]. Opět platí, že liché datagramy vysílá nadřízená stanice a sudé podřízená. Jejich přenos probíhá ve stanoveném časovém intervalu v rámci komunikačního cyklu (viz obr. 2.2), jelikož ale podřízená stanice neví, v jaké fázi cyklu bude obsluhována, musí očekávat příchod BI datagramu kdykoliv. Z tohoto důvodu je v hlavní programové smyčce vyhrazeno určité okno pro zpracování BI datagramu namísto pevného časového bodu (viz obr. 3.6), čímž je zajištěno řádné zpracování BI dat při jejich příchodu v libovolný okamžik - pokud přijdou mimo toto okno, zpracují se na jeho počátku, pokud během něj, zpracují se ihned po odeslání odpovědi. Z hlediska přenosové vrstvy je zacházeno s BI datagramy stejně jako s těmi BR, pouze nejsou kontrolovány na přijetí v synchrookně. BI datagramy předává

přenosová vrstva v poli odděleném od BR komunikace a stejně tak připravená odpověď je zapisována do zvláštního pole.

Jelikož BI komunikace slouží ke shromažďování diagnostických dat nadřízenou stanicí, probíhá zásadně tak, že NS vyzve PS k vytvoření odpovědi a ta ji v reakci vyšle. Protože ale není možné vytvořit odpověď během krátkého času přepínání směru na lince, je okamžitou odpovědí na výzvu datagram I12 (BI ekvivalent ISP). V příštím cyklu vyšle NS I11 (ekvivalent ISN), na nějž PS odpoví mezitím vytvořenou odpovědí.

Datagramy I13 a I14 slouží k předání okamžité diagnostiky, zároveň I14 obsahuje informaci o počtu nevyzvednutých záznamů v archivu. I17 a I18 slouží ke zjištění konfigurace podřízené stanice.

3.5 Externí EEPROM

K procesoru je přes sběrnici I2C připojena externí 128kB paměť typu EEPROM, která plní tři funkce:

- **Konfigurační** - Při výrobě jsou do ní před finální montáží zapsána data specifická pro konkrétní zařízení, které si zařízení při startu načítá.
- **Bezpečnostní** - Bezpečnostní značka, zapsaná rovněž při výrobě, slouží k tomu, aby se zařízení po závažné chybě nemohlo znovu spustit. Její přítomnost včetně kontrolního součtu je kontrolována při každém startu. Pokud chybí, zařízení se nespustí (skončí v nekonečné prázdné smyčce).
- **Diagnostickou** - Při nevratné bezpečné reakci jsou do paměti zapsány hodnoty vybraných proměnných a registrů, aby bylo možné určit příčinu chyby.

Organizaci paměti shrnuje tabulka 3.9. Paměť v pouzdru SO-8 není z důvodu spolehlivosti řešena jako výměnná, přístup k ní je umožněn vyvedením sběrnice I^2C na programovací konektor.

3.5.1 Bezpečnostní značka

Bezpečnostní značka je předem definovaná jedinečná posloupnost bytů a jejich kontrolního součtu. V této implementaci se jedná o řetězec znaků ASCII "Jsem v pohode a muzu se spustit.", doplněný zprava nulami na délku 50 B. Tento řetězec není při kontrole načítán do operační paměti, ale po přečtení každého bytu je počítán kontrolní součet předcházejících znaků, který je po načtení všech 53 znaků (vč. kontrolního součtu) porovnáván s v programu pevně definovanou konstantou. Není-li zjištěna rovnost, zařízení se nespustí, zároveň ale nezapisuje diagnostická data.

Při nevratné bezpečné reakci se značka maže.

Adresa	Význam dat	Zapisovány při
0x0000	Konfigurace, viz tab. 3.10	výrobě
0x0400	Bezpečnostní značka	výrobě
0x0500	Číslo spuštění	každém startu
0x0800	Stránka diagnostiky, viz tab. 3.11	nevratné reakci
0x0840	Poslední přijatý paket příčné komunikace	nevratné reakci
0x0880	Poslední odeslaný paket příčné komunikace	nevratné reakci
0x08C0	Tělo posledního přijatého datagramu	nevratné reakci
0x0900	Poslední datagram připravený k odeslání	nevratné reakci
0x0940	Číslo spuštění	nevratné reakci

Tabulka 3.9: Struktura dat v paměti EEPROM

Byty	Význam
1	Hodnota 0xFF (rezerva)
2...4	Rezerva
5	Číslo sloupu
6	Pořadí jednotky v rámci sloupu (odshora)
7...14	Adresa podřízené jednotky
15...18	Společná důvěrná informace
19...50	Rezerva
51...53	Kontrolní součet

Tabulka 3.10: Konfigurační stránka zapisovaná při výrobě

3.5.2 Konfigurace

Konfigurační stránka vychází ze struktury využité v jednotkách LEU a je uvedena v tabulce 3.10. Zařízení z ní při spuštění načítá adresu a společnou důvěrnou informaci. Chyba načtení konfigurační stránky nebo neplatný kontrolní součet vedou na nevratnou bezpečnou reakci. Kontrolní součet (otisk) konfigurační stránky si větve vyměňují při spuštění a kontrolují jeho shodnost.

3.5.3 Pořadové číslo spuštění

Čtyřbytové číslo spuštění je při výrobě inicializováno na nulovou hodnotu. Při spuštění jej procesor přečte, inkrementuje a zapíše na původní místo v paměti. Tento údaj slouží k diagnostice, zapisuje se ale při každém startu. Zápisem čísla spuštění se zároveň ověřuje, že funguje zápis do paměti, což je zásadní pro případné mazání bezpečnostní značky.

3.5.4 Diagnostika

Aby bylo možné, v případě že stanice provede nevratnou bezpečnou reakci, určit její příčinu, provede procesor předtím, než přejde do nekonečné smyčky, zápis diagnostických informací do externí EEPROM. Ty sestávají jednak

Byty	Proměnná	Význam
1...2	`reason`	Důvod nevratné reakce, viz tab. 3.12
3...5	`SysTick->VAL`	Hodnota čítače SysTick
6...9	`seconds`	Počet sekund od startu
10...13	`programCycle`	Počet programových cyklů od startu
14	`sessionLayerStatus`	Stav přenosové vrstvy, viz tab. 3.14
15...16	`TIMS->CNT`	Hodnota časovače TIMS
17...18	`TIMC->CNT`	Hodnota časovače TIMC
19...20	`TIMM->CNT`	Hodnota časovače TIMM
21...22	`ADC1->DR`	Analogová hodnota kontrolního vstupu
23	`TIM1->OR`	Aktivní analogový watchdog
24...25	`errCnt[0]`	Hodnota čítače chyb pro ticho
26...27	`errCnt[1]`	Hodnota čítače chyb pro sebetestování
28...29	`errCnt[2]`	Hodnota čítače chyb pro tón - logická 0
30...31	`errCnt[3]`	Hodnota čítače chyb pro tón - logická 1
32...33	`DMA1->ISR`	Stav přímého přístupu do paměti
34	`currentTransverseTx`	Číslo příští vysílané příčné komunikace
35	`currentTransverseRx`	Číslo příští přijímané příčné komunikace
36...41	`timMrk`	Časová značka
42...45	`relNum`	Pořadové číslo relace
46	`outputState`	Stav výstupu (TICHO/STŮJ/VOLNO)
47	`outputTone`	Hodnota modulační obálky
48	`TIMC->CR1`	LSB stavu časovače TIMC
49...52	`startNumBytes`	Číslo spuštění

Tabulka 3.11: Stránka diagnostiky

z diagnostické stránky, shrnující významné skalární proměnné, (viz tab. 3.11), a jednak z dalších stránek vyhrazených významným polím, viz tab. 3.9. Klíčové jsou zejména první dva byty diagnostické stránky udávající důvod bezpečné reakce (tab. 3.12). Vyšší byte určuje operaci, při níž došlo k chybě, nižší pak dodává bližší specifikaci.

MSB	Specifikace důvodu	Význam LSB
5	Chyba čtení bezpečnostní značky	viz chyby EEPROM (tab. 3.13)
6	Chyba čtení či zápisu čísla spuštění	viz chyby EEPROM (tab. 3.13), nejvyšší bit 1 pro chyby zápisu; FF při neúspěšné verifikaci
7	Chyba načtení konfigurace	viz chyby EEPROM nebo E0 - neplatné CRC konfigurace
8	Chyby prvotní příčné komunikace	1 - Nesprávný startovací byte 11 - Nepřišla verze SW 12 - Nesouhlasí verze SW 21 - Nepřišel otisk konfigurace 22 - Nesouhlasí otisk konfigurace
9	Chyby prvotní kontroly paměti FLASH	0...3F - Vadný blok vlastní paměti 40 - Nepřišlo CRC sousední paměti 80...BF - Vadný blok souseda
10	Nepřišla komunikace #1	-
11	Nekorektní datagram I0, I1 nebo I3 sousední stanice	viz nižší byte důvodu ukončení relace (tab. 3.8)
12	Nekorektní datagram I5 sousední stanice	viz nižší byte důvodu ukončení relace (tab. 3.8)
14	Nestejná těla datagramů přijatých jednotlivými větvemi	Pořadí nejnižšího nestejného bytu
15	Neplatná délka skrytých dat zahrnutých v kontrolním součtu	Číslo datagramu, při jehož kontrole došlo k chybě
20	Analogový watchdog nezareagoval při sebekontrole	12 - AWD2 při celkové sebekontrole 13 - AWD3 při celkové sebekontrole 22 - AWD2 při kontrole pouze sebe 33 - AWD3 při kontrole pouze sebe
21	Synchronizační impuls nepřišel ve stanoveném časovém okně	-
22	Neplatný typ vytvářeného paketu	-
30	Nepřišla komunikace #3	-
35	Nestejný MSB důvodu ukončení relace (1 v této větvi)	LSB důvodu ukončení relace této větve
36	Nestejný MSB důvodu ukončení relace (2 v této větvi)	LSB důvodu ukončení relace této větve
38	Vytvářené odpovědi se liší	Odpověď vytvářená touto větví
39	Nestejné stavy relační vrstvy	Stav sousední větve
40	Nepřišla komunikace #4	-
41	Neplatné CRC těla odpovědi sousední větve	-
50	Chyby průběžné kontroly paměti FLASH	0...3F - Vadný blok vlastní paměti 40 - Nepřišlo CRC sousední paměti 80...BF - Vadný blok souseda
A0	Přetekl čítač analog. chyb	Přeteklý čítač

MSB	Specifikace důvodu	Význam LSB
A1	Výstup by měl vydávat tón, bez navázání první relace	-
A5	Neznámé přerušení TIMM	-
B0	Neplatné CRC příčné kom.	Číslo příčné komunikace
B8	Chyba příčného USARTu (BREAK nedetekován)	Nejnižších 8 bitů registru USART1->ISR
B9	Chyba příčného USARTu (BREAK detekován)	Nejnižších 8 bitů registru USART1->ISR
C0	Vytváření odpovědi nebylo dokončeno	1 - nedokončena vlastní část 2 - chybí připojit CRC souseda
D0	Došlo k přepsání klíčové hodnoty v RAM	1 - `outputState` + `outputStateComplent` $\neq$ 0xFF 2 - Úspěšně zkontrolovaný datagram I5 neprošel opakovaným testem

Tabulka 3.12: Důvody nevratné bezpečné reakce (všechna čísla uváděna v hexadecimální soustavě)

Hodnota vyššího nibblu	Význam
0	Součet adresy a délky mimo povolený rozsah
1	Adresa a délka pro zápis přesahují rozsah stránky
2	Chyba odesílání Device select bytu (typicky chybí napájení)
3	Překročen maximální počet pokusů o přístup (vrací NACK)
4	Chyba odesílání MSB adresy
5	Chyba odesílání LSB adresy
6	Chyba čtení/zápisu datových bytů

(a) : Význam vyššího nibblu bytu chyb EEPROM

Index bitu	Zkratka	Význam
0	NACK	Paměť nepotvrdila příjem
1	BERR	Špatně umístěná START či STOP podmínka
2	ARLO	SDA v nule, přestože byla vyslána 1
3	TIMEOUT	Paměť příliš prodloužila hodinový impuls

(b) : Význam jednotlivých bitů nižšího nibblu bytu chyb EEPROM

Tabulka 3.13: Chybové kódy paměti EEPROM

Hodnota	Označení	Význam ve větvi A	Význam ve větvi B
0x10	WAIT_I1	Wait I1	Wait I1
0x31	WAIT_I3OF	Wait I3_a_b	Wait I3_a_b
0x32	WAIT_I3O	Wait I3_a	Wait I3_b
0x33	WAIT_I3F	Wait I3_b	Wait I3_a
0x51	WAIT_I5OF	Wait I5_a_b	Wait I5_a_b
0x52	WAIT_I5O	Wait I5_a	Wait I5_b
0x53	WAIT_I5F	Wait I5_b	Wait I5_a

Tabulka 3.14: Stavy relační vrstvy

3.6 Archiv

Některé události je vhodné zaznamenávat pro pozdější diagnostiku. O dlouhodobou archivaci se stará NS; než však dojde k přenosu na NS, jsou data uchovávána v archivu PS, jehož velikost je omezena na 10 záznamů. Archiv tvoří dvourozměrné pole o deseti řádcích (záznamech) a 52 sloupcích pro jednotlivé položky diagnostické stránky. Záznam v archivu má stejný formát jako diagnostická stránka ukládaná při nevratném ukončení činnosti do EEPROM (tab. 3.11), pouze kódy důvodu záznamu (první dva byty) jsou odlišné, viz tab. 3.15.

MSB	LSB	Význam
0	viz tab. 3.7	Odmítnutí datagramu přenosovou vrstvou
1	viz. tab 3.8	Zrušení relace nebo odmítnutí datagramu
2		
3	0x3x	Navázání relace, nižší nibble kóduje stavy relační vrstvy: horní dva bity jsou nejnižší dva bity kódu stavu WAIT_I3x, z nějž se přechází, nižší dva bity jsou nejnižší dva bity kódu stavu WAIT_I5x, do něhož se přechází podle tabulky 3.14.
	0x5x	Přechod mezi stavy WAIT_I5x, nižší nibble obdobně jako u navázání relace.
	0xAx	Poměrový čítač analogových chyb přesáhl 3/4 tolerované meze, nižší nibble určuje čítač. V případě neúspěšné sebekontroly (čítač 1) se zapisuje vždy.

Tabulka 3.15: Důvody záznamu do archivu

Archiv je koncipován jako kruhový zásobník, nová událost je vždy zapisována na řádek následující po posledním záznamu, po zápisu na poslední řádek se opět pokračuje od prvního. Zároveň je vedena informace o tom, které záznamy již byly odeslány na NS pomocí ukazatele čtení. Ten ukazuje na nejstarší nepřečtený záznam a inkrementuje se (modulo 10) při přepsání nejstaršího záznamu novým a po odeslání každého I16, dokud jsou v archivu nepřečtené události. Není-li v archivu žádná nepřečtená zpráva, jsou byty ADg vyplněny hodnotami 0xFF.

3.7 Kontroly pamětí

3.7.1 Kontrola RAM

Kontrola operační paměti procesoru probíhá na samotném začátku běhu programu, ještě před načtením globálních proměnných z paměti FLASH a tedy i před voláním funkce `main`. Z možných kontrolních postupů byla vybrána procedura PMOVI, která dokáže při náročnosti $O(n)$ detekovat nejvíce druhů chyb [22]. Při zavedení následující notace:

- r - čtení, tj. kontrola, že se v příslušné buňce nalézá příslušná hodnota
- w - zápis hodnoty do buňky
- $\Uparrow$ - provést operaci pro všechny adresy vzestupně
- $\Downarrow$ - provést operaci pro všechny adresy sestupně,

je postup tohoto testu charakterizován posloupností

$$\{\Downarrow(w0); \Uparrow(r0,w1,r1); \Uparrow(r1,w0,r0); \Downarrow(r0,w1,r1); \Downarrow(r1,w0,r0); \Downarrow(w0)\}.$$

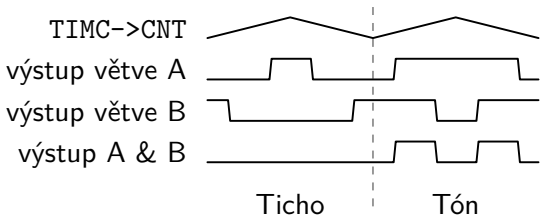
Kromě počátečního a koncového nulování jsou všechny operace prováděny po bitech. V případě zjištění chyby skončí program v nekonečné smyčce. Při úspěšném ukončení testu není možný návrat zpět příkazem `return`, jelikož kontrola přepsala návratový zásobník. Je tedy potřeba se vrátit zpět příkazem `jump` a po návratu zásobník opětovně inicializovat.

