F3

Fakulta elektrotechnická
Katedra radioelektroniky

Bakalářská práce

Kartový přístupový systém

Viktor Bohuněk

květen 2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Bohuněk** Jméno: **Viktor** Osobní číslo: **474229**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra radioelektroniky**

Studijní program: **Elektronika a komunikace**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Kartový přístupový systém

Název bakalářské práce anglicky:

Access Control System

Pokyny pro vypracování:

Cílem práce je návrh a implementace samostatného kartového přístupového systému. Při vypracování se řiďte následujícími pokyny:
1) Nastudujte normy, které návrh a provozování těchto systémů upravují.
2) Na základě teoretických podkladů navrhnětě jednotku, která bude obsluhovat jednotlivé dveře. Jednotku implementujte a otestujte v reálném provozu.
3) Navrhněte a implementujte ovládací server, který bude možné dále napojit k zdroji přístupových práv.

Seznam doporučené literatury:

[1] ČSN EN 60839-11-1, Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty, Česká technická norma, 2016
[2] ČSN EN 60839-11-2, Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace, Česká technická norma, 2016

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Stanislav Vítek, Ph.D., katedra radioelektroniky FEL

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

Datum zadání bakalářské práce: **24.01.2020** Termín odevzdání bakalářské práce: **22.05.2020**

Platnost zadání bakalářské práce: **30.09.2021**

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

III. PŘEVZETÍ ZADÁNÍ

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

. Datum převzetí zadání

Podpis studenta

Prohlášení autora

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. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č.121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne podpis

_____ _____

Viktor Bohuněk

Anotace

Cílem této práce je připravit základ pro budování vlastních elektronických systémů kontroly vstupu. Požadavky byly čerpány z technické normy ČSN EN 60839-11-1. V úvodu práce jsou krátce představena již existující komerční řešení a podobné závěrečné práce.

V rámci práce vznikla hardwarová jednotka, která obsluhuje dveře a softwarový řídicí server, se kterým jednotka komunikuje. Při implementaci bylo důležité vybrat vhodná technická řešení a cena hrála až druhou roli, protože úspory na nesprávných místech byly jedním z největších problémů podobných existujících prací. Nakonec se během vývoje ukázalo, že ne všechna nalezená řešení jsou plně funkční, tyto chyby jsou v práci popsány včetně navržených řešení, aby bylo možné je v budoucnu odstranit.

Cíl práce byl nakonec naplněn a vyvinutý systém je funkční. Až se podaří odstranit v práci popsané nedostatky, bude možné komponenty použít pro budování vlastních systémů, které budou snadno přizpůsobitelné konkrétním potřebám každé instalace.

Klíčová slova

NFC, C, Rust, elektronický systém kontroly vstupu, přístupový systém, Linux, ESP32

Annotation

In the last decade, electronic access control systems became part of our lives, and they are the next step in the evolution of physical security. With a smarter and more flexible approach than cylinder locks, they are predestined to be used in places where the amount of people makes the process of distributing standard keys difficult.

This thesis evaluates existing commercial solutions as well as similar theses. Commercial solutions are expensive but prepared for large scale deployment and integration to enterprise systems. Results of the theses, on the other hand, aim to be used in small deployments and their main quality is low price. This thesis designs and implements a system between these two extremes. The system that values good choices more than costs and is prepared to be integrated into nearly any existing credential management system.

Key words

NFC, C, Rust, electronic access control system, Linux, ESP32

Poděkování

Děkuji Ing. Stanislavu Vítkovi, Ph.D. za vedení mé bakalářské práce. Mé poděkování dále patří Ing. Tomáši Teplému za konzultace z oblasti embedded řešení, Pavlu Dostálovi za praktické rady ohledně OS Linux a paní Janě Dušátkové za korekturu práce.

Obsah

Seznam zkratek a symbolů

ACU Access control unit (Řídicí jednotka kontroly vstupu)

BCD Binary Code Decimal

BLE Bluetooth Low Energy

CAN Controller Area Network

CN Common Name

ČSN EN Česká technická norma Evropská norma

DCU Řídicí jednotka portálu

DCUS Server řídicí jednotky portálu

DPS Deska Plošných Spojů

EACS Elektronický systém kontroly vstupu (Electronic access control system)

ECC Error Checking and Correcting

EEPROM Electrically Erasable Programmable Read-Only Memory

FIFO First In, First Out

GCC GNU Compiler Collection

GND Ground

GPIO General-purpose input/output

GW Gateway

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IO Input/Output

JSON JavaScript Object Notation

LDAP Lightweight Directory Access Protocol

LED Light-Emitting Diode

LSB Least Significant Bit

MAC V práci použito ve významu HW periferie implementující funkce Media Access Control ze standardu 802.3 (Ethernet)

MOSFET Metal Oxide Semiconductor Field Effect Transistor

MSB Most Significant Byte

NFC Near Field Communication

PHY Physical Layer – HW periferie implementující funkce fyzické rozhraní podle standardu 802.3 (Ethernet)

PoE Power over Ethernet

QFN Quad-Flat No-leads

REST API Representational State Transfer Application Programming Interface

RFC Request For Comments

RFID Radio Frequency Identification

RTC Real-time clock

SPDT Single pole, double throw

SPIFFS SPI Flash File System

SRAM Static Random Access Memory

TCP Transmission Control Protocol

TLS Transport Layer Security

TOML Tom's Obvious, Minimal Language

UART Universal asynchronous receiver-transmitter

UID Unique ID pro karty typu Mifare

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Elektronické systémy kontroly vstupu představují moderní alternativu k cylindrickým vložkám. Na rozdíl od svých mechanických předchůdců nabízí flexibilitu, kladou menší finanční nároky na správu, mnohem lépe pracují s identifikačními tokeny a dokáží poskytovat informace o přístupu do chráněného prostoru. I proto se elektronické systémy kontroly vstupu používají stále častěji nejen v průmyslu, kancelářských budovách, hotelech, ale také v bytových domech nebo školách.

Na trhu je dostupné množství komerčních systémů. Tyto systémy jsou svou cenou, nároky na odbornou montáž a rozsahem integrovaných funkcí určené především pro zákazníky, kteří nemají kapacity systém budovat svépomocí. Na druhé straně spektra jsou obdobné závěrečné práce na téma elektronických systémů kontroly vstupu. Tyto práce většinou opomíjí existující technické normy a mnohdy navíc zcela zbytečně rezignují na bezpečnost komunikace. Jiné systémy jsou navrženy s myšlenkou na jednu jedinou instalaci, která se ani nerozprostírá přes více objektů. Existují i práce čistě zaměřené na maximální stlačení ceny, které vede k používání komponent neznámých výrobců a technologií, které jsou dnes na poli systémů kontroly vstupu na ústupu.

Cílem této práce je nabídnout střední cestu v podobě solidního základu vycházejícího z platných technických norem, který není vázán na konkrétní zdroj přístupových práv ani konkrétní ovládací panel. Tyto dvě komponenty sice tvoří jádro systému, ale jejich vynechání umožňuje věnovat větší pozornost zbylým částem systému a především poskytuje maximální integrovatelnost do již existujících systémů.

V úvodní kapitole budou představena konkurenční řešení z obou sfér. V teoretické části budou sepsány požadavky, které klade na elektronické systémy kontroly vstupu dvojice norem ČSN EN 60839-11-1 a ČSN EN 60839-11-2, představena koncepce vyvíjeného systému a konkrétní požadavky na jednotlivé komponenty. V praktické části bude představena implementace jednotlivých komponent systému. Na závěr bude provedeno přezkoušení systému podle postupů uvedených v ČSN EN 60839-11-1.

Kapitola 2

Použité technologie

ESP32 Mikrokontrolér od společnosti Espressif založený na 32-bitovém mikroprocesoru Xtensa LX6.

Rust Open-source programovací jazyk, staticky typovaný, zaměřený na tvorbu vysoce paralelních a zároveň paměťově bezpečných programů. Syntakticky je podobný jazyku C++.

ESP-IDF Open-source IoT framework v jazyce C pro mikrokontrolér ESP32 vyvíjený pod záštitou společnosti Espressif.

Ethernet Souhrn technologií standardizovaných jako IEEE 802.3. Dnes se jedná o dominantní technologii na poli kabelových lokálních sítí.

HTTP Internetový protokol používaný pro komunikaci se servery. Do verze 2.0 se jedná o čistě textový protokol.

TLS Kryptografický protokol poskytující zabezpečenou komunikace mezi klientem a serverem.

FreeRTOS Open-source real-time jádro pro operační systém.

NFC Technologie bezdrátové komunikace na velmi malou vzdálenost (do 4 cm) definovaná standardy ISO.

SPIFFS Speciální filesystem pro embedded zařízení určený pro provoz nad NOR flash pamětí

Kapitola 3

Teoretická část

3.1 Komerční elektronické systémy kontroly vstupu

V dnešní době existuje mnoho firem, které se zabývají návrhem a výrobou elektronických systémů kontroly vstupu (EACS). Společnosti a jejich systémy, které jsou v této práci uvedené, zná autor jako uživatel a jejich seznam rozhodně nepovažuje za vyčerpávající. U každé společnosti bude představeno, jaké produkty dodává, jaká je jejich architektura, s kterými identifikačními prostředky umí pracovat a jaké možnosti integrace jsou nabízeny.

3.1.1 Jablotron

Jablotron se dnes zaměřuje na dodávání komplexních řešení, která integrují kromě EACS také elektronickou zabezpečovací signalizaci a prvky systémů chytrých budov. Cílovou skupinou jsou jak firmy, bytové domy, tak i domácnosti. Aktuálně jsou nabízeny zařízení dvou produktových řad - JABLOTRON 80 a JABLOTRON 100 [20].

Systémy jsou postaveny kolem hardwarové ústředny, která obsluhuje bezdrátové i drátové periferie a je řídicím centrem každé instalace. Mezi periferie patří různé ovládací prvky, detektory a aktuátory.

Základní identifikaci uživatele lze provést pomocí klávesnice, která je vestavěna do ovládacího panelu systému. Samozřejmostí jsou RFID klíčenky, které ovšem používají proprietární komunikační protokol „Jedinečný kód Jablotron“ [19], a tak i přes shodnou frekvenci 125 kHz nejsou podporovány generické klíčenky. Dále je možné použít bezdrátové ovladače, které fungují do vzdálenosti několika metrů a jsou k dispozici i ve variantě s příjmem potvrzení akce.

Pro integraci do dalších systémů je k dispozici modul JA-121T [18], který zpřístupňuje systémovou sběrnici přes rozhraní RS-485.

3.1.2 IMA

IMA vyrábí systémy, které se zaměřují na identifikaci uživatelů nebo předmětů, např. zboží. V oblasti identifikace uživatelů se věnuje kromě EACS také docházkovým systémům. Rozsahem svých služeb cílí jak na malé instalace typu bytového domu, tak na rozsáhlé komplexy budov, které mohou využít jejich cloudového řešení. V nabídce [17] najdeme 4 verze systému IMAporter, které se liší především rozsahem cílové instalace.

Z veřejně dostupných informací [16] [13] lze odvodit, že v základních systémech IMAporter Mobile a Basic je veškerá logika implementována do jednotlivých čteček. Ke čtečkám je pak dodáván externí reléový modul, díky kterému je zajištěno, že není možné snadno sepnout elektronický zámek zvenčí chráněného prostoru. Co se týče systémů IMAporter Pro a Cloud, tak z [15] [14] vyplývá, že jsou tyto systémy vybaveny centrální databází, podle které se přes síť řídicích jednotek programují jednotlivé čtečky.

Systémy IMA podporují běžné karty standardu NFC a identifikaci pomocí mobilního telefonu, a to jak pomocí NFC, tak BLE. Hlavní výhodou BLE oproti NFC je delší dosah, řádově jednotky metrů.

Základní systémy Mobile a Basic nenabízí žádnou integraci do jiných systémů, naopak verze Pro a Cloud je možné propojit se systémem SAP a případně tak s dalšími produkty IMA postavit komplexní řešení, které zastřeší stravování, docházky, tisk a další.

3.1.3 2N

2N se zaměřuje na trh IP interkomů, se kterými EACS úzce souvisí. Cílová skupina jejich produktů zahrnuje jak rodinné a bytové domy, tak korporátní sektor nebo školy. V nabídce [2] je několik různých jednotek, mezi jejich hlavní výhody patří IP konektivita a PoE.

Systém 2N je distribuovaný a jednotky se programují vzdáleně pomocí dodávaného softwaru. Podle manuálu [1] se počítá s využitím relé umístěného přímo ve čtečce, což může představovat bezpečnostní riziko.

Jednotky pracují jak s RFID čipy na frekvenci 125 kHz, tak s moderními NFC kartami nebo mobilními telefony skrze BLE. K dispozici jsou ale i kombinace s klávesnicí nebo dedikovaná čtečka otisků prstů. Tyto čtečky je pak možné ještě nalézt zabudované jako součást interkomů.

K integraci čteček do aplikací třetích stran je k dispozici API.

3.1.4 Shrnutí

Je jisté, že tyto systémy mají své místo na trhu. Vhodné jsou zejména tam, kde neexistuje potřeba napojení na existující správu identit a systém tak musí být jednoduchý na nasazení a používání. Pro změnu v prostředí velkých společností je důležité mít systém s technickou podporou, a to jak při instalaci, tak především během jeho života. Navíc pro opravdu velké společnosti už jsou nabízeny integrace do jejich aktuálních systémů, a dokonce možnost obalit si EACS množstvím dalších funkcí. Všechny tyto výhody ale zabraňují využít tyto systémy v nekomerčních prostředích. Ať už se jedná o různá občanská sdružení, nebo i nedůvěřivé znalé uživatele, kteří by rádi měli celý systém pod kontrolou.

3.2 Obdobné závěrečné práce

Prací na téma EACS existuje velké množství, a proto se autor rozhodl výběr omezit na práce, které nebudou starší 5 let a jejichž součástí je konstrukce hardwaru. Dále byly vyřazeny práce, které používají jiné identifikační prostředky než komponenty RFID. Posledním kritériem byl způsob komunikace, kdy je od každého typu zastoupen jeden systém. U každé práce bude zmíněn její cíl, architektura systému, podporované identifikační prostředky a autorovy výhrady k použitým řešením.

3.2.1 Přístupový systém založený na NFC [28]

Práce si neklade za cíl instalovat navržený systém a věnuje se hlavně technologiím, které se v EACS používají.

Jednotka obsluhující portál je postavena kolem jednodeskového počítače Raspberry Pi 2 B a je vybavena obslužným programem napsaným v jazyce Java s nízkoúrovňovou knihovnou v C++. Ke čtení karet se používá modul Itead PN532, který umožňuje skrz knihovnu Libnfc využívat mnoho pokročilých NFC funkcí. Server je postaven nad Apachem s PHP a naprogramovaný ve frameworku Nette. Server kromě API pro čtečky poskytuje ovládací webové rozhraní a také zaznamenává akce, které jsou v systému provedeny. Komunikace mezi jednotkou a serverem probíhá přes HTTPS a jednotka vyžaduje připojení k serveru pro provádění autentizace uživatele. Jako komunikační rozhraní mezi serverem a jednotkou je zvolena WiFi.

Systém spolupracuje s Android aplikací, která s pomocí NFC v telefonu slouží jako identifikační token. Aplikace je připravena pro spolupráci s více instalacemi. Ověřování probíhá pomocí asymetrické kryptografie metodou challenge-response.

Za největší problém celého systému lze považovat použití Raspberry Pi, které není vhodné pro produkční prostředí. Raspberry Pi používá jako systémové úložiště SD kartu, která za běžného provozu Linuxového OS nevydrží déle než několik měsíců. Celou škálu problémů může představovat bezdrátové připojení jednotek, kromě cíleného rušení je dnes v hustě obydlených místech problém bezdrátové sítě vůbec používat. Navíc bezdrátové připojení přestane dávat smysl při dálkovém napájení, kdy je nutné k jednotce přivést kabel z nejbližší technické místnosti.

3.2.2 Přístupový systém s využitím RFID karet [9]

Cílem této práce je vytvořit z dostupných komponent jednoduchý EACS v jednom objektu o 20 portálech, které jsou navzájem 2 m až 3 m vzdálené.

Jednotka je vyvinuta s podporou dvou portálů, což odpovídá požadavkům původní práce. Jejím základem je vývojový kit od NXP Semiconductors. Výběr čipu od NXP souvisí s použitím CAN jako komunikační sběrnicí mezi jednotkami a serverem. Firmaware je postaven na FreeRTOSu. Napájení je zajištěno nevyužitými páry v použitém kabelu. Jako čtečka karet je použit noname výrobek komunikující skrz rozhraní Wiegand 26. Původnímu autorovi byl jak vývojový kit, tak čtečky určeny a poskytnuty zadavatelem. Jako server funguje NoSQL databáze Redis, ve které jsou uložena veškerá data o systému. Pro zpřístupnění CAN sběrnice v OS Linux je použita knihovna SocketCAN. Ovládací aplikace je napsána v Pythonu a přistupuje přímo k Redis. V práci je jako server testováno kromě stolního PC také Raspberry Pi.

K identifikaci uživatele se používá unikátní identifikační číslo RFID karty na frekvenci 125 kHz.

Navržený systém nešifruje komunikaci mezi jednotkami a serverem. Použití neobvyklé sběrnice nelze považovat za bezpečností opatření. Pokud bude systém nasazen s Raspberry Pi jako hlavním serverem, lze navíc očekávat potíže způsobené zničenými SD kartami. Promarněnou příležitostí je omezení výběru hardwaru zadavatelem a projekt tak používá čtečku pracující s kartami, které se běžně nepoužívají. Naštěstí čtečka využívá rozhraní Wiegand 26 a je tak možné ji snadno vyměnit.

3.2.3 Inteligentní přístupový systém pro větší objekty [31]

Cílem práce je zkonstruování bezdrátového EACS pro rozsáhlé objekty s použitím WiFi mesh.

