ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Lukáš Svoboda

Návrh a ověření IoT technologie pro vybranou lokalitu na železnici

Diplomová práce

2022

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K620..... Ústav dopravní telematiky

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Lukáš Svoboda

Studijní program (obor/specializace) studenta:

navazující magisterský – IS – Inteligentní dopravní systémy

Název tématu (česky): **Návrh a ověření IoT technologie pro vybranou lokalitu na železnici**

Název tématu (anglicky): Design and Verification of IoT Technology for a Selected Location on the Railway

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Popis dostupné komunikační technologie IoT (charakteristika, pokrytí, typy sítí apod.)
- Zhodnocení aktuálního využití IoT v prostředí Správy železnic
- Návrh architektury na vybranou lokalitu včetně návrhu konceptu řešení IoT a popisu integračního rozhraní do nadstavbových systémů
- Zohlednění bezpečnosti a kyberbezpečnosti IoT technologií
- Vypracovaní kompletního projektu pro vybranou lokalitu u Správce železnice včetně ekonomické rozvahy a výpočtu návratnosti pro navržené řešení
- Ověření navrženého řešení v prostředí Správy železnic (pilotní projekt) na vybrané lokalitě.

Rozsah grafických prací: dle požadavku vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Svítek M., Postránecký M. - Města budoucnosti, Nadatur, Praha 2018, ISBN 978-80-7270-058-5

Leso M. - ITS on Railway, Czech Technical University in Prague, Praha 2017, ISBN 978-80-01-06297-5

Vedoucí diplomové práce: **doc. Ing. Tomáš Tichý, Ph.D., MBA**
Ing. Martin Raibr (SUDOP)

Datum zadání diplomové práce: **9. července 2021**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **30. listopadu 2022**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

Ing. Zuzana Bělinová, Ph.D.
vedoucí
Ústavu dopravní telematiky

prof. Ing. Ondřej Přibyl, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Lukáš Svoboda
jméno a podpis studenta

V Praze dne 16. května 2022

Poděkování

Touto cestou bych rád poděkoval všem, kteří mi během vytváření této práce poskytli pomoc a své cenné zkušenosti. Zvláště bych chtěl poděkovat panu Ing. Martinu Štrofovi za poskytnutí materiálů potřebných k vytvoření této práce a panu doc. Tomáši Tichému a panu Ing. Martinu Raibrovi, za odborné vedení a konzultování diplomové práce. V neposlední řadě si můj dík zaslouží má rodina, přátelé a blízcí, kteří mi nejen po dobu psaní této práce, ale po dobu celého studia, poskytovali morální a materiální podporu.

Prohlášení

Předkládám tímto k posouzení a obhajobě diplomovou práci, zpracovanou na závěr studia na ČVUT v Praze Fakultě dopravní.

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

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 30.11.2022 ……

podpis

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

NÁVRH A OVĚŘENÍ IOT TECHNOLOGIE PRO VYBRANOU LOKALITU NA ŽELEZNICI

Diplomová práce
Listopad 2022
Bc. Lukáš Svoboda

ABSTRAKT

Předmětem diplomové práce „Návrh a ověření IoT technologie pro vybranou lokalitu na železnici“ je vypracovat projekt pro vybranou lokalitu u Správce železnice, včetně ekonomické rozvahy a ověřit tento projekt. Součástí této práce je také rešerše IoT technologie a navržení architektury na vybranou lokalitu.

ABSTRACT

The subject of the diploma thesis "Design and verification of IoT technology for a selected location on the railway" is to develop a project for a selected location at the Railway Administrator, including the economic balance and verify this project. Part of this work is also a search of IoT technology and design of architecture for a selected location.

OBSAH

OBSAH ... 3
SEZNAM POUŽITÝCH ZKRATEK ... 5
1 Úvod ... 6
1.1 Obecné informace ... 6
1.2 Struktura diplomové práce ... 6
2 Popis IoT technologie ... 8
2.1 Klíčová charakteristika IoT ... 8
2.2 Složení technologie IoT ... 10
2.3 Senzory, které se v IoT používají ... 12
2.4 Princip fungování IoT ... 20
2.5 Řešení konektivity v rámci sady technologií IoT ... 21
2.6 IoT sítě v ČR ... 24
3 Zhodnocení aktuálního využití IoT v prostředí Správy železnic ... 28
4 Architektura ... 29
4.1 Popis komunikace ... 29
4.2 Jednotka FlexiCube ... 30
4.3 Poskytovatel NarrowBand IoT ... 32
4.4 FlexiCube Gateway ... 32
4.5 Firewall ... 34
4.6 Dálková diagnostika TLS ... 34
5 Způsoby využití IoT na železnici a návrh konkrétního systému ... 36
5.1 Možnosti využití jednotky FlexiCube v rámci IoT na železnici ... 36
5.2 Návrh využití IoT na železnici ... 50
6 Implementace IoT pro dopravní objekty ... 54
6.1 Systém monitorování bezpečnosti mostu založený na IoT ... 54
6.2 Implementace systému monitorování kvality ovzduší založeného na internetu věcí pro zkoumání částic (PM10) v tunelech metra ... 55
6.3 Systém vizuální detekce defektů na železničních tratích založený na IoT ... 60
6.4 Systém pro včasné varování založený na IoT pro monitorování kolejnicových styků ... 63
7 Zajištění kyberbezpečnosti IoT technologie ... 66
8 Životní cyklus IoT zařízení ... 69
9 Doporučení pro používání IoT na železnici ... 73
10 Závěr ... 74
ZDROJE ... 76
SEZNAM OBRÁZKŮ ... 78

SEZNAM TABULEK 79

SEZNAM POUŽITÝCH ZKRATEK

API – **A**pplication **P**rogramming **I**nterface

CDP – **C**entrální **D**ispečerské **P**racoviště

ČR – **Č**eská **r**epublika

DDTS – **D**álková **d**iagnostika **t**echnologických **s**ystémů

EZS – **E**lektronický **z**abezpečovací **s**ystém

GUI – **G**rafické **u**živatelské **r**ozhraní

GW – **G**ate**w**ay

HTTPS – **H**ypertext **T**ransfer **P**rotocol **S**ecure

HW – **H**ard**w**are

InK – **In**tegrační **k**oncentrátor

InS – **In**tegrační **s**erver

IoT – Internet **o**f **T**hings

LTE – **L**ong **T**erm **E**volution

MUV – **M**otorový **u**niverzální **v**ozík

NB – **N**arrow**b**and

NTP – **N**etwork **T**ime **P**rotocol

NŽK – **N**árodní **Ž**elezniční **K**oridor

SMS – **S**hort **M**essage **S**ervice

SW – **S**oft**w**are

SŽ – **S**práva **Ž**eleznic

TCP – **T**ransmission **C**ontrol **P**rotocol

TeS – **Te**rminálový **s**erver

UDP – **U**ser **D**atagram **P**rotocol

VNC – **V**irtual **N**etwork **C**omputing

VRT – **V**ysoko**r**ychlostní **t**rať

ŽST – **Ž**elezniční **St**anice

1 Úvod

1.1 Obecné informace

Železniční doprava je stále vyvíjejícím a zdokonalujícím se způsobem dopravy. Neustále se zvyšuje počet železničních úseků, staví se nové tratě a rekonstruují ty stávající. V České republice tvoří železniční doprava spolu s dopravou silniční důležitou páteř tranzitní dopravy.

Železniční doprava se neustále snaží využívat nové technologie, hlavně za účelem bezpečnosti. Jednou z těchto technologií může být IoT (Internet of Things). IoT můžeme definovat jako síť zařízení, která jsou vybavena softwarem, komunikují spolu a vyměňují si data.

Hlavní cíl diplomové práce vyplývá už z názvu a je to tedy návrh a ověření IoT technologie na vybrané lokalitě. Dílčí cíle práce vyplývají z postupu, jakým bude tato práce zpracovávána jedná se konkrétně o tyto cíle:

- Popis dostupné komunikační technologie IoT
- Zhodnocení aktuálního využití IoT v prostředí Správy železnic
- Návrh architektury na vybranou lokalitu včetně návrhu konceptu řešení IoT a popisu integračního rozhraní do nadstavbových systémů
- Vypracovaní kompletního projektu pro vybranou lokalitu u Správce železnice včetně ekonomické rozvahy a výpočtu návratnosti pro navržené řešení
- Ověření navrženého řešení v prostředí Správy železnic (pilotní projekt) na vybrané lokalitě.
- Zohlednění bezpečnosti a kyberbezpečnosti IoT technologií

1.2 Struktura diplomové práce

Diplomová práce je členěna do devíti kapitol.

První část se zabývá rešerší a popisem technologie IoT. V této kapitole je popsána charakteristika technologie, tedy čím se vyznačuje, čeho se skládá a jakým způsobem funguje. Poté jsou zde vypsány senzory, které se v IoT využívají, a to i v rámci zpracovávaného projektu. Dále jsou zde vypsány typy používaných IoT sítí a v neposlední řadě je zde kapitola věnovaná pokrytí IoT v České republice.

V třetí kapitole je zhodnoceno využití IoT technologie v prostředí SŽ. Dále je popsána tato technologie z pohledu SŽ, tedy jakým způsobem je využívána a v jakém měřítku.

Čtvrtá kapitola se zabývá tvorbou architektury na vybranou lokalitu a vytvářením konceptu IoT technologie. Je zde pospáno, do jakých částí je architektura rozdělena. Dále je zde popsáno, jakým způsobem probíhá komunikace.

Pátá kapitola se zabývá hlavní částí diplomové práce a tou je vypracování návrhu systému založeného na IoT. V kapitole je také uvedeno ověření použití IoT na železnici pomocí měření a vyhodnocení dat. V neposlední řadě je zde uvedeno vyčíslení návrhu po finanční stránce a porovnání s jinými technologiemi.

Šestá kapitola je zaměřená na implementaci IoT pro dopravní objekty, které svým způsobem nesouvisí se železnici. Jsou zde uvedeny čtyři systémy, které se používají ve světě a jsou založené na IoT.

Sedmá a osmá kapitola se zabývá rešerší ohledně zajištění kyberbezpečnosti IoT technologie, resp. cyklem IoT zařízení.

V poslední kapitole jsou uvedeny doporučení ohledně používání IoT systému, kterými se mohou řídit případní konzumenti obsahu, jako je např. Správa železnic.

2 Popis IoT technologie

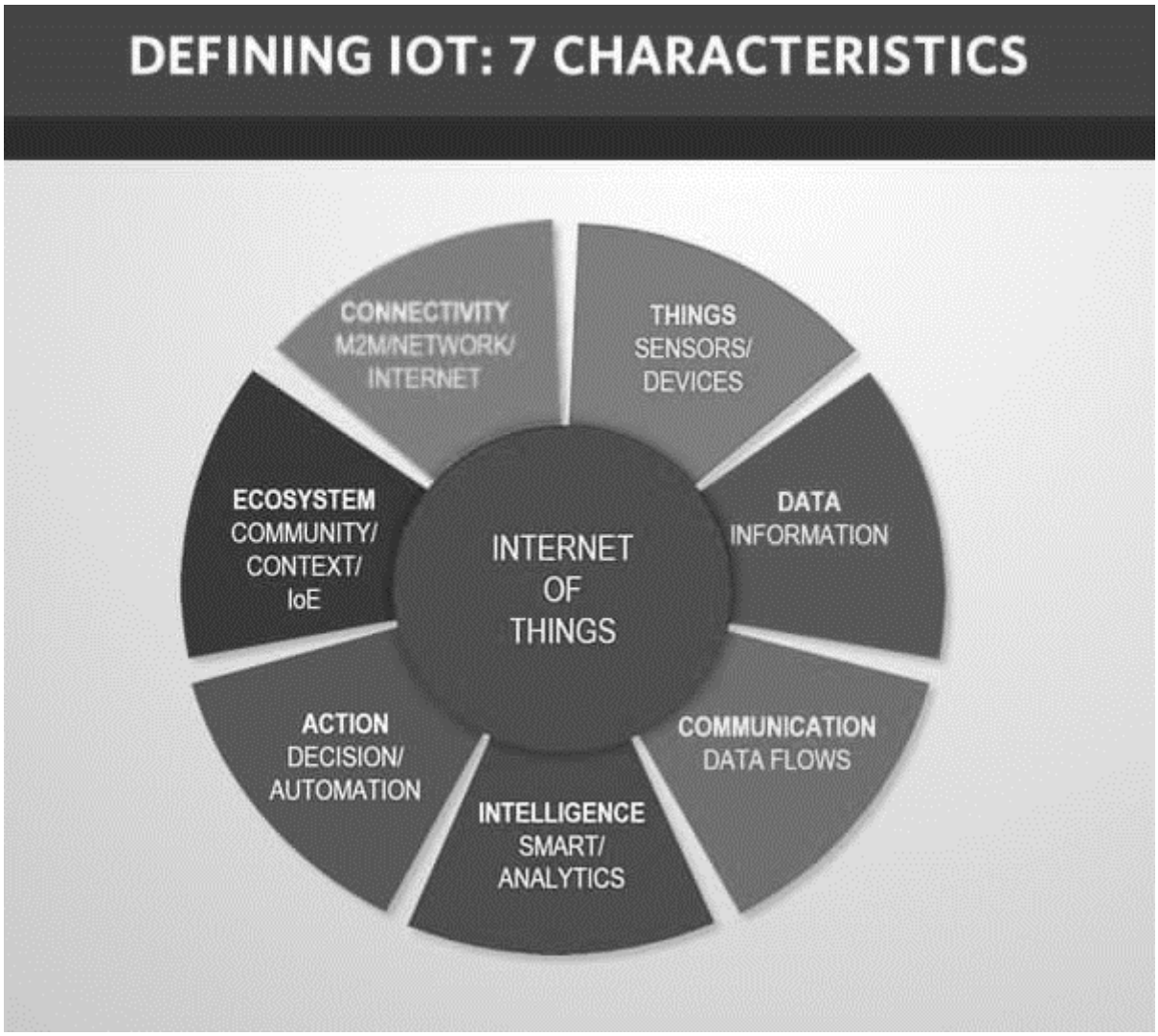
Internet věcí neboli IoT je systém vzájemně propojených počítačových zařízení, mechanických a digitálních strojů, předmětů, zvířat nebo lidí, které mají jedinečné identifikátory a schopnost přenášet data po síti, aniž by byla nutná interakce mezi lidmi nebo interakce člověka s počítačem. [1]

