UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

DIPLOMOVÁ PRÁCE

2025 Jiří Pecina

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

IIoT v průmyslové automatizaci

Diplomová práce

2025 Jiří Pecina

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jiří Pecina**
Osobní číslo:	**I23263**
Studijní program:	**N0714A150005 Automatické řízení**
Téma práce:	**IIoT v průmyslové automatizaci**
Zadávající katedra:	**Katedra automatizace a matematiky**

Zásady pro vypracování

Cílem práce je analýza současného stavu technického řešení zařízení a komponent z oblasti IoT (Internetu věcí, *Internet of Things), IIoT (*Průmyslového internetu věcí) a návrh a realizace konstrukčního řešení zvolených typů komponent IIoT průmyslové automatizace.
Teoretická část práce bude obsahovat podrobnou analýzu současného stavu této technologie. Budou analyzovány dostupné komponenty z této technické oblasti a bude uveden výčet nejvýznamnějších typů těchto komponent (jednotek) a uvedeny jejich parametry a stávající technické možnosti.
V praktické části práce budou navrženy vybrané jednotky, např. pro měření a ovládání technologických veličin (např. měření aktuální spotřeby energie, ovládání zařízení pro realizaci ohřevu/chlazení kapalného média atp.). Měřené a ovládané veličiny budou zobrazovány například pomocí webového prohlížeče osobního počítače. K realizaci vlastních návrhů IoT (IIoT) jednotek budou využity moduly s jednočipovým mikropočítačem (i pro software "Web Serveru"), např. modul ESP32 WROOM. Součástí práce budou podrobné výrobní podklady a instalační manuály k realizovaným jednotkám.

Rozsah pracovní zprávy: **60**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

GUBBI, Jayavardhana, et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 2013, 29.7: 1645-1660.
KELLY, Sean Dieter Tebje; SURYADEVARA, Nagender Kumar; MUKHOPADHYAY, Subhas Chandra. Towards the implementation of IoT for environmental condition monitoring in homes. IEEE Sensors Journal, 2013, 13.10: 3846-3853.

Vedoucí diplomové práce: **Ing. Libor Havlíček, Ph.D.**
Katedra automatizace a matematiky

Datum zadání diplomové práce: **8. listopadu 2024**
Termín odevzdání diplomové práce: **23. května 2025**

L.S.

prof. Ing. Petr Doležel, Ph.D. v.r.
děkan

Ing. Libor Kupka, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 11. listopadu 2024

Prohlašuji:

Práci s názvem IIoT v průmyslové automatizaci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že 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, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 20. 5. 2025

Jiří Pecina v.r.

PODĚKOVÁNÍ

Mé poděkování patří hlavně mému vedoucímu práce Ing. Liboru Havlíčkovi, Ph.D. za odbornou pomoc a připomínky, které mi byly nápomocné při kompletaci této diplomové práce. Dále bych touto cestou rád poděkoval mé rodině a přátelům za morální podporu při studiu.

ANOTACE

Diplomová práce se zabývá návrhem a realizací IIoT monitorovacího systému pro zemědělský provoz (proces chlazení mléka). Hlavním cílem bylo analyzovat současná technická řešení a vytvořit jednotku pro sběr dat z relevantních senzorů a jejich vizualizaci. Implementovaný systém využívá mikrokontrolér ESP32 s integrovaným Wi-Fi modulem a kryptografickými funkcemi pro nízkou spotřebu energie a bezpečnou komunikaci. Měřicí část tvoří neinvazivní proudová sonda SCT-013-015 pro sledování odběru proudu a NTC termistor pro měření teploty. Naměřená data o proudu a teplotách se zpracovávají přímo na zařízení a jsou zpřístupněna uživateli prostřednictvím vestavěného webového rozhraní. Výsledkem je funkční monitorovací jednotka, která umožňuje detailní sledování provozních parametrů. Jak diplomová práce uvádí, podrobná evidence dat umožňuje optimalizovat proces a zvýšit kvalitu finálního produktu (vyšší finanční ohodnocení) a současně včasnou detekcí poruch zabránit možným ztrátám. Přínosem řešení je tedy vytvoření prakticky využitelné IIoT platformy pro on-line monitorování, jež může zvýšit spolehlivost provozu a zlepšit plánování údržby.

KLÍČOVÁ SLOVA

IIoT, ESP32, Web Server

TITLE

IIoT in industrial automation

ANNOTATION

The thesis focuses on the design and implementation of an IIoT monitoring system for an agricultural process (milk cooling). The main goal was to analyze existing technical solutions and develop a unit that non-invasively collects operational data (current consumption and temperature) and presents them to the user. The implemented system uses an ESP32 microcontroller with built-in Wi-Fi, meeting low-power and security requirements. The measurement module includes a SCT-013-015 split-core current transformer for monitoring AC consumption and an NTC thermistor for temperature measurement. Acquired data are processed on the device and served via an integrated web interface. The result is a working monitoring unit that enables detailed real-time tracking of process parameters. According to the thesis, detailed monitoring allows process optimization, higher product quality, and early fault

detection. The contribution of the work lies in delivering a functional IIoT monitoring platform that can enhance operational efficiency and maintenance planning.

KEYWORDS

IIoT, ESP32, Web Server

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

IIoT – Industrial Internet of Things

IoT – Internet of Things

AI – Artificial Intelligence

ML – Machine Learning

MQTT – Message Queuing Telemetry Transport

TLS – Transport Layer Security

HTTP – Hypertext Transfer Protocol

Wi-Fi – Wireless Fidelity

ESP – Espressif Systems Platform

PUF – Physical Unclonable Function

NTC – Negative Temperature Coefficient

CT – Current Transformer

SD – Secure Digital

GUI – Graphical User Interface

CPU – Central Processing Unit

LED – Light Emitting Diode

PCB – Printed Circuit Board

USB – Universal Serial Bus

RST – Reset

ÚVOD

Rozvoj technologií v oblasti internetu věcí (IoT) a zejména jeho průmyslové varianty IIoT (Industrial Internet of Things) přináší zásadní změny ve způsobu monitorování a řízení průmyslových procesů. V rámci Průmyslu 4.0 hraje IIoT klíčovou roli při zvyšování efektivity, spolehlivosti a prediktivních schopností výrobních systémů. Díky propojení fyzických zařízení s digitálními systémy dochází k automatickému sběru, zpracování a analýze dat v reálném čase, což umožňuje rychlejší rozhodování a optimalizaci provozu.

Tato diplomová práce se zaměřuje na návrh a realizaci prototypu IIoT systému určeného pro sledování vybraného technologického procesu v zemědělské praxi – konkrétně pro monitoring průběhu chlazení mléka. Cílem práce je navrhnout, implementovat a ověřit funkční jednotku schopnou sběru údajů o teplotě a spotřebě elektrické energie, jejichž změny indikují stav technologického zařízení.

Jako základní výpočetní a komunikační jednotka byl zvolen mikrokontrolér ESP32, který nabízí dostatečný výpočetní výkon, nízkou spotřebu energie a integrovanou podporu bezdrátové komunikace (Wi-Fi). Systém je dále doplněn o neinvazivní proudovou sondu pro měření odběru a NTC termistor pro snímání teploty. Naměřená data jsou zpracovávána přímo na zařízení a uživatelům zpřístupněna prostřednictvím vestavěného webového rozhraní.

.

1. Průmyslový internet věcí

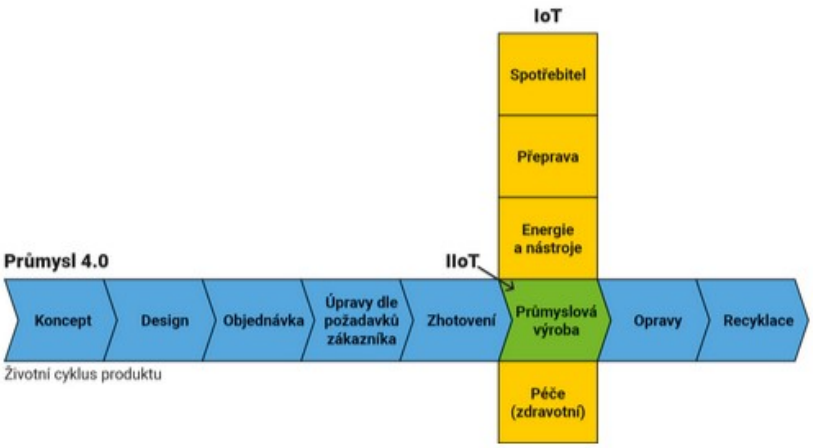
Internet věcí (IoT) dle Mezinárodní elektrotechnické komise

Infrastruktura vzájemně propojených entit, lidi, systémů a zdrojů informací společně se službami, která zpracovává informace z fyzického světa a virtuálního světa a reaguje na ně. (ISO/IEC 20924)

Průmyslový internet věcí (IIoT) dle slovníku Industrial Internet of Things

Integrace a propojeni průmyslových řídících systémů s podnikovými systémy, byznys procesy a analytickými nástroji (Karmarkar a Buchheit 2018).

Průmyslový internet věcí je technologie zaměřující se na použití propojených zařízení senzorů, softwaru, umělé inteligence a strojového učení v průmyslovém odvětví, jako je, výroba, energetika, logistika apod. Myšlenkou je sběr, sledování a analýzu dat v reálném čase. Tento koncept vede k vyšší efektivitě, snížení prostojů a lepšímu rozhodování ve firemní strategii. Koncept průmyslového internetu věcí je úzce spojen s termínem Industy 4.0. V česku známé jako Průmysl 4.0 nebo také 4. průmyslová revoluce. Jedná se o celkový koncept přístupu k průmyslovým výrobkům od jejich konceptu až po výrobu, dopravu a recyklaci s důrazem na ekologii. Přičemž průmyslový internet věcí se zabývá získáváním dat ze senzorů a zařízení a jejich zpracování s ohledem na zefektivnění výrobního procesu.

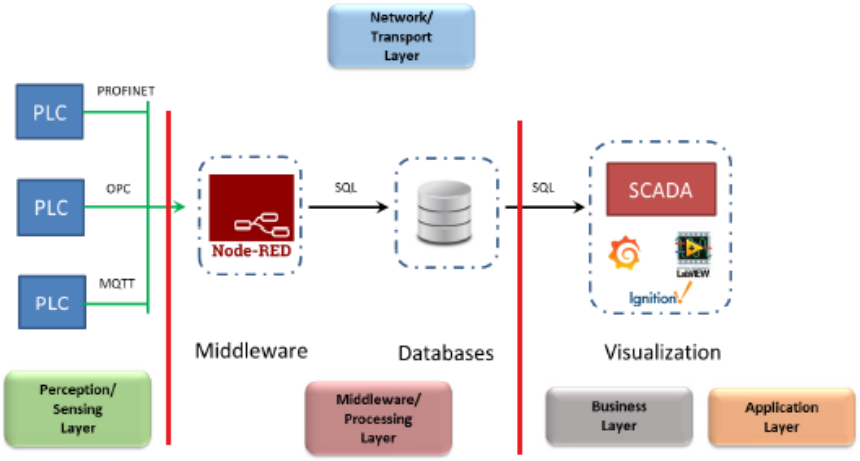


Obrázek 1 Vymezení pojmu Průmysl 4.0 a IIoT (FOXON 2024)

1.1. Referenční architektura IIoT

Architekturu systému můžeme chápat jako formální popis systému na úrovni jednotlivých komponent vedoucí k jeho implementaci nebo jako strukturu komponent a jejich vazeb včetně principů pro rozvoj systému v čase. (Sládek 2020)

Pro podrobnější popis principu a fungování IIoT zde bude využita IoT architektura z článku (Folgado 2024). Tato pětivrstvá Architektura podobná TCP/IP modelu je stupněm abstrakce v pomyslném středu mezi komplexními referenčními architekturami zaměřujícími se na aplikaci a inovaci do průmyslu 4.0 s konkrétním využitím a automatizační pyramidou jakožto představou o průmyslu 3.0 z roku 1990, kde bylo uvažováno pouze vertikální propojení. (Folgado 2024)



Obrázek 2 Zobrazení komunikace IIoT s vyznačením vrstev IIoT architektury (Folgado 2024)

Perception/ sensig Layer, tuto vrstvu je možné rozdělit na Senzory a Aktuatory, Senzory sloužící pro sběr dat z reálného světa, převod analogových signálů na digitální a aktuátory se schopností působení na reálný svět. Jedná se o nejnižší vrstvu celého modelu, která zahrnuje senzory, roboty, PLC, výrobní linky apod.

Network/ Transport Layer, vrstva také nazývaná Transmition nebo Conectivity je odpovědná za přenos dat. Tato vrstva zahrnuje technologie a protokoly, které umožňují výměnu dat mezi ostatními vrstvami. Jako příklad je možné uvést komunikační protokoly MQTT, TCP/IP,Wi-FI, PROFINET Modbus dále také síťové prvky.

Application Layer, také nazývaná Service, jedná se o vrchní vrstvu, která slouží pro komunikaci s uživatelem. Zde se nachází software pro zpracování dat a kontrolu procesu

s využitím grafického rozhraní, HMI a supervisor systémů. Data jsou zde zpracovávána softwarem tak, aby byla použitelná pro management.

Middleware/Procesing Layer, zásadními funkcemi této vrstvy je ukládání dat, filtrace, analýza a zpracování dat pro Application layer. V této vrstvě jsou přijímána data z různorodých zařízení, která používají různé protokoly. Úkolem této vrstvy je přijmout různorodá data zpracovat je a poskytnout je transportní vrstvě.

Další vrstvy nad rámec dříve zmíněných doplňují funkcionality Application layer a jsou to například Security. (Folgado 2024) (obr.2). zobrazuje vyznačení jednotlivých vrstev ve schéma komunikace PLC až vizualizační program v PC.

1.2. Strategie soustředění prostředků pro zpracování dat

Cloud computing

Označuje přístup zpracování a vyhodnocování dat v cloudovém prostředí, což snižuje nároky na fyzické zařízení uživatele. Surová data jsou přímo odesílána k zpracování na Cloud. Myšlenku tohoto přístupu zasadil na počátku šedesátých let Dr.Joseph Carl Robnett Lickyre. (IBM 2024) Jedná se o soubor serveru, které zpřístupňují software a databáze po internetu. Infrastruktura je tvořena více než 8000 datovými centry rozmístěnými po celém světě, přičemž přes 30 % z nich je umístěno v USA. (Armenta 2024) Cloud computing lze rozdělit na tři hlavní typy zprostředkovávaných služeb, a to jsou IaaS (Infrastructure as a service), PaaS (Platform as Service) a SaaS (Software as a Service). IssaS je strategie, kdy si firmy platí přístup k virtuálnímu hardwaru pro zvýšení výpočetní kapacity nebo uložiště. PaaS zprostředkovává platformové nástroje pro vývojáře aplikací. A SaaS zprostředkovává přístup k software. V dnešní době je většina těchto služeb přístupná s vazbou na měsíční poplatky. (Nikita 2024) Pro účely IIoT čelí cloud computing výzvě bezpečnosti. Proto firmy k této strategii přistupují s opatrností a většinou se jedná o kolaboraci s Edge computing strategii.

Edge computing

Je označení pro běh aplikací a ukládání dat v blízkosti řídících procesů. Kritické parametry pro okrajová zařízení (edge computing) jsou nízká latence vůči procesnímu zařízení, schopnost zpracovávat data v reálném čase a škálovatelnost aplikací. Okrajová zařízení bývá připojena přímo v síti zařízení provozní technologie. Z čehož vyplývá, že odpadá odesílaní dat na centrální servery čímž se snižuje logická vzdálenost mezi generováním dat a jejich zpracováním. Škálování infrastruktury dociluje udržení rychlosti odezvy a zachování výkonu při rostoucí síti. Edge computing muže být řešeno jako virtuální počítač nebo jako fyzické

zařízení jako například průmyslový počítač. Virtuální zařízení musí splňovat požadavky na malou latenci odezvy. Z hlediska bezpečnosti má tento přístup organizace sítě nejen výhody v dříve zmíněných bodech ale také v tom, že data zůstávají v místní sítí a ze sítě do prostředí internetu a cloudu putuje menší množství obecnějších dat. (Cates 2024)

Fog computing

Jedná se o přístup rozšiřování Cloud Computing strategie, tak aby byla blíž uživateli/firmě. Obecně lze fog označit jako mezistupeň mezi edge a cloud computing. Oproti egde computing se již nejedná o decentralizovanou strategii, což jako cloud computing přináší bezpečností rizika. Na druhou stranu přináší ke koncovým zařízení, která v některých případech nedisponují příliš robustním zabezpečením, pohled cloudového robustního zabezpečení. Dohromady tedy dochází k vyššímu stupni zabezpečení celého ekosystému. Dále přináší nespornou výhodu oproti cloud computing, protože je zde nízká latence díky bližšímu umístění serveru pro zpracovaní dat k uživateli. Což umožnuje využívání realtime aplikací a má velký vliv na rozhodovací firemní proces v reálném čase, které Cloud nedokáže zprostředkovat. (Scale 2024) Ve spojení s fog computing se v odborné literatuře objevuje pojem Mist computing. Označující Low-power servery umístěné ještě blíž koncovým zařízením s myšlenkou použití velkého počtu těchto serveru. (Clancy 2024)

Cloud-Edge computing

Jedná se o paradigma využití kladných vlastností cloud compting a edge computing strategii. Jde o snahu co nejvyšší efektivity z pohledu času zpracování dat a zatížení výpočetních prvků. V reálných aplikacích jde ve většině případů o tuto strategii využití a organizace IIoT. Například v automobilovém průmyslu sběr dat v reálném čase z výrobních linek jejich zpracování v edge prostoru (vyhodnocení hladiny vibrací – zahájení diagnostiky při nesrovnalostech) a následné sdílení statistických dat na cloud.

Blockchain

Obecně známá technologie ve spojitosti s kryptoměnami jako je třeba Bitcoin nebo Etherium. Blockchain je definován jako decentralizovaná, neměnná, důvěryhodná a sdílená účetní kniha postavená na distribuovaných sítích typu peer-to-peer (P2P). Jejím klíčovým prvkem je decentralizace, díky níž není potřeba žádné centrální autority k řízení nebo správě zapojených uzlů. Všechny uzly v síti udržují identické kopie účetní knihy, přičemž každá transakce je ověřována a validována většinou čestných uzlů. Tato architektura zajišťuje bezpečný

a robustní provoz, eliminuje riziko selhání jednotlivých bodů a zaručuje odolnost vůči manipulaci. Při přidávání nových bloků do blockchainu dochází k synchronizaci mezi všemi uzly pomocí konsensuálního protokolu, což zajišťuje správnost a jednotnost dat. Tato technologie tak nachází využití nejen v kryptoměnách, ale i v průmyslovém internetu věcí (IIoT), kde může zajistit bezpečnou a transparentní správu dat. (Wang 2024)

1.3. Implementace umělé inteligence v IIoT

Implementace uměle inteligence strojového učení a neuronových sítí do zařízení a systémů IIoT prostupuje všemi vrstvami referenčního modelu IIoT. Informace od návrhu jednotlivých zařízení, nástroje pro programátory až po zpracování dat a zajištění bezpečnosti komunikace hraje hlavní roli ve zpracování velkého objemu dat získaných ze senzorů. V dnešní době jsou vyvíjeny mikroprocesory pro implementaci AI přímo v embended systému senzoru.

Siemens Industrial Copilot

Siemens Industrial Copilot představuje průlomové řešení, které využívá generativní umělou inteligenci pro optimalizaci procesů v průmyslovém prostředí. Tento asistent zefektivňuje práci díky schopnosti generovat SCL kód, vytvářet vizualizace a usnadňovat diagnostiku chyb. Urychluje procesy projektování a řešení problémů, díky čemuž dochází k zrychlení a zlevnění vývoje. Umožňuje komunikaci v přirozeném jazyce, což zjednodušuje jeho ovládání a zvyšuje přístupnost i pro uživatele bez hlubokých technických znalostí. Důraz je kladen na bezpečnost dat a integraci s platformou Siemens Xcelerator, což umožňuje propojení s dalšími digitálními nástroji. Díky svým schopnostem nejen snižuje pracovní zatížení, ale také přispívá k vyšší efektivitě a kvalitě průmyslových procesů, čímž podporuje inovace ve výrobě.

1.4. Komunikační protokoly IIoT

Komunikační protokoly v prostředí průmyslového internetu věcí (IIoT) hrají klíčovou roli při zajišťování efektivní výměny dat mezi koncovými zařízeními, bránami a cloudovými systémy. Tyto protokoly umožňují přenos dat v reálném čase a zajišťují interoperabilitu mezi zařízeními od různých výrobců. Zaměřují se především na spolehlivost, nízkou latenci a schopnost přizpůsobit se různorodým průmyslovým aplikacím. Mezi tyto protokoly patří Modbus, Zigbee, LoRaWAN, BACnet MQTT atd. Vzhledem k orientaci práce na koncová zařízení bude v následující kapitole popsán protokol MQTT, jakožto nejpoužívanější protokol pro komunikaci mezi koncovými zařízeními a Edge zařízeními.

1.4.1. MQTT (Message Queuing Telemetry Transport)

Jedná se o protokol vycházející z protokolu HTTP ovšem byl vytvořen pro účeli IoT/ IIoT. Byl vytvořen firmou IBM roku 1999. Odpovídá standardům OASIS a ISO normě **ISO/IEC 20922.** HTTP komunikační rámec je pro využití v IoT příliš složitý. Přeposílá příliš velké množství dat. MQTT protokol byl vytvořen přímo pro tyto aplikace, kde komunikuje velké množství zařízení s jednoduchým procesorem a centrálním broker tzv. Client-Server architektura. Na základně standartního ISO/OSI modelu pracuje na transportní vrstvě. Centrální server je označen jako **broker** a klienti jsou zařízení a aplikace, které s ním komunikují. Tento protokol je určen pro aplikace, které potřebují efektivní, škálovatelné a zabezpečené zasílání malých datových paketů přes nespolehlivé nebo nízkokapacitní sítě, což ho činí ideální pro IoT/IIoT aplikace.