Jednotka obsluhující portál je postavena na ESP8266, což je mikrokontrolér s integrovanou WiFi. Firmware je postaven na frameworku Arduino, který staví na FreeRTOS. Čtení karet zajišťuje modul RFID-RC522. Komunikace jednotek a řídicího serveru probíhá přes WiFi mesh postavenou na knihovně painlessMESH, která nepodporuje šifrování a ani o něj nebyla doplněna. Kvůli zvolené komunikaci je systém navržen jako distribuovaný a k ukládání databáze přístupů a logů se používá programová flash paměť v modulu ESP8266. Řídicí server je naprogramován v jazyce Python. Samotné jednotky jsou ještě vybaveny HTTP serverem pro přístup k logům a konfiguraci jednotky.

Identifikace uživatele probíhá „odemčením“ šifrovaného sektoru interní paměti karty pomocí algoritmu Crypto-1. Tento algoritmus vyžaduje karty typu MIFARE Classic nebo MIFARE Plus viz [25]. Tyto karty jsou typem RFID tagu komunikujících na frekvenci 13,56 MHz.

Základním problémem je nešifrovaná komunikace mezi jednotkami a serverem. Původní autor sám uvádí, že při prolomení zabezpečení WiFi sítě je snadné se systémem manipulovat. K identifikaci se sice nevyužívají pouze UID karty, ale použitý algoritmus je prolomený [8] [21] a provést úspěšný útok na kartu je otázka několika hodin [4]. Autor tedy jeho použití považuje za poskytnutí falešného pocitu bezpečí. Crypto-1 navíc vyžaduje zápis do paměti karty, který není možné udělat u karty vydané třetí stranou a tento systém tak vyžaduje vydávání nových karet.

Dalším problémem může být přehnaná důvěra v kvalitu integrované flash paměti na modulu ESP8266, výrobce sice zaručuje 100000 zápisových cyklů, ale to se týká pouze originálních kitů. Navíc není snadné ověřit, jaký konkrétní čip byl použitý, protože je ukrytý pod RF stíněním.

3.2.4 Shrnutí

Představené práce byly úspěšně obhájeny. Navržené EACS jsou funkční. Vybraná řešení, uskutečněné kompromisy a popsané problémy ale diskvalifikují navržené systémy z nasazení v náročnějším prostředí.

3.3 Požadavky dle ČSN EN 60839-11-1

Norma ČSN EN 60839-11-1 se zabývá požadavky na komponenty EACS. V této práci slouží jako odrazový můstek pro stanovení podstatných vlastností navrženého řešení. Aby bylo možné vyjmenovat konkrétní požadavky, je potřeba určit klasifikační stupeň daného systému. Norma rozeznává 4 klasifikační stupně, které odpovídají 4 úrovním ochrany. Cílovým klasifikačním stupněm systému bude 2. stupeň. Odpovídá mu nízké až střední riziko. Hypotetický útočník je připraven investovat malé až střední prostředky. Je vybaven středními znalostmi z oblasti IT a identifikačních systémů a odpovídajícími dovednostmi. Typickými prostory v této úrovni jsou obchodní kanceláře a malé firmy.

3.3.1 Termíny a definice

ACU (řídicí jednotka kontroly vstupu) je část systému kontroly vstupu, která je propojena se čtečkami, uzamykacími zařízeními a snímači, rozhodující o poskytnutí nebo zamítnutí přístupu vstupním místem (převzato z [32])

Ovládací panel jedná se o nepovinnou část systému, která může být implementována jako hardware nebo software, který umožňuje zadávat/editovat data systému, monitorovat systém a zobrazovat výstrahy na definované události (definice sestavena autorem)

3.3.2 Požadavky na ACU

Zde uvedené požadavky jsou označené jako povinné a nebo autorem vybrané varianty požadavků, pro 2. klasifikační stupeň. Text následujících odstavců je převzat z [32].

Požadavky na rozhraní místa přístupu

1. Doba uvolnění musí být pro jednotlivé portály konfigurovatelná
2. Je-li doba uvolnění definována systémem, nesmí být povolená doba kratší než 3 s
3. Umožnění přístupu pro vstup do chráněného (kontrolovaného) prostoru
4. Umožnění přístupu pro odchod z chráněného (kontrolovaného) prostoru
5. Podmíněný přístup podle platnosti oprávnění (blokované, pozastavené, neplatné)
6. Stav/místo přístupu musí být monitorován/o
7. Doba otevření místa přístupu musí být konfigurovatelná pro jednotlivé portály
8. Musí být zpracovávány digitální vstupní signály (tj. jiné než komunikační signály) s aktivní periodou přesahující 400 ms

Požadavky na indikaci a hlášení

1. Požaduje se vizuální a/nebo akustická indikace, jestliže je povolen přístup
2. Požaduje se vizuální a/nebo akustická indikace, jestliže je přístup odmítnut

Požadavky rozpoznávání

1. Vestavěné hodiny reálného času musí mít přesnost 10 s za týden a umožňovat nastavení letního času a přestupného roku
2. U systémů s více propojenými řídicími jednotkami musí být hodiny synchronizovány s hlavními hodinami, nebo jiným spolehlivým zdrojem synchronizace nejméně jednou za 24 hodin
3. Hodiny reálného času musí být v provozu po dobu minimálně 24 hodin v případě úplné ztráty napájení (s výjimkou ztráty energie baterie pro uchovávání dat)
4. Minimálně 8 uživatelských přístupových úrovní
5. Minimálně 4 konfigurovatelné časové úseky
6. Minimální rozpoznávání pro čas v rámci přístupových úrovní zahrnující den v týdnu, hodinu a minutu denního času
7. Systém musí být schopen zvládnout 2 konfigurovatelné dny (např. státní svátky, speciální pracovní dny a dny pracovního klidu)
8. Systém musí přidělit jedinečnou identifikaci každému oprávněnému uživateli
9. Systém musí používat identifikační prostředky
10. Přístup musí být odmítnut po každém pokusu o získání přístupu s použitím identifikačního prostředku s neplatnou zapamatovanou informací a po předdefinovaném počtu neúspěšných pokusů o získání přístupu s identifikačním prostředkem s přístupovými oprávněními pozastavenými na přednastavené trvání. Počet pokusů může být konfigurovatelný. Není-li konfigurovatelný, musí být počet pokusů omezen na 5
11. V normálním provozním režimu musí systém pro identifikaci používat kompletní informaci identifikačního prostředku (kód objektu a číslo karty, nebo jedinečné číslo karty)
12. Nesmí být používány identifikační prvky se strukturou kódovacího systému viditelnou pouhým okem
13. Identifikační číslo identifikačního prostředku nemá být přímou reprezentací celého kódování

Požadavky na signalizaci nátlaku Jedná se o volitelnou funkci systému, která nebude implementována.

Požadavky na přemostění

1. Elektronický systém kontroly vstupu nesmí zamezit volný odchod povolený jinými nouzovými systémy (např. požární, environmentální)

Požadavky na komunikaci

1. Výpadek a/nebo obnovení komunikačního kanálu nesmí mít za následek uvolnění portálů.
2. Na finální instalaci musí být ověřeno, že zpoždění signálů přicházejících na ovládací panel je maximálně 90 s
3. Zařízení musí umožňovat autonomní provoz po přerušení komunikace s ovládacím panelem. Zařízení musí umožňovat provádění veškerých funkcí s výjimkou těch, které jsou ztrátou komunikace ovlivněny.
4. Bezpečnost informací musí být zajištěna prostředky zamezujícími neoprávněnému čtení a modifikaci přenášené informace.
5. Během zkoušení zařízení musí být poskytnut popis, jak je dosahováno opatření pro bezpečnost informací.

Požadavky na vlastní ochranu systému

1. Informace uložené v paměti (nastavení) musí být v případě úplné ztráty napájení (s výjimkou ztráty energie baterie pro uchovávání dat) zachována minimálně po 2 týdny
2. Po úplné ztrátě napájení je po obnovení primárního zdroje napájení požadován automatický restart systému kontroly vstupu
3. Nelze-li po automatickém restartu obnovit plnou funkčnost řídicí jednotky kontroly vstupu (došlo k poškození nebo ztrátě dat), musí být ohlášen problémový stav
4. Možnosti přístupu k vnitřním prvkům komponent systému kontroly vstupu musí vyžadovat použití nástroje
5. Otevření krytu uživatelského rozhraní určeného k instalaci vně kontrolovaného prostoru musí vést k detekci sabotáže, může-li manipulace s vnitřními prvky způsobit stav povoleného vstupu. K detekci sabotáže musí dojít dříve, než může být mechanismus detekce sabotáže vyřazen z činnosti
6. Kryty komponent EACS dosažitelné z vnějšku kontrolovaného prostoru musí splňovat požadované hodnocení IP4X a IK04
7. Administrace systému včetně konfigurace musí být logicky přístupná s použitím platného oprávnění (např. heslo, identifikační prostředek)
8. Minimální doba zachování dat pro zaznamenané události uložené v řídicí jednotce systému pro kontrolu vstupu během provozní ztráty napájení (v důsledku ztráty komunikace s ovládacím panelem) musí být 24 hodin
9. Porucha nebo obnovení komunikačního kanálu nesmí mít za následek uvolnění místa přístupu
10. Porucha komunikace s ovládacím panelem nesmí přerušit proces rozhodování o přístupu
11. Procesní pravidla uložená ve čtečce místa přístupu nesmí být pro uživatele systému viditelná
12. Validace systému vstupu dat. Systém musí poskytovat hlášení na ovládacím panelu, jestliže byla v průběhu konfiguračního režimu vložena neplatná data
13. Přístup ke konfiguračnímu režimu se musí přerušit po překročení přednastavené doby nečinnosti

Požadavky na napájení

1. Napájecí zdroj smí být umístěn v jednom nebo více komponentách elektronického systému kontroly vstupu nebo v samostatném krytu.

Požadavky na odolnost proti vlivům prostředí a elektromagnetickou kompatibilitu
Hardware, který bude v rámci této práce navržen, by měl odolat vlivům prostředí třídy I. Tato třída odpovídá vnitřnímu prostředí obytných anebo kancelářských prostor.

3.3.3 Požadavky na ovládací panel

Na ovládací panel jsou kladeny následující požadavky v oblasti indikace a hlášení, které jsou opět převzaty z [32].

1. Záznam transakce (událost korespondující s uvolněním místa přístupu následovaná identifikací uživatele)
2. Zobrazení, výstraha a záznam ztráty komunikace mezi řídicí jednotkou a ovládacím panelem
3. Zobrazení, výstraha a záznam detekované sabotáže
4. Zobrazení, výstraha a záznam pro uplynutí povolené doby otevření (příliš dlouho otevřený portál)
5. Maximální zpoždění signálů přicházejících a ovládací panel 90 s
6. Záznamová kapacita minimálního počtu zaznamenávaných systémových událostí v průměru na čtečku

3.4 Požadavky dle ČSN EN 60839-11-2

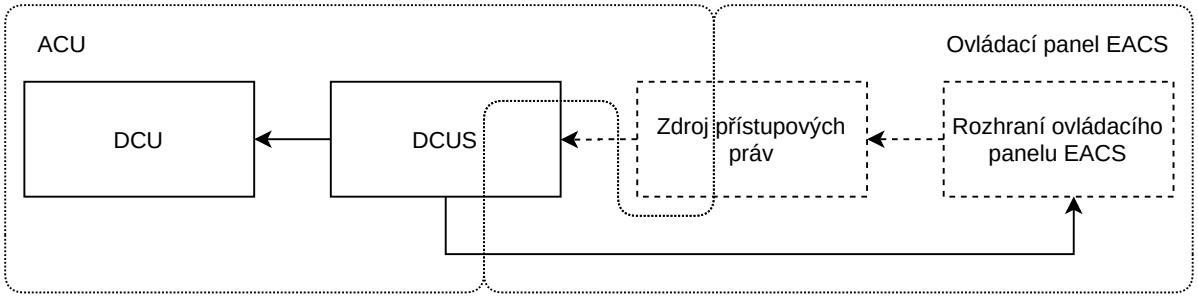
ČSN EN 60839-11-2 se věnuje požadavkům na konkrétní instalace. Cílem je poskytnout návod, jak EACS plánovat, montovat, dokumentovat a udržovat. Z hlediska návrhu vlastních komponent neobsahuje žádné požadavky, které by nebyly v ČSN EN 60839-11-1.

3.5 Koncepce

Výstupem této práce bude ACU, skládající se z:

- řídicí jednotky portálu (DCU),
- serveru řídicí jednotky portálu (DCUS).

Na Obrázku 3.1, str. 21 je znázorněna architektura výsledného EACS. Nepřerušovanou čarou jsou zakresleny komponenty a komunikační rozhraní, které jsou součástí této práce, přerušovanou čarou jsou pak vyznačeny ty, které je nutné implementovat před nasazením na konkrétní instalaci. Velmi důležitá je implementace zdroje přístupových práv. Je důležité zajistit, aby DCUS při výpadku spojení s ovládacím panelem neztratil schopnost rozhodovat o přístupech, v opačném případě bude porušen požadavek z ČSN EN 60839-11-1, viz str. 19.



Obrázek 3.1: Architektura EACS

V následujících odstavcích je diskutován technologický rámec řešení požadavků kladených na komponenty systému. Konkrétní implementace bude řešena v následujících kapitolách.

3.5.1 Požadavky a technologie pro DCU

Šifrovaná komunikace s DCUS V dnešní době je jednou z nejpoužívanějších technologií šifrování komunikace protokol TLS. Od srpna 2018 je už k dispozici RFC TLS 1.3 [26], přesto podle Mozzila.org není problém používat TLS 1.2 s vhodně zvolenými šifrovacími algoritmy [5]. Protokol TLS je z pohledu vývojáře aplikací transparentní, nehrozí tedy, že by autor této práce mohl nesprávnou implementací ohrozit jeho fungování. Navíc je postaven nad transportním protokolem TCP, který zajistí, že jsou data přenášena spolehlivě. Další vhodnou vlastností je možnost ověřování klientů jejich vlastními certifikáty.

Protokol TLS vytváří transparentní komunikační tunel, nad kterým je dále možné provozovat různé protokoly aplikační vrstvy. Pro jednoduchou aplikaci, jako je DCU, by dokonce mohl být tunel použitý pro přenos informací v binární podobě. Z pohledu jednoduché implementace jak DCU, tak DCUS je ovšem vhodné zvolit protokol HTTP. Přes jeho stáří je široce podporován v různých frameworcích a jsou pro něj dostupné hotové aplikační servery.

Dálkové napájení Aby nebylo snadné vyřadit jednotku z provozu prostým vytažením napájecího zdroje ze zásuvky, je vhodné umístit zdroj do jiné místnosti v rámci chráněného prostoru. Jednotku by mělo být možné napájet na vzdálenost alespoň 50 m.

Detekce sabotáže Pro detekci sabotáže bude implementována standardní sabotážní smyčka, která bude v normálním stavu pod napětím a její přerušení bude registrováno jako sabotáž.

Napájení aktivátoru místa přístupu Elektrické zámky jsou běžně napájeny stejnosměrným napětím 6 V, 12 V a 24 V s obvyklou tolerancí 10 % [27]. Pro zajištění dostatečného napětí je tedy lepší nevyužívat přímo dálkové napájení, ale z něj odvozené nižší napětí. Z tohoto důvodu je vhodné zvolit 12 V. Pro 12 V jsou také obvykle nabízeny varianty zámků se sníženým proudovým odběrem, který nepřesahuje 300 mA [27].

Ovládání aktivátoru místa přístupu Aby byl výstup dostatečně univerzální, je nejvhodnější zvolit relé v uspořádání SPDT, tedy přepínače. Relé jsou dimenzována pro spínání dostatečně velkých proudů, aby bylo možné používat všechny typy elektrických zámků, navíc díky zvolenému uspořádání kontaktů není problém připojit jak zámky trvale napájené (fail-safe), tak zámky spínané (fail-secure). To je největší přínos oproti výkonovým tranzistorům, které musí být udržovány sepnuté a musí se tak měnit ovládací logika v závislosti na typu zámku.

Monitorování stavu portálu K naplnění požadavku postačuje běžně používaný jazýčkový magnetický senzor (viz [11]). Na dveře se umístí magnet a na zárubeň samotný senzor. Díky šířce zárubně by nemělo být možné sepnout kontakt zvnějšku chráněného prostoru.

Identifikace uživatele K identifikaci uživatele bude použito UID NFC karty, tzn. karet kompatibilních s ISO/IEC 14443-3-A. Tento způsob identifikace je snadno napadnutelný skrz zkopírování UID a je v rozporu s požadavky dle ČSN EN 60839-11-1 (viz str. 18). Přesto je autor přesvědčen, že má smysl jej použít. Především není nutné vydávat vlastní karty, což může v rozsáhlých instalacích představovat značné finanční prostředky. Díky tomu, že není nutné nijak zasahovat do paměti karty, je možné použít karty vydané třetí stranou.

Připojení čteček DCU musí umět obsluhovat 2 čtečky, aby bylo možné autentizovat uživatele jak při příchodu, tak při odchodu. Požadavky na rozhraní se budou odvíjet od zvolené čtečky.

Tlačítko pro odchod Místo jedné ze čteček musí být možné připojit tlačítko pro vyžádání odchodu.

Záznam událostí včetně platného časového razítka Pro získání časového razítka události se bude používat obvod reálného času zálohovaný lithiovým článkem, bude tak zajišťovaný přesný čas i po delším výpadku primárního napájení DCU. Záznamy o událostech se budou ukládat na vhodnou nevolatilní paměť. Události, které je nutné zaznamenávat:

1. Start systému
2. Odemčení dveří
3. Uzamčení dveří
4. Otevření dveří
5. Uzavření dveří
6. Překročení povolené doby otevření dveří
7. Otevření bez odemčení
8. Navázání spojení s DCUS
9. Ztráta spojení s DCUS

3.5.2 Požadavky a technologie pro DCUS

Šifrovaná komunikace s DCU Požadavky byly stanoveny v části věnující se DCU, viz str. 21.

Monitorování stavu DCU DCU bude v pravidelných intervalech (15 s) oznamovat DCUS, že je připojena. DCUS potom bude mít nastavenou maximální dobu, po kterou se DCU nemusí ohlásit (krátkodobý výpadek napájení, výpadek síťové komunikace, restart apod.)