Věcí v IoT může být člověk s implantátem srdečního monitoru, hospodářské zvíře s transpondérem biočipu, automobil, který má vestavěné senzory, které řidiče upozorní, když je tlak v pneumatikách nízký, nebo jakýkoli jiný přírodní nebo umělý objekt, kterému lze přiřadit IP adresu a je schopen přenášet data po síti.

Organizace v různých odvětvích stále častěji využívají IoT k efektivnějšímu fungování, lepšímu porozumění zákazníkům, poskytování lepších služeb zákazníkům, zlepšování rozhodování a zvyšování hodnoty podniku.

2.1 Klíčová charakteristika IoT

IoT můžeme definovat pohledem na různé charakteristiky v širším kontextu. Všechny tyto charakteristiky vidíme ve většině definic internetu věcí (dále je přehled s některými z těchto definic internetu věcí).



Obrázek 1. Definování internetu věcí pomocí 7 charakteristik [2]

Existuje 7 zásadních vlastností internetu věcí:

a) Konektivita

Není třeba to příliš vysvětlovat. Se vším, co se děje v IoT zařízeních a hardwaru, se senzory a další elektronikou a připojeným hardwarem a řídicími systémy je třeba propojení mezi různými úrovněmi.

b) Věci

Cokoli, co lze označit nebo připojit jako věc, je navrženo tak, aby bylo připojeno. Od senzorů a domácích spotřebičů až po označená hospodářská zvířata. Zařízení mohou obsahovat senzory nebo lze k zařízením a předmětům připevnit snímací materiály.

c) Data

Data jsou tmelem internetu věcí, prvním krokem k akci a inteligenci.

d) Komunikace

Zařízení se propojí, aby mohla přenášet data a tato data lze analyzovat. Komunikace může probíhat na krátké vzdálenosti nebo na velkou vzdálenost až na velmi dlouhou vzdálenost. Příklady: Wi-Fi, síťové technologie LPWA, jako je LoRa nebo NB-IoT.

e) Inteligence

Aspekt inteligence, jako jsou schopnosti snímání v zařízeních IoT a inteligence získaná z analýzy velkých dat (také umělá inteligence).

f) Akce

Důsledek inteligence. Může se jednat o manuální akci, akci založenou na debatách o jevech (například v chytrých továrních rozhodnutích) a automatizaci, která je často nejdůležitějším dílem.

g) Ekosystém

Místo internetu věcí z pohledu jiných technologií, komunit, cílů a obrazu, do kterého internet věcí zapadá. Dimenze internetu všeho, dimenze platformy a potřeba pevných partnerství. [2]

2.2 Složení technologie IoT

Zorientování se v technologickém bludišti internetu věcí vzhledem k rozmanitosti a naprostému množství technologických řešení, která jej obklopují, se může ukázat jako velmi obtížný úkol.

Pro jednoduchost bychom však mohli rozdělit sadu technologií IoT na čtyři základní technologické vrstvy, které se podílejí na fungování internetu věcí. Jedná se o následující:

a) Hardware zařízení

Zařízení jsou předměty, které ve skutečnosti tvoří „věci“ v rámci internetu věcí. Fungují jako rozhraní mezi skutečným a digitálním světem a mohou mít různé velikosti, tvary a úrovně technologické složitosti v závislosti na úkolu, který mají v rámci konkrétního nasazení IoT plnit. Ať už jde o mikrofony velikosti špendlíkové hlavičky nebo těžké stavební stroje, prakticky každý hmotný objekt (dokonce i ty živé, jako jsou zvířata nebo lidé) lze proměnit v připojené zařízení přidáním potřebného vybavení (přidáním senzorů nebo akčních členů spolu s příslušným softwarem) a měřit a shromažďovat potřebná data. Je zřejmé, že senzory, akční členy nebo jiné telemetrické zařízení mohou samy o sobě tvořit samostatná chytrá zařízení. Jediným omezením, se kterým se zde lze setkat, je skutečný případ použití IoT a jeho hardwarové požadavky (velikost, snadnost nasazení a správy, spolehlivost, užitečná životnost, nákladová efektivita).

b) Software zařízení

To je to, co vlastně dělá připojená zařízení „chytrá“. Software je zodpovědný za implementaci komunikace s Cloudem, sběr dat, integraci zařízení a také provádění analýzy dat v reálném čase v rámci sítě IoT. A co víc, je to software zařízení, který také zajišťuje uživatelům na úrovni aplikace možnosti vizualizace dat a interakce se systémem IoT.

c) Komunikace

Po instalaci hardwaru a softwaru zařízení musí existovat další vrstva, která chytrým objektům poskytne způsoby a prostředky pro výměnu informací se zbytkem světa IoT. I když je pravda, že komunikační mechanismy jsou silně svázány s hardwarem a softwarem zařízení, je nezbytné je považovat za samostatnou vrstvu. Komunikační vrstva zahrnuje jak řešení fyzické konektivity (mobilní, satelitní, LAN), tak specifické protokoly používané v různých prostředích IoT (ZigBee, Thread, Z-Wave, MQTT, LwM2M). Výběr příslušného komunikačního řešení je jednou z důležitých součástí při konstrukci každé sady technologií IoT. Zvolená technologie bude určovat nejen způsoby, kterými jsou data odesílána/přijímána z Cloudu, ale také to, jak jsou zařízení spravována a jak komunikují se zařízeními třetích stran.

d) Platforma

Jak již bylo zmíněno dříve, díky „chytrému“ hardwaru a nainstalovanému softwaru je zařízení schopno „vycítit“, co se kolem něj děje, a sdělit to uživateli prostřednictvím specifického komunikačního kanálu. Platforma IoT je místem, kde se všechna tato data shromažďují, spravují, zpracovávají, analyzují a prezentují uživatelsky přívětivým způsobem. To, co činí takové řešení obzvláště cenným, tedy není pouze jeho sběr dat a možnosti správy zařízení IoT, ale spíše jeho schopnost analyzovat a najít užitečné poznatky z částí dat poskytovaných zařízeními prostřednictvím komunikační vrstvy. Na trhu je opět celá řada platforem IoT s možností výběru v závislosti na požadavcích konkrétního projektu IoT a faktorech, jako je architektura a sada technologií IoT, spolehlivost, vlastnosti přizpůsobení, použité protokoly, agnosticismus hardwaru, bezpečnost a efektivita nákladů. Za zmínku také stojí, že platformy lze instalovat buď přímo na pracovišti nebo na cloudu. Platforma Coiote IoT Device Management je dobrým příkladem takové platformy, protože ji lze nasadit na pracovišti i v cloudu. Totéž platí pro další platformu IoT od AVSystem — Coiote IoT Data Orchestration. [3]

2.3 Senzory, které se v IoT používají

Senzorů, které se v rámci IoT technologie využívají, je mnoho, a proto jsem vybral ty nejdůležitější, včetně těch, které jsou využity v rámci projektu.

1) Gyroskopické senzory (gyroskopy)

Jedná se senzory, které se používají k měření úhlové rychlosti. Úhlová rychlost je jednoduše definována jako měření rychlosti otáčení kolem osy. Jedná se o zařízení používané především pro navigaci a měření úhlové a rotační rychlosti ve 3-osých směrech. Nejdůležitější aplikací je sledování orientace objektu.

Existuje několik různých druhů gyroskopických senzorů, které jsou vybírány podle jejich pracovního mechanismu, typu výstupu, výkonu, dosahu snímání a podmínek prostředí.

- Rotační (klasické) gyroskopy
- Optické gyroskopy
- MEMS (mikro-elektro-mechanické systémy) Gyroskopy

Tyto senzory jsou vždy kombinovány s akcelerometry. Použití těchto dvou senzorů jednoduše poskytuje systému více zpětné vazby. [7]

2) Detektor kouře

Detektor kouře identifikuje přítomnost požáru detekcí přítomnosti kouře jako jeho vedlejšího produktu v okolí. Detektor kouře může být založen na fotoelektrickém nebo ionizačním principu. Fotoelektrický detektor používá světelný zdroj, světelný detektor a síťku proti hmyzu k detekci přítomnosti kouře.

Na druhou stranu detektor ionizačního typu používá jako zdroj ionizace radioaktivní izotop americium 241. Ionizační detektory kouře jsou citlivější na kouř produkovaný živým ohněm; zatímco fotoelektrické typy jsou citlivější na kouř produkovaný během doutnající fáze ohně.

Detektor na bázi ionizace cílí na menší a střední částice o velikosti 0,001 až 2,5 mikronu; zatímco fotoelektrický typ cílí na střední a velké částice o velikosti 0,04 až 12 000 mikronů. Detektor kouře je instalován na místě, kde; předpokládá se, že možné nebezpečí požáru vytváří značné množství kouře, který má být detekován.

Princip:

Fotoelektrický detektor kouře pracuje na jednoduchém principu, a to že světlo se při dopadu na malé částice rozptyluje. Na druhé straně ionizační detektor kouře využívá ionizační vlastnosti vzduchu k vedení elektřiny. Samotný fotoelektrický detektor pak může být použit ve dvou typech, detekcí zdroje světla nebo snížením jeho intenzity.
Za normálních podmínek fotodiodový přijímač nedostává žádné světlo, aby generoval dostatečný proud ke spuštění poplachu. V případě požáru kouř vycházející z ohně rozptyluje světlo a dopadá na fotodiodový přijímač. To generuje minimální proud, který pak spustí alarmový obvod.

Radioaktivní zdroj může ionizovat vzduch, aby vedl elektřinu proti dvěma nabitým elektrodám. Tyto elektrody jsou připojeny ke zdroji stejnosměrného proudu obecně k baterii přes zesilovač. Detektory ionizačního typu mají dvě oddělené komory; jednu zapečetěnou a jednu otevřenou pro sledování elektrické vodivosti mezi nimi.
Za normálních podmínek je vzduch ionizován rovnoměrně v uzavřené i otevřené nádobě, za cílem vytvořit nulový potenciálový rozdíl. V případě požáru tyto ionty reagují s kouřem a

ovlivňují tok proudu elektrodami v otevřeném prostoru. To vytváří nepatrný potenciálový rozdíl, který se poté zesílí a spustí alarm. [14]

Obrázek 2. Detektor kouře [14]

3) Detektor tepla

Tepelný detektor je zařízení používané k detekci přítomnosti požáru za podmínek tam, kde není vhodný detektor kouře, například v prostředí plném prachu nebo vlhkosti. Je to nákladově efektivní robustní konstrukce, která chrání před požárem, i za proměnlivých nebo drsných podmínek prostředí.

