TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta zdravotnických studií

Návrh prototypu přístroje k zefektivnění komunikace mezi obsluhou zdravotnického přístroje a technicky znalé osoby

Bakalářská práce

Studijní program: B3944 Biomedicínská technika
Studijní obor: Biomedicínská technika

Autor práce: **Věra Šramhauserová**
Vedoucí práce: Ing. Jan Koprnický, Ph.D.
Ústav mechatroniky a technické informatiky

Liberec 2021

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta zdravotnických studií

Zadání bakalářské práce

Návrh prototypu přístroje k zefektivnění komunikace mezi obsluhou zdravotnického přístroje a technicky znalé osoby

Jméno a příjmení: **Věra Šramhauserová**
Osobní číslo: D19000114
Studijní program: B3944 Biomedicínská technika
Studijní obor: Biomedicínská technika
Zadávající katedra: Fakulta zdravotnických studií
Akademický rok: **2020/2021**

Zásady pro vypracování:

1. Proveďte rešerši používaných metod a způsobů komunikace užívaných v nemocnicích v ČR.
2. Navrhněte zařízení k zjednodušení komunikace mezi obsluhou přístroje (lékař/sestra/sanitář) a technicky znalé osoby (biomedicínským technikem / inženýrem / servisním technikem), které bude následně realizovatelné do podoby funkčního vzorku k testování (protoypu).
3. Navržený prostředek nebude zasahovat do autonomie přístrojů a bude možné zasílat stav přístroje stiskem tlačitka. Zaslaný stav by se měl zobrazovat na mobilním zařízení (smartphone, tablet, mobilní telefon) odpovědné osobě (technikovi).
4. Vyberte potřebný HW, sestavte zařízení a otestujte ho v laboratorních podmínkách (idálně na zdravotnickém přístroji).
5. Z testování protoypu v laboratorních podmínkách proveďte zápis.
6. Diskutujte o možných technických úpravách nezbytných pro nasazení navrženého přístroje do reálného provozu.

Rozsah grafických prací:
Rozsah pracovní zprávy:
Forma zpracování práce: tištěná/elektronická
Jazyk práce: Čeština

Seznam odborné literatury:

MALÝ, Martin. *Porty, bajty, osmibity: počítače na koleni.* Praha: CZ.NIC, 2019. ISBN 978-80-88168- 39-3.
MALÝ, Martin. *Hradla, volty, jednočipy: úvod do bastlení*. Praha: CZ.NIC, 2017. ISBN 978-80-88168- 24-9.
ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 75, s. 1926-1936. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirkazakonu/ViewFile.aspx?type=c&id=6688
ČESKO. Zákon č. 110 ze dne 12. března 2019 o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. 2019, částka 47, s. 890-911. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38632
ČESKO. Zákon č. 527 ze dne 27. listopadu 1990 o vynálezech, průmyslových vzorech a zlepšovacích návrzích. In: *Sbírka zákonů České republiky*. 1990, částka 86, s. 1952-1964. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=2397
ČESKO. Zákon č. 102 ze dne 22. února 2001 o obecné bezpečnosti výrobků a o změně některých zákonů (zákon o obecné bezpečnosti výrobků). In: *Sbírka zákonů České republiky*. 2001, částka 41, s. 2833-2838. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3619
ČESKO. Zákon č. 289 ze dne 16. června 2005 o Vojenském zpravodajství. In: *Sbírka zákonů České republiky*. 2005, částka 104, s. 5388-5393. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=4702
ČESKO. ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. Vyhláška č. 241 ze dne 27. června 2012 o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů. In: *Sbírka zákonů České republiky*. 2012, částka 82, s. 3232. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6211
ČESKO. MINISTERSTVO VNITRA. Vyhláška č. 386 ze dne 17. prosince 2015 o náležitostech kryptografických klíčů a autentizačního certifikátu. In: *Sbírka zákonů České republiky*. 2015, částka 163, s. 5347. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirkazakonu/ViewFile.aspx?type=c&id=15964
MAŘÍK, Vladimír et al. *Průmysl 4.0: výzva pro Českou republiku.* Praha: Management Press, 2016. ISBN 978-80-7261-440-0.
CIRANI, Simone et al. *Internet of Things: Architectures, Protocols and Standards*. Hoboken: John Wiley & Sons, 2018. ISBN 978-1-119-35967-8

Vedoucí práce: Ing. Jan Koprnický, Ph.D.
Ústav mechatroniky a technické informatiky

Datum zadání práce: 1. září 2020
Předpokládaný termín odevzdání: 30. června 2021

L.S.

prof. MUDr. Karel Cvachovec, CSc., MBA
děkan

V Liberci dne 30. listopadu 2020

Prohlášení

Prohlašuji, že svou bakalářskou práci jsem vypracovala samostatně jako původní dílo s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Jsem si vědoma toho, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu Technické univerzity v Liberci.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti Technickou univerzitu v Liberci; v tomto případě má Technická univerzita v Liberci právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Současně čestně prohlašuji, že text elektronické podoby práce vložený do IS/STAG se shoduje s textem tištěné podoby práce.

Beru na vědomí, že má bakalářská práce bude zveřejněna Technickou univerzitou v Liberci v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

Jsem si vědoma následků, které podle zákona o vysokých školách mohou vyplývat z porušení tohoto prohlášení.

17. května 2021 Věra Šramhauserová

Poděkování

Touto cestou bych ráda vyjádřila poděkování Ing. Janovi Koprnickému, Ph.D., za odborné vedení a všestrannou pomoc při zpracování bakalářské práce. Taktéž bych chtěla poděkovat Ing. Miloši Hernychovi za diskuzi k řešenému technickému pojetí problematiky této práce. Současně bych chtěla poděkovat Štěpánovi Bechynskému z firmy Microsoft za konzultace nejen k produktům z portfolia Microsoftu, ale i za mnohé rady k softwarové integraci prototypu. Zároveň musím poděkovat generálnímu řediteli Ing. Alanovi Fabikovi a technickému řediteli Pavlovi Hübnerovi z firmy HARDWARIO za nadstandardní přístup, pomoc s výběrem i sestavením hardwarové části navrhovaného prototypu zařízení. V neposlední řadě bych ráda poděkovala vedoucímu OZT Ing. Milanovi Hřebíkovi, DiS., za umožnění krátkodobého testování navrženého prototypu v ÚPMD.

Anotace v českém jazyce

Jméno a příjmení autora:	Věra Šramhauserová
Instituce:	Technická univerzita v Liberci

Název práce:	Návrh prototypu přístroje k zefektivnění komunikace mezi obsluhou zdravotnického přístroje a technicky znalé osoby
Vedoucí práce:	Ing. Jan Koprnický, Ph.D.
Počet stran:	89
Počet příloh:	3
Rok obhajoby:	2021
Anotace:	Bakalářská práce se zabývá návrhem a realizací prototypu zařízení pro usnadnění komunikace mezi obsluhou zdravotnického přístroje a osobou, která je schopna urychleně řešit závady (servisním technikem). V teoretické části jsou popsány metody a způsoby komunikace ve zdravotnických zařízeních v ČR. Dále se práce zabývá popisem vývojových desek, internetu věcí a s tím souvisejících komunikačních, zejména bezdrátových, technologií. Zvláštní pozornost je věnována sítím LPWAN, bezpečnosti při zpracování a přenášení dat. V praktické části je popsáno hardwarové řešení prototypu. Celé řešení je vytvořeno s velkým důrazem na nezbytnou bezpečnost. Postupně jsou představeny vybrané softwarové platformy užité v aplikační části prototypu včetně popisu nastavení. Prototyp koncového komunikačního zařízení je přenosný, nezasahuje do integrity zdravotnického přístroje, nevyžaduje připojení do počítačové sítě nemocnice a je napájený primárně z baterií. Zasílá zprávy po stisku tlačítka do mobilního zařízení odpovědné osobě (biomedicínský technik, biomedicínský inženýr). O zaslání zprávy je proveden a uložen záznam. Prototyp je otestován a následně diskutováno jeho nasazení do nemocničního zařízení.
Klíčová slova:	Zdravotnictví, Komunikace, Prototyp, Internet věcí, NB-IoT, CHESTER-Z, Microsoft Power Automate, Microsoft Teams

Annotation

Name and surname:	Věra Šramhauserová
Institution:	Technical University of Liberec

Title:	Design of a prototype device to streamline communication between the operator of a medical device and a technically knowledgeable person
Supervisor:	Ing. Jan Koprnický, Ph.D.
Pages:	89
Apendix:	3
Year:	2021
Annotation:	The bachelor's thesis is focused on design and implementation of a prototype device to facilitate communication between the operator of a medical device and a person who is able to quickly resolve faults (service technician). The theoretical part describes the methods and ways of communication in medical facilities in the Czech Republic. Furthermore, the work deals with the description of development boards, the Internet of Things and related communication, especially wireless, technologies. Special attention is paid to LPWAN networks, security in data processing and transmission. The practical part describes the hardware solution of the prototype. The whole solution is created with great emphasis on the necessary security. Gradually, selected software platforms used in the application part of the prototype are introduced, including a description of the settings. The prototype of the terminal communication device is portable, does not interfere with the integrity of the medical device, does not require connection to the hospital's computer network and is powered primarily by batteries. Sends messages after pushing a button to a mobile device to a responsible person (biomedical technician, biomedical engineer). A record of the sending of the message is made and saved. The prototype is tested and then discussed for use in a hospital facility.
Keywords:	Healthcare, Communication, Prototype, Internet of Things, NB-IoT, CHESTER-Z, Microsoft Power Automate, Microsoft Teams

Obsah

Seznam zkratek

3GPP	The 3rd Generation Partnership Project, dohoda o spolupráci v oblasti mobilních komunikací
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks, protokol IPv6 pro bezdrátové osobní sítě s nízkou spotřebou energie
AES	Advanced Encryption standard, standard pokročilého šifrování
AMQP(S)	Advanced Message Queuing Protocol, protokol
API	Application Programming Interface, rozhraní pro aplikace a jejich programování
ARM	Advanced RISC Machine, původní název je Acorn RISC Machine, architektura procesorů
atd.	A tak dále
AWS	Amazon Web Services
BLE	Bluetooth Low Energy, Bluetooth s nízkou spotřebou energie
BMI	Biomedicínský inženýr
BMT	Biomedicínský technik
BSON	Binary JSON, formát pro výměnu dat
CSS	Chirp spread spectrum
CE	Coverage extension, rozsah pokrytí
CIoT	Consumer Internet of Things, spotřební internet věcí
CMOS	Complementary Metal–Oxide–Semiconductor, architektura logických členů
CoAP	Constrained Application Protocol, síťový protokol
CPU	Central processing unit, centrální procesorová jednotka
ČR	Česká republika
ČTÚ	Český telekomunikační úřad
DAS	Data Acquisition Systems, systém pro sběr dat
DC	Direct current, stejnosměrný elektrický proud
DDS	Data Distribution Service, protokol
DES	Data Encryption Standard, symetrická šifra
DNS	Domain Name System, protokol
EDGE	Enhanced Data for GSM Evolution, vývojový stupeň GSM
ESP	Typ vývojové desky
FBI	Federal Bureau of Investigation, Federální úřad pro vyšetřování
FCC	Federal Communications Commission, federální komunikační komise
FiRa	Fine ranging, konsorcium
FSK	Frequency-shift keying, klíčování frekvenčním posuvem
FTP	File Transfer Protocol, protokol
FZS	Fakulta zdravotnických studií Technické univerzity v Liberci
GET	Metoda HTTP protokolu
GNSS	Global Navigation Satellite System, Globální navigační satelitní systémy
GPIO	General Purpose Input and Output, Univerzální vstupní-výstupní pin

GPRS	General Packet Radio Service, mobilní datová služba
GPS	Global Positioning System, družicový polohový systém
GSM	Groupe Spécial Mobile, standard pro digitální mobilní sítě
HAL	Hardware Abstraction Layer, knihovna pro software STM32
HDMI	High-Definition Multimedia Interface, nekomprimovaný obrazový a zvukový signál v digitálním formátu
HF	High-Frequency, vysokofrekvenční
HMI	Human machine interface, rozhraní mezi člověkem a strojem
HPWAN	High Power Wide Area
HSDPA	High-Speed Downlink Packet Access, standard
HSPA+	Evolved High Speed Packet Access, standard
HTML	Hypertext Markup Language, značkovací jazyk
HTTP(S)	Hypertext Transfer Protocol, internetový protokol
IBM	International Business Machines Corporation
ICSP	In Circuit Serial Programming, programování po sériové lince mikrokontroléru
ID	Identity, identita
IDE	Integrated Development Environment, Arduino software
IEC	International Electrotechnical Commission, Mezinárodní elektrotechnická komise
IEEE	Institute of Electrical and Electronics Engineers, Institut pro elektrotechnické a elektronické inženýrství, označení některých standardů
IIoT	Industrial Internet of Things, průmyslový internet věcí
IoT	Internet of Things, Internet věcí
IP	Internet protokol
IPv6	Internet Protocol version 6, internetový protokol verze 6
IS	Informační systém
ISM	Industrial, scientific and medical, pásmo pro rádiové vysílání
ISO	International Organization for Standardization, Mezinárodní organizace pro normalizaci
ISO/OSI	Open System Interconnection model, OSI Reference Model, OSI Model, model pro komunikaci a spolupráci počítačových systémů pomocí standardních protokolů
ITU	International Telecommunication Union, Mezinárodní telekomunikační unie
I^2C	Internal-Integrated-Circuit Bus, datová sběrnice
JSON	JavaScript Object Notation, formát pro zápis dat
LAN	Local Area Network, místní počítačová síť
LED	Light-Emitting Diode, světlo emitující dioda
LF	Low-Frequency, nízkofrekvenční
LoRaWAN	Long Range Wide Area Network, síť dlouhého dosahu
LPWAN	Low Power Wide Area Network, Sítě dlouhého dosahu s nízkou energetickou náročností
LTE	Long Term Evolution, technologie vysokorychlostního internetu
LwM2M	Open Mobile Alliance Lightweight M2M, odlehčený síťový protokol

MCL	Maximum Coupling Loss, ztráta na výkonu
MCU	Microcontroller unit, jednočipový počítač
MicroSD	Micro Secure Digital paměťová karta
MIPI CSI	MIPI Camera Serial Interface, MIPI sériové rozhraní fotoaparátu
MIPI DSI	MIPI Display Serial Interface, MIPI sériové rozhraní displeje
MIT	Massachusettský technologický institut
MQTT	Message Queuing Telemetry Transport, síťový protokol
MTU	Maximum transmission unit, maximální velikost IP datagramu
M2M	Machine to machine, komunikace stroj-stroj
M365	Microsoft 365
NB-IoT	Narrowband IoT, úzkopásmový internet věcí
NFC	Near Field Communication, rádiová bezdrátová komunikace na krátké vzdálenosti
NIS	Nemocniční informační systém
NoSQL	Non-Relational Databases, druh databáze
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OASIS	The Organization for the Advancement of Structured Information, mezinárodní konsorcium
OPC-UA	Open Platform Communications–Unified Architecture, protokol
OS	Operační systém
OSN	Organizace spojených národů
OZT	Oddělení zdravotechniky
PATCH	Metoda HTTP protokolu
PC	Počítač
PLC	Programmable logic controller, programovatelný logický automat
POST	Metoda HTTP protokolu
PUT	Metoda HTTP protokolu
QoS	Quality of Service, kvalita služeb
RAM	Random Access Memory, paměť s náhodným přístupem
REST	Representational State Transfer, druh architektury rozhraní
RF	Radiofrequency, radiofrekvence
RFID	Radio Frequency Identification, radiofrekvenční identifikace
RSRP	Reference Signal Received Power, intenzita signálu
SaaS	Software as a Service, software jako služba
SASL	Simple Authentication and Security Layer, metoda pro ověřování v protokolech klient/server
SDK	Software Development Kit
SIM	Subscriber identity module
SINR	Signal to Interference plus Noise Ratio, kvalita signálu spolu s okolním rušením
SMS	Short message service, služba krátkých textových zpráv
SPI	Serial Peripheral Interface, sériová externí sběrnice
SRD	Short range devices, zařízení krátkého dosahu
SSL	Secure Sockets Layer, kryptografický protokol
SW	Software

TCP/IP	Transmission Control Protocol/Internet Protocol, primární přenosový protokol/protokol síťové vrstvy, skupina protokolů pro komunikaci v PC síti
tj.	To jest
TLS	Transport Layer Security, kryptografický protokol pro zabezpečenou komunikaci na internetu
TTL	Transistor-transistor-logic, tranzistorově-tranzistorová logika
TUL	Technická univerzita v Liberci
tzv.	Tak zvaný
UART	Universal asynchronous receiver-transmitter, univerzální asynchronní přijímač a vysílač, počátačová sběrnice
UDP/IP	User Datagram Protocol/Internet Protocol, skupina protokolů pro komunikaci v PC síti
UHF	Ultra-High Frequency, ultra krátké vlny
UMTS	Universal Mobile Telecommunications System, standard
UNB	Ultra Narrow Band, úzkopásmový přenos signálu
URL	Uniform Resource Locator, doménová adresa serveru
USA	United States of America, Spojené státy americké
USB	Universal Serial Bus, univerzální sériová sběrnice
UWB	Ultra WideBand, Ultra-širokopásmová síť
ÚPMD	Ústav pro péči o matku a dítě
ÚZIS	Ústav zdravotnických informací a statistiky
VOC	Volatile organic compound, pohyblivé organické sloučeniny
VoIP	Voice over Internet Protocol, protokol
WAP	Wireless Application Protocol
WiFi	Wireless Fidelity, označuje několik standardů pro bezdrátovou komunikaci
WLAN	Wireless Local Area Network
WNAN	Wireless Neighborhood Area Network
WPAN	Wireless personal area network
WSS	WebSocket Secure, protokol
WWAN	Wireless Wide Area Network
XML	Extensible Markup Language, značkovací jazyk

1 Úvod

Zdravotnictví je místo v němž se setkává mnoho různých oborů lidské činnosti se společným cílem. Zachraňovat lidské životy. Rychlý technický vývoj, zejména rozšiřující se a akcelerující digitalizace a automatizace, poskytuje možnosti pro hledání nových technických výzev, realizaci nových postupů a jejich využití ve zdravotnických zařízeních tak, aby přispěly k zefektivnění servisu, analýze zdravotnických přístrojů, usnadnění a zlepšení pracovních podmínek a výsledků.

Cílem bakalářské práce je navrhnout prototyp přístroje k zkvalitnění a zrychlení komunikace mezi osobou pracující se zdravotnickým přístrojem, jakou může být lékař, zdravotní sestra, sanitář či radiologický asistent, a technicky znalou osobou tj. biomedicínským technikem, biomedicínským inženýrem nebo servisním technikem. S návrhem zařízení je navrhován celý komunikační koncept od hardwarového po softwarové řešení. Záměrem bakalářské práce je přispět k řešení situace, zaznamenané v reálném provozu zdravotnického zařízení, kdy je v kritické situaci nutné ihned uvědomit odpovědnou osobu, technika, včetně uložení záznamu o tomto hlášení a co nejrychleji odstranit poruchu. Prototyp je navržen s ohledem na specifické požadavky plynoucí z podstaty zdravotnického zařízení. Navrhovaný prototyp zařízení by měl doplnit stávající komunikační metody, mezi které patří systém žádanek, emailová a telefonická komunikace. Díky zvolenému systému komunikace není prototyp připojen do počítačové sítě zdravotnického zařízení. Tím je zaručena nemožnost zneužití prototypu pro kybernetický útok na nemocniční systémy. V případě kritické poruchy nemocničního přístroje či jakéhokoli jiného nezbytného prostředku pro výkon práce (ošetření, vyšetření pacienta), je jedním stiskem tlačítka přivolána odborná technická pomoc. Po stisku tlačítka integrovaného v prototypu zařízení je poslána informace o naléhavosti technického zásahu při vážné situaci technikovi. Pro zasílání informace je maximální snaha využít stávajících aplikací, tj. již zdravotnickým zařízením vlastněných. Není nutné zakoupit nový produkt, odpadá povinnost školit uživatele a z toho vyplývají vysoké finanční a časové úspory. Zaslaná zpráva se technikovi zobrazí na mobilním zařízení, což sníží dobu nutnou k reakci na vzniklou vážnou situaci. Mobilním zařízením se rozumí smartphone, tablet či mobilní telefon. Navrhovaný prototyp zařízení nezasahuje do integrity zdravotnického přístroje a současně je realizován do podoby funkčního vzorku k testování.

Práce je rozdělena na dvě oblasti. První je část teoretická, druhá pak praktické sestavení a testování prototypu. Teoretická část práce je věnována rešerši metod a způsobů komunikace užívaných ve zdravotnických zařízeních v ČR. Následuje základní přehled dostupných vývojových desek, úvod do internetu věcí a bezdrátových technologií pro internet věcí s důrazem na sítě dlouhého dosahu s nízkou energetic-

kou náročností (LPWAN). Významnou kapitolou je bezpečnost a základní přehled komunikačních protokolů. Praktická část se věnuje výběru vhodného hardwaru, sestavení hardwarové části prototypu zařízení a navržení komunikační struktury. Dále jsou popsána vybraná softwarová řešení a aplikační část prototypu zařízení. Prototyp zařízení je otestován v laboratorních podmínkách v rámci praktické části. Z testování je proveden zápis a v závěrečné kapitole je vedena diskuze o možných technických úpravách nezbytných pro nasazení navrženého prototypu přístroje do reálného provozu.

2 Komunikace ve zdravotnických zařízeních v ČR

Zdravotnické zařízení, nemocnice, je specifické prostředí. Na jednom místě se setkává mnoho různých oborů lidské činnosti, aby společně poskytovaly nejlepší možnou péči klientům. Základem úspěšné spolupráce a dosahování kvalitních výsledků není jen samotné vzdělání jednotlivců nýbrž i komunikace. Spolu s rozvojem technologií, který započal v šedesátých letech minulého století, se postupně rozšiřovaly možnosti sdílení informací, bezpečné nakládání s daty pacientů, rozrůstal se počet přístrojů užívaných k podpoře a léčbě pacientů i metody, jak se o tyto přístroje starat. To, co začínalo v podobě papírových kartoték na všech odděleních zdravotnických zařízení, dnes zastřešují tzv. informační a komunikační systémy pro zdravotnictví užívající výpočetní techniku.

Pro pochopení tohoto odvětví je potřeba se zorientovat v následujícím dělení informačních systémů ve zdravotnictví. Samotné odvětví IS je progresivně rozvíjející se obor díky rychlému vývoji výpočetní a komunikační techniky a zároveň její rozumné dostupnosti. Informační a komunikační systém jako takový nabízí možnost sběru, ukládání, zpracování a vyhodnocování dat pro řízení a rozhodování [1, 2]. Aktuálně užívané informační systémy jsou navrhovány pro jednotlivé typy cílových skupin. Komplexně navržený informační a komunikační systém pro administrativu, klinické údaje a řízení financí se označuje jako nemocniční informační systém (NIS) [3]. Ve stejné kategorii, jako je NIS můžeme nalézt IS zdravotních pojišťoven, státních institucí (záchranná služba, Ministerstvo zdravotnictví ČR, ÚZIS ČR, hygienické stanice), pro praktické lékaře existují ambulantní IS. Dále jsou k dispozici speciální IS pro lázeňské provozy, psychiatrická a rehabilitační zařízení. IS užívají i zdravotní registry a systém pro domácí zdravotní péči [4].

Nemocniční informační systém respektuje strukturu nemocnice a dělí se na moduly [4]. Tyto moduly jsou navrhovány pro jednotlivé správní agendy. Nejrobustnějším a nejpodstatnějším modulem obvykle bývá klinický IS. Do něho se shromažďují data a záznamy o pacientech. Dalšími, velice častými moduly jsou: Lékárna, Logistika a skladové hospodářství, IS pro stravovací provoz, Ekonomický IS, Radiologický IS, Laboratorní IS, IS pro správu zdravotnické techniky [5, 8, 7, 6].

Dalším způsobem, jak lze popsat způsoby komunikace ve zdravotnických zařízeních, je dělení z pohledu zaměstnance. Pro účely této bakalářské práce bude toto dělení podstatnější. Pro zaměstnance zdravotnického zařízení existuje čtyři až pět možností, jak interagovat s okolím. Osobní kontakt a telefonické hovory bývají účelné, ovšem nezůstává o nich záznam v systému. Z toho pohledu jsou pro mnohé

aktivity nevhodné, především, pokud nemocnice má uveřejněné směrnice, v nichž se obvykle ustanovuje, že tyto rozhovory jsou pouze informačního druhu. E-mailová komunikace zanechává záznam včetně identifikace zaměstnance (jeho počítače), jedná se o efektivní nástroj. Jakákoli žádost musí být ovšem autorizována a zaznamenána. K tomu slouží žádankové systémy v nabízených softwarech modulů NIS [9]. Posledním podstatným druhem je soubor komunikačních a signalizačních systémů pro zdravotnictví a sociální sféru, na trhu známo jako systémy SESTRA–PACIENT.

3 Žádankový systém a systémy SESTRA–PACIENT

Moduly NIS (nemocniční informační systém) nabízejí možnost zakládat nové žádanky do systému. Tímto způsobem se objednává materiál ze skladů nemocnice, opravy a servis zdravotnických přístrojů atd. Podstatná výhoda takto zaznamenaných žádostí je prokazatelnost, uchovávání historie požadavků a jejich řešení, snadnější vykazovatelnost práce, zpřístupnění podstatných informací aj. Stav zadané žádanky lze sledovat, obvykle se zobrazují změny odeslaná/přečtená/v řešení/vyřešená/stornovaná [7].

Systémy SESTRA–PACIENT, jak plyne z názvu, jsou určeny pro komunikaci mezi zdravotnickým personálem nemocnice a samotným pacientem. Na trhu jsou k dispozici dva typy řešení. Převládajícím technickým řešením těchto systémů je užití IP adresace zařízení (internet protokol) [14, 10, 13, 11, 12]. Zařízení komunikují pomocí LAN. Klasické schéma sestává z terminálu pro personál (umístěn na sesterně), komunikačních jednotek (obvykle na zdi v pacientském pokoji), lůžkových jednotek (každé lůžko) a jednotek s táhly (vana, sprcha, záchod) pro případ pádu pacienta, volitelně signalizační svítidla. Komunikaci umožňuje hvězdicové propojení přes datový rozvaděč (switch) s přepínačem. Prvotní instalace komunikačního systému vyžaduje stavební úpravy. Výměny koncových prvků jsou díky stavebnicovému řešení výrobců nenáročné.

Druhým řešením pro komunikaci je užití bezdrátových zařízení [15, 10]. Výrobců těchto rádiově komunikujících zařízení je na trhu méně. Tato zařízení nacházejí uplatnění především v provozech, kde není možno dělat stavební úpravy nebo je nutné dočasné řešení. Topologické schéma je bod–bod (pear to pear) a skládá se z kapesní jednotky, kterou je nutno dobíjet, dále z tlačítek pro pacienty, jednotek s táhlem a případně rádiového opakovače. Rádiové řešení je jednosměrné a umožňuje pouze signalizaci, volání o pomoc, nikoli telefonní hovory jako tomu je u systémů s adresami IP. U systémů postavených na TCP/IP je přenosovým médiem většinou hvězdicová topologie strukturované kabeláže kategorie 5, což umožňuje přenos dat ve větších rychlostech a objemech.

4 Internet věcí

Internet věcí, často uváděn pod zkratkou IoT z anglického Internet of Things, označuje připojení zařízení k internetu tak, aby vzájemně komunikovala a vyměňovala si data, zároveň jsou monitorovatelná a/nebo ovládatelná na dálku. Zařízení IoT je jakákoli samostatná věc (objekt), které je jednoznačně adresovatelné a komunikuje nejčastěji po adresách IP sítě většinou podle standardizovaných komunikačních protokolů, přičemž se očekává, že nad výměnou a sdílením dat může vznikat analýza, která přispěje ke zvýšení přidané hodnoty propojeného ekosystému. Příkladem může být motor, který odesílá údaje o provozní teplotě. Tato data se vyhodnocují, zda motor pracuje správně a zároveň se efektivně plánuje údržba, správa náhradních dílů. Internet věcí se rozdělil na dva hlavní směry:

- IIoT – Industrial Internet of Things, využití v průmyslové oblasti
- CIoT – Consumer Internet of Things, spotřební sektor

Mezi IIoT aplikace patří především průmyslová automatizace, dopravní průmysl, zdravotnictví [16], energetický a chemický průmysl. Speciální kategorií v rámci IIoT je koncept Smart city, chytré město, který si vytyčil za cíl efektivně využívat nové i stávající zdroje, snižovat spotřebu energie a zátěže životního prostředí, účelně užívat sdílená data pro veřejné účely a optimalizovat dopravu.

Architektura IoT se skládá ze čtyř podstatných bloků. Prvním stavebním blokem architektury je použití senzorů, akčních členů a zařízení. Ty sbírají a zpracovávají data, která následně odesílají po komunikační síti. Tím se vytvoří fyzická vrstva, hardware, ve skutečném prostředí. Jakmile je snímací vrstva umístěná správným způsobem, následuje zřízení internetové/síťové brány (gateway). Data snímaná senzory a aktuátory jsou v analogové formě. Systém sběru dat, označovaný DAS z anglického Data Acquisition Systems, provádí agregaci a konverzi sesbíraných dat z analogového formátu na digitální. Pokročilé gatewaye (brány), primárně otevírající spojení mezi senzorovými sítěmi a internetem, mohou provádět filtrování, ochranu před malwarem, případně na základě zadaných požadavků i správu dat. Následuje vrstva pro zpracování dat, zde se předzpracovávají a analyzují před tím, než jsou odeslána do datového centra. Poslední fází je správa dat v datovém centru, cloudovém serveru nebo na lokálním úložišti [17]. Zde jsou data spravována a využívána koncovými uživateli, jakými je průmysl, zdravotnictví, zemědělství nebo dopravní sektor. IoT platformy jsou produktem softwarových firem, mezi nejvýznamnější platformy patří produkty firem AWS, Cisco, IBM, Microsoft a Oracle (řazeno abecedně).

5 Bezpečnost

Bezpečnost bezdrátové komunikace je rozsáhle diskutovaným tématem. S připojením jakéhokoli zařízení do internetu je potřeba počítat s možností napadení a potenciálního ohrožení. S daty na internetu lze provést tři věci: ukradnout je, upravovat je a omezit či znemožnit přístup majiteli dat [18]. Jsou zaznamenány případy, kdy jedno nezabezpečené zařízení připojené do vnitřní zabezpečené sítě způsobilo rozsáhlé škody na datech v síti. Typickým zástupcem může být USB flash disk z neznámého zdroje, který je připomínán zaměstnancům firem po celém světě. S rozšiřující se digitalizací a automatizací významně přibývá nových a mnohdy neočekávaných chyb v zabezpečení, které bývají opraveny až po jejich zneužití a způsobení nemalých škod. Za chyby v zabezpečení nesou zodpovědnost stejnou měrou jak samotní výrobci hardwaru, vývojáři softwaru, tak samotní uživatelé, kteří mohou svým přístupem mnohé hrozby eliminovat.

Významnými světovými deníky, jako je Forbes [19] a The Washington Post [20], ale i odbornými médii (např. The Hacker Post [21]) byl v roce 2017 zpopularizován případ napadení kasina pomocí senzoru do akvária, který byl připojen do internetu. Tento senzor reguloval teplotu a čistotu vody přičemž zafungoval jako vstupenka do ostatních částí sítě kasina a umožnil loupež citlivých dat. Název kasina ani typ uloupených dat nebyl zveřejněn. Napadení kasina bylo zveřejněno jen několik dní poté, co FBI varovala rodiče před rizikem souvisejícím s ochranou hraček připojených k internetu [22]. Ty mohou posloužit jako nekončící zdroj soukromých údajů o dítěti, jako je jméno, GPS poloha či osobní preference.

Mnozí výrobci se zaměřují především na výkon a použitelnost IoT zařízení přičemž „velkoryse“ přehlížejí bezpečnostní opatření a šifrovací mechanizmy, čímž se stávají snadným terčem pro útok. Ve snaze projektovat levná, miniaturní IoT zařízení nebývá dostatek kapacit nebo financí pro projektování v prvé řadě bezpečných IoT zařízení. První chyba se dělá už při výběru procesoru, kdy ty jednoduché dokáží číst a posílat data, nemají však dostatečný výkon k provádění matematických operací potřebných pro šifrování. Uživateli tak nezbývá mnoho variant, jak se chránit před různými druhy kybernetických hrozeb plynoucích z podstaty slabého či nulového zabezpečení. Nejlepším způsobem je připojovat k síti pouze nezbytná zařízení a to taková, která používají zabezpečenou komunikaci s využitím k tomu určených protokolů.

Z bezpečnostního hlediska mohou mít přidanou hodnotu zařízení, která nevyužívají připojení k IP síti a komunikují například pomocí bezdrátové komunikace, RS-232, RS-485 nebo jiné sítě využívané v průmyslu. Do internetu jsou následně připojena přes gateway [23], která je typicky PC a která je zabezpečená. Brána, jak

zní český název, propojuje dvě sítě pracující s odlišnými komunikačními protokoly. Bránu si lze zjednodušeně představit jako most mezi senzory/aktuátory a samotným internetem. Brána též může sloužit jako vyrovnávací paměť s lokálním uložením dat pro případ výpadku sítě, čímž předchází ztrátě měřených dat. Poskytuje sofistikované zabezpečovací techniky za pomoci tzv. secure elements, hardwarových čipů, které dokáží vytvořit zabezpečené konfigurace přímo na hardwarové úrovni a zabrání tak úniku dat či neoprávněnému přístupu k zařízením.