Šifrovaná komunikace se zdrojem přístupových práv Tato část DCUS je ponechána k implementaci pro konkrétní instalaci. Ideální bude napojit DCUS buď na nějaké REST API, LDAP, nebo jinou databázi uživatelů. Zabezpečení přenosu dat tu lze řešit buď přímo podporou TLS v protokolu (HTTPS pro REST API, LDAPS), nebo šifrovaným tunelem např. pomocí SSH, které také používá TLS.

Odesílání e-mailů s výstrahou na události v EACS Odesílání e-mailů může být náhradou za zobrazování výstrah na ovládacím panelu dle požadavků na str. 20.

Ukládání záznamů událostí z DCU Je nutné zvolit vhodnou metodu ukládání záznamů o událostech, jejich rozdělení a vyřešit případnou archivaci.

Volání předem nakonfigurovaných HTTPS endpointů Tato funkce má usnadnit propojení s dalšími systémy. Díky tomu by mělo být možné zjišťovat obsazenost místností, četnost jejich využívání apod.

Kapitola 4

Praktická část

4.1 HW DCU

Nejprve budou diskutovány konkrétní technologie a integrované obvody, které se hodí pro naplnění požadavků, potom bude představen návrh desky plošných spojů.

4.1.1 Komunikace s DCU

Nevýhodou vybraných protokolů TLS a HTTP je, že zvyšují režii komunikace a je tak potřeba hledat vhodnou komunikační technologii, která bude poskytovat dostatečnou propustnost. Vzhledem k požadavku na dálkové napájení je vhodné omezit se na technologie využívající fyzické médium dovolující vést napájecí vodiče společně s těmi signálovými v jednom kabelu. Za těchto požadavků se jeví jako nejvhodnější technologie Ethernet. Jedná se o soubor technologií standardizovaných jako IEEE 802.3 [10]. Pro tento konkrétní případ je nejvhodnější zvolit variantu 100BASE-TX, která využívá 2 páry kroucené dvojlinky (Cat5 a lepší) pro duplexní přenos dat až na 100 m.

4.1.2 Čtečka karet

Z nevelké nabídky byla především kvůli ceně a možnosti objednání u TME.eu vybrána čtečka RS-H0-06 BZ od společnosti Drexia. Čtečka má integrovanou dvoubarevnou LED (červená a zelená) a bzučák, které se ovládají připojením příslušného vodiče na GND. Podporovány jsou různé typy karet s UID do 12 byte, které je posíláno přes rozhraní RS-232 jako řetězec HEXa znaků. Její nevýhodou je, že nepodporuje obousměrnou komunikaci s kartou a není ji tak možné využít pro složitější metody identifikace. Napájena je 12 V a její maximální proudový odběr je 160 mA [12].

4.1.3 Mikrokontrolér

DCU potřebuje mikrokontrolér, který podporuje Ethernet, zvládne komunikovat pomocí HTTPS, bude dostupný a poměr ceny a výkonu bude příznivý. Nakonec byl vybrán mikrokontrolér ESP32 od Espressifu. Oproti druhé zvažované variantě, mikrokontrolérech od STMicroelectronics, má dvě 32bitová jádra, HW akceleraci šifrovacích algoritmů a stojí jednu třetinu podobně vybavené varianty od STMicroelectronics. Navíc ESP32 díky integrované WiFi a Bluetooth poskytuje prostor pro další rozvoj projektu.

4.1.4 Napájení

Dálkové napájení u Ethernetu je definováno ve standardu 802.3af/at (dnes už také 802.3bt). Napájecí napětí je z rozsahu 44 V až 52 V. Maximální proud pro 802.3af je 350 mA a pro 802.3at pak 600 mA. Standard rozeznává 3 módy napájení:

Mode-A výkon je dodáván po komunikační dvojici párů pomocí středových vývodů signálových transformátorů

Mode-B výkon je dodáván skrz nevyužitou dvojici párů (platí pro standard 100BASE-TX a 10BASE-T)

4-pair výkon je dodáván po 4 komunikačních párech skrz středové vývody signálových transformátorů (standard 1000BASE-T a vyšší)

Výběr módu je na napájecím zdroji, se kterým si musí napájené zařízení vyjednat maximální dodávaný výkon (o vyjednávání se stará tzv. Powered Device controller). Napájené zařízení musí podporovat jak Mode-A, tak Mode-B, jinak není v souladu se standardem.

Pro napájení pomocí Mode-B ještě existuje nestandardní tzv. pasivní PoE, kdy je na nevyužité páry přímo přivedeno napájecí napětí a zařízení nemusí nijak komunikovat se zdrojem. Tento způsob poskytování napájení může být nebezpečný pro zařízení, která na něj nejsou konstruována. Vzhledem k neexistujícímu standardu je možné volit napájecí napětí dle potřeb aplikace, obvykle se používá 12 V, 24 V nebo 48 V.

Aktuální verze HW DCU používá pasivní PoE s napětím 24 V a maximálním proudem 500 mA. Z výpočtu potřebného dodávaného výkonu, který je uveden níže, plyne, že zvolená varianta nemůže pokrýt spotřebu celého zařízení a bude ji nutné v další verzi HW změnit. Původní výpočet příkonu bohužel autor ztratil a není tak možné provést diskuzi nad tím, kde byla udělána chyba.

	U [V]	I [mA]	P [W]
Čtečka vnější	12	200	2.4
Čtečka vnitřní	12	200	2.4
Relé	12	33	0.396
Elektrický zámek	12	350	4.2
Ostatní elektronika	3,3	750	2.475

Tabulka 4.1: Příkon součástek DCU

Aby bylo možné určit příkon zařízení, tedy výkon dostupný na vstupu prvního měniče, je potřeba zjistit, jaký příkon mají jednotlivé části DCU, to je shrnuto v tabulce 4.1.4, str. 25. Dalším parametrem, který do výpočtu vstupuje, je topologie zapojení DC-DC měničů. Na DCU jsou dva DC-DC měniče zapojené v sérii. První má na vstupu napájecí napětí z PoE a poskytuje 12 V pro napájení relé, aktivátoru portálu a druhého DC-DC měniče. Ten vstupní napětí dále sníží na 3,3V a z této větve je pak napájena elektronika, tzn. mikrokontrolér a jeho periferie. Protože jsou DC-DC měniče v sérii a nemají 100% účinnost, nelze určit celkový příkon zařízení prostým součtem. Pro následující výpočty bude uvažována účinnost DC-DC měničů 75 %. Celkový odebíraný výkon z 3,3V větve je 2,5 W. DC-DC měnič z 12 V na 3,3 V bude z 12V větve odebírat $2{,}5\,\mathrm{W} \times 1{,}33 \approx 3{,}4\,\mathrm{W}$. Celkový odebíraný výkon z 12V větve je součet příkonu všech spotřebičů a příkonu DC-DC měniče z 12 V na 3,3 V, tedy $9{,}4\,\mathrm{W} + 3{,}4 = 12{,}8\,\mathrm{W}$. DC-DC měnič na 12 V bude mít příkon $12{,}8\,\mathrm{W} \times 1{,}33 \approx 17\,\mathrm{W}$.

Vzhledem k maximálnímu příkonu 17 W a minimální vzdálenosti, na kterou je zařízení napájeno, je potřeba použít PoE dle standardu 802.3at nebo pasivní PoE s napětím 48 V. Implementace PoE dle standardu 802.3at sice vyžaduje použití dalšího čipu, ale přínos v podobě široké kompatibility, stojí za to a proto bude v příští verzi HW použité PoE dle 802.3at. Jako Powered Device controller bude použitý čip TPS2376 od společnosti Texas Instruments.

4.1.5 Konstrukce desky plošných spojů

Základním omezením pro návrh DPS jsou její rozměry, z ekonomických a také praktických důvodů byl stanoven maximální rozměr na 10×10 cm. Další omezení vyplývají z potřeby osazovat desky ručně. Především je nutné volit dostatečně velká pouzdra pasivních součástek (nejméně 0603 dle EIA) a SMD pouzdra integrovaných obvodů, která mají vývody. Z čistě ekonomického hlediska je nutné se omezit na 2 vrstvy. Použití vícevrstvého DPS by zjednodušilo práci s napájením, ale bez metody řízené impedance by nepřineslo žádné další výhody. Veškerá schémata a motiv DPS jsou součástí přílohy této práce, viz „Podklady pro DPS".

Deska plošných spojů má pět dále podrobněji popsaných částí.

Konektor RJ-45

V této části se nachází jen nejnutnější součástky pro fungování Ethernetu, jako jsou rezistory na symetrických párech a rezistory pro LED v konektoru. Při návrhu byla dodržena doporučení z SMSC Ethernet Physical Layer Layout Guidelines [29]. Především se jedná o minimální vzdálenosti mezi jednotlivými komponentami. Použitý konektor RJ-45 (8P8C) ARJM11C7-114-BA-EW2 má integrované magnetikum a umožňuje přímé vyvedení napájecího napětí z pinů konektoru. Zapojení odpovídá standardu 802.3af Mode-B, tedy piny 4 a 5 jsou připojeny k VCC a piny 7 a 8 k GND.

Bohužel kvůli špatně provedenému výpočtu dimenzování napájení ve fázi návrhu prototypu je aktuálně použitý konektor nevhodný. Není konstruovaný na dostatečně velké proudy jednotlivými páry. V další verzi HW bude použitý vhodný konektor ARJM11C7-104-AB-EW2. Jeho nevýhodou jsou chybějící pasivní součástky na středních vývodech signálových transformátorů [3], které bude nutné doplnit externě.

Měniče DC-DC

Jedná se o dva v sérii zapojené měniče, jejichž základem je čip TPS54331 od Texas Instruments, jejich konstrukce nezajišťuje galvanické oddělení od vstupu. První měnič konvertuje vstupní napětí 24 V na 12 V, které se používá pro napájení aktivátoru místa přístupu. Druhý měnič má výstupní napětí 3,3 V a slouží k napájení mikrokontroléru a jeho periferií. Pro návrh měničů byl použit online nástroj WEBENCH POWER DESIGNER od společnosti Texas Instruments.

Během vývoje prototypu došlo k chybě ve výpočtu dimenzování napájení, důsledkem je špatně zvolené napájecí napětí a také první DC-DC měnič. V další verzi HW bude TPS54331 nahrazen TPS54560, který umožní přejít na napájecí napětí 48 V. Prototyp také nemá implementovanou žádnou formu ochrany proti přepólování, zkratu a přepětí. V další verzi HW bude přidán dvoucestný usměrňovač, za něj vratná pojistka s pracovním napětím 60 V a maximálním proudem 2 A, potom jednosměrný transil s prahovým napětím 58 V [7].

Externí IO

Tento blok se stará o ovládání aktivátoru portálu, sledování stavu portálu, komunikaci se čtečkami, sabotážní smyčku, tlačítko pro odchod a nekomunikační vstup dle ČSN EN 60839-11-1.

Aktivátor portálu je spínán relé v konfiguraci SPDT. Protože je většina aktivátorů induktivní zátěž (elektromagnet, soleniod), je každý spínaný kontakt vybaven antiparalelní diodou kvůli potlačení napěťových špiček při rozpínání. Stejně tak je antiparalelní diodou vybavena spínací cívka relé. Ke sledování stavu sepnutí relé je k normálně odpojenému kontaktu připojen optočlen, jehož výstup je přiveden do mikrokontroléru.

Ke sledování stavu portálu je připraven vstup oddělený optočlenem. K dispozici je kromě samotné vstupní svorky také napájení 12 V.

Komunikace se čtečkou je rozdělena do dvou bloků. Ovládání LED a bzučáku je řešeno MOSFETy. Kvůli nedostatku pinů mikrokontroléru jsou tyto funkce ovládány z GPIO expandéru,

který komunikuje po I2C. Komunikační linka ze čtečky je izolována pomocí optočlenu. Toto řešení se ovšem ukázalo jako nefunkční, optočlen nedokáže reagovat na rychlé změny a bude v další verzi HW nahrazen speciálním optočlenem pro komunikační linky.

Sabotážní smyčka je v aktuální verzi HW řešena špatně, kdy je přímo na svorku vyveden jeden z GPIO pinů mikrokontroléru. V další verzi bude tento vstup izolován pomocí optočlenu.

Tlačítko pro vstup není aktuálně možné připojit, protože vstup ze čtečky není oddělený od pinu mikrokontroléru a tlačítko může pracovat jen na napětí, které je dostupné pro napájení čtečky.

Aktuální verze HW opomíjí normou vyžadovaný digitální nekomunikační vstup. Bude přidán v příští verzi HW a stejně jako ostatní vstupy bude izolován pomocí optočlenu.

Periferie mikrokontroléru

Nejdůležitější periferií je PHY LAN8020 od Microchipu. Jedná se o velmi populární 100 Mbps PHY, které je podporované v ESP-IDF. Jediným problémem je QFN pouzdro, které se špatně osazuje běžnou hrotovou pájecí stanicí. Ke komunikaci s mikrokontrolérem slouží dvě rozhraní - Reduced Media Independent Interface a Serial Management Interface. Jako zdroj taktovacího signálu 50 MHz se používá fázový závěs v ESP32. PHY je pak spojeno dvojicí diferenciálních párů s konektorem RJ-45 s vestavěným magnetikem.

Dalším obvodem jsou hodiny reálného času, čip MCP7940N od Microchipu. Hodiny komunikují po sběrnici I2C. Jako zdroj hodinového signálu se používá krystal se standardní rezonanční frekvencí 32,768 kHz. Hlavním důvodem použití samostatného hodinového obvodu je možnost zálohovat jeho chod pomocí lithiového článku, díky zálohování je možné udržet si přesný čas po dlouhých výpadcích napájecího napětí.

Posledním periferním obvodem je EEPROM M24512 od STMicroelectronics. Paměť komunikuje po I2C. Má vestavěnou funkci ECC operující nad čtveřicemi bytů. Je organizována do 512 stránek, každá po 128 bytech. Podporuje jak zápis po jednotlivých bytech, tak i dávkově v rámci jedné stránky.

Vývojová deska s ESP32

Konkrétně se jedná o ESP32-DevKitC V4 s osazeným modulem ESP32-WROOM-32D vyráběný přímo Espressifem. Deska ještě integruje napěťový regulátor 5 V na 3,3 V (není použitý) a převodník UART na USB CP2102N od Silicon Labs. Použití už hotové vývojové desky poskytuje množství výhod. Není nutné navrhovat vlastní anténu pro případ, že by našla bezdrátová komunikace v projektu využití, není taky nutné osazovat samotné ESP32 ani jeho externí flash paměť a navrhovat doplňkové obvody, které jsou nutné pro správnou funkci mikrokontroléru.

4.2 FW pro DCU

FW je postaven nad vývojovým frameworkem ESP-IDF. Jedná se o Open-Source projekt podporovaný výrobcem mikrokontroléru založený na FreeRTOS. Jeho součástí jsou jak ovladače všech interních periferií, tak vybraných externích periferií, a navíc jsou k dispozici implementace mnoha oblíbených komunikačních protokolů. Součástí frameworku je také toolchain, který používá kompilátor GCC od společnosti Xtensa a několik utilit napsaných v Pythonu. Pro automatizaci kompilace se používá CMake, díky kterému je snadné rozdělit kód do mnoha jednotlivých komponent a zpřehlednit tak celý projekt.

Firmware se skládá z 9 komponent, které budou dále představeny.

4.2.1 Komponenta butils

V této komponentě jsou shromážděny často se opakující části kódu, které se používají ve více komponentách. Především se tu nachází wrappery na funkci strtol a strtoll, které poskytují pohodlné rozhraní pro práci s chybou převodu. K dispozici je ještě implementace funkce na přečtení celého těla odpovědi HTTP serveru a funkce k parsování JSON odpovědi.

4.2.2 Komponenta card_reader

Tato komponenta obsluhuje čtečky a dveře. Je rozdělena do několika souborů podle jednotlivých funkcí.

card_reader.c

Zde se nachází většina logiky obsluhy dveří a také main funkce pro CARD_READER task. Ta je spuštěna každých 100 ms. V každém běhu se zkontroluje stav dveří, jestli není přečtena karta a nakonec se provede obsluha signalizace na čtečkách. Pokud je k dispozici UID přečtené karty, tak je skrz komponentu server_link odesláno na DCUS k ověření, následně se vyhodnotí odpověď serveru a na jejím základě se odemknou dveře. Pokud karta nemá povolený vstup, tak ji DCU na serveru neověří dříve než za 2 s. Pokud jsou odemčeny dveře, dojde k záznamu příslušné události pomocí komponenty dcu_log.

V další verzi FW přibude dynamická cache přístupů, kdy si DCU uloží 20 posledních ověřených karet a v případě výpadku spojení se serverem umožní na tyto karty vstup po předem definovanou dobu. Dále bude přidáno místo na 10 karet pro nouzový přístup, jim bude umožněn vstup vždy.

door.c

Zde je implementován stavový automat dveří, který přechází mezi stavy LOCKED, UNLOCKED, OPEN, OPEN_AFTER_TIMEOUT. Do stavu UNLOCKED je možné přejít jen zavoláním funkce door_unlock, mezi ostatními stavy dochází k přechodu v rámci kontroly dveří volané z hlavní funkce tasku každých 100 ms. Kromě stavu portálu se sleduje také stav relé pomocí vstupu, který je aktivní, pokud je relé nesepnuté. V případě, že nesouhlasí aktuální stav relé s nastaveným stavem, je vyhlášen poplach. Poplach je také vyhlášen v případě, kdy je zaznamenáno otevření dveří ve stavu LOCKED nebo při dlouhotrvajícím stavu OPEN.