3.7.2 Kontrola FLASH

Paměť FLASH je pro účely kontroly rozdělena do 126 kontrolovaných bloků o velikosti 2 kB. Ještě před nahráním programu do procesoru jsou jednoduchým programem `flashCRCCalc` (zdrojový kód přiložen na CD) vypočítány kontrolní součty jednotlivých bloků programové paměti vlastní i sousední větve, které jsou následně uloženy do posledních 4 kB programové paměti obou větví. Tyto dvoubytové kontrolní součty jsou generovány pomocí polynomů druhého stupně, viz tab. 2.2b. Mezisoučet není před výpočtem dalšího bloku inicializován, výsledný kontrolní součet n-tého bloku je tedy počítán ze všech bloků $1 \ldots n$. Tím je zajištěno, že bloky se stejnými daty (typicky prázdné bloky na konci) nemají stejné kontrolní byty.

Při kontrole každá větev spočítá jednak zbytky po dělení řetězce kontrolovaného bloku (se započtením předchozího výsledku) a dvou bytů zabezpečení uložených ve vlastní paměti vlastními kontrolními polynomy, který porovnává s nulovou hodnotou a jednak zbytky po dělení bloku cizími kontrolními polynomy, které předá příčnou komunikací #5 sousední větvi. Ta k nim přidá kontrolní byty uložené ve své paměti a výsledek pak kontroluje vlastními kontrolními polynomy.

Paměť FLASH je kontrolována celá při startu zařízení, za běhu je kontrolován vždy jeden blok v každém komunikačním cyklu. Postupy kontroly paměti znázorňují obrázky 3.12 a 3.4.



Obrázek 3.16: Časování výstupních signálů

	Ticho	Tón
Větev A	27 000	9 000
Větev B	9 000	27 000

Tabulka 3.16: Hodnoty CC registrů časovače TIMC

3.8 Generování a kontrola výstupního signálu

Dle zadání má být EAM buzen signálem o frekvenci 1 kHz, na jehož syntéze se podílejí obě větve. Při poruše jedné větve musí ta druhá být schopna vždy nastavit výstup do bezpečného stavu, tedy jej umlčet a informovat o této poruše nadřízenou stanici. Z toho vyplývá navržené řešení, kdy výstupní signály obou větví jsou sloučeny logickým členem AND tvořeným tranzistory optočlenů oddělujících výstupní obvody od obou větví. Aby bylo možné okamžitě detekovat poruchu (zkrat) jednoho z optočlenů, generuje každá z větví jiný výstupní signál podle obrázku 3.16. Logickým součinem signálů obou větví vznikne buď tón o správné frekvenci nebo nulový signál.

3.8.1 Časovač generující výstupní křivky - TIMC

Ke generování požadovaných výstupních křivek je použit časovač TIMC (TIM2). Časovač pracuje v center-aligned módu, tedy čítá střídavě vzestupně až do hodnoty nastavené v registru `TIMC->ARR` a sestupně k nule. Hodnoty předděličky (`TIMC->PSC`) a auto-reload registeru (`TIMC->ARR`=36 000) jsou voleny tak, aby perioda časovače byla 2 ms.

Výstupní signál je získáván pomocí capture/compare (CC) kanálů. Ty jsou nastaveny v PWM 2 (větev A, CC4), resp. PWM 1 (větev B, CC2) módu, tedy jsou aktivní, pokud hodnota časovače je vyšší, resp. nižší než hodnota v příslušném CC registru. Hodnoty CC registrů se liší při vydávání tónu nebo tichu a mezi větvemi a jsou uvedeny v tabulce 3.16. Výstupy těchto komparátorů jsou pomocí alternativních funkcí přivedeny přímo na brány procesoru.

Synchronizace časovačů TIMC

Časovače generující výstupní signál musejí být synchronizovány přesněji, než jak dovoluje komunikace pomocí příčného USARTu. Proto je od větve A k větvi B veden signál vyhrazený pro tento účel. Ve větvi A je v příslušném

bodě programové smyčky výstup CC1 nastaven jako neaktivní (výstup je invertován, tedy v logické 1) a ve chvíli, kdy časovač dosáhne spodní úvrati (`TIMC->CCR1`=0), objeví se na výstupu sestupná hrana. Ve větvi B je TIMC konfigurován do slave módu, v němž externí spouštěč (ETR) způsobí reset, tedy nastaví TIMC větve B rovněž na hodnotu 0.

Uvedený způsob synchronizace nezávislý na programové smyčce zajišťuje vysokou přesnost a garantuje spojitost výstupního signálu, pokud se fáze obou časovačů liší o méně než 1/8 periody.

3.8.2 Modulační časovač - TIMM

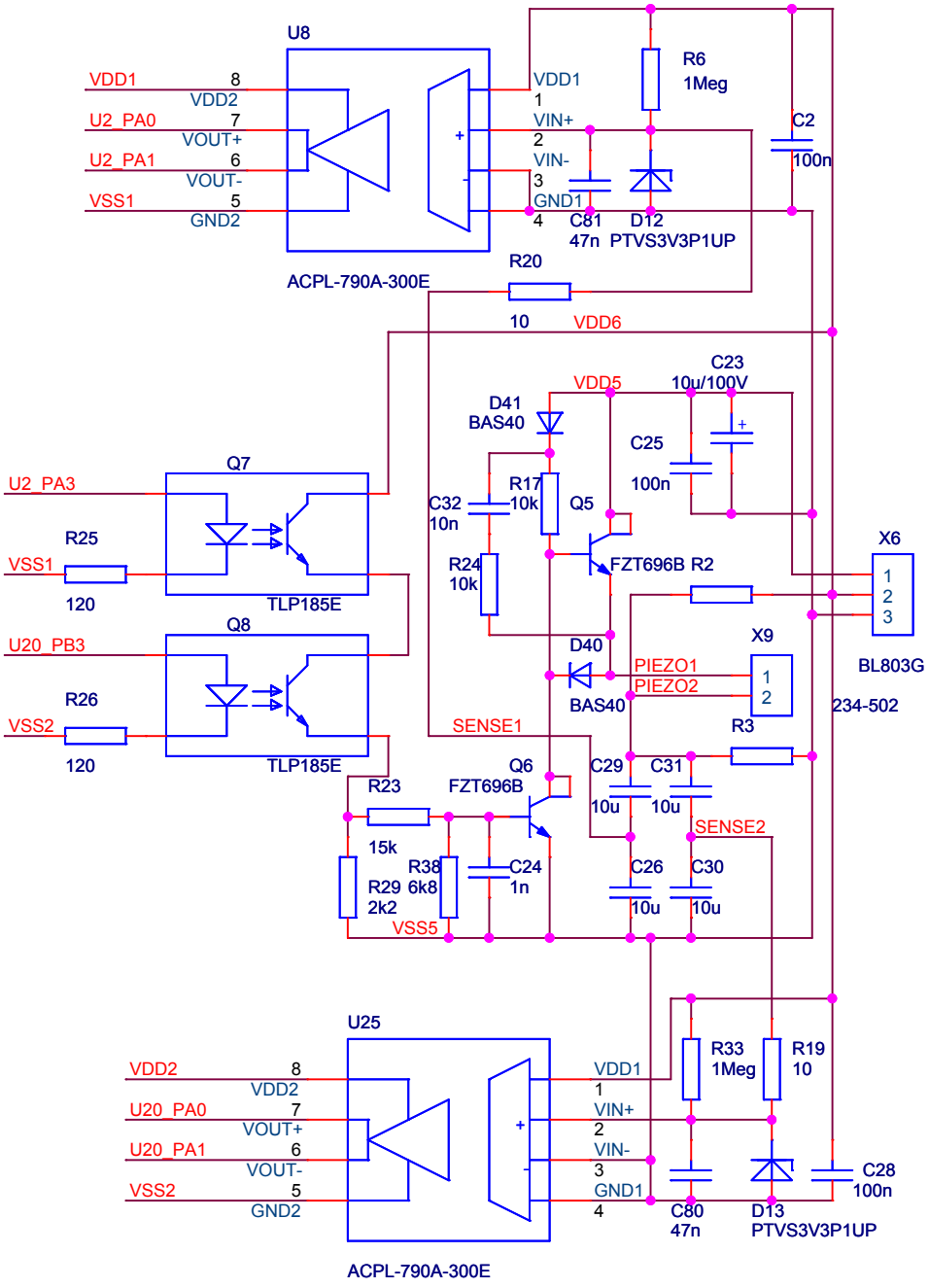
Časovač TIMM zajišťuje střídání tónu a ticha a tím vytváření signálů STŮJ a VOLNO dle zadání (obrázek 1.1). Má-li být výstup ve stavu TICHO, je TIMM zakázán. Časovač TIMM čítá vzestupně; předdělič je nastaven tak, aby frekvence vstupu vlastního časovače byla 2 kHz, auto-reload register tím pádem na hodnotu 1333 pro STŮJ a 499 pro volno, čímž je dosaženo period čítání 667, resp. 125 ms. Přetečení generuje přerušení, které nastaví výstup do stavu TÓN, CC kanál 3 je nastaven tak, aby generoval přerušení při hodnotě `TIMM->CNT`=100, tedy po 50 ms, kdy je výstup opět uveden do stavu TICHO.

Veškeré změny nastavení TIMM a tedy i výstupního signálu se odehrávají v přerušení vyvolaném sestupnou hranou synchronizační linky. V něm je TIMM podle požadovaného výstupu buď zakázán, přičemž TIMC je nastaven do stavu TICHO, nebo je do registru `TIMM->ARR` nastavena hodnota 1333 či 499 a do `TIMM->CNT` dvojnásobek přijaté fáze modulo 667, resp. 125 (viz obr. 3.13).

3.8.3 Budič

Zapojení budiče volně vychází z řešení navrženého pro předchozí verzi zařízení ASN. Výřez ze schématu zobrazující budicí a snímací obvody je na obrázku 3.17. Logický součin signálů z obou větví je zajištěn sériovým spojením fototranzistorů optočlenů Q1 a Q3 ovládaných výstupy jednotlivých procesorů. Při navrženém způsobu buzení spínají tyto fototranzistory střídavě i tehdy, když nemá být vydáván žádný zvuk. Kapacita zavřeného tranzistoru ovšem způsobovala průnik ostrých špiček, které se projevovaly slabým tónem. Tento problém byl vyřešen vřazením RC článku tvořeného R22, R28 a C20 mezi fototranzistory a bázi tranzistoru Q4. Časová konstanta je volena tak, aby špičky byly spolehlivě potlačeny (špičkové napětí na bázi tranzistoru je asi 0,3 V), ale náběžná hrana byla co nejméně zpomalena.

Jsou-li oba fototranzistory zavřené a tedy Q4 není sepnut, je přes rezistor R15 přivedeno napětí na bázi tranzistoru Q2, díky čemuž je tento otevřen a na EAM přivedeno kladné napětí. Ve chvíli, kdy se současně rozsvítí LED obou optočlenů a tranzistor Q4 sepne, přivede se nulové napětí nejen na EAM, ale i na bázi Q2, díky čemuž se tento uzavře. Při opětovném uzavírání Q4 udržuje kondenzátor C22 vyšší napětí na přechodu BE tranzistoru Q2, čímž zvyšuje kolektorový proud a tím urychluje nabíjení piezoměniče.



Obrázek 3.17: Schéma zapojení budiče a snímacích obvodů (výřez ze schématu, upraveno)

3.8.4 Snímání proudu do EAM

Snímání proudu bývá klasicky založeno na vyhodnocování napětí na rezistoru zapojeném sériově se sledovanou zátěží. Piezoreproduktor vykazuje dominantně kapacitní chování (použitý typ KPE-1600NC má dle katalogového listu [23] kapacitu 30 nF ±30%), proto při buzení obdélníkovým napětím do

něj teče proud během krátkých špiček. Takovýto signál by se špatně vyhodnocoval, proto je namísto proudu snímán náboj, kterým je piezoreproduktor nabit, a to vyhodnocováním napětí na sériově zařazeném kondenzátoru. Aby bylo docíleno nezávislosti měření v obou větvích, je místo jednoho kondenzátoru použita čtveřice kondenzátorů C17, C18, C19, C21 zapojená do můstku. Jejich kapacita je volena tak, aby napětí ve snímacích bodech SENSE_A a SENSE_B nepřesáhlo 0,2 V, což je mez, po níž výrobce oddělovacích zesilovačů ACPL-790, do nichž je signál veden, zaručuje linearitu [21]. Transily D10 a D11 chrání obvod před vysokým napětím v případě zkratu EAM. Výstupní diferenciální napětí jsou přiváděna na brány procesorů. Rezistory R5 a R32 mezi vstupem a napájením kompenzují proud tekoucí do vstupu izolačního zesilovače a nastavuje klidové napětí.

Uvedené oddělovací zesilovače byly zvoleny proto, že na sekundární straně mohou být napájeny napětím již od 3 V a snadno se tedy připojují k napájení procesoru. Primární strana vyžaduje pětivoltové napájení, které se získává ze samostatné větve napájecího zdroje.

3.8.5 Vyhodnocování snímaného signálu

Kanál 1 analogově digitálního převodníku (ADC) 1, k jehož vstupům je připojen výstup oddělovacího zesilovače, je konfigurován v diferenciálním módu. Měření na tomto kanálu probíhá kontinuálně, pro vyhodnocení přípustnosti měřené hodnoty jsou použity okénkové komparátory ("analogové watchdogy"-AWD). Jejich výstupy jsou interním signálem připojeny na vstup časovače TIM1, jehož časování hradlují. Použité procesory jsou vybaveny třemi AWD, z nichž dva jsou použity pro snímání dvou úrovní nabití piezoreproduktoru (AWD2 pro nabitý, tj. logickou nulu na vstupu budiče a AWD3 pro vybitý, tj. log 1 na vstupu budiče). Aktivní AWD je určen hodnotou registru `TIM1->OR`. Pokud je na výstupu tón, je tento registr přepisován při každé hraně výstupního signálu pomocí přímého přístupu do paměti (DMA) 1 kanálu 7, který je spouštěn CC kanály 2 a 4 časovače TIMC, kdy jeden z nich je nastaven na hodnotu, při níž dochází k hraně na výstupu této větve, a druhý na hodnotu, při níž by se měla překlápět druhá větev. Je-li na výstupu ticho, je tento kanál DMA zakázán a aktivní je trvale pouze AWD2.

Časovač TIM1 tedy čítá pouze tehdy, je-li snímaná hodnota mimo tolerované pásmo. Tato situace nastává po každé hraně, vzhledem ke konečné strmosti nabíjení piezoreproduktoru a zpoždění izolačních zesilovačů. Časovač je nulován každou periodu výstupu pomocí DMA kanálu 1 spouštěného CC kanálem 3 časovače TIMC nastaveného na hodnotu 18 000. Pokud je během periody snímaná hodnota mimo tolerované pásmo po menší než stanovenou tolerovanou dobu, je vždy včas vynulován a běh programu není narušen. Pokud ale tuto dobu překročí a TIM1 načítá hodnotu uloženou v registru CC 1, je vyvoláno přerušení indikující analogovou chybu výstupu, které způsobí inkrementaci příslušného poměrového čítače chyb (viz obr. 3.15).

#	Popis	Inkrementační hodnota	Tolerovaná mez
0	Na výstupu není tón	20	200
1	Sebekontrola	2	5
2	Na výstupu je tón, chyba v logické 0	40	2000
3	Na výstupu je tón, chyba v logické 1	40	2000

Tabulka 3.17: Poměrové čítače analogových chyb

3.8.6 Poměrové čítače analogových chyb

Jedna analogová chyba, která může být způsobena například elektromagnetickým rušení z okolního prostředí, nemá vést k ukončení činnosti zařízení. Pokud ale úrovně snímaného napětí vybočují z tolerovaných hodnot po určitou dobu trvale, nebo přinejmenším často, značí to pravděpodobnou závadu na zařízení a v takovém případě je třeba provést nevratnou bezpečnou reakci.