Tepelný hlásič se většinou používá tam, kde je klíčovým kritériem ochrana majetku, protože nedetekuje přítomnost kouře, který odpovídá za většinu úmrtí souvisejících s požárem. Na druhou stranu nejlepší na tom je, že většina tepelných hlásičů je propojena s hasicím systémem, takže požár uhasí v rekordním čase.

Požární hlásič snímající teplo spustí poplach, když okolní teplota dosáhne prahové hodnoty nebo vykazují nepřirozenou rychlost nárůstu teploty. Systém se skládá z bimetalového pásku nebo termistoru pro vytvoření nebo přerušení obvodu. Jediný problém s těmito systémy je, že má vysokou tepelnou setrvačnost.

Tepelná setrvačnost je časová prodleva mezi teplotou, kterou se má dosáhnout od zdroje k detektoru v závislosti na dalších faktorech prostředí. To znamená, že k aktivaci nebo spuštění tepelného hlásiče požáru je potřeba určitý čas a dostatek tepla.

Princip:

Elektromechanický tepelný detektor vyrobený z bimetalového pásku funguje na jednoduchém principu tepelné roztažnosti. Jedna část proužku je připojena k okruhu, zatímco druhá je otevřena okolnímu prostředí. Mezi otevřeným koncem pásku a další svorkou obvodu je malá vzduchová mezera.
Bimetalový pásek se roztahuje, jak se teplota v průběhu času zvyšuje. Po určitém bodě se dostatečně roztáhne, aby došlo ke kontaktu s terminálem – k uzavření okruhu a spuštění alarmu. V některých provedeních se používají dva bimetalové pásky, jeden rychle působící a jeden pomalu působící pásek. To pomáhá spustit alarm při rychlém i pomalém zvyšování teploty.

Na druhou stranu elektronický tepelný detektor pracuje na základě vlastností termistoru – mění svůj odpor se změnou teploty. V zásadě se odpor termistoru snižuje s rostoucí teplotou. Základní obvod se skládá z částí jako je termistor, bzučák, odpor, napájecí zdroj, zenerova dioda a NPN tranzistor.
Zenerova dioda je zapojena mezi zápornou svorku napájecího zdroje a emitorem NPN tranzistoru. Podobně je alarm zapojen mezi kladnou svorku napájecího zdroje a NPN kolektorem. Termistor je zapojen mezi zdroj a bázi NPN tranzistoru s odporem v sérii.
Zenerova dioda udržuje napětí emitoru na cca 4,5 V. Když se teplota zvýší, odpor termistoru se sníží, což má za následek větší proud protékaný bází tranzistoru. Tím se spustí alarm. [14]

4) Detektor ohně

Zatímco detektor kouře a detektor tepla, spoléhají na detekci vedlejších produktů plamene nebo ohně, tak detektor plamene se zaměřuje na přítomnost plamene, aby identifikoval požár. Detektor plamene se skládá z optického detektoru, který zjišťuje a reaguje na přítomnost plamene přes UV a infračervené paprsky vycházející z plamene.

Detektor plamene se používá tam, kde je vyžadována okamžitá odezva, např. vysokoteplotní pracovní oblast, práci s vysoce hořlavým materiálem a pro bezobslužný strojní prostor. Nevýhodou takového požárního hlásiče je, že funguje pouze v případě požáru plamenem a má tendenci vydávat falešný poplach v blízkosti obloukového svařování.

Detektor plamene může být typu UV, infračerveného nebo obojího. Ultrafialový detektor funguje dobře v rozsahu 150 až 250 nm, detekuje jakýkoliv požár nebo výbuch během 2 až 4 milisekund. Infračervený detektor pracuje v rozsahu 4 až 4,5 mikrometru. Využívá se pro detekci požáru i pronikající částice, jako je prach, kouř a další nečistoty ve vzduchu.

Princip:

Během procesu spalování jsou vyzařovány elektromagnetické vlny od ultrafialového po infračervené záření. K detekci požáru se používá fotodioda. Pracuje na způsobu identifikace ultrafialových a infračervených paprsků pro úzké pásmo vlnových délek vyzařovaných během spalování/ohně. Zařízení se skládá z elektronického obvodu s odporovým a logickým hradlem spolu s detektorem.

Fotodioda používaná k detekci elektromagnetického záření prochází radiačním filtrem, aby se odstranilo nebo zabránilo nežádoucímu záření na pozadí. Tyto diody jsou citlivé na pevné pásmo vlnové délky obvykle spojené s ohněm. Když přijme takovou vlnovou délku záření, tak jeho hodnota odporu začne klesat.

Protože dioda je připojena přes svorky napájecího zdroje s odporem, tak zahajuje vedení pod vlivem záření z ohně. Tento výstupní proud pak prochází logickým hradlem, aby se vytvořil digitální výstup, který se porovnává s přednastavenou hodnotou. Pokud je výstupní hodnota za prahovou hodnotou, tak řídící jednotka spustí požární poplach. [14]

5) Senzor vlhkosti

Senzory vlhkosti lze rozdělit do dvou skupin, protože každá kategorie používá k výpočtu vlhkosti jinou metodu: senzory relativní vlhkosti (RH) a senzory absolutní vlhkosti (AH). Relativní vlhkost se vypočítá porovnáním skutečné hodnoty vlhkosti při dané teplotě s maximálním množstvím vlhkosti pro vzduch o stejné teplotě. Snímače relativní vlhkosti proto musí měřit teplotu, aby bylo možné určit relativní vlhkost. Naproti tomu absolutní vlhkost se měří bez vztahu k teplotě.

Dva nejběžnější snímače relativní vlhkosti jsou kapacitní a odporové snímače vlhkosti. Kapacitní senzory používají dvě elektrody ke sledování kapacity (tj. schopnosti ukládat elektrický náboj) tenkého kovového pásku umístěného mezi nimi. Kapacita kovu se zvyšuje nebo snižuje rychlostí, která je přímo úměrná změně vlhkosti v okolí senzoru. Rozdíl v náboji (napětí) generovaný zvýšením vlhkosti je poté zesílen a odeslán do vestavěného počítače ke zpracování. Odporová čidla vlhkosti fungují na jiném principu. Tyto senzory využívají malý

polymerový hřeben, jehož velikost se zvětšuje a zmenšuje se změnou vlhkosti, což přímo ovlivňuje schopnost systému ukládat náboj.
Teplotní čidla vlhkosti se používají k měření absolutní vlhkosti. Na rozdíl od snímačů RH využívají snímače tepelné vlhkosti dvě sondy, jednu pro měření suchého dusíku a jednu pro měření vzduchu v okolním prostředí. Když se vlhkost shromažďuje na exponované sondě, senzor zaznamená rozdíl v tepelné vodivosti a vypočítá AH. [15]

6) Senzor přiblížení (proximity senzor)

Zařízení, které detekuje přítomnost nebo nepřítomnost blízkého objektu nebo vlastnosti tohoto objektu a převádí jej na signál, který může uživatel nebo jednoduchý elektronický přístroj snadno přečíst, aniž by se s nimi dostal do kontaktu.

Senzory přiblížení se ve velké míře používají v maloobchodě, protože dokážou detekovat pohyb a korelaci mezi zákazníkem a produktem, který by ho mohl zajímat. Uživatel je okamžitě informován o slevách a speciálních nabídkách okolních produktů.

Dalším velkým a docela starým případem použití jsou vozidla. S autem couváte a při couvání jste upozorněni na překážku, to je práce senzoru přiblížení.

Používají se také pro dostupnost parkování v místech, jako jsou nákupní centra, stadiony nebo letiště.

Mezi senzory přiblížení patří:

- Indukční snímače - Indukční snímače přiblížení se používají k bezdotykové detekci ke zjištění přítomnosti kovových předmětů pomocí elektromagnetického pole nebo paprsku elektromagnetického záření. Mohou pracovat při vyšších rychlostech než mechanické spínače a také se zdají být spolehlivější díky své robustnosti.
- Kapacitní senzory - Kapacitní senzory přiblížení mohou detekovat jak kovové, tak i nekovové cíle. Téměř všechny ostatní materiály jsou dielektricky odlišné od vzduchu. Může být použit pro snímání velmi malých objektů přes velkou část cíle. Obecně se tedy používá v obtížných a komplikovaných aplikacích.
- Fotoelektrické senzory - Fotoelektrický senzor se skládá z částí citlivých na světlo a využívá paprsek světla k detekci přítomnosti nebo nepřítomnosti předmětu. Je ideální alternativou indukčních snímačů. A používá se pro snímání na velké vzdálenosti nebo pro snímání nekovových předmětů.

- Ultrazvukové senzory - Ultrazvukové senzory se také používají k detekci přítomnosti nebo k měření vzdálenosti cílů podobně jako radar nebo sonar. To představuje spolehlivé řešení pro drsné a náročné podmínky. [7]

7) Tlakové senzory

Tlakový senzor je zařízení, které snímá tlak a převádí jej na elektrický signál. Zde množství závisí na úrovni použitého tlaku.

Existuje spousta zařízení, která se spoléhají na kapalinu nebo jiné formy tlaku. Tyto senzory umožňují vytvářet systémy IoT, které monitorují systémy a zařízení, která jsou poháněna tlakem. Při jakékoli odchylce od standardního rozsahu tlaku zařízení upozorní správce systému na jakékoli problémy, které je třeba opravit.

Nasazení těchto senzorů je velmi užitečné nejen ve výrobě, ale také při údržbě celých vodních systémů a topných systémů, protože je snadné detekovat jakékoli kolísání nebo pokles tlaku. [7]

8) Senzory detekce pohybu

Detektor pohybu je elektronické zařízení, které slouží k detekci fyzického pohybu (pohybu) v daném prostoru a převádí pohyb na elektrický signál; pohyb jakéhokoli předmětu nebo pohyb lidských bytostí.

Detekce pohybu hraje důležitou roli v bezpečnostním průmyslu. Firmy využívají tyto senzory v oblastech, kde by neměl být neustále detekován žádný pohyb, a je snadné si všimnout přítomnosti kohokoli, když jsou tyto senzory nainstalovány.

Používají se především pro systémy detekce narušení, automatické ovládání dveří, závoru, chytrou kameru (tj. snímání na základě pohybu/videozáznam), mýtné náměstí, automatické parkovací systémy, automatizovaná umyvadla/splachovače záchodů, osoušeče rukou, systémy řízení energie.

Na druhou stranu mohou tyto senzory také dešifrovat různé typy pohybů, díky čemuž jsou užitečné v některých odvětvích, kde může zákazník komunikovat se systémem mávnutím ruky

nebo provedením podobné akce. Někdo může například zamávat na senzor v maloobchodě a požádat o pomoc se správným rozhodnutím o nákupu.

Toto jsou nejpoužívanější senzory detekce pohybu:

- Pasivní infračervený - Detekuje tělesné teplo (infračervenou energii) a je to nejrozšířenější pohybový senzor v domácích bezpečnostních systémech.
- Ultrazvukový - Vysílá pulsy ultrazvukových vln a měří odraz od pohybujícího se objektu sledováním rychlosti zvukových vln.
- Mikrovlnný - Vysílá pulsy rádiových vln a měří odraz od pohybujícího se objektu. Pokrývají větší plochu než infračervené a ultrazvukové senzory, ale jsou citlivé na elektrické rušení a jsou dražší. [7]

9) Senzory akcelerometru

Akcelerometr je převodník, který se používá k měření fyzického nebo měřitelného zrychlení objektu v důsledku setrvačných sil a převádí mechanický pohyb na elektrický výstup. Je definována jako hodnota změny rychlosti v závislosti na čase.

Tyto senzory jsou nyní přítomny v milionech zařízení, jako jsou chytré telefony. Jejich použití zahrnuje detekci vibrací, naklánění a zrychlení obecně. To je skvělé pro sledování vašeho vozového parku nebo pomocí chytrého krokoměru.

V některých případech se používá jako forma ochrany proti krádeži, protože senzor může poslat upozornění prostřednictvím systému, pokud se pohne objekt, který by měl zůstat nehybný.