Architektura MQTT se skládá ze tří hlavních komponent:

Broker (MQTT Broker): Centrální server, který přijímá všechny zprávy od klientů a distribuuje je k ostatním klientům na základě jejich předplatného.

Klient (MQTT Client): Zařízení nebo aplikace, která se připojuje k brokeru a buď odesílá zprávy (publikuje), nebo je přijímá (předplácí).

Témata (Topics): MQTT používá hierarchická témata, která definují kanály pro komunikaci mezi klienty. Klienti mohou publikovat zprávy na určitá témata a jiní klienti se mohou na tato témata přihlásit, aby je přijímali.

Broker obstarává všechny operace s předplatnými a publikovanými zprávami. Klienti

se připojují k brokeru pomocí jednoduché TCP/IP nebo TLS komunikace. Komunikace mezi klientem a brokerem je založena na tzv. *publish-subscribe* modelu, což umožňuje efektivní distribuci dat. Jedná se o kontrast oproti běžnému šíření zpráv, které probíhá v režimu publisher (broker) odesílá zprávu přímo konkrétnímu klientovi (Subscriber).

Základní operace v MQTT komunikaci

Publish: Klient odesílá zprávu na určité téma. Tuto zprávu obdrží všichni klienti přihlášeni

na toto téma.

Subscribe: Klient se přihlašuje na určitá témata. Na základě tohoto přihlášení mu následně broker odesílá zprávy na toto téma.

Unsubscribe: Klient se odhlásí od tématu, což znamená, že nebude dostávat žádné nové zprávy na toto téma.

MQTT zpráva

Přenášená jednotka dat, která obsahuje hlavičku (header) a data (payload). V hlavičce jsou uchována data o typu zprávy, téma, velikost dat.

MQTT a QoS

MQTT umožňuje definovat tři úrovně kvality služby (Quality of Service, QoS), které určují, jak spolehlivě bude zpráva doručena:

QoS 0 (At most once): Zpráva je odeslána pouze jednou a není zaručeno její doručení. Pokud je klient offline nebo dojde k přerušení komunikace, zpráva se nezopakuje.

QoS 1 (At least once): Zpráva bude doručena alespoň jednou. Pokud dojde k výpadku připojení, zpráva bude znovu odeslána, dokud nebude úspěšně doručena. Odesilatel zprávy si uchová kopii, dokud mu od příjemce nepřijde PUBACK paket potvrzující přijetí zprávy. Pokud toto v určitém čase odesilatel neobdrží tento paket odesílá zprávu znovu dokud tento potvrzující paket od příjemce nedostane.

QoS 2 (Exactly once): Každá zpráva bude doručena přesně jednou, bez ohledu na přerušení komunikace. Tento QoS je nejnáročnější na šířku pásma a výkon brokeru, protože vyžaduje mechanismus potvrzení zprávy. Jedná se o princip, kdy je příjem každé zprávy potvrzován tzv. 4-way handshake. Odesilatel odešle zprávu, na kterou mu příjemce odešle potvrzovací paket. Po přijetí potvrzovacího paketu odesilatel tento paket uloží a vymaže z paměti odesílanou zprávu a odešle paket potvrzující vymazáni dat, na který mu příjemce odpoví paketem s informaci o vymazání stavů. Díky, čemuž je zajištěno, že byla zpráva doručena právě jednou a nedošlo k její duplikaci. (HiveMQ 2024)

Bezpečnost v MQTT

Bezpečnost je důležitým aspektem komunikace v IoT. MQTT standardně nezajišťuje šifrování ani autentifikaci, ale tato funkcionalita je často implementována pomocí dalších protokolů nebo prostřednictvím konfigurace brokeru. Bezpečnostní opatření zahrnují:

Autentifikace a autorizace: MQTT podporuje autentifikaci uživatelů pomocí uživatelského jména a hesla. Broker může zkontrolovat, zda je uživatel oprávněn k připojení a přístupu k určitým tématům.

Šifrování pomocí TLS/SSL: MQTT může používat TLS/SSL pro šifrování komunikace mezi klientem a brokerem, což zajišťuje bezpečný přenos dat.

Ověření integrity zpráv: Pro zajištění integrity a ochrany před neoprávněnými změnami zpráv může MQTT využívat šifrování a digitální podpisy.

Výhody MQTT pro IIoT

MQTT je ideální pro použití v IIoT, a to z několika důvodů. Nízké nároky na šířku pásma v IIoT jsou odesílány zprávy s malým objemem dat. Dále nízká latence, která je klíčová v průmyslovém prostředí. Rychlé doručování zpráv umožnuje aplikaci Real-Time sledování a ovládání. Díky propracovanému QoS 1 a 2 je zajištěna spolehlivost komunikace. Nedochází ke ztrátě důležitých dat. Na úrovni brokerů umožnuje rozšiřovat topologii, tedy propojovat mezi sebou jednotlivé brokery větších sítí a tím vytvářet komplexní strukturu například hvězdicovou.

Příklady použití MQTT v IIoT a IoT

MQTT se široce používá v průmyslových aplikacích pro sběr dat ze senzorů, ovládání zařízení a řízení procesů. Mezi běžné příklady použití patří monitorování a řízení výrobních linek, inteligentní budovy, sledování energetické spotřeby, logistika a transport osob. Při monitorování a řízení výrobních linek hraje v dnešní době hlavní roli v **edge computing** procesech, protože zprostředkovává propojení a synchronizaci dat mezi koncovými zařízeními a serverem. To umožnuje analýzu dat v reálném čase a rozprostření výpočetního výkonu mezi edge a server. Na což navazuje sledování parametrů provozu a možnost prediktivní plánování a rozhodování a zvyšování kvality produktu. Tvoří zde propojeni mezi IT OT světem a průmyslem 4.0. (IMB 2024)

V kontextu inteligentních budov se jedná o kontrolu spotřeb energii, zabezpečení. Hlavní výhodou je konektivita mezi různými druhy sítí jako například mobilní či Zigbee pomocí bran. Díky tomu je možné tvořit komplexní propojené řešení s implementací různých komerčně dostupných produktů. Škálovatelnost sítě umožnuje rozdělení budovy na jednotlivá patra, díky čemu je docíleno přehlednosti a jednoduchosti. (Beviwise 2024) V energetice protokol MQTT usnadňuje integraci obnovitelných zdrojů (solární, větrné elektrárny) díky zefektivnění řízení distribuce energie tak aby byla vyvážena nabídka a poptávka. Umožnuje zvýšení kontroly a plánování údržby transformátorů, turbín a čerpadel. Z naměřených dat o provozních podmínkách teplotě, vibracích a dalších je možné údržbu plánovat přesněji a snížit tak prostoje.

Výhodou protokolu MQTT oproti často využívanému MODBUS protokolu je že umožnuje zabezpečenou komunikaci, mobilní přístup a efektivní zpracování dat. (Beviwise 2024)

MQTT je robustní, efektivní a flexibilní komunikační protokol, který je ideální pro prostředí IIoT, kde je potřeba spolehlivě a efektivně přenášet malé objemy dat mezi zařízeními s nízkými nároky na šířku pásma a nízkou latencí. Díky své jednoduchosti, podpoře pro různé QoS úrovně, a možnosti šifrování a autentifikace je MQTT velmi vhodný pro široké spektrum aplikací v oblasti IoT, od domácí automatizace až po průmyslové řízení procesů.

1.5. Zabezpečení IIoT

Kybernetické útoky na průmyslový internet věcí (IIoT) představují stále rostoucí hrozbu v digitálním prostředí, které se neustále vyvíjí. Přijetí pokročilých technologií v průmyslu vedlo ke zlepšení provozní efektivity, ale zároveň zvýšilo zranitelnost těchto systémů vůči kybernetickým hrozbám. Tyto útoky mohou mít vážné následky, které sahají od narušení provozu až po ohrožení lidské bezpečnosti a ochrany soukromí. S postupným rozvojem útoků je nezbytné stále aktualizovat a zefektivňovat metody ochrany a minimalizace rizik. Na rozdíl od IT zabezpečení je zde velká limitace nízkou spotřebou energie a jednoduché síťové protokoly.

1.5.1. Typy útoků

Typy útoků se liší podle toho, na kterou vrstvu referenčního modelu jsou útoky vedeny. V této práce budou rozebrány pouze typy útoků vedených na Fyzickou (Perception) vrstvu a s ní bezprostředně spojenými systémy. Útoky vedeny na tuto vrstvu se zaměřují na znehodnocování dat získaných ze senzorů nebo jako brána pro vstup do zabezpečené časti interní sítě.

Fyzický útok

Fyzické útoky zahrnují přímý přístup útočníků k zařízením, jako jsou senzory, kamery nebo akční členy. Útočníci mohou manipulovat s hardwarem, odpojit napájení, měnit nastavení nebo zařízení zcela poškodit. Manipulace se senzorovými daty může výrazně ovlivnit správnost operací v IIoT systému a vést k nesprávným výsledkům nebo rozhodnutím. Riziko je ještě vyšší v prostředí, kde jsou senzory klíčovým prvkem pro monitorování a řízení výrobních procesů nebo energetických systémů.

Obranou je fyzické zabezpečení všech zařízení a další zabezpečení na vyšší vrstvě.

Adversariální útoky

Adversarilní útoky jsou dalším typem hrozby, při níž dochází k útoku na modely strojového učení určené k detekci průniku do sítě nebo ovlivnění vyhodnocování dat. Například u zpracování obrazových dat tyto útoky vytvářejí jemné poruchy, které jsou pro lidské pozorovatele nepostřehnutelné, ale dokáží zmást klasifikační modely strojového učení. Provádí je tak, že využívá „slepých míst“, mezer mezi body dat, které model viděl při trénování. To vede k chybným rozhodnutím a narušení provozu. Útoky je možné rozdělit na dva základní typy a to ovlivnění dat, v tomto případě útočník přidává do vzorů drobné promyšlené změny, tak aby model strojového učení překročil hranice rozhodování a klasifikuje data jako jinou třídu a zvýšení chybovosti modelu, při které je snížena efektivita modelu, protože model není schopný správně klasifikovat hodnoty dříve neviděných dat. (ANTHI 2022)

Útoky na bezdrátovou komunikaci

Bezdrátové platformy často využívají šifrování, které však může být nedostatečné. Útočníci se snaží narušit komunikaci mezi zařízeními a získat přístup k citlivým datům. Bezdrátová komunikace mezi zařízeními v perception layer je zranitelná vůči odposlechu (eavesdropping), rušení signálu (jamming) a podvrhům (spoofing). Útočníci získávají přístup k citlivým informacím, které mohou být zneužity k dalším útokům nebo manipulaci se systémem. Tyto útoky mohou vést ke ztrátě dat, manipulaci s informacemi nebo narušení dostupnosti služeb. Zvláště v průmyslových aplikacích je kontinuita komunikace klíčová pro bezpečnost a efektivitu provozu.

Útoky typu Denial of Service (DoS)

Útoky Denial of Service (DoS) a jejich distribuované varianty (Distributed Denial of Service, DDoS) představují vážnou hrozbu pro průmyslový internet věcí (IIoT). Tyto útoky cílí na dostupnost systémů tím, že zahlcují síť, zařízení nebo služby nadměrným provozem, což znemožňuje legitimním uživatelům přístup k prostředkům. V prostředí IIoT mohou mít DoS útoky dalekosáhlé dopady, zahrnující výpadky výroby, narušení procesů a ekonomické ztráty. Útočníci při DoS útocích v prostředí IIoT často využívají několik klíčových mechanismů. Jedním z nich je zasypání síťového provozu, kdy útočníci zahltí síť obrovským množstvím dat, což vede k přetížení síťových zdrojů. Tento typ útoku způsobuje, že senzory, akční členy nebo jiné IIoT zařízení nejsou schopny komunikovat se systémem v reálném čase. Dalším mechanismem je exploatace protokolů, protože lehké komunikační protokoly, jako MQTT nebo CoAP, používané v IIoT, často nemají dostatečnou ochranu proti zahlcení. Útočníci mohou tyto protokoly zneužít k vyvolání zahlcení zařízení a systémů. Kromě toho se útoky

mohou zaměřit na konkrétní zařízení, jako jsou řídicí jednotky (PLC) nebo senzory, což může způsobit lokální výpadky s kaskádovým efektem na celý systém.

Dopady útoků na IIoT zařízení

Dopady útoků na IIoT systémy jsou velmi významné. Nejvýznamnějším a nejextrémnějším dopadem je selhání zabezpečení v průmyslové výrobě, kdy muže dojít ke ztrátě lidských životů a újmě na zdravý obsluhy strojů. Dalšími dopady jsou výpadky produkce, představující jednu z nejzávažnějších hrozeb, kdy kritické průmyslové procesy, závislé na nepřerušené komunikaci mezi zařízeními, mohou být zastaveny. To vede k přerušení výroby a ekonomickým ztrátám jak z hlediska zastavení produkce, tak z hlediska nenávratného poškození výrobních strojů.

1.5.2. Metody obrany

Kybernetické útoky na IIoT se stávají stále sofistikovanějšími, což vyžaduje vývoj pokročilých metod obrany a minimalizace rizik. Mezi klíčové obranné strategie, které zvyšují odolnost těchto systémů vůči hrozbám, patří techniky využívající pokročilé strojové učení, speciální architektury pro detekci a prevenci útoků a šifrování. Další v tomto odvětví důležitou částí je hardwarové provedení a zabezpečení jednotlivých zařízení.

Hardwarové zabezpečení

Hardwarové zabezpečení hraje klíčovou roli v ochraně zařízení a systémů v prostředí Průmyslového internetu věcí (IIoT). Tato zařízení často operují v náročných prostředích s omezenými zdroji, což zvyšuje jejich zranitelnost vůči různým druhům útoků.

Základním bodem pro zabezpečení na Perception vrstvě je tzv **Hardwarový RoT** (Root of Trust). V praxi jde o co-procesor nebo zabezpečenou část procesoru která zajišťuje bezpečné bootování systému a bezpečné komunikace. Díky tomu zařízení komunikuje jen s certifikovanými uživateli a aplikacemi. Díky tomu se snižuje schopnost hackerů posílat zprávy na zařízení nebo do ekosystémů zařadit vlastní zařízení. Hardwarový RoT disponuje runtime memory, která zajišťuje ochranu dat při načítání požadovaných softwarem do STACK a HEAP. Secure CPU bezpečnostní čip, který tvoří silný základ důvěryhodného RoT. Cryptografic akcelerators slouží k provádění kryptografických operací, tím snižuje spotřebu zařízení a odlehčuje secure CPU. Secure clock je důležitý pro aplikace, které vyžadují důvěryhodný zdroj času. Většinou se jedná o RTC (real time clock obvod), který je napájený z vlastní baterie. Posledním důležitým modulem je True random number generator, který poskytuje vysokou entropii potřebnou pro bezpečnostní funkce. Jako praktický příklad můžeme uvést procesory s architekturou TrustZone u rodiny procesoru ARM, které fungují na principu

s hardwarovým rozdělení procesoru na dvě části, a to na důvěryhodnou (secure world), pro které je základem RoT a nedůvěryhodnou (Normal world). Díky tomu může v důvěryhodné části běžet bezpečný kód s daty a díky tomu provádět šifrování a autentizaci a zajisti bezpečné bootování systému, což výrazně snižuje možnosti hackerských útoků a v Normal World probíhají běžné aplikace.

Trusted Platform Module (TPM) je specializovaný čip, který poskytuje bezpečnostní základ pro zařízení. Tento modul umožňuje bezpečné ukládání kryptografických klíčů, certifikátů a jiných citlivých dat, což zajišťuje ochranu proti neoprávněným přístupům. TPM také podporuje bezpečnost na úrovni autentizace hardwaru a zabezpečení dat. Dále umožňuje generování a správu kryptografických klíčů přímo v čipu, čímž minimalizuje riziko jejich kompromitace během přenosu. Na rozdíl od RoT se jedná o samostatný čip. (InHand Networks 2024)

Hardware Security Modules (HSM) jsou specializovaná zařízení určená k ochraně kryptografických operací. Jsou navržena tak, aby odolávala fyzickým i softwarovým útokům. V prostředí IIoT se HSM často používají k zabezpečení komunikace mezi senzory, akčními členy a centrem správy sítě. Tato zařízení také podporují správu certifikátů, ochranu klíčů a akceleraci šifrovacích procesů, což je nezbytné pro zařízení s omezenými zdroji. (HiveMQ 2024)

Mechanismus Secure Boot (Zabezpečené spuštění) ověřuje legitimitu a integritu softwaru při spouštění zařízení. Zajišťuje, že se systém spustí pouze s důvěryhodným firmwarem, což brání zavedení škodlivého kódu během startu. Tento proces zahrnuje kontrolu digitálních podpisů všech klíčových komponent, čímž eliminuje riziko nahrání neautorizovaného softwaru. (Integra 2025)

Physical Unclonable Function (PUF) využívá unikátní fyzické vlastnosti jednotlivých komponent zařízení ke generování jedinečných identifikátorů. Tato technologie umožňuje autentizaci zařízení bez nutnosti ukládání citlivých dat do nevolatilní paměti, což zvyšuje odolnost vůči útokům. PUF se používá zejména tam, kde je potřeba vysoká míra bezpečnosti s minimálními nároky na výkon zařízení. (Synopsys 2025)

Hardware-Based Encryption (hardwarově akcelerované šifrování) je nezbytné pro ochranu dat přenášených v IIoT. Používá kryptografické algoritmy implementované na hardwarové úrovni, což zajišťuje vysoký výkon a minimální zpoždění při zpracování dat. Tato forma šifrování

umožňuje ochranu citlivých informací i v prostředí s omezenými výpočetními kapacitami. (SHARMA 2024)

Tamper-Resistant Hardware (zařízení odolná proti neoprávněné manipulaci) zahrnují technologie, které detekují pokusy o fyzické narušení a reagují na ně například deaktivací zařízení nebo vymazáním citlivých dat. Tato ochrana je klíčová pro nasazení v průmyslových a kritických aplikacích, kde by fyzická manipulace mohla způsobit vážné narušení provozu. Umožnuje automatickou reakci na útok, čímž minimalizuje riziko poškození a zastavení výroby. (SHARMA 2024)

Edge Computing Security zařízení provádějí část zpracování dat lokálně, což snižuje riziko případného odcizení dat během přenosu. Hardwarové zabezpečení těchto zařízení zahrnuje kryptografické moduly a ochranu paměti, aby byla minimalizována zranitelnost. Díky těmto opatřením jsou data chráněna i v případě přerušení komunikace se vzdálenými servery. (SHARMA 2024)

Pokročilé metody šifrování a blockchain

Použití technologií jako je blockchain pro zajištění integrity dat a šifrování pro ochranu citlivých informací patří mezi klíčové obranné techniky proti kybernetickým hrozbám. V kombinaci s metodami strojového učení, jako jsou klasifikátory (např. Extra Tree, SVM, NB, RF, a Deep Learning), poskytují silnou obranu proti útokům, jako jsou DDoS nebo spoofingové útoky, a zajišťují, že aplikace zůstávají funkční a bezpečné.

Pokročilé metody obrany, jako jsou deep reinforcement learning a real-time monitorování, jsou klíčové pro zajištění bezpečnosti a odolnosti IIoT systémů. Zajištění ochrany těchto systémů vyžaduje komplexní přístup, který zahrnuje nejen technologické inovace, ale i vývoj a implementaci pokročilých analytických a šifrovacích metod, které dokážou čelit stále sofistikovanějším kybernetickým hrozbám. (ZHUKABAYEVA 2025)

Deep Reinforcement Learning (DRL)

Jednou z efektivních metod, jak zvýšit odolnost vůči útokům, je využívání metod hlubokého učení, konkrétně hlubokého posilovaného učení (DRL). Tato technika se ukazuje jako robustní při ochraně energetických systémů před útoky, které se zaměřují na zavádění malých narušení sítě. Systémy řízené DRL mohou detekovat a reagovat na tyto rušivé vlivy v reálném čase, což zlepšuje jejich schopnost obrany a napravení škod. DRL agenti (programy nebo algoritmy)

samostatně interagují s prostředím, provádějí akce a na základě dosažené zpětné vazby se učí optimalizovat své strategie. Cílem je najít akce, které maximalizují celkový zisk, což je v kontextu kybernetické bezpečnosti obvykle maximální ochrana systému před hrozbami, jako jsou útoky, nebo minimalizace zranitelnosti. Hlavními výhodami jsou adaptibilita, automatizace procesu hledání slabých míst v zabezpečení a využívá komplexní modelování pro analýzu síťové komunikace a chování jednotlivých zařízení.

Monitorování v reálném čase

Real-time monitorovací systémy, využívající metody jako je časová logika a analýza anomálií, hrají zásadní roli při detekci a prevenci útoků v energetických sektorech. Tyto systémy sledují síťová data a hledají odchylky od očekávaného chování, což pomáhá včasně identifikovat potenciální hrozby a minimalizovat riziko kybernetických útoků v kritických systémech, jako jsou chytré rozvodné sítě (smart grids) a SCADA systémy.

Zlepšení autentizace

Pro prevenci neoprávněného přístupu a zamezení spoofingovým útokům je kladen velký důraz na posílení autentizačních procesů. Zlepšené autentizace zajišťují, že pouze oprávněné zařízení a uživatelé mohou komunikovat v rámci systému, což významně snižuje riziko zneužití identit nebo neoprávněného přístupu.