Pro odlišení ojedinělých a dlouhodobých chyb jsou použity poměrové čítače chyb (PČCh). Jejich inicializační hodnota je nulová, při každé chybě dochází k inkrementaci o stanovenou hodnotu. Dekrementace by měla probíhat průběžně ve stanovených časových intervalech; aby se nicméně předešlo častému přerušování procesoru, je ve skutečnosti prováděna najednou, vždy při změně výstupu (čítač 0 se dekrementuje při změně z ticha na tón, čítače 2 a 3 při změně opačné) a před inkrementací, a to o rozdíl okamžitého reálného času v milisekundách (určeného z hodnoty čítače SysTick a proměnné `seconds`) a reálného času uloženého do statické proměnné `previousmillis` při poslední dekrementaci kteréhokoliv čítače. Pokud po inkrementaci hodnota PČCh přesáhne tolerovanou úroveň, dojde k nevratné bezpečné reakci.

Celkem jsou použity 4 poměrové čítače chyb, uvedené v tabulce 3.17. Dojde-li k analogové chybě ve chvíli, kdy výstup nemá vydávat tón (ať už je vydáván signál TICHO, nebo v prodlevě mezi tóny u signálů STŮJ a VOLNO), je inkrementován čítač 0, je-li vydáván tón, inkrementuje se čítač 2 nebo 3 podle toho, zda k chybě došlo v logické 0 nebo v logické 1 (ale dekrementovány jsou předtím oba).

V případě detekce analogové chyby během sebekontroly (viz kapitolu 3.8.7) se inkrementuje pouze čítač 1 (nezávisle na logické úrovni), který se dekrementuje při provedení úspěšné sebekontroly. Pokud hodnota čítače 1 není nulová, opakuje se sebekontrola každých 5 s.

3.8.7 Detekovatelné chyby

V souladu s požadavky zadání nesmí jedna chyba způsobit nebezpečné chování. Z tohoto důvodu je třeba každou chybu detekovat a ukončit činnost zařízení dříve, než by druhá chyba mohla způsobit nebezpečí. Je třeba detekovat následující hardwarové chyby:

- chybu budiče, kdy logická úroveň na výstupu neodpovídá logickému součinu vstupních signálů

- zkrat nebo přerušení piezoreproduktoru
- změnu kapacity kondenzátorů ve snímacím můstku

Chybná logická úroveň trvající déle než stanovenou toleranční dobu, je detekována snadno, neboť toleranční pásma hodnot se nepřekrývají. V případě zkratu piezoreproduktoru vzroste významně napětí na snímacím můstku a izolační zesilovač se dostává do saturace, čímž pádem jeho výstupní napětí leží mimo vhodně stanovené toleranční pásmo. Drobná změna kapacity snímacích kondenzátorů nemá vliv na funkci, významná změna ovlivní hodnoty výstupního napětí, které se tak dostane mimo tolerované pásmo.

Přerušení piezoreproduktoru nebo snímacích kondenzátorů bohužel nelze detekovat v klidovém stavu, proto jednou za stanovenou periodu kontroly musí být piezoreproduktor vybit a nabit, aby se zjistilo, zda je schopen udržet náboj odpovídající hodnotám v tolerančním pásmu AWD3. Perioda sebekontroly je určena jako tisícina středního času do poruchy, který byl vypočítán příslušným oddělením zadavatele pro celé zařízení s výsledkem 621 559 hodin. Sebekontrola, která probíhá po spuštění zařízení a následně periodicky vždy po uplynutí stanoveného počtu programových period (11 188 062) od předchozí vždy po synchronizačním impulsu, sestává ze tří fází, kromě výše uvedeného ověření základní funkce je třeba rovněž periodicky kontrolovat, že AWD dokáží generovat přerušení v případě vybočení hodnot z tolerovaného pásma. Bezprostředně po testovací periodě při standardním nastavení AWD (fáze 1) je zakázán kanál 7 DMA 1 a je testováno, zda AWD2 zareaguje na nepřípustné hodnoty během druhé testovací periody (fáze 2), kdy je výstup aktivní. Ve fázi 3 je výstup deaktivován, DMA 1 kanál 7 je naopak po dobu jedné periody povolen, čímž je testována reakce AWD3.

Aby se předešlo vydávání zbytečných zvuků, dochází k testování AWD2 i pokaždé tehdy, kdy po synchronizačním impulsu je na výstupu tón, a to obdobným způsobem, jakým probíhá fáze 2 výše uvedeného kompletního testu. Při nejbližším synchronizačním impulsu, po němž na výstupu není tón, je testován AWD3. Tímto způsobem dojde postupně k provedení stejných testů, jako při výše uvedeném kompletním testu, čímž je možné snížit jejich frekvenci a tím omezit vydávání zbytečných zvuků.

3.9 Optická indikace

Pro účely rychlé diagnostiky v terénu disponuje každá větev zařízení tříbarevnou LED (RGY - červená, zelená, žlutá). Význam jednotlivých signálů je uveden v tabulce 3.18.

Signál	Význam
Tma	Větev nenastartovala nebo se neočekávaně zastavila
Žlutá svítí	Větev čeká na příjem inicializačního bytu souseda
Zelená svítí	Start úspěšný, komunikace nenavázána
Zelená bliká	Komunikace navázána, signál TICHO
Žlutá bliká	Komunikace navázána, signál STŮJ
Zelená a žlutá blikají střídavě	Komunikace navázána, signál VOLNO
Červená bliká	Zablokování větve z důvodu výpadku napájení
Červená svítí	Nevratná bezpečná reakce

Tabulka 3.18: Význam optické signalizace

3.10 Napájecí zdroj

3.10.1 Požadavky

Úkolem napájecího zdroje je z napájecího napětí 48 V∼ ±10 % vytvořit několik galvanicky oddělených výstupů. Konkrétní hodnoty jejich napětí a proudových požadavků shrnuje tabulka 3.19. Maximální proud je roven součtu katalogových hodnot maximálních napájecích proudů použitých obvodů. Tyto hodnoty proudu musí být zdroj schopen dodat.

3.10.2 Koncepce

Z tabulky je patrné, že s odstupem největší výkonové požadavky jsou kladeny na výstupy 1 a 2, tedy napájení mikrokontrolérů a k nim přidružených obvodů. Zároveň lze očekávat, že proudové nároky dvojic výstupů 1-2 a 3-4 budou v čase velmi podobné, nikoliv však přesně stejné. Odběr elektroakustického měniče se koncentruje do krátkých impulzů s frekvencí 1 kHz, které lze pokrýt dostatečným blokovacím kondenzátorem, přitom střední hodnota odběru je relativně nízká. Z výše uvedeného vyplývá následující řešení: Napájecí zdroj je navržen jako spínaný zdroj s transformátorem s několika sekundárními vinutími. Sekundární napětí jsou navržena na hodnoty o zhruba 20 % vyšší oproti požadovaným a následně stabilizována lineárními stabilizátory. Tato rezerva pokrývá situace, kdy nestabilizované napětí poklesne z důvodu nestejnoměrného odběru. Zpětná vazba do budiče je zavedena pouze ze sekundárních obvodů č. 1 a 2 (před lineárním stabilizátorem). Zdroj je navržen tak, aby napětí před stabilizátorem v obvodech 3, 4, 5 a 6 nemohlo poklesnout pod minimální hodnotu vstupního napětí použitých stabilizátorů ani při nejmenším možném odběru na výstupech 1 a 2, který činí asi 30 mA při nečinném procesoru.

Stejnosměrné napětí vstupující do spínaného zdroje je získáno usměrněním a vyhlazením střídavého vstupu.

#	Napětí [V]	Proud [mA]	Sekce	Pozn.
1	3,3	210	Vnitřní A	μP větev A
2	3,3	210	Vnitřní B	μP větev B
3	5	9,5	Vnější A	budiče linky A
4	5	9,5	Vnější B	budiče linky B
5	56	10	Vnitřní C	elektroakustický měnič
6	5	37	Vnitřní C	snímače proudu

Tabulka 3.19: Požadavky na napájecí zdroj

3.10.3 Návrh

Ze vstupní napájecí linky 48 V ±10 % je po usměrnění a vyhlazení získáno stejnosměrné napětí v rozsahu 59 … 73 V. Kapacita nabíjecího kondenzátoru je určena podle vzorce

$$C = \frac{I_{\text{in,max}}}{2 f_{\text{in}} \Delta U}, \tag{3.1}$$

kde $f_{\text{in}} = 50\,\text{Hz}$ je vstupní frekvence, maximální vstupní proud $I_{\text{in,max}}$ bude přibližně

$$I_{\text{in,max}} = \frac{\sum_i I_{\text{out,max},i} U_{\text{out},i}}{\eta U_{\text{in,min}}}, \tag{3.2}$$

kde $i = 1 \ldots 6$ jsou indexy jednotlivých výstupů. Účinnost η bude zhruba rovna katalogové hodnotě 82,5 % vydělené koeficientem 1,2 zohledňujícím napěťovou rezervu 20 % na výstupu, tedy zhruba 68 %, povolené zvlnění napětí ΔU budiž 2 V. Dosazením do výše uvedených vzorců vychází maximální vstupní proud 56 mA a hodnota kondenzátoru 277 µF, je tedy použit kondenzátor 470 µF.

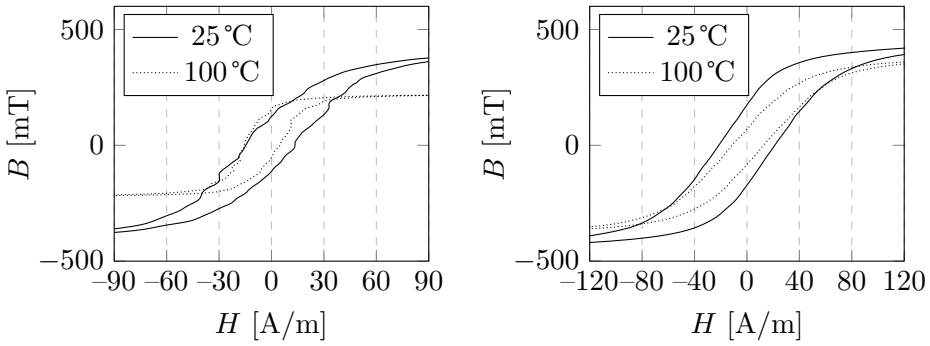
Jako budič byl vybrán obvod LM5030 firmy Texas Instruments [25]. Tento obvod je určen pro řízení spínaných zdrojů s transformátorem typu push-pull se vstupním napětím do 100 V. Obvod je vybaven interním stabilizátorem pro rozběh, nicméně ten není určen pro trvalý provoz, neboť pouzdro nedokáže dlouhodobě efektivně rozptylovat vysoký ztrátový výkon. Obvod je proto po rozběhu napájen ze samostatného vinutí transformátoru.

Transformátor

Z důvodu unifikace v rámci firemního portfolia zadavatele bylo vybíráno mezi toroidními jádry z materiálů N30 a N87 výrobce Epcos o vnějším průměru $d_0 = 16\text{mm}$, vnitřním průměru $d_{\text{i}} = 9{,}6\,\text{mm}$ a výšce $h = 6{,}3\,\text{mm}$. Hysterezní smyčka těchto materiálu pro různé teploty je na obrázku 3.18. Data pocházejí z programu TDK Electronics: Ferrite Magnetic Design Tool [24].

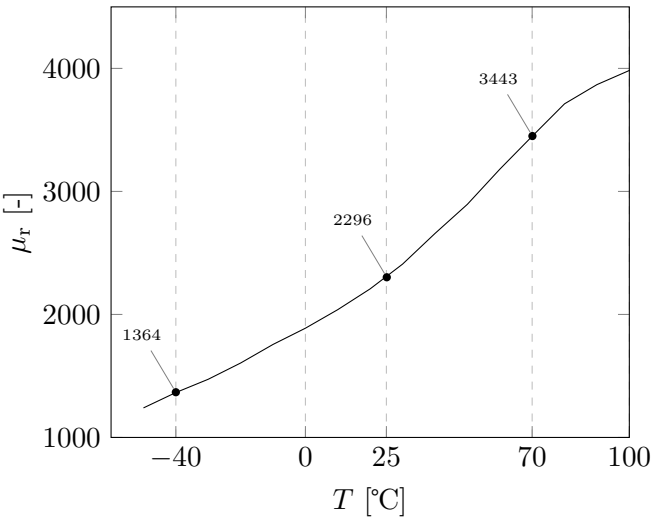
Z grafů bylo určeno maximální sycení $H_{\text{max}}(\text{N30}) = 30\,\text{A/m}$ resp. $H_{\text{max}}(\text{N87}) = 80\,\text{A/m}$. Nejmenší délka siločáry je $l_{\text{min}} = \pi d_{\text{i}} \doteq 30\,\text{mm}$ (u vnitřního okraje jádra bude při daném proudu největší intenzita magnetického pole). Z Ampérova zákona

$$Hl = N_{\text{P}} I \tag{3.3}$$



(a) : N30 **(b) :** N87

Obrázek 3.18: Hysterezní křivky uvažovaných materiálů jader



Obrázek 3.19: Závislost počáteční permeability jádra N87 na teplotě

byl vypočítán maximální počet závitů primární cívky N_P:

$$N_{\mathrm{P,max}} = \frac{H_\mathrm{max} l_\mathrm{min}}{2 I_{\mathrm{in,max}}} \doteq \begin{cases} 12 & \text{pro N30} \\ 31 & \text{pro N87} \end{cases} \tag{3.4}$$

Koeficient 2 ve jmenovateli vychází z toho, že $I_{\mathrm{in,max}}$ je střední hodnota proudu; v každém cyklu ale dochází k přibližně lineárnímu nárůstu proudu od nuly po maximální hodnotu, která je tudíž oproti střední dvojnásobná. Při pouhých 12 závitech by vycházelo velmi málo závitů sekundárních vinutí (pro 4 V sekundárního napětí méně než jeden), proto bude dále uvažováno pouze jádro N87, jehož závislost počáteční permeability na teplotě je na obrázku 3.19.

Maximální indukčnost primární cívky při maximálním počtu závitů lze velmi přibližně určit ze vztahu

$$L_\mathrm{P} = \frac{N_\mathrm{P}\Phi}{I} = \frac{N_\mathrm{P}}{I}\frac{\mu_0\mu_\mathrm{r} S N_\mathrm{P} I}{l_\mathrm{S}} = N_\mathrm{P}^2 \frac{\mu_0\mu_\mathrm{r} S}{l_\mathrm{S}} \doteq 2\,\mathrm{mH}, \tag{3.5}$$

kde Φ je magnetický indukční tok, $S = h(d_\mathrm{o} - d_\mathrm{i})/2$ je průřez jádra a $l_\mathrm{S} = \pi(d_\mathrm{o}+d_\mathrm{i})/2$ je střední délka siločáry, $\mu_0 = 4\pi \cdot 10^{-7}$ je permeabilita vakua, $\mu_\mathrm{r} = 4876$ je maximum počáteční permeability jádra přes uvažovaný rozsah teplot. Tento vztah nelze obecně pro cívky s feritovým jádrem použít a slouží tak pouze ke hrubé orientaci. Maximální čas sepnutí budicího tranzistoru byl určen za vztahu

$$t_\mathrm{ON,max} = \frac{L_\mathrm{P,max} I_\mathrm{in,max}}{U_\mathrm{in,min}} = 2{,}6\,\mu\mathrm{s}. \tag{3.6}$$

Při maximální střídě $D_\mathrm{max,min} = 47{,}5\,\%$ potom vychází vhodná pracovní frekvence

$$f = \frac{D_\mathrm{max,min}}{t_\mathrm{ON,max}} = 180\,\mathrm{kHz}. \tag{3.7}$$

Při této frekvenci je hloubka vniku elektromagnetické vlny do mědi

$$\delta = \sqrt{\frac{\rho}{\pi f \mu_0}} \doteq 0{,}15\,\mathrm{mm}, \tag{3.8}$$

kde $\rho = 15 \cdot 10^9\,\Omega\mathrm{m}$ je rezistivita mědi podle [12]. Na základě tohoto výsledku byl zvolen drát o průměru 0,2 mm. Při zvoleném počtu závitů vychází napětí na jeden závit 1,9 V, z čehož jsou dopočítány počty závitů sekundárů. Výsledné počty závitů po zaokrouhlení nahoru udává tabulka 3.20. Zvolená sekundární napětí vycházejí z požadovaného výstupního napětí, úbytku na stabilizátoru a usměrňovacích diodách a vhodné rezervy. Vinutí č. 1, 2, 3, 4 a 6 jsou koncipována jako dvojitá z důvodu minimalizace ztrát na usměrňovacích diodách, ostatní vinutí jsou jednoduchá kvůli omezenému počtu vývodů zvoleného pouzdra. Pomocné vinutí P slouží k napájení řídicího obvodu.