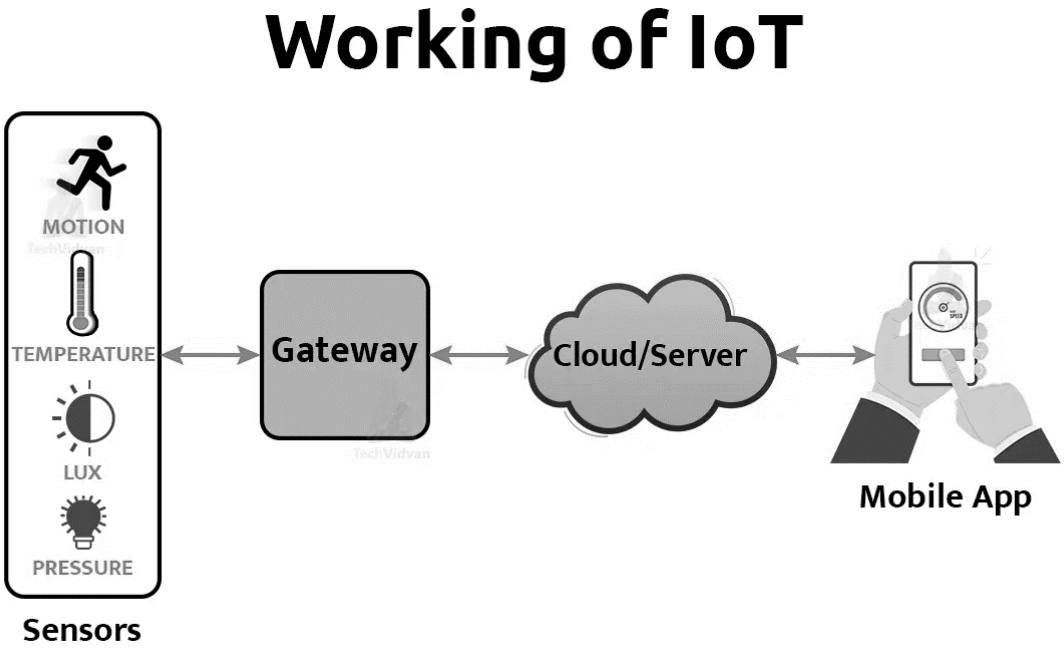
Jsou široce používány v celulárních a mediálních zařízeních, měření vibrací, ovládání a detekce automobilů, detekce volného pádu, leteckém průmyslu, detekci pohybu, sledování chování sportovců, spotřební elektroniky, průmyslových a stavenišť atd.

Existují různé druhy akcelerometrů a několik z nich se používá hlavně v projektech IoT:

- Akcelerometry s Hallovým efektem - Akcelerometry s Hallovým efektem využívají Hallův princip k měření zrychlení, měří změny napětí způsobené změnami magnetického pole kolem nich.

- Kapacitní akcelerometry - Kapacitní akcelerometry snímají výstupní napětí závislé na vzdálenosti mezi dvěma rovinnými plochami. Kapacitní akcelerometry jsou také méně náchylné k šumu a změnám teploty.
- Piezoelektrické akcelerometry - Princip piezoelektrického snímání pracuje na piezoelektrickém jevu. Akcelerometry založené na piezofilmu se nejlépe používají k měření vibrací, rázů a tlaku. [7]

2.4 Princip fungování IoT



Obrázek 3. Fungování IoT [4]

Zařízení IoT mají v sobě zabudované senzory. Tyto senzory jsou schopny snímat své okolí. Zařízení ukládají informace v nějaké formě dat. Mezi tato zařízení patří spotřebiče, jako jsou mobilní telefony, kávovary, mikrovlnné trouby, gejzíry, požární hlásiče, klimatizace, auta a tak dále.

Senzory zabudované v těchto zařízeních neustále vysílají data o okolí a o pracovních informacích těchto zařízení. IoT slouží jako platforma pro výpis všech dat shromážděných těmito zařízeními.

Platforma IoT zahrnuje cloudové servery a rozsáhlé databáze. Platforma IoT pracuje na datech. Integruje a zpracovává informace. Platforma dále důkladně analyzuje data, aby

shromáždila důležité podrobnosti. Platforma pak na základě poskytnutých dat odešle zpět pokyny.

Nakonec je agregace dat sdílena s dalšími zařízeními pro lepší výkon v budoucnu. Je to také provedeno pro lepší uživatelský zážitek. [4]

2.5 Řešení konektivity v rámci sady technologií IoT

Existuje několik možných reálných aplikací technologií IoT, mezi kterými není nouze o řešení konektivity. V závislosti na specifikacích daného případu použití IoT může každá možnost komunikace nabízet různé scénáře aktivace služeb a zároveň mít kompromisy mezi spotřebou energie, dosahem a šířkou pásma. Pokud například stavíte chytrý dům, možná budete chtít mít senzory vnitřní teploty a regulátor vytápění integrované do smartphonu, abyste mohli na dálku sledovat teploty v každé místnosti a upravovat je v reálném čase podle aktuální potřeby. V takovém případě by byl doporučeným řešením síťový protokol IPv6 na bázi IP s názvem Thread, speciálně navržený pro prostředí domácí automatizace.

S ohledem na tuto mnohonásobnost a rozmanitost komunikačních standardů a protokolů si lze položit otázku o skutečné potřebě vývoje nových řešení, zatímco existují některé osvědčené internetové protokoly, které se používají již desítky let. Důvodem je to, že stávající internetové protokoly, jako je Transmission Control Protocol / Internet Protocol (TCP/IP), často nejsou dostatečně efektivní a příliš náročné na energii, aby mohly efektivně fungovat v rámci nově vznikajících aplikací technologie IoT. Tato část představí krátký přehled hlavních alternativních internetových protokolů speciálně vyhrazených pro použití systémy IoT.

Přehled se týká nejoblíbenějších rádiových technologií IoT v členění podle rádiového frekvenčního rozsahu dosaženého každým z těchto řešení: síťová řešení IoT krátkého dosahu, řešení středního dosahu a řešení sítí WAN (Long Range Wide Area Network).

a) Síťová řešení IoT krátkého dosahu

Bluetooth

Jako dobře zavedená technologie konektivity s krátkým dosahem je Bluetooth považováno za klíčové řešení zejména pro budoucnost trhu s nositelnou elektronikou, jako jsou bezdrátová sluchátka nebo geolokační senzory, zejména s ohledem na jeho širokou integraci se smartphony. Protokol Bluetooth Low-Energy (BLE), navržený s ohledem na nákladovou

efektivitu a sníženou spotřebu energie, vyžaduje ze zařízení velmi málo energie. To však přichází s kompromisem: při často přenášených větších objemech dat nemusí být BLE tím nejefektivnějším řešením.

RFID

Radiofrekvenční identifikace (RFID) je jednou z prvních implementovaných aplikací IoT a nabízí řešení pro určování polohy pro aplikace IoT, zejména v řízení dodavatelského řetězce a logistice, které vyžadují schopnost určit polohu objektu uvnitř budov. Budoucnost technologie RFID zjevně daleko přesahuje jednoduché lokalizační služby, s možnými aplikacemi od sledování nemocničních pacientů přes zlepšení efektivity ve zdravotnictví až po poskytování údajů o poloze zboží v reálném čase, aby se minimalizovaly situace, kdy nejsou sklady v maloobchodních prodejnách.

b) Řešení středního dosahu

WIFI

Vyvinutý na základě IEEE 802.11 zůstává nejrozšířenějším a obecně známým bezdrátovým komunikačním protokolem. Jeho široké využití v celém světě IoT je omezeno především nadprůměrnou spotřebou energie vyplývající z potřeby zachovat vysokou sílu signálu a rychlý přenos dat pro lepší konektivitu a spolehlivost. Jako klíčová technologie ve vývoji IoT poskytuje WiFi širokou škálu pro ohromující počet řešení IoT, ale je také třeba jej spravovat a používat z hlediska marketingu, aby přinášelo zisky poskytovatelům služeb i uživatelům. Dobrým příkladem platformy pro správu WiFi, která nabízí službu s přidanou hodnotou umožňující veřejné přístupové body WiFi, je Linkify. Jako jedno ze špičkových řešení AVSystem umožňuje Linkify prakticky neomezené možnosti přizpůsobení WiFi a marketingu hostům.

Zigbee

Tento oblíbený bezdrátový síťový standard nachází své nejčastější aplikace v systémech řízení dopravy, domácí elektronice a strojírenském průmyslu. Zigbee, postavený na standardu IEEE 802.15.4, podporuje nízkou rychlost výměny dat, provoz s nízkou spotřebou energie, bezpečnost a spolehlivost.

Thread

Thread, navržený speciálně pro produkty pro chytrou domácnost, využívá konektivitu IPv6, která umožňuje připojeným zařízením komunikovat mezi sebou, přistupovat ke službám v cloudu nebo komunikovat s uživatelem prostřednictvím mobilních aplikací Thread. Kritici

Thread poukázali na to, že vzhledem k nasycenosti trhu vede další bezdrátový komunikační protokol k další fragmentaci v rámci technologické sady IoT.

c) Řešení sítí WAN (Long Range Wide Area Network)

NB-IoT

Narrowband IoT, produkt stávajících technologií 3GPP, je zcela nový standard rádiové technologie, který zajišťuje extrémně nízkou spotřebu energie (10 let provozu na baterie) a poskytuje konektivitu se silou signálu cca. o 23 dB nižší než v případě 2G. Navíc využívá stávající síťovou infrastrukturu, která zajišťuje nejen globální pokrytí v sítích LTE, ale také garantovanou kvalitu signálu. Tato skutečnost v mnoha případech umožňuje implementovat NB-IoT místo řešení, která vyžadovala vybudování lokálních sítí, jako je LoRa nebo Sigfox.

LTE-CAT M1

LTE-Cat M1 je standard pro připojení široké oblasti s nízkou spotřebou (LPWA), který propojuje zařízení IoT a M2M se středními požadavky na přenosovou rychlost. Podporuje delší životnost baterie a nabízí rozšířený dosah v budově ve srovnání s celulárními technologiemi, jako jsou 2G, 3G nebo LTE-Cat 1.

Vzhledem k tomu, že je kompatibilní se stávající sítí LTE, CAT M1 nevyžaduje, aby operátoři pro její implementaci vybudovali novou infrastrukturu. Ve srovnání s NB-IoT se LTE Cat M1 ukazuje jako perfektní pro případy mobilního použití, protože manipulace s předáváním mezi buňkami je výrazně lepší a je velmi podobná vysokorychlostnímu LTE.

LoRaWAN

LoRaWAN je nízkoenergetický protokol Long Range Wide-Area Networking optimalizovaný pro nízkou spotřebu energie a podporující velké sítě s miliony zařízení. LoRaWAN, zaměřený na aplikace rozlehlých sítí (WAN), je navržen tak, aby poskytoval nízkoenergetické WAN funkcemi potřebnými pro podporu levné, mobilní a zabezpečené obousměrné komunikace v rámci IoT, M2M, chytrých měst a průmyslových aplikací.

Sigfox

Koncepcí Sigfoxu je poskytnout efektivní řešení konektivity pro M2M aplikace s nízkou spotřebou, které vyžadují nízké úrovně přenosu dat, pro něž je rozsah WiFi příliš krátký a rozsah buněk příliš drahý a příliš hladový po výkonu. Sigfox používá UNB, technologii, která

mu umožňuje pracovat s nízkou rychlostí přenosu dat 10 až 1000 bitů za sekundu. Spotřebou až stokrát nižší energie ve srovnání s řešeními pro mobilní komunikaci poskytuje typickou pohotovostní dobu 20 let pro 2,5Ah baterii. Nabízí robustní, energeticky účinnou a škálovatelnou síť schopnou podporovat komunikaci mezi tisíci tisíci bateriových zařízení na ploše několika čtverečních kilometrů, Sigfox se osvědčuje jako vhodný pro různé M2M aplikace, včetně inteligentního pouličního osvětlení, inteligentních měřičů, monitorů pacientů, bezpečnostních zařízení a senzorů prostředí. [3]

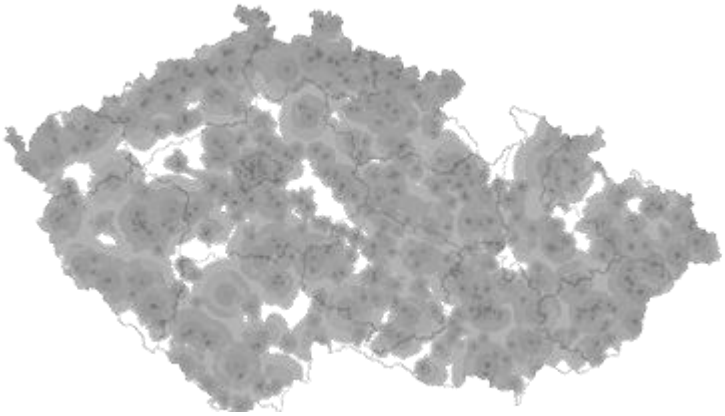
2.6 IoT sítě v ČR

K nejvýznamnějším sítím v ČR patří:

- LoRaWAN – síť u nás rozvíjí a spravuje CRA
- Sigfox – pomáhá rozvíjet česká firma SimpleCell
- NB-IoT – v ČR rozvíjí O_2 a Vodafone

Lorawan

Technologie LoRaWAN vznikla díky více subjektům (narozdíl od Sigfoxu), takže zákazníci mohou využívat více zařízení (komponent) od různých výrobců.
LoRAWAN využívá radiovou komunikaci, která je určena pro přenos menšího množství informací na velkou vzdálenost. Velká výhoda je hlavně v nízké náročnosti na energii, takže baterie mohou vydržet až 10 let.