Tento stavový automat je nutné ještě upravit, aby byl plně v souladu s požadavky v ČSN EN 60389-11-1, kde je uveden diagram časování uvolnění portálu (viz. Obrázek B.1, str. 55). Aktuální implementace totiž nerozlišuje čas uvolnění (Doba, po kterou je portál odemčený.) a dobu pro ponechání otevřeného portálu (V této době dveře nelze otevřít, ale mohou zůstat otevřené.). V souvislosti s touto změnou dojde také k úpravě komunikace s DCUS, aby bylo možné obě tyto doby konfigurovat na serveru.

signalisation.c

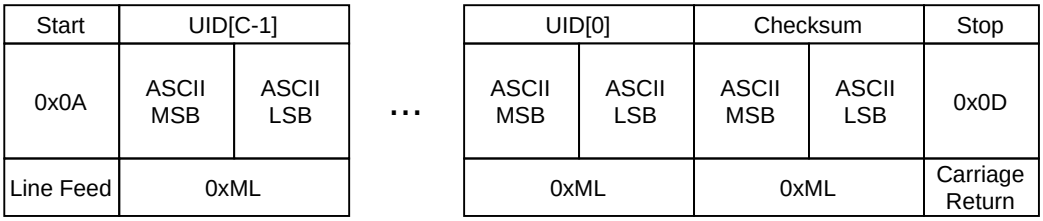
V tomto souboru je implementováno ovládání LED a bzučáku jednotlivých čteček. Protože tyto signalizační prvky jsou připojeny k GPIO expandéru, tak se pro jejich ovládání využívají funkce z komponenty hw/gpioe. Součástí je krátká rutinně spouštěná funkce, která zajišťuje blikání a hlídá maximální délku trvání indikace neplatné karty.

Do budoucna je potřeba přidat další druhy signalizace. Aktuálně chybí varování před koncem povolené doby otevření portálu a signalizace výpadku komunikace s DCUS.

uart_decode.c

Jedná se o implementaci dalšího stavového automatu, jeho jádrem jsou 2 HW periferie UART. Použitá je jen RX část, TX je odpojena na úrovni IO matice mikrokontroléru.

Čtečka posílá UID jako hexstring, kdy každý byte je jeden ASCII znak reprezentující číslici v šestnáctkové soustavě, viz Obrázek 4.1, str. 29. Poslední 2 byty před Stop bytem jsou kontrolní součet ve stejném formátu jako byty UID. Kontrolní součet je spočítán jako XOR bytů UID.



Obrázek 4.1: Formát dat přijímaných ze čtečky, kde C je délka UID karty

V main funkci tasku je volána funkce, která se pokouší vybrat data z FIFO bufferu driveru UART. Pokud jsou nějaká data vyčtena, tak se v nich hledá Start byte sekvence, pokud je nalezen, tak se buffer dál parsuje. Cílem je získat string a zkontrolovat kontrolní součet.

4.2.3 clock

Komponenta poskytuje UNIXový čas pro celý systém (tzn. UTC) ve formě 64bitového integeru. Čas je odměřován pomocí přerušení interního časovače. Je také zajištěna synchronizace s externím RTC, které slouží pro získání přesného času po restartu systému. Pro přístup k RTC se používá komponenta hw/rtc. K dispozici je ještě funkce pro synchronizaci s časem DCUS. Synchronizace probíhá při velkém rozdílu (více jak 10 s), při startu systému nebo v pravidelném intervalu 4 h.

Zatím chybí pravidelná synchronizace interního času s RTC, pro případ, že DCU bude dlouho bez spojení s DCUS.

4.2.4 config_menu

Úkolem komponenty je pomocí UART komunikovat s uživatelem a umožnit mu nastavit základní parametry DCU. Aktuálně jsou k dispozici tyto parametry:

- DHCP
- IP adresa DCU
- IP adresa GW
- Maska sítě
- URL DCUS
- Povolení bzučáku pro alarm dlouho otevřených dveří
- Povolená doba otevření portálu po uplynutí intervalu odemčení

Veškerá interakce s uživatelem je soustředěna do main funkce samostatného tasku CONFIG_MENU. Do konfiguračního režimu se přejde stiskem klávesy enter, čímž dojde k vypsání aktuální konfigurace. Dál se program ptá na nové hodnoty jednotlivých parametrů, pokud uživatel nezadá žádnou odpověď, tak se ponechá aktuální hodnota. Na závěr je vypsána upravená

konfigurace a je možné ji buď uložit, nebo zahodit. Potom je uživatel vyzván k restartování DCU.

Do další verze je nutné přidat ochranu konfigurace heslem, které se uloží jako hash do SPIFFSu a dobu, po které se konfigurace automaticky přeruší. S úpravami stavového automatu dveří (viz str. 28) a přidáním dalších možností ověření uživatele (viz str. 28), se budou měnit konfigurovatelné parametry a s nimi konfigurační menu.

4.2.5 dcu_log

Komponenta zajišťuje záznam událostí, které jsou buď odeslány na DCUS skrz komponentu server_link, nebo uloženy do EEPROM pomocí hw/eeprom. Kvůli přehlednosti zdrojového kódu je rozdělena do více souborů.

dcu_log.c

Zde je implementována hlavní část celé logiky záznamu událostí. Je zde umístěna main funkce tasku DCU_LOG, ve kterém se z RTOS Queue vybírají události k zaznamenání. Queue byla zvolena proto, aby záznam událostí neblokoval jiné tasky v rámci DCU. DCU rozlišuje následující události:

0x01 Start DCU

0x02 Ztráta spojení s DCUS

0x03 Obnovení spojení s DUCS

0x04 Odemčení dveří

0x05 Otevření dveří

0x08 Přerušení tampering smyčky

0x09 Uzamčení dveří

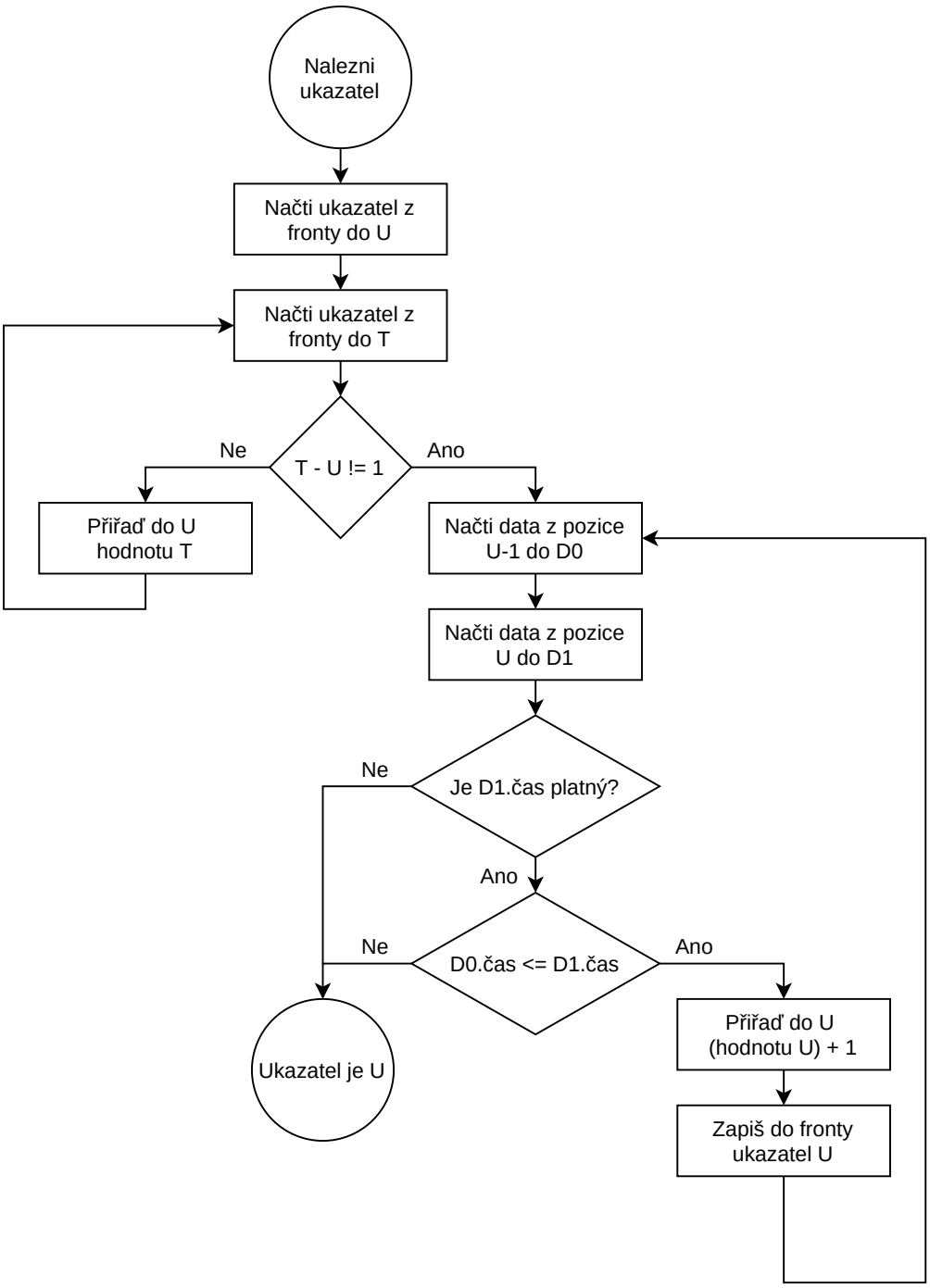
Dále se rozhoduje, jak bude událost zaznamenána. K dispozici je odeslání na DCUS skrz komponentu server_link nebo záznam do EEPROM pomocí eeprom_log.c. Pokud je spojení s DCUS aktivní, tak se často vyskytující události (odemčení dveří, otevření dveří a uzamčení dveří) odesílají jen na DUCS, pokud je DCUS nedostupný nebo neodpoví na zaslaný požadavek, tak jsou tyto události ukládány do EEPROM. Ostatní události jsou vždy odeslány na DCUS a uloženy do EEPROM. Cílem tohoto mechanismu je snížit zátěž EEPROM, která má jen omezený počet zápisových cyklů.

S úpravou stavového automatu dveří (viz str. 28) a přidáním dalších možností ověření uživatele (viz str. 28) dojde k úpravě seznamu zaznamenávaných událostí.

eeprom_log.c

Záznam událostí do EEPROM je realizován binárně, proto je hlavní částí převod stringu UID karty do binární podoby. Čas a číslo události už jsou binární čísla a stačí je pouze zapsat. Další důležitou funkcí je snížení opotřebení EEPROM, a tedy prodloužení její životnosti. Za tímto účelem byla implementována upravená metoda dvou cyklických front viz [6]. Datová fronta má délku 3000 záznamů a fronta ukazatelů má délku 10 záznamů. Nejprve se uloží data a pak se uloží ukazatel na příští pozici v datové frontě. Po startu DCU se projde krátká fronta ukazatelů a hledá se v ní poslední ukazatel (viz Obrázek 4.2, str. 31). Poslední platný ukazatel se hledá podle nespojitosti v rostoucí řadě. Tam, kde se ukazatelé liší o více než 1, se nachází poslední uložený ukazatel. Pro případ, že DCU bylo resetováno před zapsáním ukazatele, se zkontroluje, jestli

na sebe navazují časová razítka posledního a následujícího záznamu. Pokud razítka navazují, je ukazatel na příští pozici v datové frontě posunut a také je zapsán do EEPROM, aby se udržela rostoucí posloupnost. Postup se opakuje, dokud razítko příštího záznamu není starší nebo neplatné. Tento algoritmus zaručí, že nebudou přepisována aktuální data.



Obrázek 4.2: Algoritmus hledání ukazatele na příští datový záznam po startu DCU

4.2.6 heartbeat

Zde je implementováno pravidelné ohlašování DCU DCUS. S pomocí času z komponenty clock se každých 15 s skrz komponentu server_link odešle na DCUS zpráva, že DCU žije. DCUS zpět posílá aktuální čas serveru a ten se pak předává komponentě clock pro případnou synchronizaci.

4.2.7 hw

Do této komponenty jsou soustředěny ovladače externích periferií mikrokontroléru. Každý ovladač je ve vlastním souboru, a protože externí periferie komunikují po I2C, tak je tu ještě ovladač interní periferie I2C.

dcu_i2c.c

Zde se nachází jen inicializace I2C periferie.

eeprom.c

Implementace ovladače EEPROM vychází z možností, které poskytuje vybraná paměť M24512. Pro čtení a zápis jsou nejmenší rozlišovanou jednotkou skupiny 4 bytů. Důvodem je interní ECC logika, která pracuje se stejnou skupinou. Zápis je navíc možné provádět dávkově jen v rámci jedné stránky, takže je nutné kontrolovat splnění této podmínky, v opačném případě by byla přepisována data na začátku stránky [30]. Zápis trvá až 5 ms a během něj paměť neposílá ACK na svoji adresu. Číst už je možné bez ohledu na stránky.

gpioe.c

Rozhraní pro práci s GPIO expandérem [23] se blíží běžné práci s registry. Vzhledem k využívaným funkcím jsou zprostředkované 16bitové registry GPIO (ovládá výstup) a IODIR (určuje typ pinu - vstupní/výstupní). Pro každý registr se udržuje místní kopie v proměnné, která odpovídá stavu registru v expandéru. Registry jsou pouze zapisovány, čtení není třeba, protože po každém úspěšném zápisu se aktualizuje místní kopie.

rtc.c

Ovladač externího obvodu reálného času slouží k obousměrné synchronizaci času v rámci DCU. Při zápisu času do RTC je na vstupu unixový čas z komponenty clock, který se pomocí standardní knihovny time převede na jednotlivé komponenty, které se následně vyjádří pomocí BCD kódu a rozdělí do bytů tak, aby je bylo možné zapsat do SRAM v RTC. Při čtení času z RTC se použije opačný postup, z RTC jsou vyčteny jednotlivé části data v BCD kódu, ze kterých se po převodu poskládá struktura `tm`, a ta je pak pomocí knihovny `time` převedena na 64bitový integer. [24]

4.2.8 server_link

Server_link je implementací rozhraní pro komunikaci s DCU. Využívá komponenty http_client z ESP-IDF. Vystavuje funkce, které lze volat z ostatních komponent, stará se o opakované pokusy o odeslání požadavku, přechod mezi stavy DCUS dostupný/nedostupný a parametrizaci http klienta.

DCU po startu začíná ve stavu, kdy neví, jestli je DCUS dostupný. Pokud se podaří připojit, tak je DCUS prohlášený za dostupný. Do stavu DCUS nedostupný je možné se dostat z každé funkce, která posílá požadavek na DCUS, a to po selhání 3 pokusů o připojení. O znovu připojení se DCU pokouší jen v rámci odesílání heartbeatu a pro přechod zpět do stavu DCUS dostupný stačí, aby prošel 1 požadavek.

Přestože má ESP32 integrovaný HW akcelerátor šifrovacích algoritmů, trvá TLS handshake přibližně 2 s. Tato doba je příliš dlouhá, obzvlášť pro uživatele čekajícího na ověření karty. Proto se při komunikaci s DCUS využívá tzv. keep-alive, kdy se udržuje navázané TCP spojení se serverem i potom, co skončil přenos aktuální HTTP zprávy. TLS handshake se tak dělá jen jednou za 4,5 min, a to hned po příjmu poslední odpovědi. Tato opatření by měla vést k minimalizaci počtu případů, kdy nebude uživatel identifikován okamžitě.

V příští verzi FW budou přesunuty certifikáty do SPIFFSu a bude je tak možné nahrát nezávisle na FW.

4.2.9 system_config

Pro fungování DCU je nutné implementovat konfiguraci, kde budou uloženy důležité parametry a kterou bude možné uložit a znovu načíst po startu DCU. Konfigurace je uložena ve struktuře, která se pomocí funkcí dá uložit v binární podobě do SPIFFSu, nebo z něj načíst. K dispozici jsou ještě funkce převádějící string na jednotlivé položky v konfiguraci, jako je IP adresa DCU nebo IP adresa DNS serverů.

4.2.10 main.c

Zde se inicializují všechny komponenty okolo sítě, tzn. MAC a PHY Ethernetu. Také se tu inicializují všechny komponenty FW a aplikuje systémová konfigurace.

4.2.11 Chybějící požadované funkce

Detekce sabotáže Vzhledem k vadné HW implementaci sabotážní smyčky a nedostatku času zatím není implementována detekce sabotáže a nemohou tedy ani fungovat na ní závislé funkce a výstrahy. Přidat detekci sabotáže je prioritou v rámci další verze FW.

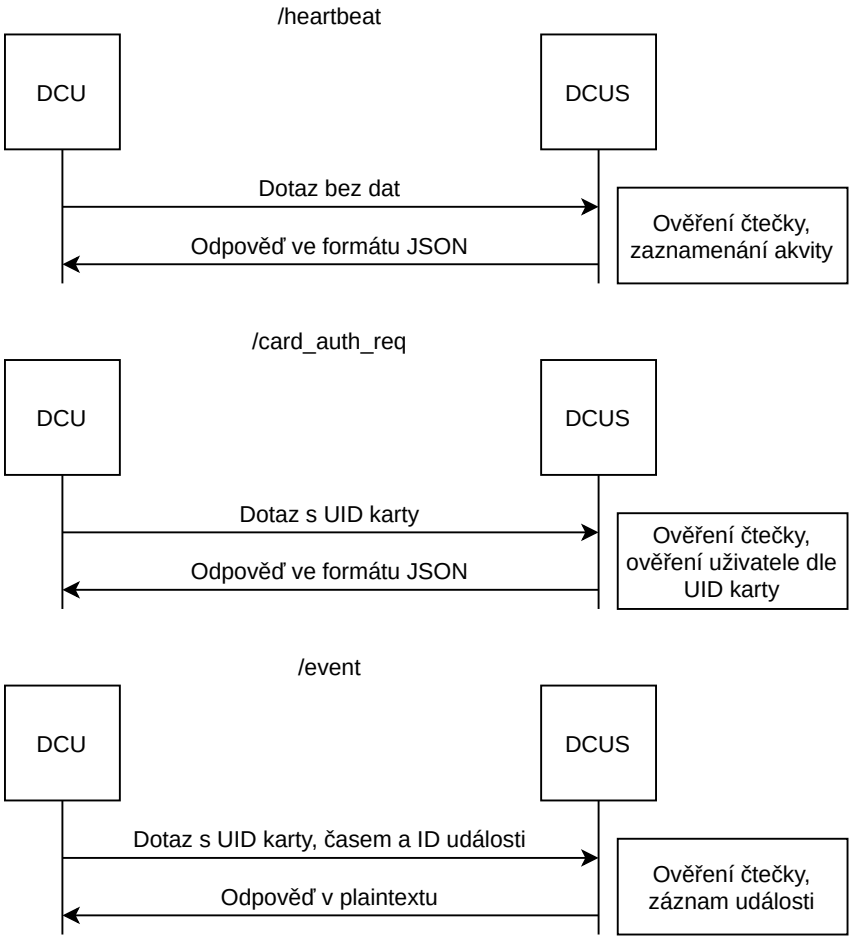
Tlačítko pro odchod Opět nebylo kvůli chybě v HW implementaci dále řešeno. K jeho zprovoznění v FW bude potřeba nahradit inicializaci jedné UART periferie prostým přerušením reagujícím na vhodnou hranu signálu doplněné o filtr zákmitů.