#	požadované sekundární napětí [V]	počet závitů
1	4,5	2 × 3
2	4,5	2 × 3
3	6	2 × 4
4	6	2 × 4
5	60	35
6	6	2 × 4
P	10	6

Tabulka 3.20: Počty závitů jednotlivých sekundárních vinutí.

Zpětná vazba a stabilizace

Zpětná vazba je zavedena ze sekundárů č. 1 a 2. Obvod TL431 je nastaven odporovým děličem na hlídání hodnoty 3,95 V, při jejímž podkročení se sníží napětí na katodě, LED optočlenu začne procházet větší proud a napětí na fototranzistoru klesne. Váhování vazeb je provedeno sériovým spojením tranzistorů těchto optočlenů připojených ke vstupu COMP řídicího obodu.

Výstupní napětí č. 1…4 a 6 jsou stabilizována low-drop stabilizátory LF33 a LE50 na hodnoty 3,3 V resp. 5 V. Napájení budiče EAM je stabilizováno jednoduchým diskrétním stabilizátorem.

Chlazení

Provoz lineárních stabilizátorů je provázen vznikem tepla. Je třeba ověřit, že i v nejnepříznivějších podmínkách nepřesáhne teplota čipu použitých stabilizátorů dovolené maximum. Uvažme nejprve pětivoltové výstupy. Při maximálním dovoleném napájecím napětí může dosáhnout napětí na sekundáru 9,6 V, po odečtení úbytku na usměrňovači 9 V, na stabilizátoru tedy bude úbytek 4 V. Při nejvyšším uvažovaném proudu 37 mA bude činit výkonová ztráta 148 mW. Stabilizátor LE33 má podle katalogového listu tepelný odpor mezi čipem a okolím 55 °C/W. Při maximální dovolené teplotě čipu 125 °C [26] tedy smí být teplota vzduchu v krabičce maximálně 116,8 °C.

U třívoltových stabilizátorů lze předpokládat, že díky zpětné vazbě nepřesáhne vstupní napětí výrazně hodnotu 4 V. Pokusy ukázaly, že i při silně nesymetrickém odběru nevzroste toto napětí nad 5 V. Při této hodnotě bude úbytek napětí na stabilizátoru 1,7 V, výkonová ztráta při maximálním odběru 357 mW. Teplotní spád mezi čipem a okolím při tepelném odporu pouzdra DPAK 100 °C/W bude 36 °C, tedy při maximální dovolené teplotě čipu 125 °C [27] smí být v krabičce nejvýše 89 °C.

Na sekundáru pro buzení EAM může vzniknout napětí až 85 V, což povede k úbytku napětí na tranzistoru 29 V, tedy výkonovou ztrátu 290 mW. Tepelný odpor při minimálním chladiči je 104 °C/W, rozdíl teplot mezi čipem a okolím bude 30 °C, čili nejvyšší teplota v krabičce nesmí překročit 120 °C, neboť maximální teplota přechodů je 150 °C[28].

Z uvedeného vyplývá, že pokud teplota vzduchu v krabičce nepřekročí 89 °C, budou teplotní limity použitých komponent splněny. Vzhledem k tomu, že tepelný odpor krabičky není znám, bude vnitřní teplota za provozu zjištěna měřením na realizovaném prototypu.

3.11 Elektromagnetická kompatibilita

Požadavky na elektromagnetickou kompatibilitu drážních zařízení stanovuje norma [11]. Z hlediska návrhu přepěťových ochran je zásadní splnění zkoušek pro rázový impuls. Zařízení nemá být uzemněno, důležitá je tedy zkouška mezi vodiči navzájem, pro niž norma stanoví profil 1,2 / 50 µs (délka náběžné/sestupné hrany) se špičkovým napětím ±1 kV. Blíže tuto zkoušku specifikuje norma [13], která určuje výstupní impedanci generátoru 2 Ω, z níž vyplývá špičkový zkratový proud 500 A.

Přepěťová ochrana zařízení je řešena z důvodu časových parametrů použitých součástek vždy jako vícestupňová. Hrubou ochranu napájecí linky tvoří varistor připojený přímo na vstupní svorky. Maximální pracovní napětí zvoleného typu CT2220K60G [29] je 60 V_{rms}, clamping voltage 165 V. Za něj jsou připojeny soufázová tlumivka 47 mH a dvojice jednoduchých tlumivek 15 mH. Zatímco indukčnost soufázové tlumivky může být volena vysoká, neboť v běžném provozu se její účinky vyruší, hodnota obyčejných tlumivek je volena tak, aby jejich induktance nezpůsobovala úbytek napětí větší než 2 %. Soustava tlumivek zároveň odděluje varistor od jemné přepěťové ochrany -

transilu. Ten je volen tak, aby jeho zápalné napětí bylo bezpečně větší než maximální amplitudové napětí 75 V. Optimálně by jeho clamping voltage nemělo překročit 100 V, aby nemohlo dojít ke zničení řídicího obvodu zdroje. Takový transil ale na trhu není, byl tedy vybrán typ SMCJ70A [30], u nějž tato hodnota činí 113 V. Následující můstkový usměrňovač způsobí další zpomalení rázového impulsu, je tedy možné za něj připojit jako další, nejjemnější, stupeň ochrany dodatečnou Zenerovu diodu se Zenerovým napětím 75 V.

Požadavky na odolnost komunikační linky jsou mírně odlišné. Jednak impedance testovacího přístroje je 42 Ω, díky čemuž je při stejném vrcholovém napětí proudový impuls výrazně nižší, jednak vysoce symetrické páry, k nimž patří i vodiče A a B linky, nejsou testovány proti sobě, ale pouze vůči společnému vodiči. Protože kapacita varistoru je pro použití na lince nepřípustně vysoká, jsou místo něj použity bleskojistky, a to typ s co možná nejnižším zápalným napětím (75 V). Oddělovací tlumivka je nahrazena dvojicí rezistorů 10 Ω. Použitý převodník THVD2410 [31] má sice dovolené napětí na vstupech až 70 V, nicméně ochranný transil je volen na napětí výrazně nižší (5 V), aby dokázal vstřebat co největší proudový impuls.

3.12 Výpadky napájecího napětí

Návrh zařízení musí počítat s tím, že může dojít k výpadkům napájecího napětí. Dlouhé výpadky nepředstavují závažnější problém - obě větve se postupně vypnou a při obnovení napájení opět zapnou. Krátkodobé výpadky mohou ale způsobit, že vlivem nestejných hodnot blokovacích kapacit v jednotlivých větvích se jedna z větví restartuje, zatímco druhá zůstane běžet. Taková situace by vedla k nesouladu v chování procesorů a neočekávaná data v příčné komunikaci by způsobila nevratné ukončení činnosti zařízení. Aby k popsanému jevu nedocházelo, hlídají obě větve přítomnost střídavého napájecího napětí. Při jeho výpadku přejdou po určité době, během které dokáží ještě napájecí napětí bezpečně dodávat nabíjecí a filtrační kapacity, do nekonečné smyčky. Dojde-li tedy k výše popsané situaci, větev, která zůstala běžet, skončí v nekonečné smyčce, ve které nevysílá nic sousední větvi, větev, která se restartovala, se nespustí, neboť od sousední větve nedostane počáteční byte. Z tohoto stavu se může zařízení dostat pouze déletrvajícím vypnutím napájení, při němž dojde k restartu obou větví.

Po hardwarové stránce je hlídání řešeno pomocí dvou optočlenů, jejichž LED jsou sériově připojeny přes usměrňovací diodu, Zenerovu diodu, která zajistí vypnutí i při nedovoleném poklesu napětí, a rezistor na střídavé napájecí napětí. Výstupy optočlenů jsou připojeny na vývody PA8 procesorů, nastavené v alternativní funkci jako TIM4_ETR.

Čítač TIM4, označený jako TIMV, je nastaven jako vzestupně běžící čítač, který je resetován sestupnou hranou na externím vývodu. Při přítomnosti napájecího napětí je tedy každých 20 ms resetován. Dojde-li k déle trvajícím výpadku, časovač dosáhne hodnoty uložené v CC registru 1. To vyvolá přerušení, které uvede procesor do nekonečné smyčky; předtím ale nastaví linku příčného USARTu do logické nuly. Framing error příčné komunikace tedy

nevede na nevratné ukončení činnosti, ale způsobí umělé vyvolání přerušení při výpadku napájení. Tím je zajištěno, že v případě, kdy je napájecí napětí hraničně nízké a mohlo by se tedy stát, že jeden z optočlenů ještě sepne, ale druhý už ne, dojde vždy k ukončení činnosti obou větví.

Kapitola 4

Analýza rizika

Norma [6] požaduje provedení analýzy rizika, kterou blíže specifikuje norma [7]. Ta se sestává z následujících kroků:

1. Identifikace nebezpečí spojených se systémem.
2. Identifikace posloupností událostí vedoucích k nebezpečí.
3. Ohodnocení rizik plynoucích pro systém z jednotlivých nebezpečí.
4. Stanovení a klasifikování přijatelnosti rizik plynoucích pro systém z jednotlivých nebezpečí
5. Vypracování záznamů o nebezpečí pro průběžný management rizika

Tato práce si neklade za cíl provedení kompletní analýzy rizika, některé její postupy zde ovšem budou naznačeny.

4.1 Nebezpečí spojená se systémem

Za nebezpečné stavy řešeného systému, tedy stavy které mohou vést ke zranění osob nebo poškození majetku, se považují:

1. Vydávání signálu VOLNO nebo jiného za něj zaměnitelného zvuku, má-li být vydáván signál STŮJ.
2. Vydávání signálu TICHO, má-li být vydáván signál STŮJ, bez indikace nadřízené stanici. Nevratné ukončení činnosti zařízení z důvodu poruchy, provázené jeho ztichnutím, se považuje za bezpečný stav, neboť v takovém případě dojde k přerušení komunikace s nadřízenou stanicí, na jejíž straně jsou následně provedena další opatření.

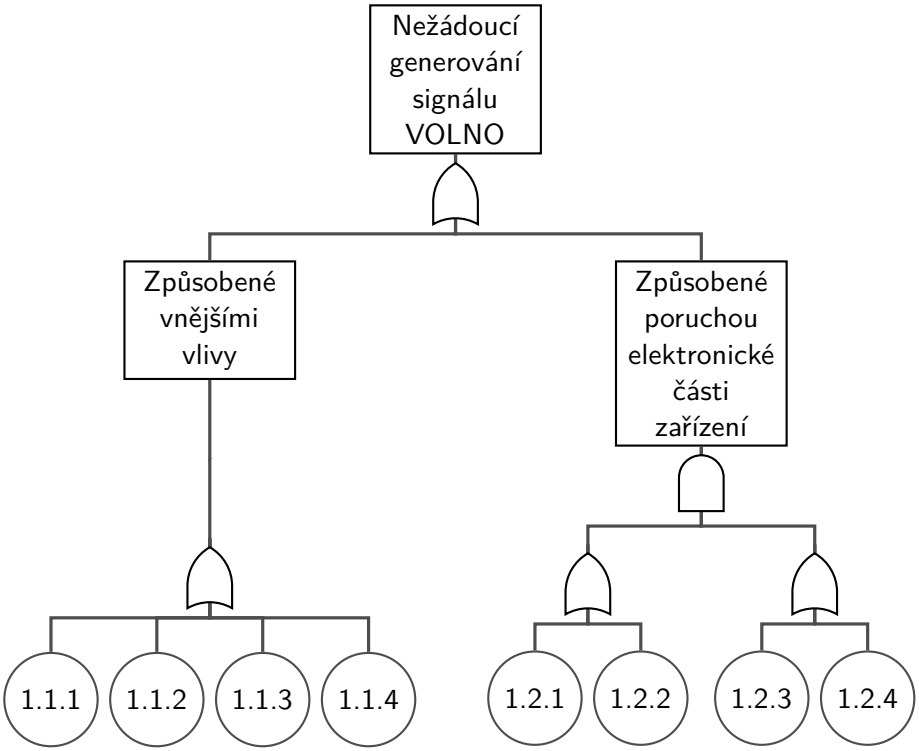
4.2 Události vedoucí k nebezpečím

Základní metodou této části jsou stromy poruch (FTA - Fault Tree Analysis). Vrcholem každého stromu je jedno nebezpečí. K němu jsou uvedeny všechny dedukované příčiny jeho vzniku, včetně jejich kombinací (ve stromu

se používají logické operátory AND a OR). V následujících podkapitolách jsou uvedeny jednotlivé prvotní příčiny a protiopatření k zabránění jejich vzniku.

4.2.1 Nežádoucí generování signálu VOLNO

Strom poruch je na obrázku 4.1.



Obrázek 4.1: Strom poruch způsobujících nežádoucí generování signálu VOLNO.

1.1. Vnější vlivy vedoucí k nežádoucímu generování signálu VOLNO:

1.1.1. **Elektromagnetické jevy způsobující zarušení komunikační linky.** Potenciální nebezpečí spočívá ve změně příslušné části datagramu vlivem silného vnějšího elektromagnetického pole působícího na datovou linku z povelu TICHO nebo VOLNO na povel STŮJ. *Protiopatření:* Používání komunikace zabezpečené cyklickým kódem, takže poškozené datagramy nejsou podřízenou stanicí brány v úvahu.

1.1.2. **Elektromagnetické jevy způsobující selhání mikrokontroléru.** Potenciální nebezpečí spočívá v chybě v běhu programu procesoru vlivem silného vnějšího elektromagnetického pole, v jejímž důsledku dojde k nevyžádanému vydávání signálu STŮJ. *Protiopatření:* Používání systému 2oo2, kdy selhání jednoho procesoru vyvolá nevratnou bezpečnou reakci druhé větve.

1.1.3. **Chybný požadavek nadřízené stanice.** Potenciální nebezpečí spočívá ve vygenerování špatného datagramu nadřízenou stanicí. *Protiopatření:* Chybný požadavek nadřízené stanice se neuvažuje, neboť tato musí generovat datagramy bezpečným způsobem.

1.1.4. **Záměna signálu stůj z více zařízení za signál volno.** Potenciální nebezpečí spočívá v generování signálu STŮJ více zařízeními s takovým posuvem fáze modulační obálky, že tento signál může být vyhodnocen lidským uchem jako jediný signál VOLNO. *Protiopatření:* Povelový datagram obsahuje kromě informace o požadovaném akustickém signálu rovněž hodnotu čítače modulo nejmenší společný násobek period signálů STŮJ a VOLNO (v milisekundách). Fáze modulační obálky všech zařízení na lince je tedy shodná. Předávání hodnoty čítače do datagramů v nadřízené stanici musí být prováděno bezpečným způsobem.

1.2. Poruchy elektronické části vedoucí k nežádoucímu generování signálu VOLNO:

1.2.1. **Porucha budiče**. Zahrnuje poruchy součástek od optočlenů tvořících člen AND až po koncové tranzistory. Potenciální nebezpečí spočívá v takové poruše některé ze součástek, která způsobí chybu buzení EAM. *Protiopatření:* Použití kvalitních součástek ve vhodném zapojení.

1.2.2. **Chyba mikrokontroléru.** Zahrnuje neočekávaný skok v programu, chybné zpracování kódu, chybné vyhodnocení přijatého datagramu a poruchy periferií. *Protiopatření:* Komparace analogových hodnot sousední větví a nevratné ukončení činnosti v případě nesouladu.

1.2.3. **Chyba obvodu snímání proudu.** Porucha obvodu přenášejících velikost náboje EAM na velikost napětí na vstupech procesorů. *Protiopatření:* Funkce obvodů zajišťujících komparaci úrovně výstupu je periodicky ověřována injektováním testovacího signálu.