Obrázek 4. Pokrytí v ČR v roce 2019 [23]

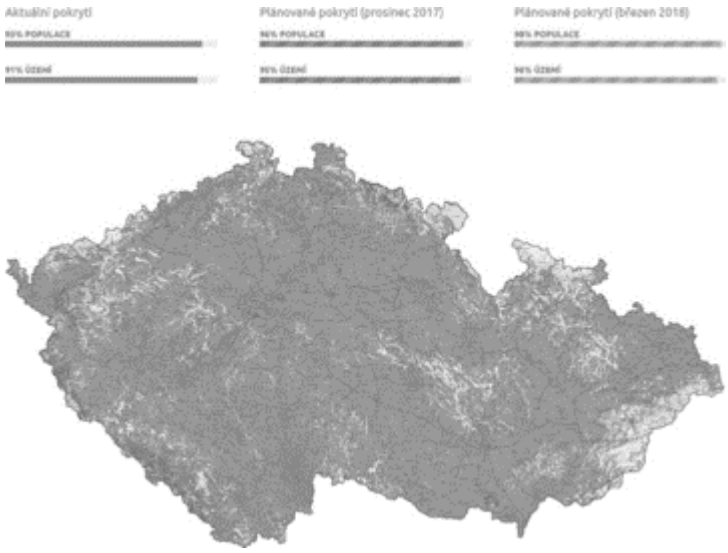
Po síti mohou informace proudit rychlostí od 300 bit/s do 50 000 bit/s. Stejně jako Sigfox i LoraWAN pracuje v nelicencovaném pásmu na frekvenci 868 MHz.

Velká výhoda tkví v tom, že do sítě nelze připojit žádné zařízení (čidlo, měřič nebo senzor), které od CRA nedostane certifikaci. To nutí výrobce IoT zařízení se dívat na IoT i z bezpečnostního hlediska.

V síti LoRaWAN je navíc možné zařízení bez problému aktualizovat díky lepší obousměrné komunikaci. Díky tomu mohou výrobci a dodavatelé zařízení průběžně opravovat případné chyby, nebo jen čistě třeba nahrávat nový firmware.

Sigfox

Takovým českým ambasadorem pro Sigfox se stala česká firma SimpleCell. Na stožáry se umístí moduly, které umožní komunikovat v síti Sigfox.



Obrázek 5. Pokrytí v ČR [23]

Všechna Sigfox zařízení musí obsahovat komunikační čip, který poskytuje možnost komunikovat na síti Sigfox. Zajímavé je, že takový čip nemá žádnou SIM kartu nebo IP adresu. Místo toho používá unikátní 32bitové Sigfox ID, které se vygeneruje hned při výrobě zařízení.

Rychlost přenosu dat po síti je pouze 100 bit/s, ale má to své důvody. Rychlost je dána především omezením ze strany Sigfoxu, aby zařízení poslala do světa maximálně 144 zpráv denně. Právě tím zajišťuje malou spotřebu energie a díky tomu zařízení mohou přežít 5 až 15 let na jednom místě a bez výměny.

Jedna z nevýhod Sigfoxu je obousměrná komunikace. Je aktivovaná pouze na vyžádání koncovým zařízením. Proto se Sigfox hodí spíše na jednosměrnou komunikaci. Ve zkratce

tam, kde vám stačí přenášet denně pouze malou část dat. Hlavní nevýhoda je proto složitější aktualizace připojených zařízení (pokud je vůbec možná).

U Sigfoxu mohou vznikat problémy s připojením. Na vině bývá to, že mají minimum tzv. gateways (GWY). Vedle toho nefunguje za pohybu, takže se tato síť nehodí například pro mobilní aplikace.

Přenos dat funguje podobně jako u LoRaWAN. Zařízení odešlou data do nejbližší stanice a ta je převede do cloudu. V případě Sigfoxu je cloud ve Francii. Odtamtud data získávají firmy a mohou s nimi dál pracovat. Pomocí API je pak převádějí do vlastních aplikací, které dodávají koncovým zákazníkům.

NB-IoT

Celým názvem Narrow Band IoT. V ČR za touto sítí stojí mobilní operátoři. Komerčně ji zatím provozuje pouze Vodafone. Ostatní jsou zatím ve fázi testů. Vodafone využívá svou stávající infrastrukturu. Nemusí budovat novou síť, ale stačí pouze upravit software na vysílacích stanicích. Takový malý zásah vyhradí část LTE pásma čistě pro IoT zařízení. Narozdíl od svých dvou konkurentů nemusí investovat takové prostředky do rozvoje infrastruktury, jako antény a přijímače.

NB-IoT je náročnější na spotřebu energie. A to nevyužívá 4G ani 3G sítě, které jsou pro komunikaci s IoT zařízení ještě náročnější a zároveň spotřebují spousty dat. To je pro IoT nepraktické. Proto se v O2 a Vodafone rozhodli využít LTE pásmo. Dalším důvodem je, že na ostatních sítích fungují i mobilní zařízení, které komunikují se svými ústřednami mnohem častěji, což by mohlo působit problémy.

Obrázek 6. Pokrytím NB-IoT dosáhne k 96 % obyvatelům v ČR [23]

Pro komunikaci musejí zařízení podporující technologii NB-IoT obsahovat SIM kartu. Zařízení mají už v sobě zabudovaný komunikační modul se SIM kartou, který zákazník při spuštění aktivuje. Následně se zařízení propojí s NB-IoT sítí a komunikace je na světě. [5]

3 Zhodnocení aktuálního využití IoT v prostředí Správy železnic

V momentální situaci bohužel není IoT aktivně využíváno, ale už bylo na železnici několikrát testováno. Příkladem může být město Ostrava, kde si pracovníci SŽ neustále stěžovali na krádeže trakčního vedení. Z toho důvodu bylo trakční vedení osazenou jednotkami FlexiCube, o které je více uvedeno v následující kapitole. Byly zvoleny právě tyto jednotky, protože jsou to jediné jednotky, které jsou pro toto využití schválené SŽ. Jednotky měly zabudovaný gyroskop, který zachovává polohu svých os. Data o poloze os byla neustále posílána do integračního koncentrátoru, kde se shromažďují a následně posílají na integrační server dálkové diagnostiky. Na integrační server jsou napojena klientská pracoviště a pomocí webového rozhraní mají přehled o svých jednotkách a datech. Pomocí SW filtru jsou odstraněna data, která mohou způsobovat falešné poplachy, u trakčního vedení např. působením silnějšího větru nebo průjezdem vlaku.

4 Architektura

Architektura ukazuje technologie, které patří do IoT a jak jsou tyto technologie mezi sebou propojeny. Architektura se v tomto případě skládá z těchto částí:

- FlexiCube jednotky

  Jedná se o nejnižší část architektury. Jsou to víceméně senzory, které sbírají data v reálném čase.

- Poskytovatel NarrowBand IoT

  Data musí být po nějaké síti přenesena k diagnostikování, k tomu slouží právě NB IoT.

- FlexiCube GateWay

  Bránu můžeme brát jako centrum IoT zařízení. Slouží k propojení jednotek FlexiCube s koncovým zařízením, tedy DDTS.

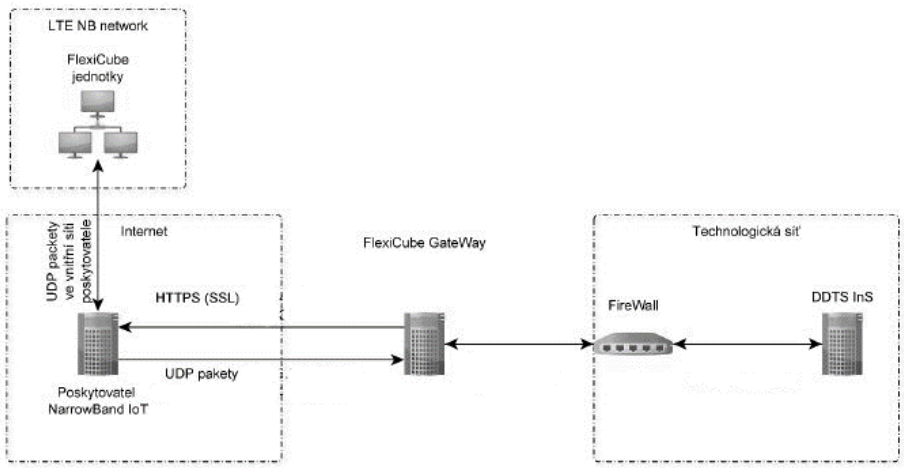
- DDTS

  Nejvyšší vrstvou architektury je DDTS. Je zodpovědný za vyhodnocování naměřených dat, ovládání technologických systémů a zaručení provozuschopnosti na železnici. Součástí DDTS je Firewall, který filtruje komunikaci.

Všechny části jsou podrobněji popsány v dalších kapitolách. O kapitolu níže je popsána komunikace, včetně grafického zobrazení propojení jednotlivých částí architektury.

4.1 Popis komunikace

Schéma komunikace



Obrázek 7. Schéma komunikace [9]

Popis komunikace

Jednotky FlexiCube NB komunikují obousměrně se serverem poskytovatele LTE NB připojení v rámci jeho uzavřené sítě pomocí UDP packetů v určených časových intervalech metodou request – response (požadavek – odpověď).

UDP packet z jednotky je ze serveru poskytovatele s pevně danou IP přesměrován na danou veřejnou IP adresu a port FlexiCube Gateway. Packety z jiné zdrojové IP nebo na jiném cílovém portu nejsou přijaty. Zde je packet zpracován a odeslán na integrační server DDTS.

Zpětné povely a nastavení pro jednotky jsou z integračního serveru předány na FlexiCube Gateway, kde dojde ke zpracování a odeslání HTTPS protokolem na server poskytovatele s pevně danou IP adresou. Server poskytovatele data předá jako UDP packet zpět jednotce FlexiCube NB. Z principu fungování IoT zařízení nejsou data do jednotek předávána okamžitě, ale až jako odpověď na obdrženou zprávu z jednotky v určeném časovém intervalu. [9]

V dalších podkapitolách jsou popsány jednotlivé komponenty.

4.2 Jednotka FlexiCube

Popis

Jednotka FlexiCube je navržena jako nízkonákladové a nízkoenergetické zařízení postavené na technologii přenosové sítě NarrowBand IoT. Zařízení slouží k monitoringu a ovládání vybraných informací jako jsou měření teploty a vlhkosti, detekce pohybu, informace o poloze (GPS), stavové informace (otevření dveří, okna, poklopu apod.), detekce zaplavení, zakouření prostoru, měření výšky hladiny v nádrži, řece apod. Zařízení je dostupné ve variantě pro vnitřní i venkovní použití.
Mezi základní konfigurace zařízení FlexiCube patří:

- Zabezpečení pomocí PIR senzoru a magnetického kontaktu
- Sběr a ovládání binárních a analogových signálů (např. výpadek jističe apod.)
- Měření parametrů prostředí – teplota, vlhkost, CO2
- Řízení vytápění – regulace elektrického topení na nastavitelnou teplotu dle časového kalendáře
- Hlídání zaplavení
- Hlídání zakouření prostoru (certifikovaný kouřový senzor)
- Dálkový odečet spotřeby energie (např. elektroměr)

• Hlídání polohy (např. pozice vagonu)

Zařízení FlexiCube vyžaduje pro zajištění plné funkčnosti vložené 2 baterie 3,6 V DC nebo napájení v rozsahu 4,5-10V DC s rozsahem pracovních teplot -20 °C až +60 °C. Pro předávání dat do nadřazených systémů je dále požadována vložená a aktivovaná SIM karta operátora NarrowBand sítě pro zajištění síťové konektivity.
Zařízení FlexiCube se skládá z HW a SW části. HW část je tvořena samotnou jednotkou FlexiCube a senzory dle typu využití. SW část je tvořena firmwarem jednotky FlexiCube zajišťujícím požadovanou funkcionalitu zařízení.