4.3 Komunikační protokol

Pro komunikaci mezi DCU a DUCS se používá REST API [22]. DCUS vystavuje 4 endpointy (viz Tabulka 4.3, str. 33). Komunikaci vždy zahajuje DCU, které reaguje na dodaná data z DCUS viz Obrázek 4.3, str. 34.

Umístění	Metoda	Význam
/	GET	Pro navázání spojení
/heartbeat	GET	Pravidelná odezva od DCU
/card_auth_req	GET	Požadavek na ověření karty
/event	GET	Příjem událostí z DCU k záznamu

Tabulka 4.2: Endpointy DCUS



Obrázek 4.3: Diagram průběhu komunikace mezi DCU a DCUS pro různé endpointy

Endpoint /heartbeat

```
DCU:
    ---

DCUS:
    {"unix_timestamp": "0xXXXXXXXXXXXXXXXX"}
```

Endpoint /card_auth_req

```
DCU:
    ?card-uid=XXXXXXXX

DCUS:
    {"cmd": "granted", timeout: UINT}
    {"cmd": "denied"}
```

Endpoint /event

```
DCU:
    ?time=UINT&event=UINT&card-uid=XXXXXXXX

DCUS:
    OK
```

4.4 DCUS

DCUS je napsán v OpenSource jazyce Rust. Pro vytvoření HTTP serveru byl zvolen framework actix-web především proto, že umožňuje s pomocí OpenSSL vytvořit HTTPS server, který je určený pro produkci. DCUS je napsán pro OS Linux.

Pro odesílání e-mailů se používá program `postfix`, spuštěný jako služba, v konfiguraci „Satellite system“ a utilita `mail` z balíčku `mailutils`. E-maily jsou odesílány prostřednictvím nezávislého procesu, do kterého jsou data předávána pomocí struktur `std::sync::mpsc::Sender` a `Reciever`, které dohromady tvoří jednosměrnou frontu s více odesílateli a jedním příjemcem.

Pro logování během vývoje se používá crate `env_logger`. Pro logování na produkci potom crate `syslog`, který zprávy posílá na lokální syslog instanci, která je nakonfigurována tak, aby zprávy z DCUS byly odkloněny do zvláštního souboru. Ten je pomocí programu logrotate dělen na jednotlivé dny a případně komprimován. Součástí zdrojového kódu jsou vzorové konfigurační soubory. Obě zvolená řešení usnadňují vývoj aplikace a zároveň ponechávají prostor pro úpravy chování.

Projekt má jeden hlavní soubor main.rs a zbytek kódu je rozdělen do 3 modulů, které budou dále popsány.

4.4.1 main.rs

Zde je načtena konfigurace DCUS, inicializováno logování a HTTPS server s ověřováním klientských certifikátů. Dále jsou tu spuštěny dva obslužné procesy. Jeden z nich slouží k odesílání e-mailů, které přijme skrz jednosměrnou frontu z jiné části DCUS. Druhý proces pak v pravidelném intervalu 30 s kontroluje, zda se všechny DCU pravidelně ohlašují. Pokud se některá DCU neohlásí do nakonfigurované doby, je její stav změněn na Down (offline) a je odeslán e-mail s notifikací.

4.4.2 mod dcus

V tomto modulu jsou jednotlivé funkce, které se volají pro obsluhu endpointů a jejich podpůrné struktury a funkce. K ověření DCU se používá její certifikát, který je už při navazování spojení zkontrolován a dál už se dostanou jen požadavky odeslané z DCU s validním certifikátem.

Aby bylo možné dál s certifikátem pracovat ve funkcích volaných pro zpracování požadavků, bylo nutné upravit soubor server.rs v crate `actix-web`, kde byl přidán jeden callback, který vloží certifikát do struktury `Request`. Pro další zpracování certifikátu se používá struktura `Authorized`, která implementuje trait `FromRequest`. Díky tomu je možné přidat proměnnou typu `Authorized` mezi parametry, které požaduje funkce obsluhující endpoint. Během zpracování požadavku se pak musí vykonat funkce `from_request` ze struktury `Authorized`, která vyjme z dodané struktury `Request` certifikát a ověří, že jeho CN souhlasí s dohodnutým formátem `DCU_ID@DCU_IP` a že IP adresa se shoduje s tou, ze které byl požadavek odeslán. Díky vhodně zvolenému formátu CN není nutné vytvářet seznam známých DCU, který by se podobal souboru `~/.ssh/known_host`, který si generuje program openSSH.

Pro získávání dat z požadavků se používá metoda podobná ověřování DCU strukturou `Authorized`. Rozdílem je, že není nutné implementovat trait `FromRequest` pro každou strukturu odpovídající vstupním datům, ale ve frameworku už jsou připravené tzv. extraktory, kterým lze určit, jaký datový typ (tedy i strukturu) budou z požadavku získávat. Extraktory jsou připravené jak pro standardní situace typu QueryString v URL, tak pro JSON v těle požadavku apod. Jediné, co musí mít struktury, aby je bylo možné automaticky extrahovat, je implementace traitu `Serialize` z crate `serde`.

Funkce reagující na požadavky mohou mít ještě mezi požadovanými parametry proměnnou typu struktura `web::Data<Mutex<DcuData>>`. Pro vysvětlení je podstatná uvnitř zabalená struktura `DcuData`, která v sobě nese HashMapu, která přiřazuje DCU_ID Stringu strukturu

`DcuInfo` (Ta obsahuje konfiguraci DCU, jestli je DCU online a kdy naposledy se ohlásilo.) a strukturu `Sender`, která patří k frontě pro odesílání e-mailů.

V modulu zatím chybí volání endpointů na události z DCU. K tomu, aby je bylo možné používat, se musí rozšířit konfigurace a vyhodnotit možnosti, jak požadavky posílat. Také ještě není implementováno zaznamenávání událostí. DCUS sice umí přijmout požadavek na provedení záznamu, ale dál už není s daty nic provedeno a tedy ani nefungují e-mailová upozornění na události z DCU.

4.4.3 mod config

Modul obsahuje jen strukturu `SystemConfig`, která uchovává konfiguraci DCUS. Konfigurace je uložena ve formátu TOML v souboru s předem danou cestou. Díky zvolenému formátu není problém celou konfiguraci načíst do struktur pomocí už hotového parseru, navíc TOML si nese informaci o datovém typu dané položky, a proto už při parsování dochází k základní validaci dat.

4.4.4 mod acl

Modul má za úkol zprostředkovat zdroj přístupových práv. Jeho implementace pro konkrétní instalaci je nedílnou součástí integrace tohoto systému do už existujících řešení.

Aktuální implementace je velmi jednoduchý mock-up, který bude v další verzi nahrazen základním systémem řízení oprávnění, který bude založen na souborech se seznamy UID, která mají povolený vstup. Díky tomu bude možné systém nasadit samostatně, případně jej vyzkoušet bez pracné integrace.

4.5 Zkoušení

Způsoby zkoušek jsou popsány v technické normě ČSN EN 60839-11-1 [32]. Kromě funkčních zkoušek jsou ještě prováděny odolnostní zkoušky, kdy je zařízení vystaveno definovaným podmínkám, které odpovídají zvolenému stupni odolnosti vůči vnějším vlivům. Odolnostní zkoušky musí být prováděny v souladu s IEC 62599-1 a IEC 62599-2. Pro jejich provádění je nutné vlastnit speciální vybavení a být akreditovanou laboratoří, proto nebudou součástí této práce.

Před zahájením funkční zkoušky musí být zkoušený systém uveden do následujícího stavu:

- připojen k napájecímu zdroji s napětím v rozsahu definovaném výrobcem, které bude po celou dobu zkoušky konstantní
- pro detekování jakýchkoliv doplňkových signálů připojen k zařízení, které tyto signály umožní detekovat
- vstupní signály/zprávy musí být správně zakončeny v souladu s dokumentací
- výstupy musí být připojeny k maximální povolené zátěži
- veškeré přenosové cesty musí být připojeny ke kompatibilním zařízením

Zkoušený systém musí být v následující konfiguraci:

- systém k testování musí obsahovat alespoň jeden od každého typu podporovaného uživatelského místa přístupu, aktivátoru místa přístupu, nebo jejich ekvivalentu (z pohledu zátěže)
- testovaný systém musí obsahovat ovládací panel, nebo jeho ekvivalent
- systém musí umožňovat provoz v souladu s požadavky podle klasifikačního stupně

- předložený systém k testování musí být standardní produkcí výrobce
- předložený systém musí obsahovat proklamované volitelné funkce

Zkoušený systém musí být instalován v souladu s pokyny výrobce, pokud je možné systém instalovat více způsoby, je nutné zvolit ten méně příznivý.

4.5.1 Rozhraní místa přístupu – čas uvolnění

Postup je převzat z [32].

1. Systém musí být naprogramován pro jednu platnou uživatelskou informaci (oprávnění) a v normálním stavu.
2. Ověří se dokumentace výrobce a stanoví se, zda je čas uvolnění definován systémem, nebo je konfigurovatelný pro každé místo přístupu (portál).
3. Vloží se uživatelská informace, musí dojít k poskytnutí přístupu.
4. Změří se čas uvolnění a zaznamená se výsledek, funkce musí odpovídat požadavkům 1 a 2 ze seznamu „Požadavky na rozhraní místa přístupu“ na str. 17.

Vyvinutý systém zkouškou prošel.

4.5.2 Rozhraní místa přístupu – kontrola vstupu

Postup je převzat z [32].

1. Systém musí být naprogramován pro jednu platnou uživatelskou informaci (oprávnění) a v normálním stavu. Systém musí být vybaven dvěma místy přístupu, jedno programované jako vstup a druhé jako výstup z kontrolovaného prostoru.
2. Ověří se dokumentace výrobce a stanoví se, zda je implementováno pravidlo zábrany proti opakovanému průchodu a které varianty jsou podporovány (zábrana proti opakovanému průchodu s následným zamítnutím přístupu, výstraha při nerespektování zábrany proti opakovanému průchodu, časově závislá zábrana proti opakovanému průchodu, globální zábrana proti opakovanému průchodu, překonání/vyřazení zábrany proti opakovanému průchodu a časy zábrany).
3. V místě vstupu se vloží uživatelská informace a ověří se, že došlo k poskytnutí vstupu. Funkce musí odpovídat požadavku 3 ze seznamu „Požadavky na rozhraní místa přístupu“ na str. 17.
4. Vloží se tatáž uživatelská informace na místě vstupu (Před naprogramovaným časem zábrany proti opakovanému průchodu i po něm.) a zaznamená se výsledek.
5. Vloží se uživatelská informace na místě východu a ověří se, že byl východ povolen. Funkce musí odpovídat požadavku 4 ze seznamu „Požadavky na rozhraní místa přístupu“ na str. 17.
6. Vloží se tatáž uživatelská informace na místě vstupu (Před naprogramovaným časem zábrany proti opakovanému průchodu i po něm.) a zaznamená se výsledek.
7. Opakuje se zkouška pro každou variantu zábrany proti opakovanému průchodu podporovanou zkoušeným systémem kontroly vstupu.
8. Funkce pro podporované varianty musí odpovídat požadavkům v ČSN EN 60839-11-1.

9. Naprogramuje se účinné datum vypršení uživatelské informace.

10. Vloží se uživatelská informace v místě příchodu v rámci povoleného data/před datem vypršení nastaveného data pro toto oprávnění, přístup musí být povolen.

11. Vloží se uživatelská informace v místě příchodu po uplynutí povoleného data nebo po nastaveném datu vypršení pro toto oprávnění, přístup musí být odmítnut. Funkce musí odpovídat požadavkům v ČSN EN 60839-11-1 a požadavku 5 ze seznamu „Požadavky na rozhraní místa přístupu“.

12. Naprogramují se dvě uživatelské informace s toutéž přístupovou úrovní.

13. Místo přístupu se naprogramuje pro umožnění vstupu, pouze jsou-li v rámci programovaného časového úseku učiněny dva následné autorizované pokusy o přístup. Naprogramuje se povolené časové okno na 2 minuty.

14. Prezentuje se jedna uživatelská informace, přístup nesmí být povolen.

15. V rámci 2 minut se prezentují první a druhá uživatelská informace, přístup musí být povolen.

16. Prezentuje se první uživatelská informace, počká se 2 minuty, prezentuje se druhá uživatelská informace, přístup nesmí být povolen. Funkce musí odpovídat požadavkům v ČSN EN 60839-11-1.

Vyvinutý systém nepodporuje zábranu proti opakovanému průchodu, podmíněný přístup do data platnosti ani dvojnásobný přístup, a proto na tyto funkce nemůže být testován. V ostatních částech zkoušky systém uspěl.

4.5.3 Rozhraní místa přístupu – kontrola vstupu

Postup je převzat z [32].

1. Systém musí být naprogramován pro jednu platnou uživatelskou informaci (oprávnění) a v normálním stavu.

2. Ověří se dokumentace výrobce a stanoví se, je-li systémem definován čas otevření místa přístupu, programovatelný pro každé místo přístupu/portál.

3. Vloží se uživatelská informace, přístup musí být povolen.

4. Změří se doba otevření portálu a zaznamená se výsledek. Funkce musí odpovídat požadavkům 6 a 7 ze seznamu „Požadavky na rozhraní místa přístupu“ na str. 17.

Systém prošel zkouškou částečně, přestože je možné definovat povolenou dobu otevření dveří, tak systém nijak neindikuje blížící se konec této doby.

4.5.4 Rozhraní místa přístupu – zpracování vstupních signálů

Aplikuje se vstupní signál (například sabotáž) s aktivní dobou trvání nejméně 400 ms a zaznamená se, zda je událost ohlášena na ovládacím panelu. Funkce musí odpovídat požadavku 8 ze seznamu „Požadavky na rozhraní místa přístupu“ na str. 17. Převzato z [32].

Vyvinutý systém zkouškou neprošel. Systém má v aktuální verzi jen jeden nekomunikační vstup a ten slouží k monitorování stavu portálu, tedy nesplňuje požadavky této zkoušky.

V další verzi HW a FW budou už k dispozici dva nekomunikační vstupy, z toho jeden bude vyhrazen pro sabotážní smyčku.

4.5.5 Indikace portálu

Postup je převzat z [32]. Z postupu jsou vypuštěny části týkající se ovládacího panelu, který není předmětem této práce.

1. Pokud je tato funkce k dispozici, ověří se, že je stav zamčení portálu zobrazen do okamžiku poskytnutí přístupu. Funkce musí být v souladu s ČSN EN 60839-11-1.

2. Na místě přístupu se pro vytvoření stavu povoleného přístupu prezentuje platné oprávnění. Zaznamená se odezva oznamovacích výstupů na portálu. Funkce musí být podle požadavku 1 ze seznamu „Požadavky na indikaci a hlášení“ na str. 18.

3. Na místě přístupu se pro vytvoření stavu odmítnutého přístupu prezentuje neplatné oprávnění a zaznamená se odezva oznamovacích výstupů. Zjistí se, zda je příčina zamítnutí přístupu zaznamenána v paměti událostí. Funkce musí být podle požadavku 2 ze seznamu „Požadavky na indikaci a hlášení“ na str. 18.

4. Pro systémem definovanou činnost se na místě přístupu prezentuje pro vytvoření stavu povoleného přístupu platné oprávnění a simuluje se otevření portálu. Portál se ponechá otevřený až do začátku systémem definovaného času před výstrahou a zaznamená se odezva oznamovacího výstupu na portálu. Portál se ponechá otevřený do uplynutí systémem definovaného času otevření a potvrdí se, že byla na ovládacím panelu generována výstraha. Funkce musí být v souladu s ČSN EN 60839-11-1.

5. Zavře se portál a zaznamená se čas uplynulý do pominutí výstrahy. Funkce musí odpovídat požadavkům v ČSN EN 60839-11-1.

Vyvinutý systém nepodporuje funkci zobrazení stavu uzamčení portálu, a proto na ni nemůže být testován. Systém podporuje indikaci překročení doby otevření, ale její časování v aktuální verzi neodpovídá požadavkům v ČSN EN 60839-11-1. Ostatní indikace sice fungují správně, ale systém zkouškou neprošel.

4.5.6 Úrovně přístupu

Postup je převzat z [32].

1. Na počátku všech zkoušek se nastaví hodiny reálného času na správný čas. Po uplynutí jednoho dne se zkontroluje, zda se hodiny reálného času neliší od správného času o víc, než je povolená hodnota, vypočtená podle požadavku 1 ze seznamu „Požadavky rozpoznávání“ na str. 18.

2. Nastaví se datum na datum změny ze zimního času na letní čas a čas na čas dvě minuty před očekávanou změnou. Ověří se, zda změna ze zimního času na letní čas nastane v úřední dobu změny, a tedy odpovídá požadavku 1 ze seznamu „Požadavky rozpoznávání“ na str. 18.

3. Nastaví se datum na datum změny letního času na zimní čas a čas na čas dvě minuty před očekávanou změnou. Ověří se, zda změna z letního času na zimní čas nastane v úřední dobu změny, a tedy odpovídá požadavku 1 ze seznamu „Požadavky rozpoznávání“ na str. 18.