1.2.4. **Chyba vyhodnocení snímaného náboje v sousední větvi.** *Protiopatření:* Viz 1.2.3.

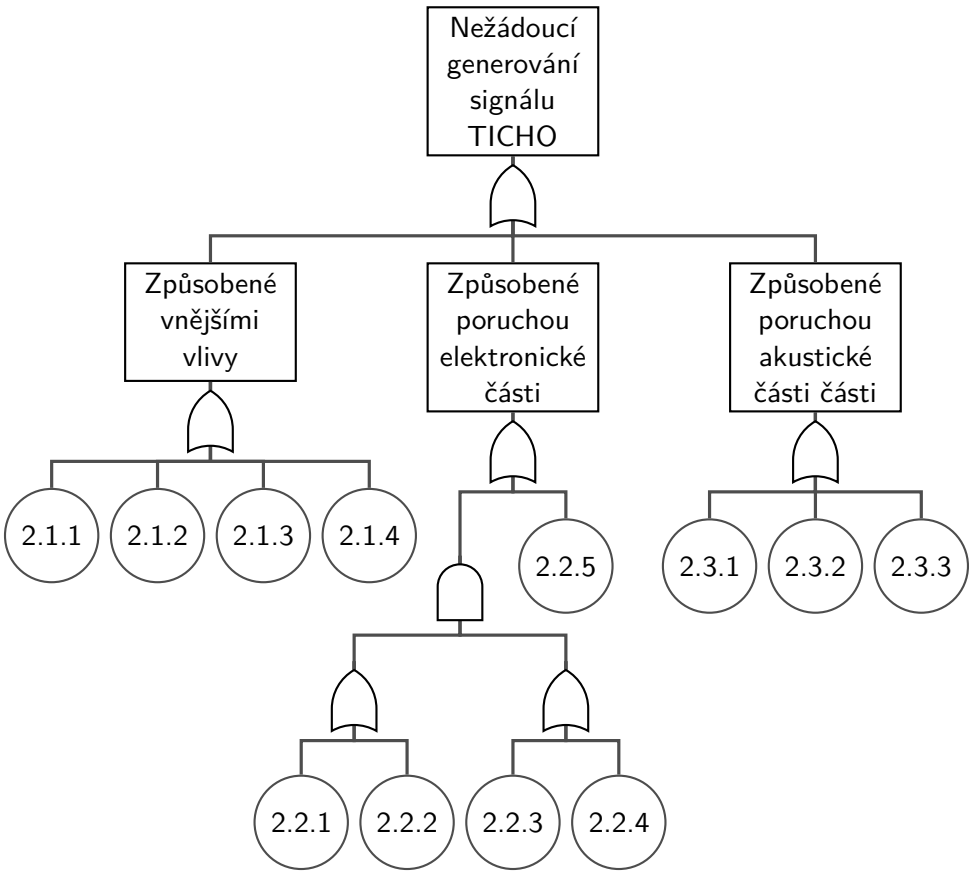
4.2.2 Nebezpečné generování signálu TICHO

Strom poruch je na obrázku 4.2. Nevratný bezpečný stav, který se rovněž projevuje ztichnutím zařízení, není uvažován, protože informace o přechodu do něj je bezpečným způsobem předávána nadřízené stanici přerušením komunikace.

2.1. Vnější vlivy způsobující nežádoucí generování signálu TICHO:

2.1.1. **Elektromagnetické jevy způsobující zarušení komunikační linky.** Viz 1.1.2

2.1.2. **Elektromagnetické jevy způsobující selhání mikrokontroléru.** Viz 1.1.1



Obrázek 4.2: Strom poruch způsobujících nežádoucí generování signálu TICHO.

2.1.3. **Chybný požadavek nadřízené stanice.** Viz 1.1.3

2.1.4. **Vybočení napájecího napětí z povolených tolerancí.** Vlivem nesprávného napájení může dojít k přerušení činnosti zařízení, což se projeví jeho ztichnutím. V takovém případě dojde i k přerušení komunikace, tato porucha tedy není nebezpečná.

2.2. Poruchy elektronické části způsobující nežádoucí generování signálu TICHO:

2.2.1. **Porucha budiče.** Viz 1.2.1.

2.2.2. **Chyba mikrokontroléru.** Viz 1.2.2.

2.2.3. **Chyba obvodu snímání proudu.** Viz 1.2.3.

2.2.4. **Chyba vyhodnocení snímaného náboje v sousední větvi.** Viz 1.2.4.

2.2.5. **Výpadek komunikace.** Zahrnuje poruchy vnějších komunikačních obvodů. *Protiopatření:* V případě poruchy komunikačních obvodů jedné větve je zařízení stále schopné bezpečně komunikovat po druhé lince. Při poruše v obou větvích dojde k přerušení komunikace, čímž je předána informace o poruše nadřízené stanici, která bezpečně zareaguje.

2.3. Poruchy akustické části způsobující nežádoucí generování signálu TICHO:

2.3.1. **Přerušení obvodu EAM.** Potenciální nebezpečí spočítá v elektrickém přerušení přívodních vodičů k piezomembráně. *Protiopatření:* V takovém případě EAM ztrácí kapacitu. Při periodické sebekontrole nedojde k nabití membrány, napětí na kapacitách ve snímacím můstku se nezmění, analogová kontrola vyhodnotí chybnou úroveň a dojde k inkrementaci poměrového čítače chyb. Pokud se tato chyba objeví ve třech po sobě jdoucích testech opakovaných po 5 s, přejde zařízení do nevratného bezpečného stavu.

2.3.2. **Zkrat EAM.** Potenciální nebezpečí spočívá ve zkratu elektrod EAM, ať už uvnitř nebo mezi přívodními vodiči. *Protiopatření:* V takovém případě dojde k výraznému zvýšení napětí na kondenzátorech snímacího můstku, což je po uplynutí stanovené toleranční doby vyhodnoceno jako analogová chyba a vede k neustálé inkrementaci poměrového čítače chyb. Po překročení tolerované meze dojde k nevratné bezpečné reakci.

2.3.3. **Pokles hlasitosti EAM** může být zapříčiněn zanesením vnějších částí mechanickými nečistotami. *Protiopatření:* Pravidelná kontrola.

4.3 Vyhodnocení rizika

Jednotlivým poruchám je přiřazena v souladu s [7] jedna z následujících úrovní závažnosti:

- **Katastrofická** - mnoho obětí na životech nebo vážných zranění
- **Kritická** - jedno úmrtí nebo vážné zranění
- **Okrajová** - jedno lehké zranění
- **Nevýznamná** - možné lehčí zranění

Dále je určena četnost výskytu jednotlivých poruchových událostí. Kategorie četností, blíže specifikované v [7] jsou:

- **častá**
- **pravděpodobná**
- **občasná**
- **malá**
- **nepravděpodobná**
- **vysoce nepravděpodobná**

Závažnost / Četnost	Nevýznamná	Okrajová	Kritická	Katastrofická
Častá	Nežádoucí	Nepřípustné	Nepřípustné	Nepřípustné
Pravděpodobná	Přípustné	Nežádoucí	Nepřípustné	Nepřípustné
Občasná	Přípustné	Nezádoucí	Nežádoucí	Nepřípustné
Malá	Zanedbatelné	Přípustné	Nežádoucí	Nežádoucí
Nepravděpodobná	Zanedbatelné	Zanedbatelné	Přípustné	Přípustné
Vysoce nepravděpodobná	Zanedbatelné	Zanedbatelné	Zanedbatelné	Zanedbatelné

Tabulka 4.1: Přiřazení rizika kombinacím četností a závažností

Zmiňovaná norma definuje četnosti pouze kvalitativně, kvantitativní odstupňování stanovuje provozovatel dráhy. Přiřazení četností v této práci bylo provedeno pouze na základě kvalitativního popisu.

Jednotlivým kombinacím četností a závažností je pak podle tabulky 4.1 přiřazeno jedno z následujících rizik:

- **Nepřípustné** - Musí být odstraněno
- **Nežádoucí** - Musí být odstraněno, jestliže je to prakticky dosažitelné. S jeho přijetím musí souhlasit provozovatel dráhy.
- **Přípustné** - Lze ho přijmout při přiměřené kontrole a se souhlasem provozovatele dráhy.
- **Zanedbatelné** - Lze ho přijmout bez souhlasu.

Tabulka 4.2 shrnuje všechny výše uvedené poruchy, jejich závažnosti a četnosti bez provedení protiopatření a s ním. Jejich kombinacím jsou přiřazena rizika. Přiřazení závažnosti jako kritické vychází z toho, že zařízení je určeno pro orientaci nevidomých osob, přičemž lze předpokládat, že těch se v jeho okolní nebude vyskytovat mnoho najednou. S provedenými opatřeními jsou všechna rizika zanedbatelná, pouze riziko zanesení membrány mechanickými nečistotami, které nelze elektricky detekovat, je klasifikováno jako přípustné.

Číslo poruchy	Závažnost	Bez protiopatření		S protiopatřením	
		Výskyt	Riziko	Výskyt	Riziko
1.1.1	Kritická	Pravděpodobný	Nepřípustné	Vysoce nepravděpodobný	Zanedbatelné
1.1.2	Kritická	Malá	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
1.1.3	Kritická	Vysoce nepravděpodobný	Zanedbatelné	-	-
1.1.4	Kritická	Častý	Nepřípustné	Vysoce nepravděpodobný	Zanedbatelné
1.2.1	Kritická	Nepravděpodobný	Přípustné	Vysoce nepravděpodobný	Zanedbatelné
1.2.2	Kritická	Malá	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
1.2.3	Kritická	Občasný	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
1.2.4	Kritická	Nepravděpodobný	Přípustné	Vysoce nepravděpodobný	Zanedbatelné
2.1.1	Kritická	Pravděpodobný	Nepřípustné	Vysoce nepravděpodobný	Zanedbatelné
2.1.2	Kritická	Malá	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.1.3	Kritická	Vysoce nepravděpodobný	Zanedbatelné	-	-
2.2.1	Kritická	Občasný	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.2.2	Kritická	Malá	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.2.3	Kritická	Občasný	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.2.4	Kritická	Nepravděpodobný	Přípustné	Vysoce nepravděpodobný	Zanedbatelné
2.2.5	Kritická	Občasný	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.3.1	Kritická	Malý	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.3.2	Kritická	Malý	Nežádoucí	Vysoce nepravděpodobný	Zanedbatelné
2.3.3	Kritická	Občasný	Nežádoucí	Nepravděpodobný	Přípustné

Tabulka 4.2: Vyhodnocení rizika jednotlivých uvažovaných poruch

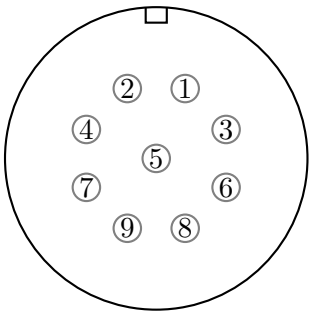
Kapitola 5

Realizace

Výsledkem úvah v předcházejících kapitolách jsou po hardwarové stránce schémata a desky plošných spojů v příloze A Vzhledem k prostorovým možnostem uvažovaných krabiček bylo vhodné realizovat napájecí zdroj a ostatní obvody (procesory, budič a spol.) jako dvě samostatné desky ZDROJ a PROC, umístěné nad sebou a propojené lištovými konektory.

Jako mechanický obal byl vybrán výrobek firmy GAINTA označený G212. Tato celoplastová krabička se skládá ze spodního dílu, který lze pomocí čtyř šroubů upevnit k podložce nebo držáku a k němuž lze přichytit rovněž pomocí čtyř šroubů desky plošných spojů, a průhledného víka. Díky průhlednému víku není třeba vrtat do krabičky díry pro indikační LED. Krabička sama o sobě splňuje stupeň krytí IP67. Pro připevnění piezoreproduktoru je ve víku vyříznuta díra a po jeho zasazení je provedeno dodatečné utěsnění tmelem, aby zařízení splnilo požadovaný stupeň krytí IP65 dle [32]. Konektor SP2113/P9 výrobce WEIPU, který je připevněn do výřezu ve spodním dílu krabičky a který zajišťuje připojení všech vnějších vodičů, splňuje stupeň krytí IP68. Jeho zapojení je na obrázku 5.1.

Desky plošných spojů jsou navrženy jako oboustranné. Deska ZDROJ je připevněna čtyřmi šrouby ke spodnímu dílu krabičky, deska PROC je uchycena pomocí tří distančních sloupků k desce ZDROJ. Výška těchto sloupků je 20 mm. Tvar desky PROC je ovlivněn požadavkem na přístup k napájecí WAGO svorce umístěné na desce ZDROJ a výškou soufázové tlumivky. Návrh desek byl proveden v softwaru OrCAD 16.2.



1 - GND B
2 - GND A
3 - DATA+ B
4 - DATA+ A
5 - NC
6 - DATA– B
7 - DATA– A
8 - napájení
9 - napájení

Obrázek 5.1: Zapojení vnějšího konektoru

Obrázek 5.2: Celkový pohled na navržené zařízení

5.1 Zkoušky

V průběhu všech zkoušek (není-li uvedeno jinak) bylo zařízení napájeno nominálním napětím 48 V z oddělovacího transformátoru LTS604. Jako nadřízená stanice sloužil stejně jako v průběhu celého vývoje přípravek S_PENET sloužící k simulaci nadřízené stanice v síti PENET se softwarovou úpravou pro protokol LEUNET.

5.1.1 Zkouška rozsahu napájecího napětí

Dle specifikace by zařízení mělo pracovat s napájecím napětím 48 V $\sim \pm 10\%$, tedy od 43,2 V do 52,8 V. S původní hodnotou Zenerova napětí diody D18 56 V docházelo ke vratném ukončení činnosti zařízení (viz kap. 3.12) již při napětí 44,5 V. Po výměně za diodu se Zenerovým napětím 51 V funguje zařízení od 39,5 V až k nejvyšší dovolené hranici. Její dlouhodobé překročení nebylo z důvodu možného poškození přepěťových ochran testováno.

5.1.2 Zkouška teploty

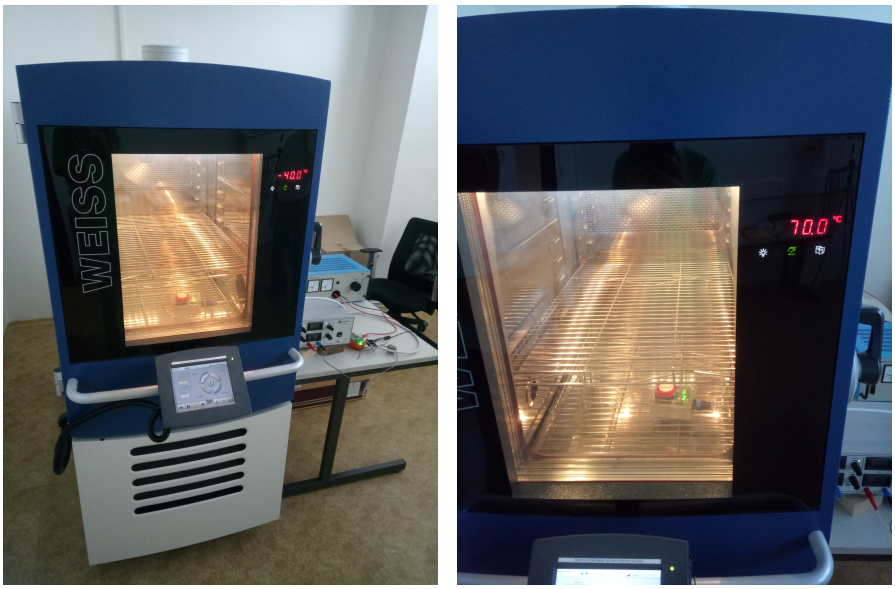
Zadání práce požaduje provedení zkoušky funkce v teplotním rozsahu $-40 \ldots 70\,^{\circ}\mathrm{C}$ v souladu s požadavky normy [33] pro zařízení klimatických tříd T1 a T2 umístěná v přístrojové skříni. Průběh zkoušek chladem a teplem blíže specifikují normy [34] a [35].

Zkouška chladem se provádí tak, že testované zařízení je umístěno do tepelné komory ve vypnutém stavu, následně je komora vychlazena na požadovanou teplotu a po jejím dosažení se čeká ještě 2 h pro dokonalé vyrovnání teplot. Poté je zařízení zapnuto a testuje se jeho funkce.