Konstrukce

Zařízení FlexiCube je umístěno v UV odolném plastovém krytu zajišťujícím krytí IP67 pro použití jak ve vnitřním, tak venkovním prostředí. Výrobní údaje jsou uvedeny na výrobním štítku, který je nalepen na vnějším plášti zařízení (na spodní straně). Na každém kusu zařízení FlexiCube jsou uvedeny údaje:

- Označení typu
- Výrobní číslo
- Značku CE [10]

Obrázek 8. Jednotka FlexiCube [10]

4.3 Poskytovatel NarrowBand IoT

Poskytovatelem NB-IoT sítě je v České republice operátor Vodafone. Dostupnost signálu je na 100% území České republiky a sahá i na těžko přístupná místa nebo pod zem.

4.4 FlexiCube Gateway

Popis

Zařízení FlexiCube Gateway je soubor technických prostředků a software realizující sběr a ovládání informací z koncových zařízení komunikujících prostřednictvím sítě NarrowBand, Sigfox či prostřednictvím API poskytovatele dat. Zařízení FlexiCube Gateway následně informace zpracovává, archivuje a předává prostřednictvím interního API do nadřazených systémů.

Zařízení FlexiCube Gateway vyžaduje pro zajištění plné funkčnosti napájení 230 V AC s rozsahem pracovních teplot 15 °C až +35 °C. Požadavkem je dále síťová internetová konektivita pro sběr dat z koncových zařízení a síťová konektivita ve směru předávání dat nadřazenému systému, a to minimálně Ethernet 100 Mbit.

Zařízení FlexiCube Gateway se skládá z HW a SW části. HW část je tvořena PC serverového typu v 19“ provedení nebo virtuální session v rámci virtualizačního serveru. SW část je dělena na část operačního systému, aplikace a podpůrných SW modulů, umožňujících požadovanou činnost systému, servisní práce a vzdálenou servisní a dohledovou činnost přístupem.

Zařízení FlexiCube Gateway je navržen na platformě PC serverového typu v 19“ provedení. Požadavek na hloubku skříně je min. 1000 mm, maximální výška 2U. Jádro tvoří výkonný procesor s parametry min. 4-jádra, 3GHz. Operační paměť je tvořena moduly s min. kapacitou 32 GB. Server je osazen min. 2 síťovými rozhraními Ethernet 100Mbit a HDD min. 250 GB.

Variantně lze využít virtualizované prostředí virtualizačního serveru. Minimální parametry pro virtuální session jsou výkon odpovídající procesoru min. 2x 4-jádra, 3GHz, 32GB operační paměti, HDD min. 250GB, síťové rozhraní Ethernet min. 100Mbit.

Konstrukce

Na zařízení FlexiCube Gateway jsou uvedeny jednoznačné popisy všech svorek a konektorů. Výrobní údaje jsou na výrobním štítku, který je nalepen na vnějším plášti zařízení (většinou na boční straně).

Software

Na zařízení FlexiCube Gateway je povoleno provozovat pouze aplikaci výrobce spolu s jejími nadstavbami a nezbytným SW pro servisní činnost a vzdálenou správu a dohled. Komunikační drivery jsou brány jako součást aplikace.

Operační systém

Na zařízení FlexiCube Gateway je provozován operační systém Linux zajišťující přístup k HW prostředkům, standardní GUI, TCP služby a základní prostředí pro podpůrné aplikační prostředky a aplikaci.

Aplikace

Základem aplikace je prostředí FlexiPortal. Vlastní aplikace zajišťuje obousměrnou komunikaci s koncovými zařízeními a s nadřazeným systémem, zejména přenos stavových dat, měřených hodnot, ovládání a zadávání parametrů.
Aplikace zařízení FlexiCube Gateway dále zabezpečuje archivaci stavových a měřených hodnot s časovou značkou. Archivace je zabezpečena v délce min. 1 rok.
Jádro aplikace tvoří následující moduly, které běží jako nezávislé procesy:

- moduly pro komunikaci s koncovými zařízeními
- modul archivace
- modul pro komunikaci s nadřazenými systémy (interní API)
- modul interní diagnostiky
- modul vzdáleného servisu a dohledu (VNC)
- modul lokálních (servisních) obrazovek
- modul synchronizace času (NTP)
- modul pro zasílání SMS a e-mailových zpráv prostřednictvím SMS gateway a e – mailového serveru [11]

Servisní přístup na FlexiCube Gateway je možný pouze pomocí povolované drážní VPN s otevřeným portem.

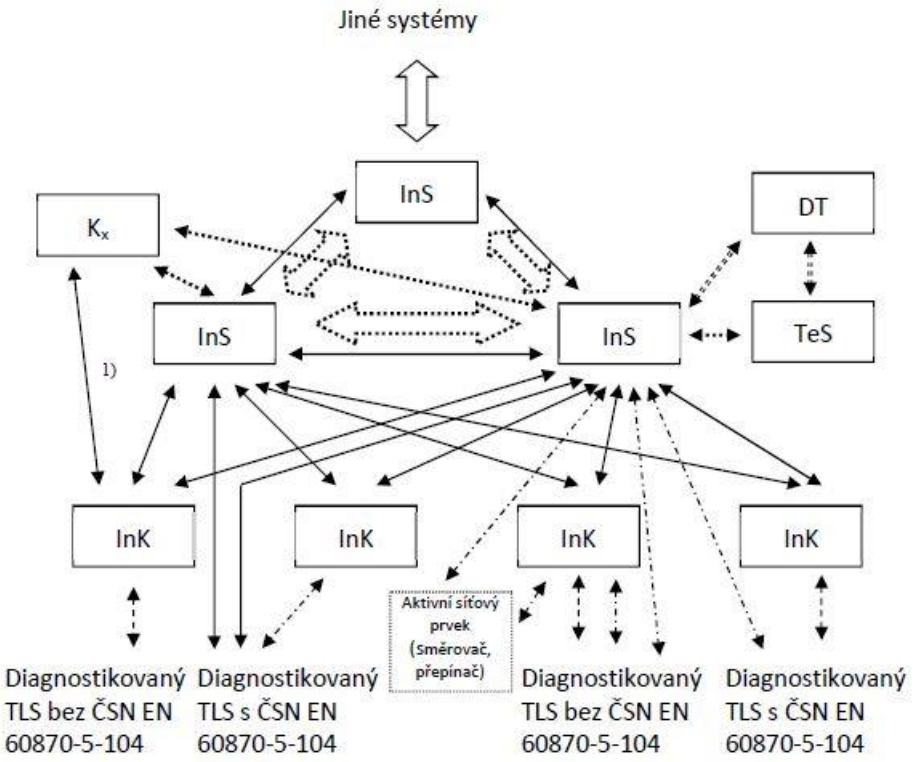
4.5 Firewall

HW firewall v rámci technologické sítě filtruje komunikaci mezi FlexiCube Gateway a InS na provoz pouze na určitém portu a příslušných IP adresách. SW firewall na FlexiCube Gateway filtruje komunikace vnějšího rozhraní. [9]

4.6 Dálková diagnostika TLS

Systém dálkové diagnostiky TLS se skládá z integračních diagnostických serverů, integračních koncentrátorů, terminálových serverů, klientů InS nebo TeS (včetně mobilních), které tvoří součásti systému dálkové diagnostiky TLS, a přenosového systému včetně lokálních technologických datových sítí. Struktura součástí systému dálkové diagnostiky TLS je uvedena na obr. 8.

Jak už bylo zmíněno výše, systém slouží k přenosu informací, ovládání technologických systémů a zajištění provozuschopnosti na železnici. Dálková diagnostika využívá k měření dat FlexiCube jednotky. Pomocí FlexiCube GateWay jsou data přenášena do DDTS. DDTS využívá IoT ve všech směrech, počínaje senzory, ovládáním systémů konče.



Obrázek 9. Struktura a protokoly dálkové diagnostiky TLS [8]

Data z technologických systémů jsou shromažďována v integračních koncentrátorech. Ty jsou připojeny do integračních serverů. Na integrační servery jsou připojeny klientská pracoviště a dispečerské terminály.

Technologické systémy nevyžadují rychlou odezvu na události, avšak zaznamenání vzniku události nesmí překročit více jak 2 minuty. Mezi technologické systémy patří např.:

- Elektrický ohřev výměn (EOV)
- Osvětlení železničních stanic a zastávek (OSV)
- Autonomní stabilní hasicí zařízení (ASHS)
- Zařízení pro detekci požáru (ZPDP)
- Poplachové zabezpečovací a tísňové systémy (PZTS)
- Informační systémy pro cestující – vizuální (ISC)
- Informační systémy pro cestující – hlasové (ROZ)
- Kamerové systémy (KAMS)
- Elektrická předtápěcí zařízení (EPZ)

Informace z jedné dálkově kontrolované oblasti na trati NŽK jsou uloženy nejméně ve dvou integračních serverech, které jsou umístěny geograficky odlišně. Jeden z těchto integračních serverů musí být na CDP a druhý nějaký místně příslušný integrační server (Pardubice, Ústí nad Labem, Plzeň, České Budějovice, Brno, Ostrava). Informace jsou uloženy v SQL databázích. Údaje musí být v integračních serverech archivovány nejméně 60 dnů. Po této době mohou být uloženy na vhodném paměťovém médiu, kde musejí být k dispozici po dobu nejméně 1 roku.

Integrační koncentrátory jsou umístěny v železničních stanicích. V každé stanici může být maximálně jeden integrační koncentrátor. Integrační koncentrátor také musí být umístěn v každé odbočné železniční stanici. Musí být umístěn blízko přenosovému zařízení technologické datové sítě.
Každý integrační koncentrátor je řešen na bázi průmyslového počítače bez pohyblivých částí. Podmínkou je paměť, která uchovává záznam po 12 hodin pro případ výpadku. Koncentrátor nesmí obsahovat monitor ani klávesnici. [8]

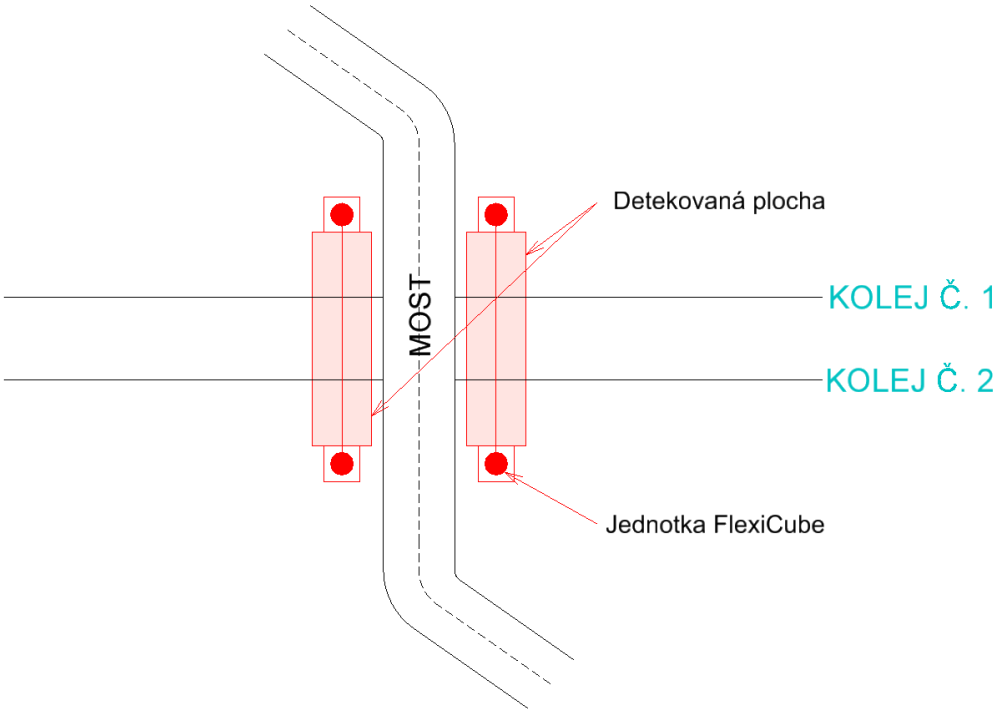
5 Způsoby využití IoT na železnici a návrh konkrétního systému

V této kapitole jsou nejdříve popsány různé možnosti, jak může být technologie IoT využita na železnici. Každý způsob je stručně popsán z funkčního hlediska. U některých způsobů využití se mi podařilo získat data, ty jsou u jednotlivých způsobů přiložena.
Dále je zde kapitola, která obsahuje můj vlastní návrh systému, který se zabývá kontrolou vstupu do tunelu. Systém je detailněji popsán a následně finančně vyčíslen. Systém může být použit např. na připravované stavbě VRT Praha-Běchovice – Poříčany, ale lze ho využívat i na konvenčních tratích.