4. Nastaví se datum na 28. únor příštího přestupného roku a čas na 23:58. O půlnoci se ověří, zda se datum změní na 29. únor, jak odpovídá požadavku 1 ze seznamu „Požadavky rozpoznávání“ na str. 18. Nastaví se datum na 28. únor nepřestupného roku a čas na 23:58. O půlnoci se ověří, zda se datum změní na 1. březen, jak odpovídá požadavku 1 ze seznamu „Požadavky rozpoznávání“ na str. 18.

5. Hlavní hodiny se nastaví na správný čas a datum. Závislé hodiny reálného času se nastaví na nesprávný čas a nesprávné datum. Čas hlavních hodin se nastaví 2 minuty před časem synchronizace (daném výrobcem). Ověří se, zda jsou po čase synchronizace závislé hodiny reálného času synchronizovány na tentýž čas a datum jako na hlavních hodinách. Prohlídkou přiložené dokumentace se ověří, že se synchronizace opakuje každý den (tj. bez uvedení data). Funkce musí odpovídat požadavku 2 ze seznamu „Požadavky rozpoznávání“ na str. 18.

6. Hlavní hodiny řídicí jednotky kontroly vstupu se nastaví na nesprávný čas a nesprávné datum. Hlavní hodiny EACS se nastaví na oficiální čas místa, což určuje oficiální čas. Po uplynutí nejvýše 15 minut se ověří, zda se hlavní hodiny EACS synchronizovaly s oficiálním časem, jak odpovídá ČSN EN 60839-11-1.

7. Potvrdí se, že jsou hodiny reálného času nastaveny na správný čas. Odpojí se síťový přívod napájení a baterie záložního zdroje napájení (baterie pro uchování dat musí zůstat připojeny). Po uplynutí doby definované podle příslušného stupně se opět připojí síťový přívod napájení a baterie záložního zdroje napájení. Pořadí opětného připojování musí být v souladu s doporučeními výrobce zařízení. Ověří se, zda hodiny reálného času systému pro kontrolu vstupu zobrazují správný čas. Funkce musí odpovídat požadavku 3 ze seznamu „Požadavky rozpoznávání“ na str. 18.

8. Přezkoumá se dokumentace výrobce a určí se, zda počet uživatelských úrovní přístupu a počet časových pásem splňuje, nebo překračuje požadavky kladené v požadavcích 4 a 5 ze seznamu „Požadavky rozpoznávání“ na str. 18.

9. Ověří se, zda je pro příslušné úrovně možné zadávání dne, týdne, hodiny, minuty, nebo data, roku, měsíce a dne, nebo hodiny a minuty, podle požadavku 6 ze seznamu „Požadavky rozpoznávání“ na str. 18.

10. Ověří se, zda je elektronickým systémem kontroly vstupu správně zpracováván uvedený počet konfigurovatelných dní (tj. mimořádných dní) podle požadavku 7 ze seznamu „Požadavky rozpoznávání“ na str. 18.

Koncepce vyvinutého systému přenechává práci s časovými zónami, úrovněmi přístupu a zpracování mimořádných dní na zdroji přístupových práv, který není součástí této práce.

Hodiny reálného času použité v DCU splňují nároky v oblasti přesnosti. Synchronizace hodin DCU s DUCS (kdy DCUS představuje hlavní hodiny systému) probíhá nejméně jednou za 4 hodiny a synchronizace probíhá i okamžitě po prvním připojení k DCUS. DCUS je implementováno nad OS Linux, který podporuje protokol NTP a umí své hodiny automaticky synchronizovat s nastaveným časovým pásmem. Obvod RTC dokáže po odpojení hlavního zdroje napájení fungovat dostatečně dlouho dobu, aby vyhověl požadavkům.

V oblastech, které byly vyvinuty jako součást této práce, systém zkouškou prošel. Ovšem bez znalosti implementace zdroje přístupových oprávnění nelze rozhodnout, že systém jako celek zkouškou prošel.

4.5.7 Zařízení a způsoby rozpoznávání

Postup je převzat z [32].

1. Zkusí se přidat do systému nový identifikační prostředek se stejným číslem, jako již mají autorizovaní uživatelé, nebo se zkusí přidělit stejný identifikační prostředek dvěma uživatelům. Ověří se, že je pokus odmítnut. Funkce musí odpovídat požadavku 8 ze seznamu „Požadavky rozpoznávání“ na str. 18.

2. EACS se uvede do provozního režimu, aniž by přístupové úrovně byly přiděleny jakémukoli uživateli/držiteli karet. Přidělí se patřičné oprávnění uživateli/držiteli karty. Pro tohoto uživatele se přidělí přístupová úroveň. Oprávnění se během povolené doby vstupu aplikuje u vhodné čtečky/klávesnice, nebo biometrického snímače. Potvrdí se, že byl přístup povolen. Aplikuje se jakékoli jiné oprávnění, které systému není známé, u čtečky, nebo biometrického snímače a potvrdí se, že byl přístup odmítnut. Funkce musí odpovídat požadavku 9 ze seznamu „Požadavky rozpoznávání“ na str. 18.

3. Ověří se, že dojde k zamítnutí přístupu s platným identifikačním prostředkem a neplatnou zapamatovanou informací. Ověří se, že po počtu pokusů stanoveným v ČSN EN 60839-11-1 bude toto oprávnění blokováno v souladu s parametry nastavenými v konfiguraci systému.

4. Prostuduje se dokumentace výrobce a ověří se, že jsou uvedeny požadované úrovně FAR pro biometrická zařízení (jsou-li v řídicí jednotce použita pro příslušný stupeň). Informace musí odpovídat požadavkům v ČSN EN 60839-11-1.

5. Přezkoumá se dokumentace a ověří se, že jsou splněny požadavky variant kódů na počet systémem povolených uživatelů pro každý stupeň. Informace musí odpovídat požadavkům v ČSN EN 60839-11-1.

6. Přezkoumá se dokumentace a ověří se, že minimální počet používaných číslic používaný pro zapamatované informace odpovídá požadavkům v ČSN EN 60839-11-1.

7. 10 uživatelům se přidělí identifikační prostředek s kódem objektu/uživatele. Založí se nový uživatel/držitel karty a zkusí se mu přidělit již použitý identifikační prostředek. Potvrdí se, že to systém odmítne a poskytne upozornění, že tento identifikační prostředek již byl přidělen. Funkce musí odpovídat požadavkům v ČSN EN 60839-11-1.

8. Přidělí se identifikační prostředky s různými kódy objektu a se stejnými kódy uživatele dvěma nebo více uživatelům. Potvrdí se, že systém umožní vložení různých kódů objektu. Funkce musí odpovídat požadavkům v ČSN EN 60839-11-1.

9. Přezkoumá se dokumentace výrobce a potvrdí se, zda je, nebo není podporován degradovaný režim činnosti. Ověří se, že degradovaný režim činnosti může být vyřazen z činnosti automaticky, nebo manuálně přístupovou úrovní dohlížitel, jestliže je prověřován systém pro funkce stupně 4. Funkce musí odpovídat požadavkům v ČSN EN 60839-11-1.

10. Na identifikačních prostředcích, které mají být se systémem použity, se ověří, zda je struktura kódování viditelná (např. průhledný identifikační prostředek), nebo zda je kompletní kódování natištěno na identifikačním prostředku. Funkce musí odpovídat požadavkům 12 a 13 ze seznamu „Požadavky rozpoznávání“ na str. 18.

Práce s uživateli, jim přidělenými identifikačními prostředky a uživatelskými oprávněními je přenechána na zdroj přístupových oprávnění, který není součástí práce. Systém nepoužívá ani biometrii ani zapamatovanou informaci. Degradovaný režim provozu také není implementovaný.

Systém pro rozhodování o přístupu používá identifikační prostředky. Pokud budou použity vhodné karty třetích stran, tak na nich nebude pouhým okem viditelné kódování systému. Kompletní kódování je ovšem reprezentováno jen identifikačním číslem prostředku a z tohoto důvodu a také z důvodu neznalosti implementace zdroje přístupových práv systém zkouškou neprošel.

Tuto zkoušku při aktuálně zvolené koncepci nelze splnit. K jejímu splnění by bylo nutné provést jak HW, tak SW změny a zbavit se možnosti používat karty vydané třetí stranou.

4.5.8 Komunikace a vlastní ochrana

Postup převzatý z [32] byl autorem zkrácen.

1. Z dat poskytnutých výrobcem paměti pro ukládání záznamů a konfigurace se ověří, že data jsou uchovávána po dostatečně dlouho dobu, která odpovídá požadavku 1 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

2. Po dobu definovanou v požadavcích 1 a 8 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19 se odpojí napájení jednotky.

3. Po uplynutí doby pro odpojení je jednotka opět připojena a musí dojít k jejímu automatickému restartu dle požadavku 2 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

4. Po obnovení napájení je zkontrolováno, že uložená data (konfigurace a záznamy) nejsou poškozena nebo ztracena. Dále je zkontrolováno, že hodiny reálného času ukazují správný čas.

5. Po simulované ztrátě dat (vymazání konfigurace apod.) jednotka ohlásí problémový stav v souladu s požadavku 3 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

6. Přezkoumáním dokumentace se ověří, že pro otevření krytu jednotky je nutné použít nastroje. Funkce musí být v souladu s požadavkem 4 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

7. Komponenta systému s bezpečně uzavřeným krytem se namontuje dle pokynů výrobce.

8. S pomocí normálních prostředků, tzn. nástrojů a pokynů výrobce, se otevře kryt zařízení. Následně se do něj zasune sabotážní nástroj dle IEC 60529 (kovová tyčka o průměru 1 mm a délce 100 mm). Zasunutí sabotážního nástroje se musí provést před zapůsobením detekce sabotáže. Manipulací se sabotážním nástrojem nesmí dojít k fyzickému poškození přístroje.

9. Pokud se úspěšně podařilo sabotážní nástroj zasunout, má se pokračovat pokusem zasáhnout do fungování protisabotážního mechanismu, nebo ostatních součástek pod krytem za účelem vyvolání stavu povoleného přístupu. Funkce musí odpovídat požadavku 5 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

10. Prověří se dokumentace výrobce ve vztahu k charakteristikám IP a IK, informace musí souhlasit s požadavkem 6 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

11. Při odpojeném komunikačním kanálu mezi ACU a ovládacím panelem se generují pokusy o přístup s platným oprávněním a ověří se, že funkce odpovídá požadavkům 9 a 10 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

12. Během normální činnosti systému se od jednotky odpojí čtečka. Funkce musí odpovídat požadavku 9 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

13. Přezkoumá se dokumentace a potvrdí se, že přístup ke konfiguraci jednotky je omezen používáním platných ověření a že je možné omezit přístup k různým funkcím systému na základě úrovně přístupu. Funkce musí odpovídat požadavku 7 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

14. Ověří se, že pravidla zpracování nejsou viditelná pohledem na zakrytou jednotku. Funkce musí být v souladu s požadavkem 11 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

15. V konfiguračním režimu jednotky se učiní pokus o zadání neplatných dat (chybný formát, jiné než očekávané znaky apod.) a ověří se, že data nejsou akceptována. Funkce musí odpovídat požadavku 12 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

16. Vstoupí se do konfiguračního režimu, nevloží se žádná data a sleduje se účinek doby nečinnosti systému. Funkce musí odpovídat požadavku 13 ze seznamu „Požadavky na vlastní ochranu systému“ na str. 19.

Jednotka používá dva typy paměti pro trvalé ukládání dat. Pro konfiguraci se jedná o flash paměť typu NOR, která je součástí modulu ESP32, a pro záznam událostí se používá paměť EEPROM. Obě paměti vyhovují kladeným nárokům na retenci dat. Jednotka se po připojení napájení automaticky restartuje, tento proces je zajištěn HW implementací v mikrokontroléru. Po obnovení napájení byla zkontrolována data záznamů událostí, konfigurace a čas hodin reálného času. Data byla v pořádku a hodiny ukazovaly správný čas. Pokud dojde ke ztrátě konfigurace, tak se DCU nedokáže ohlásit DCUS, který po uplynutí doby pro ohlášení DCU odešle e-mail s upozorněním, že DCU se nepřipojila. Systém zatím nemá instalační dokumentaci a nelze tak ověřit, jestli se musí použít nástroje k otevření jeho krytu. Části systému, které budou instalovány vně chráněného prostoru (čtečky), nemají vestavěnou detekci sabotáže, takže samy o sobě nesplňují požadavky. Čtečky je ovšem možné umístit do krytu, který nebude bránit jejich běžnému používání a který půjde v souladu s požadavky vybavit detekcí sabotáže. Charakteristiky IP a IK nelze bez dokumentace systému ověřit. Odpojením DCU od DCUS dojde k přerušení rozhodování o přístupu. V další verzi bude tento nedostatek mírně kompenzován cache oprávnění a nouzovými přístupy. Pravidla zpracování nejsou viditelná ani na nekryté jednotce. Konfigurační režim DCU umí validovat vložené hodnoty, stejně tak DCUS validuje hodnoty v konfiguračním souboru. Přístup do konfigurace DCU není v aktuální verzi chráněn heslem. Přístup ke konfiguraci DCUS je chráněn prostřednictvím OS Linux, nad kterým je DCUS postaveno. Konfigurace DCU v aktuální verzi neomezuje čas strávený v konfiguračním režimu. U DCUS tuto dobu měřit nelze, protože konfigurační soubor je načten jen při spuštění.

Některé funkce jsou implementovány jinak, než je požadováno, jiné funkce ještě není možné ověřit a celkově tedy systém zkouškou neprošel.

4.5.9 Zkouška reálného provozu

Vzhledem k existenci zatím jediného prototypu DCU není možné vyzkoušet, jak se bude DCUS chovat v reálné instalaci s desítkami DCU. Proto autor navrhl jednoduché otestování DCUS se zátěží pomocí utility ab (Apache benchmark) z balíčku apache2-utils. Utilita ab umí od verze 2.4.6 používat klientské certifikáty a bylo tak možné věrně simulovat chování reálných DCU. Pro test za plného provozu byl ab nakonfigurován tak, aby se na serveru prokázal platným certifikátem a pokoušel se o 50 připojení v jeden okamžik. DCUS za těchto podmínek bez problémů stíhal odpovídat na dotazy DCU a uživatel žádající o přístup nedokázal rozeznat rozdíl v odezvě mezi vytíženým a nevytíženým DCUS.

Kapitola 5

Závěr

Základní cíl práce byl naplněn. Navržené a implementované komponenty byly v době odevzdání funkční a bylo je možné otestovat proti požadavkům, které na ně klade ČSN EN 60389-11-1. Systém sice v některých oblastech neuspěl, ale to je dáno především nekompletní nebo chybnou implementací. Tyto nedostatky jsou v práci zdokumentovány a autor má silnou motivaci pokračovat ve vývoji systému i po obhájení práce a odstranit je. Po jejich odstranění bude možné prohlásit za splněný také druhý cíl, tedy dát komunitě k dispozici solidní základ pro budování systémů kontroly vstupu.

Po implementaci všech chybějících funkcí autor počítá s nasazením systému do místností na Strahovských kolejích spravovaných místní studentskou samosprávou - klubem Silicon Hill a integrací do Informačního systému klubu Silicon Hill. V dnešní době se ke stejnému účelu využívá systém provozovaný VIC ČVUT, dodávaný společností IMA. Vzhledem k právnímu vztahu mezi studentskou samosprávou a ČVUT není možné tento systém integrovat do Informačního systému, což značně komplikuje jeho správu. Další problém představuje rozšiřování systému, které si žádá kooperaci několika součástí ČVUT a studentské samosprávy. Po přechodu na vlastní systém lze očekávat zvýšení komfortu jak správců, tak uživatelů.

Bibliografie

[1] 2N TELEKOMUNIKACE a.s. *Instalační manuál 2N Access Unit [online]*. cit. 8. 5. 2020. 2020. URL: https://wiki.2n.cz/download/attachments/43189827/2N_Access_Unit_Installation_Manual_EN_2.14.pdf.

[2] 2N TELEKOMUNIKACE a.s. *Webová prezentace společnosti 2N [online]*. cit. 8. 5. 2020. 2016. URL: https://www.2n.cz.

[3] ABRACON, LLC. *ARJM11 - RJ45 SINGLE PORT 100/1000/2.5G/5G BASE-T MAGNETICS [online]*. cit. 15. 5. 2020. 2019. URL: https://abracon.com/Magnetics/ARJM11.pdf.

[4] Márcio Almeida. *Hacking Mifare ClassicCards - BlackHat slides [online]*. cit. 11. 5. 2020. 2014. URL: https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf.

[5] Apking a Ulfr. *Security/Server Side TLS [online]*. cit. 12. 5. 2020. 2020. URL: https://wiki.mozilla.org/Security/Server_Side_TLS.

[6] ATMEL. *AVR101: High Endurance EEPROM Storage [online]*. cit. 17. 5. 2020. 2002. URL: http://ww1.microchip.com/downloads/en/Appnotes/doc2526.pdf.

[7] BOURNS, INC. *Transient Voltage Suppressor (TVS) Diodes [online]*. cit. 15. 5. 2020. 2019. URL: https://www.bourns.com/docs/technical-documents/technical-library/chip-diodes/publications/bourns_tvs_diode_short_form.pdf.

[8] Nicolas T. Courtois, Karsten Nohl a Sean O'Neil. *Algebraic Attacks on the Crypto-1 StreamCipher in MiFare Classic and Oyster Cards [online]*. cit. 10. 5. 2020. 2008. URL: https://eprint.iacr.org/2008/166.pdf.

[9] Petr Elexa. *Přístupový systém s využitím RFID karet [online]*. Bakalářská práce. cit. 9. 5. 2020. 2020. URL: https://dspace.cvut.cz/handle/10467/86619.

[10] Adam Healey. *Webová prezentace IEEE 802.3 ETHERNET WORKING GROUP [online]*. cit. 12. 5. 2020. 2020. URL: http://www.ieee802.org/3/.