6 Dostupné vývojové desky s MCU

Vzhledem k stálé platnosti Mooreova zákona, prvně vyřčeného roku 1965, není s podivem, že se nabídka vývojových desek rozrůstá. Výrobci vývojových desek se přizpůsobili poptávce a proto jsou na trhu nabízeny desky pro amatérské použití, kde mnohdy výrobce poskytuje své know-how pod open source licencí, ale i široká základna uživatelů, komunita, která sdílí své projekty. To napomáhá dalšímu rozšiřování popularity a základny uživatelů. Pokud má daná procesorová deska velké množství dostupných podpůrných materiálů, jako návody, kódy, dokonce i literaturu a zároveň je cena desky dostupná, je jisté, že si najde mnohé kupce. Vývojovou deskou se rozumí deska osazená mikrokontrolérem (MCU), s plošnými spoji, s mikroprocesorem a dalšími součástkami, včetně logiky nutné k programování. Mezi taková zařízení s otevřenou architekturou patří světově známé Arduino, micro:bit či Raspberry Pi.

Na opačném konci spektra se nacházejí profesionální zařízení označovaná jako PLC (Programmable Logic Controller). Programovatelný logický automat je malý průmyslový počítač, který je schopen převzít řízení procesů a ovládání strojů. Klasické PLC je robustnější konstrukce s uzavřenou architekturou. Své místo má v průmyslové automatizaci a rozvoji robotiky, tak i v jiných odvětvích než ve výrobě. Tato zařízení splňují přísné standardy kladené na kvalitu hardwarových komponent i na softwarovou spolehlivost. Životnost těchto zařízení se počítá na roky při stálém vytížení.

Mezi těmito dvěma póly, amatérské vývojové desky versus PLC, se nachází široká nabídka desek [24]. Ty se liší především procesory, komunikačními rozhraními, operační pamětí a z toho odvíjejícím se výkonem, kvalitou hardwarových součástek a cenou. Rozhodujícím faktorem pro výběr vhodné vývojové desky je vždy zohlednění požadovaných funkcí, plánovaného prostředí, kam bude zařízení nasazeno a finanční stránky.

6.1 Arduino

Jedna z nejznámějších vývojových desek s mikrokontroléry pro amatérské použití, vyvíjená od roku 2005 v Itálii. V Interaction Design Institute ve městě Ivrea byl vytvořen jednoduchý a levný vývojový set pro studenty jako alternativa k drahé, a v té době rozšířené, vývojové desce BASIC stamp. Arduino se rozšířilo po celém světě a stále se rozšiřuje nabídka jednotlivých modelů, různorodost procesorů a komunikačních rozhraní. Jedná se o open source projekt, tj. že všechna schémata jsou volně přístupná společně s návody. Arduino je elektronická platforma sestávající se

z jednoduché počítačové desky s procesorem a vývojového prostředí sloužícího k psaní softwaru [25]. Rozšiřující desky pro Arduino se nazývají Arduino Shieldy. Shieldy sbírají údaje ze senzorů či snímačů a na základě zjištěných informací ovládají výstupy. Na vytvoření programu pro Arduino mikrokontrolér použijeme programovací jazyk Wiring, který vychází z programovacího jazyka C++, a Arduino software. Arduino software, často zkracován na IDE je otevřený systém umožňující snadné psaní kódu a jeho nahrávání do mikrokontroléru. IDE 1.8.13 je dostupné ke stažení online na oficiálních stránkách Arduino. Program je navržen pro systémy Windows, macOS a Linux. Prostředí je napsáno v programovacím jazyce Java. Program je kompatibilní s deskami na trhu i s libovolnými Arduino Shieldy. K instalaci jsou k dispozici i starší verze IDE, specializované verze pro Linux nebo nejnovější Arduino IDE 2.0 beta verze (2.0.0-beta.4) [26]. Nejvýznamnějším modelem je Arduino UNO osazené jednočipovým počítačem ATmega328. Ten provádí program, který na něj byl nahrán. Deska obsahuje 14 digitálních vstupních/výstupních pinů, 6 analogových vstupů, 16MHz krystal, připojení pomocí USB, napájecí konektor, ICSP rozhraní a resetovací tlačítko.

6.2 Raspberry Pi

Raspberry Pi, RPi, je jednodeskový počítač osazený ARM procesorem. Nabízí široké možnosti pro multimediální využití. Za devět let od prvního uvedení se již vyvinul do čtvrté generace. Za tu dobu se rozrostly možnosti konektivity, rozhraní. Čtvrtá generace umožňuje připojení k WiFi na 2,4 GHz a 5 GHz IEEE 802.11.b/g/n/ac, podporuje Bluetooth 5.0, Gigabitový Ethernet (1000 Mbit/s) a nabízí dva USB 2.0 konektory a dva USB 3.0 konektory. Ze dvou HDMI ve třetí generaci se ve čtvrté staly 2 microHDMI 2.0 konektory. Pro připojení displeje je k dispozici MIPI DSI konektor, pro kameru MIPI CSI. Dále čtyřpólový 3,5mm jack pro výstup zvuku. Bez změny zůstal standardní GPIO konektor [27]. Na MicroSD kartu je nutné nahrát operační systém kompatibilní k ARM platformě. Typická nabídka obsahuje varianty Linuxu, nejčastěji Raspberry PI OS, verze Debianu navržená přímo pro Raspberry Pi, Androidu, vzácněji speciální edice Windows. Tak jako Arduino, i Raspberry Pi vznikla pro účely výuky, tentokrát v Anglii, jako dostupný nástroj k výuce programování. Pro nenáročného uživatele může pracovat jako stolní počítač. Rasbian Linux má již předinstalované některé aplikace jako je webový prohlížeč a kancelářský balík LibreOffice. Uplatnění nalézá v domácí automatizaci, kdy k GPIO rozhraní lze připojit širokou paletu příslušenství. Na trhu jsou k dispozici nejen různá čidla a senzory, nýbrž i rozšiřující moduly, označované jako HAT [28]. Část z vyrobených Raspberry Pi je užita jako hardware pro prototypování či malosériové nasazení ve výrobě, kdy se finančně nevyplatí navrhovat požadovaný systém na míru. Pro některá technická řešení představuje problém absence datového úložiště. To nahrazují MicroSD karty, které mají ale omezený počet zápisů a nejsou prvotně navrženy jako úložiště pro OS, kde je vyžadováno velké množství operací pro zápis. Při velkém počtu zápisů, i vlivem prostředí, tak může MicroSD karta vykazovat chyby a ztrátu dat.

6.3 STM Nucleo /STM32 Nucleo

Vývojové desky STM32 Nucleo umožňují vytvářet prototypy, které mohou být rozšířeny o přídavná hardwarová zařízení. Jedná se o produkt z portfolia STMicroelectronics NV. Tyto produkty patří do výše zmíněné univerzální skupiny, která nabízí výkonné vývojové desky. Tyto desky necílí tak široce na amatérské zájemce jako Arduino, nýbrž na poloprofesionální a profesionální užití ve vývoji a v prototypování. Přesto konkrétně Nucleo 64 zahrnuje konektory Arduino Uno REV3 a ST Morpho. Deska Nucleo STM32 má již debugger/programátor ST-Link integrovaný. Existuje souhrnná knihovna HAL (Hardware Abstraction Layer) pro software STM32, společně s různými příklady, která pracuje s velkým množstvím vývojových prostředí včetně Mbed. Mbed je platforma a OS pro vývoj aplikací na zařízeních, která používají mikrořadiče ARM navržené pro IoT. Nabízí dobrou konektivitu, bezpečnost a kompatibilitu. Uživatelé STM32 Nucleo mají volný přístup k online zdrojům [29].

6.4 Průmyslová IoT zařízení HARDWARIO

Průmysl 4.0 a internet věcí se poslední roky stávají podstatným tématem v průmyslu, ale i mezi širokou veřejností. Významným důkazem jsou plány na chytré domácnosti, které se do jisté míry již realizovaly. Nabídka inteligentních světel, hlasových asistentů, co zapnou hudbu na požádání a připomenou plánované aktivity, je na trhu nespočet. Společně s popularitou internetu věcí se vyvíjela i technická řešení, která by pomohla realizovat projekty na amatérské nebo poloprofesionální úrovni. Na trhu tuto kategorii zastupuje například průmyslová IoT stavebnice od firmy HARDWARIO s.r.o. Tato stavebnice, TOWER IoT Kit [30], je řešena modulárním způsobem, umožňuje sestavit stovky IoT projektů kombinací více než 50 modulů. Díky vstupní průmyslové kvalitě hardwarových komponent splňuje požadavky náročných uživatelů z řad veřejnosti i pro průmyslové využití. Dalším neopomenutelným bodem je energeticky úsporná (low-power) architektura, díky které je zařízení schopno pracovat několik let z baterie a to včetně bezdrátové komunikace. Základním prvkem stavebnice je tzv. Core Module osazený 32bitovým ARM mikrokontrolérem s 192 kB flash pamětí a 20 kB RAM. Na desce je integrovaný rádiový modul komunikující v pásmu 868/915 MHz postavený na SPIRIT1 od ST, také obsahuje digitální senzor teploty, tříosý akcelerometr, tlačítko a bezpečnostní čip. Deska má 18 GPIO (univerzální vstupní/výstupní pin) konektorů, tři UART, dvě I^2C sběrnice a jednu SPI. Analogově-digitálních převodníků nabízí pět, digitálně analogové dva. Pro nahrávání firmwaru je k dispozici HARDWARIO Firmware Tool podporující OS Windows, Linux a macOS. Firmware je pro většinu aplikací připravený, lze ho ale upravovat či psát pomocí HARDWARIO Firmware SDK (Software Development Kit). Pro rádiovou komunikaci je podstatný tzv. Radio Dongle, který funguje jako gateway (brána switch) až pro 32 zařízení a je plně kompatibilní ke Core Module [31]. Tak jako Core Module i Radio Dongle je osazen 32bitovým ARM mikrokontrolérem o stejné paměti a Sub-GHz rádiem pásma 868/915 MHz. Firmware se nahrává do desky

z HARDWARIO Firmware Tool. Deska obsahuje dva bezpečnostní čipy a připojuje se pomocí klasického USB rozhraní do počítače či do Raspberry Pi. V nabídce jsou již sestavené sady, do kterých je potřeba nahrát vhodný firmware a jsou připravené na použití. Jednotlivé moduly jsou k dispozici též, zároveň lze pořídit tzv. tagy. Tag umožňuje připojení čidel měřené veličiny o jednu další, jedná se o hardwarové senzory vlhkosti a teploty, tlaku, NFC, intenzity světla a plynového senzoru pro měření koncentrace volatilních organických sloučenin (VOC). Pro některé aplikace nestačí standardní 868 MHz Sub-GHz radio a proto je možné rozšířit sestavu o LoRa Module nebo Sigfox Module. TOWER IoT Kit nachází uplatnění v IoT pilotech, ověřování konceptů Industry 4.0, jako testery LPWAN technologií, ve výuce nebo chytrých domácnostech.

Vyšší kategorií je tzv. CHESTER IoT Hub [32], víceúčelové zařízení umožňující monitoring veličin, telemetrii dat, vzdálené ovládání a sledování polohy. Významnou předností tohoto hardwarového zařízení je odolnost vůči vodě a prachu, snadné rozšíření o senzory, připojitelnost k jiným systémům a integrovatelnost prostřednictvím API (Application Program Interface). Komunikace je postavená na IoT sítích LTE. V budoucnosti bude možné CHESTER integrovat se satelitními technologiemi. V základu je osazeno MCU (Microcontroller Unit) s BLE modulem, GNSS/GPS modulem, tříosým akcelerometrem, kryptočipem a 8 MB Flash pamětí. Dále je osazeno senzory teploty a vlhkosti, tříbarevnou RGY LED, sadou konektorů pro připojení senzorů a rozhraní a držákem na baterii. Komunikační moduly jsou volitelné mezi NB-IoT, LoRaWAN a případně Kinéis modulem pro satelitní komunikaci. Pro rozšíření o externí senzory a propojení k dalším systémům slouží pomocné moduly, tzv. CHESTER-X. Mezi žádané podporované (průmyslové) technologie patří I^2C, 1-Wire, TTL/CMOS UART, RS-485. Je možno připojit analogové/digitální vstupy 0 až 28 V, tlačítka, tenzometry, senzory Pt1000, termočlánky nebo proudové smyčky 4 až 20 mA. Napájení je řešeno baterií, přímo z externího zdroje přes DC/DC měnič 5 až 28 V nebo prostřednictvím modulu CHESTER-Z, který z externího zdroje dobíjí lithiové baterie a umožňuje také připojení solárního panelu [33]. Je nabízen i enviromentální multisenzor, pod názvem COOPER IoT Multisenzor, osazený devíti senzory pro monitoring vnitřního klimatu.

6.5 PLC

Průmyslové počítače, častěji označované jako PLC z anglického Programmable Logic Controller, jsou zařízení, která pomocí programu řídí činnosti v oblasti technologických a průmyslových procesů. Stala se páteřním systémem průmyslové automatizace. Největším dodavatelem PLC na světě je Siemens s portfoliem řídicích systémů Simatic [34]. Dále lze zmínit firmy Rockwell, Mitsubishi [35], ABB, WAGO [36], GE, české Teco [37], Panasonic [38] atd. Průmyslové počítače se nachází ve výrobních procesech různých průmyslových odvětví. Počínaje automobilovým průmyslem, přes chemický průmysl konče u průmyslu farmaceutického. Na trhu se nachází odhadem dvě desítky celosvětově známých výrobců PLC [39], přičemž existuje i PLC Controllino [40], které je kompatibilní se standardem Arduino a softwarem Arduina,

případně Kunbus PLC [41] vycházející z výpočetního modulu Raspberry Pi. Klasické PLC se skládá z řídicí jednotky. Na její vstupy se obvykle připojují tlačítka či senzory k monitorování aktuálního stavu stroje. K ovládacím prvkům stroje, řízeného PLC, jako je elektromotor, hydraulický pohon či ventily, se zapojují výstupy řídicí jednotky, tj. výstupy se připojí ke spotřebiči. PLC zahrnuje CPU, sběrnice a napájecí zdroj. Do PLC je nahrán požadovaný software řídící jednotlivé procesy (výstup z řídicí jednotky) podle informací získaných ze vstupu. Komunikační rozhraní umožňuje připojit PLC do jiného systému [42]. Obecně lze PLC rozdělit na kompaktní systémy a systémy modulární. V prvním případě se pořizuje hotové řešení s minimálními možnostmi modifikace či rozšíření, zatímco modulární systémy mají víceméně „neomezené“ možnosti rozšiřování a kombinací. Všeobecně jsou PLC navrhována a konstruována do extrémních pracovních podmínek, hardware je v průmyslové kvalitě, obvykle výrobce ručí za dostupnost náhradních dílů po deset let od ukončení výroby, čemuž odpovídá značná pořizovací cena.

7 Bezdrátové technologie pro internet věcí

Užívání bezdrátových technologií pro přenos informací se za posledních 30 let vyvinulo a stalo nepostradatelnou součástí průmyslového rozvoje [43].

První možnou formou komunikace je jednosměrný přenos, jedná se o zasílání naměřených hodnot, výjimečně příkazů danému zařízení. Druhou formou komunikace je obousměrný provoz, kdy spolu mohou komunikovat dvě a více zařízení najednou a to včetně realizace komplexních komunikačních protokolů. Bezdrátový přenos signálu probíhá ve vybraných částech elektromagnetického spektra, kdy každá část spektra má různé přenosové charakteristiky. Tyto vlastnosti mají vliv na celkovou kvalitu komunikačního média, určují snadnost šíření signálu a jeho náchylnost k různým druhům rušení [44]. Podle typu aplikace jsou některé možnosti vhodnější než jiné. Klíčovými faktory pro správný výběr je dosah, nároky na energii, přenosová rychlost a frekvence. Podle přenosového dosahu lze technologie pro IoT dělit na dotekovou vzdálenost do 15 cm, do které spadají NFC a RFID. V oblasti s krátkým dosahem 10 až 100 metrů se můžeme setkat u Bluetooth, BLE (Bluetooth Low Energy), ZigBee [45], Thread (6LoWPAN) nebo Z-Wave. Označuje se jako WPAN, Wireless Personal Area Network. V krátkém až středně dlouhém dosahu, označováno WLAN, Wireless Local Area Network, lze komunikovat na vzdálenost 100 až 1000 metrů. Nalezneme zde standardy pro WiFi pásmo, jako je IEEE 802.11 a/b/g/n/ac, IEEE 802.11af, IEEE 802.11ah a IEEE 802.11p [46]. Uváděný střední dosah, WNAN, Wireless Neighborhood Area Network, má 5 až 10 kilometrů a jako příklad lze uvést ZigBee NAN nebo Wi-SUN. WWAN, neboli Wireless Wide Area Network, síť dlouhého dosahu má všeobecně uváděný přenos do 100 km. Uvedené vzdálenosti jsou pouze orientační, reálné hodnoty závisí na vybrané bezdrátové komunikační platformě a na úrovni pokrytí zřizovatelem. WWAN se dále dělí dle spotřeby energie na High Power Wide Area (HPWAN) a na Low Power Wide Area (LPWAN). Do HPWAN lze zařadit satelitní technologie, GSM, 3G, 4G a plánované 5G. Zástupcem LPWAN jsou sítě LoRaWAN, Sigfox, LTE-M (LTE Cat M1) nebo NB-IoT [47].

7.1 RFID a NFC

Radio Frequency Identification je technologie komunikace mezi čipem s anténou, tj. tagem, a čtečkou. Dle požadavků mohou RFID systémy pracovat v různých frekvenčních pásmech. Proti rušení jsou obvykle vybaveny ISM frekvenčními pásmy. Jedná se o volná pásma pro průmyslové, vědecké a zdravotnické užití. Pro RFID technologii je nejdůležitějším prvkem transpordér neboli nosič dat. Transpordéry

se dělí na aktivní a pasivní podle toho, jakým způsobem jsou zásobovány energií. Pasivní tagy jsou zásobovány elektromagnetickým polem čtecího zařízení, jsou levnější, menších rozměrů, ale dosah čtení je maximálně 8 metrů. Zatímco aktivní transpordér má integrovanou vlastní baterii, je větší, dražší leč dosah čtení může být až 100 metrů. Oblast pasivních aplikací pracuje se třemi frekvenčními rozsahy. Low-Frequency (LF) užívá pásmo 125 kHz a 134 kHz. LF má krátký dosah čtení, při zasílání větších objemů dat vykazuje pomalé přenosové časy. Přesto dobře snáší vlhkost a nezpůsobují zkreslení v blízkosti kovových povrchů. Dnes se technologie 125 kHz používá na okrajové aplikace, kde nezáleží na bezpečnosti, příkladem je označování zvířat pro sledování jejich polohy (animal tagging). High-Frequency (HF) pracuje na 13,56 MHz. Nabízí krátké až středně dlouhé dosahy při vysoké rychlosti přenosu. Možnosti užití ve vlhkém prostředí či kovovém okolí jsou omezené. Na této frekvenci pracuje technologie NFC. Ultra-High Frequency (UHF) má dosah až 6 metrů pro pasivní transpordéry při vysoké rychlosti přenosu. Pracuje ve frekvenčním pásmu 850–950 MHz. Nachází uplatnění především v oblasti etiket [48, 49].

Near Field Communication (NFC) je mezinárodním standardem pro bezkontaktní přenos dat na frekvenci 13,56 MHz. Jedná se o nový standard bezdrátové komunikace na krátkou vzdálenost. Umožňuje čtení do vzdálenosti 10 cm a při jednom spojením kratším než 0,1 sekundy dosahuje přenosového výkonu dat maximálně 424 kbit/s. Významnou výhodou je užití mobilních koncových zařízení s integrovaným NFC rozhraním jako náhrady dražších RFID přístrojů coby čteček. Koncové přístroje vybavené NFC umožňují autorizaci různých činností, velice populární jsou nyní například platby pomocí telefonu [48, 49].

7.2 Bluetooth a BLE

Bluetooth a Bluetooth Low Energy (BLE) jsou bezdrátové technologie určené ke komunikaci na krátké vzdálenosti. Ve volném prostoru při přímé viditelnosti mezi zařízeními může být přenos úspěšný na desítky až stovky metrů, v uzavřených prostorech se tato vzdálenost zkracuje řádově na centimetry. Bluetooth pracuje v nelicencovaném frekvenčním pásmu 2,4 GHz (ISM), o které se dělí s několika dalšími bezdrátovými systémy (IEEE 802.11). Šířka pásma je pro většinu světových a evropských zařízení 2400 až 2483,5 MHz. V tomto pásmu je 79 kanálů širokých 1 MHz. Aby nedocházelo k porušování norem mimo pásmo, byla stanovena tzv. ochranná pásma. V tomto případě má dolní ochranné pásmo šířku 2 MHz a horní 3,5 MHz. Výjimkou je například Španělsko a Francie, kde používají variantu s šířkou frekvenčního pásma 2446,5 až 2483,5 MHz. Obsahuje pouze 22 kanálů, opět po 1 MHz. Ochranné pásmo je 7,5 MHz pro obě hranice. Maximální přenosová rychlost nepřesahuje 723 kbit/s [50].

BLE je součástí specifikace Bluetooth 4.0. Používá se pro aplikace, kde je nutné snížit spotřebu baterie na minimum. Pracuje v pásmu 2,4 GHz jako klasický Bluetooth, přesto s ním není kompatibilní. Liší se počtem kanálů i jejich šířkou, která je 2 MHz. BLE užívá 40 kanálů [51].

7.3 WiFi

Technologie Wireless Fidelity je aktuálně jednou z nejrozšířenějších forem bezdrátové komunikace. Pracuje v pásmu 2,4 GHz a 5 GHz. Podřizuje se standardu IEEE 802.11. Router je základním bodem hvězdovitě uspořádané komunikační sítě IP. Hranice dosahu se odvíjí od prostředí a umožňuje připojení velkého množství zařízení najednou. Pro připojení je podstatný tzv. přístupový bod. Ten vysílá signál, který je zařízení schopné rozeznat a zpracovat. Jedná se o velice výkonné řešení, finančně nenáročné, ovšem s poměrně malým dosahem a velkým odběrem energie. Zařízení, která nejsou osazena embedded WiFi mohou využít WiFi čip, který nezatěžuje mikrokontrolér. Vzhledem k vysokým nárokům na spotřebu energie je pro IoT zařízení s WiFi komunikačním modulem vhodné využít napájení ze sítě, případně vhodně navrhnout low power (nízkoenergetickou) architekturu. Nově vznikají standardy WiFi pro IoT, jako je například Wi-Fi HaLow [52].

7.4 2G, 3G, LTE a 5G

Nejrozšířenější datovou sítí na světě je Globální systém pro mobilní komunikaci, zkráceně GSM nebo také 2G. Užívá se především k přenosu hlasových dat a SMS. Datový přenos dosahuje rychlosti 21,4 kbit/s a používá frekvence 900 MHz, 1800 MHz a 1900 MHz. Zvýšení přenosových rychlostí na 171 kbit/s umožnil až nástup 2,5G označovaného jako GPRS. General Packet Radio Service navíc umožnil přenos dat na základě TCP/IP a WAP (Wireless Application Protocol) protokolů. GPRS je stále světově nejužívanější technologií na poli M2M řešení, neboli machine to machine. Dosavadního maxima v 2G přenosových rychlostech dosáhl aktuálně používaný EDGE (Enhanced Data for GSM Evolution) díky modulaci s vyšším počtem stavů. Papírově přenosové rychlosti mohou dosahovat až 473,6 kbit/s, přesto se častěji uvádí 236,8 kbit/s, reálně operátoři dosahují 60 až 120 kbit/s [53, 54].

Síť třetí generace, 3G, je první mobilní technologie navržená jak na přenos hovorů a SMS, tak i dat. Pracuje v pásmu 2100 MHz. 3G není jedna technologie, nýbrž se pod názvem skrývá mnoho standardů. Tím nejznámějším je UMTS (Universal Mobile Telecommunications System). Hlavním přínosem UMTS je podpora kvality služeb (QoS), což je rozdělení kvality služeb sítě s ohledem na požadavky jednotlivých typů provozu. První realizace proběhly již roku 2001, do reálného povědomí se však v ČR dostala síť až kolem roku 2010. V tu doby už začínaly být dostupné telefony s podporou internetu. V základním nastavení je papírově uváděná rychlost přenosu dat 384 kbit/s. Obvykle je ale potřeba odečíst 20–30 procent z papírové hodnoty a v závislosti na vytížení sítě se teprve lze dostat na reálné rychlosti. Následovalo zvýšení rychlosti pomocí HSDPA (High-Speed Downlink Packet Access). Tento doplněk posunul 3G síť na 3,5G síť a rychlost se zvýšila na megabity za sekundu. Aktuální technologie je HSPA+, neboli vysokorychlostní paketový přístup [55]. Teoretická rychlost pro stahování je 84 Mbit/s a pro nahrávání na 22 Mbit/s, reálné hodnoty se sotva dostávají na polovinu teoretických, operátory je rychlost uváděna jen v Mbit/s, ti troufalejší si stojí za desítkami Mbit/s [53, 54]. V letošním roce

je plánováno ukončení provozu této sítě na území ČR, Německa ale i třeba Itálie [56]. Pravděpodobné ukončení ve světě se plánuje do roku 2022. 3G by mělo být nahrazeno LTE(4G) a 5G sítí.

Long Term Evolution (LTE), označovaná jako čtvrtá generace bezdrátových mobilních telekomunikačních technologií. Technologie byla vyvinuta pro vysokorychlostní internet a klíčovým cílem bylo zvýšení datové prostupnosti a snížení latence poskytovaných služeb. LTE získala pro marketingové účely označení 4G, což není přesné, jelikož nesplnila některé specifikace pro bezdrátové standardy, stanovené například skupinou 3GPP nebo ITU (Mezinárodní telekomunikační unie). LTE v ČR pracuje na frekvenčních pásmech 800, 900, 1800, 2100 a 2600 MHz při šířce pásma 10 nebo 20 MHz. Uváděná rychlost přenosu se pohybuje od desítek po stovky Mbit/s v závislosti na operátorovi a pokrytí službou. Jedná se o vyvíjející se standard, jsou k dispozici různé verze, například LTE Advanced či LTE Advanced Pro. LTE Advanced je již plnohodnotným 4G, jelikož splnilo požadavky Mezinárodní telekomunikační unie [57].

Síť páté generace, 5G, navazuje na předchozí technologie a odráží potřeby efektivnější komunikace jak ze strany uživatelů, tak i z oblasti průmyslu. 5G technologie je postavená na aktivních anténách, kterými lze lépe směřovat vysílané svazky rádiových vln (signál) a tím zlepšit využití kmitočtů. 5G by mělo nabídnout vyšší přenosovou rychlost při dostatečné kapacitě pro připojení tisíců zařízení v jeden moment. Odhaduje se, že na jednom kilometru čtverečním bude moci být připojeno až milion zařízení, zatímco LTE pokryje připojení pouze deseti tisíc zařízení na stejnou plochu. Síť páté generace by měla podpořit rozvoj průmyslu 4.0 a s tím spojeného IoT. Využívat bude kmitočtová pásma stávajících technologií 2G, 3G, 4G, také pásmo 3400–3800 MHz. Specifickým pásmem pak bude 700 MHz, 26 GHz nebo 66–71 GHz. V ČR bylo 5G spuštěno před koncem roku 2020 a to v pásmech kmitočtů již užívaných [58].

Všech pět generací sítí nabízí velice spolehlivý přenos, dobré pokrytí, poslední generace nabízejí i vysoké přenosové rychlosti a jsou energeticky nenáročné.

7.5 UWB

Ultra WideBand neboli ultra-širokopásmová síť, označovaná jako technologie budoucnosti, je poměrně málo veřejně známá bezdrátová technologie. Přestože se již od 60. let minulého století využívala pro vojenské účely, speciálně v souvislosti s radary. Až roku 2002 byly Federální komunikační komisí USA (FCC) vydány předpisy umožnující nelicencované využívání přiděleného spektra. Roku 2018 vznikla UWB Alliance [59], jejími členy jsou výrobci elektroniky i několik automobilek. O rok později vzniklo konsorcium FiRa [60], jehož posláním je vývoj a popularizace UWB. Síť je schopna přenášet velké objemy dat, až v Gb/s, na krátkou vzdálenost. Vysoká propustnost této sítě je vhodná zejména pro aplikace s vysokými nároky na šíři pásma a QoS, především přenos videa a videokonference. Mobilní sítě a WiFi zpravidla pracují v pásmech o šířce 20–80 MHz. UWB má minimální šířku pásma 500 MHz. Klasické rádiové sítě používají frekvenční modulaci sinusové nosné vlny. UWB užívá

krátkých pulzů, řádově kolem 0,5 nanosekundy, o nízkém výkonu při současném přenosu pulzů přes vysoký počet frekvenčních kanálů při přesném časování. Zasahuje tedy do spekter, která využívají WiFi nebo mobilní sítě. Je schopné pracovat na frekvencích od jednoho do deseti GHz, ČTÚ povoluje kmitočty 3,1–4,8 GHz a 6–9 GHz. Jelikož vysílá při nízkém výkonu, $-41,3$ dBm/MHz, může sdílet pásma s ostatními rádiovými sítěmi aniž by docházelo k vzájemnému rušení. Z pohledu mobilních sítí a WiFi se UWB vysílání jeví jako šum. UWB má dvě důležité vlastnosti. První je vysoká bezpečnost provozu, je prakticky nemožné komunikaci odposlechnout nebo detekovat přítomnost takto komunikujících zařízení v síti. Druhou podstatnou vlastností je lokalizovatelnost dané stanice a vysoká rychlost přenosu s téměř zanedbatelnou latencí. Díky velice krátkým impulzům lze přesněji odhadovat čas letu signálu mezi 2 zařízeními a i směr. Je možno dosáhnout přesnosti lokalizace na desítky cm a několik úhlových stupňů. Aktuálně nachází uplatnění pro přesnou lokalizaci, detekci pohybu, pro přesnou navigaci, měření vzdáleností, pro komunikační sítě i v medicíně. S technologií pracují i automobilky nebo výrobci mobilních telefonů. Automobilky již vyvíjejí řešení na bezpečné odemykání aut, lze jmenovat například Audi, BMW, Kia, Hyundai nebo Ford [61].

7.6 LPWAN

Skupina rádiových přenosových technologií skrývající se pod názvem Low Power Wide Area Network byla navržena zejména za účelem minimální spotřeby energie. LPWAN umožňuje přenos dat na dlouhé vzdálenosti s vysokou spolehlivostí. Energetická nenáročnost předurčuje tyto technologie k napájení z bateriových zdrojů. Jsou vhodné pro přenos dat v desítkách kilobajtů až několika megabajtů za měsíc, z čehož vyplývá, že se nejedná o technologii vhodnou k přenosu velkých objemů dat. Vyznačují se nízkými přenosovými rychlostmi a pracují především v nelicencovaných pásmech na frekvenci 169, 433 a 868 MHz. Nízká frekvence má lepší prostupnost prostředím, což se projevuje především v zastavěných oblastech. Tato technologie byla vyvinuta speciálně pro IoT aplikace a přestože existuje mnoho různých LPWAN sítí, celá řada protokolů a standardů, všechny splňují podstatné rysy této skupiny: nízká přenosová rychlost, dlouhý dosah, nízká spotřeba energie koncových zařízení, nízké náklady na koncová zařízení i výstavbu a provozování sítě. Na trhu jsou tři významní zástupci této technologie a to LoRa, Sigfox a NB-IoT.

7.6.1 Bezlicenční pásmo ISM

Zařízení vysílající elektromagnetické vlny na vybraném rádiovém kmitočtu musí dbát na to, aby pro dané kmitočtové pásmo měla přidělenou příslušnou licenci. V České republice přidělení licence zajišťuje Český telekomunikační úřad (ČTÚ). Mimo licencovaná pásma, která ve velké míře převažují, existují pásma bezlicenční pro jejichž využití není třeba žádat ČTÚ o povolení. Velice významným bezlicenčním pásmem je tzv. ISM pásmo, pochází z anglického Industrial Science Medical. Označuje kmitočtové pásmo původně určené pro průmyslové, vědecké a zdravotnické

aplikace. Tento termín zavedla Mezinárodní telekomunikační unie (ITU) spadající pod OSN (Organizace spojených národů). Jednou z agend ITU je celosvětová koordinace využívání rádiového spektra. ISM pásmo bylo navrženo pro užití mimo oblast komunikací, slouží pro provoz zařízení, která by mohla způsobovat rušení v rádiového provozu, např. 2,45 GHz mikrovlnná trouba, a být sama rušena. ISM pásma jsou vedena jako součást podmínek pro vysílací zařízení krátkého dosahu tzv. short range devices (SRD), pro něž platí všeobecné oprávnění VO-R/10 vydaná ČTÚ [62]. Protože je většina výkonových zařízení dobře odstíněná, užívají se bezlicenční pásma i pro komunikační účely. Významná jsou pásma 2450 MHz pro Bluetooth, 2,4 a 5 GHz pro standard IEEE 802.11 a 169, 433 a 868 MHz pro síť Sigfox a LoRa. Pro WiFi a Bluetooth regulace stanoveny nejsou, pro sítě na 169 a 868 MHz je klíčovací poměr stanoven na 1 procento. Klíčovací poměr (duty cycle) je stanoven jako podíl času, kdy zařízení aktivně vysílá, v rámci jakékoliv jedné hodiny. Pro 433 MHz je stanoven klíčovací poměr na 10 procent vysílacího času za 60 minut. Tato pásma nejsou vhodná pro kritické aplikace, jednak z hlediska bezpečnosti a zároveň možnosti rušení.