5.1 Možnosti využití jednotky FlexiCube v rámci IoT na železnici

Detekce pádu vozidla z mostu do kolejiště

Tento systém je velmi využívaný v úsecích, kterými vede trať pod silničním mostem, kde hrozí pád vozidla do kolejiště. Z tohoto důvodu se pod most umísťují detektory s pohybovým čidlem, které kontrolují jakýkoliv pohyb v kolejišti pod mostem. Detektory mají vymezený úsek, ve kterém mohou vozidlo snímat. Schéma provedení je vyobrazeno na obr. 9. Tento způsob detekce je také velmi využívaný např. ve Francii. Jednotka FlexiCube ve spolupráci s pohybovým čidlem, které reaguje na pohyb, neustále sbírá informace. Ve chvíli, kdy je detekováno narušení oblasti, je informace přes GateWay poslána na integrační server DDTS. Dispečer je nucen situaci neprodleně řešit. Musí dojít k odklonu vlaku, jestli je to možné, pokud ne, tak dochází k zastavení jízdy vlaku do doby, než bude cesta průjezdná.



Obrázek 10. Schéma provedení detekce pádu vozidla do kolejiště [vlastní]

Detekce sesuvu půdy

Jelikož samotná jednotka obsahuje gyroskop, je možné ji použít k detekci sesuvu půdy. Jednotky jsou rozmístěné ve vzdálenosti 10 metrů od sebe. Jednotky neustále odesílají data o poloze os gyroskopu do DDTS. Jakmile dojde ke větší změně polohy osy gyroskopu, provoz na trati musí být okamžitě zastaven, popřípadě vlaky odkloněny, pokud je to možné. Na místo jsou povoláni pracovníci SŽ, aby situaci zkontrolovali. Ve chvíli, kdy bude situace v pořádku, může být provoz na trati obnoven.

Zabezpečení trakčního vedení

Jednotka FlexiCube je spolu se senzorem umístěna na trakčním vedení, viz obr. 9 a 10. Senzor má v sobě zabudovaný akcelerometr. Jednotka neustále odesílá data o orientaci akcelerometru. Pokud dochází k velikému vychýlení orientace, znamená to, že došlo k manipulaci s trakčním vedením. Data jsou přes GateWay posílána do DDTS. Jsou vyfiltrována data menšího vychýlení, která vznikají např. vlivem větru. Jakmile dojde k velkému

vychýlení, jsou do akce povolány bezpečnostní jednotky a provoz na trati je omezen, v ojedinělých případech dokonce zastaven.

Obrázek 11 a 12. Umístění jednotky na trakčním vedení [Firma Intesys]

Tento způsob využití jednotky FlexiCube byl ověřen také ověřen v praxi. Dále je popsán průběh měření a data, která při měření vznikla.

Postup měření:

Jednotka byla pro účely ověření instalována na trakčním vedení. V rámci instalace bylo zvoleno nejvhodnější místo pro optimální detekci. Senzor, který zde byl umístěn spolu s jednotkou funguje na základě vestavěného akcelerometru a magnetického senzoru.

Průběh měření:

Měření probíhalo v červnu tohoto roku. Probíhalo po celý měsíc, kdy jednotka dvakrát denně posílala data na server. Nadřazeným prvkem serveru je dohledový portál FlexiPortal, ze kterého byl vytvořen csv soubor s daty níže. V tomto portálu má klient přehled o všech svých jednotkách i informacích, které jednotky poskytují (GPS, orientace, náklon, teplota, vlhkost, kontakt, vzdálenost…).

V jednotlivých sloupcích vygenerovaného csv souboru můžeme vidět různá data (platí pro tabulky 1 a 2).

- Sloupec A (Hardware id) – V tomto sloupci je uvedeno id hardwarové jednotky, která byla použita, jelikož se jednotka neměnila, tak je v každém řádku stejné číslo.
- Sloupec B (Datum a čas) – Data byla obdržena vždy 2x za den, po 12 hodinách. Pokud ale došlo ke změně orientace jednotky, byla data přenášena do doby, než se jednotka vrátila do původní polohy.
- Sloupec C (Úroveň napětí baterie) – V tomto sloupci je uvedeno napětí baterie, které se po dobu měření nezměnilo a jeho hodnota byla 3 V.
- Sloupec D (Orientace) – Tento sloupec popisuje, jakým směrem byla jednotka orientována. Zde bylo 6 možností orientace (naplocho – standartní poloha, obráceně, nahoru, dolu, doleva, doprava).
- Sloupec E (Náklon X) – V tomto sloupci je uvedena číselná hodnota, o kolik stupňů je jednotka vychýlena v ose X. Do 5 stupňů bylo vychýlení přičítáno počasí. Pokud se jednotka vychýlila o více, jak 5 stupňů přišla alarmující zpráva.
- Sloupec F (Náklon Y) – V tomto sloupci jsou podobná data jako pro sloupec F, akorát jsou zaměřena na náklon v ose Y.
- Sloupec G (Interní teplota) – Tento sloupec je v tomto případě pro vyhodnocení dat irelevantní. Je v něm uvedena teplota ve stupních Celsia.
- Sloupec H (Důvod zprávy) – Tento sloupec nás zajímá nejvíce. Mohli zde být vypsány 3 možnosti. V případě klidného stavu se vypsalo slovo „Čas.“ Když došlo k vychýlení nad rámec tolerovaných stupňů, vypsalo se slovo „Alarm.“ Toto slovo se vypsalo také, když došlo k navrácení jednotky do původní polohy, jako konec alarmové situace. V průběhu alarmové situace se přenášela data pod výrazem „Info,“ což označovalo, orientaci jednotky v průběhu alarmové situace.

Jak už jsem zmiňoval, tak měření započalo 1.6. První alarmová situace byla zaznamenána 7.6. v 13:15, viz Tabulka 1. Z tabulky můžeme vidět, že došlo k vychýlení orientace jednotky směrem doleva. Do minuty byla jednotka orientována zpátky do původní polohy, tedy naplocho.

1	Datum a čas	Úroveň napětí baterie	Orientace	Náklon X [°]	Náklon Y [°]	Interní teplota [°C]	Důvod zprávy
50	09.06.2022 21:28	3	naplocho	-2	-3	16	Čas
51	09.06.2022 9:28	3	naplocho	-3	-5	27	Čas
52	08.06.2022 21:28	3	naplocho	-2	-3	16	Čas
53	08.06.2022 9:28	3	naplocho	-3	-3	15	Čas
54	07.06.2022 21:28	3	naplocho	-3	-4	14	Čas
55	07.06.2022 13:15	3	naplocho	-3	-6	40	Alarm
56	07.06.2022 13:15	3	naplocho	-3	-6	39	Info
57	07.06.2022 13:15	3	doleva	-15	72	40	Alarm
58	07.06.2022 9:28	3	naplocho	-4	-4	31	Čas
59	06.06.2022 21:28	3	naplocho	-1	-4	15	Čas
60	06.06.2022 9:29	3	naplocho	-3	-4	22	Čas
61	05.06.2022 9:28	3	naplocho	-4	-4	26	Čas
62	04.06.2022 21:28	3	naplocho	-2	-4	15	Čas
63	04.06.2022 9:29	3	naplocho	-3	-4	21	Čas
64	03.06.2022 21:29	3	naplocho	-1	-4	17	Čas
65	03.06.2022 9:29	3	naplocho	-3	-4	25	Čas
66	02.06.2022 21:29	3	naplocho	-2	-2	12	Čas
67	02.06.2022 9:29	3	naplocho	-3	-3	20	Čas
68	01.06.2022 21:29	3	naplocho	-1	-4	14	Čas
69	01.06.2022 9:29	3	naplocho	-3	-4	24	Čas

Tabulka 1. První zaznamenání alarmové situace

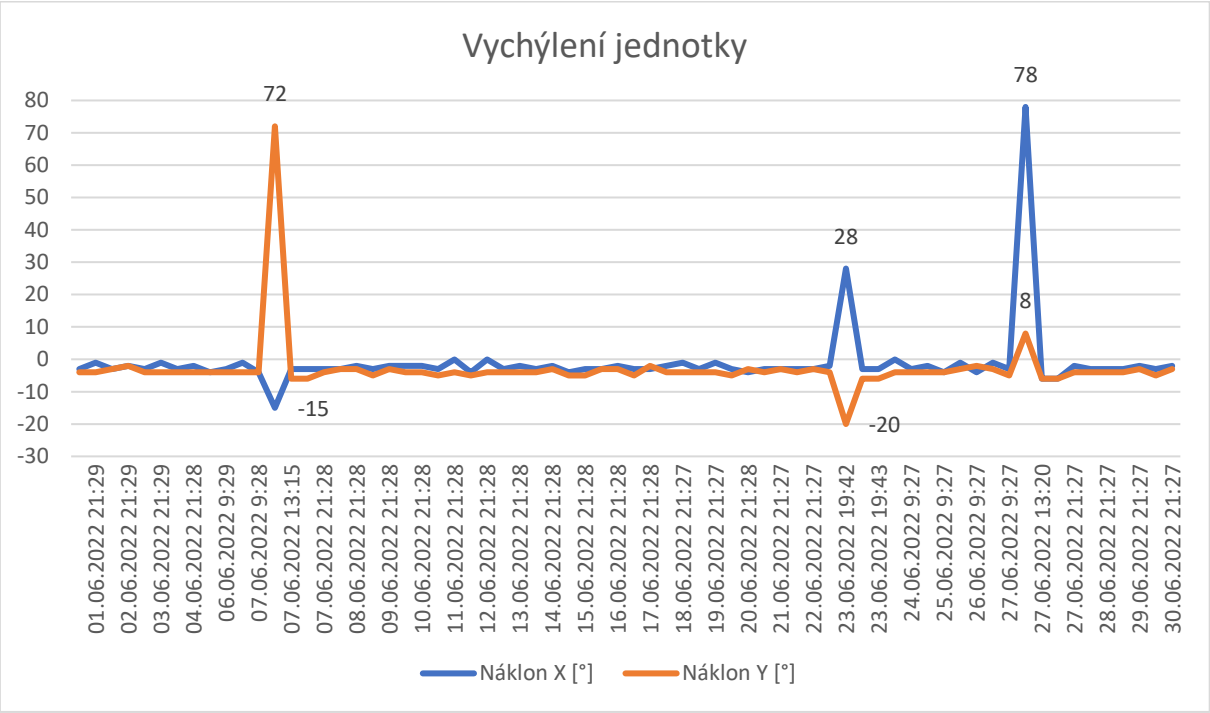
Do konce měsíce byly zaznamenány další dvě alarmové situace, a to ve dnech 23.6. a 27.6. V obou případech došlo k vychýlení jednotky orientace ve směru dolů. Ale opět byla jednotka do jedné minuty v původní poloze. Obě alarmové situace jsou k vidění v tabulce 2.