2. Hardwarové prostředky IIoT

Průmyslový internet věcí (IIoT) představuje komplexní ekosystém, ve kterém jednotlivá zařízení spolupracují a vytvářejí integrovaný systém pro monitorování, řízení a optimalizaci průmyslových procesů. Zařízení v této oblasti lze rozdělit podle jejich funkce, způsobu připojení, oblastí využití a dalších kritérií. Základními stavebními kameny jsou senzory a akční členy. Senzory měří různé fyzikální veličiny, jako je teplota, tlak, vlhkost, vibrace či hladina, a získávají tak data, která jsou klíčová pro sledování provozního stavu strojů a zařízení. Tyto senzory se dělí na analogové a digitální, přičemž mezi jejich varianty patří i optické, ultrazvukové nebo infračervené senzory. Na druhé straně akční členy umožňují ovládání a regulaci procesů – například otevření nebo zavření ventilu, nastavení polohy motoru či spínání zařízení. Mezi používané komponenty patří elektromagnetické ventily, servomotory, relé nebo i hydraulické a pneumatické mechanismy, které spolupracují na zajištění efektivního řízení průmyslových operací.

Další důležitou součástí IIoT infrastruktury jsou edge zařízení a brány (gatewaye). Tato zařízení se nacházejí na okraji sítě a jejich úkolem je předzpracování a filtrování dat přímo na místě

nasazení. Díky lokální analýze a konverzi komunikačních protokolů edge zařízení snižují zátěž komunikačních sítí a umožňují rychlou reakci na lokální události, což je zásadní zejména v kritických aplikacích. Tyto brány a lokální řídicí jednotky, jako jsou programovatelné logické automaty (PLC) nebo specializované edge servery, zároveň propojují senzorovou vrstvu s centrálními systémy, jako jsou SCADA (Supervisory Control And Data Acquisition) a HMI (Human Machine Interface), které poskytují operátorům přehledné uživatelské rozhraní a umožňují detailní monitorování a řízení procesů.

Pro zajištění spolehlivé komunikace mezi jednotlivými zařízeními a systémy se využívají jak drátová, tak bezdrátová připojení. Drátová řešení, založená především na průmyslovém Ethernetu a jeho variantách (EtherNet/IP, ProfiNet, EtherCAT), poskytují stabilní spojení s nízkou latencí a vysokou odolností vůči rušení. Používané protokoly jako Modbus TCP nebo OPC UA umožňují standardizovanou komunikaci a integraci různých zařízení. Naopak bezdrátová připojení, využívající technologie jako Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT či moderní 5G, nabízejí vysokou flexibilitu instalace a jsou ideální pro monitorování zařízení v těžko přístupných či pohyblivých lokalitách. I když bezdrátová řešení představují řadu výzev, například z hlediska zabezpečení dat nebo optimalizace přenosové kapacity, jejich využití stále roste a otevírá nové možnosti pro mobilní a distribuované aplikace.

IIoT zařízení nacházejí uplatnění v celé řadě průmyslových odvětví a aplikací. Při **prediktivní údržbě**, jejímž cílem je předcházet poruchám a snižovat náklady na odstávky, se využívají senzory měřící vibrace, teplotu či akustické parametry, které pomáhají včas odhalit opotřebení strojních komponent. V oblasti **automatizace** výroby hrají klíčovou roli robotická ramena, CNC stroje, PLC a HMI systémy, které společně zvyšují efektivitu, přesnost a bezpečnost výrobních procesů. **Energetický management** využívá inteligentní elektroměry a senzory spotřeby, což umožňuje optimalizovat energetickou náročnost provozovaných zařízení a **snižovat provozní náklady**. Další oblastí, kde IIoT technologie nacházejí uplatnění, je **logistika a sledování majetku**. Pomocí RFID čteček a GPS trackerů je možné efektivně sledovat pohyb zboží a optimalizovat dodavatelské řetězce. Stejně tak **environment monitoring** využívá senzory pro měření kvality ovzduší, hladiny hluku nebo emisí, což přispívá k ochraně životního prostředí a lepšímu městskému plánování.

Bezpečnost a odolnost jsou dalšími klíčovými aspekty při implementaci IIoT řešení. Kybernetická bezpečnost vyžaduje šifrování dat, autentizaci, segmentaci sítí a pravidelné aktualizace softwaru, aby byla komunikace mezi zařízeními chráněna před neoprávněným

přístupem a kybernetickými útoky. Kromě toho je důležité, aby zařízení byla fyzicky odolná vůči náročným podmínkám, jako jsou vysoké teploty, vibrace či prach. Certifikace dle standardů, například IP nebo NEMA, zaručují, že zařízení splňují přísné požadavky a jsou schopna fungovat i v extrémních podmínkách.

Moderní IIoT systémy jsou obvykle postaveny na vícevrstvé architektuře, která zahrnuje řadu vrstev začínajících přímo u zařízení, přes edge computing a komunikační vrstvu až po cloudová řešení a aplikační vrstvy. Tato architektura umožňuje efektivní škálovatelnost, vysokou míru bezpečnosti a flexibilitu, jelikož jednotlivé vrstvy spolupracují na zpracování, ukládání a analýze dat. Data získaná ze senzorů jsou nejprve předzpracována na okraji sítě a poté přenesena do centrálních systémů, kde jsou dále analyzována pomocí pokročilých algoritmů, často včetně umělé inteligence a strojového učení. Výsledkem je optimalizace výrobních a energetických procesů, včasné odhalování potenciálních poruch a celkové zlepšení provozní spolehlivosti.

S pokračujícím vývojem technologií se do oblasti IIoT stále více integrují nové trendy, jako je například rozvoj bezdrátových sítí s nízkou latencí prostřednictvím 5G, nebo snaha o standardizaci a interoperabilitu zařízení prostřednictvím protokolů jako OPC UA. Integrace umělé inteligence a strojového učení dále umožňuje sofistikovanější prediktivní údržbu a automatizaci rozhodovacích procesů, čímž se posouvá efektivita průmyslových procesů na novou úroveň. V neposlední řadě se klade stále větší důraz na robustní kyberbezpečnost a ochranu kritické infrastruktury, což je zásadní v době, kdy počet propojených zařízení roste exponenciálně.

Celkově lze říci, že průmyslový internet věcí představuje klíčovou technologii pro moderní průmysl, neboť integrací senzorů, akčních členů, edge zařízení, komunikačních sítí a centrálních analytických systémů umožňuje efektivní monitorování, řízení a optimalizaci výrobních a dalších procesů. Tato komplexní integrace vede ke zvýšení bezpečnosti, snížení provozních nákladů a zlepšení celkové spolehlivosti provozovaných zařízení, což je nezbytné pro udržení konkurenceschopnosti v rychle se měnícím technologickém prostředí. Z dat ze serveru automation.com a loriot.io vychází, že k roku 2024 je v nějaké formě IIoT implementováno v téměř 75% firmách zabývajícími se průmyslovou výrobou.

2.1.1. Webový programovatelný ovladač s podporou IoT

Webový programovatelný ovladač umožňuje integraci s cloudovými systémy IIoT pomocí protokolu MQTT. Tento ovladač funguje jako MQTT klient, který zajišťuje komunikaci s lokálními i cloudovými brokery MQTT. Mezi jeho klíčové funkce patří publikování dat, sběr dat od externích brokerů MQTT a správa zařízení připojených k ovladači pomocí příkazů MQTT. Tímto způsobem může plnit roli brány mezi zařízeními a cloudovými systémy.

WISE-5231 od ICP DAS

WISE-5231 je pokročilý ovladač od společnosti ICP DAS, vybavený širokou škálou funkcí a technických specifikací. Zařízení obsahuje 32bitový ARM procesor a slot pro microSD kartu s podporou až 32 GB paměti. Pro komunikaci nabízí jeden Ethernet port s rychlostí 10/100/1000 Mbps, dva porty RS-232 a dva porty RS-485. Podporuje řadu rozšiřujících desek a vzdálených I/O modulů, jako jsou I-7000, M-7000, (P)ET-7000, WISE-7000 a WF-2000, stejně jako zařízení třetích stran s protokolem Modbus RTU Slave. Integrovaná logika IF-THEN-ELSE umožňuje pokročilé automatizační procesy. Zařízení obsahuje hodiny reálného času (RTC) a podporuje protokoly Modbus RTU/TCP, DCON, SNMP v2c a CGI. Jeho konstrukce umožňuje provoz v náročných podmínkách, s rozsahem provozních teplot od -25 do +75 °C a širokým rozsahem vstupního napájení. (Ipc2U 2024)

Moduly vzdáleného vstupu/výstupu

Moduly řady WISE-4000 od společnosti Advantech umožňují shromažďování dat ze senzorů a vstupních a výstupních kanálů. Tato data lze dále přenášet do nadřazených systémů, jako jsou řídicí systémy nebo SCADA. Modely s LAN připojením disponují podporou protokolů TCP/IP, UDP, HTTP, HTTPS, DHCP, ARP, SNTP a Modbus TCP. Dále nabízejí RESTful Web API ve formátu JSON, možnost záznamu dat s časovým razítkem a jejich ukládání do služeb, jako je Dropbox nebo Baidu. Provoz je možný v teplotách od -40 do +70 °C. Modely s Wi-Fi připojením podporují standardy 802.11b/g/n, režimy AP i infrastruktury a nabízejí zabezpečení WPA2. Obsahují odstranitelnou anténu a mohou pracovat v rozmezí teplot od -25 do +70 °C. (Ipc2U 2024)

Série MQ-7000 od ICP DAS

Diskrétní vstupní a výstupní moduly řady MQ-7000 mají zabudovaného klienta MQTT, který umožňuje přenos a správu stavů kanálů pomocí tohoto protokolu. Moduly nabízejí osm diskrétních vstupů, které lze nakonfigurovat jako suché kontakty nebo externí napájecí kontakty, a osm diskrétních výstupů s kolektorovým zapojením NPN/PNP. Podporují protokol

MQTT ve verzi 3.1.1, disponují dvojitým hlídacím časovačem a vestavěným webovým rozhraním. Kovové pouzdro zajišťuje odolnost a zařízení může fungovat v teplotách od -25 do +75 °C. Tato řešení nabízejí spolehlivost a flexibilitu pro široké spektrum průmyslových aplikací. (Ipc2U 2024)

2.1.2. IIoT brány

IoT brány jsou navrženy pro sběr dat z koncových zařízení pomocí průmyslových protokolů a jejich následný přenos do cloudu, kde mohou být data dále analyzována a monitorována.

UA-5231 od ICP-DAS

UA-5231 je IIoT brána vybavená procesorem s architekturou RISC AM3352 o frekvenci 720 MHz a operačním systémem Linux 3.2.14. Toto zařízení umožňuje získávat a zpracovávat informace ze vzdálených zařízení připojených přes ethernetové nebo sériové porty, dále IIoT servery a PID řízení. Vestavěný OPC UA server a podpora protokolu MQTT usnadňují integraci s různými průmyslovými protokoly. Díky nízké spotřebě energie a kompaktnímu provedení je UA-5231 vhodná pro instalaci i v omezených prostorách. (Ipc2U 2024)

MXE-101i od ADLink

MXE-101i je vestavěný počítač s funkcí IIoT brány, založený na procesoru Intel Quark SoC X1021. Operačním systémem zařízení je Wind River, který podporuje Intel IoT Gateway. Software Edge Pro umožňuje efektivní integraci zařízení s cloudovým systémem a zrychluje vývoj aplikací. (Ipc2U 2024)

NIO-50 od NEXCOM

NIO-50 je brána určená pro připojení zařízení podporujících protokoly Modbus TCP/IP, Modbus RTU a Modbus ASCII. Shromážděná data jsou přenášena do cloudových služeb prostřednictvím Wi-Fi nebo LAN pomocí protokolu MQTT pro jejich další analýzu. (Ipc2U 2024)

NIO-100 series od NEXCOM

Brány NIO-100 sbírají data z koncových zařízení prostřednictvím rozhraní RS-232/485 nebo DIO a přenášejí je do cloudu pomocí 3G, Wi-Fi nebo Ethernetu. Zařízení obsahuje systém Node-RED, který umožňuje snadné nastavení chování brány prostřednictvím konfigurace a propojení existujících funkčních modulů. Uživatel má navíc možnost vytvořit vlastní funkční jednotky. (Ipc2U 2024)

Série UC-8100-LX-CG od MOXA

Vestavěný počítač ze série UC-8100-LX-CG využívá software MOXA ThingsPro, který podporuje přenos dat z terénních zařízení do cloudu. Tento software rozšiřuje možnosti zařízení o nástroje pro správu a přenos dat v rámci IoT ekosystému. (Ipc2U 2024)

SIMATIC CC712 a CC716

Zařízení SIMATIC CC712 je průmyslová IoT brána od společnosti Siemens, navržená pro připojení jednoho SIMATIC S7-300 nebo S7-400 řídicího systému prostřednictvím průmyslového Ethernetu pomocí S7 protokolu. Podporuje cloudové platformy jako Siemens MindSphere, IBM Cloud, Microsoft Azure IoT Hub, Oracle IoT a AWS IoT Core, využívající protokoly MQTT a HTTP (REST API) pro komunikaci. Zařízení umožňuje standardizovanou výměnu dat pomocí OPC UA protokolu, což usnadňuje integraci s MES systémy, HMI a dalšími řídicími jednotkami třetích stran. Zařízení CC716 umožnuje připojení až 7 PLC SIMATIC S7.

2.1.3. Platformy IIoT

Počítačové platformy pro Internet věcí zajišťují výměnu dat mezi koncovými zařízeními a cloudovým úložištěm. Platformy IoT podporují různé typy komunikace a lze je snadno aplikovat ve výrobních zařízeních, v průmyslových oblastech, v dozorových systémech a automatizačních aplikacích.

SIEMENS SCALANCE LPE

SCALANCE LPE (Local Processing Engine) je kompaktní a robustní zařízení od společnosti Siemens, navržené pro lokální zpracování dat v průmyslových aplikacích. Díky výkonnému CPU umožňuje SCALANCE LPE sběr a analýzu dat přímo v místě jejich vzniku, což zajišťuje rychlé a efektivní zpracování bez nutnosti odesílání dat do vzdálených serverů nebo cloudových platforem. Tato vlastnost je klíčová pro aplikace vyžadující nízkou latenci a vysokou spolehlivost, jako je prediktivní údržba, monitorování stavu zařízení nebo detekce anomálií v reálném čase.

SCALANCE LPE podporuje běh více aplikací současně, například pro prediktivní údržbu nebo detekci anomálií, a to v bezpečném prostředí OT (Operational Technology). Díky podpoře kontejnerové technologie Docker lze na zařízení nasazovat různé softwarové služby, což zvyšuje flexibilitu a škálovatelnost řešení. Integrace s existující síťovou infrastrukturou je usnadněna díky různým možnostem připojení a monitorování průmyslových sítí, aniž by byla ohrožena jejich integrita a bezpečnost díky implementaci zero-trust přístupu. Další metodou

ochrany dat je softwaru Guardian Remote Collector vyvinutý společnosti Nozomi Networks, který umožňuje pasivní detekci anomálií a monitorování průmyslových sítí v reálném čase, aniž by byla narušena provozní kontinuita nebo přidána další složitost do stávající infrastruktury. (Siemens 2024)

Série tBOX300 od AXIOMTEK

Vestavěné počítače tBOX pro automobilovou a železniční dopravu jsou schopné pracovat při teplotě -40 °C. Jsou odolné proti vibracím a poklesu napětí. (Ipc2U 2024)

eBOX560-300-FL od AXIOMTEK

Počítače s pevným krytem s anti-vibračními vlastnostmi a ochranou před otřesy. Tyto počítače podléhají rozsáhlému testování a jsou charakteristické vysokou odolností proti chybám. (Ipc2U 2024)

ICO300 od AXIOMTEK

Spolehlivé počítače Axiomtek s dokonalým poměrem kvality a ceny využívají produktivní a energeticky účinné procesory Intel Atom a optimální sadu vstupních/výstupních rozhraní. (Ipc2U 2024)

Série rBOX od AXIOMTEK

Hliníkový kryt, IP30, rozšířený teplotní rozsah, izolace vstupu/výstupu, hojnost napájecích zdrojů a shoda s normou EN/IEC umožňují uživateli úspěšně provozovat zařízení řady rBOX v náročných provozních podmínkách. (Ipc2U 2024)

IFB122 od AXIOMTEK

Systém bez ventilátoru, založený na procesoru iMX6UL RISC od společnosti Axiomtek. Funkce počítače obsahují základní rozhraní pro připojení počítače k okolnímu světu. Zařízení se vyznačuje výjimečnou cenou. (Ipc2U 2024)

2.1.4. Koncová zařízení

Mezi koncová zařízení jsou řazeny taková zařízení, která přímo interagují s prostředí a zprostředkovávají tak sběr dat, která předávají vyšší vrstvě ke zpracování.

SIMATIC S7-1200 a S7-1500

Nejnovější modely programovatelných logických automatů (PLC) Siemens řady SIMATIC S7 kombinují vysoký výpočetní výkon s pokročilou komunikační konektivitou, což umožňuje jejich efektivní nasazení v prostředí Průmyslového internetu věcí (IIoT). Model SIMATIC S7-

1500 nabízí výkonný procesor, rozšířenou paměť, rychlou interní sběrnici a pokročilé diagnostické funkce, včetně kybernetického zabezpečení. Pro menší aplikace je určen SIMATIC S7-1200, který integruje vstupy a výstupy, podporuje analogové i digitální signály a je optimalizován pro nízkou spotřebu energie. Oba modely umožňují snadnou škálovatelnost a flexibilní integraci do průmyslových prostředí díky modulárnímu designu.

Klíčovou vlastností těchto PLC je široká podpora průmyslových komunikačních protokolů, které umožňují efektivní výměnu dat a propojení s IT infrastrukturou. Mezi nejdůležitější patří Profinet a Profibus pro připojení k decentralizovaným zařízením, OPC UA pro standardizovanou výměnu dat, Modbus TCP pro komunikaci se senzory a MQTT či REST API pro integraci s cloudovými službami, včetně Siemens MindSphere nebo AWS IoT Core. Díky těmto funkcím jsou PLC SIMATIC S7-1500 a S7-1200 plně připraveny pro implementaci Průmyslu 4.0, kde hraje klíčovou roli vzdálené monitorování, adaptivní řízení procesů a prediktivní údržba. (Siemens B 2024)

Měřiče CO, CO2, teploty a vlhkosti

Měřiče CO, CO2, teploty a vlhkosti s podporou protokolu MQTT. Data z měřicího zařízení lze získat v reálném čase pomocí svobodné softwarové aplikace Windows nebo aplikace pro iOS nebo Android. (Ipc2U 2024)

Série DL-300 od ICP-DAS

Modul pro měření teploty, vlhkosti, koncentrace CO s vizualizací. (Ipc2U 2024)

Tabulka 1 srovnání dostupných zařízení

Zařízení	Typ zařízení	Hlavní funkce	Protokoly	Komunikace	Provozní teploty
WISE-5231 (ICP DAS)	Webový programovatelný ovladač	Integrace s cloudovými systémy	MQTT, Modbus RTU/TCP, DCON, SNMP, CGI	Ethernet (10/100/1000 Mbps), RS-232, RS-485	-25 °C až +75 °C
Moduly WISE-4000 (Advantech)	Moduly vzdáleného I/O	Shromažďování dat SCADA	TCP/IP, UDP, HTTP, HTTPS, Modbus TCP	LAN, Wi-Fi (802.11b/g/n)	-40 °C až +70 °C

Série MQ-7000 (ICP DAS)	Diskrétní vstupní/výstupní moduly	vstupů/výstupů kontakty	MQTT 3.1.1	Ethernet, Web rozhraní	-25 °C až +75 °C
UA-5231 (ICP-DAS)	IIoT brána	Vstupů/výstupů kontakty	OPC UA, MQTT	Ethernet, sériové porty	-
MXE-101i (ADLink)	IIoT brána	Propojení koncových zařízení zpracování dat	-	Ethernet, Wi-Fi, 3G	-
NIO-50 (NEXCOM)	IIoT brána	Propojení koncových zařízení	Modbus TCP/IP, Modbus RTU, MQTT	Wi-Fi, LAN	-25 °C až +70 °C
NIO-100 series (NEXCOM)	IIoT brána	Propojení koncových zařízení zpracování dat	Modbus, MQTT, RS-232/485	Wi-Fi, 3G, Ethernet	-
UC-8100-LX-CG (MOXA)	IIoT brána	Zpráva IoT systému, přenos dat	MQTT, SNMP, Modbus	Ethernet, Wi-Fi	-25 °C až +70 °C
Série tBOX300 (AXIOMTEK)	Počítače pro IIoT	Průmyslové PC s integraci IIoT	-	-	-40 °C až +70 °C
eBOX560-300-FL (AXIOMTEK)	Počítače pro IIoT	Průmyslové PC s integraci IIoT odolnost vůči vybracím	-	-	-40 °C až +70 °C
ICO300 (AXIOMTEK)	Počítače pro IIoT	Průmyslové PC s integraci IIoT energeticky úsporný	-	-	-
rBOX (AXIOMTEK)	Počítače pro IIoT	Průmyslové PC s integraci IIoT , shoda s normami EN/IEC.	-	-	-40 °C až +70 °C
IFB122 (AXIOMTEK)	Počítače pro IIoT	Průmyslové PC s integraci IIoT cenová dostupnost	-	-	-
DL-300 (ICP-DAS)	Měřiče CO, CO2, teploty a vlhkosti	Měření (CO, CO2, teplota, vlhkost)	MQTT	Wi-Fi, LAN	-25 °C až +75 °C

3. Návrh a realizace monitorovacího systému

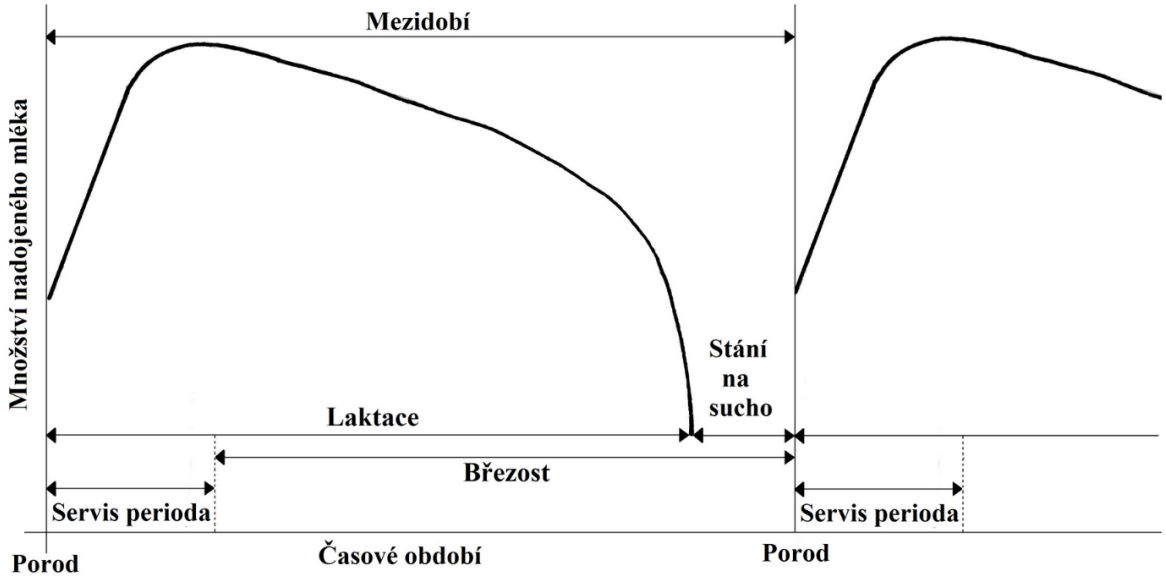
V následující kapitola obsahuje rozbor a návrh hardwarové jednotky pro monitorování chodu technologického procesu. V rámci, kterého je neinvazivně měřen příkon monitorovaného zařízení, teplota zařízení a teplota zpracovávaného media. Zařízení dále zpracovává získaná data a přístup k těmto zpracovaným datům je zprostředkován webovým serverem implementovaným v rámci monitorovací jednotky.