7.6.2 LoRa

Bezdrátová vysokofrekvenční technologie, vyvíjená a spravovaná organizací LoRa Alliance, v roce 2015 vytvořená firmou Semtech [63]. LoRa je zkratkou pro Long Range, neboli dlouhý dosah. Je odvozená od chirp spread spectrum (CSS), což je jedna z technik modulace rozprostřeného spektra. Technologie se skládá z LoRa modulace a LoRaWAN síťového protokolu. Síťový protokol umožňuje bezpečný přenos dat mezi koncovým zařízením a LoRa Gateway. Gateway pracuje na principu hvězdicové topologie. Je určena pro IoT aplikace v ISM pásmu, v Evropě pracuje v nelicencovaném kmitočtovém pásmu kolem 868 MHz nebo 433 MHz. Přenos dat zabezpečuje 128bitová šifra Advanced Encryption standard (AES), nahradila DES algoritmus. Šířka pásma je 125 kHz. Využití rádiového kanálu je oprávněním VO-R/10 omezeno na 1 procento za 60 minut, což umožňuje připojit velké množství zařízení při malém množství přenesených dat na jedno koncové zařízení. Počet zpráv za den je bez omezení při přenosové rychlosti od 300 bit/s do 50 kbit/s. Délka zprávy musí být v rozmezí 51 až 243 bajtů. České Radiokomunikace deklarují pokrytí všech krajských měst ČR a dále možnost připojení rozšiřují. Pro vlastní potřebu je možné si postavit vlastní LoRa síť. Obvyklý dosah je 5–10 km na jednu stanici. Existují 3 třídy nastavení koncových zařízení [64].

- Třída A je určena k napájení na baterii, optimálně pro sběr dat. Komunikace je zahájena ze strany koncového zařízení v momentě, kdy jsou splněny přednastavené podmínky nebo na základě nastaveného intervalu, tj. v případě kouřového čidla je zaslána informace až v momentě, kdy je kouř zachycen. Zasílání zpráv k čidlu se vždy provede s časovou prodlevou.

- Třída B je vhodná k obousměrné komunikaci. Umožňuje přijímat zprávy v libovolném okamžiku nebo v závislosti na aktivaci čidla typu A. Ve stanovených intervalech aktivují svou přijímací radiovou část aniž by nutně musela vysílat

zprávu. Třída B je vhodná pro aplikace, kde je potřeba často přepínat mezi stavy. Takovým případem může být pohybové čidlo, hlásící detekci pohybu nebo žádný pohyb. Sítí jsou vysílány impulzy s intervalem 128 sekund, které synchronizují časovače koncových zařízení a tím udržují přesnost nastavení.

- Třída C je vhodná pro zařízení, kde není nutno řešit napájení přes baterie. Přijímací část čidla je trvale aktivována a může přijmout ovládací zprávu ze sítě v libovolném okamžiku.

7.6.3 Sigfox

Je francouzská společnost založená roku 2009 jako startup. Síť má topologii hvězdicovou, skládá se z koncových zařízení, základnových stanic neboli gateway a Sigfox back-endového řešení. Pokrytí území jednotlivých států se řeší pomocí národních operátorů Sigfox [25]. Základnové stanice Sigfox se umisťují již na existující vysílací věže mobilních operátorů. Sigfox užívá bezlicenční pásmo ISM na frekvenci 868 MHz (Evropa) a 915 MHz v USA. Technologie je postavená na úzkopásmovém přenosu signálu, anglicky Ultra Narrow Band (UNB). Šířka pásma je 100 Hz a přenosová rychlost 100 bit/s. Tím je získána vyšší citlivost, což ovlivňuje pozitivně dosah a zároveň i snižuje šum. Maximální délka zprávy je pro odesílání (Uplink) 12 bajtů a pro příjem (Downlink) 8 bajtů. Šifrování je řešeno stejným způsobem jako u LoRa, tedy technologií AES 128bitů. Sigfox omezuje počet zpráv na koncové zařízení a to na 140 odeslaných zpráv a 4 přijaté. Jedná se o proprietární technologii nabízející až 96% pokrytí ČR a pokrývá i místa, kam mobilní operátoři nedosahují. Pro technologii platí omezený klíčovací poměr 1 procento s maximálním vyzářeným výkonem 500 mW pro příjem a 25 mW pro vysílání. Pro IoT aplikace, kde je nutné komunikovat mezi více státy se tato technologie jeví jako ideální. Sigfox pokrývá 65 zemí světa [65].

7.6.4 NB-IoT

NB-IoT je mobilní technologie pracující v licencovaném pásmu LTE. Lze se s ním setkat i pod názvem LTE Cat NB1. Poprvé byla zveřejněna uskupením 3GPP, což je dohoda z roku 1998 o spolupráci v oblasti mobilních komunikací (Partnerský projekt třetí generace). Technologie byla navržena s cílem lepšího pokrytí území než jaké má GSM síť [66]. Síť se skládá z koncového zařízení s modulem pro NB-IoT, SIM karty operátora sítě a serveru, kam jsou data zasílána. Šířka pásma je 180 kHz a přenosová rychlost je pro Uplink 32 kbit/s a Downlink 27 kbit/s. Vysílací výkon je oproti 14 dBm technologie LoRa a Sigfox zvýšen na 20 nebo 23 dBm[1]. Počet zpráv komunikovaných za jeden den není nijak omezen a délka zprávy může maximálně dosáhnout 1280 bajtů. Šifrování probíhá systémem LTE, lze použít 128bitový klíč případně silnější 256bitový klíč. NB-IoT definuje 3 úrovně pokrytí službou, *Normal*, *Robust* a *Extreme* [67, 68]. Častěji se lze setkat s označením CE (coverage extension).

[1] logaritmická jednotka výkonu

Úroveň se volí na základě podmínek signálu, ty se určují měřením intenzity signálu (RSRP) a měřením kvality signálu vzhledem k okolnímu rušení (SINR) [69].

- CE level 0 (Normal) obvykle pokrývá i zastavěné plochy včetně vnitřního pokrytí budov. MCL neboli Maximum Coupling Loss [70] je 144dB. MCL je maximální ztráta na výkonu, kterou lze ještě tolerovat, jelikož stále zůstává přijatelná přijímací úroveň výkonu, tj. nedojde k narušení funkčnosti.
- CE level 1 a 2 se používají pro podzemní prostory, obecně v místech, kde jsou nepříznivé podmínky pro šíření signálu. Pro level 1 se udává MCL 154 dB a level 2 MCL 164 dB. Level 1 a 2 mají větší nároky na množství energie pro přenos signálu, přesto jsou stále efektivní pro bateriový provoz.

8 Komunikační protokoly

Komunikaci v ISO/OSI modelu lze rozdělit podle druhu komunikace mezi vrstvami (fyzická až aplikační vrstva). Ve vrstvách jednoho systému hovoříme o komunikaci přes interface, rozhraní. Mezi stejnými vrstvami různých systémů komunikace probíhá pomocí protokolů. Sada protokolů OSI je pro většinu aplikací považována za komplikovanou a neefektivní. Obsahuje mnoho volitelných funkcí, implementace různými dodavateli pak vedla k neschopnosti různých systémů vzájemně spolupracovat. Z toho důvodu se sada internetových protokolů stala standardem pro práci v síti. Nezávislé implementace zjednodušených protokolů a pragmatický přístup TCP/IP k počítačovým sítím se ukázalo jako správná cesta. Některé protokoly a specifikace OSI přesto byly zachovány a přizpůsobeny pro použití na internetu s TCP/IP. Komunikační protokoly TCP/IP lze definovat jako soubor pravidel určujících, jak se data odesílají do internetu a mezi sebou v síti. Typ protokolu závisí na architektuře systému a odesílání probíhá přímo nebo přes gateway. Část IoT zařízení používá ke komunikaci UDP/IP, to je ale pro svou bezstavovost a nulové záruky na doručení zprávy mnohdy nevyhovující. Typy komunikací se dělí na zařízení – zařízení (M2M), zařízení – gateway/úložiště, gateway – úložiště, úložiště – úložiště, přičemž pod pojmem úložiště se předpokládá datové centrum či cloud. Velice významnou formou dělení je dle komunikačních vrstev. Nejblíže k hardwaru je vrstva fyzická, sem patří většina výše zmíněných komunikačních systémů/protokolů, jako Ethernet, 802.11a/b/g/n/ac (WiFi), Bluetooth, LPWAN, ale i třeba 802.15.4 (Zigbee, Thread), Z-Wave, RS-232 a RS-485, ISM rádio – FSK 19,2 kbps. Protokoly fyzické vrstvy tvoří kanál mezi zařízeními a specifickým prostředím. Každé komplexní zařízení má svou fyzickou vrstvu (BLE, WiFi, HARDWARIO RF). Nad touto vrstvou se nachází vrstva síťová, jako příklad je možno zmínit 6LoWPAN a IPv6. Ta řeší komunikaci mezi zařízením a routerem. Výše je vrstva transportní, zde se uvádí především TCP a UDP protokoly. Nižší komunikační vrstvy jsou zodpovědné za přenos dat mezi zařízeními, komunikaci mezi zařízením a úložištěm apod. Obvykle nestanovují, jak s přenášenými daty nakládat nebo co data reprezentují. To je definováno vyššími aplikačními vrstvami OSI modelu. Aplikační vrstva tvoří rozhraní mezi uživatelem a zařízením. Těmi může být TLS, HTTP, MQTT, LwM2M (CoAP), DDS, WebSocket nebo třeba AMQP. Protokoly lze dělit na proprietární (closed source) a open source. Další možností dělení je podle oboru využití tj. v průmyslových aplikacích se používá OPC-UA, proprietární protokoly od výrobců průmyslových řešení (např. Siemens) nebo protokoly pro IoT. K zabezpečení dat se používají různé metody, které nejčastěji využívají symetrický klíč nebo certifikát. Principem je, že dvě komunikující strany mají klíč, který dešifruje a šifruje data nebo data podepisuje.

Protokoly jako takové lze definovat jako sadu pravidel, která umožňuje komunikaci serveru a klienta (cloudu a zařízení).

Bezdrátová komunikace obvykle obsahuje vlastní zabezpečení na síťové vrstvě. Zvýšení bezpečnosti zajistí TLS šifrovaný kanál. Transport Layer Security vychází z generačně staršího SSL (Secure Sockets Layer). Jedná se o kryptografický protokol aplikační vrstvy. TLS řeší chyby SSL a podporuje silnější formy šifrování. Také řeší ověřování zpráv kódem hash (Keyed-hash Message Authentication Code), čímž se kontroluje, že data během přenosu nebyla pozměněna. Vylepšila se také správa klíčů a šifrovacích algoritmů [71]. Pomocí TLS je vytvořen zabezpečený tunel a tímto tunelem migrují data podle vybraného protokolu aplikační vrstvy (např. MQTT), ten stanovuje komunikační port a nastavuje pravidla komunikace. U většiny firemních sítí je přístup mimo interní síť, do internetu, kontrolován pomocí tzv. *firewallu*, který chrání síť před neautorizovaným přístupem zvenčí. Situace ale může být i opačná, kdy firewall zamezuje přístupu k některým službám z vnitřní sítě blokováním portů TCP/IP a UDP/IP protokolu. V některých případech jsou na firewallu povoleny pouze porty HTTP či zakázány porty nad 1023, záleží na nastavení interní sítě. To lze obejít pomocí technologie WebSocket [72]. WebSocket vytvoří tunel pomocí HTTP příkazu CONNECT, požadavek otevře TCP/IP spojení se serverem na stanoveném portu protokolu HTTP, který je na firewallu běžně povolen. Takto vybudovaný tunel umožní přenášet zprávy mezi klientem a serverem v reálném čase. Podobným, ovšem lépe zabezpečeným, principem je komunikace WSS (WebSocket over SSL/TLS).

8.1 TCP a UDP

Dva význačné protokoly transportní vrstvy. TCP je zkratkou pro Transmission Control Protocol. Zajišťuje přenos dat se spolehlivým doručením. Jedná se o službu klient – server/handshake. Obsah zpráv posílá rozdělený do segmentů neboli paketů (MTU). Doručení se ověřuje pomocí kontroly pořadí neboli pořadových čísel paketů. Potvrzení, že pakety byly úspěšně přijaty je generováno na základě kontrolního součtu paketů. TCP porty jsou velice významné, užívá je například HTTP, DNS nebo např. FTP. Nevýhodou je komplexita a blokování fronty paketů, vyřizují se postupně [73].

User Datagram Protocol je jednoduchý a bezstavový protokol. Neuchovává pořadí zpráv a nezaručuje jejich bezchybný přenos, tj. nedává záruku na doručení datagramu. To je podstatný rozdíl mezi TCP a UDP. UDP má své opodstatnění například pro nasazení, kde je kladen důraz na jednoduchost, pro aplikace typu otázka – odpověď tj. DNS nebo sdílení souborů v LAN. Bezstavovost je efektivní pro servery, které komunikují s mnoha uživateli a nebo pro nasazení v aplikacích, kde se počítá s možnými ztrátami datagramů a není čas na znovuzasílání starých nedoručených zpráv, např. systém online her nebo digitální přenos hlasu (IP telefonie) a Voice over Internet Protocol (VoIP) [73].

8.2 HTTP

Hypertext Transfer Protocol je internetový protokol přenášející data ve formátu HTML, XML atd. Definuje jaký typ dat lze přenášet, jak jsou data formátována a jak by server měl reagovat na konkrétní příkazy. Původně byl navržen na přenos hypertextových dokumentů, nyní má ale mnohem širší využití. Neumí uchovávat stav komunikace klient/server, předchozí dotazy na stejnou stránku nemají z pohledu HTTP souvislost. Proto se jedná o bezstavový protokol, funguje na principu dotaz/odpověď. Tento protokol je velice rozšířen, obsahuje hlavičku Authorization, což je hlavička pro autentifikaci. Vlastní autentifikaci a autorizaci však řeší aplikace nebo web server. Při použití TLS společně s HTTP, vznikne zabezpečená komunikace označovaná HTTPS, neboli Hypertext Transfer Protocol Secure. TLS vytvoří bezpečný komunikační tunel a v něm probíhá komunikace HTTP. HTTP používá TCP port 80, HTTPS pak TCP port 443 [71, 74].

8.3 MQTT

Message Queue Telemetry Transport je kompaktní, lehký, otevřený a asynchronní protokol aplikační vrstvy pro výměnu dat navržený pro omezenou šířku pásma, vysokou latenci, nespolehlivé sítě a zároveň je vhodný i tam, kde je vyžadována malá velikost kódu. Princip návrhu spočívá v minimalizaci potřebné šířky pásma a požadavků na prostředky zařízení při udržení spolehlivosti a míry zajištění doručení zprávy. Tyto principy činí protokol ideálním pro připojená zařízení M2M (machine-to-machine), IoT nebo mobilní aplikace. MQTT vzniklo roku 1999 za přispění IBM a společnosti Arcom (Eurotech). MQTT v5.0 a v3.1.1. jsou standardy OASIS. Version 3.1.1. je ratifikována jako ISO standard. Protokol podporuje bezpečnostní šifrování. První metodou je autentizace klienta polem USERNAME a PASSWORD, druhou možností je kontrola přístupu klienta pomocí Client ID a třetí možností je připojení brokeru prostřednictvím TLS. Využívá návrhový vzor Publish – Subscribe, tzn. Publisher odesílá data a nestará se o příjemce. Zatímco Subscriber odebírá data, ke kterým se přihlásil. Předávání dat většinou zařizuje Broker. Zpráva se skládá z tzv. Topic (tématu) a Payload (obsah). MQTT je data-agnostic protokol, tzn. nedefinuje formát obsahu. Nejčastěji se přenáší ve zprávě JSON. QoS z anglického Quality of Service nabízí 3 úrovně zasílání zpráv.

- Level 0 – fire and forget
- Level 1 – at least once
- Level 2 – exactly once

MQTT pracuje na portu 1883 a pro MQTT přes TLS je vyčleněn port číslo 8883 [75, 76, 77].

8.4 AMQP

Advanced Message Queuing Protocol je otevřený standardizovaný komunikační protokol aplikační vrstvy navržený k bezpečnému a efektivnímu přenosu informací mezi aplikacemi, organizacemi, přes distribuovaná cloudová výpočetní prostředí a mobilní infrastruktury. Protokol je výrazně robustnější než MQTT a primárně vyvinutý pro komplexní řešení s velkou orientací na zasílání zpráv. Lze se setkat se dvěma verzemi AMQP, AMQP 0.X. a AMQP 1.0. AMQP 1.0. je uznaný OASIS, ISO a IEC International Standard, zatímco AMQP 0.X. nikoli. Dalším významným rozdílem mezi těmito dvěma verzemi spočívá v definovaném (AMQP 0.X.) a nedefinovaném (AMQP 1.0.) způsobu vývoje brokeru. Z toho plyne další rozdíl mezi MQTT a AMPQ, tj. AMQP 1.0. je protokol typu peer-to-peer, tzn. lze komunikovat mezi dvěma zařízeními na přímo, bez užití brokeru. Aktuálně lze již upgradovat na verzi 2.4.1. Hlavními vlastnostmi je orientace a směřování zpráv, řazení zpráv a zajištění spolehlivosti a bezpečnosti. Protokol sjednocuje chování poskytovatele zpráv a klienta tak, aby i aplikace odlišných dodavatelů mohly kooperovat. Jedná se o wire-level protokol, tzn. protokol na drátové úrovni. To je popis formátu dat, která jsou posílána po síti jako proud bajtů. Díky tomu může jakýkoli nástroj, který umí vytvářet a interpretovat zprávy v tomto formátu, spolupracovat s kterýmkoli kompatibilním nástrojem bez ohledu na implementační jazyk. Specifikace AMQP je definována do 4 vrstev, první je typový systém, druhá vrstva obsahuje symetrický, asynchronní protokol pro přenos zpráv z jednoho procesu do druhého. Třetí vrstva obsahuje standardní rozšiřitelný formát zpráv a čtvrtá je sada standardizovaných rozšiřitelných schopností zasílání zpráv. Záruky doručení zprávy (QoS) se dělí stejným způsobem jako u MQTT, tj. na nanejvýš jednou (zpráva přijde jednou nebo nikdy), alespoň jednou (doručení jisté, zpráva může přijít několikrát) a přesně jednou. Autentizace a šifrování probíhá na základě SASL (Simple Authentication and Security Layer) nebo TLS. AMQP stojí na základním spolehlivém protokolu TCP. Pro komunikaci jsou vyhrazeny dva porty, číslo 5672 a 5671 pro AMQPS na TLS certifikátu [78, 79, 80, 81].

9 Návrh prototypu komunikačního zařízení

Předmětem této práce je vyhotovení komunikačního zařízení (jednoduchého Servicedesku) pro zefektivnění komunikace mezi biomedicínskými techniky, inženýry, servisními techniky a zdravotnického personálu nemocnic. Zařízení nesmí zasahovat do autonomie přístrojů a zároveň musí být schopno zaslat stav přístroje, informaci o poruše, stiskem tlačítka. Ta projde přes softwarová úložiště (cloudy) a uloží se do excelové tabulky. Informace by se měla zobrazit na mobilním zařízení odpovědné osobě. Nemusí být speciálně kryptovaná, nejedná se o zasílání citlivých či kritických dat, jejich životnost na síti je krátká.

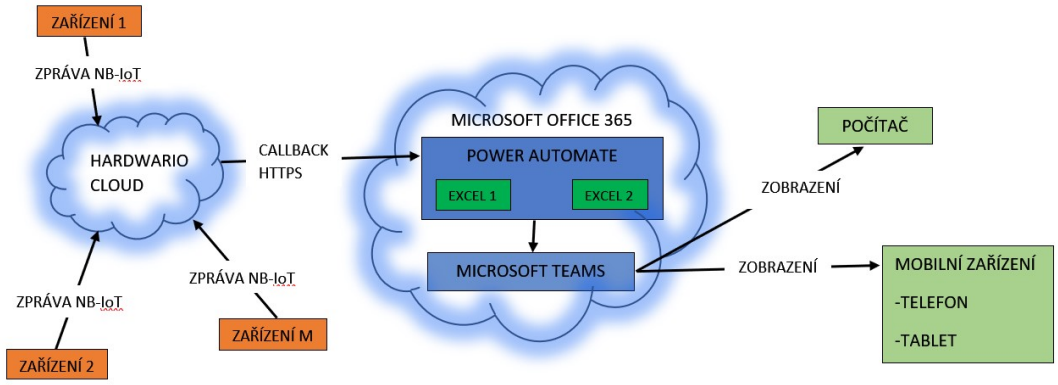
Jak již bylo popsáno v teoretické části této práce, vývojových desek je na trhu nespočet. Nabízela se i možnost navržení vývojové desky včetně vlastní desky plošného spoje a osazení součástkami. Tento postup byl vyloučen pro svou časovou náročnost, nespolehlivost, komplikovanou reprodukovatelnost, otázku bezpečnosti i finanční nerentabilitu. Při výběru vhodného hardwarového řešení navrhovaného zařízení bylo vzato do úvahy několik podstatných podmínek. Určující podmínkou bylo samotné plánované nasazení do specifického prostředí, tj. *ve zdravotnictví*. Vstupním požadavkem byly vysoké nároky na mechanickou odolnost, spolehlivost, bezpečnost i odolnost vůči chemickým prostředkům užívaným k dezinfekci a očistě ploch ve zdravotnictví. Pro tyto vysoké nároky kladené na vývojovou desku bylo postupně zavrženo mnoho veřejně známých a oblíbených (amatérských) vývojových desek. Jedinou objektivně vhodnou volbou se ukázala zařízení v průmyslové kvalitě. Zároveň se však jedná o návrh prototypu a nasazování průmyslových počítačů do zdravotnictví bylo hodnoceno jako neefektivní. Cílem bylo nalézt hardware:

- v průmyslové kvalitě
- optimálně open source (svobodný software) s již hotovými řešeními, která by potvrdila vhodnost pro nasazení ve zdravotnickém zařízení
- vyloučení stavebních zásahů a úprav, tj. hardware musel být napájen z baterie a být schopen zasílat informaci bezdrátově

Předem stanovené požadavky splnil produkt od libereckého startupu HARDWARIO založený roku 2016. HARDWARIO s.r.o. nabízí pro tuto práci vhodnou průmyslovou stavebnici IoT Kit TOWER, tak i víceúčelový IoT Hub CHESTER, který byl použit v některých případových studiích. Zařízení CHESTER nabízí konektivitu pro LPWAN sítě, je schopno pracovat z baterie dlouhé měsíce, jedná se o open source a hardware je v průmyslové kvalitě. Produkty HARDWARIO jsou nasazované v průmyslu i dalších odvětvích a jsou k dispozici hotová řešení.

Pro úspěšné řešení nastavení přenosu pro zasílání stavu přístroje stiskem tlačítka bylo nutno zvolit cloudové úložiště, kam se určená data budou předávat a kde bude možné tyto data dále zpracovávat. Cloud je všeobecný název pro, odkudkoli z internetu dostupné, serverové úložiště dat. Skupinu diskových polí a serverů atd. si může do svého prostoru zakoupit a spravovat jak jednotlivec, tak i organizace, jakými jsou zdravotnická zařízení. Jedná se o řešení nákladné, s velkými nároky na obsluhu i servis. Druhou možností je pronájem nebo zakoupení jistého výpočetního výkonu či úložného místa od provozovatele cloudových služeb. Tato úložiště poskytují i velké softwarové firmy, jako AWS, Cisco, IBM, Microsoft, Oracle aj. (řazeno abecedně).

Vzhledem k plánovanému nasazení do zdravotnického zařízení se nabízela dvě efektivní řešení. První možností bylo užití nemocnicí vlastněných serverů, diskových polí atd. Ovšem cílem této práce je navrhnout prototyp, který bude univerzálně použitelný nezávisle na nastavení soukromých serverových úložišť. Druhou možností bylo použití zdravotnickým zařízením již vlastněného produktu, případně jeho drobné rozšíření. Takovýmto univerzálním produktem je Microsoft 365[1]. Ve velkém nachází uplatnění jeho kancelářský balík Microsoft Office. Jelikož je Microsoft 365 používán ve velké míře ve zdravotnických zařízeních, byl vybrán jako vhodná softwarová platforma i pro navrhované řešení prototypu. Výběrem M365 byly splněny požadavky stanovené na softwarové zpracování a zasílání zprávy. Jedná se o všeobecně známou a používanou platformu, je nezávislá na výpočetním zařízení (serveru) a tedy snadno reprodukovatelná a v neposlední řadě nebude způsobovat výrazné vícenáklady spojené s nasazením navrhovaného prototypu.

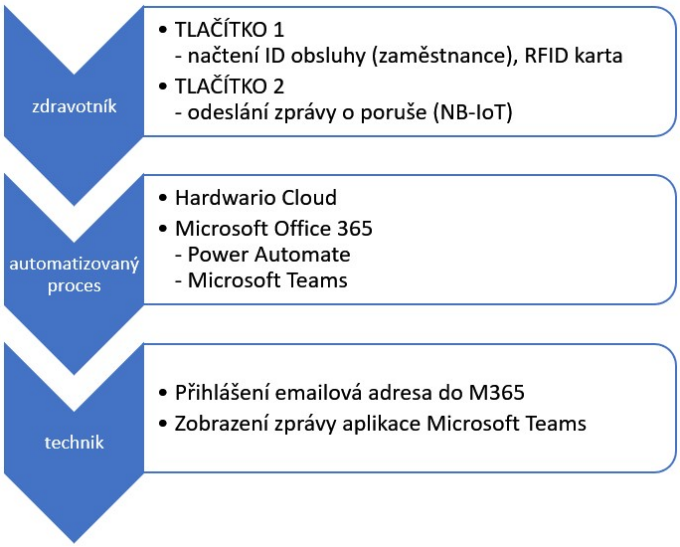


Obrázek 9.1: Topologie prototypu komunikačního zařízení

Prototyp komunikačního zařízení je navržen podle schématu zobrazeného na obrázku 9.1. Navržený prototyp č. 1, 2, …M zasílá přes Vodafone LPWAN síť NB-IoT zprávy do HARDWARIO Cloud. V HARDWARIO Cloud je vytvořen callback z prototypu č. 1, 2, …M. Metodou HTTPS neboli Webhook je poslán obsah callbacku do připraveného softwarového konektoru v Power Automate. Power Automate je

[1]Do dubna roku 2020 známo jako Office 365, po přidání dalších služeb byl název změněn.

součástí licence Microsoft 365. V Power Automate se vytvoří automatizovaný tok pomocí dalších softwarových konektorů, přesněji konektoru na práci s excel tabulkami, konektorem pro nastavení logické operace a konektorem pro zobrazení zprávy na Microsoft Teams ve vytvořené skupině. Microsoft Teams lze prohlížet po přihlášení emailovou adresou v počítači ve webovém prohlížeči nebo v desktopové aplikaci. Zároveň je možné aplikaci Microsoft Teams mít nainstalovanou v tabletu či mobilu, případně si zobrazit zprávy opět ve webovém prohlížeči po přihlášení se přiděleným účtem.



Obrázek 9.2: Ideální tok informace

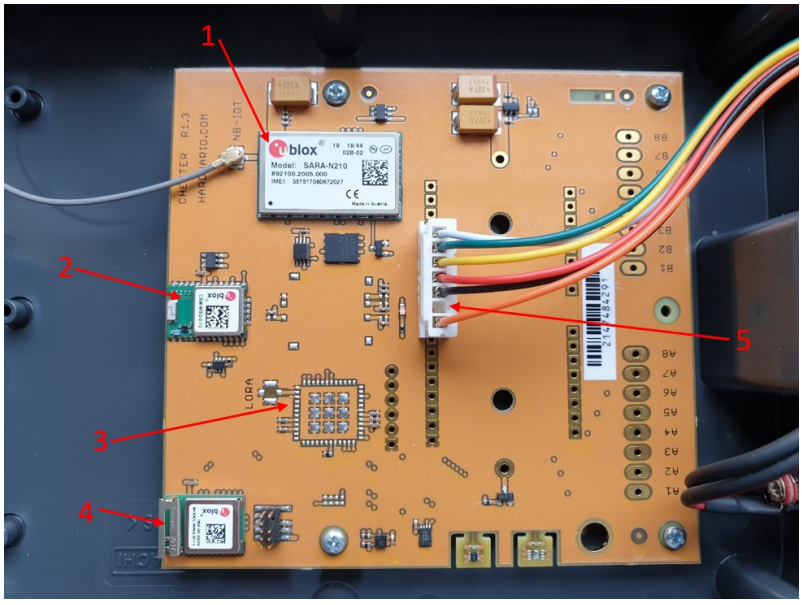
Na obrázku 9.2 je vyobrazeno zpracování dat od vyslání zprávy ze zařízení po zobrazení informace u technika z pohledu zúčastněných stran. Prototyp je umístěn na oddělení na vybraném zdravotnickém přístroji. V případě kritické poruchy zdravotnický personál stiskne tlačítko číslo 1 pro načtení zaměstnanecké RFID karty. Tím je dosaženo identifikace zaměstnance, který nahlašuje vzniklý stav a lze administrátorem nastavit i přístupová práva k nahlašování, tj. ne všichni zaměstnanci budou smět oprávněnou zprávu zaslat. Poslání zprávy se uskuteční po stisku tlačítka číslo 2 po síti NB-IoT. Načtení RFID karty vyžaduje hardwarovou integraci čtečky RFID karet. Jedná se o ideální nastavení prototypu zařízení a pro účely této práce byla hardwarová čtečka RFID karet simulována softwarovým nástrojem cURL a byl vytvořen celý ideální proces. Hardwarově řešený prototyp zařízení umožňuje zasílání zpráv bez autorizace po stisku osazeného tlačítka. Následuje automatizovaný proces, který zprávu uloží do připravené excelové tabulky (obrázek A.4) a vygeneruje dle připraveného formátu zprávu pro technické pracovníky (obrázek A.13). Každý zaměstnanec oddělení zdravotnických přístrojů se přihlásí pomocí pracovního emailu do aplikace Microsoft Teams, kde se zobrazí veškeré zaslané zprávy v založené skupině (team), v tomto případě pojmenované OZT. V rámci teamu je skupinový chat, ve kterém bude moci technik a jeho přihlášení kolegové nejen sledovat nově příchozí zprávy o poruše, ale i o nízkém stavu baterie některého z prototypových zařízení a i sám reagovat na jednotlivé výzvy odpovědí v chatu (obrázek 11.8).

10 Hardwarová část zařízení

Víceúčelový IoT Hub CHESTER byl zvolen jako odpovídající koncept pro hardwarovou část navrhovaného prototypu [82]. Základní představení tohoto zařízení se nachází v teoretické podkapitole s názvem Průmyslová IoT zařízení HARDWARIO. Jako vhodný modul byl zvolen CESTER-Z v kombinaci s CHESTER-M. Celé hardwarové řešení je postaveno jako neinvazivní zařízení, které nezasahuje do lékařského přístroje a tedy není nutná certifikace NÚKIB.

10.1 CHESTER-M

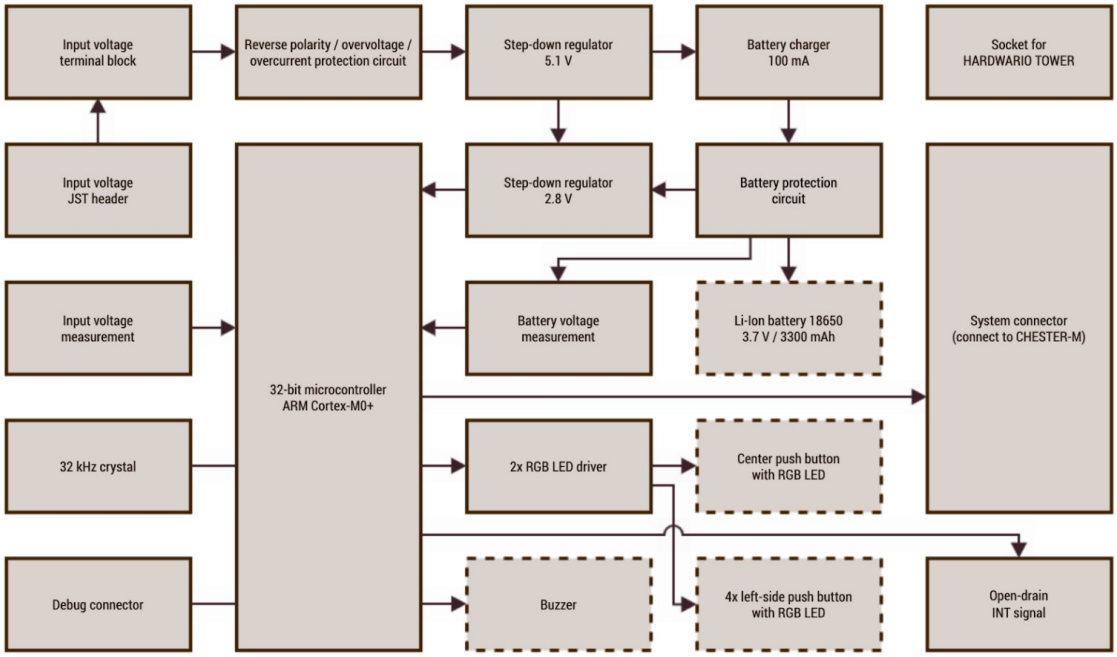
CHESTER-M je základní deska plošných spojů a stavební kámen každého IoT CHESTER Hub. Na obrázku 10.1 jsou číselně označeny podstatné součástky na desce. Číslo jedna je modul pro komunikaci technologií NB-IoT. Při pozorné prohlídce lze na desce vidět gravírované označení. Číslo dva popisuje modul pro technologii GNSS (GPS, Galileo, GLONASS, BeiDou). Pod číslem tři se na druhé straně desky nachází modul pro komunikaci technologií LoRa a číslo čtyři označuje modul pro komunikační technologii Bluetooth. Konektor sběrnice I2C je označen číslem pět.