Při této zkoušce byl odhalen problém v programu, kdy při přechodu stavu z VOLNO nebo STŮJ na TICHO a tedy deaktivaci čítače TIMM bylo vyvoláno přerušení jako při přetečení, ovšem až po nastavení výstupu do klidového stavu, čímž pádem toto přerušení opětovně nastavovalo výstup na TÓN. Při pokojové teplotě se tento problém neprojevoval, protože zřejmě přerušení z TIMM přišlo dříve než nucené nastavení výstupu do klidu a jeho účinek byl tudíž negován. Tato chyba byla opravena přidáním podmínky v přerušení TIMM, že pro nastavení tónu musí být požadovaný stav výstupu STŮJ či VOLNO.

Dále byl zjištěn problém s měřicím můstkem. Návrh počítal s použitím různých typů kondenzátorů C29, C31 (velikost 1210, maximální napětí 70 V) a C26, C30 (velikost 0805, maximální napětí 25 V) kvůli úspoře místa na plošném spoji. Za určitých teplot (zhruba kolem -20 °C) ovšem docházelo k významnému vybočení měřených hodnot z tolerovaného pásma. Sjednocením typu kondenzátorů byl tento problém vyřešen.

Zkouška suchým teplem se provádí s testovaným zařízením v provozu od počátku zahřívání. Po dosažení stanovené teploty musí zařízení fungovat bez poruchy po dobu 2 h. Tato zkouška ukázala nutnost drobné úpravy parametrů vyhodnocování snímané hodnoty, poté fungovalo zařízení bezvadně.



(a) : Studený start při -40 °C **(b) :** Provoz při 70 °C

Obrázek 5.3: Testování zařízení v klimatické komoře

Obě zkoušky byly provedeny při nejnižším i nejvyšším dovoleném napájecím napětím.

Při nejvyšší dovolené teplotě okolí byla při samostatné zkoušce měřena rovněž teplota vzduchu v krabičce. Po zhruba hodině provozu při teplotě okolí 70 °C a vydávání signálu VOLNO se její hodnota ustálila na 75 °C, tedy s velkou rezervou pod nejvyšší přípustnou teplotou 89 °C, určenou výpočtem v kapitole Chlazení.

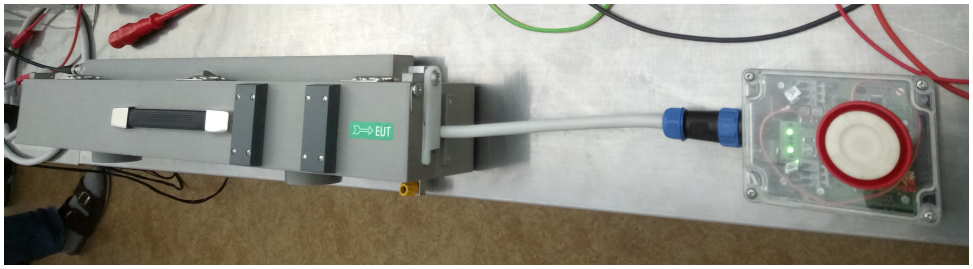
5.1.3 Zkouška elektromagnetické odolnosti

Norma [11] předepisuje provedení zkoušky odolnosti na napájení i komunikačních vodičích sestávající se ze tří částí: vysokofrekvenčního napětí nesymetricky, rychlých přechodných jevů a rázových impulsů.

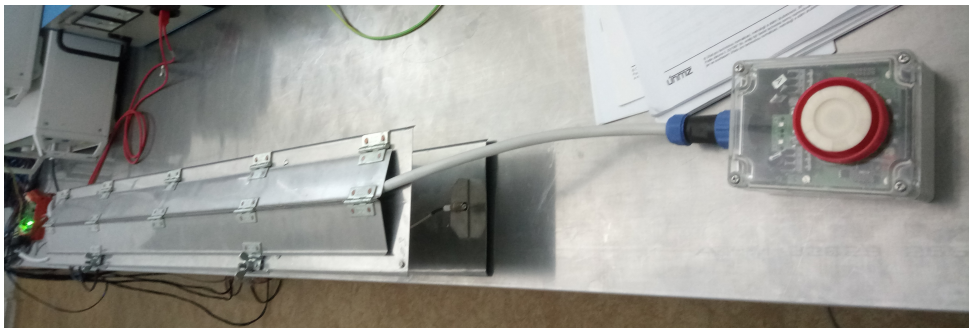
Vysokofrekvenční napětí o předepsané amplitudě v požadovaném frekvenčním rozsahu 150 kHz. . . 80 MHz generované přístrojem CWS500 výrobce EMTEST bylo injektováno do přívodního kabelu pomocí indukčních kleští Lüthi EM 101. Zařízení v průběhu testu nevykázalo poruchu, ani nedošlo k výpadku komunikace.

Rychlé přechodné jevy generované přístrojem UCS500M výrobce EMTEST byly injektovány pomocí kapacitních kleští na přívodním kabelu. Bohužel přípravek S_PENET nebyl určen k testování odolnosti podřízených stanic a není tedy vybaven příslušnými ochranami. Každý injektovaný přechodný jev tedy způsobil jeho výpadek. Testované zařízení nevykázalo poruchu, komunikace ovšem nebyla navázána.

Rázové impulsy nebyly zkoušeny, aby nedošlo ke zničení simulátoru nadřízené stanice.



(a) : s induktivními kleštěmi



(b) : s kapacitními kleštěmi

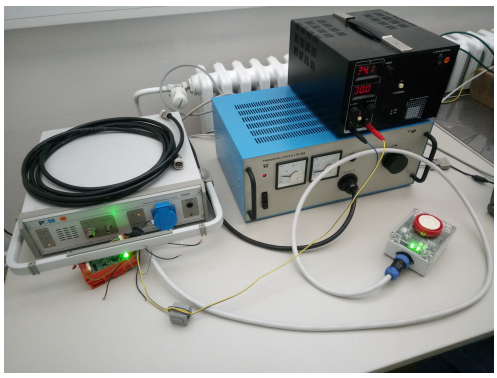
Obrázek 5.4: Testy elektromagnetické odolnosti

Kromě výše uvedených zkoušek aplikovaných na přívodní vodiče je vyžadován test odolnosti vůči elektrostatickému výboji. Byla provedena zkouška vzduchovým výbojem 8 kV aplikovaným na různá místa krabičky. Aplikace výboje neměla vliv na činnost zařízení.

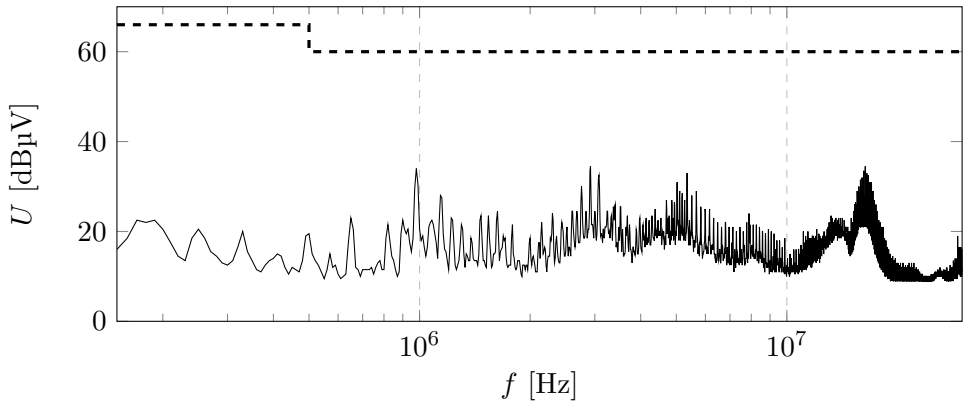
5.1.4 Zkouška elektromagnetické interference

Vyzařování zařízení do napájecích přívodů bylo měřeno přístrojem PMM 7000 výrobce Narda STS. Naměřené hodnoty včetně normou tolerovaných mezí jsou zobrazeny v grafech na obrázku 5.7.

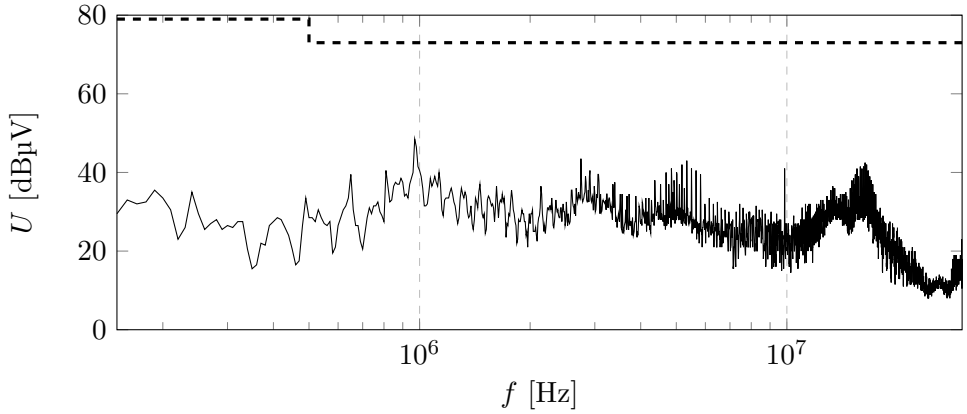
Obrázek 5.5: Zkouška elektrostatickým výbojem



Obrázek 5.6: Měření elektromagnetické interference



(a) : Střední hodnota



(b) : Kvazišpičková hodnota

Obrázek 5.7: Úroveň emise na napájecích svorkách (čárkovaně přípustná mez)

5.1.5 Zkouška navazování komunikace

Není-li komunikace navázána, musí být příjem datagramu očekáván v libovolné fázi programové smyčky. Tato zkouška měla prokázat, že je zařízení schopno přijmout datagram mimo synchrookno a zasynchronizovat programovou smyčku s komunikací.

Při testování byl simulátor nadřízené stanice externě restartován s prodlevami v intervalu 6…6,2 s s krokem 50 µs. Tím bylo zajištěno, že první datagram přišel postupně v různých fázích programové smyčky. Krok byl volen menší než délka jednoho symbolu příčné komunikace (78 µs), aby se projevila případná chyba při příchodu v průběhu každého jejího znaku.

Tato zkouška byla provedena třikrát, při zapojení pouze linky A, pouze linky B a obou linek.

5.1.6 Zkouška hlasitosti

Orientační zkouška hlasitosti byla provedena na volném prostranství. Testované zařízení bylo umístěno do výšky 2,5 m, což přibližně odpovídá budoucímu

Úhel [°]	Intenzita hlasitosti [dBA]
0	75
30	73
90	65
180	64

Tabulka 5.1: Naměřené intenzity zvuku

reálnému umístění na sloupku. Intenzita hlasitosti byla měřena hlukoměrem SM-20-A výrobce AMPROBE v módu "Slow"ve výšce 1,5 m nad zemí a vzdálenosti 7 m od testovaného zařízení vydávajícího signál VOLNO. Měření bylo provedeno při různém natočení testovaného zařízení vůči hlukoměru. Výsledky měření shrnuje tabulka 5.1. Úhel 0° odpovídá směru osy EAM. Naměřené hodnoty ve všech směrech splňují požadavky kladené normou [4].

Kapitola 6

Závěr

Podařilo se navrhnout a realizovat modul Akustické signalizace pro nevidomé jako součást Výstražného zabezpečení pro přechod kolejí v souladu s technickou specifikací [2] splňující požadavky norem pro drážní zařízení. Datové ovládání umožňuje nejen výrazně snížit počet vodičů od nadřízené stanici k jednotlivým ASN, ale i přenášet diagnostické informace. Díky maximálnímu využití periferií mikrokontrolérů a tím minimalizaci počtu externích součástek bylo docíleno malých rozměrů.

Na zařízení byly provedeny některé zkoušky ověřující jeho funkci za požadovaných podmínek prostředí. Splnění dosud netestovaných požadavků (například odolnosti vůči rázům a rychlým přechodným jevům) bude možné ověřit až po realizaci dostatečně odolné nadřízené stanice.

Zkoušky ukázaly, že potenciální slabinou návrhu je kontrola proudu do EAM pomocí kapacitního můstku. Keramické kondenzátory vykazují značné tolerance a nezanedbatelnou změnu kapacity se změnou teploty. Rovněž rozptyl kapacit použitého piezoměniče není zanedbatelný. Testování při různých teplotách ukázalo nutnost výrazného rozšíření tolerovaných mezí oproti původním předpokladům, přičemž je otázkou, zda bude vůbec možné dosáhnout jednotného nastavení mezí pro sériovou výrobu, nebo bude nutné každý vyrobený kus kalibrovat. Vzhledem ke kapacitnímu charakteru piezomembrány by nebylo vhodné přímo nahradit kapacitní můstek rezistorovým, neboť místo stálých úrovní by byly měřeny pouze špičky, jejichž velikost a šířka by navíc závisely na zesílení budicích tranzistorů. Určitým kompromisem by mohl být rezistorový můstek v kombinaci s aktivním integrátorem, čímž by pokleslo množství kondenzátorů na polovinu. Je ovšem s otazníkem, zda by takové řešení vůbec přineslo nějaké zlepšení.

Problematická je rovněž hlasitost zařízení - pokusy s několika exempláři EAM ukázaly značné rozdíly v jejich hlasitosti při stejné úrovni buzení. Vzhledem k malému počtu dostupných typů piezoměničů pro venkovní použití by náhrada jiným typem byla komplikovaná a výsledek nejistý. Normou dovolené pásmo hlasitostí je ovšem poměrně velkorysé a mělo by tak být možné po vyhodnocení hlasitosti většího počtu vzorků nastavit buzení tak, aby byla požadovaná úroveň hlasitosti splněna pro všechny exempláře daného typu.

Určitá vylepšení by bylo možné provést i na zdroji. Ukázalo se, že navržený

transformátor je výrobně poměrně komplikovaný, z čehož vyplývá jeho vysoká cena. Při akceptování mírně vyšších ztrát na usměrňovacích diodách by bylo možné nahradit dvojitá sekundární vinutí jednoduchými. Jednoduchý primár by naopak zřejmě nebyl ekonomický, protože můstkové buzení by znamenalo komplikovanější řídicí elektroniku a poloviční můstek by vyžadoval použití velkých kapacit, které by se nevešly do použité krabičky.

Před zahájení schvalovacího procesu bude kromě vyřešení výše uvedeného nutné nechat v souladu s požadavky normy [9] napsat software pro jednu z větví jiným programátorem.

Literatura

[1] NAŘÍZENÍ KOMISE (EU) č. 1300/2014 ze dne 18. listopadu 2014, *o technických specifikacích pro interoperabilitu týkajících se přístupnosti železničního systému Unie pro osoby se zdravotním postižením a osoby s omezenou schopností pohybu a orientace* (Text s významem pro EHP), Úřední věstník Evropské komise, 2014

[2] SŽDC TS 1/2018-Z *Výstražné zařízení pro přechod kolejí*, SŽDC, s. o., schváleno pod čj. 25864/2018-SŽDC-GŘ-O14 dne 10. 5. 2018

[3] Vyhláška č. 294/2015 Sb., *kterou se provádějí pravidla provozu na pozemních komunikacích,* In: Sbírka zákonů. 19. 3. 2020. ISSN 1211-1244.

[4] ČSN 34 2650 *Železniční zabezpečovací zařízení - Přejezdová zabezpečovací zařízení* ed. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010, 68 s.

[5] ČSN 34 2600 *Drážní zařízení - Železniční zabezpečovací zařízení* ed. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009, 12 s.

[6] ČSN EN 50129. *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektroniceké zabezpečovací systémy* ed. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2019, 158 s. Třídicí znak 34 2675

[7] ČSN EN 50126. *Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS).* Český normalizační institut, Praha, 72 s. Třídicí znak 33 3502

[8] ČSN EN 50159. *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Komunikace v přenosových zabezpečovacích systémech* ed. 3. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 60 s. Třídicí znak 34 2670

[9] ČSN EN 50128. *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy* ed.2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012, 108 s. Třídicí znak 34 2680

[10] ANDERLIK, Stefan. *Gemeinsames Subset der MISRA C Guidelines*, Version 1.0.3, Volkswagen AG, 2004.