Motivací pro vývoj systému pro monitoring procesu chlazení mléka je zvýšení standardu a spolehlivosti stávající mechanicky dobře fungující technologie na systém s vyšší spolehlivostí. Díky podrobným záznamům o provádění procesu je možno optimalizovat proces, tak aby byla zvýšena kvalita finálního produktu, což vede k vyššímu finančnímu ohodnocení produktu. A dále včasné detekci selhání stávajícího systému a možnosti včas selhání řešit a zachránit možnou finanční ztrátu při degradaci produktu.

3.1. Monitorovaná technologie

V zemědělském provozu s tržní produkcí mléka jsou dva klíčové technologické procesy, které jsou prováděny každodenně a nemohou být v žádném případě ve stavu poruchy déle než 24 h. Těmito procesy jsou dojení a chlazení mléka. Při poruše dojícího zařízení a zpoždění procesu dojení vzniká dlouhodobá nevratná finanční ztráta vlivem biologických pochodů skotu.

U skotu s tržní produkcí mléka je definována tzv. laktační křivka, která zobrazuje množní produkovaného mléka v závislosti na čase od porodu. Křivku je možné rozdělit na úseky *rozdoj* bezprostředně po porodu, kdy produkce mléka strmě stoupá. Poté *vrchol laktace*, kdy skot produkuje nejvíce mléka a následně *postupné snižování produkce* až k *odstavení* a *stání na sucho*, kdy dochází k regeneraci přípravě na další laktační cyklus (obr.3).



Obrázek 3 Laktační křivka skotu (kzv.zf.jcu.cz 2017)

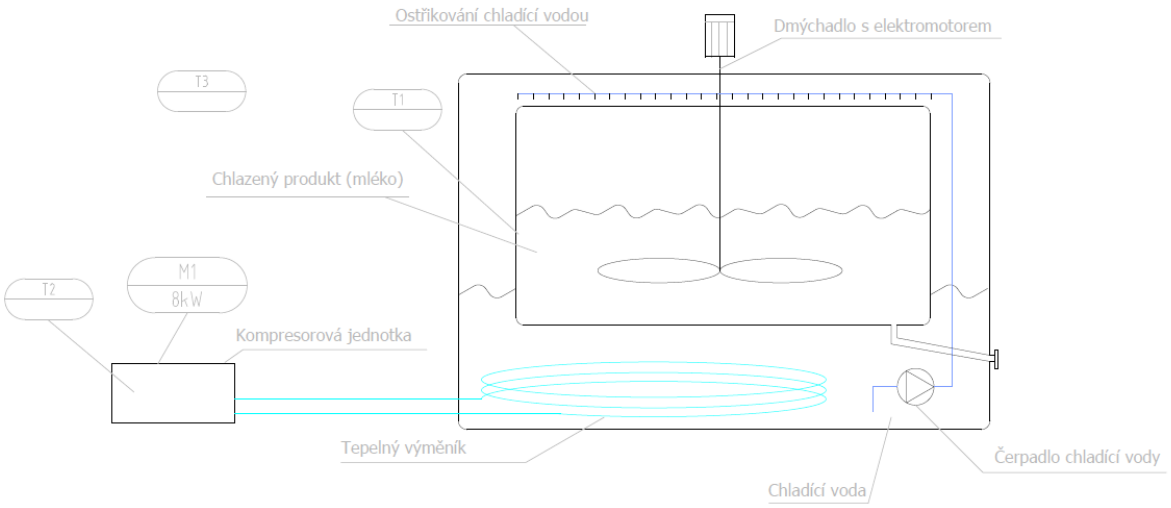
Při nedodržení pravidelného cyklu dojení například při poruše dojícího zařízení dochází k velmi významnému a trvalému poklesu množství nadojeného mléka, což má velký vliv na ekonomiku celého chovu. Pokud by došlo ke zpoždění dojícího procesu o 24-48 hodin mělo by to za následek 20% – 40% pokles celkové produkce a vysoké riziko vniku mastitidy a dalších zdravotních problémů skotu. Z toho vyplívají vysoké nároky na spolehlivost celého technického zařízení.

Druhý kritický proces prováděný v zemědělském provozu s tržní produkcí mléka je proces chlazení mléka. Mléko má při nadojení teplotu 37,5 – 39 °C a je třeba tuto teplotu rychle snížit na teplotu pod 4 °C z důvodu uchování mléka v dobré kvalitě. Při dlouhodobé teplotě na 7 °C dochází k rychlému množení baterii, což vede k rapidnímu snižování kvality. Při poruše chladícího zařízení bez včasné detekce dochází ke kysnutí mléka (znehodnocení vyráběného produktu) a velké jednorázové finanční ztrátě.

3.1.1. Systém chlazení surového mléka

Chladicí jednotka PACO 2500 l od Pacovských strojíren je navržena pro efektivní a hygienické skladování mléka na farmách a mlékárenských provozech. Zajišťuje rychlé zchlazení mléka po nadojení a udržování jeho teploty tak, aby nedocházelo k růstu a množení mikroorganismů. Chladící tank je dvouplášťové konstrukce z důvodu efektivního chlazení mléka a tvrdým hygienickým standardům. Hliníkový tank o objemu 2500 l s dmýchadlem pro chlazené medium (mléko) uzavřený v hliníkovém izolovaném plášti pomocí polyuretanové pěny. V prostoru mezi

plášti se nachází chladící kapalina (chladící voda) ochlazována pomocí tepelného výměníku kompresorové jednotky. V meziplášťovém prostoru je dále instalováno čerpadlo pro distribuci chladící vody na stěny vnitřního tanku, aby docházelo k rovnoměrnému ochlazování celého objemu chladícího tanku. Chladící výkon je dimenzovaný tak, aby dokázal zchladit celý objem nádrže s mlékem o teplotě 35 °C na teplotu 4 °C v časovém rozmezí 2 – 3 h. Pro dvoustavovou regulaci chlazení je vyžito měření teploty chlazeného média a pro regulaci chladící jednotky je chladící výměník vybaven námrazovými čidly a termostatem (obr.4). Ve schématu jsou označeny měřené veličiny teploty T1-T3 a odebíraný proud na M1.



Obrázek 4 Technologie chlazení

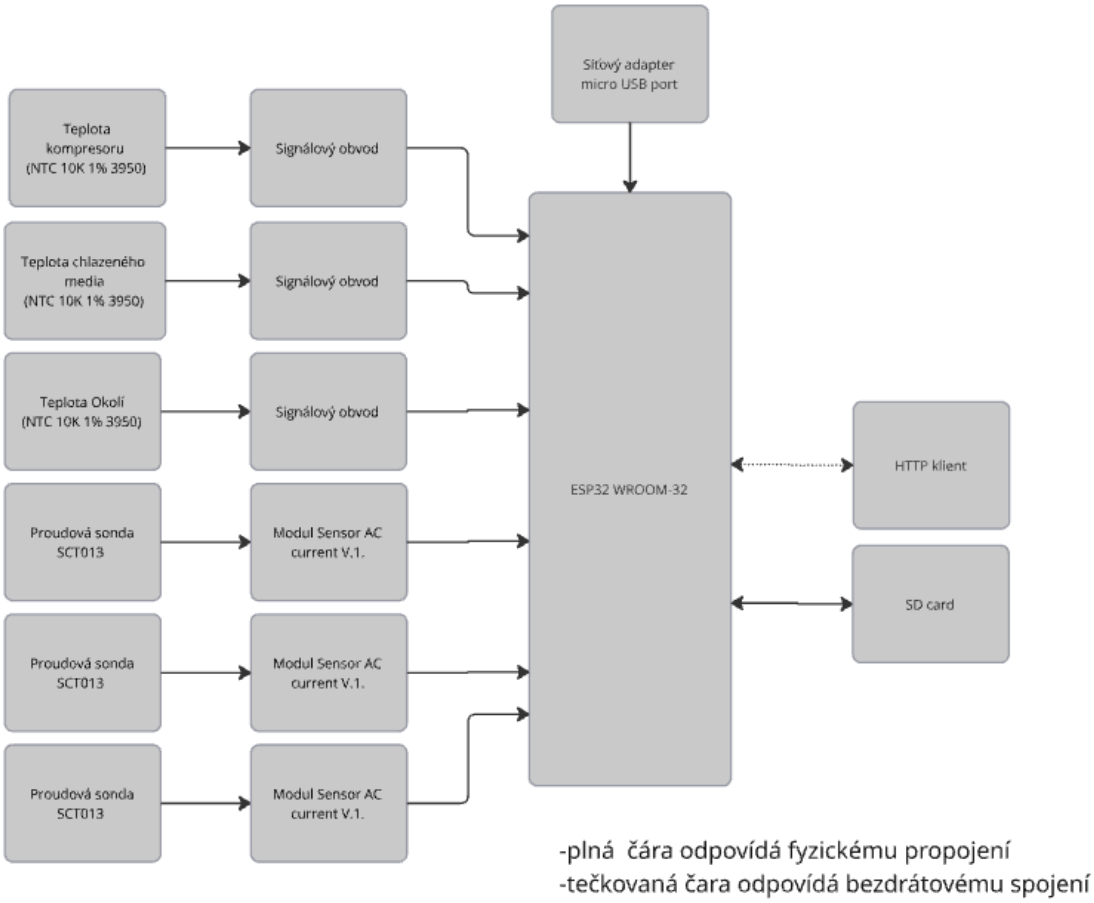
3.1.2. Vývěva dojícího zařízení

Pro proces dojení je kritickým prvkem vývěva vyvíjející podtlak pro dojící ustrojí v prostorách dojírny. Vývěva je poháněna elektromotorem pomocí řemenového převodu. Pro sledování spolehlivého chodu je sledován příkon a teplota elektromotoru jakožto kritického prvku technologie.

3.2.Hardwarové požadavky

Tabulka 2Parametry zařízení

Provozní teplota (okolí)	0 °C až 40 °C
Měření odebíraného proudu (Měřený příkon)	Do 20 A
Měření teploty chladícího zařízení	0 °C až 70 °C
Měření teploty chlazeného media	0 °C až 40 °C
Měření teploty okolí	0 °C až 40 °C



Obrázek 5 Blokové schéma zařízení

3.3. Použité hardwarové prostředky

Pro navrhované zařízení byla zvolena vývojová deska s procesorem ESP32, protože disponuje wifi modulem, kryptografickým hardwarem pro zajištění bezpečnosti a odpovídá požadavkům IoT zařízení na malou spotřebu energie.

3.3.1. ESP32 WROOM A ESP32 S3

Procesor čínské firmy Espressif Systems se sídlem v Šanghaji sestavená na TSMC low-Power 40nm technologii. Tento procesor disponuje 2,4Ghz Wifi a Bluethooth modulem, kryptografickým hardwarovým akcelerátorem, RTC, 34 programovatelnými I/O, PWM a 12-bitový ADC na principu postupné aproximace signálu. Podporuje základní komunikační protokoly od I2C po UART. (Espressif 2024)

ESP32 je výkonný a flexibilní mikrokontrolér, který je široce využíván v oblasti IoT (Internet věcí) a IIoT (Průmyslový internet věcí). Tento čip kombinuje vysoký výpočetní výkon, nízkou spotřebu energie a pokročilé funkce připojení, což z něj činí ideální řešení pro širokou škálu aplikací. (Espressif 2024)

Hardwarové vlastnosti ESP32

ESP32 je vybaven dvoujádrovým procesorem Tensilica Xtensa LX6, který pracuje na frekvenci až 240 MHz, a nabízí až 520 kB SRAM. Čip podporuje více druhů připojení, včetně:**Wi-Fi** (802.11 b/g/n) pro rychlé bezdrátové připojení a **Bluetooth** (včetně BLE - Bluetooth Low Energy) pro nízkoenergetickou komunikaci. (Espressif 2024)

Díky těmto vlastnostem je ESP32 schopno fungovat jako samostatné zařízení nebo jako součást větších systémů. Navíc je vybaveno řadou periferií, jako jsou UART, SPI, I2C, ADC, DAC, PWM a další, což umožňuje snadné propojení s různými senzory, akčními členy a dalšími zařízeními. (Espressif 2024)

Wi-Fi modul integrovaný v ESP32 je komplexní systém skládající se z několika klíčových komponent, které společně zajišťují bezdrátovou komunikaci se standardem 802.11 b/g/n, což umožnuje komunikaci rychlostí až 150Mbps. RF transceiver v ESP32 je zodpovědný za vysílání a příjem rádiových signálů v pásmu 2,4 GHz. Tato komponenta zahrnuje RF přepínač, řídí směr signálu mezi vysílačem a přijímačem, RF balun transformující nesymetrický signál na symetrický a naopak, což je důležité pro správnou funkci antény, výkonový zesilovač (Power Amplifier), zvyšuje sílu vysílaného signálu pro dosažení požadovaného dosahu a anténový zesilovač (Low Noise Amplifier, LNA) zesiluje přijatý signál s minimálním přidáním šumu,

což zlepšuje citlivost přijímač. Tyto komponenty společně umožňují efektivní bezdrátovou komunikaci v pásmu 2,4 GHz.

Baseband procesor zpracovává základní pásmo signálu, což zahrnuje modulaci a demodulaci dat. Tato část systému převádí digitální data na analogové signály vhodné pro vysílání a naopak. Zahrnuje také funkce pro kódování a dekódování signálů, což je nezbytné pro správnou komunikaci v rámci Wi-Fi protokolu.

MAC (Media Access Control) vrstva řídí přístup k bezdrátovému médiu a zajišťuje správu datových rámců. V ESP32 je implementována podpora pro agregaci MAC Protocol Data Unit (AMPDU), což umožňuje zvýšení propustnosti Wi-Fi přenosem více rámců v jednom přenosu. Tato funkce je důležitá pro efektivní využití šířky pásma a zlepšení celkového výkonu sítě.

ESP32 moduly mohou být vybaveny různými typy antén. Některé moduly jsou vybaveny Integrovaná PCB anténa, jako například ESP32-S2, obsahuje vestavěnou anténu přímo na desce plošných spojů. Tato konstrukce šetří místo a zjednodušuje design zařízení.

Jiné moduly vybavené konektorem pro externí anténu umožňují připojení externí antény přes konektor, což poskytuje flexibilitu při optimalizaci signálu pro specifické aplikace nebo prostředí.

Dalí možností připojení je Bluetooth, i když se obvykle nevyužívá pro webové servery, může být užitečné pro připojení s jinými zařízeními v rámci IoT a IIoT ekosystému.

Wi-Fi modul v ESP32 nabízí širokou škálu funkcí, které umožňují flexibilní a efektivní bezdrátovou komunikaci. Pro komunikaci jsou k dispozici dva hlavní režimy provozu, a to Station Mode (STA), kdy se ESP připojuje k existující Wi-Fi síti jako klient. Tento režim je běžně používán pro připojení zařízení k domácímu routeru nebo přístupovému bodu a režim Access Point Mode (AP), kdy ESP funguje jako přístupový bod, ke kterému se mohou připojit jiná zařízení. Tento režim je užitečný pro vytváření lokálních sítí bez potřeby externí infrastruktury. Dual Mode (STA+AP) umožnuje ESP současně fungovat jako klient i přístupový bod, což umožňuje složitější topologie sítí a aplikace, které vyžadují obě role současně.

Wi-Fi modul podporuje moderní bezpečnostní standardy, včetně WPA/WPA2, zajišťující bezpečnou komunikaci v bezdrátových sítích. V rámci sítové komunikace je integrován TCP/IP stack umožňující ESP32 komunikovat přes standardní internetové protokoly, což usnadňuje

integraci s webovými službami a dalšími síťovými aplikacemi. Síťová konektivita je klíčová pro realizaci webového serveru. (Espressif 2024)

Výhody ESP32 v IIoT aplikacích

ESP32 představuje ideální řešení pro mnoho IIoT aplikací díky kombinaci nízké spotřeby energie, vysoké konektivity, flexibility a cenové dostupnosti. Díky podpoře různých režimů nízké spotřeby energie je ESP32 ideální pro zařízení napájená z baterií, například senzory nebo monitorovací zařízení ve vzdálených lokalitách. Integrované Wi-Fi a Bluetooth umožňují snadné připojení k průmyslovým sítím a cloudovým platformám, což zajišťuje efektivní analýzu dat a vzdálené řízení. Podpora různých komunikačních protokolů a široká nabídka periferií poskytuje vysokou flexibilitu, která umožňuje nasazení ESP32 v mnoha scénářích, jako je prediktivní údržba nebo monitorování výrobních procesů. Cenová dostupnost ESP32 ve srovnání s jinými průmyslovými mikrokontroléry z něj činí atraktivní volbu pro velkoobjemové aplikace, což umožňuje výrazné snížení nákladů na implementaci IoT systémů.

ESP32 může být využito v různých aplikacích v průmyslové automatizaci. V oblasti monitorování stavu zařízení lze integrovat senzory pro sledování vibrací, teploty nebo spotřeby energie, které poskytují cenná data pro analýzu stavu strojů. Díky nízké latenci a vysoké spolehlivosti může sloužit i jako řídicí jednotka pro řízení menších automatizačních procesů na výrobních linkách. Kromě toho je schopné provádět prediktivní údržbu – shromažďováním dat ze senzorů, dokáže předvídat potenciální problémy, což umožňuje jejich včasné řešení před samotnou poruchou. Využití edge computingu pak znamená, že ESP32 dokáže zpracovávat data přímo na místě, čímž minimalizuje množství dat odesílaných do cloudu a urychluje reakční dobu celého systému.

Podpora vývoje a ekosystém

ESP32 je podporováno širokou komunitou vývojářů a nabízí kompatibilitu s různými vývojovými prostředími, jako jsou Arduino IDE, PlatformIO nebo Espressif IDF (IoT Development Framework). K dispozici je také rozsáhlá dokumentace a knihovny, které usnadňují implementaci pokročilých funkcí.

Omezení

Přestože je ESP32 velmi schopný mikrokontrolér, existují určitá omezení, která je třeba zvážit při jeho nasazení v průmyslových aplikacích: **Omezený počet GPIO pinů:** Pro aplikace vyžadující připojení velkého množství periferií může být počet dostupných GPIO pinů

nedostatečný. **Odolnost vůči prostředí:** Standardní verze ESP32 není navržena pro extrémní průmyslové podmínky, ale existují varianty s vyšší odolností.