Obrázek 10.1: Deska CHESTER-M

10.2 CHESTER-Z

CHESTER-Z kombinuje dobíjecí lithium-iontovou bateriovou zálohu, široký rozsah napájecího napětí a volitelné rozhraní člověk – stroj (HMI) s osvětlenými tlačítky a akustickou zpětnou vazbou. Primárně se používá s CHESTER-M, což je základní deska, ale lze jej použít také s HARDWARIO TOWER a ekosystémy třetích stran, jako jsou Raspberry Pi, Arduino, ESP atd. Modul je instalován pod vnějším krytem řady Takachi WP13-18. CHESTER-Z také poskytuje digitální komunikační rozhraní I2C. Prostřednictvím I2C mohou být poskytovány funkce jako příkazy HMI, detekce událostí, informace o stavu, identifikace produktu a informace o verzi. Mezi příkazy HMI patří ovládání LED a bzučáku, jako je jednorázová indikace nebo na pozadí běžící souvislé vzory. Detekcí událostí se označují události tlačítek, tj. stisknutí, uvolnění, klik a podržení. Detekovat lze i události stejnosměrného síťového napětí, tzn. připojení a odpojení. Informací o stavu se rozumí hodnoty stejnosměrného síťového napětí, napětí na baterii a stav tlačítka. Na obrázku 10.2 je zobrazené blokové schéma zapojení CHESTER-Z s 32-bit mikrokontolérem ARM Cortex-M0+.



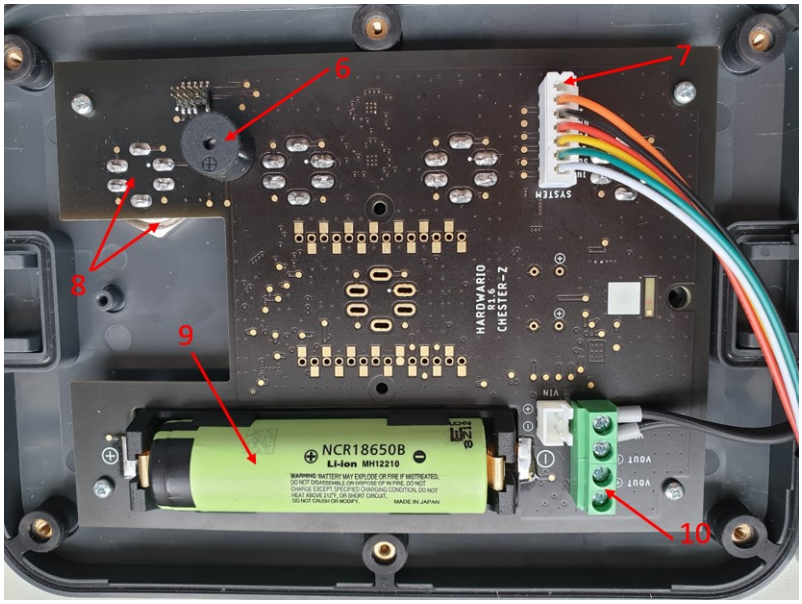
Obrázek 10.2: Blokové schéma CHESTER-Z

Na blokovém schématu jsou přerušovaným okrajem znázorněny volitelné komponenty k osazení na desku. Jedná se o 4 tlačítka na straně a jedno tlačítko ve středu vrchního krytu pouzdra Takachi. Osazení tlačítky je možné v jakékoli kombinaci, případně je možno osazení tlačítky vynechat úplně. Volitelné osazení je též možné u bzučáku a dobíjecího bateriového zdroje.

Na obrázku 10.3 je vyobrazena zadní strana desky plošných spojů včetně osazených součástek. Přední strana není k nahlédnutí z důvodu konstrukčního uspořádání, tj. deska je připevněna připájenými tlačítky k vrchnímu krytu pouzdra Takachi.

Čísla označují podstatné komponenty této desky a začínají číslem šest ve snaze maximálně zpřehlednit popis desky CHESTER-M a CHESTER-Z.

Volitelná komponenta bzučáku, na blokovém schématu uvedená pod anglickým označením Buzzer, je na obrázku 10.3 vedena pod číslem šest. Číslo sedm označuje konektor pro I2C sběrnici. Pod číslem osm je pod dvojicí šipek vidět šestice připájených pinů a kus šestihranné šroubové matice tlačítka v průmyslové kvalitě. Na desce prototypu jsou viditelně naletována čtyři tlačítka, vždy o šesti pinech. Páté místo pro tlačítko ve středu desky je neosazeno. V držáku pro baterii, číslo devět, je nainstalován dobíjecí lithium-iontový článek 18650. Systémový konektor, svorkovnice, nese číslo deset.



Obrázek 10.3: Deska CHESTER-Z

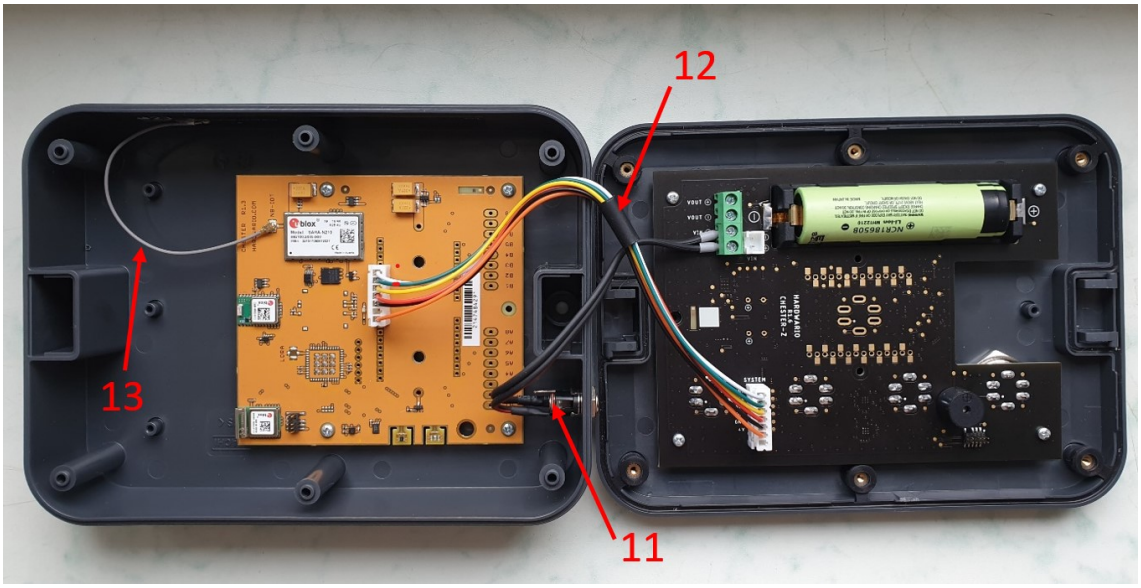
10.3 Prototyp

Varianta hardwarového osazení CHESTER-Z, která byla použita pro sestavení prototypu se nazývá CHESTER-Z1-9 a kód popisuje osazení dobíjecím článkem 3,6 V a 4 tlačítky. Tlačítka jsou osazena v horní části krytu od Takachi, jak je vidět na obrázku 10.4. Tlačítka jsou konstrukčně řešena přišroubováním pomocí šestihranné matice do krytu Takachi a následně jsou piny tlačítek naletovány do desky plošných spojů CHESTER-Z. Na témže obrázku je vidět reakce tlačítka na stisk. Po stisku tlačítka se projeví nastavená audiovizuální kontrola. Ta spočívá v podsvícení tlačítka zelenou barvou po stanovenou dobu, v případě prototypu zařízení je podsvícení nastavené na jednu sekundu. Zároveň se ozve zvukové potvrzení stisku.

Přenos zpráv je realizován po identifikaci účastníka v síti (SIM karta) prostřednictvím modemu NB-IoT po síti provozovatele Vodafone. CHESTER-M je osazen čipem SIM karty. NB-IoT síť byla zvolena pro velice kvalitní pokrytí signálem,

předpokládá se spolehlivé zasílání zpráv i z podzemních či jinak špatně dostupných prostor zdravotnických zařízení. Zároveň není třeba stavět nákladnou vlastní přenosovou síť, jelikož NB-IoT je postavena na již existující architektuře.

Obrázek 10.4: Vzhled prototypu zařízení



Obrázek 10.5: Kompletní vnitřní hardwarové uspořádání

Prototyp komunikačního zařízení pracuje na hardwarové úrovni následujícím způsobem. Deska CHESTER-Z je napájena akumulátorem o maximálním napětí 3,6 V a prostřednictvím nabíjecího konektoru po zapojení adaptéru. Na obrázku 10.5 je tento konektor označen číslem jedenáct, zároveň je viditelný na obrázku

10.4. Přes systémový konektor se vstupy, svorkovnici, jde napájení do komunikátoru CHESTER-Z. Bez externího nabíjení je komunikátor CHESTER-Z zásoben energií z baterie. Ze zdroje jsou napájena tlačítka, procesor a bzučák. Deska CHESTER-Z je do jisté míry autonomní a je osazena držákem pro baterii, do kterého lze nainstalovat dobíjecí lithium-iontový článek s označením 18650. Přes konektor I2C sběrnice komunikuje deska CHESTER-Z s deskou CHESTER-M. I2C komunikace probíhá po svazku vodičů označených na obrázku 10.5 číslem dvanáct. Stav tlačítka po stisku je zaznamenán procesorem na desce CHESTER-Z a poslán do desky CHESTER-M, která následně vyhodnotí událost a dá povel desce CHESTER-Z k indikaci svícení/zvukového signálu a odešle přes NB-IoT síť zprávu. NB-IoT modul integrovaný na desce CHESTER-M používá anténu označenou na obrázku 10.5 číslem třináct. Na desce CHESTER-M je osazena čtveřice modulů pro komunikaci technologií NB-IoT, Bluetooth, GNSS (získání polohy) a LoRa. Rozměrově největší a pro tento prototyp nejpodstatnější je modul SARA-N210 [83]. Jedná se o NB-IoT modul s pásmem pro Evropu, respektive jde o LTE pásmo operátora Vodafone pro Evropu.

10.3.1 Výběr RFID

V zadání této práce nebylo stanoveno, že by bylo vhodné, aby prototyp navrhovaného zařízení byl schopen identifikovat či autorizovat zaslání zprávy. Předmětem bylo pouze navržení systému k zaslání zprávy. Po úvaze celkové koncepce navrhovaného prototypu bylo vhodné nějaký způsob zabezpečení proti neautorizovaným zprávám přidat. Jednak bylo nutno ošetřit situaci, kdy pacient, návštěva pacienta či kdokoli z nemocničního personálu je schopen zasílat zprávy o poruše. Ať již nedopatřením či ze zvídavosti. Druhým podstatným argumentem pro přidání RFID čtecího zařízení byl samotný proces identifikace a autorizace. Přiložením zaměstnanecké karty se načte identifikační kód zaměstnance a bude zaznamenáno, kdo žádal o pomoc. Zároveň je možno nastavit i omezený počet zaměstnanců, který tento úkon budou smět provádět. Autentizace a autorizace požadavku bude zpracována v M365. Každý požadavek bude zaznamenám, ale jen ten od zaměstnance s právy bude zaslán do Microsoft Teams. Tím se zajistí i relevance požadavku. Samotný princip prototypu je postaven na spolupráci zaměstnanců zdravotnického zařízení a jeho zneužívání by vedlo k postupnému přehlížení příchozích zpráv. Došlo by ke ztrátě věrohodnosti i vážnosti situace, pokud by bylo zasláno x neopodstatněných zpráv jen proto, že to prototyp umožňuje a zároveň není způsob, jak odesílatele nalézt a případné zneužívání řešit. Jelikož každý zaměstnanec je vybaven vlastní RFID kartou, bylo nejlogičtějším řešením tuto kartu použít i k identifikaci a autorizaci k posílání zprávy.

RFID technologie pro přístupové karty v naprosté většině užívá jeden ze dvou standardů. Tím prvním je starší nízkofrekvenční systém, anglicky označovaný jako proximity, pracující na frekvenci 125 kHz. Druhým standardem je užití vysokofrekvenční technologie na 13,56 MHz. Tato technologie se označuje též jako MIFARE z Mikron FARE Collection System podle značky RFID čipu. Karty pracující na 125 kHz jsou o krok dále před tradiční magnetickou kartou. Jsou vybaveny mikročipem, který čtečce poskytne identifikační číslo či jiný jedinečný kód. Proces čtení je

aktivován po dodání elektromagnetické energie čipu na kartě z čtečky. Tato krátká dodávka energie je dostatečná k předání ID čísla čipu karty čtečce, která vyhodnotí, zdali je tomuto ID číslu vstup do zařízení povolen. MIFARE v sobě nese předprogramované sériové číslo, jedná se o jedinečné a náhodné uskupení. Šifrovací klíč DES chrání tyto informace a vyšle je až po vzájemné autentizaci mezi kartou MIFARE a čtečkou karet. Dalším rozdílem mezi RFID kartami pracujícími na 125 kHz a 13,56 MHz souvisí s jejich pamětí a možnostmi programování. MIFARE dokáže uložit až 1 kilobajt dat a tudíž nabízí sofistikovanější potenciál pro programování. Lze tak na ní uložit další data. V praktickém využití karet je primární rozdíl ve frekvenci, kterou musí čtečka umět přečíst [84, 85].

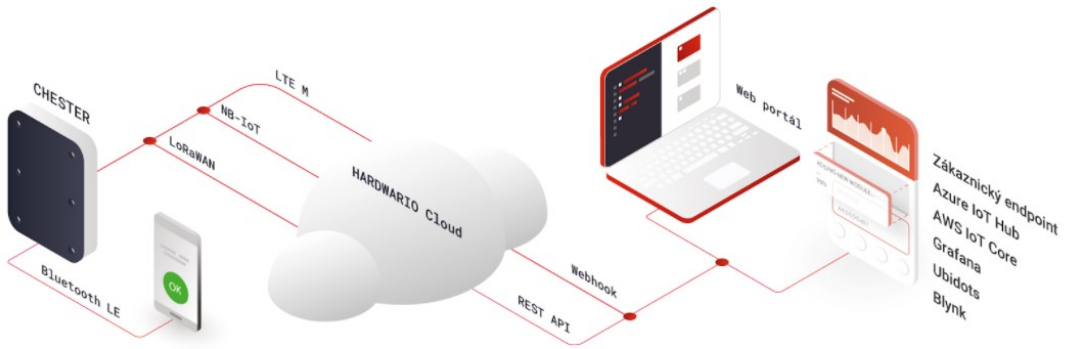
Pečlivým zvážením prošly 2 RFID čtečky, které připadaly v úvahu. Jednalo se o STM32 Nucleo expansion board na 13,56 MHz RFID a o HARDWARIO RFID Module na 125 kHz, které jsou schopné kartu načíst. Hardwarová integrace obou z výše uvedených čteček byla zvážena, ovšem s přihlédnutím k zadání této práce a k časové náročnosti samotného integračního procesu bylo usouzeno, že se jedná o záležitost přesahující rámec této bakalářské práce. Z důvodu časového deficitu nebylo možno integrovat RFID čtečku hardwarově, byla ovšem do plně funkční verze vytvořena část softwarové integrace a to za pomoci softwarového nástroje cURL, který nahradil komunikační zařízení osazené RFID čtečkou. Celá výsledná softwarová struktura ideálního komunikačního prototypu je popsána v kapitole 11.2.2 Power Automate.

11 Aplikační část

V této části je popsána nejprve vždy vybraná platforma a následně její nastavení pro získání žádoucího výsledku, kterým je spolehlivě pracující zařízení. Nejsou přenášeny informace spojené s pacientem, léčbou či jinak chráněnými citlivými údaji. Opět není nutné řešit certifikaci NÚKIB navrhovaného prototypu.

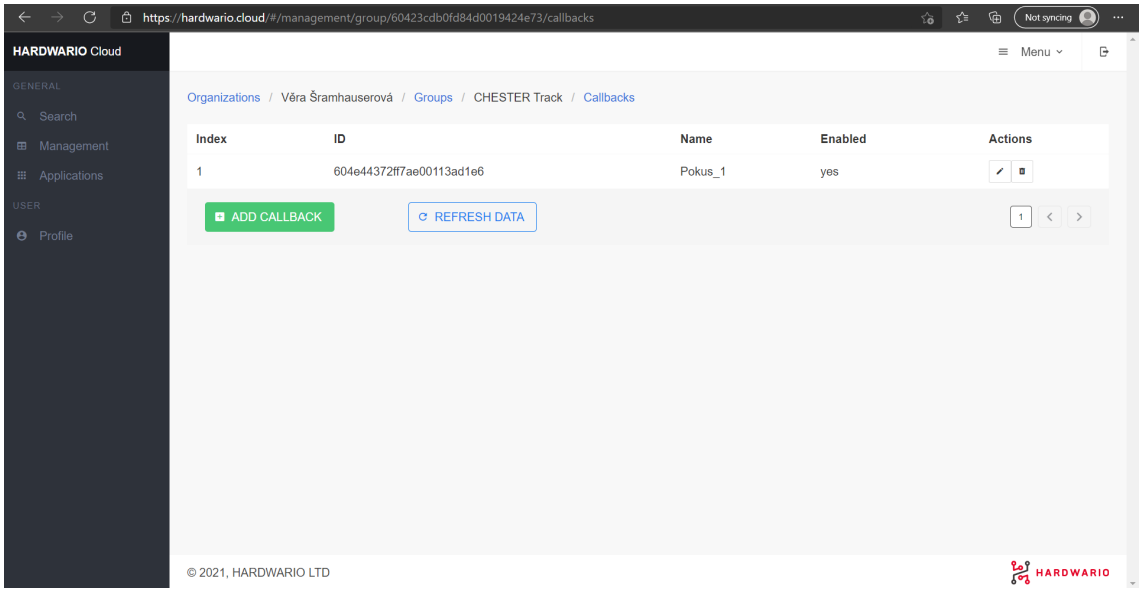
11.1 HARDWARIO Cloud

Pro efektivní propojení byl užit HARDWARIO Cloud. Jedná se o službu výrobce hardwaru, který byl použit pro sestavení fyzického zařízení. Celé prostředí je navržené v anglickém jazyce, proto v popisu níže byly ve velké míře ponechány originální anglické názvy. Infrastruktura HARDWARIO Cloudu je postavená na databázi MongoDB. MongoDB je NoSQL open source software, jedná se o dokumentově orientovanou databázi pracující místo relačních tabulek s dokumenty podobnými formátu JSON, tzv. BSON. Tuto službu lze pro navrhované zařízení použít ve zdravotnictví, jelikož nejsou zasílána citlivá data o pacientech, zaměstnancích ani přístroji. Jedná se o zaslání stavu, který obsahuje pouze identifikaci navrhovaného zařízení (prototypu), stav baterie a případně číslo RFID karty zaměstnance. HARDWARIO Cloud, obrázek 11.1, umožňuje koncentrovat do jednoho bodu cesty jednotlivých podporovaných LPWAN sítí, v tomto případě NB-IoT sítě a propojovat data ze zařízení s dalšími službami.



Obrázek 11.1: Hardwario Cloud

Zařízení mohou být organizována do stromové struktury, na jejímž vrcholu je organizace (zákazník). V případě navrhovaného zařízení jsou data posílána jen jedním hardwarovým zařízením, proto není nastavená stromová struktura. Položka s názvem organizace v HARDWARIO Cloud může mít N skupin (IoT piloty, projekty) a mohou být řazeny dle umístění či účelu. Každá skupina může obsahovat N zařízení a zároveň dovoluje nastavit M tzv. callbacků. Callback je softwarový mechanismus k přenosu zpráv. Každá skupina umožňuje zapnout mechanismus hlášení (reporting) o svých zařízeních, lze uplatnit na jednotlivé uživatele. HARDWARIO Cloud má vlastní webový portál hostovaný na URL adrese https://hardwario.cloud [86]. Po přihlášení do účtu je možno spravovat svůj profil včetně změny hesla. V záložce Management se zobrazuje seznam organizací náležících účtu. Uživatel má pojmenované organizace a po rozkliknutí Groups (skupiny) se lze podívat, jaké skupiny patří pod jednotlivé organizace. Každá skupina má své označení a je možné sledovat, jaká zařízení patří do vybrané skupiny výběrem tlačítka Devices (zařízení). U zařízení lze prohlížet zprávy, záložka Messages, které se zobrazují jako seznam s časovou posloupností. Na každou jednotlivou zprávu je možno se podívat, každá zpráva má svůj unikátní identifikátor. Dále se zobrazuje, kdy zpráva vznikla, tedy časová značka. Na levé straně řádku je šipka, která po otevření zobrazí obsah JSON zprávy generovaný parserem v Cloudu, včetně raw dat (hrubá data) za zařízení. Zároveň, když se vrátíme zpět do seznamu Devices, tak lze vlevo na řádku opět vidět rozbalovací šipku. Po jejím stisku se zobrazí informace o aktivitě zařízení za poslední uplynulý rok. Lze se podívat, kolik zpráv zařízení odvysílalo v kterém jednotlivém dni.

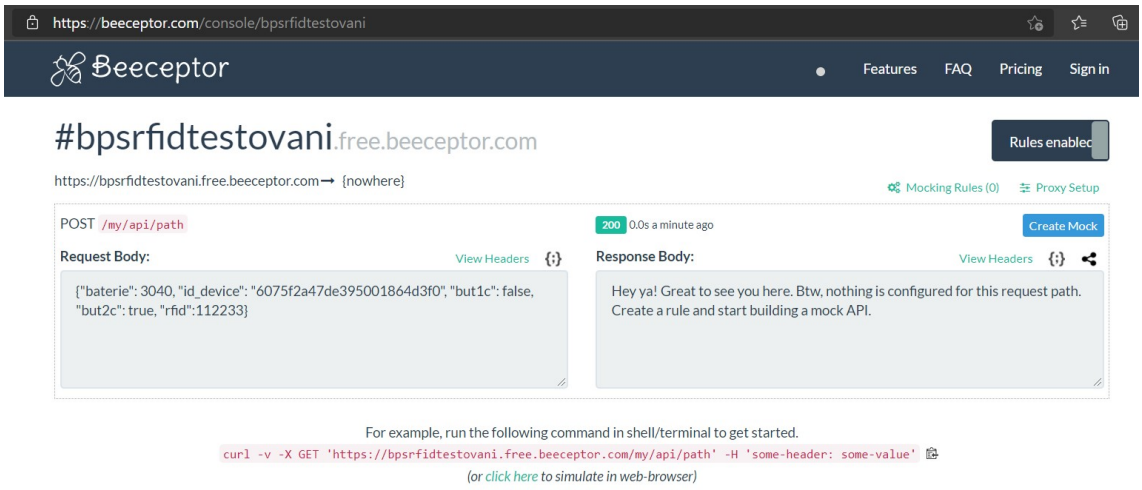


Obrázek 11.2: Zobrazení callbacků

Po návratu do skupin je možné vstoupit do editace skupiny (ikona tužky), konfigurovat reporting, určit pomocí checkboxů, ve které dny HARDWARIO Cloud zašle email s informacemi o dané skupině, o době neaktivity jednotlivých zařízení. V seznamu skupin je vedle možnosti náhledu do zařízení možnost nastavovat callbacky.

Na obrázku 11.2 je náhled v prostředí HARDWARIO Cloud v záložce callbacky. Pro demonstrativní zařízení je vytvořen pouze jeden callback.

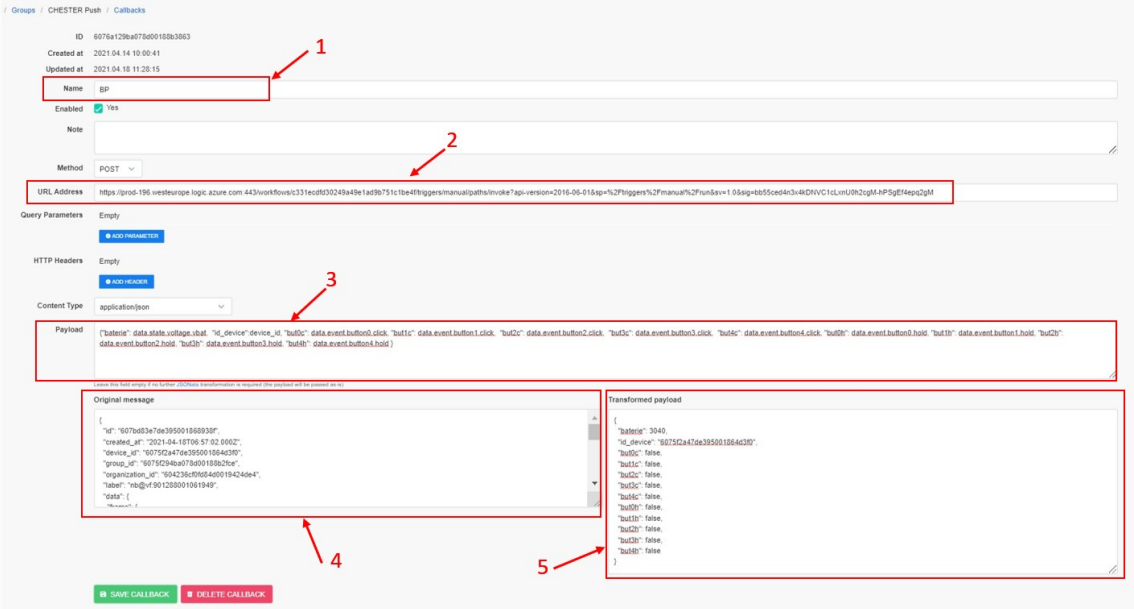
Callback je softwarový mechanismus, který umožňuje přijatou zprávu okamžitě doručit do koncového bodu příjemce (endpoint). HARDWARIO Cloud aktuálně podporuje pouze protokol HTTP pro dopravování zpráv, tzv. Webhooky. Jsou podporovány HTTP metody POST, GET, PUT a PATCH. Je nutné specifikovat URL adresu (obrázek 11.4 číslo pole 2), volitelně je možno zadat parametry dotazu (query parametry) a HTTP hlavičky (především užívané pro autentizaci vůči cílovému koncovému bodu). V dolní části lze transformovat přenášenou zprávu (Payload). Pod polem přenášené zprávy je zobrazená originální zpráva (obrázek 11.4 číslo pole 4), vedle zpráva transformovaná (obrázek 11.4 číslo pole 5). V Payload poli lze vytvořit vlastní šablonu zprávy, která respektuje vybranou cestu za informací z originální zprávy (obrázek 11.4 číslo pole 3). Nejprve se vytvoří prázdný JSON objekt, následně klíč a poté pomocí JSON Data selektoru je popsána cesta k vybrané informaci. Pod polem Payload se nachází odkaz na dokumentaci JSON Data, což je funkcionální jazyk, kterým se provádí transformace. V transformované zprávě se zobrazí JSON, který je očekáván vstupním koncovým bodem. Po vyplnění URL adresy lze callback uložit. Pro testování dopravování zpráv callbacku lze užít např. službu Beeceptor, která je zdarma, vygeneruje URL adresu a umožní vytvořit provizorní koncový bod. Služba Beeceptor byla užita společně se softwarovým nástrojem cURL pro testování a vývoj aplikační softwarové části prototypu zařízení. Na obrázku 11.3 je část z prováděného ladění finální formy JSON pro simulované zasílání zprávy po načtení zaměstnanecké RFID karty. Toto odlaďování předcházelo samotnému zasílání již připravené JSON zprávy na vygenerovanou doménovou adresu serveru Power Automate.



Obrázek 11.3: Nástroj Beeceptor s cURL

Pro zakázání callbacku je nutno odškrtnout checkbox a smazat jde tlačítkem Delete callback. Užití callbacků má výhodu v tom, že informaci umí zaslat hned poté, co data dorazí do cloudu. Existuje i druhá možnost přístupu a to pomocí REST

API. REST API je dokumentované na URL adrese https://api.hardwario.cloud. Dokumentace využívá standardní průmyslem akceptovaný formát Swagger. V dokumentaci se nachází seznam všech koncových bodů. Webový portál HARDWARIO Cloud je v podstatě frontend pro REST API. Prakticky nejdůležitější je koncový bod zprávy (messages). Podporuje nejčastější metodu GET a Received and Confirm. Received and Confirm funguje podobně jako poštovní klient. Pomocí Received je stažena nepřečtená zpráva a po zpracování je pomocí Confirm potvrzena. Koncový bod následně Received už nezasílá znovu, což zjednodušuje implementační strukturu. Měsíční poplatek za HARDWARIO Cloud činí 50 Kč za jedno zařízení.



Obrázek 11.4: Vytvoření callbacku

Na obrázku 11.4 je vidět stav po uložení nově nastaveného callbacku pro navrhovaný prototyp komunikačního zařízení. Callback byl pojmenován BP, jakožto zkratka bakalářské práce, na obrázku je pole pro název vyznačeno číslem 1. Do URL adresy, pole označené číslem 2, byl vložen odkaz vygenerovaný SW konektorem v Power Automate s názvem *When a HTTP request is recieved*, který je popsán v podkapitole 11.2.2. Pro účel komunikačního zařízení bylo nutné zasílat identifikační číslo CHESTER a napětí na bateriovém článku pro prediktivní údržbu prototypu. Toto nastavení bylo provedeno z původní zprávy (Original message), pole s číslem 4, v poli Payload s číslem 3. Pro filtrování zpráv došlých po stisku tlačítka jsou zasílány Booleovské logické operátory. Hodnota true se zasílá po stisknutí tlačítka, ostatní tlačítka bez stisknutí zasílají hodnoty false. Výsledná podoba vybraných informací z originální zprávy je zobrazena ve zprávě transformované (Transformed payload), pole s číslem 5.

Na obrázku A.1, nacházejícím se v přílohách, je záznam callbacku jedné z vybraných zpráv. Tato zpráva byla odeslána po stisku tlačítka číslo čtyři, jak je možno vidět v oddělení požadavku (Request). Stisknuté tlačítko zaslalo datový typ boolean pravda (true). Ostatní tlačítka zůstala bez odezvy ve stavu false. V Request je

zaznamenána metoda HTTP POST, uživatel, tedy HARDWARIO Cloud Callback, URL adresa koncového bodu, kterým je softwarový konektor v Power Automate s názvem *When a HTTP request is recieved*. Níže jsou pod sebou seřazeny vybrané informace posílané ve formátu JSON. Druhá část je odpověď (Response) serveru na zasílaný požadavek.

11.2 Microsoft 365

Microsoft 365, do dubna minulého roku známo pod názvem Office 365, je skupina cloudových služeb poskytovaných firmou Microsoft na základě předplatného. Poprvé se tento produkt objevil v nabídce v roce 2011. Microsoft 365 podporuje snadné sdílení souborů, týmovou komunikaci a propojuje samostatné softwarové nástroje s online službami.

Speciálně pro nabídku softwarových nástrojů byl založen účet Microsoft 365 předplatné typu E5 pro adresu vera.sramhauserova@nemocnicehornidolnilhota.onmicrosoft.com. Tento účet je administrátorský. Za účelem simulace pracoviště správy zdravotechniky byly založeny další dva účty v rámci licence M365. Jedná se o účet Zdravotechnika@nemocnicehornidolnilhota.onmicrosoft.com a Metrologie@nemocnicehornidolnilhota.onmicrosoft.com. Tyto účty představují fiktivní zaměstnance fiktivního oddělení správy zdravotechniky fiktivní Nemocnice Horní Dolní Lhota.

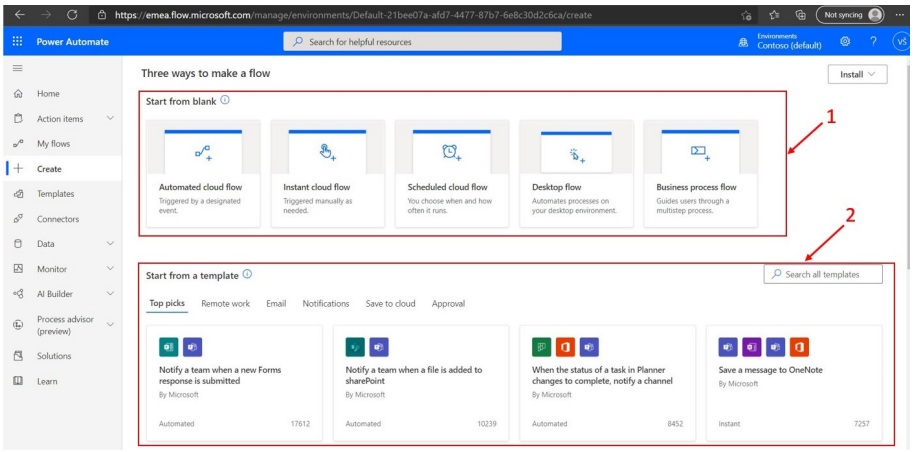
11.2.1 Power Platform

Power Platform je souhrný název pro čtyři produkty Microsoftu. Jedná se o Power BI, PowerApps, Power Automate a Power Virtual Agents. Toto spojení vytváří výkonnou platformu podnikových aplikací. Poskytují prostředky pro snadnější nakládání, zobrazování, automatizování a analýzu dat. Mohou být použity s Microsoft 365, Dynamics 365 i s aplikacemi třetích stran a dalšími službami od Microsoftu. Power Platform umožňuje spolupráci všech služeb prostřednictvím Common Data Service neboli Dataverse, což je základní datová platforma poskytující jednotné schéma spolupráce [87].

11.2.2 Power Automate

Power Automate, dříve známé jako Microsoft Flow, je cloudová služba umožňující a usnadňující automatizovat časově náročné úkoly a procesy. Je integrovanou součástí M365. Pro přihlášení je potřeba emailová adresa, lze použít i mobilní aplikaci. Je k dispozici pouze jako veřejná cloudová služba. Power Automate umožňuje propojení s více než 100 různými zdroji dat. Těmi jsou standardní služby od Microsoftu i služby třetích stran. Propojení se zdroji dat umožňují tzv. SW konektory. Konektor je obálka (wrapper) kolem API (Application Programming Interface), který umožňuje komunikaci mezi základní službou a Microsoft Power Automate, Power Platform. Poskytuje způsob, jak propojit své účty a využívat sadu předpřipravených

softwarových akcí a spouštěčů pro vytváření aplikací a postupů. Jedná se o rozsáhlý ekosystém konektorů softwaru jako služby (SaaS). Součástí každého softwarového konektoru je sada operací klasifikovaných jako Akce (Actions) a Spouštěče (Triggers). Akce jsou změny řízené uživatelem, jsou vhodné například k vyhledávání, zápisu, aktualizaci či odstranění dat v databázi. Několik SW konektorů poskytuje Triggery, které jsou schopné upozornit na nastalou konkrétní událost.