[11] ČSN EN 50121-4. *Elektromagnetická kompatibilita - Část 4: Emise a odolnost zabezpečovacích a sdělovacích zařízení* ed. 4. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017, 24 s. Třídicí znak 33 3432

[12] MIKULČÁK Jiří et al. *Matematické, fyzikální a chemické TABULKY A VZORCE pro střední školy*. Praha: Prometheus, 2012, ISBN: 978-807196-264-9

[13] ČSN EN 61000-4-5. *Elektromagnetická kompatibilita (EMC) - Část 4-5: Zkušební a měřicí technika - Rázový impulz - Zkouška odolnosti.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015, 68 s. Třídicí znak 34 2670

[14] AŽD PRAHA s.r.o. *Protokol LEUNET verze 1.0*, 2018, 67 stran

[15] AŽD PRAHA s.r.o. *Implementace protokolu LEUNET v LEA*, 2018, 31 stran

[16] WOLF, Jack K., EVANS, Paula a PFISTER, Henry D. *An Introduction to Reed-Solomon Codes*, dostupné online z `http://pfister.ee.duke.edu/courses/ecen604/rspoly.pdf` [cit. 10. 12. 2019]

[17] GURUSWAMI, Venkatesan a BLAIS, Eric. *Notes 6: Reed-Solomon, BCH, Reed-Muller, and concatenated codes*, únor 2010, dostupné online z `https://www.cs.cmu.edu/~venkatg/teaching/codingtheory/notes/notes6.pdf` [cit. 10. 12. 2019]

[18] ADÁMEK, Jiří. *Kódování a teorie informace*. Praha: ČVUT, 1991.

[19] STMicroelectronics. *RM0365 Reference manual* STM32F302xB/C/D/E and STM32F302x6/8 advanced ARM®-based 32-bit MCUs [online][Cit. 5. 10. 2020] Dostupné z `https://www.st.com/en/microcontrollers-microprocessors/stm32f302cc.html#resource`

[20] STMicroelectronics. *STM32F302xB STM32F302xC* Arm®-based Cortex®-M4 32b MCU+FPU, up to 256KB Flash+ 40KB SRAM, 2 ADCs, 1 DAC ch., 4 comp, 2 PGA, timers, 2.0-3.6 V [online][Cit. 5. 10. 2020] Dostupné z `https://www.st.com/en/microcontrollers-microprocessors/stm32f302cc.html#resource`

[21] AVAGO TECHNOLOGIES. *ACPL-790B, ACPL-790A, ACPL-7900* Precision Isolation Amplifiers

[22] HAMDIOUI, Said. *Testing Static Random Access Memories: Defects, Fault Models and Test Patterns*. Springer US, 2004, ISBN: 978-1-4020-7752-4 [online][Cit. 4. 11. 2020] Dostupné z `https://www.broadcom.com/products/optocouplers/industrial-plastic/`

isolation-amplifiers-modulators/isolation-amplifiers/acpl-790a-000e

[23] Vigan. *Specification for approval* Piezo Audio Transducer KPEG1600NC [online][Cit. 4. 11. 2020] Dostupné z https://www.gme.cz/data/attachments/dsh.640-056.1.pdf

[24] TDK ELECTRONICS. *Ferrite Magnetic Design Tool*, [cit. 7. 11. 2019], dostupné z https://www.tdk-electronics.tdk.com/en/180490/design-support/design-tools/ferrite-magnetic-design-tool

[25] TEXAS INSTRUMENTS. *LM5030 100-V Push-Pull Current Mode PWM Controller* [online][Cit. 4. 11. 2020] Dostupné z https://www.ti.com/lit/ds/symlink/lm5030.pdf?&ts=1590003055079

[26] STMicroelectronics. *LEXX* Very low-dropout voltage regulator with inhibit function [online][Cit. 15. 11. 2020] Dostupné z https://www.st.com/resource/en/datasheet/cd00000545.pdf

[27] STMicroelectronics. *LFXX* Very low-dropout voltage regulator with inhibit function [online][Cit. 15. 11. 2020] Dostupné z https://www.st.com/resource/en/datasheet/lfxx.pdf

[28] DIODES INCORPORATED. *FZTH696B* 180V NPN MEDIUM POWER HIGH GAIN TRANSISTOR IN SOT223 [online][Cit. 17. 12. 2020] Dostupné z https://www.diodes.com/assets/Datasheets/FZT696B.pdf

[29] TDK. *CTVS Ceramic transient voltage suppressors* SMD multilayer varistors (MLVs), surge protection series [online][Cit. 1. 2. 2020] Dostupné z https://www.tdk-electronics.tdk.com/inf/75/db/CTVS_14/Surge_protection_series.pdf

[30] Littelfuse. *Transient Voltage Suppression Diodes* Surface Mount – 1500W > SMCJ series [online][Cit. 1. 2. 2020] Dostupné z https://www.littelfuse.com/~/media/electronics/datasheets/tvs_diodes/littelfuse_tvs_diode_smcj_datasheet.pdf.pdf

[31] TEXAS INSTRUMENTS. *THVD24x0 ±70-V Fault-Protected 3.3-V to 5-V RS-485 Transceivers With IEC ESD* [online][Cit. 1. 2. 2020] Dostupné z https://www.ti.com/lit/ds/symlink/thvd2410.pdf?&ts=1590004240472

[32] ČSN EN 60529 *Stupně ochrany krytem (krytí - IP kód)*, Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 1993, 40 s. Třídicí znak 33 0330

[33] ČSN EN 50125-3 *Drážní zařízení - Podmínky prostředí pro zařízení - Část 3: Zabezpečovací a sdělovací zařízení*, Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2003, 28 s. Třídicí znak 33 3504

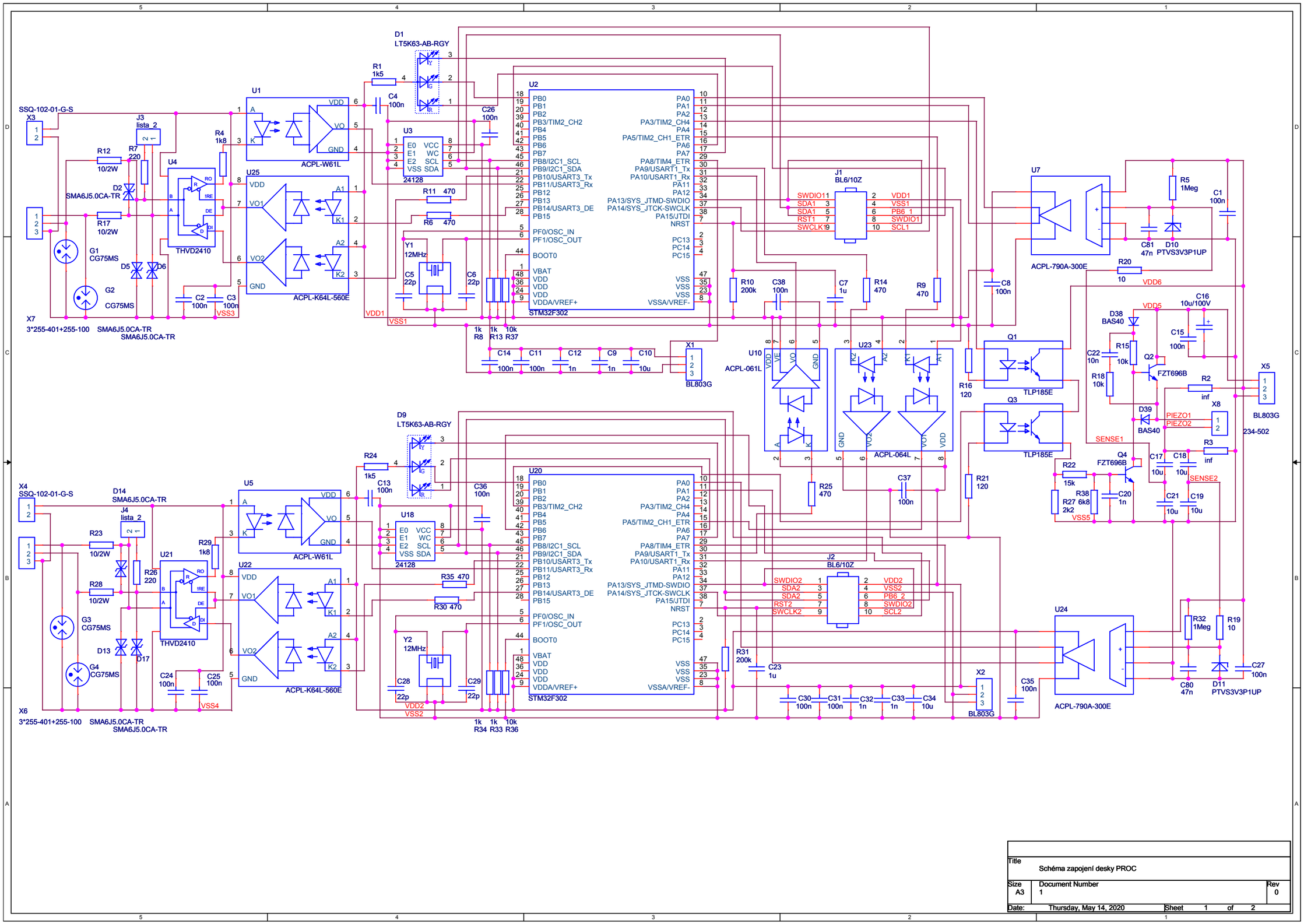
[34] ČSN EN 60068-2-1 *Zkoušení vlivů prostředí - Část 2-1: Zkoušky - Zkouška A: Chlad*, Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2008. Třídicí znak 34 5791

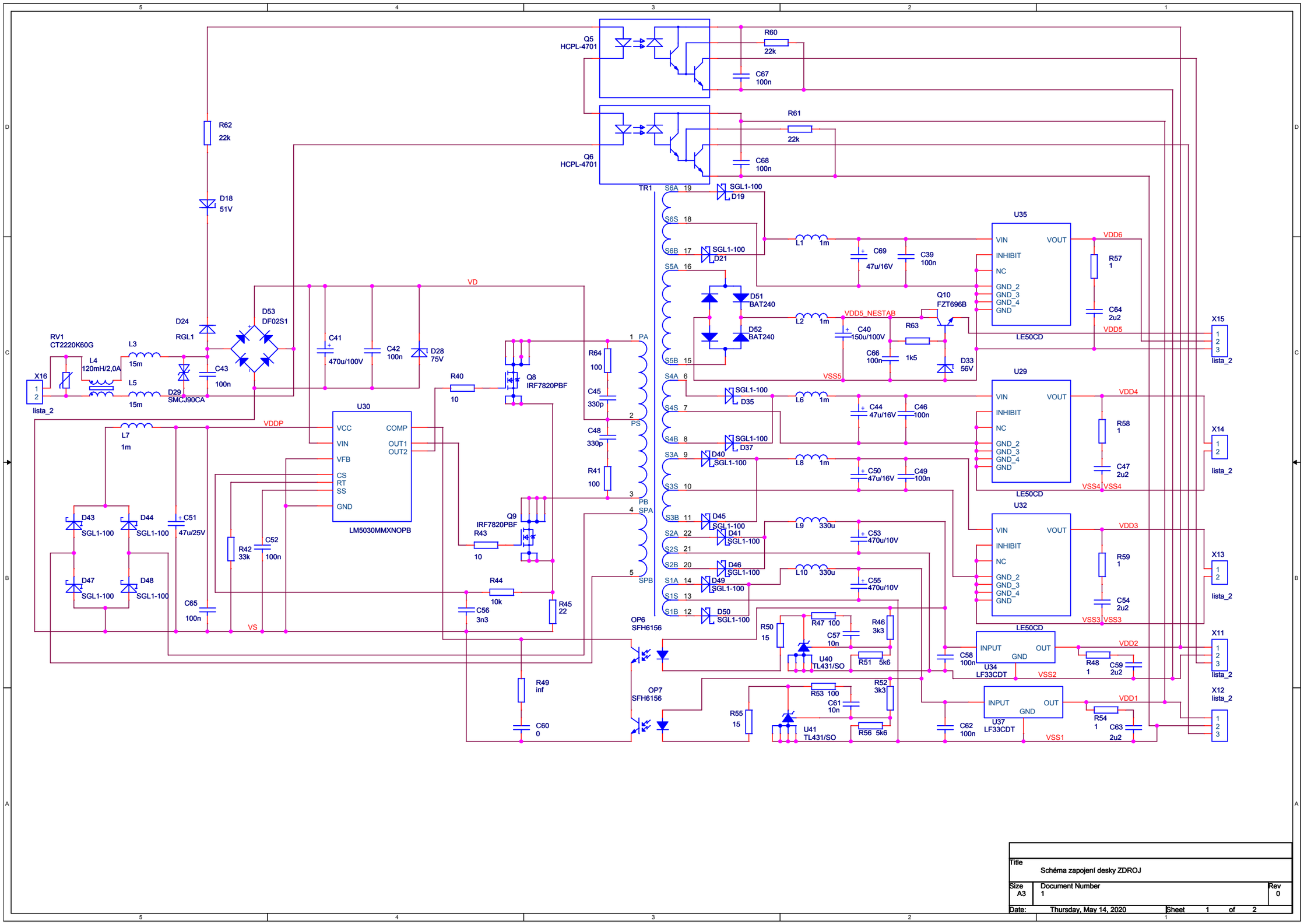
[35] ČSN EN 60068-2-2 *Zkoušení vlivů prostředí - Část 2-2: Zkoušky - Zkouška B: Suché teplo*, Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2008. Třídicí znak 34 5791