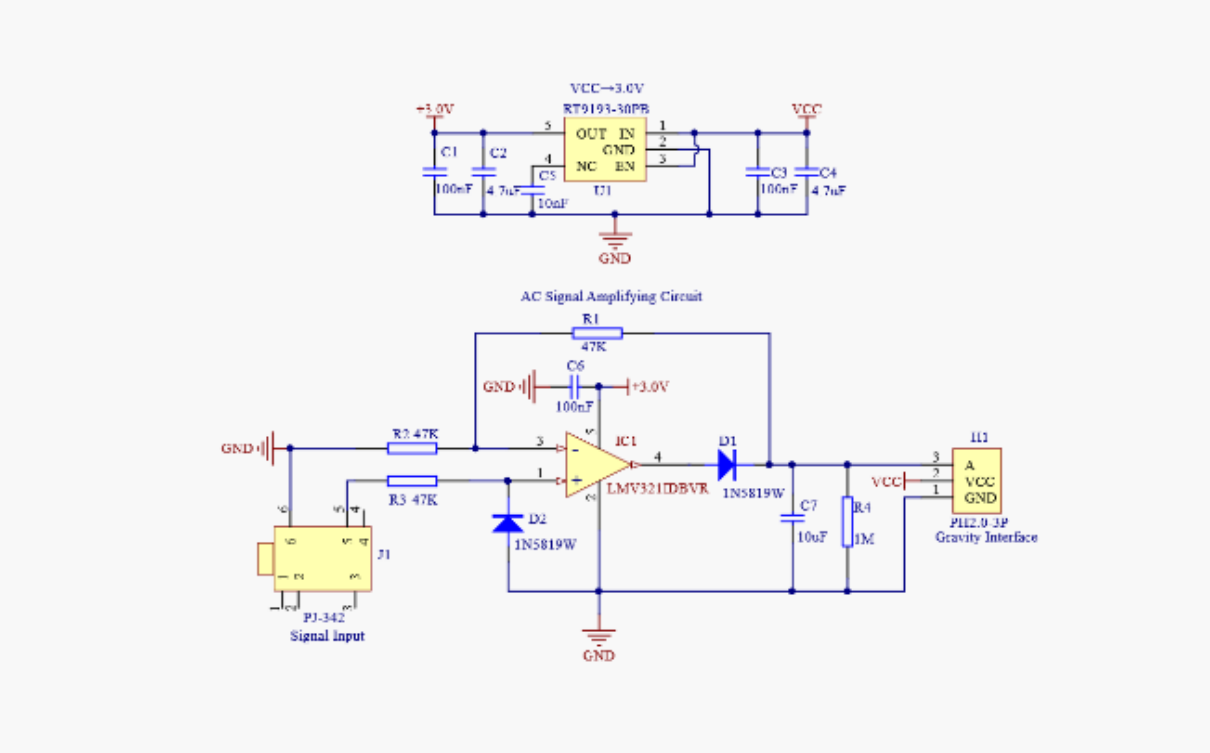
3.3.2. Proudová sonda SCT-013-015

Proudový transformátor SCT013 s děleným jádrem(Split-core) je určen pro neinvazivní měření střídavého proudu s výstupním napětím 0,333 při protékajícím proudu v měřeném vodiči 15 A. Zařízení je vybaveno vestavěným vzorkovacím rezistorem a dodává se s 1metrovým kabelem zakončeným standardním 3,5mm třípólovým konektorem. Patentovaný design (číslo patentu ZL 2015 3 0060067.X) zajišťuje vysokou spolehlivost a přesnost měření, přičemž zařízení podporuje frekvenční rozsah 50 Hz až 1 kHz a pracuje při napětí do 660 V. Přesnost měření je 1 % a linearita rovněž dosahuje 1 %. Konstrukce umožňuje zavěšenou montáž, přičemž mechanické rozměry jsou 34 × 23,5 × 31 mm a průměr otvoru pro primární vinutí činí 13 mm. Provozní teplota transformátoru se pohybuje v rozmezí od -25 °C do +70 °C a skladovací teplota od -30 °C do +90 °C. Zařízení je navrženo tak, aby splňovalo požadavky na bezpečnost s elektrickou pevností 3,5 kV při 50 Hz po dobu jedné minuty. Díky snadné montáži a vysoké přesnosti nachází tento transformátor uplatnění v průmyslových a komerčních aplikacích, jako je monitorování spotřeby energie, řízení strojního zařízení a měření elektrických veličin v IoT systémech (obr.6).

Obrázek 6 Proudová sonda SCT-015

Vzhledem k sinusovému výstupnímu signálu ze sondy je nutné provést úpravu a zpracování signálu. Jednou z variant řešení je prostřednictvím napěťového děliče signál přizpůsobit

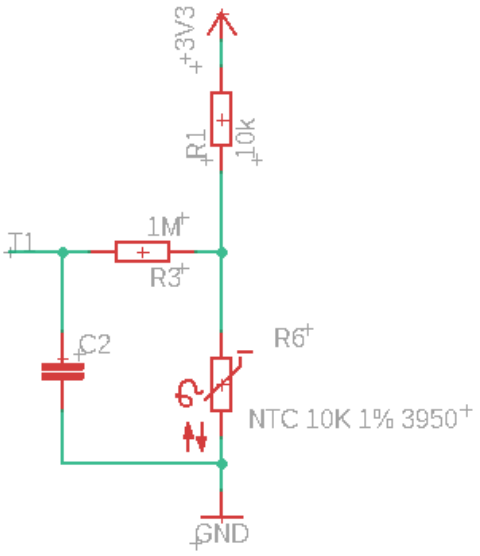
na napěťový rozsah vhodný pro analogově-digitální převodník samotného ESP32 a následně provádět čtení hodnoty napětí na vstupu ADC a programově provádět výpočet pro tzv. True RMS, ovšem to je neefektivní řešení a zabírá velké množství výpočetního výkonu mikropočítače. Druhou variantou řešení je využít zapojení s operačním zesilovačem v integrujícím zapojení, který je ekvivalentem pro numerický výpočet „True RTM“. Výstupní hodnota z operačního zesilovače odpovídá hodnotě měřeného proudu, což snižuje náročnost pro mikropočítač.



Obrázek 7 Zapojení převodníku proudové sondy se stabilizátorem napětí (DFROBOT 2016)

3.3.3. Termistor

NTC 10KΩ 3950 Temperature Probe od HandsOn Technology je teplotní senzor, který využívá NTC (Negative Temperature Coefficient) termistor. Tento termistor mění svůj odpor v závislosti na teplotě, což umožňuje sledovat teplotní změny prostřednictvím analogu. Senzor má odpor při 25 °C 10KΩ ±1% a koeficient B= 3950 ±1%. Teplotní rozsah je od -20 °C do 125 °C. Konstrukce sondy je vodotěsná, což zaručuje dlouhou životnost i v náročných podmínkách. Dále je charakterizován rychlou tepelnou časovou konstantou 15 sekund, což znamená, že rychle reaguje na změny teploty (obr.7).

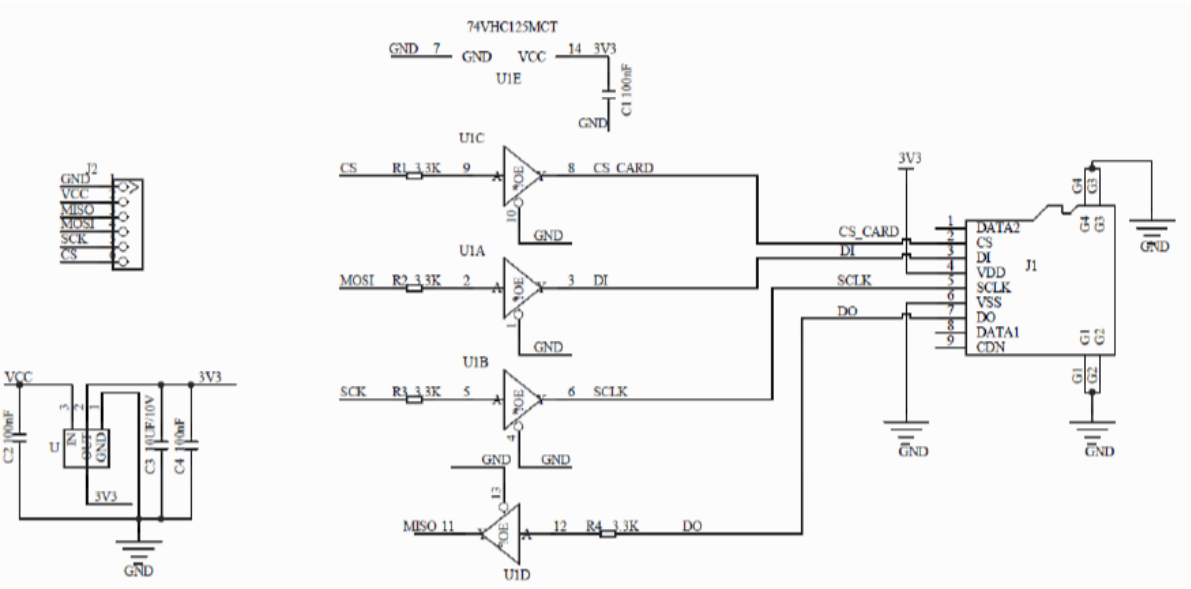


Obrázek 8 Obvodové schéma zapojení termistoru

Termistory jsou zapojeny do odporového děliče a signál na pin mikropočítače prochází přes dolnopropustní filtr.

3.3.4. Modul SD karty

Pro ukládání dat byl zvolen modul pro SD kartu WPI304N. Modul je osazen vlastním LDO pro stabilní napájení a třístavovým bufferem 74VHC125 pro ochranu všech komunikačních signálů. Komunikace mezi SD a mikropočítačem je zajištěna komunikační rozhraní SPI (obr.8).

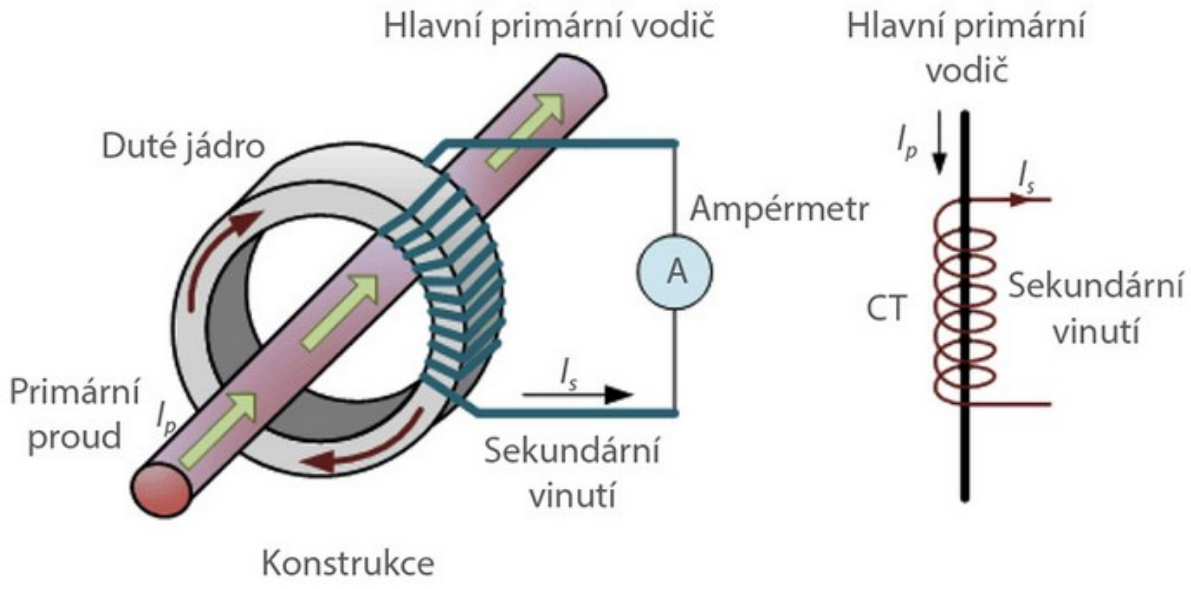


Obrázek 9 Zapojení modulu SD karty (WHADDA 2025)

3.4. Principy měření

V následující kapitole jsou popsány principy měření využité v návrhu zařízení.

3.4.1. Neinvazivní měření proudu



Obrázek 10 Proudový měřící transformátor (Elektroprůmysl 2024)

Proudový transformátor (CT) je zařízení určené pro neinvazivní měření elektrického proudu v primárním vodiči. V konstrukci tohoto transformátoru prochází primární vodič středem kruhového nebo obdélníkového jádra, kolem kterého je obtočeno sekundárním vinutím. Princip činnosti CT spočívá ve využití elektromagnetické indukce, kdy střídavý proud protékající primárním vodičem generuje magnetický tok v jádře, který následně indukuje napětí na sekundární straně (obr.9).

Primární vinutí je v tomto případě tvořeno jedním závitem (samotným vodičem). Poměr transformace k je proto roven počtu závitů sekundárního vinutí N_s. Sekundární proud I_s je pak definován vztahem:

$$k = N_s$$

k… Převodový poměr transformátoru [-]

N_s.. Počet závitů sekundárního vinutí [-]

kde je proud protékající primárním vodičem. Tento vztah zajišťuje, že sekundární proud je přímo úměrný měřenému primárnímu proudu, což umožňuje přesné měření při správně dimenzovaném transformátoru.

Dalším důležitým parametrem CT je magnetická indukce, která závisí na intenzitě magnetického pole generovaného proudem v primárním vodiči. Magnetická indukce je dána vztahem:

$$B = \frac{\mu * I_p}{l_m}$$

B… magnetická indukce (T),

μ … permeabilita materiálu (H/m),

I_p… primární proud (A),

l_m…délka magnetického obvodu (m)

Pro správnou funkci proudového transformátoru je klíčové minimalizovat ztráty. Mezi hlavní typy ztrát patří ztráty v měděném vinutí způsobené ohmickým odporem sekundárního vinutí. Dále jsou přítomny ztráty v jádře, které zahrnují hysterezní ztráty a ztráty způsobené vířivými proudy. Další důležitou charakteristikou je saturační proud. Při překročení této hodnoty se jádro dostává do stavu magnetické saturace, což vede k výrazné nelinearitě a zkreslení měřeného signálu.

Proudové transformátory nacházejí uplatnění v řadě aplikací, od ochranných a měřicích systémů v průmyslových zařízeních až po diagnostické nástroje. Jejich přesnost a stabilita jsou klíčové pro spolehlivost a bezpečnost celého systému.

Výsledný vztah pro měřený proud vychází z parametrů proudového transformátoru a jeho zapojení do měřícího řetězce.

3.4.2. Měření teploty NTC termistor

NTC termistor (Negative Temperature Coefficient) je typ elektronické součástky, jejíž odpor klesá s rostoucí teplotou. NTC termistory jsou ceněny pro svou jednoduchost, nízké náklady a schopnost rychle reagovat na změny teploty.

Závislosti teploty na odporu termistoru vyjadřuje Steinhartuv-Hartův vztahů:

$$\frac{1}{T} = A + Bln\left(\frac{R}{R_0}\right) + Cln^2\left(\frac{R}{R_0}\right) + Dln^3\left(\frac{R}{R_0}\right)$$

T… teplota [°K]

A,B,C,D… koeficienty upravující strmost charakteristiky [-]

R_0… referenční odpor termistoru při 25°C [Ω]

R... aktuální hodnota odporu[Ω]

V technické praxi je využit zjednodušený tvar:

$$\frac{1}{T} = \frac{1}{T_0} + \frac{1}{B} ln\left(\frac{R}{R_0}\right)$$

NTC termistory jsou široce používané teplotní senzory, které nabízejí vysokou citlivost na změny teploty. Jejich hlavní výhodou je schopnost rychle reagovat na teplotní změny a přesně měřit teplotu v různých aplikacích, jako jsou ochrana obvodů, teploměry nebo stabilizace teploty v elektronických zařízeních. Díky své nízké ceně a kompaktní velikosti jsou ideální pro použití v širokém spektru produktů. Tyto termistory mají také široký teplotní rozsah, což je činí velmi univerzálními. Nicméně jejich odpor klesá s rostoucí teplotou, což znamená, že jejich charakteristika není lineární, a tedy vyžaduje kalibraci pro přesné měření.

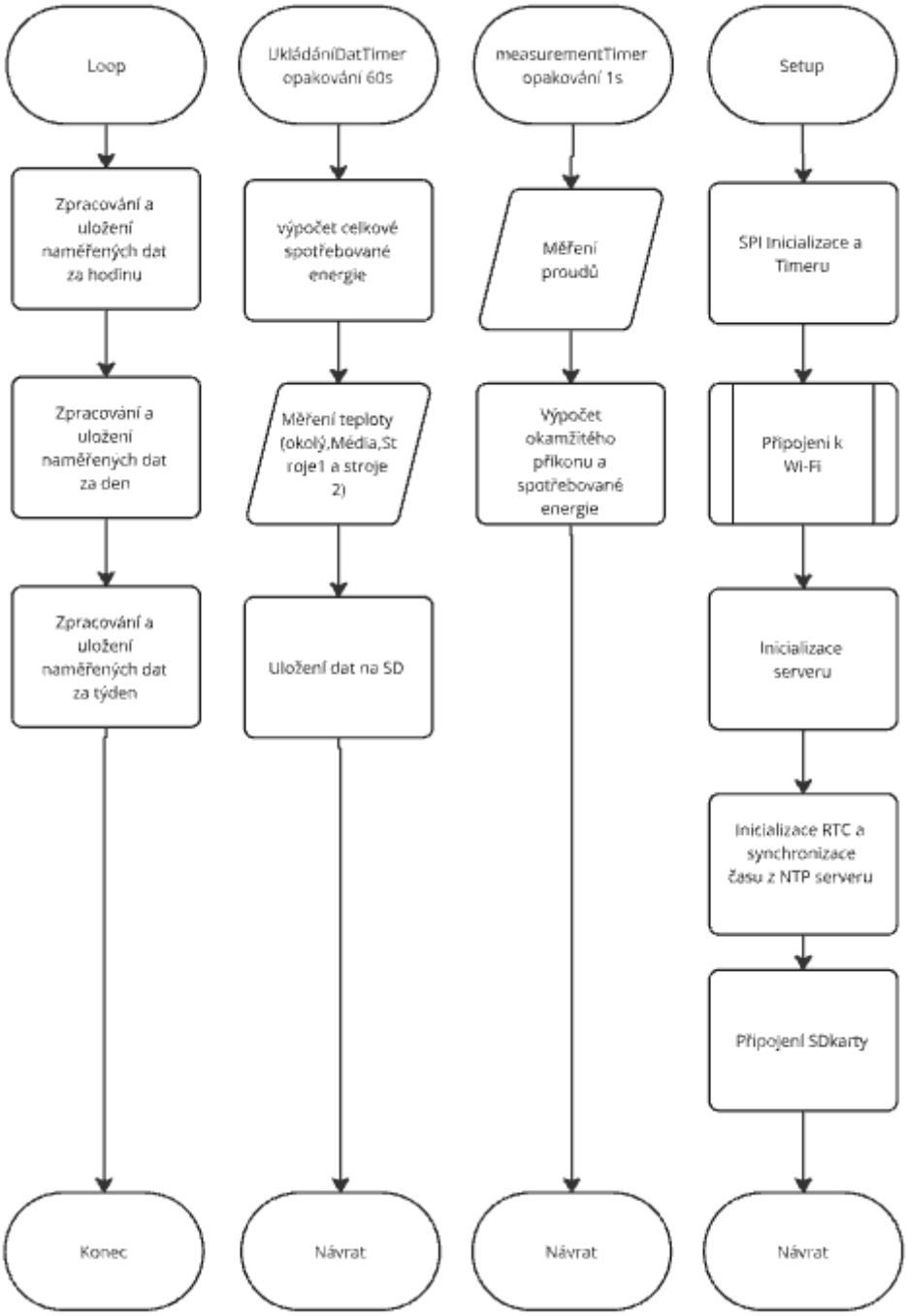
Na druhou stranu, NTC termistory mají i několik nevýhod. Největší omezení představuje nelineární vztah mezi odporem a teplotou, což může komplikovat jejich použití v aplikacích, kde je třeba přesné a lineární měření. Kromě toho mohou být citlivé na okolní podmínky, jako je vlhkost nebo elektromagnetické rušení, což může ovlivnit jejich výkon. Dalším problémem je omezený teplotní rozsah, přičemž při extrémních teplotách mohou NTC termistory ztratit svou stabilitu nebo se poškodit. I přes tyto nevýhody však zůstávají velmi populární díky své jednoduchosti a efektivitě v mnoha běžných aplikacích. (Handson Technology 2024)

3.5. Firmware

Pro realizaci firmwarové časti zařízeni bylo využito vývojové studio Arduino IDE s implementací knihoven pro programování jednočipový počítač ESP32 v prostředí Arduino IDE a realizaci serveru na jednočipovém počítači.