Obrázek 11.5: Vytvoření nového toku

Triggery se dělí na dva typy, prvním je dotazování. Tento spouštěč volá vytvořenou službu podle zadané frekvence a kontroluje nová data. Pokud jsou nová data k dispozici, vyvolá nové spuštění pracovního postupu s daty jako vstupem. Druhým typem je „postrčení“, častěji se užívá anglické označení push, kdy Trigger naslouchá datům v koncovém bodě a čeká na výskyt nové události. Výskyt události, např. stisk tlačítka, způsobí nové spuštění nastaveného pracovního postupu. V Power Automate lze vytvořit vlastní toky (Flow), obrázek 11.5, seřazením potřebných konektorů (pole označené číslem 1) nebo využít již připravených šablon (pole číslo 2) [88].

Šablony jsou předem vytvořené datové toky pro oblíbené a často vyhledávané scénáře. Použití šablony vyžaduje pouze přístup ke službám v šabloně a zároveň vyplnění všech požadovaných nastavení. Pro připojení k REST API je potřeba vytvořit vlastní SW konektor, který využívá JSON a podporuje nejméně jednu z metod ověřování. Některé SW konektory jsou označené jako Premium a tedy dostupné ve zkušební verzi na 60 dní, následně se platí poplatek 15 dolarů měsíčně. Vytvořené toky je možno sdílet, nastavovat práva pro spravování a úpravy či udělovat oprávnění ke spouštění. Množství toků se odvíjí od vlastněné licence a u každého toku lze pomocí přepínače zapnuto/vypnuto nastavovat zpracovávání žádostí.

Na obrázku 11.6 se nacházejí dvě grafická schémata vytvořených toků. Oba dva toky jsou označeny šipkou ve směru průběhu sestavených logických operací za pomoci jednotlivých softwarových konektorů. Tok označený šipkou „A“ byl vytvořen pro sestavené hardwarové zařízení, které bylo popsáno v kapitolách výše. Tok označený šipkou „B“ byl vytvořen pro modelové zařízení s integrovaným RFID modulem. Pro oba dva nastavené toky byly užity stejné SW konektory v různém počtu. Prvním softwarovým konektorem je funkce pro příjem HTTP požadavku, anglicky *When*

a HTTP request is recieved. Tento SW konektor vygeneruje po uložení flow (toku) URL adresu zadanou v callbacku z HARDWARIO Cloud. Do vnitřního pole se vkládá JSON formát očekávané zprávy z callbacku. Tímto způsobem probíhá poslání zprávy z prostředí HARDWARIO Cloud do prostředí Power Automate. obrázky jednotlivých vyplněných softwarových konektorů jsou v kapitole A.2 Přílohy a to včetně výpisu JSON zprávy, připravených excelových tabulek a requestu posílaného pomocí cURL pro RFID tok a případných poznámek.

Obrázek 11.6: Grafické znázornění toků

Následuje softwarový konektor *Convert time zone*, který, jak anglický název popisuje, upravuje časovou zónu z výchozího nastavení koordinovaný světový čas (UTC) na časovou zónu České republiky. Softwarové konektory se znakem excelové tabulky s názvem *Add a row into a table* a *Get a row* pracují s předem připravenými a následně pomocí těchto SW konektorů připojenými excelovými tabulkami. V prvním případě se vybrané hodnoty do tabulky zapisují, v druhém případě flow

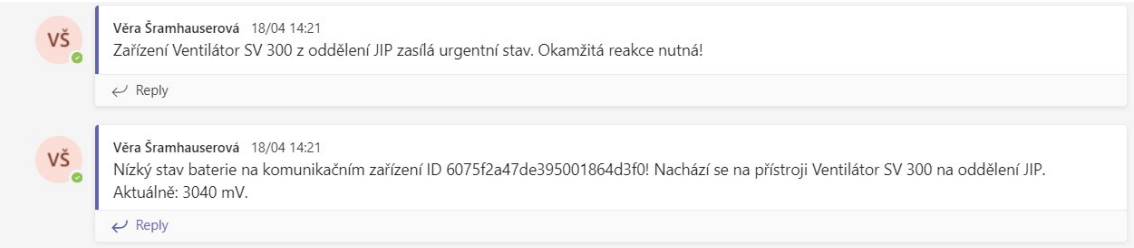
do tabulky nahlíží a vybírá si z ní data. Tabulka, do níž je prováděn zápis přijatých zpráv, slouží jako databáze a zároveň nad ní později jde vytvořit analýza a statistika (vhodné především při reálném dlouhodobém nasazení prototypu ve zdravotnickém zařízení). Šedou barvou označený softwarový konektor *Condition* je stavový konektor s možností nastavení porovnání dat a následnou akcí v případě splnění podmínky, zelený konektor *If yes*, případně nesplnění podmínky, oranžový konektor *If no*. Posledním použitým softwarovým konektorem je *Post a message (V3)* neboli pošli zprávu do služby Microsoft Teams. V tomto konektoru je nutno nastavit vybraný team (skupinu) a formát zasílané zprávy.

Vytvořené toky byly exportovány ve formátu .zip souboru z Power Automate a přiloženy k elektronické verzi této bakalářské práce. Cílem je zpřístupnit tuto šablonu a zjednodušit tak nasazení do zdravotnického zařízení. Ke stažené šabloně je potřeba vytvořit nové excelové tabulky a připojit Microsoft Teams. Pro spustění je nutno vlastnit licenci M365 a za poplatek patnáct dolarů měsíčně získat prémiový softwarový konektor *When a HTTP request is recieved*. Pro testování je možno si tento SW konektor bezplatně vyzkoušet po dobu dvou měsíců.

11.2.3 Microsoft Teams

Microsoft Teams je služba integrovaná v Microsoft 365. Jedná se o platformu umožňující textovou komunikaci, sdílení souborů a videokonference. Zároveň poskytuje datové úložiště a možnost integrace s dalšími aplikacemi. Microsoft Teams lze po přihlášení zobrazit ve webovém prohlížeči, v počítačové i mobilní aplikaci [89].

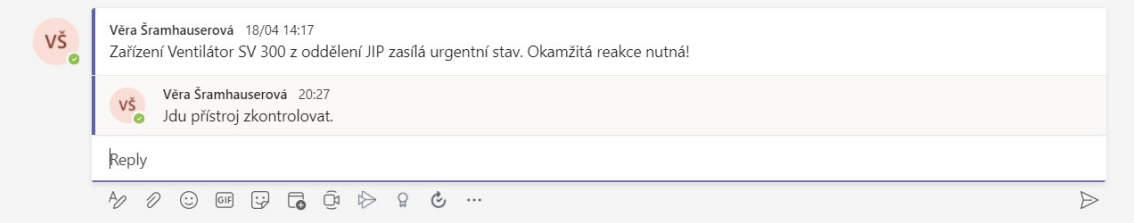
V nemocnicích používané, a proto pro tento projekt vybrané, licence M365 je součástí i služba Microsoft Teams, kde byl založen team (skupina) s názvem OZT, OZT je zkrácený název pro oddělení zdravotechniky. V teamu se nachází správce a vlastník skupiny a dva fiktivní zaměstnanci Jana Zdravotechnika a Tomáš Metrologie. V záložce Posts se zobrazují hlášení s žádostí o okamžitý zásah na zařízení a v případě poklesu napětí na baterii i oznámení, že je nutná údržba nasazeného zařízení. V momentě, kdy je doručena některá z výše popsaných zpráv do aplikace Microsoft Teams, některý ze zaměstnanců, příp. správce může okamžitě reagovat a přistoupit k nápravě urgentního stavu.



Obrázek 11.7: Zobrazení zprávy v Microsoft Teams

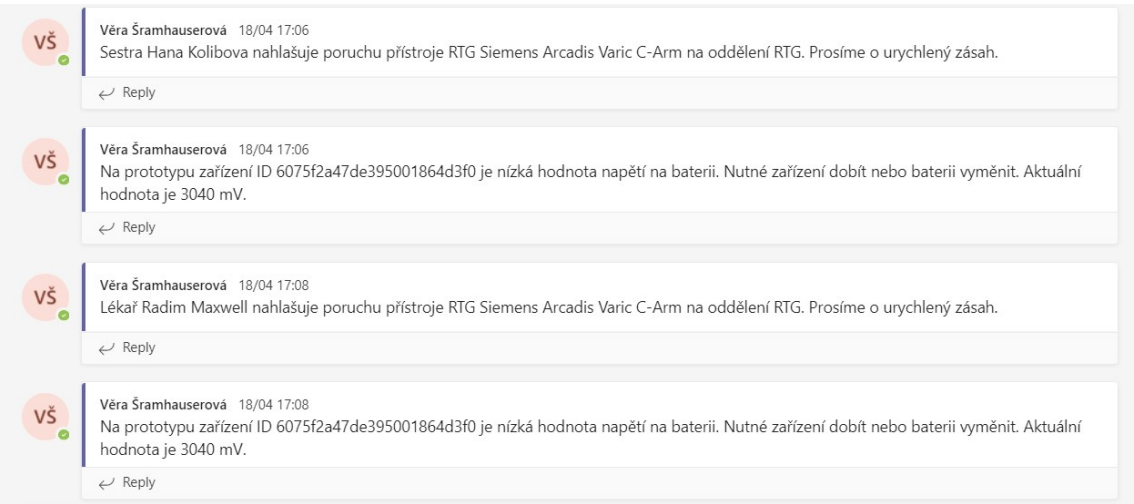
Na obrázku 11.7 jsou zaznamenány dvě zprávy ze sestaveného hardwarového zařízení. První zobrazená zpráva o poruše na ventilátoru SV 300 je zaslána po stisku tlačítka na navrženém a sestaveném prototypu komunikačního zařízení. Druhá

zpráva s informací o nízkém napětí na baterii se zašle v případě, že hodnota napětí klesne pod, v Power Automate a excelové tabulce nastavený, limit 2,8 V. Každý sestavený prototyp zařízení zasílá v každé zprávě svůj jedinečný identifikátor (ID), který je možno ztotožnit v databázi s výrobním číslem/typem zdravotnického přístroje, ke kterému je přiřazen. Ten se zobrazuje ve zprávě o nutnosti dobít či vyměnit bateriový článek, aby bylo jednoznačné, které zařízení vyžaduje údržbu. V případě použitého Li-Ion článku, který má maximálně 3,6 V, byla limitní hranicí nastavena hodnota 2,8 V. Na takto zobrazenou zprávu může technický pracovník reagovat odpovědí po stisku Reply (odpověď), jak je vidět na obrázku 11.8. Tím se otevře řádek pro písemnou odpověď, případně lze přiložit k přijaté zprávě například obrázek poškozeného přístroje pořízený technikem.



Obrázek 11.8: Reakce v chatu

Všechny zde přiložené obrázky zpráv z Microsoft Teams byly pořízeny z webové formy tohoto softwarového nástroje. V aplikaci Microsoft Teams, ať na počítači, tabletu či v mobilním zařízení je formát zpráv identický a to včetně funkcí. V mnohých ohledech je aplikace praktičtější pro reálné každodenní používání. Používání tohoto SW nástroje v mobilním zařízení především zjednodušuje přikládání fotodokumentace poruchy zařízení, tím může být například poškozená izolace napájecího kabelu, poškozený kryt přístroje nebo chybová hláška na displayi zdravotnického přístroje.



Obrázek 11.9: Zprávy po identifikaci RFID kartou

Na obrázku 11.9 jsou zobrazeny čtyři zprávy ze simulovaného prototypu komunikačního zařízení s integrovaným RFID modulem. Dvě zprávy nahlašují nízký stav napětí na dobíjecím Li-Ion článku. Systém zobrazení nízkého napětí je identický se zprávou zasílanou hardwarovým prototypem. Přidaná hodnota RFID identifikace se projevuje v možnosti nastavit do zobrazované zprávy jak pracovní pozici zaměstnance nahlašujícího poruchu, tak jeho jméno, jak je vidět na dvou totožných zprávách oznamující poruchu na RTG zařízení. Totožnou zprávu poslali dva různí fiktivní zaměstnanci. Tím prvním je sestra Hana Kolibova, druhým lékař Radim Maxwell. Načtení čipu RFID karty a zaslání zprávy neautorizovaným zaměstnancem, tj. zaměstnancem, jehož číslo čipu RFID karty není uloženo v seznamu autorizovaných zaměstnanců k nahlašování poruchy zdravotnického zařízení, je zaznamenáno do databáze zaslaných zpráv v excelové tabulce, ovšem do zpráv v Microsoft Teams pro biomedicínské techniky a inženýry se nezobrazí. Nicméně je možno s touto událostí pracovat prostřednictvím administrátorského účtu. Tím jsou vyřešeny dvě věci. Tou první je možnost kontroly a případné řešení zneužívání nastaveného komunikačního prototypu osobami, které k tomu nemají nastavená práva. Druhou, že k technickým pracovníkům se dostávají pouze autorizované žádosti o naléhavé řešení vzniklé vážné situace.

Obsah simulovaných zpráv zaslaných po načtení RFID čipu byl generován, jak již v této práci několikrát zaznělo, pomocí SW nástroje cURL. Tento nástroj je postaven na SW knihovně LibcURL a nástroji pro příkazový řádek cURL. Podporuje množství běžných komunikačních protokolů, je multiplatformní a publikovaný pod licencí MIT. Snímek 11.11 je obrázkem příkazové řádky přes níž je posílán stav baterie, ID zařízení, stav tlačítek, RFID číslo čipu zaměstnance a URL adresa koncového bodu, tj. SW konektoru *When a HTTP request is recieved* v Power Automate.

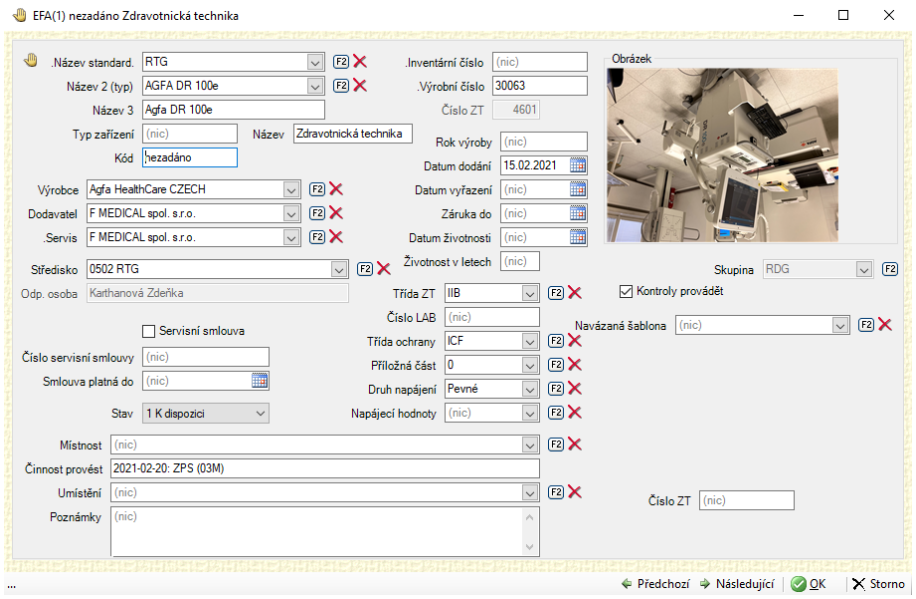
```
curl -H "Content-Type: application/json" -d "{\"baterie\": 3040, \"id_device\": \"6075f2a47de395001864d3f0\"
, \"but1c\": true, \"but2c\": false, \"rfid\":112112}" "https://prod-132.westeurope.logic.azure.com:443/
workflows/d4fce7c0e4fb499f887b40c8d7f9e9c5/triggers/manual/paths/invoke?api-version=2016-06-01&sp=%
2Ftriggers%2Fmanual%2Frun&sv=1.0&sig=Y7CBdExF7Mj5sj0ENd6OHwXWxvqMz0AJoDvOpNCwgug"
```

Obrázek 11.10: Kód k vložení do příkazové řádky

Obrázek 11.11: Vstupní data pro simulaci RFID zprávy v příkazové řádce

12 Otestování na zdravotnickém přístroji

Otestování navrženého prototypu se uskutečnilo v reálném provozu na radiologickém oddělení Ústavu pro péči o matku a dítě v Praze (dále jen ÚPMD). Radiologické oddělení je uzavřené, s kontrolovaným pohybem pacientů a tudíž pro krátkodobé testování ideální. Prototyp nenarušoval běžný provoz. Testování proběhlo ve dvou týdnech a to se dvěma kusy navrženého prototypu komunikačního zařízení. Tyto dva prototypy byly umístěny na dva rentgenové přístroje a to na RTG AGFA DR 100e s výrobním číslem 30063 a RTG AGFA DR 400 s výrobním číslem 2212.



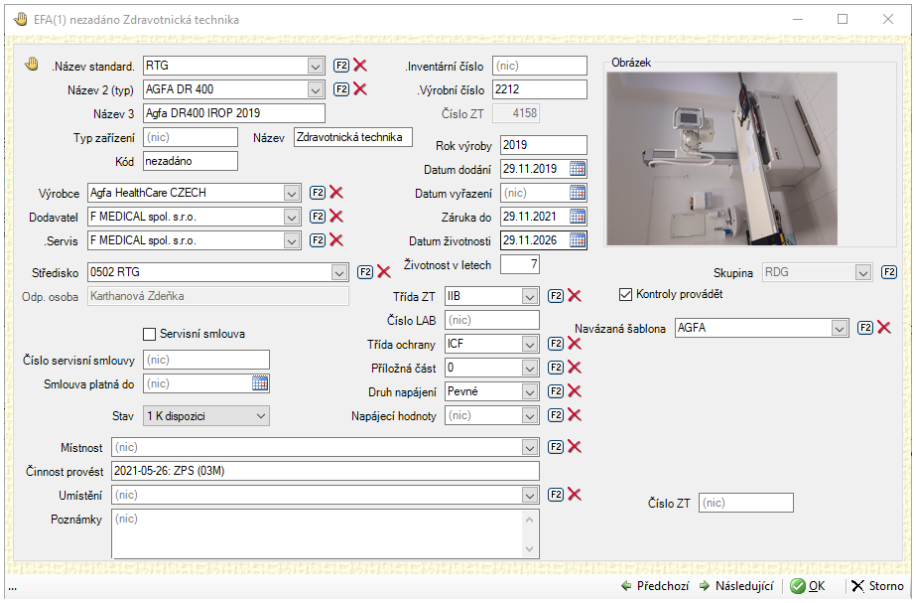
Obrázek 12.1: RTG AGFA DR 100e

Na obrázku 12.1 je snímek karty[1] zdravotnického přístroje AGFA DR 100e pořízený z databázového systému pro správu zdravotnických přístrojů SW EFA od firmy EFA SERVICES. Na obrázku 12.2 je karta[2] druhého zdravotnického přístroje, na němž se testoval navržený prototyp. Jedná se o RTG AGFA DR 400. Navrhovaný prototyp má význam nasazovat především u strategických a životně důležitých přístrojů, jakými jsou například plicní ventilátory, operativa, RTG aj.

[1] Obrázek rentgenového přístroje je otočen o 180 stupňů, jelikož se jedná o snímek karty v systému EFA a je tímto způsobem do karty uložen.

[2] Obrázek rentgenového přístroje je otočen o 90 stupňů, jelikož se jedná o snímek karty v systému EFA a je tímto způsobem do karty uložen.

V databázovém systému SW EFA byly vyhledány historicky řešené požadavky formou žádanky. Z nich vyplývá, že doba reakce biomedicínského technika či biomedicínského inženýra na žádankou zaslanou informaci o poruše se pohybuje, v případě dvou výše zmíněných rentgenových přístrojů, do 60 minut. Jedná se o přístroje strategické a životně důležité. Za reakci je považováno přijetí této žádanky a následná návštěva oddělení s vyhodnocením stavu a stanovením následného řešení. Přestože se jedná o dlouhou dobu, je nutné přihlédnout k obvyklému postupu. Ten na straně BMT či BMI začíná přihlášením do databáze pro správu zdravotnických přístrojů, přihlášení do emailové schránky a případných dalších aplikací na stolním počítači. K SW EFA je možno zakoupit taktéž licenci pro mobilní zařízení, tj. smartphone či tablet. Tuto rozšiřující licenci však ÚPMD aktuálně nevlastní.

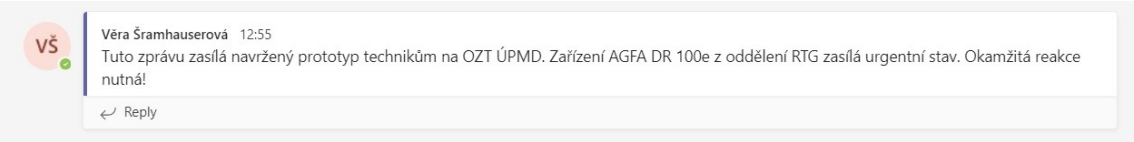


Obrázek 12.2: RTG AGFA DR 400

Žádanek ve zdravotnickém zařízení o velikosti ÚPMD, při kvalitním vedení servisních zásahů, přichází na oddělení zdravotechniky průměrně každý den dvacet. Při tomto počtu lze reakci na nahlášení vzniklého stavu v řádech hodin považovat za uspokojivě rychlou. Do tohoto času však není započítán čas strávený nelékařskými zdravotnickými pracovníky (nejčastěji zdravotní sestra) při psaní žádanky. Zdravotní sestra musí najít během pracovní doby, obvykle mezi příjmem jednotlivých pacientů, čas na spuštění databázového systému pro správu zdravotechniky a ve vhodném modulu napsat žádanku s popisem události. Čas k této činnosti je do značné míry individuální a odvíjí se i od IT schopností každého jednotlivého zaměstnance. Přesto lze uvést, že průměrná doba napsání jedné žádanky včetně všech s tím souvisejících úkonů, je asi třicet minut. Z praxe vyplývá, že vzhledem k přednosti řešení stavu pacientů je psaní žádanek, vyžadujících průměrně třicet minut z času zdravotní sestry, zdržující a je odsouváno na konec pracovní doby, případně až na dobu, kdy bude méně pacientů vyžadovat péči. Tímto odsouváním nahlášení poruchy či jakéhokoli neobvyklého stavu zdravotnického přístroje vzniká další časo-

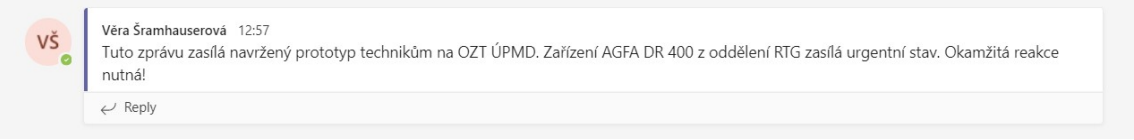
vá prodleva protahující servisní zásah až na několik dní, v extrémních případech až na týdny (zde se nejedná o život ohrožující přístroje). Je nutno též uvažovat dobu nevyužití zdravotnického přístroje, který při poruše negeneruje žádný zisk, ten je vytvářen zdravotnickým přístrojem pouze při jeho používání. Do tohoto shrnutí není zahrnut čas, který na opravu vyžadují externí servisní organizace, jedná se o data pro tuto práci bezpředmětná. Externí servisní organizace potřebuje čas na opravu, který je nezávislý na interních procesech zdravotnického zařízení.

Během testování navrženého prototypu zařízení přišlo sedm zpráv, z nichž čtyři byly testovací a zbylé tři reagovaly na, za provozu vzniklé, události. Testovací zprávy byly zaslány vždy na počátku týdne z každého prototypu zařízení. Po dvou týdnech a při dvou testovaných prototypech zařízení zde dostáváme ony čtyři zprávy, které byly zmíněny výše. Jedna zpráva (obrázek 12.3) přišla po stisku tlačítka na prototypu umístěném na RTG AGFA DR 100e s výrobním číslem 30063.



Obrázek 12.3: Formát zprávy při testování pro AGFA DR 100e

Zbylé dvě zprávy (obrázek 12.4) byly zaslány z prototypu přiděleného pro RTG AGFA DR 400 s výrobním číslem 2212. Pro testování navrženého prototypu komunikačního zařízení byl na oddělení správy zdravotechniky zapůjčen pro tuto práci vytvořený účet Microsoft Teams. Z toho důvodu se formát zpráv výrazně neodlišuje od těch, které byly prezentovány v podkapitole 11.2.3 Microsoft Teams.



Obrázek 12.4: Formát zprávy při testování pro AGFA DR 400

Zaslání informace zdravotnickým personálem vyžaduje, v případě navrhovaného prototypu, ve všech sedmi zaslaných zprávách, čas do dvou minut, přičemž samotný stisk tlačítka trvá do deseti sekund, jak plyne z dat uložených v HARDWARIO Cloud. Zbylý čas dvou minut je uveden, aby byla zahrnuta též úvaha zdravotníka nad samotným úkonem zaslání zprávy. V případě simulovaného zařízení osazeného RFID čtečkou přibude přiložení zaměstnanecké karty do vzdálenosti dvou centimetrů od prototypu CHESTER. Předpokládané časové nároky v tomto případě narostou z deseti sekund na třicet sekund. Po odeslání zprávy se do deseti sekund zobrazí zpráva pověřenému biomedicínskému technikovi či biomedicínskému inženýrovi na preferované zařízení, případně na všechna zařízení vlastněná BMT a BMI, smartphone, tablet, počítač, jak bylo zaznamenáno v excelové databázi a ve výpisu historie proběhlých toků v Power Automate. Biomedicínský technik nebo biomedicínský inženýr

si na mobilním zařízení zprávu prohlédne v horizontu do deseti minut, na počítači do hodiny.

Z testování prototypu v reálném provozu lze vyčíst úsporu času o celé řády, prototyp je schopen zaslat zprávu včetně stisku tlačítka zdravotní sestrou a zobrazení zprávy BMT či BMI v ideálním případě do tří minut. Pokud bude počítán jen čistý čas pro proces stisk tlačítka, zasílání zprávy po NB-IoT, zobrazení zprávy v Microsoft Teams, hovoříme o třiceti sekundách až jedné minutě v závislosti na síle pokrytí NB-IoT signálem. Žádankový systém vyžaduje v ideálním případě úkony v časovém horizontu v desítkách minut při ideální optimalizaci. Reálné záznamy v databázovém systému SW EFA však hovoří o hodinách až dnech. Zde uvedené číselné hodnoty zaznamenané v HARDWARIO Cloud, historii proběhlých toků v Power Automate a excelové databázi zaslaných zpráv, tak jako z databáze SW EFA získané přehledy, nejsou statisticky významné, pro přehledné porovnání časových nároků obou systémů na zaměstnance však postačují.

13 Závěr

Cílem bakalářské práce bylo navržení komunikačního zařízení pro usnadnění a urychlení komunikace mezi zdravotnickými profesemi a biomedicínskými techniky i inženýry. V roce 2013 byla Milanem Hřebíkem napsána diplomová práce zabývající se samotným návrhem oddělení biomedicínského inženýrství ve zdravotnickém zařízení Ústav pro péči o matku a dítě [90]. O dva roky později byla Jiřím Randou uveřejněna diplomová práce věnující se zavedení databázového systému pro správu zdravotnické techniky, a to SW EFA do menší nemocnice s cílem zvýšení efektivity procesů spjatých se správou zdravotnické techniky [91]. Nyní, o šest let později, tato bakalářská práce reflektuje významný technický pokrok směrem k digitalizaci a automatizaci včetně nově vznikajících komunikačních sítí a nových technologických postupů.

V rámci bakalářské práce bylo navrženo kompletní řešení obsahující jak hardwarové zařízení, tak softwarovou a aplikační implementaci. Práce je rozdělena do dvou částí. Teoretická část začíná seznámením čtenáře s aktuální situací na poli komunikačních prostředků a metod komunikace ve zdravotnických zařízeních a to včetně velice podstatných systémů žádanek v databázových softwarech a systémů nazývaných SESTRA–PACIENT, sloužících k přivolání sestry k pacientovi pomocí k tomu navržených modulů. Následovalo uvedení do problematiky vývojových desek a do konceptu IoT. Na kapitolu o IoT navazuje seznámení s bezdrátovými technologiemi nacházejícími uplatnění v automatizaci, digitalizaci i v běžném životě. Speciální pozornost byla věnována sítím dlouhého dosahu s nízkými nároky na energii, tzv. LPWAN. V rámci toho bylo zmíněno i velmi používané bezlicenční ISM pásmo. Samostatná kapitola byla věnována tématu bezpečnosti internetu věcí a bezdrátových zařízení obecně. S bezpečností úzce souvisí komunikační protokoly, s jejichž základním popisem se zabývá kapitola následující.

Praktická část bakalářské práce popisuje vybrané hardwarové součásti navrhovaného prototypu včetně podmínek na hardware kladených z pohledu kvality a bezpečnosti. Zde je popsána základní deska plošných spojů s označením CHESTER-M, osazená komunikačním modulem pro NB-IoT, a s ní použitá druhá deska plošných spojů s označením CHESTER-Z, osazená tlačítky a Li-Ion článkem. Vybranou bezdrátovou komunikační sítí bylo NB-IoT pro své široké pokrytí a vysokou kvalitu signálu v zastavěných oblastech. Nad rámec zadání práce bylo vhodné integrovat RFID čtečku čipů zaměstnaneckých karet jako ochranu před neautorizovanými zprávami. Toto vylepšení bylo vytvořeno na softwarové bázi, tj. hardware, ač je ve vývoji, nebylo možné sestavit a pro jeho náhradu byl použit softwarový nástroj cURL. Pro návrh aplikační části prototypu byl vybrán HARDWARIO Cloud, do něhož přicházejí zprávy z hardwarové části zařízení, tj. z desky CHESTER-M. V HARDWARIO

Cloud byl vytvořen callback, který se propojil se SW konektorem v Power Automate pomocí protokolu HTTPS metodou GET. Tím byla vytvořena URL cesta pro zasílanou zprávu až do M365. V Power Automate byly vytvořeny dva toky. První tok byl sestaven pro navržený a reálně postavený prototyp zařízení. Druhý vytvořený tok byl poskládán ze stejných SW konektorů, jako tok první, reflektoval však možnost autorizace pomocí jedinečného čísla RFID čipu a data byla v tomto případě zasílána simulovaným zařízením pomocí nástroje cURL. Oba navržené prototypy, jeden z hardwarových komponent a druhý řešený softwarově (RFID), zasílají po stisku tlačítka zprávy do M365, do aplikace Power Automate a zobrazují se v nastaveném formátu v aplikaci Microsoft Teams do chatu založené skupiny OZT (oddělení zdravotechniky). Zároveň navržený prototyp zasílá informaci o napětí na baterii a v případě nízkého stavu Li-Ion článku je zaslána zpráva do Microsoft Teams, do skupiny OZT, s aktuální hodnotou napětí a žádostí o údržbu formou výměny baterie či jejího dobití pomocí adaptéru. Pro účely této práce byla použita licence M365 s administrátorským účtem a dvěma účty, které zastupují fiktivní zaměstnance fiktivní Nemocnice Horní Dolní Lhota.

Sestavený prototyp komunikačního zařízení byl testován po dobu dvou týdnů ve zdravotnickém zařízení Ústav pro péči o matku a dítě v Praze Podolí a to na radiologickém oddělení. Oba testované prototypy, z nichž jeden byl zapůjčen společností HARDWARIO pouze pro účely testování po stanovenou dobu, byly umístěny na dva rentgenové přístroje a to na AGFA DR 100e s výrobním číslem 30063 a AGFA DR 400 s výrobním číslem 2212. Oba prototypy po celou dobu testování nevykazovaly žádné softwarové ani hardwarové chyby. Zasílání zpráv probíhalo spolehlivě. Po stisku tlačítka se vždy zobrazila zpráva zaměstnancům oddělení zdravotechniky do chatu OZT v licenci M365 v aplikaci Microsoft Teams. Licence M365 byla na testování zapůjčena. Při porovnání záznamů v žádankovém systému v SW EFA a záznamů v excelové tabulce o zaslaných zprávách pomocí navrženého prototypu zařízení, lze usoudit, že navržený prototyp je schopen zjednodušit a výrazně urychlit žádost zdravotníka o řešení poruchy či jiného neobvyklého stavu. Z obvyklého systému, trvajícího asi třicet minut, se sníží časové nároky na dvě až tři minuty v případě zaslání zprávy pomocí navrženého prototypu. Na straně BMT je úspora času a rychlejší reakce na zaslanou žádost dána především zobrazením v Microsoft Teams na mobilním zařízení, které technik nosí stále při sobě a není tedy odkázán na přítomnost stolního počítače.

Pro získání statisticky významných výsledků by bylo nutné testování většího množství navržených prototypů, alespoň v počtu deseti až dvaceti kusů a to po dobu několika měsíců pro nashromáždění dostatku relevantních zpráv zaslaných zdravotníky prostřednictvím navrženého prototypu. Zároveň by bylo pro nasazení do reálného provozu vhodné hardwarově integrovat RFID čtečku, která by umožnila lepší kontrolu, relevantnější filtrování zasílaných zpráv a tedy zobrazení pouze ověřených požadavků v Microsoft Teams. Konečné použití typu RFID čtečky bude závislé na použité identifikační kartě zaměstnance, lze do budoucna zvažovat i ověření pomocí biometrie. Taktéž by bylo možno přidat potvrzení pro zdravotníka o doručení odeslaného požadavku technikovi, ať formou emailu či s využitím aplikace Microsoft Teams.

Použitá literatura

[1] DOLNÍČEK, Lukáš. Rozhovor: Petr Šuráň, CompuGroup Medical. *IT Systems* [online]. 2013, roč. 14, č. 12, s. 18–20 [cit. 2021-04-11]. ISSN 1802-002X. Dostupné z: https://www.systemonline.cz/it-pro-verejny-sektor-a-zdravotnictvi/rozhovor-petr-suran-compugroup-medical.htm.