[11] HSI Sensing. *Reed Switch Appliaction Notes [online]*. cit. 12. 5. 2020. 2013. URL: https://www.hsisensing.com/wp-content/uploads/2016/03/HSI_Reed_Switch_Applicaton_Notes_v12_2013.pdf.

[12] iButtons I& RFID - Drexia. *RS-H0-06 BZ Product card [online]*. cit. 15. 5. 2020. 2018. URL: https://drexia.pl/en/index.php?controller=attachment&id_attachment=53.

[13] IMA s. r. o. *IMAPorter Basic [online]*. cit. 8. 5. 2020. 2016. URL: https://www.ima.cz/wp-content/uploads/web-IMAporter-Basic_A41.pdf.

[14] IMA s. r. o. *IMAPorter Cloud [online]*. cit. 8. 5. 2020. 2016. URL: https://www.ima.cz/wp-content/uploads/web-IMAporter-Cloud_A41.pdf.

[15] IMA s. r. o. *IMAPorter Pro [online]*. cit. 8. 5. 2020. 2017. URL: https://www.ima.cz/wp-content/uploads/brozura_imaporter_web_final.pdf.

[16] IMA s. r. o. *PŘÍSTUPOVÝ SYSTÉM PATRON-PRO [online]*. cit. 8. 5. 2020. 2015. URL: https://www.ima.cz/wp-content/uploads/IMAporter-Mobile-brozura_A41.pdf.

[17] IMA s. r. o. *Webová prezentace společnosti IMA [online]*. cit. 8. 5. 2020. 2020. URL: https://www.ima.cz/.

[18] Jablotron a. s. *Stránka JA-121T Sběrnicové rozhraní RS-485 [online]*. cit. 9. 5. 2020. 2020. URL: https://www.jablotron.com/cz/produkt/sbernicove-rozhrani-rs-485-426/.

[19] Jablotron a. s. *Stránka JA-192J RFID přívěsek [online]*. cit. 8. 5. 2020. 2020. URL: https://www.jablotron.com/cz/produkt/rfid-privesek-510/.

[20] Jablotron a. s. *Webová prezentace společnosti Jablotron [online]*. cit. 8. 5. 2020. 2020. URL: https://www.jablotron.com/.

[21] Ya Liu et al. "Legitimate-reader-only attack on MIFARE Classic". In: *Mathematical and Computer Modelling* 58.1-2 (2013), s. 219–226. ISSN: 08957177. DOI: 10.1016/j.mcm.2012.07.020. URL: https://linkinghub.elsevier.com/retrieve/pii/S0895717712002038.

[22] Martin Malý. *REST: architektura pro webové API [online]*. cit. 17. 5. 2020. 2009. URL: https://www.zdrojak.cz/clanky/rest-architektura-pro-webove-api/.

[23] Microchip Technology Inc. *MCP23017/MCP23S17: 16-Bit I/O Expander with Serial Interface [online]*. cit. 17. 5. 2020. 2016. URL: http://ww1.microchip.com/downloads/en/devicedoc/20001952c.pdf.

[24] Microchip Technology Inc. *MCP7940N: Battery-Backed I2C Real-Time Clock/Calendar with SRAM [online]*. cit. 17. 5. 2020. 2014. URL: http://ww1.microchip.com/downloads/en/devicedoc/20005010f.pdf.

[25] NXP Semiconductors. *NXP Contactless identification portfolio [online]*. cit. 10. 5. 2020. 2017. URL: https://www.nxp.com/docs/en/product-selector-guide/MIFARE-ICs-linecard.pdf.

[26] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3 [online]*. cit. 12. 5. 2020. 2018. URL: https://tools.ietf.org/html/rfc8446.

[27] ASSA ABLOY Czech I& Slovakia s.r.o. *Elektrické otvírače FAB 2019 [online]*. cit. 14. 5. 2020. 2019. URL: https://www.assaabloyopeningsolutions.cz/Local/CZ/oneweb%202.0/Ke%20sta%c5%been%c3%ad/Katalogy/AA%20Elektrick%c3%a9%20otv%c3%adra%c4%8de%202019%20R1.pdf.

[28] Martin Sadový. *Přístupový systém založený na NFC [online]*. Bakalářská práce. cit. 9. 5. 2020. 2016. URL: http://dspace.vsb.cz/handle/10084/116324.

[29] SMSC. *SMSC Ethernet Physical Layer Layout Guidelines [online]*. cit. 6. 5. 2020. 2008. URL: http://ww1.microchip.com/downloads/en/AppNotes/en562748.pdf.

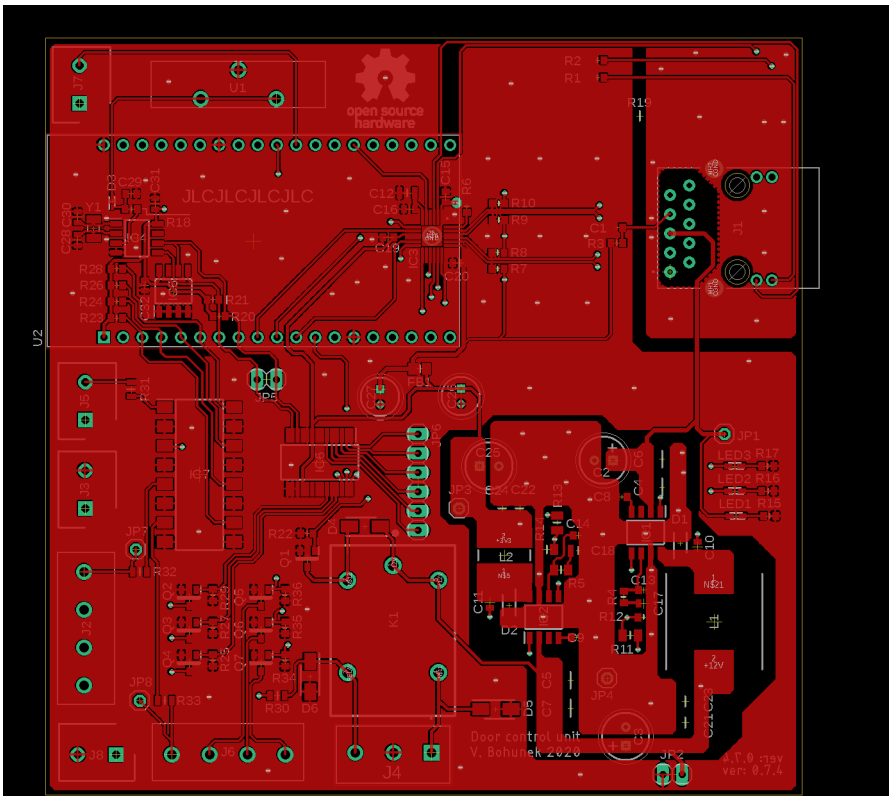
[30] STMicroelectronics. *M24512-W, M24512-R, M24512-DF: 512-Kbit serial I2C bus EEPROM [online]*. cit. 17. 5. 2020. 2018. URL: https://www.st.com/resource/en/datasheet/m24512-r.pdf.

[31] Jan Truhlář. *Inteligentní přístupový systém pro větší objekty [online]*. Bakalářská práce. cit. 10. 5. 2020. 2017. URL: https://dspace.cvut.cz/handle/10467/86619.

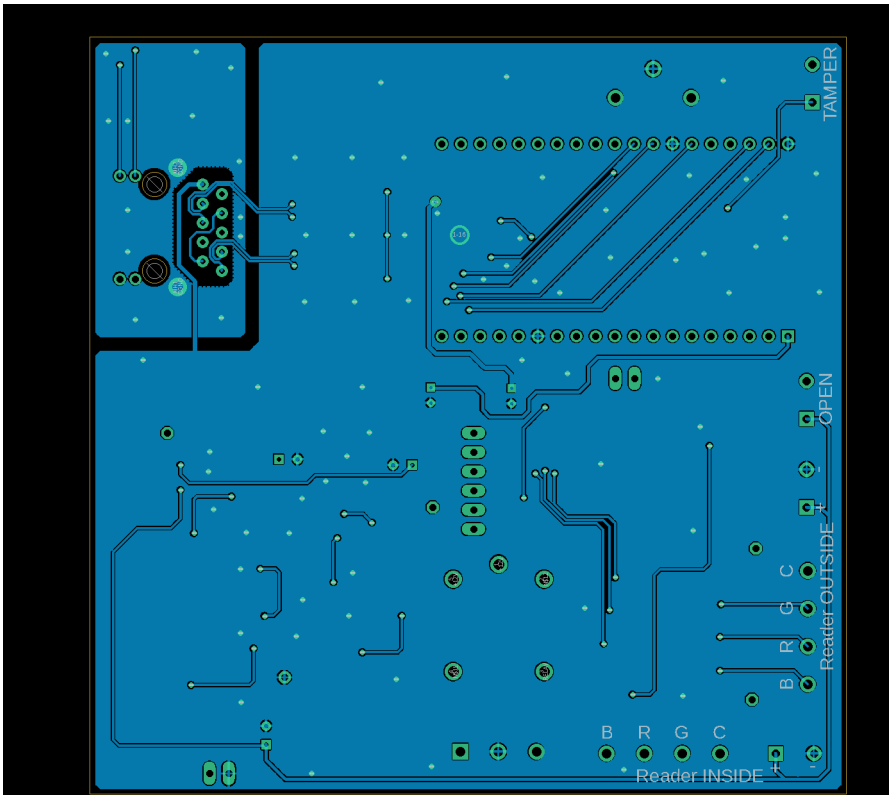
[32] Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. *ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy - část 11-1*. Třídicí znak 334593. 2014, s. 56.

Příloha A

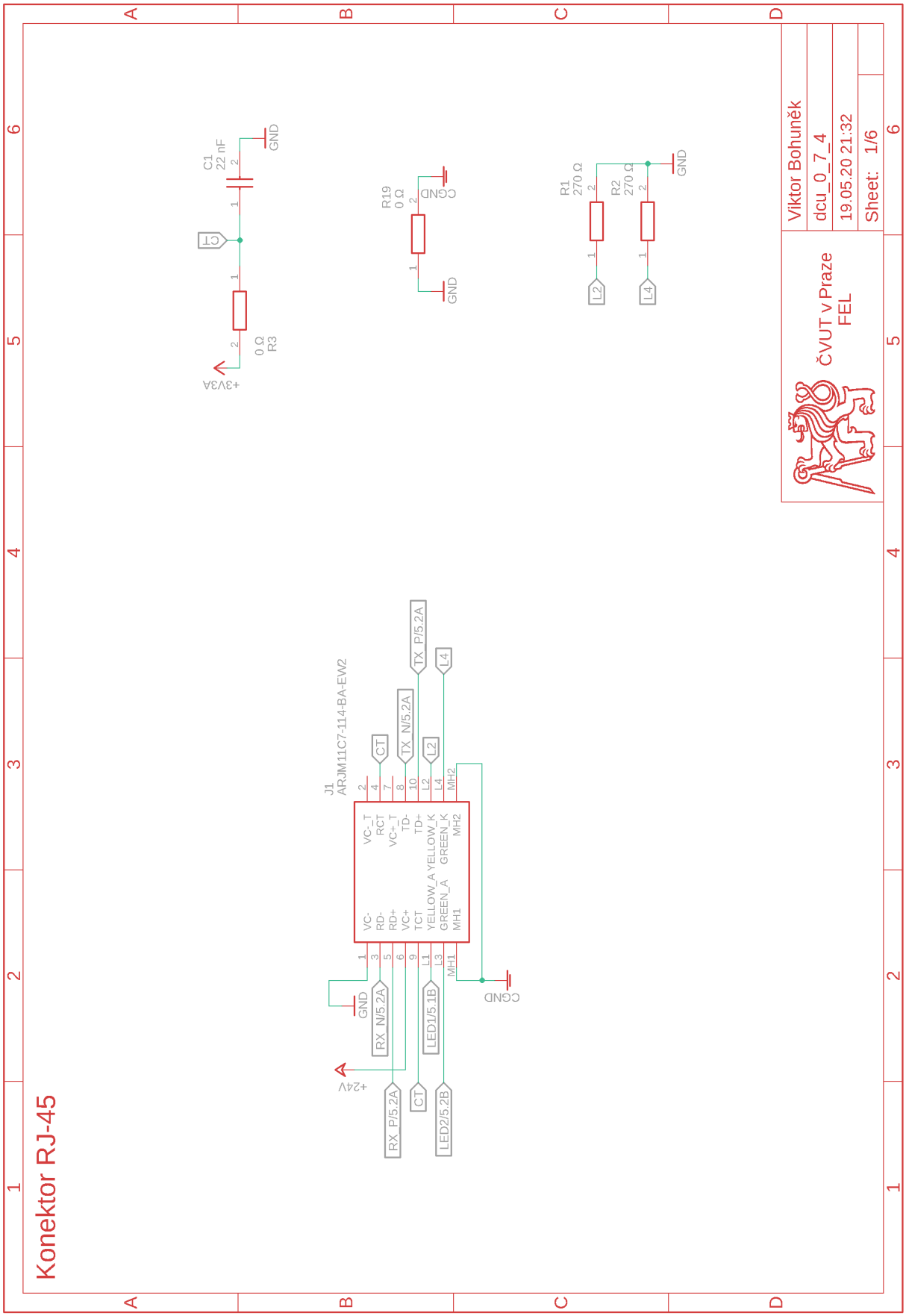
Podklady pro DPS



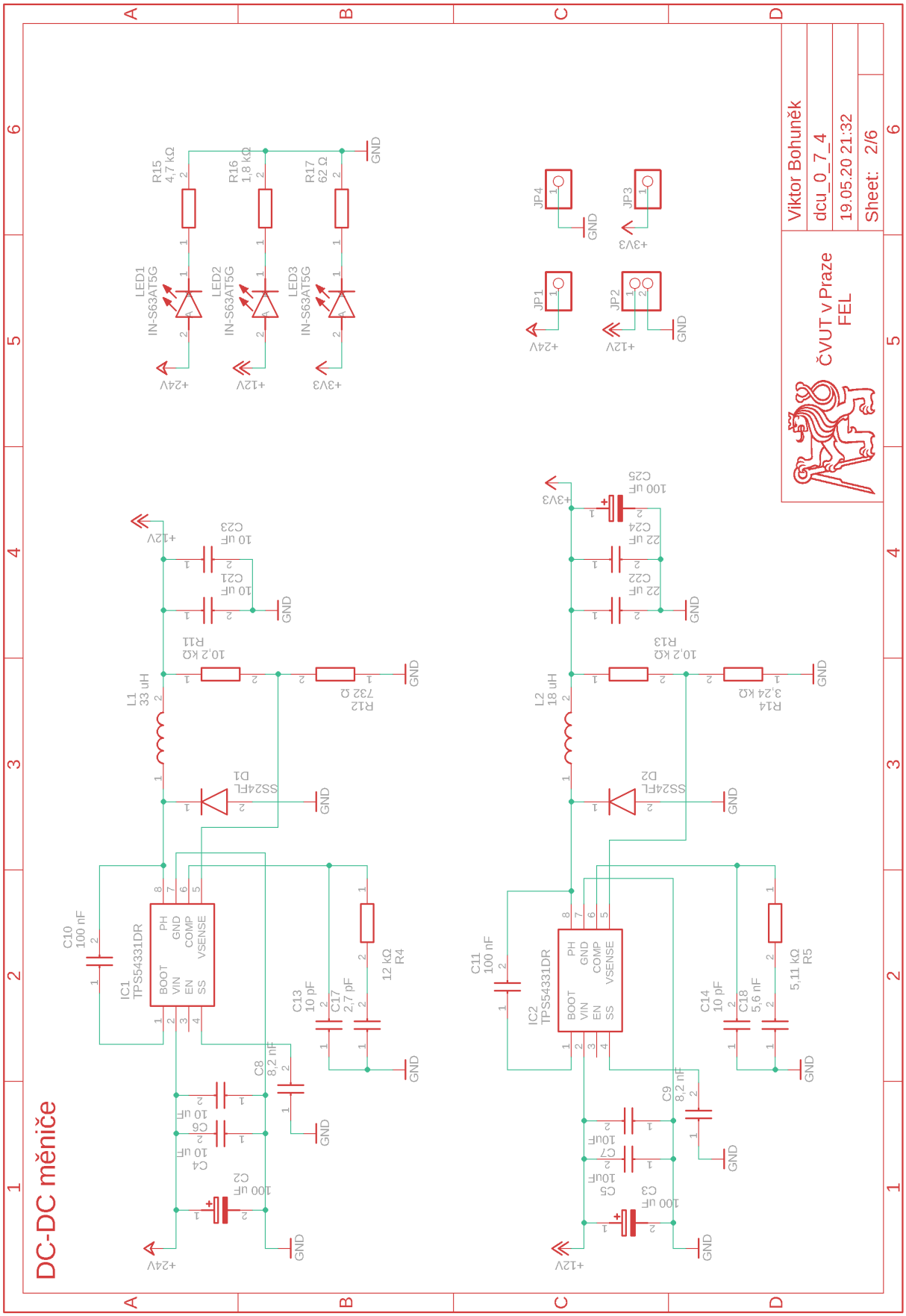
Obrázek A.1: Vrstva TOP motivu plošného spoje DCU