Při spuštění zařízení dojde k inicializaci komunikační sběrnice SPI , timeru,WiFi, karty SD a RTC. Následně je proveden pokusu o připojení k Wi-Fi s použitím údajů uložených ve flash paměti. Pokud dojde k připojení k Wi-Fi proběhne inicializace obsluhy serverových procesů

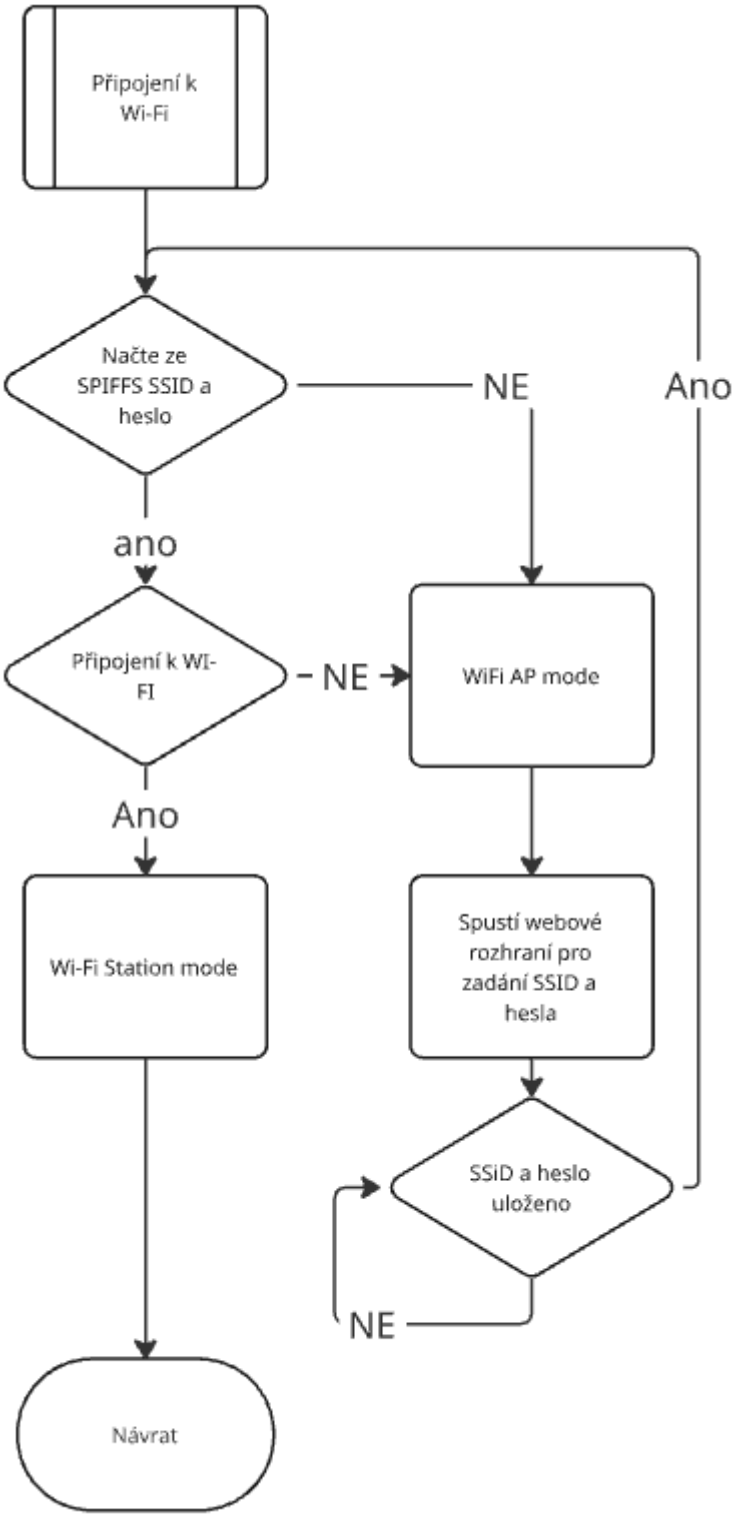
v modu klient Wi-Fi sítě, inicializace RTC a synchronizace s NTP serverem a připojení SD karty pro ukládání dat (obr.10).



Obrázek 11 Vývojový diagram Setup, loop, timer

Pokud k při připojení nedojde k úspěšnému připojení k Wi-Fi zařízení inicializuje síťové rozhraní jako AP vytvoření vlastní Wi-Fi sítě. Po přihlášení do této sítě pomocí PC nebo telefonu je možné po zadání IP adresy zařízení do prohlížeče provést nastavení názvu (SSID)

a hesla sítě, ke které má být zařízení připojeno a po uložení dojde k opětovnému pokusu o připojení k dané síti (obr.11).



Obrázek 12 Vývojový diagram Wi-Fi

Dva časovače zajištují pravidelné provádění měření proudu a teploty a ukládání dat. Časovač measurementTimer vyvolává přerušení pro provedení měření aktuální spotřeby proudu a výpočet okamžitého příkonu a při přerušení od časovač UkládáníDatTimer se provádí měření teplot technologického procesu, výpočet spotřebované energie z dat naměřeného odebíraného proudu a ukládání na SD kartu(obr.10).

Pro měření technologických veličin je využito vnitřního analogově-digitálního převodníku (ADC) a periferie přímého přístupu do paměti (DMA) pro urychlení a zefektivnění programu. Pomocí DMA jsou data z ADC ukládány do bufferu v SRAM paměti bez zatěžování MCU, to si data bufferu nahraje až pro zpracování a vyhodnocení. Vnitřní komunikace mezi ADC a DMA je zprostředkována pomocí I2C sběrnice.

Naměřené vzorky jsou zprůměrovány a vzniklá surová data jsou uložena na SD kartu.

Hlavní smyčka provádí vyhodnocení dat naměřených za hodinu, den a týden (obr.10).

3.5.1. Server na jednočipovém mikropočítači

Realizace webového serveru na jednočipovém počítači pro aplikace IoT a IIoT vyžaduje specifické hardwarové požadavky. Tyto požadavky závisí na několika faktorech, jako je typ platformy, nároky na výkon, připojení k síti, požadavky na úložný prostor a energetickou náročnost. V této kapitole se podrobně zaměříme na hardware, který je potřebný pro implementaci webového serveru.

Webový server na jednom čipu musí mít dostatečný výpočetní výkon k zajištění efektivního zpracování HTTP požadavků a obsluhy více uživatelů zároveň. Výkon procesoru závisí na několika faktorech, kterými jsou počet jader, frekvence procesoru a architektura. Dvoujádrové nebo více jádrové procesory, jaké nabízí například ESP32, umožňují efektivnější zpracování požadavků, protože každé jádro může obsluhovat jinou část zátěže (například jedno pro zpracování webových požadavků a druhé pro komunikaci s externími zařízeními). Frekvence procesoru ovlivňuje rychlost zpracování požadavků. Vyšší frekvence znamená rychlejší zpracování, což je zvláště důležité pro složitější aplikace, které vyžadují větší množství výpočtů. 32bitové mikropočítače jako ESP32 nebo 64bitové počítače jako Raspberry Pi mají odlišnou kapacitu pro zpracování dat, přičemž 64bitové systémy zvládají komplexnější operace a větší množství dat.

Pro běh webového serveru je důležitá dostupnost dostatečného množství paměti. Dvě hlavní složky paměti jsou RAM a Flash. RAM (Random Access Memory) slouží pro dočasné ukládání dat během zpracování požadavků. V případě webového serveru to zahrnuje například načítání HTML stránek, zpracování formulářových dat a ukládání stavů připojení uživatelů. Flash paměť slouží k uchovávání souborů, jako jsou HTML, CSS, JavaScript, obrázky nebo jiný obsah, který server poskytuje uživatelům. U mikropočítačů s menší pamětí je důležité optimalizovat velikost těchto souborů, protože omezená velikost flash paměti může vést k problémům s ukládáním většího množství dat. Mikropočítač ESP32 obvykle disponuje 520 KB RAM a až 4 MB Flash, což je dostačující pro jednoduché webové aplikace s dynamickým obsahem. Raspberry Pi 4 nabízí až 8 GB RAM a 32 GB eMMC nebo microSD kartu pro úložiště, což je ideální pro náročné aplikace, které vyžadují velkou kapacitu pro ukládání souborů a databází.

Knihovna **ESPAsyncWebServer** je vysoce výkonná knihovna pro realizaci webových serverů na jednočipových počítačích jako je ESP32 a ESP8266. Byla navržena na základě asynchronní architektury, která umožňuje efektivní zpracování více požadavků současně. Díky této vlastnosti je knihovna ideálním řešením pro aplikace vyžadující rychlou odezvu a schopnost zpracovat vysoký objem datových požadavků, například pro IoT systémy. Jednou z klíčových vlastností knihovny ESPAsyncWebServer je její schopnost asynchronního zpracování požadavků. To znamená, že server dokáže obsluhovat více klientů najednou, aniž by se blokovalo hlavní vlákno aplikace. Tato vlastnost výrazně zlepšuje výkon a plynulost provozu zejména u aplikací, kde se očekává větší počet paralelních připojení.

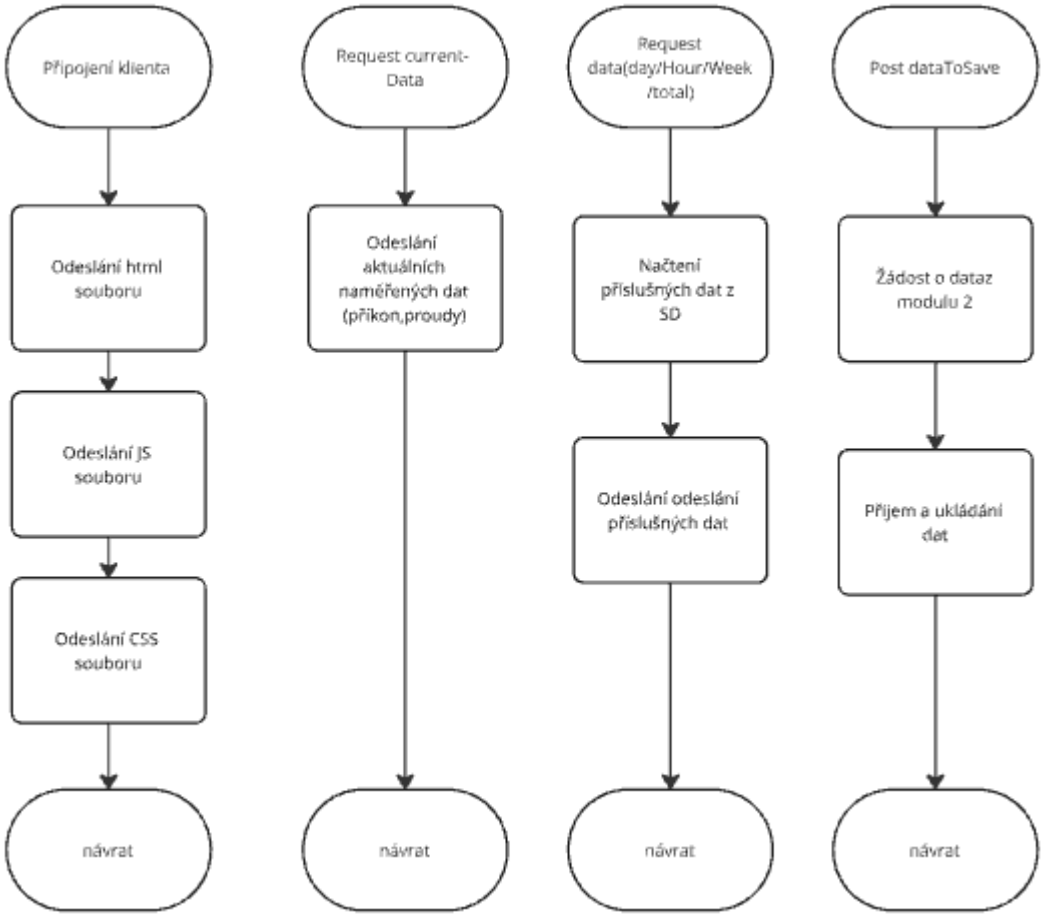
Knihovna podporuje všechny standardní HTTP metody, včetně GET, POST, PUT, DELETE a OPTIONS. To usnadňuje implementaci REST API pro komunikaci mezi serverem a klientem. Díky integrované podpoře WebSocket je možné realizovat obousměrnou komunikaci v reálném čase.

Další významnou funkcionalitou knihovny je podpora servírování statických souborů. To umožňuje hostovat soubory jako HTML, CSS nebo JavaScript přímo na zařízení. Tyto soubory mohou být uložené na SPIFFS nebo LittleFS, což jsou systémy souborů podporované zařízením ESP32. Díky tomu je možné vytvořit kompletní webové rozhraní bez potřeby externího serveru (obr.12).

Realizace webového rozhraní pro zobrazování sledovaných dat byla provedena pomocí značkovacího jazyka HTML, stylistického jazyka CSS a skriptovacího jazyka JavaScript.

Rozhraní umožnuje sledování aktuálních hodnot příkonu obou zařízení, odebíraného proudu na jednotlivých fázích, celkovou spotřebu energii, a dále zobrazení trendů příkonů zařízení a technologických teplot s možností volby zobrazovaného časového horizontu v rozmezí jedné hodiny, dne, týdne a celkově od počátku nasazení

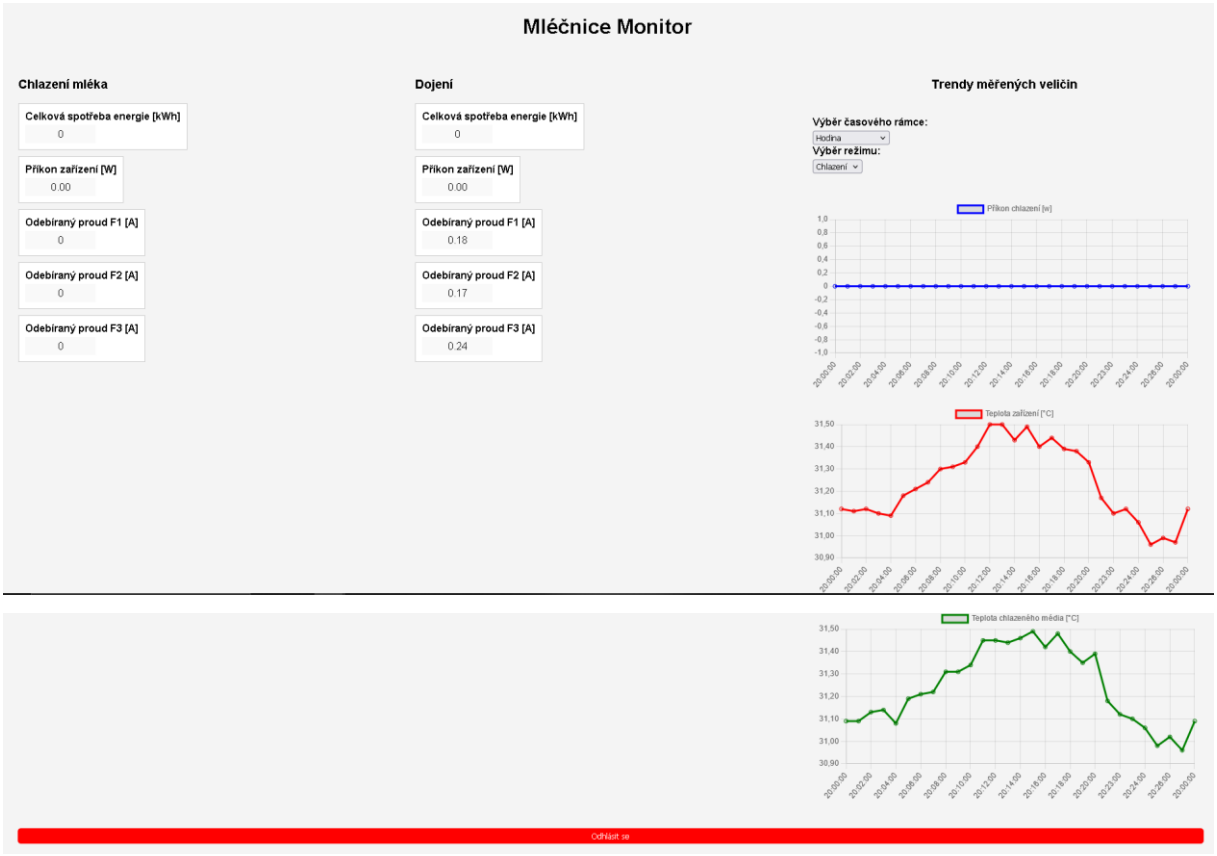
Při realizaci je využito dvou jader mikroprocesoru ESP32, přičemž jádro core 0 je využíváno pro běh hlavní smyčky a měření a jádro core 1 je využíváno pro obsluhu webových požadavků a obsluhy Wi-Fi.



Obrázek 13 Vývojový diagram server

Při připojení uživatele k serveru je vyžadováno přihlašovací jméno a heslo. Po zadání správných údajů je zobrazena hlavní stránka s měřenými údaji.

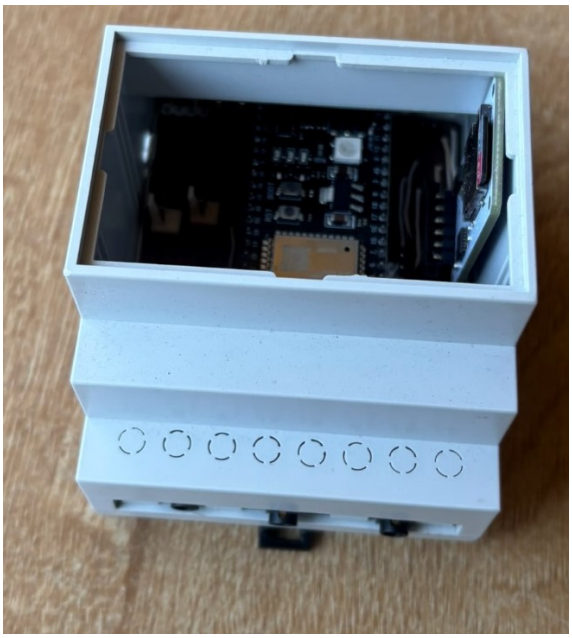
Hlavní strana pro zobrazení měřených dat zobrazuje aktuální informace o spotřebovávaném proudu a celkovém příkonu zařízení a celkovou spotřebovanou energii za časové období. Dále grafy se zobrazením časové závislosti teplot technologického procesu s možností zobrazení trendů za poslední hodinu, den a týden (obr.14).



Obrázek 14 Stránka zobrazování dat

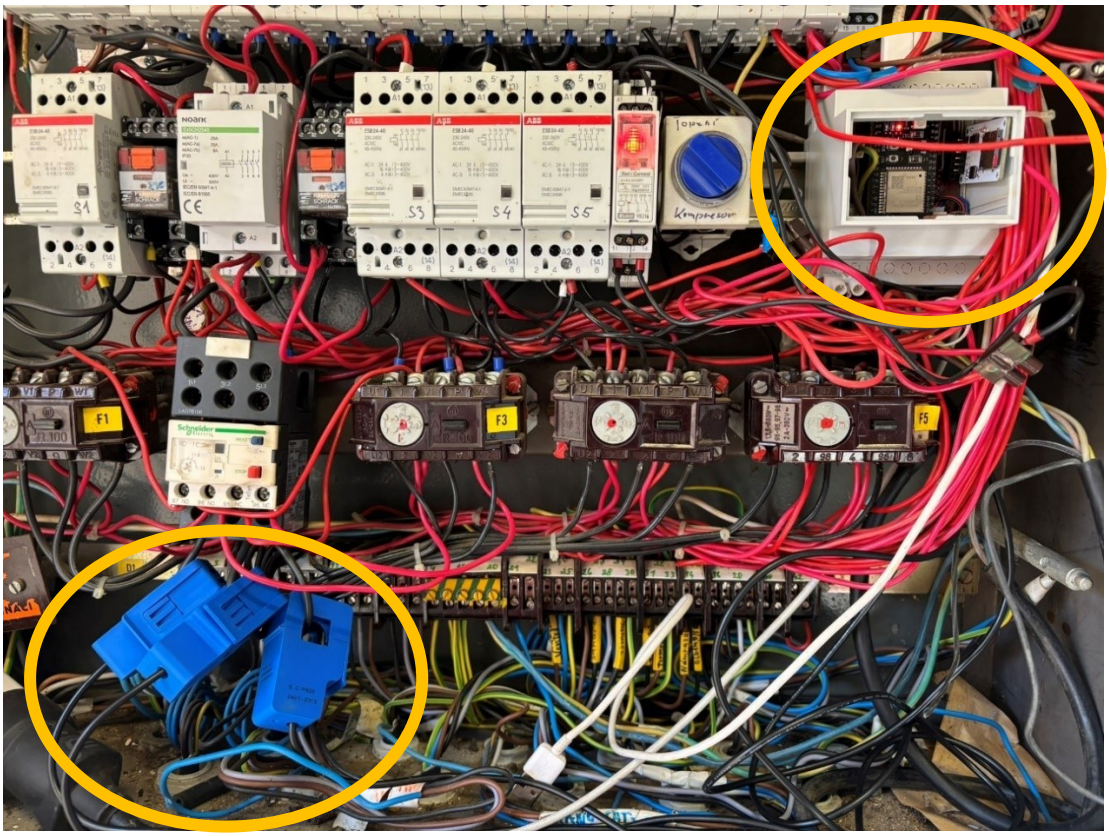
3.6.Instalace a umístění zařízení

Hardware je umístěn v boxu pro montáž na DIN lištu. S uzpůsobením, tak aby bylo možné vyjmout SD kartu a ovládat modul ESP32.



Obrázek 15 Prototypové zařízení

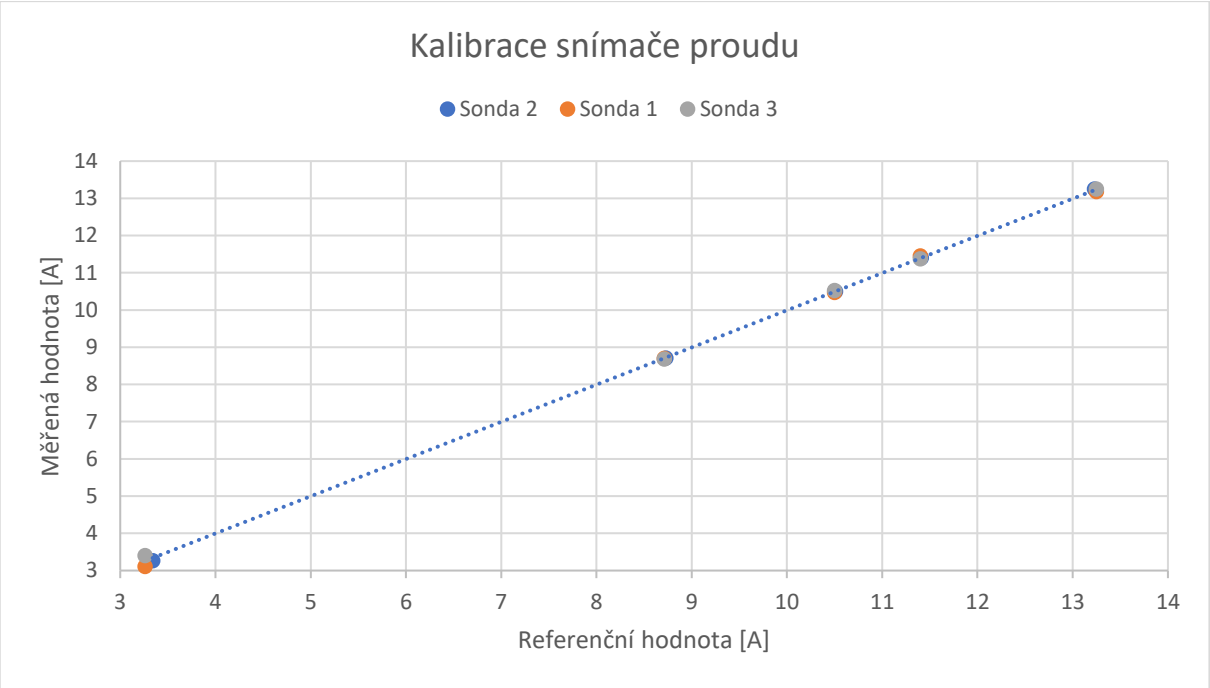
Zařízení je instalováno v rozvodné skříni chladícího zařízení (obr.21 vpravo nahoře). Proudové sondy jsou připojeny k jednotlivým fázovým vodičům chladícího kompresoru (obr.21 vlevo dole). Čidla měření teploty jsou umístěna na vhodných místech tak, aby poskytovala relevantní informace. Čidlo teploty chlazeného média (mléka) je umístěno na vnitřním plášti tanku.