[2] KÝČEK, Michal. *Nemocniční informační systémy: Kvalita v informačních systémech ve zdravotnictví*. České Budějovice, 2008. Dostupné také z: https://theses.cz/id/b8fsc3/downloadPraceContent_adipIdno_11178. Diplomová práce. Jihočeská univerzita v Českých Budějovicích.

[3] BEHROVÁ, Jana. *Porovnání komerčních NIS (nemocničních informačních systémů) používaných v jednotlivých zdravotnických zařízeních v ČR* [online]. Kladno, 2016 [cit. 2021-04-11]. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/67620/FBMI-DP-2016-Behrova-Jana-prace.pdf?sequence=1%5C&isAllowed=y. Diplomová práce. České vysoké učení technické v Praze.

[4] STEINER, David. *Informační systémy ve zdravotnictví* [online]. Praha, 2009 [cit. 2021-04-11]. Dostupné z: http://bio.felk.cvut.cz/~huptycm/Vyuka/IKTZ_prednasky/IKTZ_20091125.pdf. prezentace. ČVUT.

[5] *ICZ a.s. Integrace a komunikace ve zdravotnictví* [online]. Praha: ICZ a.s. [cit. 2021-04-11]. Dostupné z: https://www.iczgroup.com/produkty-a-sluzby/zdravotnictvi/integrace-komunikace-ve-zdravotnictvi/.

[6] *NAM system: Řešení pro nemocnice* [online]. Havířov: NAM system [cit. 2021-04-11]. Dostupné z: https://www.nam.cz/category/zakaznici/nemocnice/.

[7] *EFA SERVICES: Informační systém EFA pro evidenci a správu budov, technologických zařízení, zdravotnické techniky* [online]. Praha: Univerzita Karlova, 2021 [cit. 2021-04-11]. Dostupné z: https://cuni.cz/UK-4113-version1-EFAmanual.pdf.

[8] *TESCO SW* [online]. Olomouc: TESSELA HOLDING SE, 2021 [cit. 2021-04-11]. Dostupné z: https://famaplus.cz/tpis/.

[9] DOLEŽAL, Ludvík. *Evidence a správa zdravotnických prostředků: Zaměření na team OZT a sestry* [online]. Žďár nad Sázavou, [n.d.] [cit. 2021-04-11]. Dostupné z: https://slideplayer.cz/slide/2996280/. prezentace. EFA SERVICES.

[10] *Codaco Electronic s.r.o.* [Online]. Valašské Meziříčí: Codaco Electronic s.r.o. [cit. 2021-04-11]. Dostupné z: http://www.codaco.cz/.

[11] *Komunikační systém Sestra-Pacient* [online]. Ostrovačice: 2D system s.r.o., 2021 [cit. 2021-04-11]. Dostupné z: https://www.alcad.cz/sekce/komunikacni-system-sestra-pacient.

[12] *ZPT Vigantice* [online]. Vigantice: ZPT Vigantice spol. s r.o. [cit. 2021-04-11]. Dostupné z: http://www.zptvigantice.org/index.php?action=product%5C&mainProduct=medicall%5C&subProduct=mdcv04%5C&chapter=prvky.

[13] *Schrack Seconet: HealthCare* [online]. Praha: Schrack Seconet, 2012 [cit. 2021-04-11]. Dostupné z: https://www.schrack-seconet.com/cs/products_solutions/health_care/index.html.

[14] *ICS - systémy s.r.o.* [Online]. Karlovy Vary: ICS - systémy s.r.o., 2021 [cit. 2021-04-11]. Dostupné z: http://www.ics-kv.cz/?nemocnice-a-zdravotnictvi,46.

[15] *Trex: Bezdrátový signalizační systém* [online]. Praha: Multitone.cz [cit. 2021-04-11]. Dostupné z: https://www.multitone.cz/wp-content/uploads/2020/02/N%5C%C3%5C%A1vod-TREX-2G-v4.2.pdf.

[16] WILSON, Connor. *HIPAA-Compliant IoT Solutions* [online]. Houston: SSL, 2021 [cit. 2021-04-14]. Dostupné z: https://www.ssl.com/blogs/hipaa-compliant-iot-solutions/.

[17] CIRANI, Simone, Gianluigi FERRARI, Marco PICONE a Luca VELTRI. *Internet of things: architectures, protocols and standards*. First edition. Hoboken, NJ: Wiley, 2019. ISBN 9781119359678.

[18] *The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters* [online]. London: VICE MEDIA GROUP, 2021 [cit. 2021-04-14]. Dostupné z: https://www.vice.com/en/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

[19] *Criminals Hacked A Fish Tank To Steal Data From A Casino* [online]. Jersey: Forbes Media, 2021 [cit. 2021-04-14]. Dostupné z: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/?sh=35e81e3f32b9.

[20] SCHIFFER, Alex. *How a fish tank helped hack a casino* [online]. Washington: Nash Holdings, 1996 [cit. 2021-04-14]. Dostupné z: https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/.

[21] WEI, Wang. *Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer* [online]. Chandigarh: The Hacker News, 2019 [cit. 2021-04-14]. Dostupné z: https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

[22] NEWCOMB, Alyssa. *FBI Warns Parents of Privacy Risks With Internet-Connected Toys* [online]. New York: NBC UNIVERSAL, 2021 [cit. 2021-04-14]. Dostupné z: https://www.nbcnews.com/tech/security/fbi-warns-parents-privacy-risks-internet-connected-toys-n784126.

[23] *SECTRON s.r.o.* [Online]. Ostrava: SECTRON s.r.o. [cit. 2021-04-14]. Dostupné z: https://eshop.sectron.cz/cs/.

[24] TOMAR, Ankur. Není deska jako deska, aneb výběr správné vývojové desky: Vývoj-články. *DPS: Elektronika od A do Z* [online]. 2017, roč. 2017, č. 4, s. 12–14 [cit. 2021-04-13]. ISSN 1805-5044. Dostupné z: https://www.dps-az.cz/vyvoj/id:51854/neni-deska-jako-deska-aneb-vyber-spravne-vyvojove-desky.

[25] MALÝ, Martin. *Hradla, volty, jednočipy: úvod do bastlení.* 1. vydání. Praha: CZ.NIC, z.s.p.o., 2017. ISBN 978-80-88168-23-2.

[26] *Software* [online]. Turin: Arduino.cc, 2021 [cit. 2021-04-13]. Dostupné z: https://www.arduino.cc/en/software.

[27] *Raspberry Pi 4 Model B - 8GB RAM* [online]. České Budějovice: Michal Prenner, 2021 [cit. 2021-04-13]. Dostupné z: https://rpishop.cz/raspberry-pi/2611-raspberry-pi-4-model-b-8gb-ram-0765756931199.html.

[28] VALÁŠEK, Michal Altair. *Raspberry Pi mění svět: Seznamte se s nejzajímavějším počítačem dneška* [online]. Praha: Economia, 1996 [cit. 2021-04-13]. Dostupné z: https://tech.ihned.cz/geekosfera/c1-65195330-raspberry-pi-meni-svet-seznamte-se-s-nejzajimavejsim-pocitacem-dneska.

[29] *STM32 Nucleo Boards* [online]. Ženeva: ST, 2021 [cit. 2021-04-13]. Dostupné z: https://www.st.com/en/evaluation-tools/stm32-nucleo-boards.html.

[30] *Průmyslová IoT stavebnice* [online]. Liberec: HARDWARIO, 2021 [cit. 2021-04-13]. Dostupné z: https://www.hardwario.com/cs/kit/.

[31] *Core Module* [online]. Liberec: HARDWARIO, 2021 [cit. 2021-04-13]. Dostupné z: https://obchod.hardwario.cz/core-module/.

[32] *Víceúčelový IoT Hub CHESTER* [online]. Liberec: HARDWARIO, 2021 [cit. 2021-04-13]. Dostupné z: https://www.hardwario.com/cs/chester/.

[33] *IoT Hub CHESTER* [online]. Liberec: HARDWARIO, 2021 [cit. 2021-04-13]. Dostupné z: https://obchod.hardwario.cz/hub/.

[34] *Řídicí systémy SIMATIC – chytré řešení pro vaše automatizační úlohy* [online]. Praha: Siemens, 2021 [cit. 2021-04-13]. Dostupné z: https://new.siemens.com/cz/cs/products/automation/systems/industrial/plc.html.

[35] *Výrobky* [online]. Praha: Mitsubishi Electric, 2021 [cit. 2021-04-13]. Dostupné z: https://cz3a.mitsubishielectric.com/fa/cs/products.

[36] *Controller* [online]. Minden: WAGO, 2021 [cit. 2021-04-13]. Dostupné z: https://www.wago.com/mx-en/c/plcs-controllers.

[37] *Teco a.s.* [Online]. Kolín: Teco a.s., 2017 [cit. 2021-04-13]. Dostupné z: https://www.tecomat.cz/.

[38] *Programovatelné automaty (PLC)* [online]. Otobrunn: Panasonic, 2020 [cit. 2021-04-13]. Dostupné z: https://www.panasonic-electric-works.com/cz/programovatelne-automaty-plc.htm.

[39] FRANCIS, Sam. *Top 20 programmable logic controller manufacturers* [online]. WordPress, 2021 [cit. 2021-04-13]. Dostupné z: https://roboticsandautomationnews.com/2020/07/15/top-20-programmable-logic-controller-manufacturers/33153/.

[40] *Controllino: Arduino* [online]. Praha: Conrad Electronic, 2020 [cit. 2021-04-13]. Dostupné z: https://www.conrad.cz/o/controllino-arduino-0213023.

[41] *KUNBUS: Raspberry* [online]. Praha: Conrad Electronic, 2020 [cit. 2021-04-13]. Dostupné z: https://www.conrad.cz/o/kunbus-raspberry-0213022.

[42] *PLC - základní fakta a zajímavosti* [online]. Elektro 4.0, 2021 [cit. 2021-04-13]. Dostupné z: http://www.elektro40.cz/clanek/plc-zakladni-fakta-a-zajimavosti--101.

[43] BARNETT, Thomas, Shruti JAIN, Usha ANDRA a Taru KHURANA. *Cisco Visual Networking Index (VNI) Complete Forecast Update: 2017-2022 APJC Cisco Knowledge Network (CKN) Presentation* [online]. San Jose, 2018 [cit. 2021-04-14]. Dostupné z: https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/1213-business-services-ckn.pdf. prezentace. Cisco.

[44] *Bezpečnost bezdrátových technologií: Zpravodaj ÚVT MU* [online]. Brno: Ústav výpočetní techniky Masarykovy univerzity, 2009 [cit. 2021-05-02]. Č. 1. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/624.html.

[45] *Zigbee Alliance* [online]. Davis CA: Zigbee Alliance, 2020 [cit. 2021-04-15]. Dostupné z: https://zigbeealliance.org/.

[46] ŽALUD, Václav. Rádiová komunikace v internetu věcí pro průmyslovou automatizaci. *Automa* [online]. 2017, roč. 2017, č. 1, s. 54–55 [cit. 2021-04-15]. ISSN 1210-9592. Dostupné z: https://automa.cz/Aton/FileRepository/pdf_articles/9493.pdf.

[47] VOJÁČEK, Antonín. *Základní úvod do oblasti internetu věcí (IoT)* [online]. Praha: HW server, 1997 [cit. 2021-05-08]. Dostupné z: https://automatizace.hw.cz/zakladni-uvod-do-oblasti-internetu-veci-iot.html.

[48] *FAQ: Často kladené otázky* [online]. Oberhaching: Smart-TEC, 2021 [cit. 2021-04-15]. Dostupné z: https://www.smart-tec.com/cs/navigationen/footer-gnav/faq.

[49] *RFID versus NFC. Co bylo první a … co je lepší?* [Online]. Praha: KODYS [cit. 2021-04-15]. Dostupné z: https://www.kodys.cz/o-nas/blog/rfid-vs-nfc.

[50] *Specifikace rádiové části systému Bluetooth* [online]. Brno: Vysoké učení Technické v Brně, 2004 [cit. 2021-04-28]. Dostupné z: http://www.elektrorevue.cz/clanky/04003/index.html.

[51] PALIVEC, Pavel. *Bluetooth Low Energy* [online]. Liberec: CADware s.r.o., 2021 [cit. 2021-04-28]. Dostupné z: https://www.dps-az.cz/soucastky/id:9912/bluetooth-low-energy.

[52] KLAUZ, Milan. *Bezdrátové technologie pro internet věcí* [online]. Liberec: CADware s.r.o., 2021 [cit. 2021-05-02]. Dostupné z: https://www.dps-az.cz/zajimavosti/id:56560/bezdratove-technologie-pro-internet-veci.

[53] *Rychlost našeho internetu: Mobilní datové služby* [online]. Praha: T-Mobile Czech Republic, 2021 [cit. 2021-05-02]. Dostupné z: https://www.t-mobile.cz/podpora/rychlost-internetu.

[54] *Jak se připojit na internet a jaká je rychlost připojení?* [Online]. Praha: Vodafone Czech Republic, 2021 [cit. 2021-05-02]. Dostupné z: https://www.vodafone.cz/pece/internet-data/internet-v-pocitaci/moznosti-pripojeni-k-internetu-jeho-rychlost/.

[55] DOSEDĚL, Tomáš. *UMTS, HSPA+, LTE: vyznejte se v datových přenosech* [online]. Brno: DK Media Net, 2012 [cit. 2021-05-02]. Dostupné z: http://www.mobinfo.cz/umts-hspa-lte-vyznejte-se-v-datovych-prenosech/.

[56] ČTK. *Konec 3G v Česku. Operátoři letos tuto technologii vypnou* [online]. Praha: MAFRA, 1999 [cit. 2021-05-02]. Dostupné z: https://www.idnes.cz/mobil/mobilni-operatori/konec-3g-v-cesku-operatori-ji-zmeni-na-4g-a-5g.A210208_105349_mobilni-operatori_jm.

[57] BLEICHER, Ariel. *LTE-Advanced Is the Real 4G* [online]. New York: IEEE Spectrum, 2021 [cit. 2021-05-02]. Dostupné z: https://spectrum.ieee.org/telecom/standards/lte-advanced-is-the-real-4g.

[58] *5G sítě: FAQ - často kladené dotazy* [online]. Praha: ČTÚ, 2018 [cit. 2021-05-02]. Dostupné z: https://www.ctu.cz/5g.

[59] *UWB Alliance* [online]. UWB Alliance, 2019 [cit. 2021-05-02]. Dostupné z: https://uwballiance.org/.

[60] *FiRa Consortium* [online]. Beaverton: FiRa Consortium, 2020 [cit. 2021-05-02]. Dostupné z: https://www.firaconsortium.org/.

[61] BAKR, Mustafa. *Introduction to Ultra-Wideband (UWB) Technology* [online]. Boise: EETech Media [cit. 2021-05-02]. Dostupné z: https://www.allaboutcircuits.com/technical-articles/introduction-to-ultra-wideband-uwb-technology/.

[62] *Všeobecné oprávnění č. VQ-R/10/06.2009-9 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu* [online]. Praha: Český telekomunikační úřad, 2009 [cit. 2021-05-03]. Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2009/vo-r_10-06_2009-09.pdf.

[63] *DNA of IoT* [online]. Camarillo: Semtech, 2021 [cit. 2021-05-03]. Dostupné z: https://www.semtech.com/lora.

[64] *Architektura a popis jednotlivých funkčních bloků* [online]. Praha: PIXMAN, 2009 [cit. 2021-05-03]. Dostupné z: https://pripoj.me/technicke-aspekty-technologie-lora/.

[65] *Sigfox* [online]. Praha: Sigfox Česká republika, 2016 [cit. 2021-05-03]. Dostupné z: https://sigfox.cz/cs.

[66] *Internet of Things: Narrowband – Internet of Things (NB-IoT)* [online]. London: GSM Association, 2021 [cit. 2021-05-08]. Dostupné z: https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/.

[67] *NARROWBAND IOT DELIVERS: INSIGHTS FROM THE LARGEST NB-IOT INDOOR MEASUREMENT CAMPAIGN* [online]. Bonn: Deutsche Telekom, 2019 [cit. 2021-05-03]. Dostupné z: https://iot.telekom.com/resource/blob/data/165170/aedf685e59ad421069657ff7d3408fde/narrowband-iot-delivers.pdf.

[68] *Stvořili jsme síť pro budoucnost: NB-IoT propojuje stroje, věci i lidi* [online]. Praha: Vodafone Czech Republic, 2021 [cit. 2021-05-03]. Dostupné z: https://www.vodafone.cz/firmy-a-korporace/internet-veci/nb-iot1/.

[69] *Vysvětlení parametrů signálu RSRP RSRQ SINR a RSSI* [online]. Brno: Velmo, 2017 [cit. 2021-05-08]. Dostupné z: https://www.velmo.cz/vysvetleni-parametru-signalu-rsrp-rsrq-sinr-a-rssi/.

[70] *Maximum Coupling Loss (MCL) and Maximum Path Loss (MPL)* [online]. Gurgaon: Techplayon, 2019 [cit. 2021-05-08]. Dostupné z: http://www.techplayon.com/maximum-coupling-loss-mcl-and-maximum-path-loss-mpl/.

[71] *Šifrování a autentizace: Co je to SSL, TLS a HTTPS* [online]. Praha: Veracomp, 2021 [cit. 2021-05-08]. Dostupné z: https://www.ictblog.cz/sifrovani-a-autentizace-co-je-to-ssl-tls-a-https/.

[72] MALÝ, Martin. *Web Sockets* [online]. Praha: Devel.cz Lab, 2021 [cit. 2021-05-09]. Dostupné z: https://zdrojak.cz/clanky/web-sockets/.

[73] *TCP/IP Ports and Protocols* [online]. Hoboken: Pearson Education, 2021 [cit. 2021-05-09]. Dostupné z: https://www.pearsonitcertification.com/articles/article.aspx?p=1868080.

[74] *HTTP* [online]. Bratkovice: Štráfelda [cit. 2021-05-09]. Dostupné z: https://www.strafelda.cz/http.

[75] *Co je MQTT a k čemu slouží ve IIoT?: Popis protokolu MQTT* [online]. Praha: IPC2U, 2021 [cit. 2021-05-09]. Dostupné z: https://ipc2u.tech/blogs/news/mqtt-protokol?gclid=EAIaIQobChMIp_zOpsX97gIVYRDmCh1bHw2_EAAYASAAEgKscfD_BwE.

[76] *MQTT: The Standard for IoT Messaging* [online]. Burlington: MQTT, 2020 [cit. 2021-05-09]. Dostupné z: https://mqtt.org/.

[77] *TLS/SSL - MQTT Security Fundamentals* [online]. Landshut: HiveMQ, 2021 [cit. 2021-05-09]. Dostupné z: https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl/.

[78] *AMQP Protocol* [online]. Ottawa Ontario: Netify, 2021 [cit. 2021-05-09]. Dostupné z: https://www.netify.ai/resources/protocols/amqp.

[79] *AMQP* [online]. Stockholm: VMware, 2011 [cit. 2021-05-09]. Dostupné z: https://www.cloudamqp.com/docs/amqp.html.

[80] *AMQP: Advanced Message Queuing Protocol* [online]. Woburn: OASIS, 2021 [cit. 2021-05-09]. Dostupné z: https://www.amqp.org/.

[81] *OASIS Advanced Message Queuing Protocol (AMQP) TC* [online]. Woburn: OASIS, 2021 [cit. 2021-05-09]. Dostupné z: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp.

[82] *HARDWARIO CHESTER Documentation: CHESTER Datasheet* [online]. Portland: Read the Docs, 2021 [cit. 2021-05-09]. Dostupné z: https://chester.hardwario.com/en/latest/index.html%5C#chester-datasheet.

[83] *Narrowband IoT (NB-IoT)* [online]. Thalwil: U-blox, 1997 [cit. 2021-05-08]. Dostupné z: https://www.u-blox.com/en/narrowband-iot-nb-iot.

[84] VOJÁČEK, Antonín. *Více i méně běžné RFID frekvence a jejich vliv na komunikaci* [online]. Praha: HW server, 1997 [cit. 2021-05-09]. Dostupné z: https://automatizace.hw.cz/vice-i-mene-bezne-rfid-frekvence-jejich-vliv-na-komunikaci.

[85] *What are the general differences between the following card types?: Proximity, MIFARE®, MIFARE DESFire®* [online]. Torrance: PCSC, 2021 [cit. 2021-05-09]. Dostupné z: https://www.pcscsecurity.com/wp-content/uploads/2018/05/Prox_and_Mifare_Explained.pdf.

[86] *HARDWARIO Cloud* [online]. Liberec: HARDWARIO [cit. 2021-05-09]. Dostupné z: https://hardwario.cloud/%5C#/login.

[87] *Microsoft Power Platform documentation* [online]. Redmond: Microsoft, 2021 [cit. 2021-05-09]. Dostupné z: https://docs.microsoft.com/en-us/power-platform/.

[88] *Microsoft Power Automate* [online]. Redmond: Microsoft, 2021 [cit. 2021-05-09]. Dostupné z: https://docs.microsoft.com/en-us/learn/powerplatform/power-automate.

[89] *Microsoft Teams admin documentation* [online]. Redmond: Microsoft, 2021 [cit. 2021-05-09]. Dostupné z: https://docs.microsoft.com/en-us/microsoftteams/.

[90] HŘEBÍK, Milan. *Návrh oddělení biomedicínského inženýrství ve zdravotnickém zařízení Ústav pro péči o matku a dítě – Praha Podolí* [online]. Kladno, 2013 [cit. 2021-05-16]. Dostupné z: https://theses.cz/id/0mojds/17_MSDP_322860_Milan_Hrebik_Diplomova_prace.pdf. Diplomová práce. České vysoké učení technické v Praze.

[91] RANDA, Jiří. *Systém pro správu zdravotnické techniky* [online]. Kladno, 2015 [cit. 2021-05-16]. Dostupné z: https://theses.cz/id/3d7af8/17PMSDP2_-_Randa/5.DP_kompletni_Randa_Jiri.pdf. Diplomová práce. České vysoké učení technické v Praze.

A Přílohy

Tato část obsahuje seznam příloh na přiloženém CD. Následují snímky nastavení všech podstatných částí navrženého prototypu. Zároveň je přiložen snímek zdrojového kódu ukázkového callbacku. Příloha A2 obsahuje podrobné ukázky správného nastavení použitých excelových tabulek i jednotlivých SW konektorů v Power Automate. Příloha A3 je členěna totožně jako A2 s tím, že se jedná o komplexnější nastavení softwarově řešeného prototypu s RFID čtečkou.

A.1 Obsah přiloženého CD

1. Bakalářská práce
2. Exportovaný .zip soubor z Power Automate obsahující kompletní zdrojový kód toku fyzicky sestaveného prototypu zařízení. Název souboru je Flow_sestaveny_prototyp_zarizeni
3. Exportovaný .zip soubor z Power Automate obsahující kompletní zdrojový kód toku softwarově navrženého prototypu zařízení s RFID čtečkou. Název souboru je Flow_SW_nastavena_logika_s_RFID
4. Textový soubor obsahující zdrojový kód pro vložení do příkazové řádky ke spuštění softwarového nástroje cURL. Název souboru je Kod_cURL_CMD
5. Tři Excel tabulky vytvořené pro fyzicky sestavený prototyp zařízení. Názvy tabulek:
   - podminka_stisk_BP
   - nizke_napeti_BP
   - zaznam_zprava_BP
6. Čtyři Excel tabulky vytvořené pro softwarově řešený návrh prototypu s RFID čtečkou. Názvy tabulek:
   - RFID_nastaveni_pristupovych_prav
   - napeti_pristroj_oddeleni_RFID
   - podminka_stisk_RFID
   - zaznam_zprava_RFID

A.2 Sestavený prototyp zařízení

A.2.1 Zdrojový kód ukázkového callbacku

Callback BP

Request:

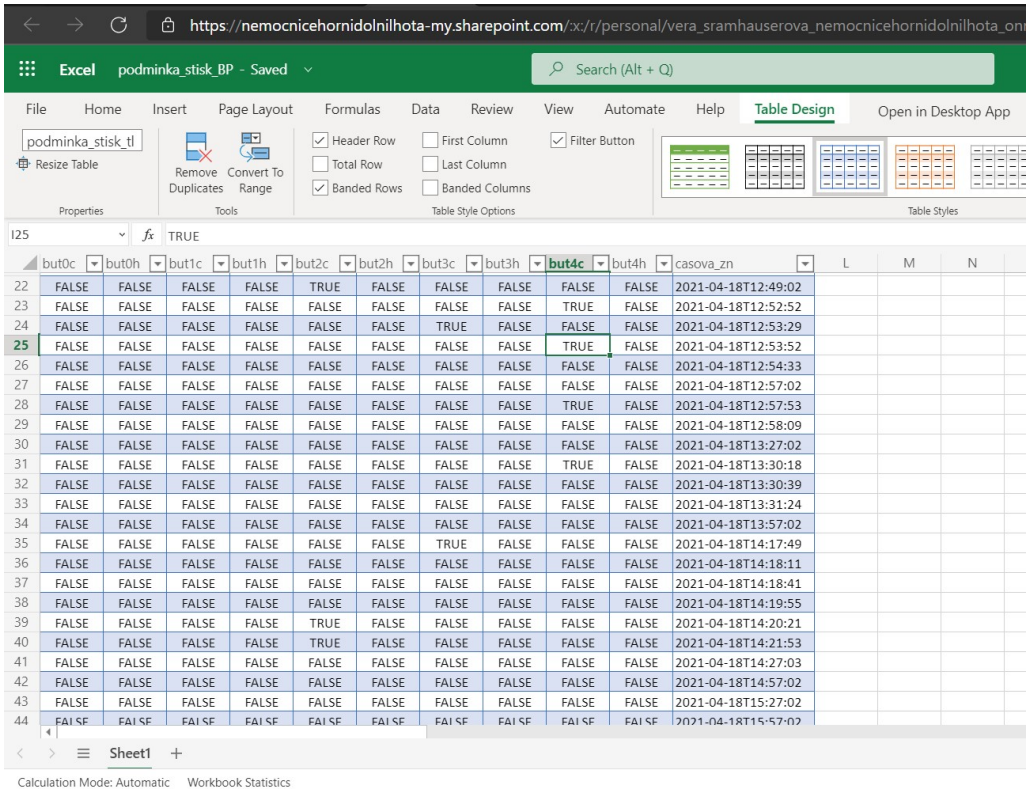

```
{
  "method": "POST",
  "headers": {
    "User-Agent": "HARDWARIO Cloud Callback"
  },
  "url": "https://prod-
  196.westeurope.logic.azure.com:443/workflows/c331ecdfd30249a49e1ad9b751c1be4f/triggers/manual/paths/invoke?api-
  version=2016-06-01&sp=%2Ftriggers%2Fmanual%2Frun&sv=1.0&sig=bb55ced4n3x4kDNVC1cLxnU0h2cgM-hPSgEf4epq2gM",
  "json": {
    "baterie": 3040,
    "id_device": "6075f2a47de395001864d3f0",
    "but0c": false,
    "but1c": false,
    "but2c": false,
    "but3c": false,
    "but4c": true,
    "but0h": false,
    "but1h": false,
    "but2h": false,
    "but3h": false,
    "but4h": false
  }
}
```


Response:

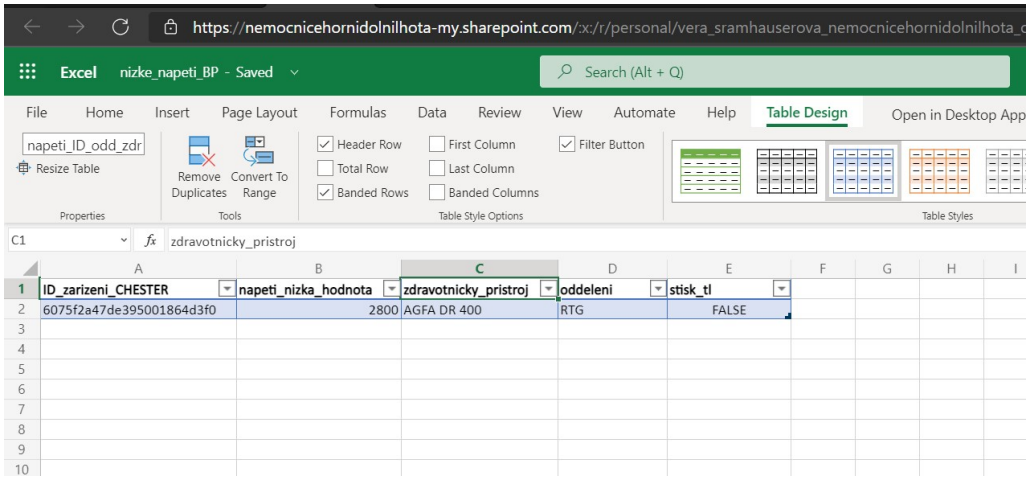

```
{
  "_id": "607c03dc9c28a500199526ae",
  "created_at": "2021-04-18T10:03:08.423Z",
  "code": 202,
  "headers": {
    "cache-control": "no-cache",
    "pragma": "no-cache",
    "expires": "-1",
    "x-ms-workflow-run-id": "085858286669680933555644065845CU08",
    "x-ms-correlation-id": "d0c6dfb9-6210-418a-af3c-09b59068af7b",
    "x-ms-client-tracking-id": "085858286669680933555644065845CU08",
    "x-ms-trigger-history-name": "085858286669680933555644065845CU08",
    "x-ms-execution-location": "westeurope",
    "x-ms-workflow-system-id": "/locations/westeurope/scaleunits/prod-196/workflows/c331ecdfd30249a49e1ad9b751c1be4f",
    "x-ms-workflow-id": "c331ecdfd30249a49e1ad9b751c1be4f",
    "x-ms-workflow-version": "08585828669102641055",
    "x-ms-workflow-name": "ce1fa51f-ca45-4fb6-8ecd-8d441a2461b0",
    "x-ms-tracking-id": "d0c6dfb9-6210-418a-af3c-09b59068af7b",
    "x-ms-ratelimit-burst-remaining-workflow-writes": "186",
    "x-ms-ratelimit-remaining-workflow-download-contentsize": "134217728",
    "x-ms-ratelimit-remaining-workflow-upload-contentsize": "134217534",
    "x-ms-ratelimit-time-remaining-directapirequests": "12499847",
    "x-ms-request-id": "westeurope:d0c6dfb9-6210-418a-af3c-09b59068af7b",
    "strict-transport-security": "max-age=31536000; includeSubDomains",
    "date": "Sun, 18 Apr 2021 10:03:08 GMT",
    "connection": "close",
    "content-length": "0"
  }
}
```


Obrázek A.1: Zobrazení vytvořeného callbacku.

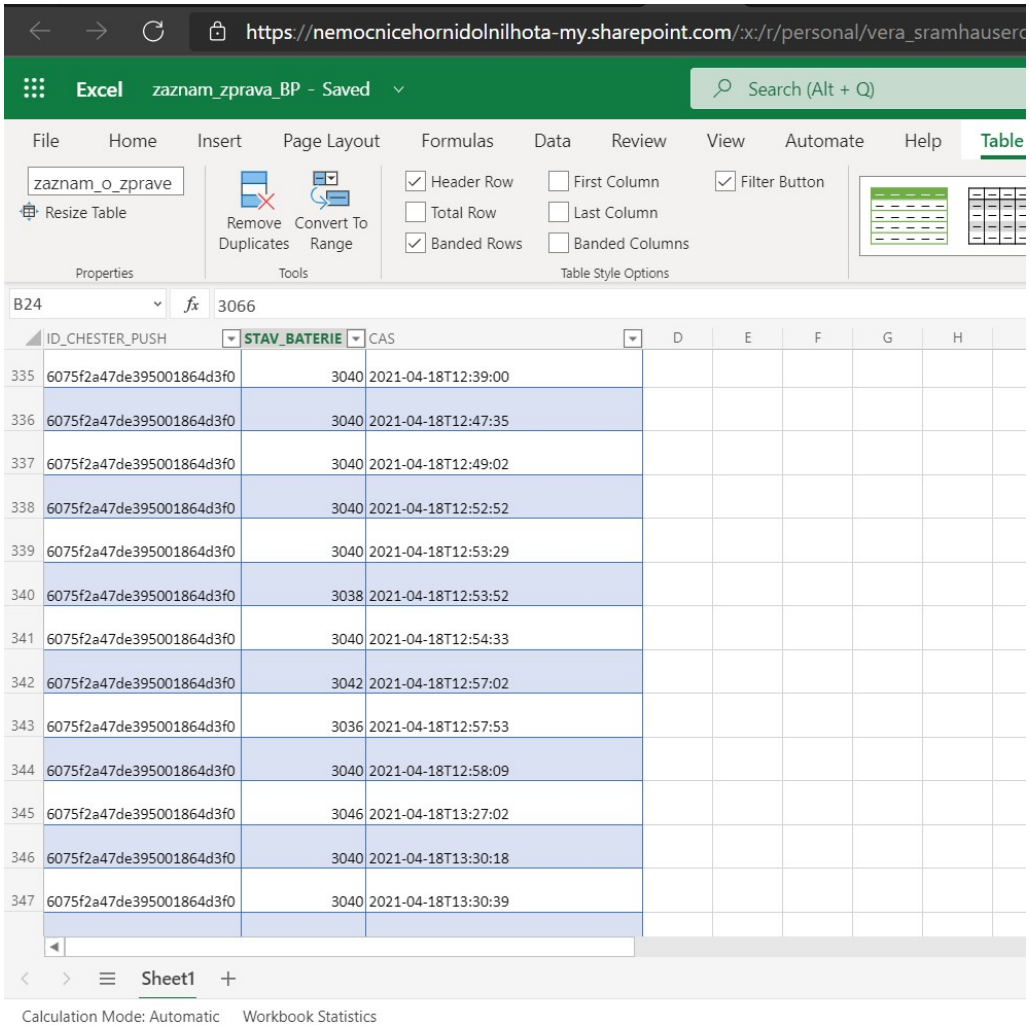
A.2.2 Excelové dokumenty



Obrázek A.2: Tabulka pro nastavení podmínky pro uložení a zobrazení zprávy v M365. V případě, že je zaslána hodnota TRUE po stisku tlačítka na prototypu, zaslaná zpráva se uloží a zobrazí se informace BMT či BMI v Microsoft Teams. Ukládá se i časová značka.