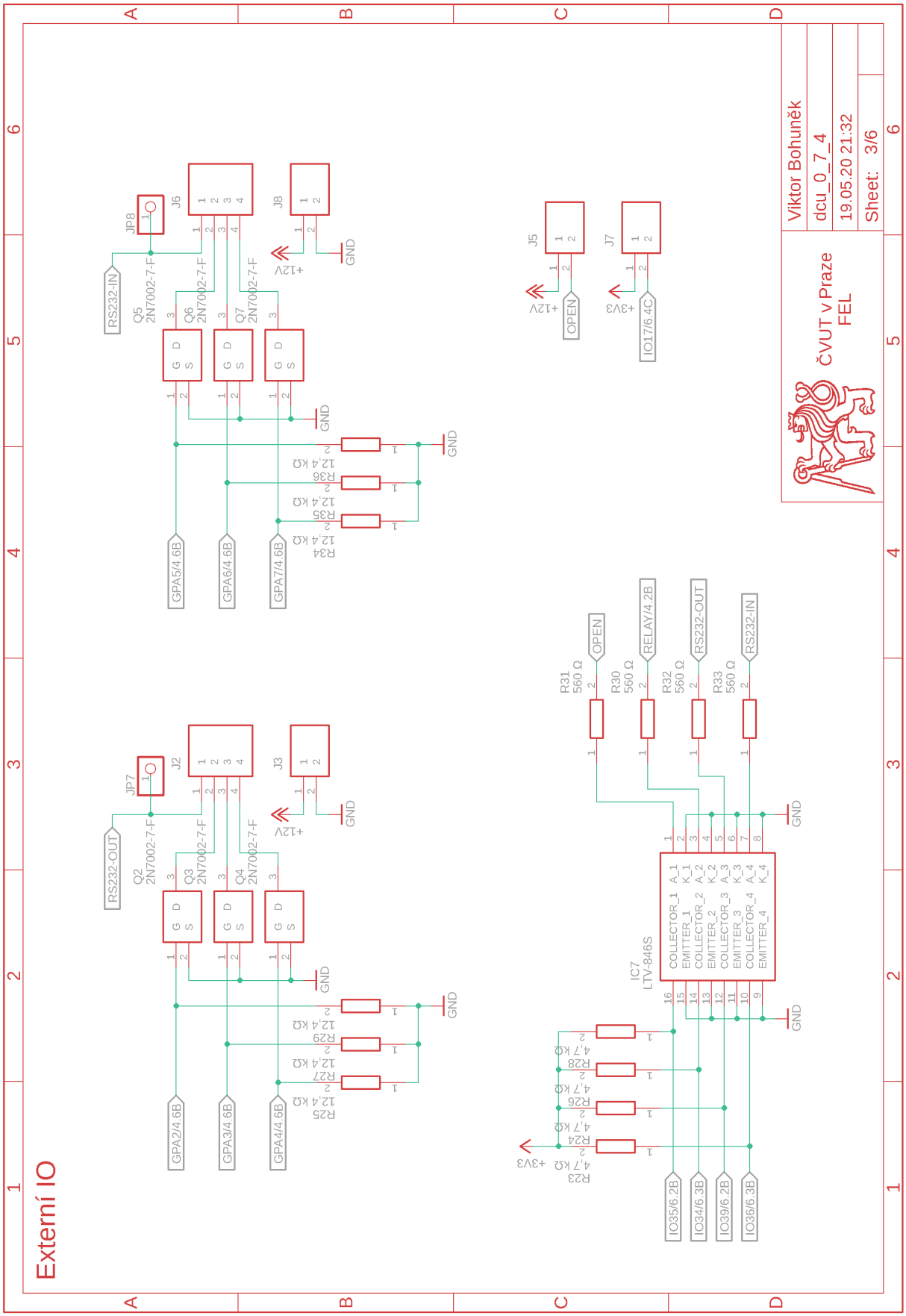
Obrázek A.2: Vrstva BOTTOM motivu plošného spoje DCU



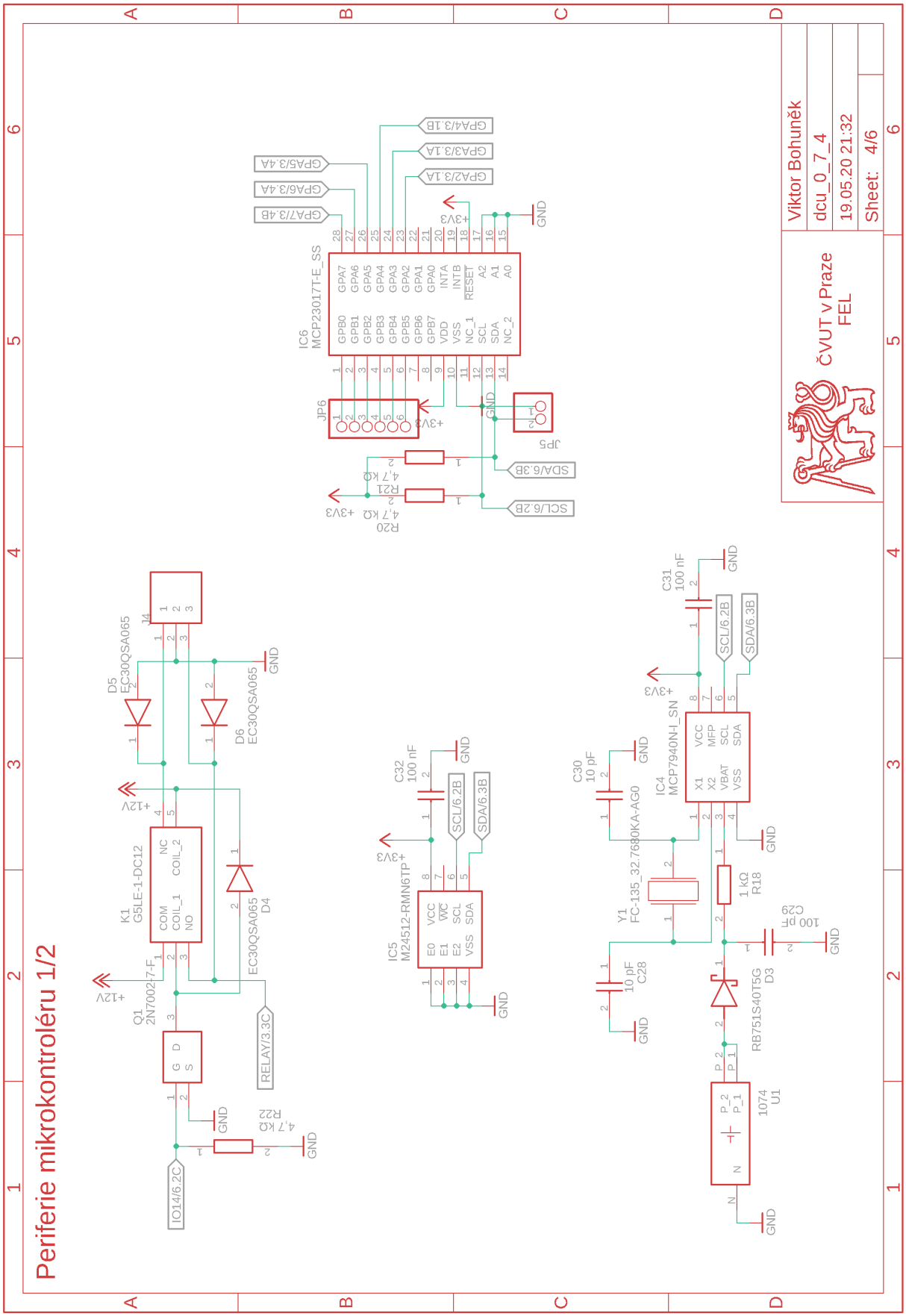
Obrázek A.3: Schéma zapojení DCU - List 1/6 - Konektor RJ-45



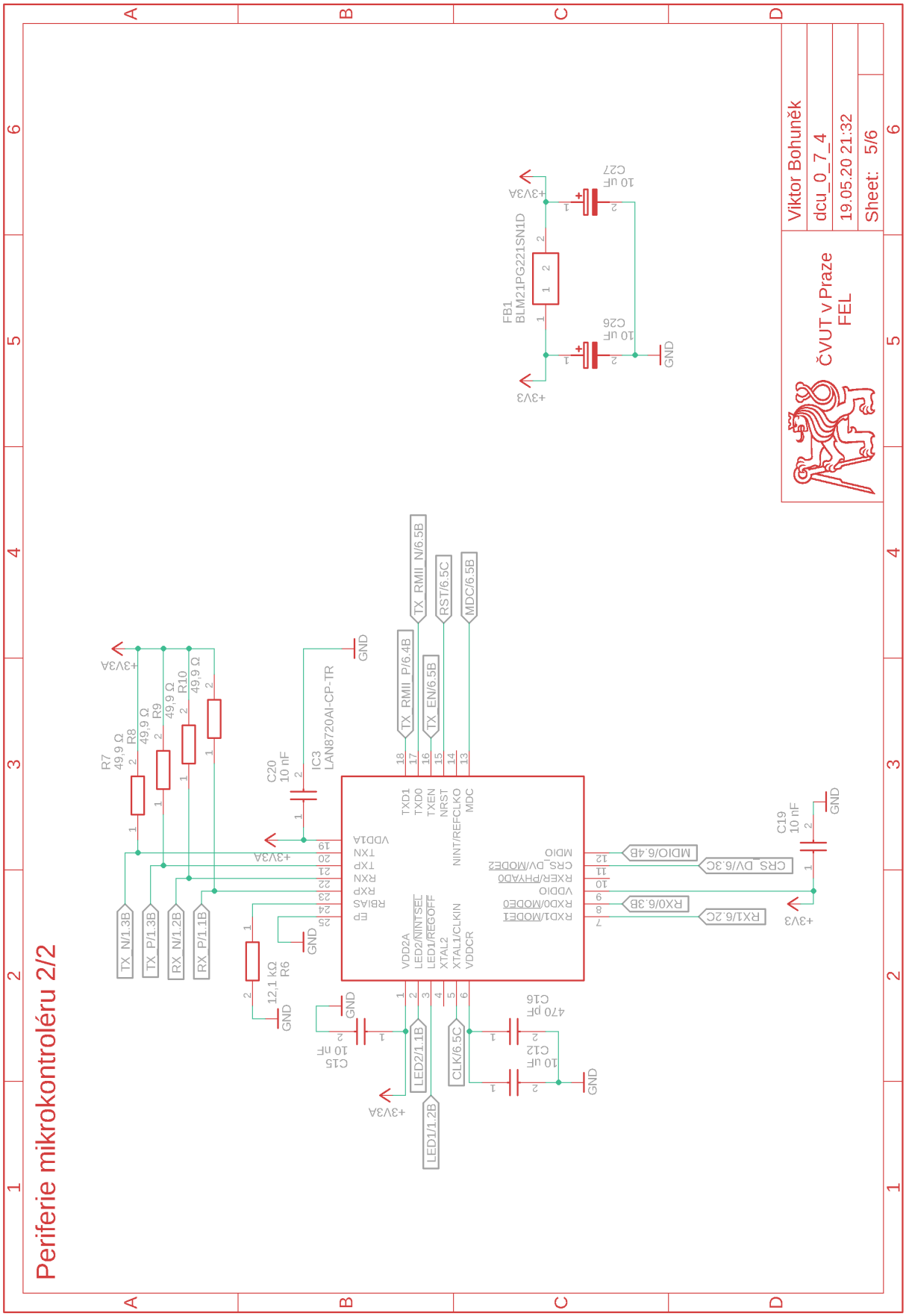
Obrázek A.4: Schéma zapojení DCU - List 2/6 - DC-DC měniče



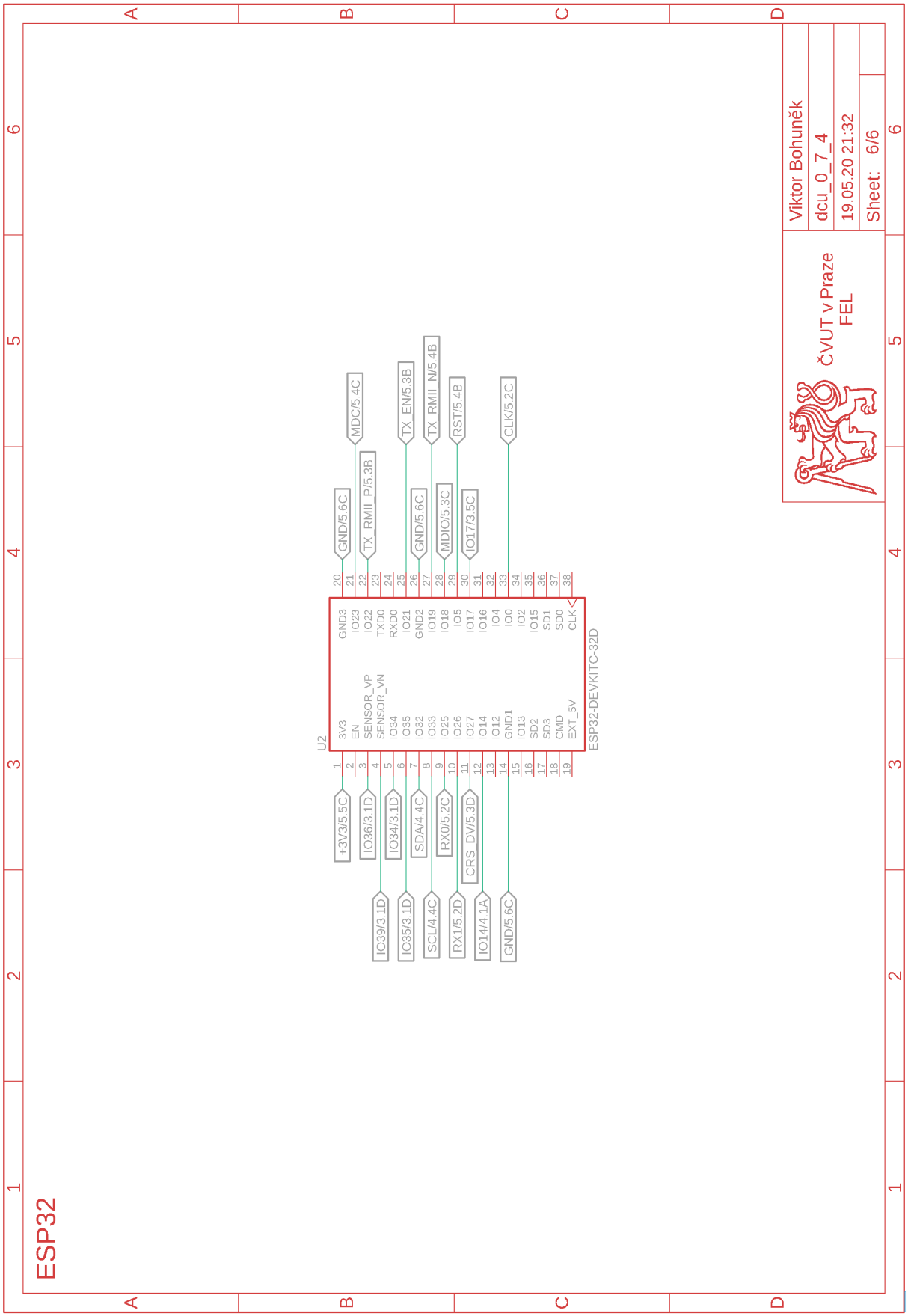
Obrázek A.5: Schéma zapojení DCU - List 3/6 - Externí IO



Obrázek A.6: Schéma zapojení DCU - List 4/6 - Periferie mikrokontroléru 1/2



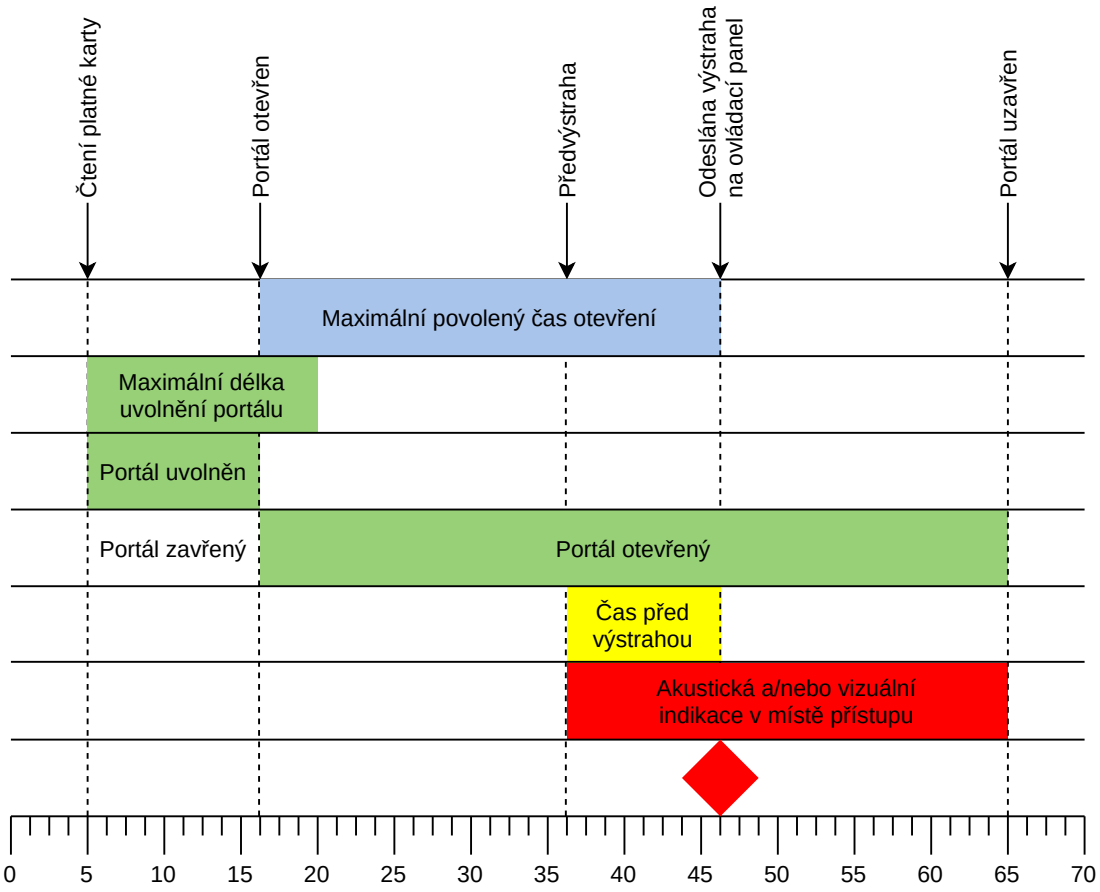
Obrázek A.7: Schéma zapojení DCU - List 5/6 - Periferie mikrokontroléru 2/2



Obrázek A.8: Schéma zapojení DCU - List 6/6 - ESP32

Příloha B

Ostatní obrázky



Obrázek B.1: Diagram časování uvolnění portálu, převzato z [32]