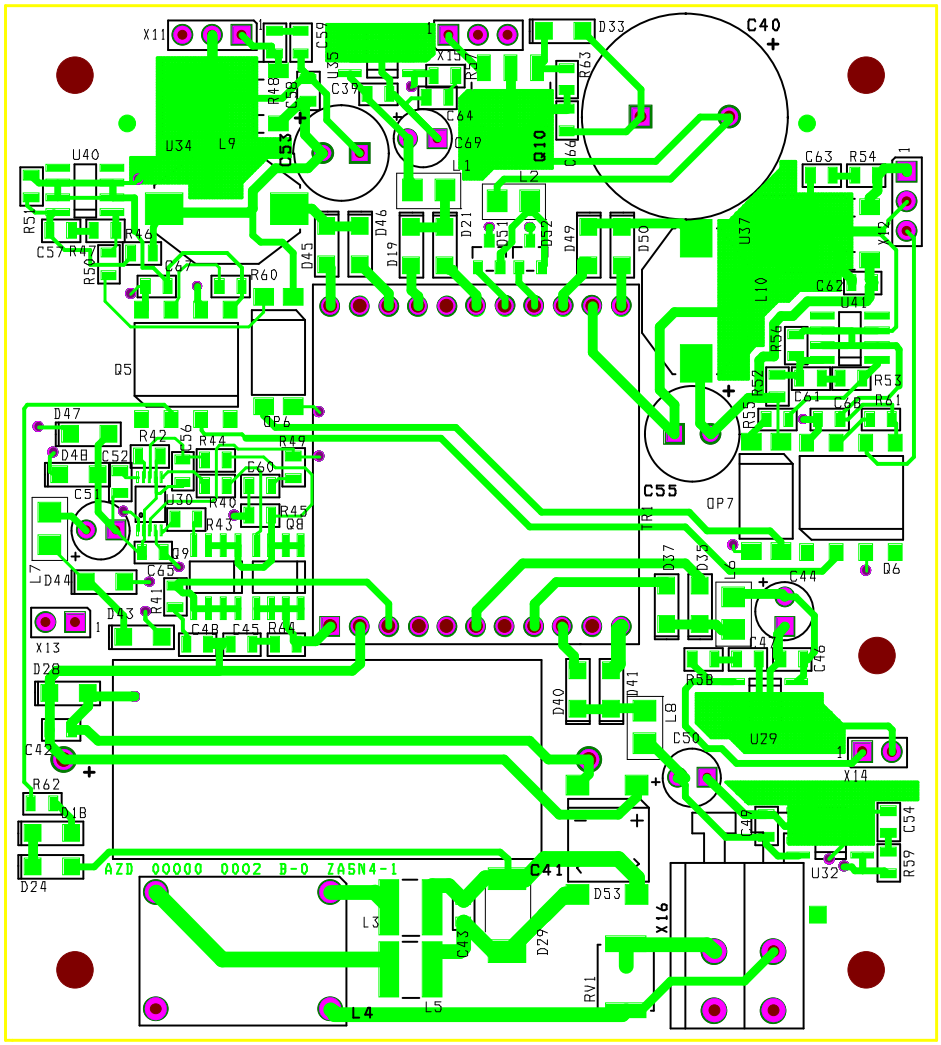
Příloha A

Schémata a DPS

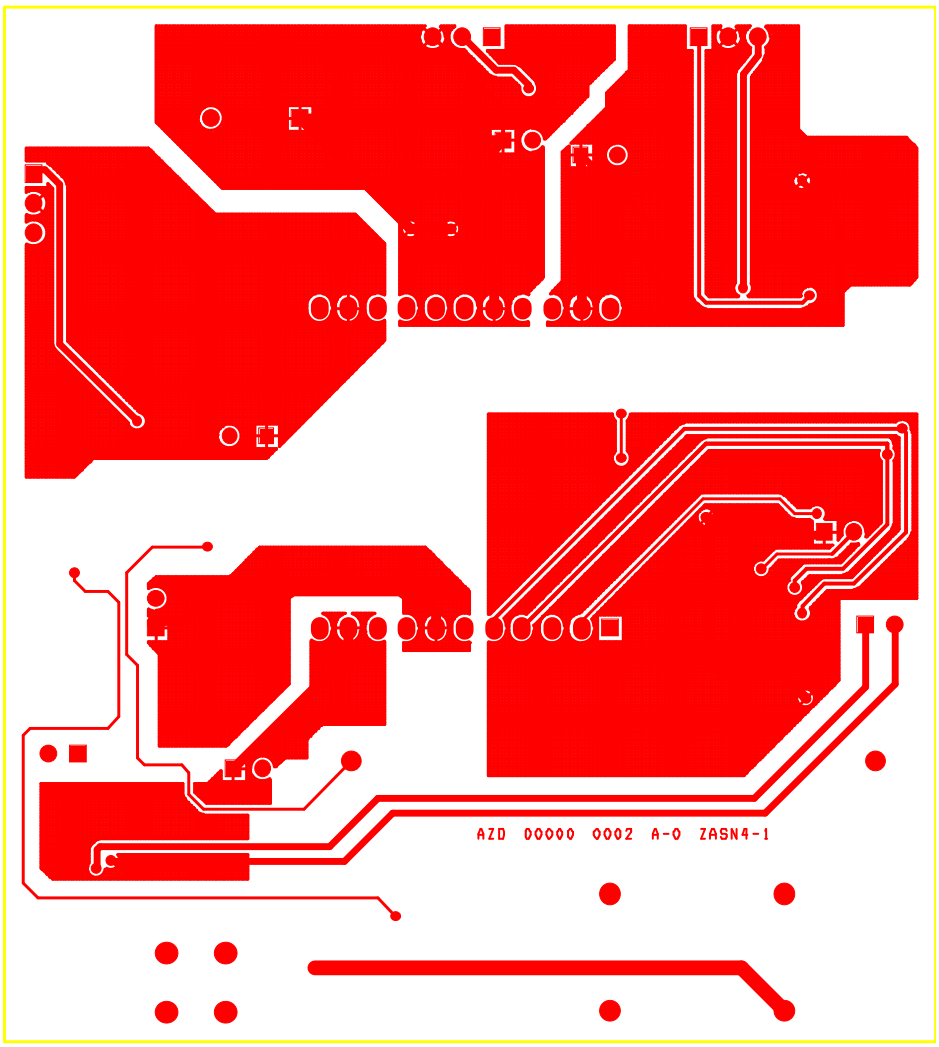
Tato příloha obsahuje schéma zapojení celého přístroje a pohled na obě desky plošných spojů (DPS) z obou stran. Schéma je rozděleno na dva listy, odpovídající jednotlivým DPS.


D1
LT5K63-AB-RGY
R1
1k5
C4
100n
C26
100n
U1
ACPL-W61L
U2
STM32F302
U3
24128
R11 470
R6 470
Y1
12MHz
C5
22p
C6
22p
C14 C11 C12 C9 C10
100n 100n 1n 1n 10u
X1
BL803G
VDD1
VSS1
SSQ-102-01-G-S
X3
J3
lista_2
R12
10/2W
R7
220
R4
1k8
U4
THVD2410
D2
SMA6J5.0CA-TR
R17
10/2W
G1
CG75MS
G2
CG75MS
D5
D6
C2
100n
C3
100n
VSS3
X7
3*255-401+255-100
SMA6J5.0CA-TR
SMA6J5.0CA-TR
U25
ACPL-K64L-560E
J1
BL6/10Z
SWDIO1
SDA1
SDA1
RST1
SWCLK1
VDD1
VSS1
PB6_1
SWDIO1
SCL1
R10
200k
C38
100n
C7
1u
R14
470
R9
470
C8
100n
U10
ACPL-061L
U23
ACPL-064L
R16
120
Q1
TLP185E
Q3
TLP185E
U7
ACPL-790A-300E
R5
1Meg
C1
100n
C81
47n
D10
PTVS3V3P1UP
R20
10
VDD6
VDD5
C16
10u/100V
C15
100n
D38
BAS40
C22
10n
R15
10k
Q2
FZT696B
R18
10k
R2
inf
X5
BL803G
234-502
X8
PIEZO1
PIEZO2
D39
BAS40
SENSE1
R3
inf
Q4
FZT696B
R22
15k
R38
2k2
R27
6k8
C20
1n
C17
10u
C18
10u
C21
10u
C19
10u
SENSE2
VSS5
D9
LT5K63-AB-RGY
R24
1k5
C13
100n
C36
100n
U5
ACPL-W61L
U18
24128
R35 470
R30 470
Y2
12MHz
C28
22p
C29
22p
VDD2
VSS2
U20
STM32F302
X4
SSQ-102-01-G-S
D14
SMA6J5.0CA-TR
J4
lista_2
R23
10/2W
R28
10/2W
R26
220
R29
1k8
U21
THVD2410
U22
ACPL-K64L-560E
G3
CG75MS
G4
CG75MS
D13
D17
C24
100n
C25
100n
VSS4
X6
3*255-401+255-100
SMA6J5.0CA-TR
SMA6J5.0CA-TR
J2
BL6/10Z
SWDIO2
SDA2
SDA2
RST2
SWCLK2
VDD2
VSS2
PB6_2
SWDIO2
SCL2
R25
470
C37
100n
R21
120
R31
200k
C23
1u
C30 C31 C32 C33 C34
100n 100n 1n 1n 10u
X2
BL803G
C35
100n
U24
ACPL-790A-300E
R32
1Meg
R19
10
C80
47n
D11
PTVS3V3P1UP
C27
100n
1k R8
1k R13
10k R37
1k R34
1k R33
10k R36
Title
Schéma zapojení desky PROC
Size
A3
Document Number
1
Rev
0
Date:
Thursday, May 14, 2020
Sheet
1
of
2

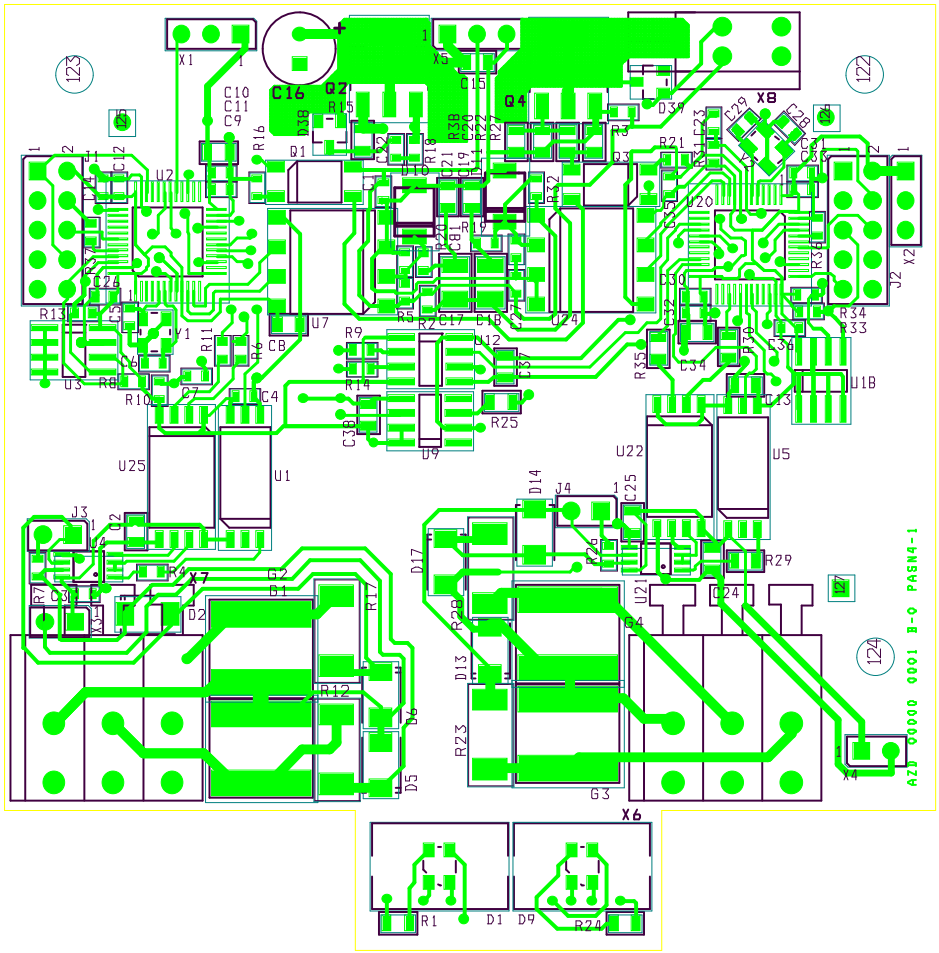

Q5 HCPL-4701
R60 22k
C67 100n
Q6 HCPL-4701
R61 22k
C68 100n
R62 22k
D18 51V
TR1
S6A 19
S6S 18
S6B 17
S5A 16
S5B 15
S4A 6
S4S 7
S4B 8
S3A 9
S3S 10
S3B 11
S2A 22
S2S 21
S2B 20
S1A 14
S1S 13
S1B 12
SGL1-100 D19
SGL1-100 D21
SGL1-100 D35
SGL1-100 D37
D40 SGL1-100
D45 SGL1-100
D41 SGL1-100
D46 SGL1-100
D49 SGL1-100
D50 SGL1-100
L1 1m
L6 1m
L8 1m
L9 330u
L10 330u
C69 47u/16V
C39 100n
C44 47u/16V
C46 100n
C50 47u/16V
C49 100n
C53 470u/10V
C55 470u/10V
D51 BAT240
D52 BAT240
L2 1m
VDD5_NESTAB
C40 150u/100V
C66 100n
R63 1k5
Q10 FZT696B
D33 56V
VSS5
U35
VIN
INHIBIT
NC
GND_2
GND_3
GND_4
GND
VOUT
LE50CD
VDD6
R57 1
C64 2u2
VDD5
X15
lista_2
U29
VDD4
R58 1
C47 2u2
VSS4
X14
U32
VDD3
R59 1
C54 2u2
VSS3
X13
U34 LF33CDT
INPUT
OUT
VDD2
R48 1
C59 2u2
X11
U37 LF33CDT
VDD1
R54 1
C63 2u2
X12
VD
RV1 CT2220K60G
L4 120mH/2,0A
L3 15m
L5 15m
X16
lista_2
D24 RGL1
D53 DF02S1
D29 SMCJ90CA
C43 100n
C41 470u/100V
C42 100n
D28 75V
R40 10
Q8 IRF7820PBF
R64 100
C45 330p
C48 330p
R41 100
Q9 IRF7820PBF
R43 10
R44 10k
C56 3n3
R45 22
R49 inf
C60 0
1 PA
2 PS
3 PB
4 SPA
5 SPB
VDDP
L7 1m
U30
VCC
VIN
VFB
CS
RT
SS
GND
COMP
OUT1
OUT2
LM5030MMXNOPB
D43 SGL1-100
D44 SGL1-100
C51 47u/25V
D47 SGL1-100
D48 SGL1-100
C65 100n
R42 33k
C52 100n
VS
OP6 SFH6156
OP7 SFH6156
R50 15
R47 100
C57 10n
R46 3k3
U40 TL431/SO
R51 5k6
C58 100n
R53 100
C61 10n
R52 3k3
R55 15
U41 TL431/SO
R56 5k6
C62 100n
VSS1
VSS2
VSS3
VSS4
Title
Schéma zapojení desky ZDROJ
Size A3
Document Number 1
Rev 0
Date: Thursday, May 14, 2020
Sheet 1 of 2



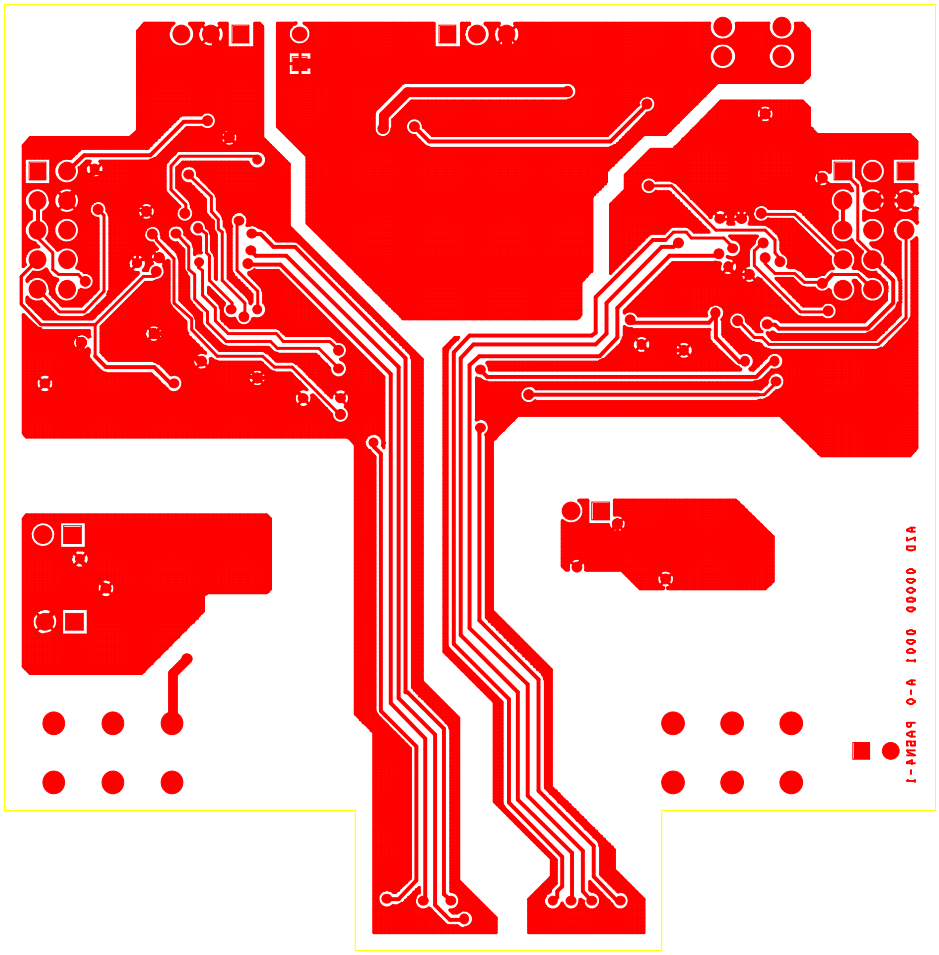
Obrázek A.3: Deska ZDROJ - strana TOP s potiskem



Obrázek A.4: Deska ZDROJ - strana BOT



Obrázek A.5: Deska PROC - strana TOP s potiskem



Obrázek A.6: Deska PROC - strana BOT

Příloha B

Zdrojový kód

Zdrojový kód je přiložen na CD. Pro obě větve je kód stejný, rozlišení větví se provádí pomocí příkazu preprocesoru, a sice definováním makra `BRANCH` v souboru `config.h` jako 0 nebo 1 pro větev A, resp. B.

Kromě toho je přiložen jednoduchý program pro zápis kontrolních součtů programové paměti `flashCRCCalc`.