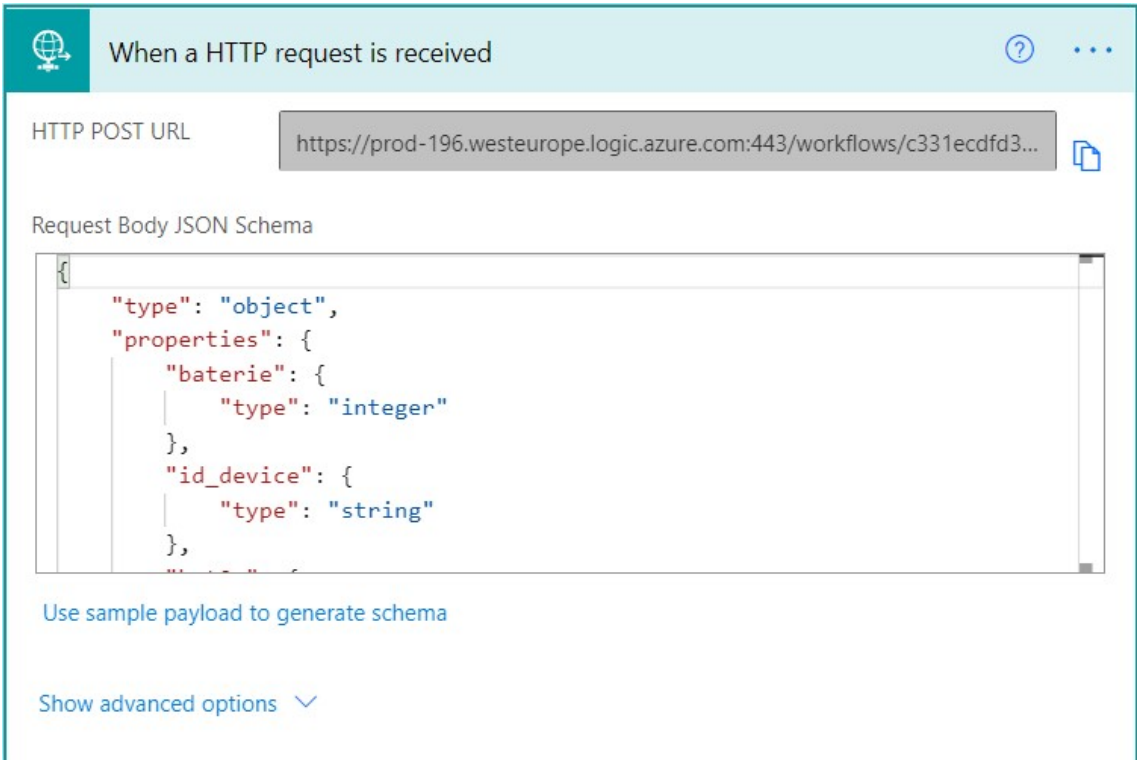
Obrázek A.3: Hodnoty ID prototypu, napětí na baterii, název zdravotnického přístroje, oddělení a časové značky, které jsou použity v dalších SW konektorech.



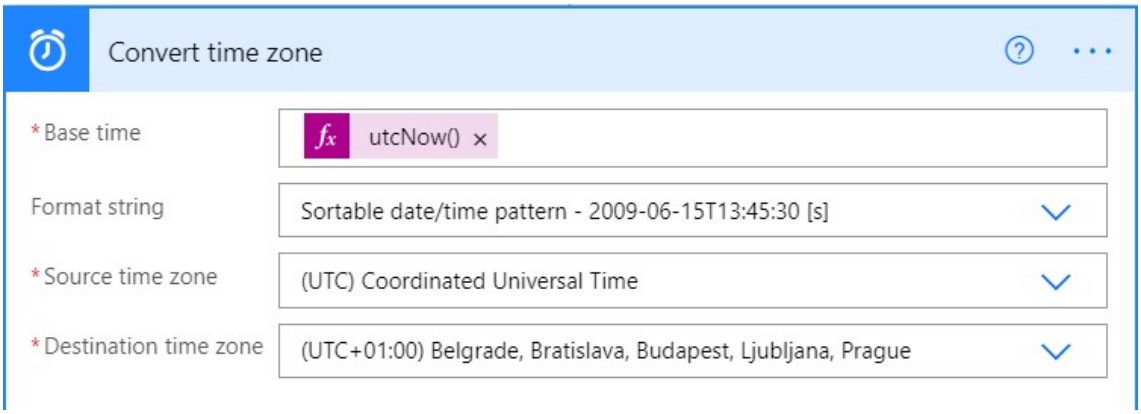
Obrázek A.4: Tabulka, do níž se ukládají zaslané zprávy, které splnily podmínku stisku tlačítka (TRUE). Do této databáze se ukládá *číslo ID zařízení navrženého prototypu*, *napětí na baterii v mV* a *časová značka* pro účely kontroly a přehlednosti.

A.2.3 Tok v Power Automate

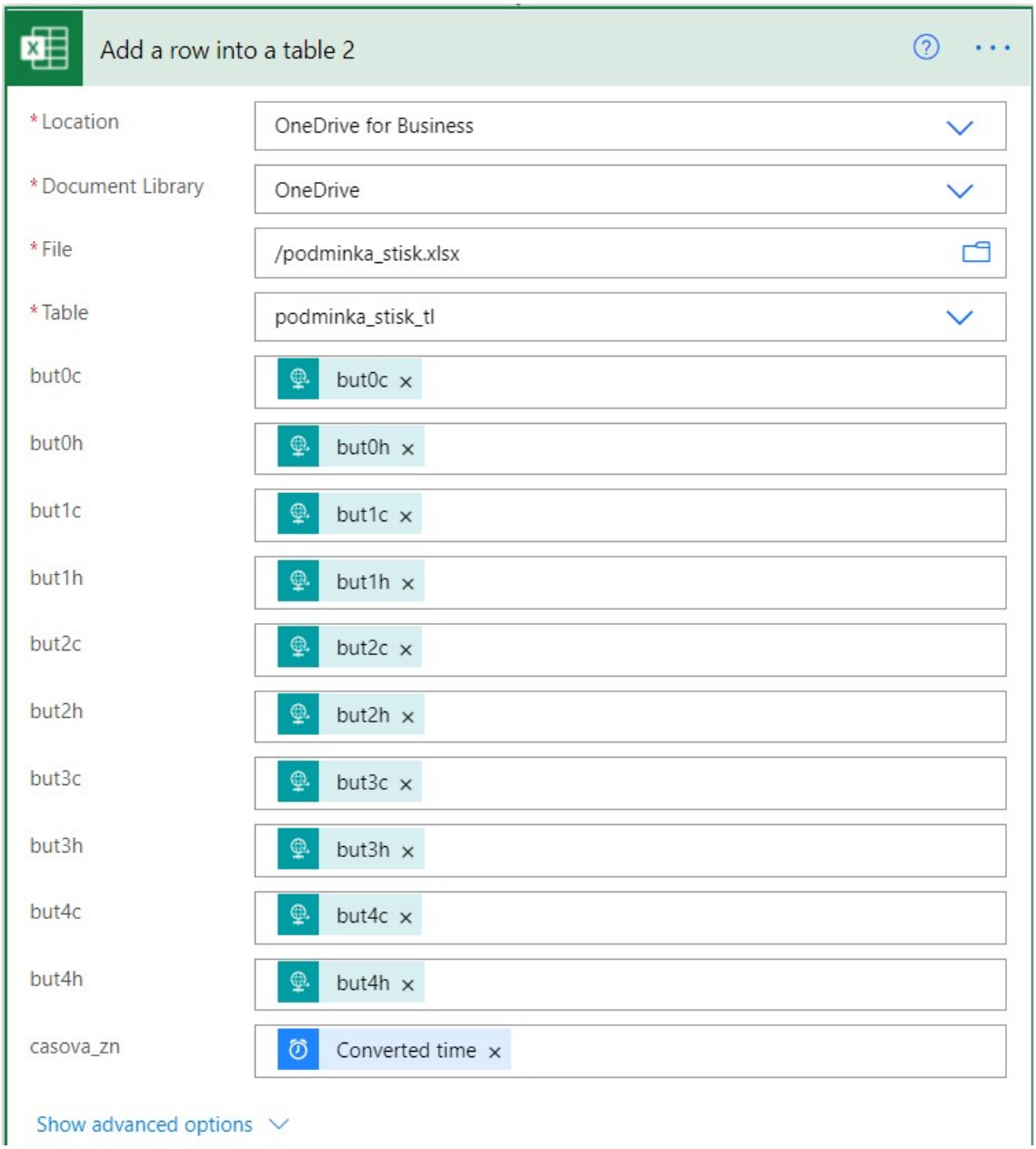
Dle schématu obrázek 11.6 tok označený písmenem A.



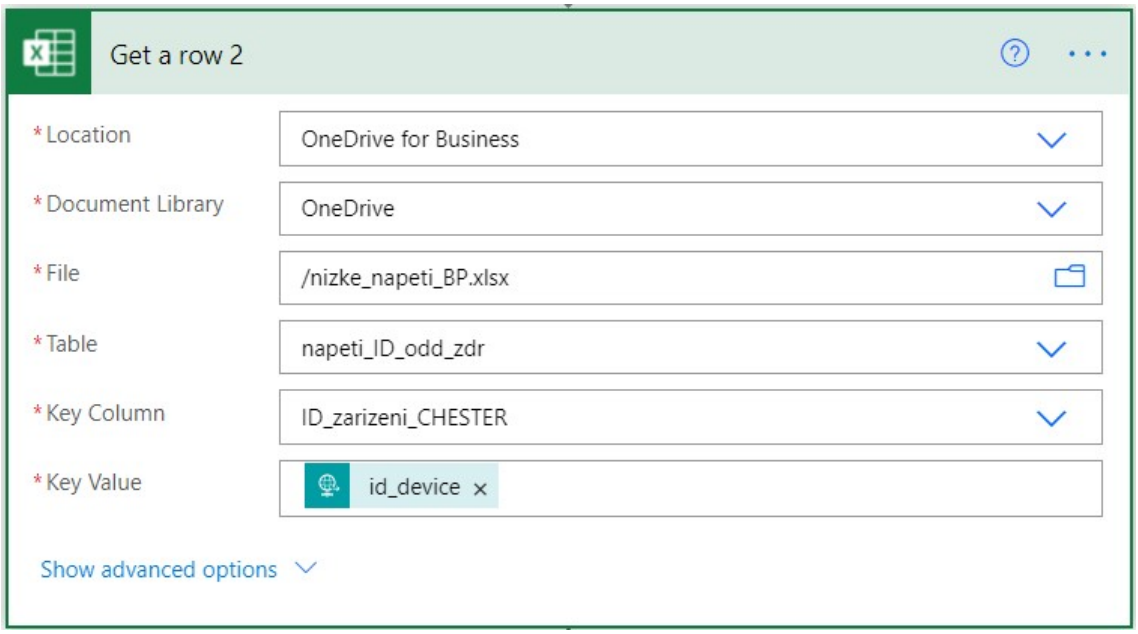
Obrázek A.5: Formát JSON zprávy a URL adresa, která se vkládá do nastaveného callbacku v HARDWARIO Cloud.



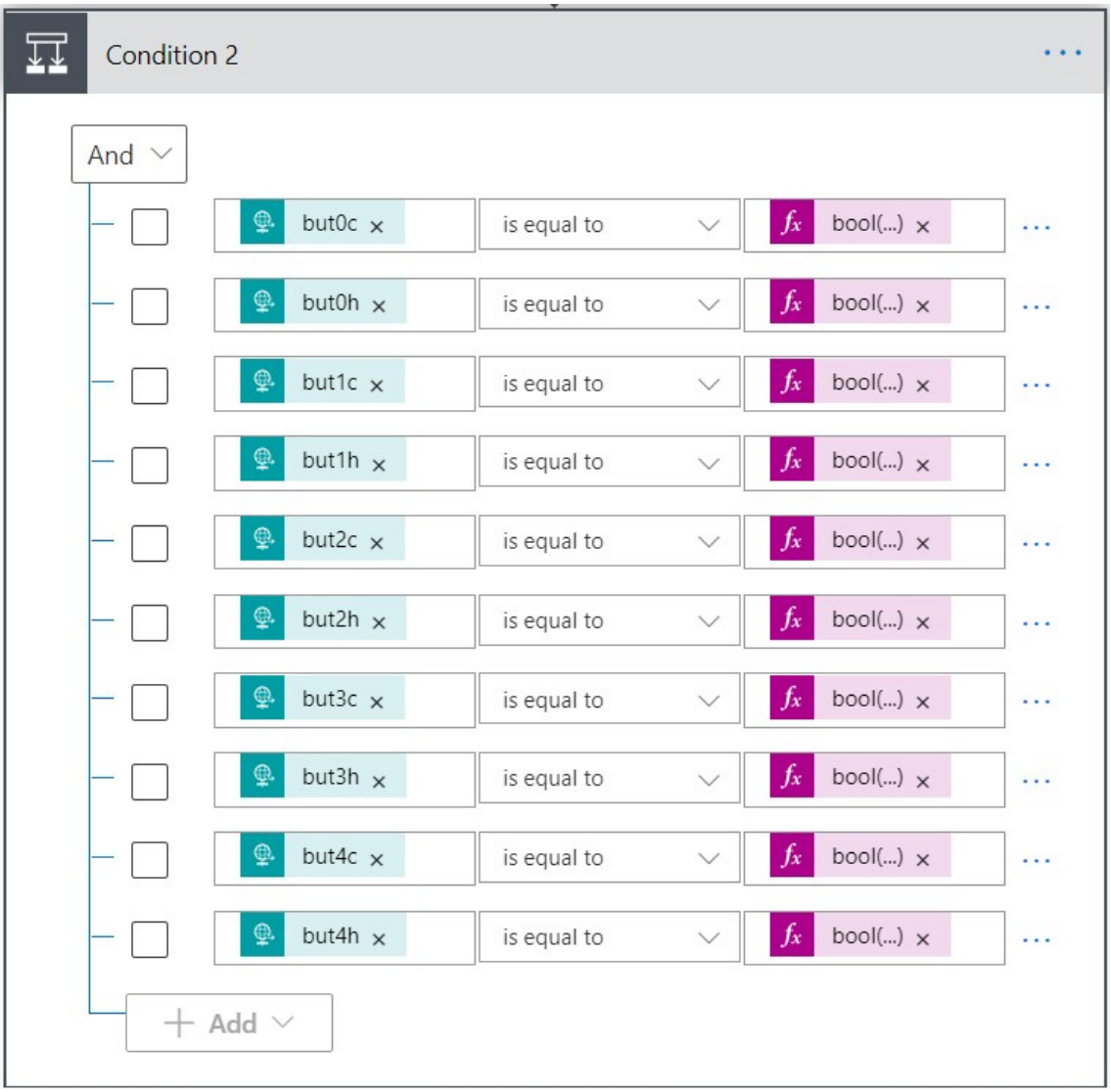
Obrázek A.6: Změna časového pásma z UTC na Českou republiku.



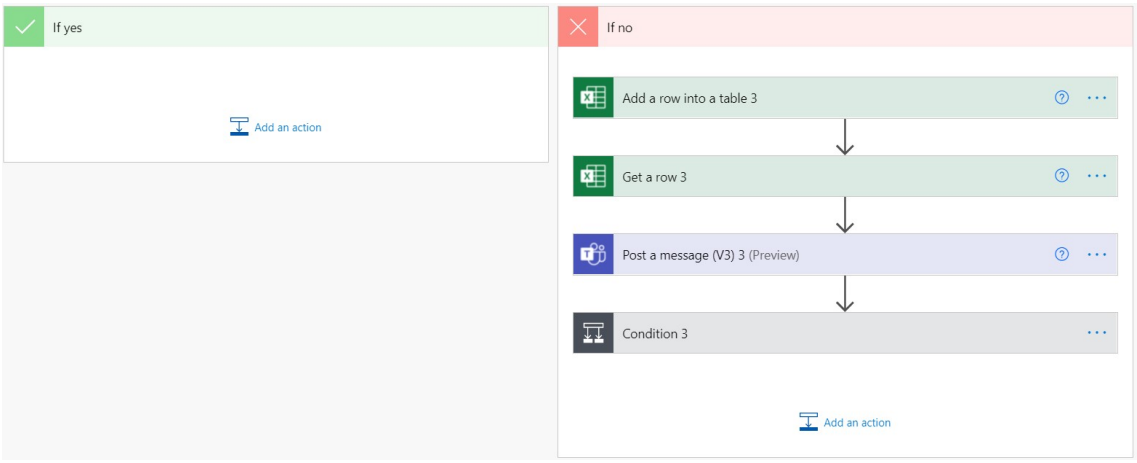
Obrázek A.7: Vkládání zaslaných dat o stisku tlačítka na prototypu zařízení do excelové tabulky na obrázku A.2 pomocí připravených proměnných. But je zkratkou pro button (tlačítko).



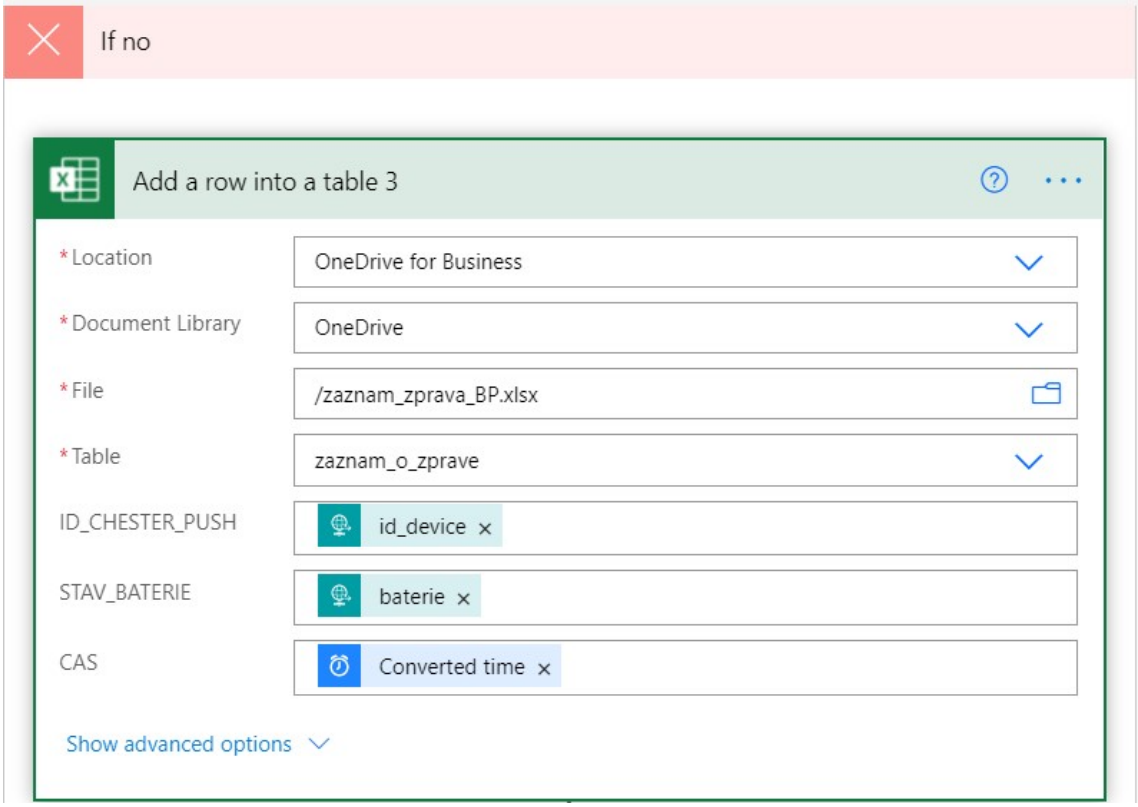
Obrázek A.8: Nastavení SW konektoru pro získání dat z excelové tabulky na snímku A.3. V následujícím SW konektoru bude použit sloupec *stisk_tl* s proměnnou FALSE, který je nejprve nutno si předpřipravit tímto krokem.



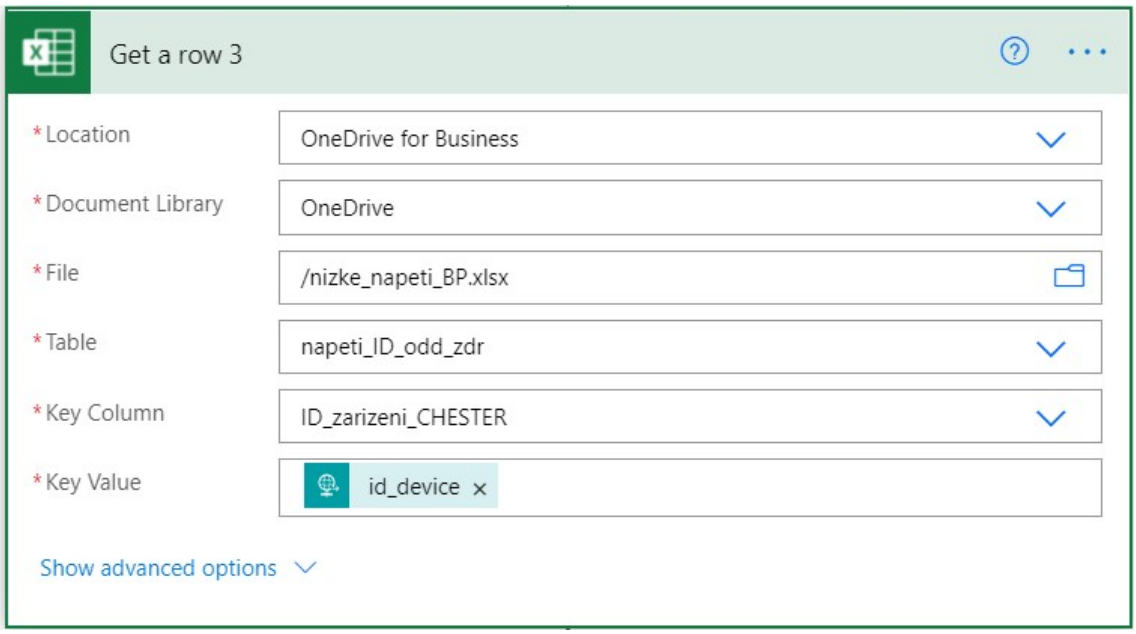
Obrázek A.9: Porovnávání prototypem zaslaných proměnných s hodnotou FALSE.



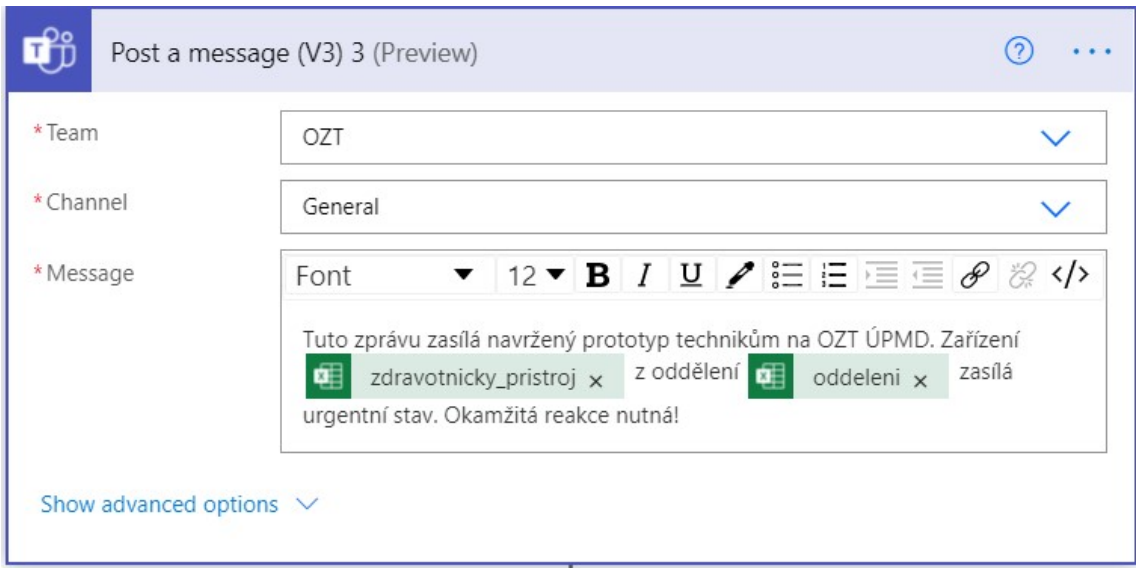
Obrázek A.10: Logická operace po splnění podmínky na obrázku A.9.



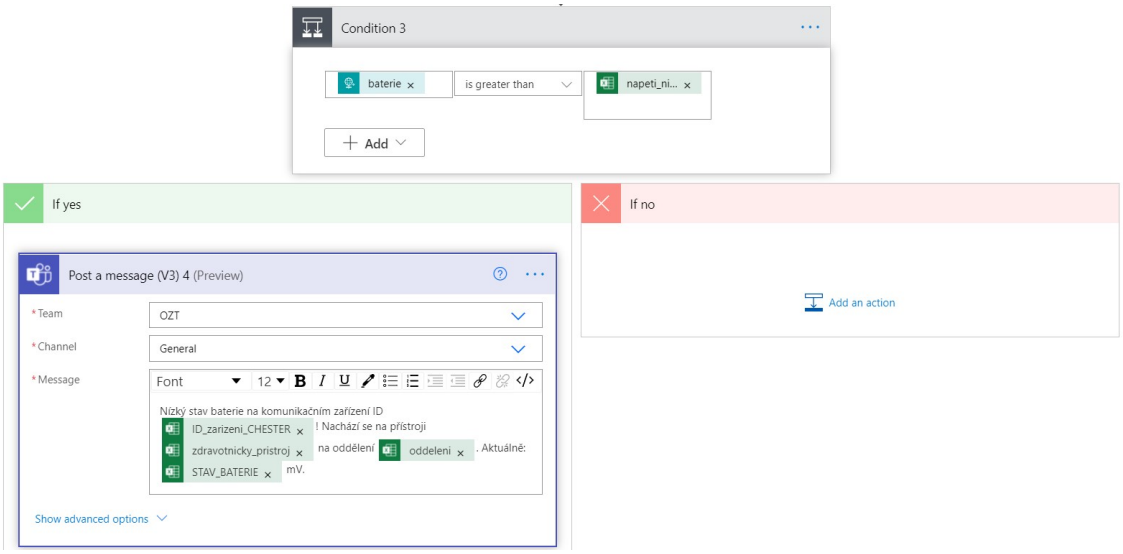
Obrázek A.11: Uložení zaslaných dat do tabulky A.4. V tomto konektoru jsou přiřazeny proměnné *číslo prototypu zařízení*, *napětí na baterii* a *časová značka* k sloupcům tabulky.



Obrázek A.12: Nastavení SW konektoru pro získání dat z excelové tabulky na snímku A.3. V následujícím SW konektoru bude použit sloupec *C* a *D*.



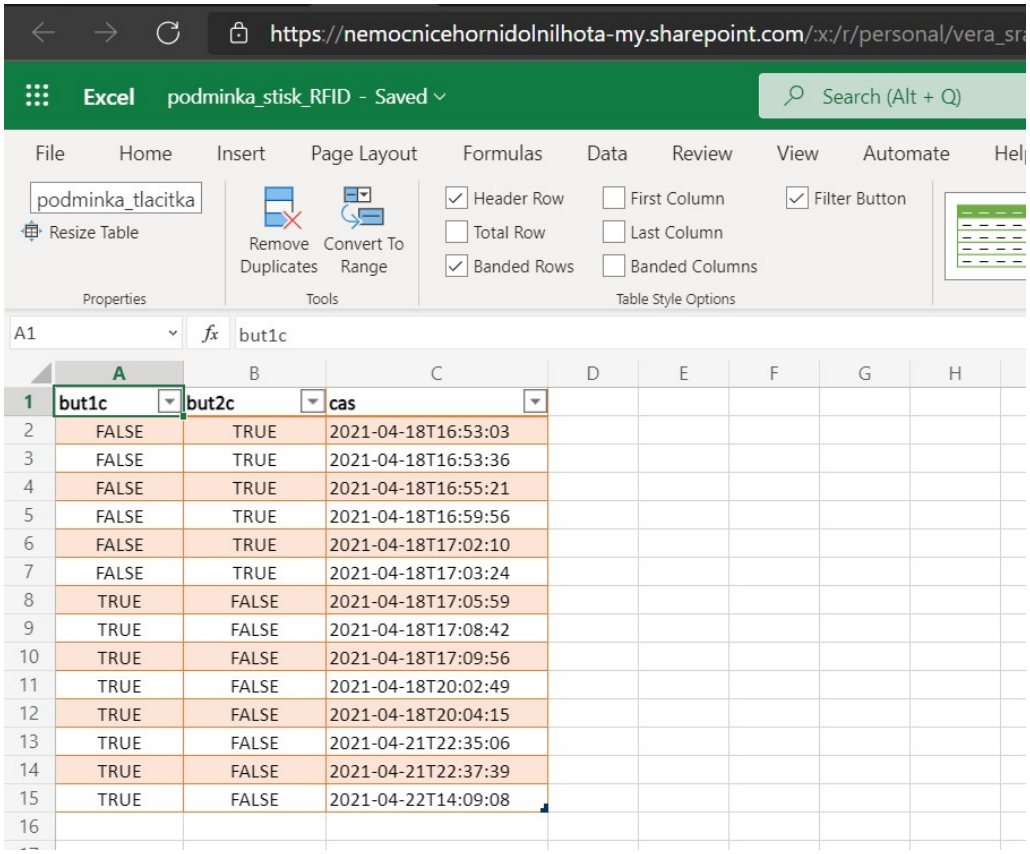
Obrázek A.13: Formát zprávy zobrazené v Microsoft Teams pro biomedicínské techniky a inženýry.



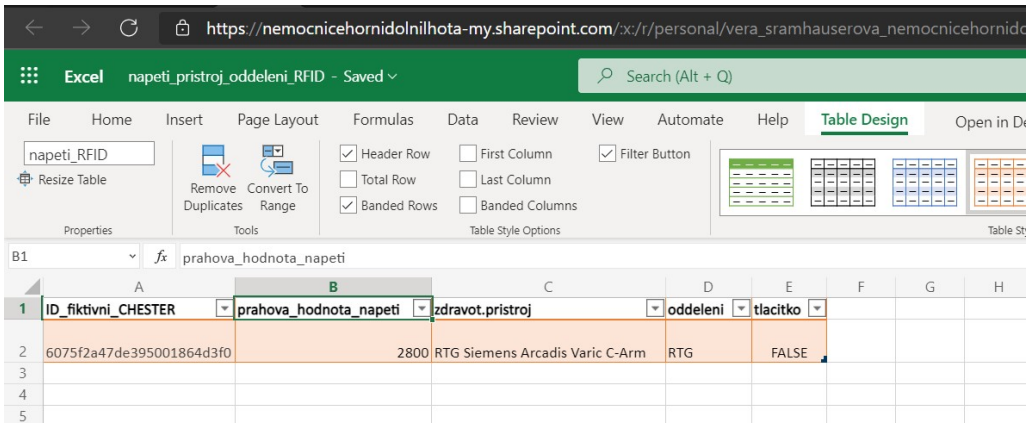
Obrázek A.14: Nastavení podmínky pro zasílání stavu Li-Ion článku, včetně zobrazení zprávy o nutnosti provedení údržby, do Microsoft Teams.

A.3 Softwarově navržený prototyp s RFID

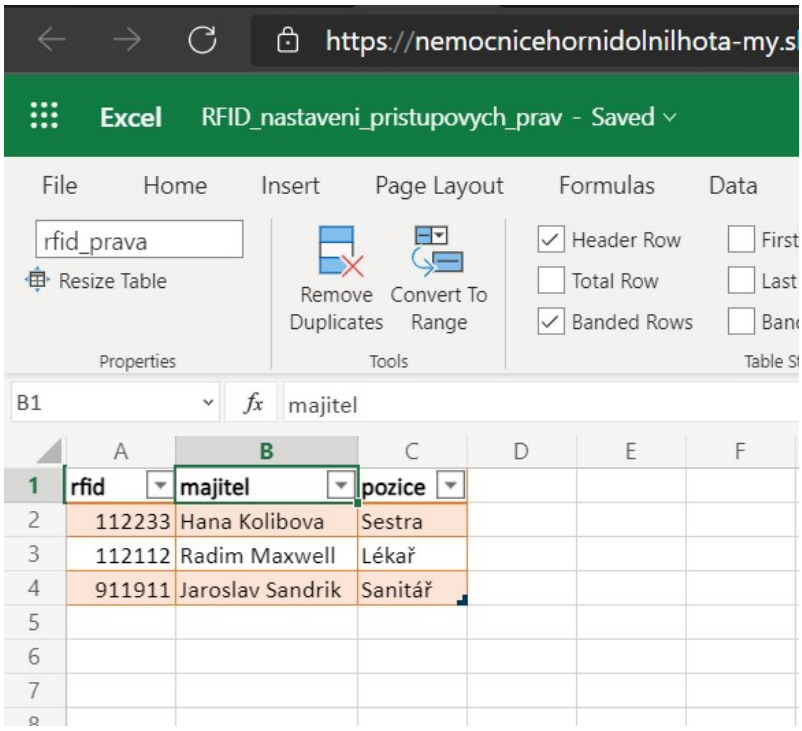
A.3.1 Excelové dokumenty



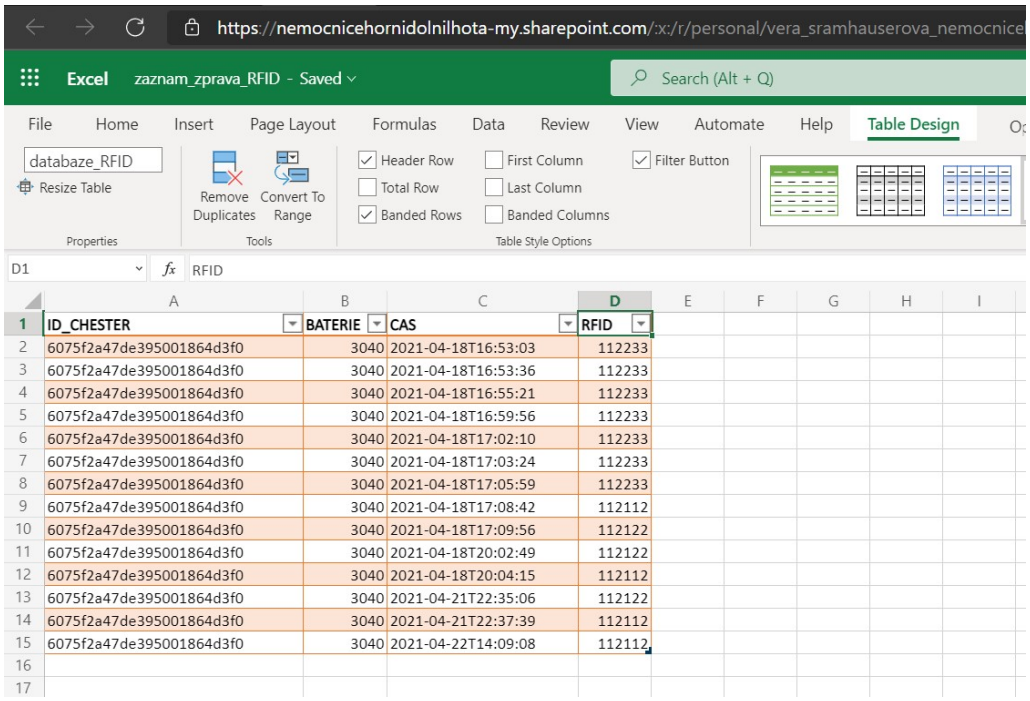
Obrázek A.15: Tabulka pro uložení zaslané hodnoty TRUE po stisku tlačítka.