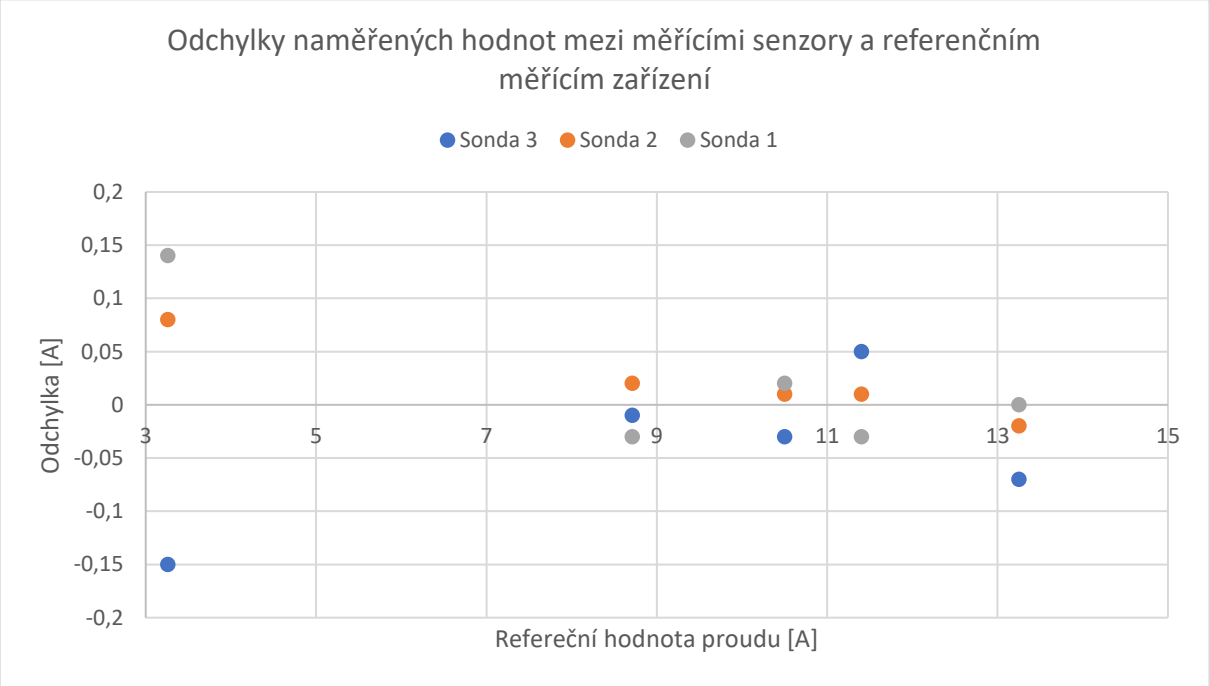
Obrázek 16 Umístění zařízení

3.7. Kalibrace zařízení

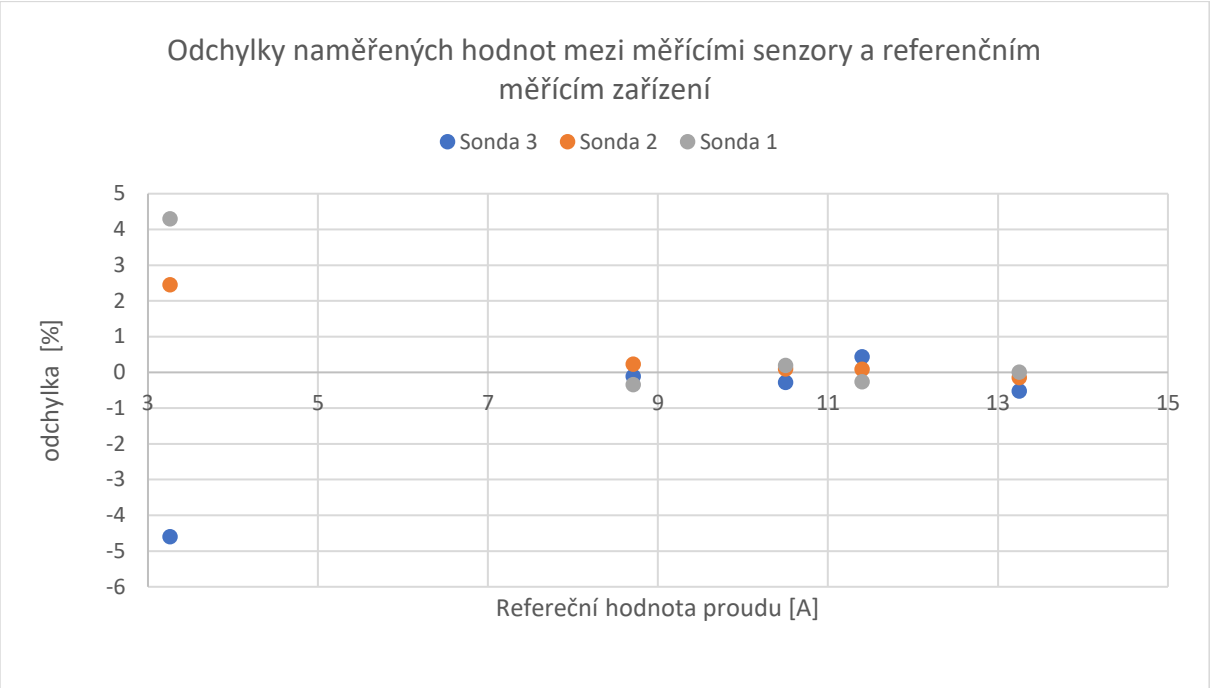
Pro zhodnocení přesnosti měření u vyvíjeného zařízení byl využit klešťový ampérmetr HT208D pro měření referenční hodnoty proudu (obr. 15-17) a pro měření referenční hodnoty teploty analogový teploměr instalovaný v nádrži na mléko (obr. 18-20).



Obrázek 17 Kalibrační křivky proudových sond

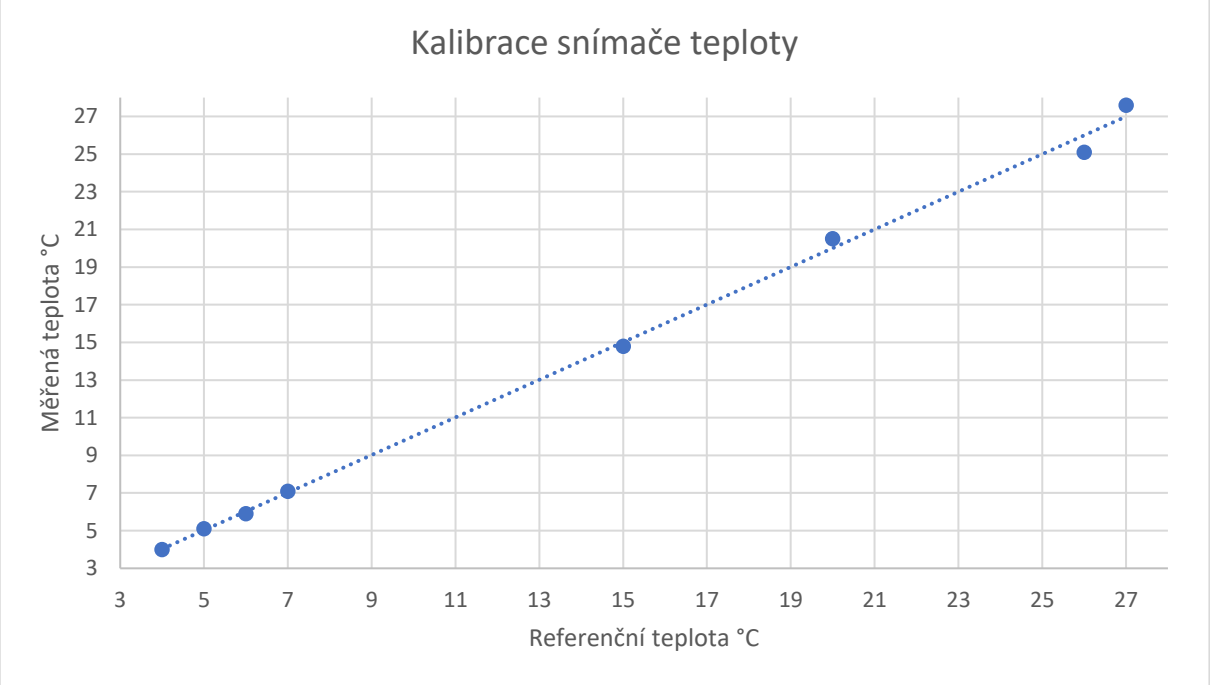


Obrázek 18 Absolutní odchylka proudových sond od referenční hodnoty

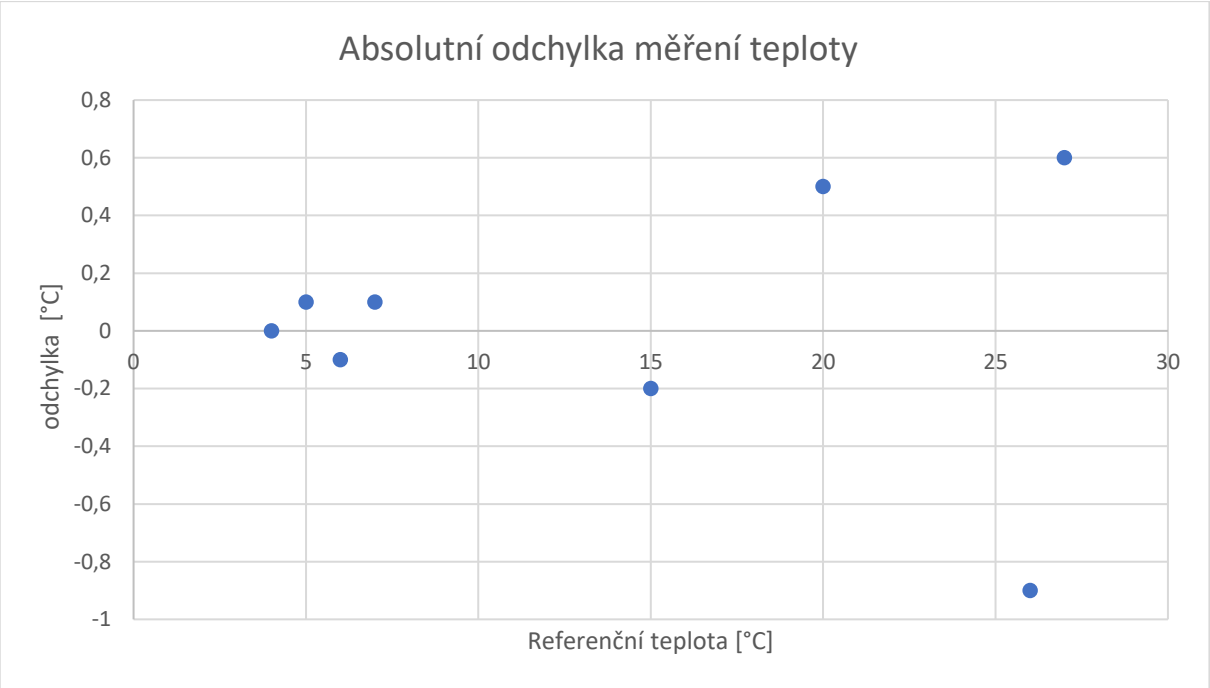


Obrázek 19 Relativní odchylka proudových sond

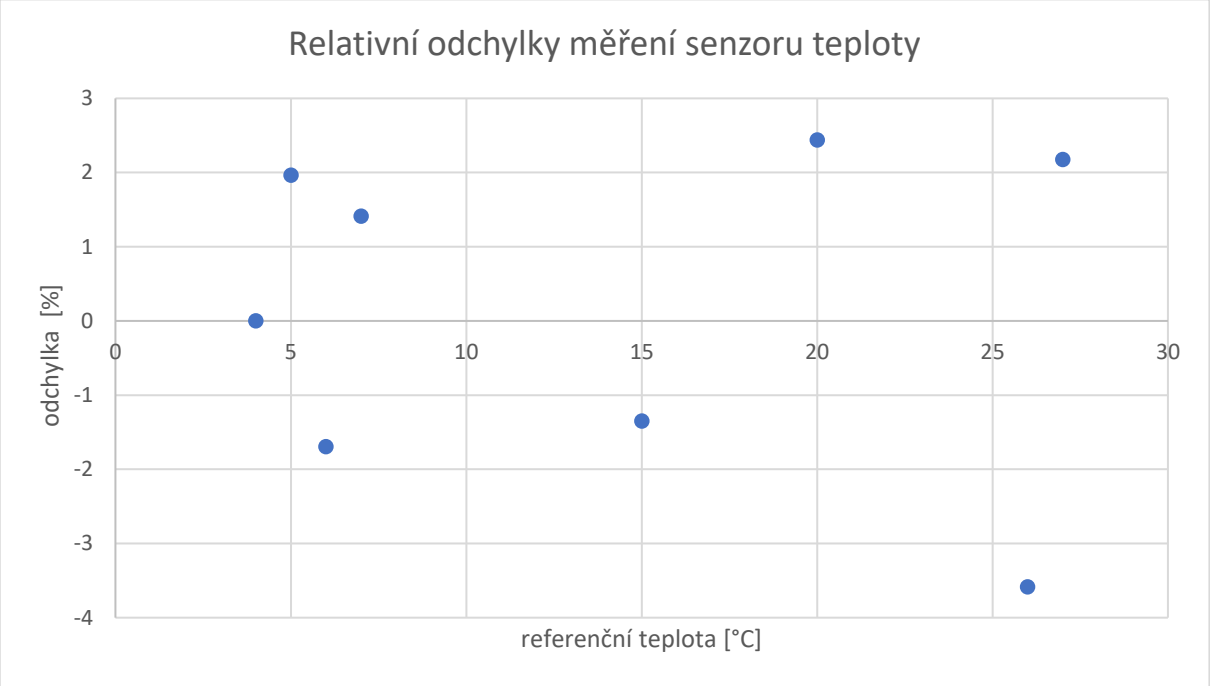
Z grafů pro měření proudu je možné vyčíst velkou odchylku od referenční hodnoty při měření malého proudu, což v případě toho zařízení je možno zanedbat, neboť měřený proud je v rozmezí 6 – 20 A a v tomto rozmezí je měření prováděno s dostatečnou přesností. Nepřesnost je způsobena nelinearitou ADC ESP32.



Obrázek 20 Kalibrační křivka termistoru



Obrázek 21 Absolutní odchylka termistoru



Obrázek 22 Relativní odchylka termistoru

Velké odchylky při měření teploty byly způsobeny konstrukcí chladícího tanku. Pro kalibraci nebylo z konstrukčních důvodů možno umístit termistor do stejného místa jako je umístěn instalovaný analogový teploměr.

ZÁVĚR

V této práci byl navržen a vyvinut IIoT monitorovací systém pro sledování klíčových provozních parametrů vybraného technologického procesu (chlazení mléka) ve stádiu prototypu. Byly popsány a analyzovány dostupné technologie a standardy IIoT, na jejichž základě byla implementována jednotka s mikrokontrolerem ESP32 a integrovanými senzory (SCT-013-015 a NTC termistor) pro měření elektrického příkonu a teploty. Navržené zařízení kontinuálně sbírá a zpracovává data, která jsou zpřístupněna v reálném čase prostřednictvím webového rozhraní běžícího na samotném zařízení.

Realizovaný systém umožňuje podrobné sledování provozu. Podrobná data o procesu lze využít k jeho optimalizaci, což vede ke zvýšení kvality výsledného produktu a současně k včasné identifikaci poruch. Přínosem práce je tedy funkční prototyp monitorovací jednotky, která zvyšuje schopnost sledovat a vyhodnocovat provozní stav technologických zařízení. Tento systém může zlepšit efektivitu výroby a umožnit preventivní údržbu na základě získaných dat.

Další možnosti rozvoje zahrnují:

Rozšíření systému o sledování procesu dojení a podporu dalších komunikačních protokolů (např. MQTT přes TLS) pro rozšíření funkčnosti a zabezpečení.

Využití algoritmů strojového učení pro prediktivní údržbu a detekci anomálií v měřených datech.

Vylepšení softwarové architektury (např. zavedení HTTPS, optimalizace webového rozhraní, mobilní aplikace) pro zvýšení bezpečnosti a uživatelského komfortu.

POUŽITÁ LITERATURA

ANTHI Eirini, Lowri Williams, Matilda Rhode, Pete Burnap, Adam Wedgbury,
Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems,[2021] ISSN 2214-2126, dostupné z:https://doi.org/10.1016/j.jisa.2020.102717[2024]

ARMENTA A., Cloud computing and the Industrial Internet of Things, Control Automation 2022[Online] Dostupné z: https://control.com/technical-articles/cloud-computing-and-the-industrial-internet-of-things/ [cit.2024-27-10]

CATES. J., Malott N., Thelenová T., Tři důležité aspekty zavádění edge computingu. [Online] Dostupné z: https://www.vseoprumyslu.cz/digitalizace/prumyslovy-internet-veci/tri-dulezite-aspekty-zavadeni-edge-computingu.html [cit.2024-27-10]

CLANCY R, Whait Is For Computing? Definition, Applications, Everything to know, 2023, [Online] Dostupné z: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/fog-computing-everything-to-know/ [cit.2024-27-10]

DFROBOT, 2016 ,Dostupné z: https://github.com/DFRobot/DFRobot_AnalogACurrentSensor/blob/master/resources/doc/SEN0211%20Analog%20AC%20Current%20Sensor%20Schematic.PDF [cit.2024-27-10]

ELEKTROPRŮMYSL, Vše o transformátorech proudu [2021] [Online] Dostupné z:https://www.elektroprumysl.cz/merici-technika/vse-o-transformatorech-proudu[cit.2024-27-10]

ESPRESSIF, ESP32WROOM32 Version 3.4 Espressif Systems[2024] [Online] dostupné z: https://www.espressif.com/en/support/documents/technical-documents
Ipc2U, Kompletní nabídka vybavení pro průmyslový internet věcí (IIoT) [2024] [Online] dostupné z: https://ipc2u.cz/blogs/news/full-range-of-equipment-for-industrial-internet-of-things-iiot?srsltid=AfmBOooiadShRG5dg1-4sPdE7a6OJ67VzU45LYl3SFyYTrEJkfRcF4Aw [cit.2024-27-10]

FOLGADO, F.J.; Calderón, D.;González, I.; Calderón, A.J. Review o Industry 4.0 from the Perspective ofAutomation and Supervision Systems:Definitions, Architectures and Recent Trends. Electronics 2024, 13, 782. Dostupné z: https://doi.org/10.3390/electronics13040782
https://www.3pillarglobal.com/insights/blog/edge-computing-and-iiot [online]. [cit. 2024-21-10].

FOXON, IIoT není totéž jako Průmysl 4.0 2017 [Online] Dostupné z: https://www.foxon.cz/blog/ostatni-clanky/191-iiot-neni-totez-jako-prumysl-4-0 [cit.2024-27-10]

HANDSON TECHNOLOGY, NTC 10KΩ 3950 Temperature Probe [2024] [Online] dostupné z: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.handsontec.com/dataspecs/sensor/NTC-10K-3950-HT.pdf&ved=2ahUKEwjOyu7-pPCKAxVd_rsIHedvFecQFnoECBsQAQ&usg=AOvVaw1T6HhTy2qiNZZaDJlXYpB6[cit.2024-27-10]

HIVE MQ a, What is MQTT Quality of Service (QoS) 0,1, & 2? – MQTT Essentials: Part 6 2024 [Online] Dostupné z:https://www.hivemq.com/blog/mqtt-essentials-part-6-mqtt-quality-of-service-levels/ [cit.2024-25-11]

HIVE MQ b, Navigating Cybersecurity Concerns in Industrial IoT Deployments [2024]

https://www.hivemq.com/blog/navigating-cybersecurity-concerns-iiot-deployments/[cit.2024-27-10]
IBM a , Telemetry use case: Home energy monitoring and control 2024[Online] Dostupné z:https://www.ibm.com/docs/en/ibm-mq/9.4?topic=cases-telemetry-use-case-home-energy-monitoring-control [cit.2025-01-10]

IBM b, Cloud computing, 14.2.2024 [Online]Dostupné z : https://www.ibm.com/topics/cloud-computing [cit.2024-27-10]

IHDC , 0.333V Split core current transformer [2024] [Online] Dostupné z : https://www.alldatasheet.com/datasheet-pdf/pdf/1160246/YHDC/SCT013-100.html [cit.2024-25-11]

INHAND NETWORKS,Enhancing IoT security with Trusted Platdorm Module (TPM) [2024] dostupné z : https://www.inhand.com/en/support/blogs/enhancing-iot-security-with-tpm/ [cit.2024-27-10]

ISO/IEC 20924 (36 9020) Internet věcí (IoT) a digitální replika – Slovník. Zdroj Česká agentura pro standardizaci 2024

INTEGRA, Industrial IoT(IIoT) Device Security
Dostupné z: https://iss-networks.com/industrial-iot-device-security.html [cit.2024-27-10]

KARMARKAR, Anish a Marcellus BUCHHEIT, 2018. The Industrial Internet Vocabulary Technical Report V2.0 | Industrial Internet Consortium [online]. 22. srpen 2018. B.m.: Industrial Internet Consortium..Dostupne z: https://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.1.pdf [online]. [cit. 2024-26-10].