Obrázek A.16: Hodnoty ID fiktivního prototypu, napětí na baterii, název zdravotnického přístroje, oddělení, časové značky a stavu tlačítka FALSE.



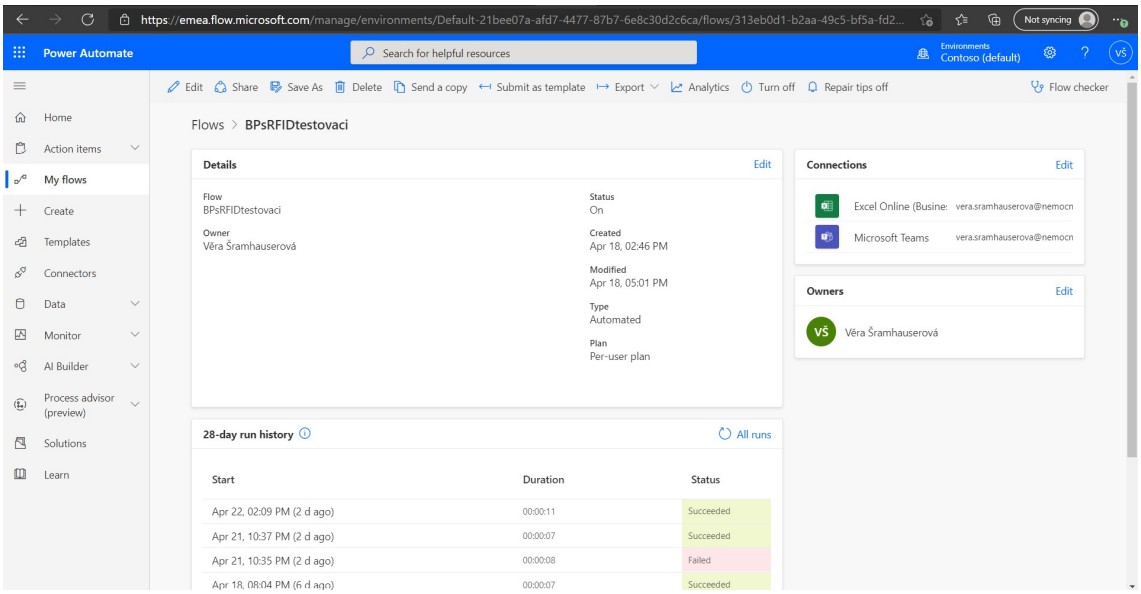
Obrázek A.17: Databáze osob s udělenými právy pro zaslání autorizované zprávy.



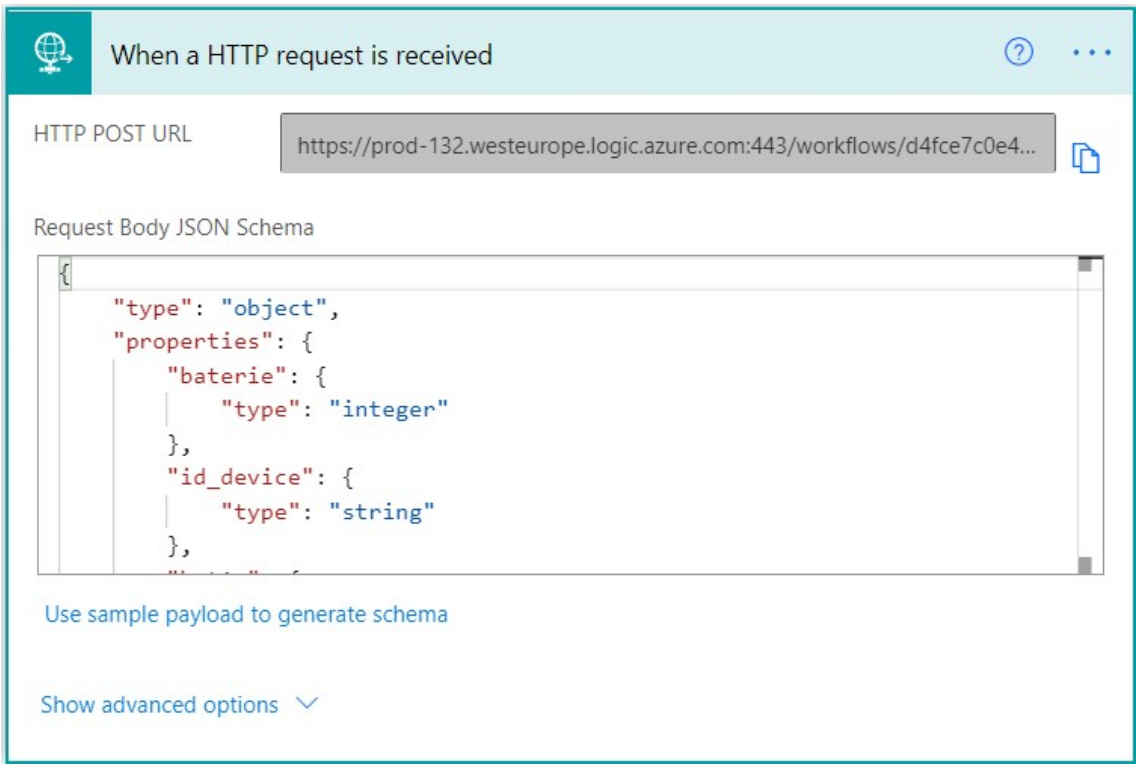
Obrázek A.18: Tabulka, do níž se ukládají zaslané zprávy, které splnily podmínku stisku tlačítka (TRUE). Do této databáze se ukládá *číslo ID zařízení navrženého prototypu*, *napětí na baterii v mV*, *časová značka* a *číslo RFID karty zaměstnance* posílajícího zprávu o poruše zdravotnického přístroje.

A.3.2 Tok v Power Automate

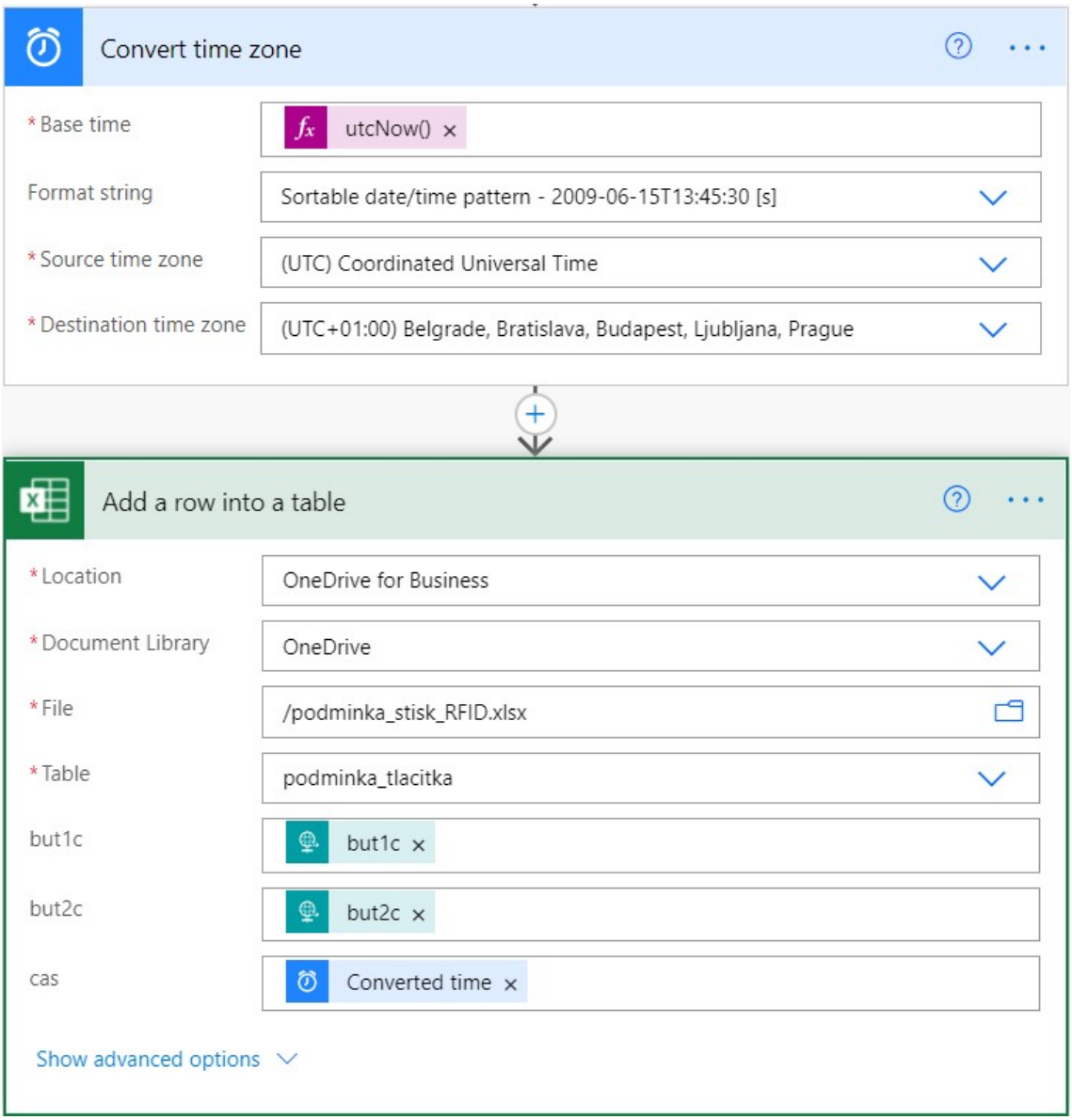
Dle schématu obrázek 11.6 tok označený písmenem B.



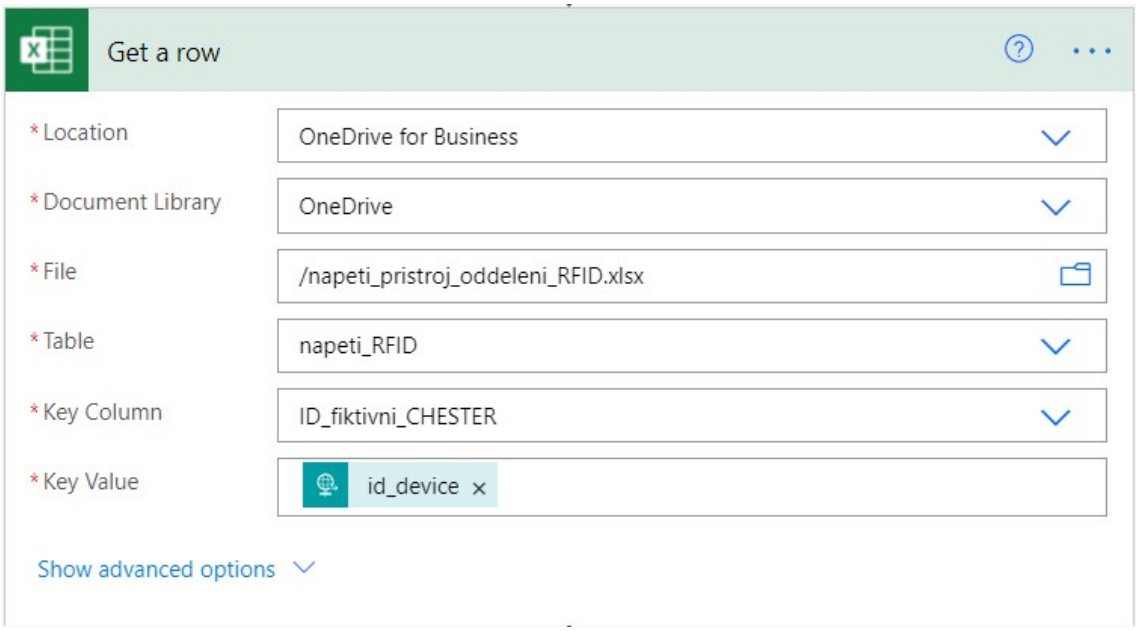
Obrázek A.19: Ukázka prostředí Power Automate se zobrazeným tokem pro simulovaný hardware s RFID čtečkou. Zobrazení informací o toku.



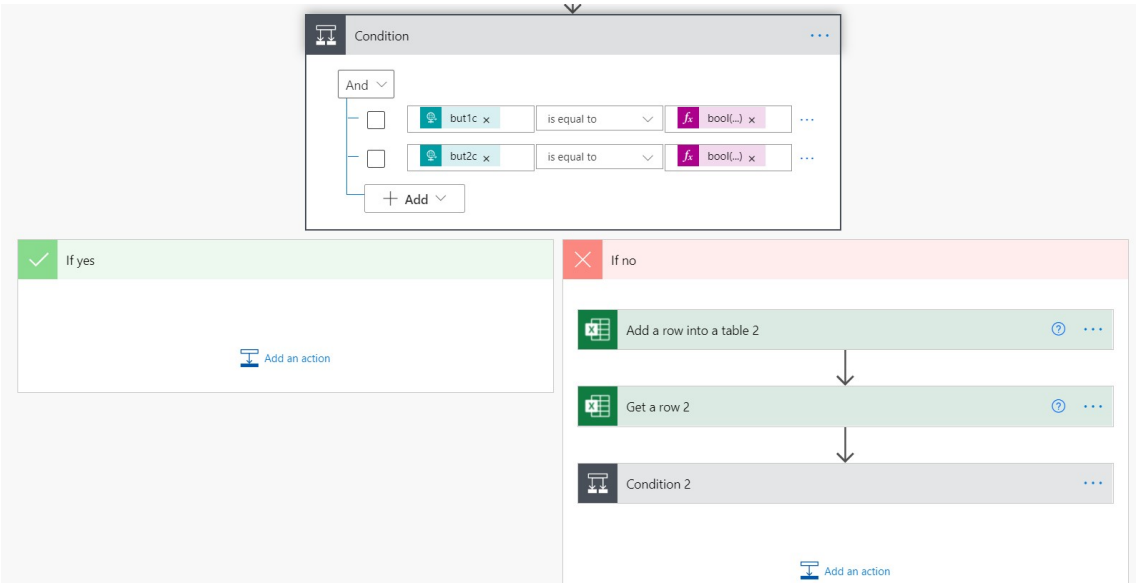
Obrázek A.20: Zasílaná zpráva ve formátu JSON a URL adresa toku.



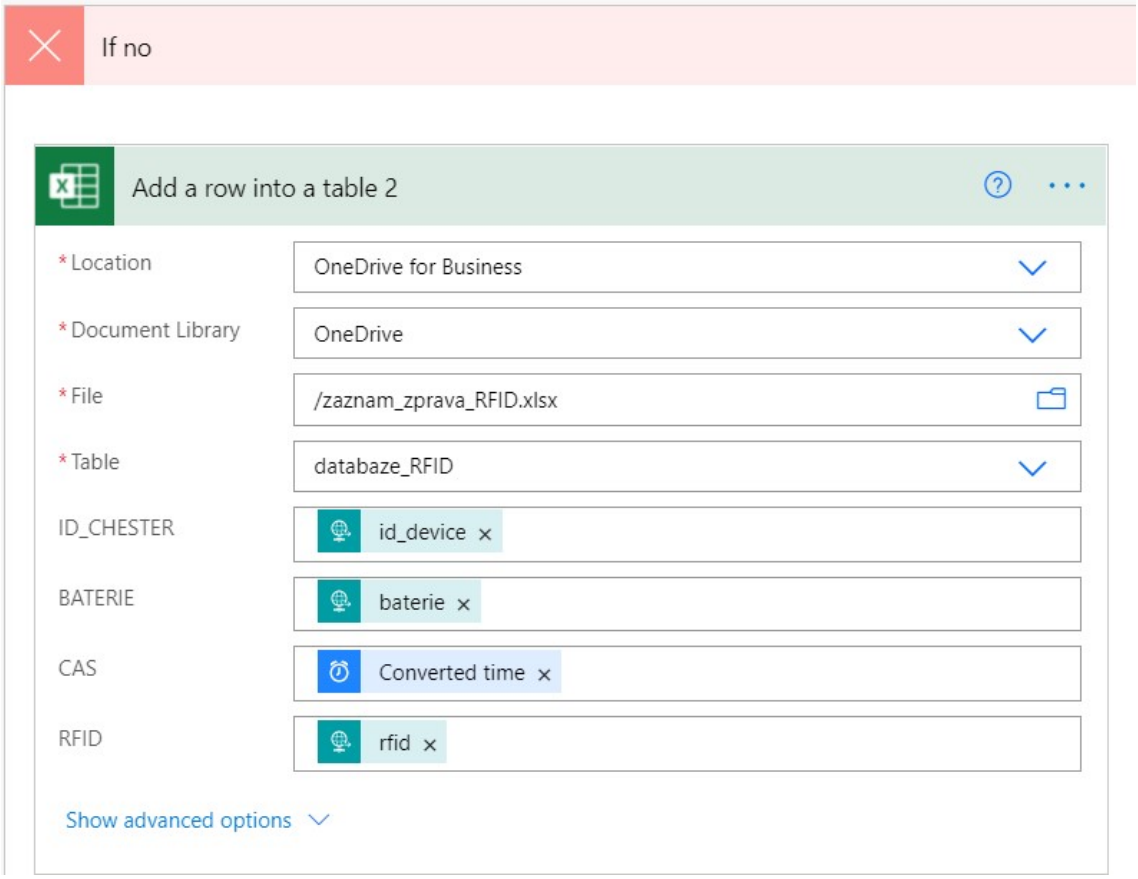
Obrázek A.21: SW konektor pro změnu časového pásma společně se SW konektorem pro zápis řádků do excelové tabulky na obrázku A.15 pomocí připravených proměnných. But je zkratkou pro button (tlačítko).



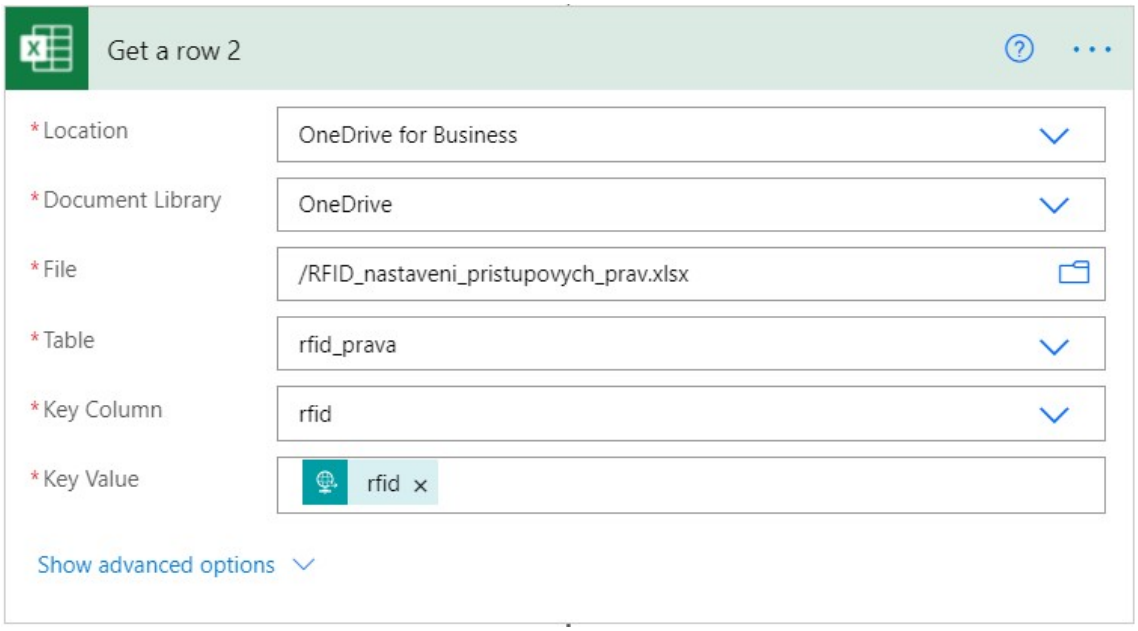
Obrázek A.22: Nastavení SW konektoru pro získání dat z excelové tabulky na snímku A.16. V následujícím SW konektoru bude použit sloupec *tlacitko* s proměnnou FALSE, který je nejprve nutno si předpřipravit tímto krokem.



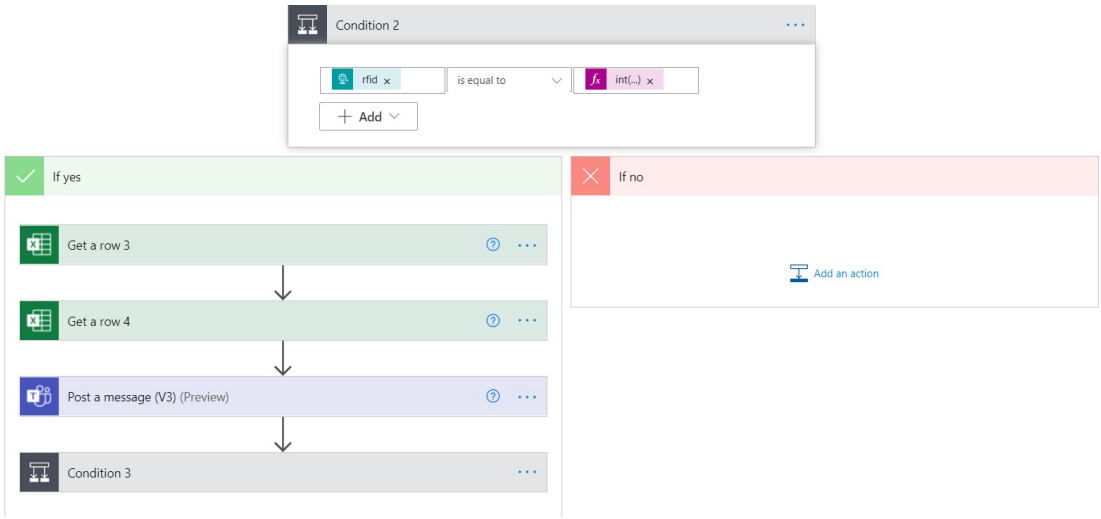
Obrázek A.23: Porovnávání prototypem zaslaných proměnných s hodnotou FALSE, předpřipravenou předchozím SW konektorem, a logická operace po splnění podmínky.



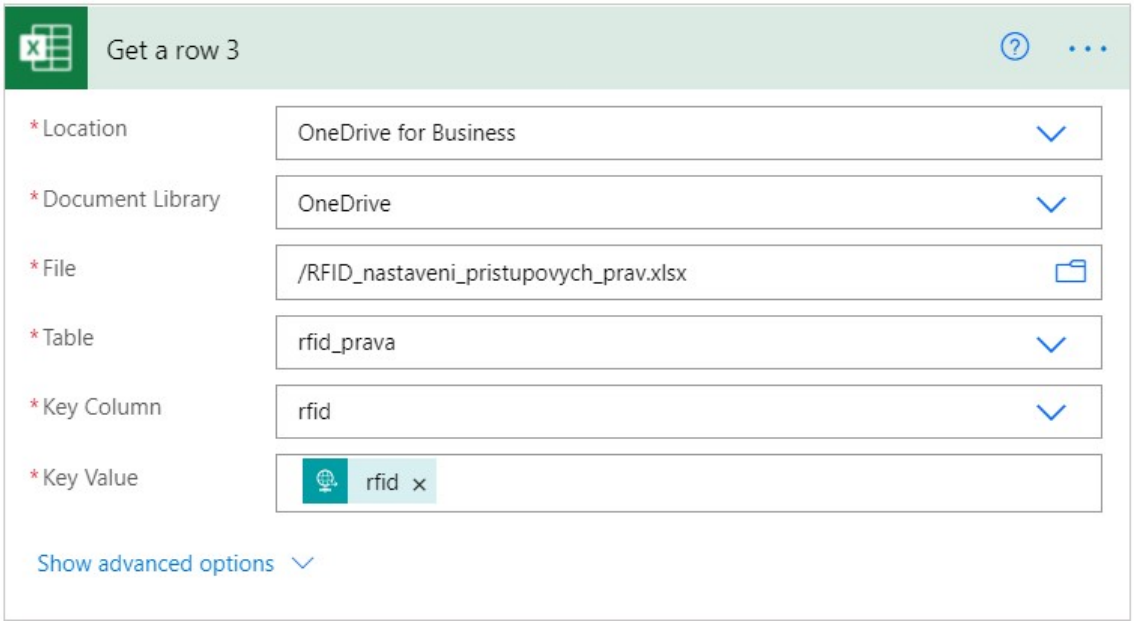
Obrázek A.24: Uložení zaslaných dat do tabulky A.18. V tomto konektoru jsou přiřazeny proměnné k sloupcům tabulky.



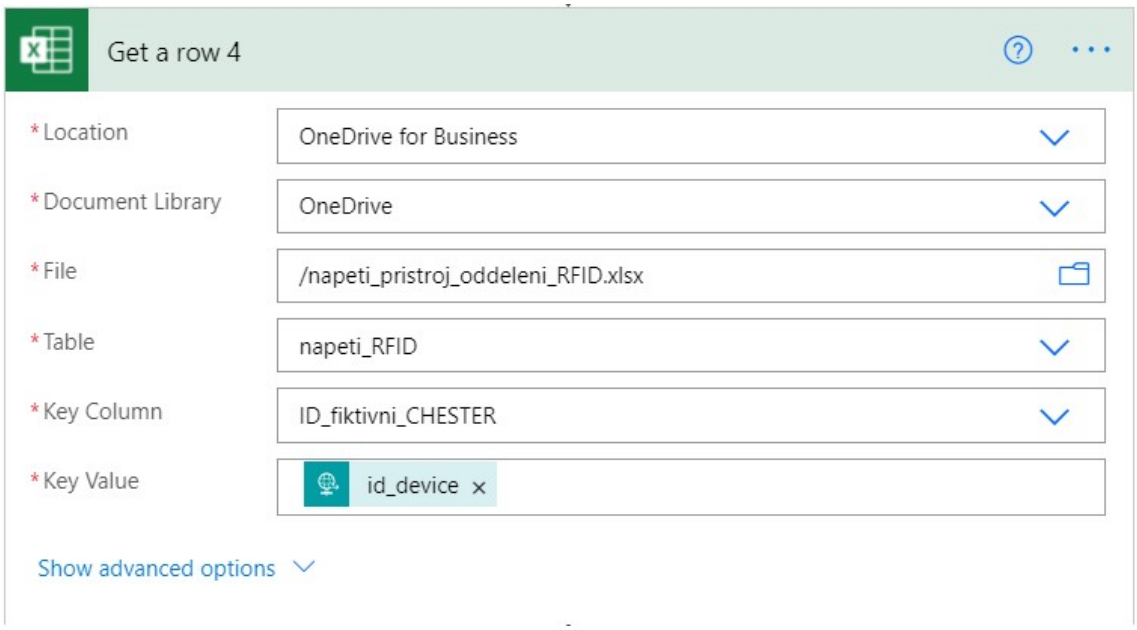
Obrázek A.25: Nastavení SW konektoru pro získání dat o autorizovaných zaměstnancích z A.17.



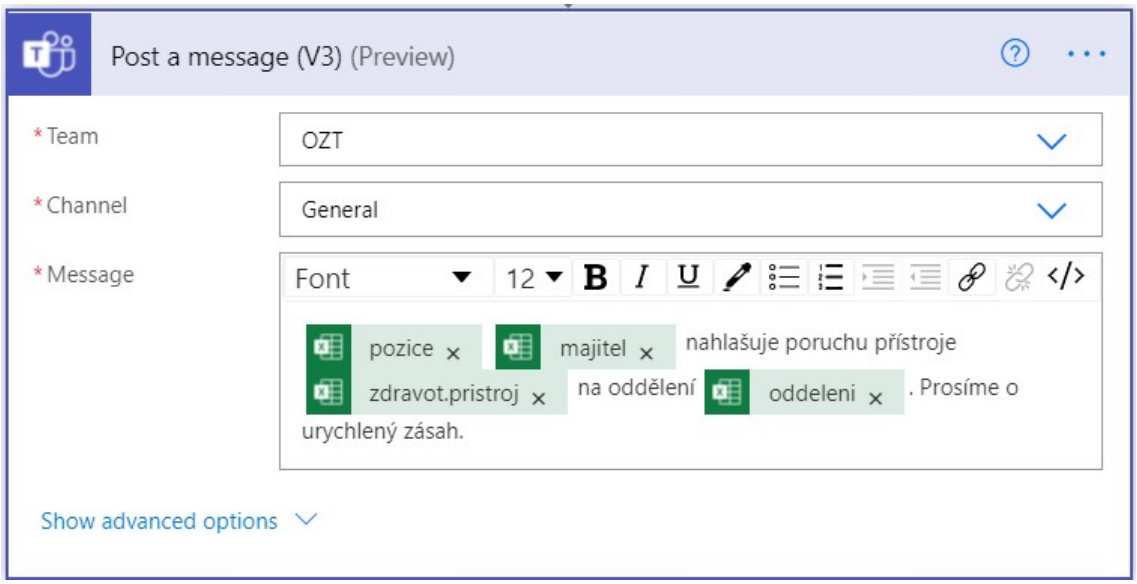
Obrázek A.26: Nastavení podmínky pro zaslanou zprávu autorizovanou/neautorizovanou osobou a následná logická operace.



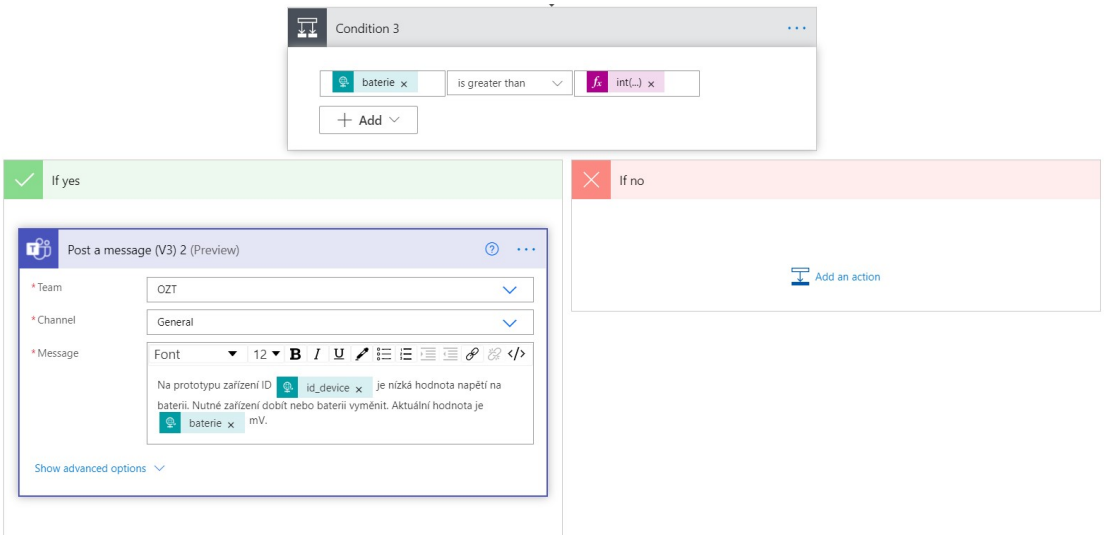
Obrázek A.27: Nastavení SW konektoru pro získání hodnot z excelové tabulky na snímku A.17. V SW konektoru pro výpis zprávy v Microsoft Teams budou použity sloupce *majitel* a *pozice*.



Obrázek A.28: Nastavení SW konektoru pro získání dat z excelové tabulky na snímku A.16 pro výpis zprávy v Microsoft Teams. V následujícím SW konektoru budou použity sloupce *zdravot.pristroj* a *oddeleni*, které je nejprve nutno si předpřipravit tímto krokem.



Obrázek A.29: Nastavení formátu zobrazované zprávy v chatu v aplikaci Microsoft Teams s použitím předpřipravených proměnných.



Obrázek A.30: Nastavení podmínky pro zasílání stavu Li-Ion článku, včetně zobrazení zprávy o nutnosti provedení údržby, do Microsoft Teams.