LATIF, S.; Driss, M.; Boulila,W.; Huma, Z.e.; Jamal, S.S.; Idrees, Z.;Ahmad, J. Deep Learning for the Industrial Internet of Things (IIoT):A Comprehensive Survey of Techniquess Implementation Frameworks, Potential Applications,and Future Directions. Sensors 2021,21, 7518. [online].

[cit. 2024-21-10].

MQTT a, Use Cases 2024[Online] Dostupné z: https://mqtt.org/use-cases/Beviwise [cit.2024-27-12]

MQTT b, Implementation on Celikler Holding's Power Plant Monitoring 2024[Online]] Dostupné z: https://www.bevywise.com/blog/iot-success-stories-mqtt-broker-celikler-holding/ [cit.2024-21-11]

NIKITA .S, IoT and Cloud Computing: How Do They Work Together?, 2023 [Online] Dostupné z: https://www.cloudpanel.io/blog/iot-and-cloud-computing/#the-relationship-between-iot-and-cloud-computing [cit.2024-27-10]

SCALE Exploring Computing Models: Edge Computing vs Fog Computing vs Cloud Computing, 2023[Online] Dostupné z: https://www.scalecomputing.com/resources/edge-computing-vs-fog-computing-vs-cloud-computing [cit.2024-27-10]

SHARMA, Garima, Securing Industrial IoT (IIoT): The Role of Semiconductors in Cybersecurity [2024] https://www.bisinfotech.com/securing-industrial-iiot-the-role-of-semiconductors-in-cybersecurity/[cit.2024-27-10]
KZV.zf.jcu.cz, [2024] dostupné z: http://kzv.zf.jcu.cz/studium-a-vzdelavani/studijni-materialy-a-informace/obecna-zootechnika/oz-2017-2018/laktacni-krivka.jpg/image_view_fullscreen [cit.2024-26-11]

SIEMENS a, SCALANCE LPE[Online] [2024] dostupné z: https://www.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/local-processing.html[cit.2024-27-10]

SIEMENS b, Simatic S7 controler [Online] [2024] dostupné z: https://xcelerator.siemens.com/global/en/all-offerings/products/s/simatic-s7-controllers.html[cit.2024-27-10]

SIEMENS c, Industrial IoT Gateways SIMATIC CloudConnect 7 [Online] [2024] dostupné z: https://www.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/industrial-iot-gateway-simatic-cloudconnect-7.html [cit.2024-25-12]

SLÁDEK, P. (2020), Implementační rámec řešení průmyslového Internetu věcí, VŠE-FIS, Praha, 2020 http://www.vse.cz/vskp/eid/81070 [online]. [cit. 2024-21-10].

SYNOPSYS, What is a Physical Unclonable Function (PUF) [2024] https://www.synopsys.com/glossary/what-is-a-physical-unclonable-function.html [cit.2024-27-10]

WANG Gang, SoK: Applying Blockchain Technology in Industrial Internet of Things 2024 [Online] Dostupné z : https://www.researchgate.net/publication/353572249_Blockchain_technology_for_the_industrial_Internet_of_Things_A_comprehensive_survey_on_security_challenges_architectures_applications_and_future_research_directions/citations[cit.2024-27-10]

WHHADA, Exciting Electronics microSD Card Logging Shield for Arduino. https://cdn.velleman.eu/downloads/25/wpi304na4v01.pdf?_gl=1*1c0fe3o*_gcl_au*MjcwMzM1MDExLjE3NDcxMTYwMjQ. [cit.2025-20-05]
ZHANG, Y.; Tang, D.; Zhu,H.; Zhou, S.; Zhao, Z. An EfficientIIoT Gateway for Cloud–Edge Collaboration in CloudManufacturing. Machines 2022, 10,850. Dostupné z : https://doi.org/10.3390/machines10100850[online]. [cit. 2025-11-5].

ZHUKABAYEVA, T.;Zholshiyeva, L.; Karabayev, N.; Khan,S.; Alnazzawi, N. CybersecuritySolutions for Industrial Internet ofThings‑Edge Computing Integration:Challenges, Threats, and Future Directions. Sensors 2025, 25, 213.https://doi.org/10.3390/s25010213 [online]. [cit. 2025-11-5].

SEZNAM PŘÍLOH

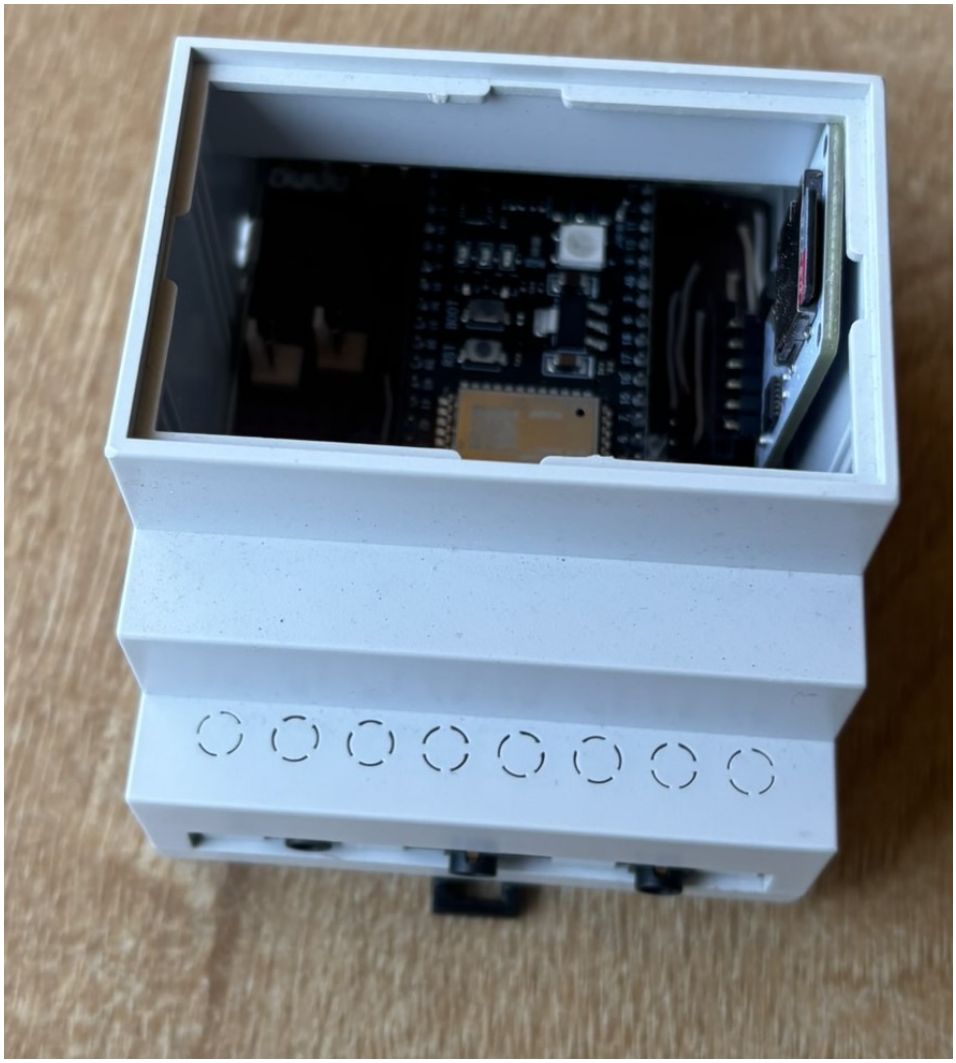
PŘÍLOHA A*:* Instalační manuál

Instalační manuál kontrolního sytému mléčnice

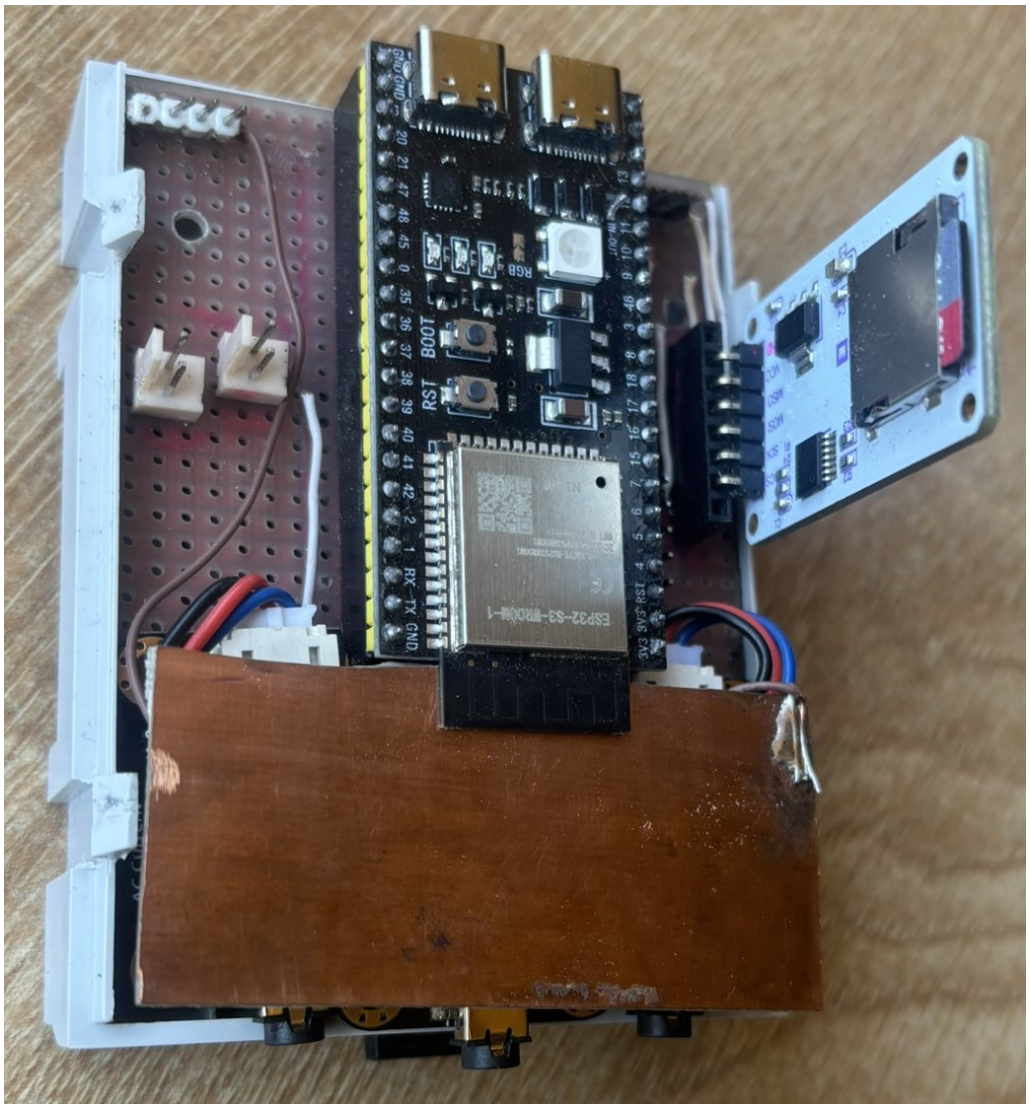
1) Připnutí proudových sond na jednotlivé fázové vodiče
2) Umístění teplotních čidel na vhodné pozice
   a) Teplotní čidlo 1 pro měření okolní teploty
   b) Teplotní čidlo 2 pro měření teploty chlazeného média
   c) Teplotní čidlo 3 pro měření teploty chladícího zařízení
3) Připojení proudových sond pomoct jack konektoru k hlavní jednotce
4) Připojení konektorů teplotních čidel s příslušným číslem na základní desku kontrolní jednotky
5) Připojení USB-C konektoru a připojení do sítě přes síťový adaptér
6) Pomocí mobilního zařízení/PC se připojte k Wi-Fi s názvem ESP-Config
7) Po připojení do vyhledávače zadejte IP adresu 192.168.4.1
8) Po zobrazení konfigurační stránky zadejte jméno a heslo pro připojení do místní sítě Wi-Fi. Po uložení se zobrazí na stránce IP adresa pro následné připojení ke kontrolní jednotce.
9) Restartujte zařízení pomocí tlačítka RST
10) Pomocí dříve uložené IP adresy se připojte k zařízení. Po přihlášení jsou dostupné záznamy o provozu.

    Přednastavené přihlašovací údaje jsou Jméno: Admin Heslo: heslo123

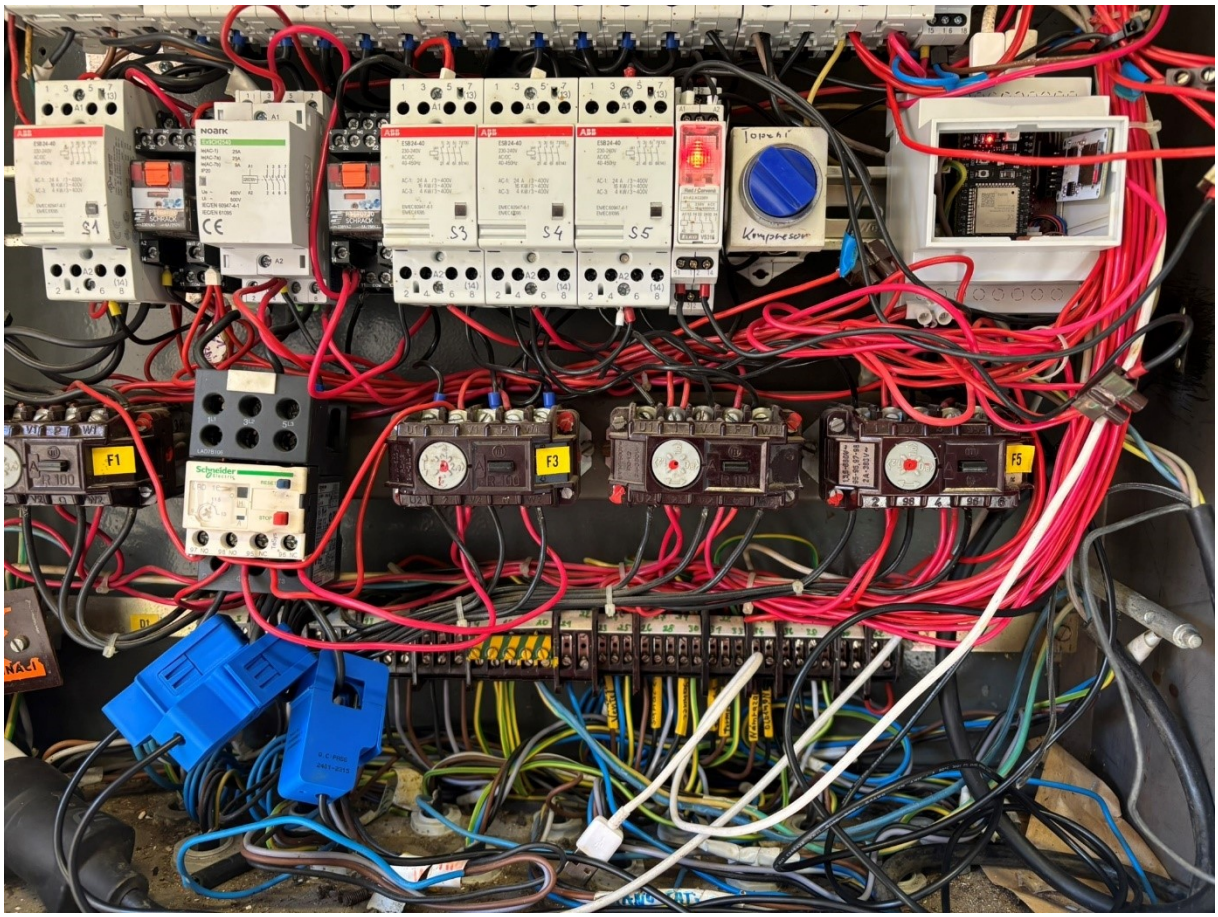
Příloha B: Fotodokumentace a schéma zapojení



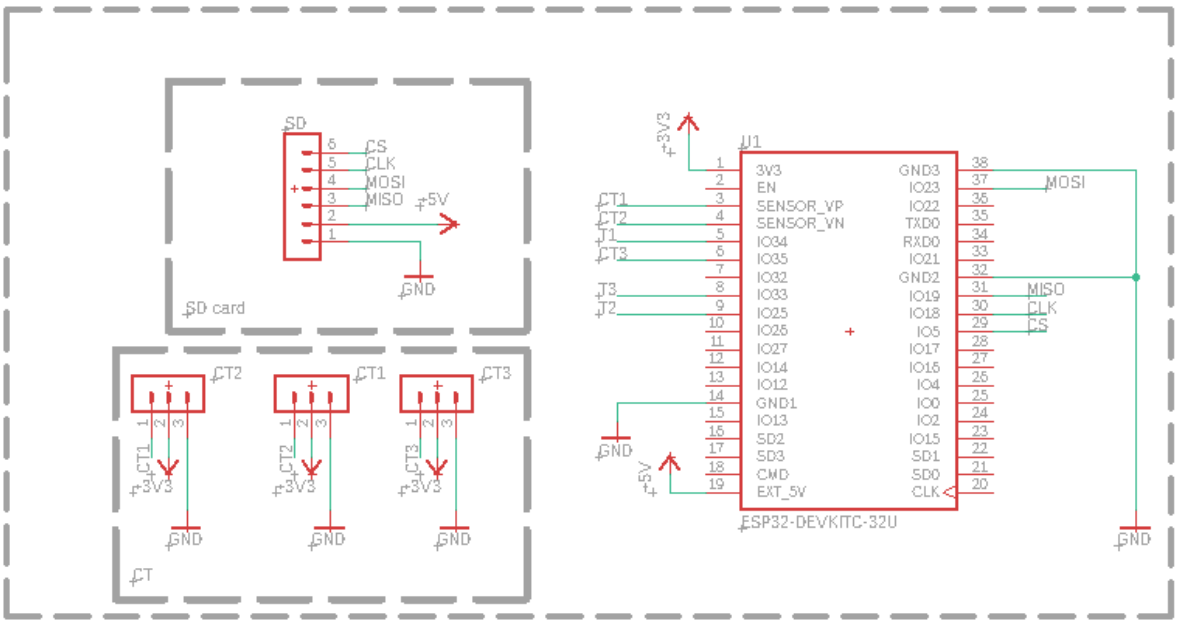
Obr. 1 Hotový prototyp



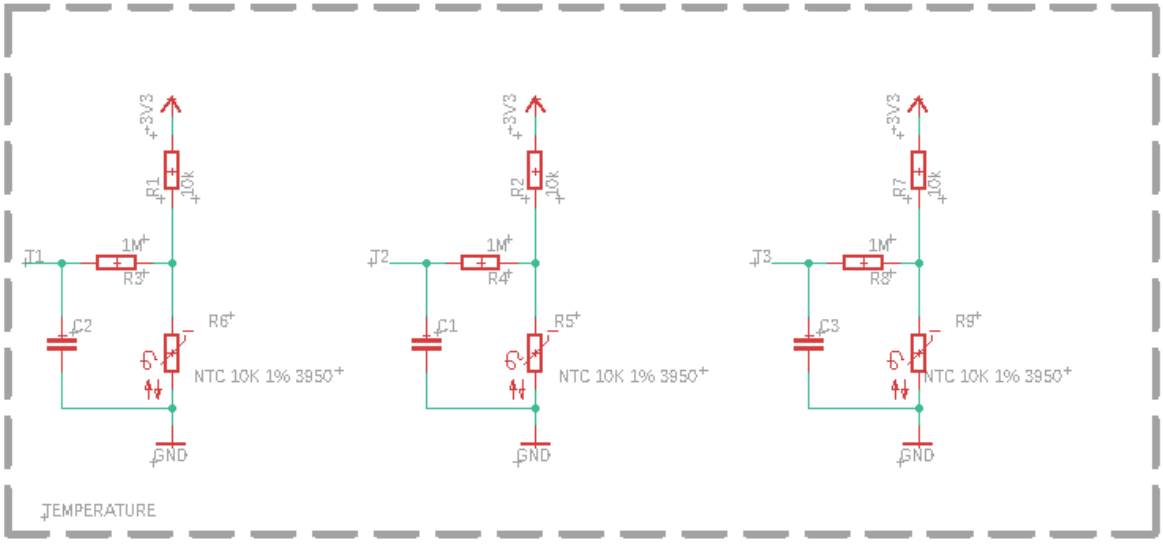
Obr. 2 Hardwarové uspořádání



Obr. 3 Instalace zařízení v rozvaděči



Obr. 4 Schéma zapojení modulu esp32



Obr. 5 Schéma zapojení teplotních čidel