1	Datum a čas	Úroveň napětí baterie	Orientace	Náklon X [°]	Náklon Y [°]	Interní teplota [°C]	Důvod zprávy
2	30.06.2022 21:27	3	naplocho	-2	-3	24	Čas
3	30.06.2022 9:27	3	naplocho	-3	-5	33	Čas
4	29.06.2022 21:27	3	naplocho	-2	-3	22	Čas
5	29.06.2022 9:27	3	naplocho	-3	-4	24	Čas
6	28.06.2022 21:27	3	naplocho	-3	-4	18	Čas
7	28.06.2022 9:27	3	naplocho	-3	-4	23	Čas
8	27.06.2022 21:27	3	naplocho	-2	-4	23	Čas
9	27.06.2022 13:20	3	naplocho	-6	-6	40	Alarm
10	27.06.2022 13:20	3	naplocho	-6	-6	39	Info
11	27.06.2022 13:19	3	dolu	78	8	40	Alarm
12	27.06.2022 9:27	3	naplocho	-3	-5	38	Čas
13	26.06.2022 21:27	3	naplocho	-1	-3	21	Čas
14	26.06.2022 9:27	3	naplocho	-4	-2	33	Čas
15	25.06.2022 21:27	3	naplocho	-1	-3	20	Čas
16	25.06.2022 9:27	3	naplocho	-4	-4	30	Čas
17	24.06.2022 21:27	3	naplocho	-2	-4	22	Čas
18	24.06.2022 9:27	3	naplocho	-3	-4	32	Čas
19	23.06.2022 21:27	3	naplocho	0	-4	16	Čas
20	23.06.2022 19:43	3	naplocho	-3	-6	23	Alarm
21	23.06.2022 19:43	3	naplocho	-3	-6	22	Info
22	23.06.2022 19:42	3	dolu	28	-20	22	Alarm
23	23.06.2022 9:27	3	naplocho	-2	-4	32	Čas
24	22.06.2022 21:27	3	naplocho	-3	-3	15	Čas
25	22.06.2022 9:27	3	naplocho	-3	-4	28	Čas

Tabulka 2. Druhá a třetí alarmová situace

V případě, že by došlo k výpadku komunikace mezi jednotkou a serverem, tak by ve sloupci „Důvod zprávy“ byl uveden „výpadek,“ ale to se po celý měsíc nestalo, tudíž můžeme považovat jednotku za funkční.

V následujícím grafu jsem přehledně vyobrazil, kdy došlo k vychýlení orientace jednotky, v jaké ose a o kolik stupňů.



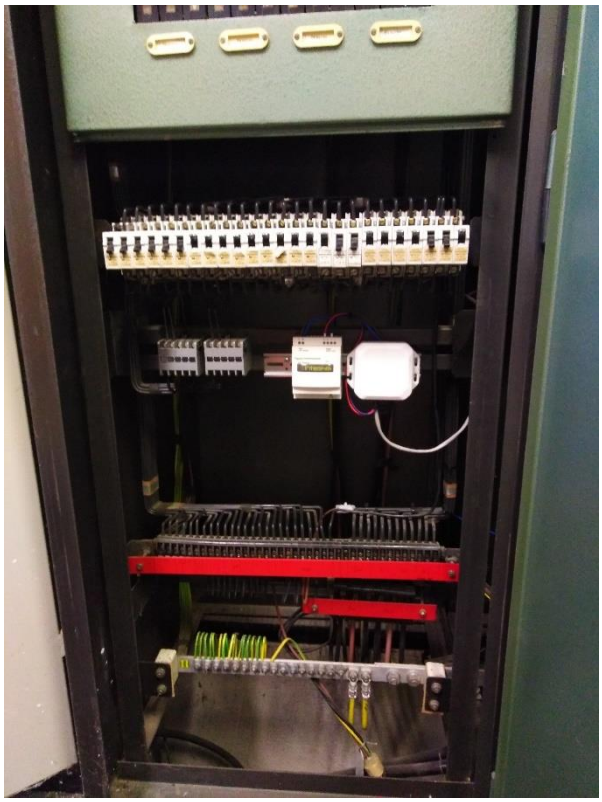
Graf 1. Vyobrazení jednotlivých vychýlení orientace jednotky

Vyhodnocení dat:

Během ověřovacího provozu nebyla zjištěna žádná nefunkčnost či výpadek zařízení. Po dobu ověření zařízení vykazovalo občasné alarmové detekce, které můžeme popsat jako změnu orientace. Vzhledem k jejich velmi krátkému času působení je však jejich výskyt přičítán fyzikální podstatě fungování senzoru detekující změnu orientace. Ten funguje na základě vestavěného akcelerometru a magnetického senzoru a vlivem prudkých manipulací může krátkodobě vykazovat falešné hodnoty. Po ustálení již však spolehlivě předává korektní data. Prudkým rozkmitání trakčního vedení z důvodu průjezdu vlaku či silnějšího větru tak může docházet k falešnému alarmovému hlášení. Vhodným filtrem v SW, který zpracovává naměřená data, však lze spolehlivě tyto falešné detekce odstranit. Měření tak prokázalo vhodnost použití zařízení pro hlídání trakčního vedení proti neoprávněné manipulaci, resp. krádeži.

Odečet elektroměrů

Jednotka je umístěna v elektroměru. Elektroměry komunikují pomocí sběrnice RS485. Jednotka je napájena z 230V zdroje. Jednotka neustále sbírá informace a 1x za hodinu je předává na GW a do DDTS, která data vyhodnocuje.



Obrázek 13 a 14. Umístění jednotky v elektroměru [Firma Intesys]

Zabezpečení čekárny

V této situaci je jednotka osazena na dveře nebo okna. Funkcí jednotky je zabezpečení prostoru s ovládáním zamykání. Napájecí jednotka je umístěna u ústředny EZS s možností připojení zámků dveří. Pro zabezpečení vstupu do čekárny lze využít magnetický kontakt na dveře nebo okna. Jakmile dojde k porušení magnetického kontaktu, jednotka vyšle signál do DDTS.

Přejezdové zabezpečovací zařízení

Jednotka je umístěna do technologického domku u přejezdu v ŽST Podivín. Jednotka je osazena požárním čidlem a záplavovým senzorem. Jednotka je bateriově napájena.
Pro detekci požáru byl použit kouřový senzor a pro detekci zaplavení záplavový senzor s plováčkem. Jednotka neustále odesílá data přes GW do DDTS, která informace vyhodnocuje. Pokud je v technologickém domku detekován kouř anebo zaplavení, je okamžitě do akce povolán hasičský záchranný sbor. [13]

Obrázek 15 a 16. Umístění jednotky s požárním čidlem [Firma Intesys]

Obrázek 17. Umístění jednotky se záplavovým senzorem [Firma Intesys]

Způsob detekce požáru a zaplavení přejezdového zabezpečovacího zařízení byl ověřen i v provozu. Dále je popsán postup měření a získaná data při měření.

Postup měření:
Přejezdová jednotka byla pro účely ověření instalována v technologickém (přejezdovém) domku v ŽST Podivín. V rámci instalace v objektu bylo zvoleno nejvhodnější umístění pro optimální detekci v případě zaplavení, resp. požáru (viz obrázky 15-17). Během doby ověření byly provedeny kontrolní testy funkčnosti zařízení simulací, tzn. v případě zaplavení přizvednutím plováčku a v případě kouřového senzoru generováním kouře z elektronické cigarety a testovacím tlačítkem kouřového senzoru. V následující tabulce je uveden náhled na získaná data.

Průběh měření:
Měření probíhalo v říjnu tohoto roku. Probíhalo po celý měsíc, kdy jednotka dvakrát denně posílala data na server. Nadřazeným prvkem serveru je dohledový portál FlexiPortal, ze kterého byl vytvořen csv soubor s daty níže. V tomto portálu má klient přehled o všech svých jednotkách i informacích, které jednotky poskytují (GPS, orientace, náklon, teplota, vlhkost, kontakt, vzdálenost…).

V jednotlivých sloupcích vygenerovaného csv souboru můžeme vidět různá data (platí pro tabulky 3 a 4).

- Sloupec A (Hardware id) – V tomto sloupci je uvedeno id hardwarové jednotky, která byla použita, jelikož se jednotka neměnila, tak je v každém řádku stejné číslo.
- Sloupec B (Datum a čas) – Data byla obdržena vždy 2x za den, po 12 hodinách. Pokud ale došlo k alarmové situaci, tak byla data odesílána v rozsahu pár minut, do té doby, dokud neskončila alarmová situace.
- Sloupec C (Úroveň napětí baterie) – V tomto sloupci je uvedeno napětí baterie, které se po dobu měření měnilo v rozsahu 1V – 3V.
- Sloupec D (Zaplavení) – Tento sloupec ověřuje funkčnost senzoru zaplavení. V datech můžeme vidět simulaci přizvednutím plováčku, která je vyjádřena hodnotou 0. Po simulaci je do jedné minuty uvedena hodnota 1, což ověřuje funkčnost senzoru.
- Sloupec E (Interní teplota) – V tomto sloupci je uvedena hodnota teploty ve stupních Celsia v technologickém domku. Teplota se po celou dobu měření nezměnila a činila 25° Celsia.
- Sloupec F (Požární alarm) – V tomto sloupci si můžeme ověřit, zda došlo ke spuštění požárního alarmu po detekování kouře z elektronické cigarety nebo testovacím tlačítkem kouřového senzoru. Hodnota 1 vyjadřuje spuštění požárního alarmu a hodnota 0 udává klidný stav.
- Sloupec G (Test požárního senzoru) – Zde je vyjádřeno, zda došlo k testu požárního alarmu pomocí testovacího tlačítka kouřového senzoru. Hodnota 1 vyjadřuje spuštění testu požárního senzoru a hodnota 0 vyjadřuje klidný stav. Test požárního senzoru vždy předchází požárnímu alarmu.
- Sloupec H (Důvod zprávy) – V tomto sloupci být vypsány 2 možnosti. V případě klidného stavu se vypsalo slovo „Čas.“ V případě simulace některého ze senzorů docházelo k alarmovému hlášení.

K prvnímu kontrolnímu testu funkčnosti došlo 7.10. V 9:47 bylo zaznamenáno zvednutí plováčku záplavového senzoru. V 9:48 došlo k testu požárního senzoru a minutu na to byl spuštěn požární alarm. V 10:00 došlo k druhému testu požárního senzoru a dvě minuty na to byl spuštěn alarm. V 10:04 a 10:06 byly ještě provedeny dva kontrolní testy zaplavení.

1	Hardware id	Datum a čas	Úroveň napětí baterie	Zaplavení	Interní teplota [°C]	Požární alarm	Test požárního senzoru	Důvod zprávy
77	77205	09.10.2022 10:40	2	1	25	0	0	Čas
78	77205	08.10.2022 22:40	2	1	25	0	0	Čas
79	77205	08.10.2022 10:40	2	1	25	0	0	Čas
80	77205	07.10.2022 22:40	3	1	25	0	0	Čas
81	77205	07.10.2022 10:40	3	1	25	0	0	Čas
82	77205	07.10.2022 10:06	2	1	25	0	0	Alarm
83	77205	07.10.2022 10:06	3	0	25	0	0	Alarm
84	77205	07.10.2022 10:04	3	1	25	0	0	Alarm
85	77205	07.10.2022 10:04	2	0	25	0	0	Alarm
86	77205	07.10.2022 10:04	3	1	25	0	0	Alarm
87	77205	07.10.2022 10:02	2	1	25	1	0	Alarm
88	77205	07.10.2022 10:02	3	1	25	0	1	Alarm
89	77205	07.10.2022 10:01	2	1	25	0	0	Alarm
90	77205	07.10.2022 10:00	2	1	25	0	1	Alarm
91	77205	07.10.2022 9:51	3	1	25	0	0	Alarm
92	77205	07.10.2022 9:49	3	1	25	1	0	Alarm
93	77205	07.10.2022 9:48	2	1	25	0	1	Alarm
94	77205	07.10.2022 9:47	3	1	25	0	0	Alarm
95	77205	07.10.2022 9:47	2	0	25	0	0	Alarm
96	77205	06.10.2022 22:40	2	1	25	0	0	Čas

Tabulka 3. Kontrolní testy 7.10.

Druhý testovací den byl 12.10. V 10:53 bylo zaznamenáno zvednutí plováčku záplavového senzoru. V 10:54 došlo k testu požárního senzoru. Požární alarm byl spuštěn v 10:57. V 11:01 došlo k druhému testu záplavového senzoru. Minutu na to byl ještě jednou proveden test požárního senzoru a alarmu.

1	Hardware id	Datum a čas	Úroveň napětí baterie	Zaplavení	Interní teplota [°C]	Požární alarm	Test požárního senzoru	Důvod zprávy
50	77205	13.10.2022 22:40	2	1	25	0	0	Čas
51	77205	13.10.2022 10:40	2	1	25	0	0	Čas
52	77205	12.10.2022 22:40	3	1	25	0	0	Čas
53	77205	12.10.2022 11:03	2	1	25	0	0	Alarm
54	77205	12.10.2022 11:02	1	1	25	1	0	Alarm
55	77205	12.10.2022 11:02	3	0	25	1	0	Alarm
56	77205	12.10.2022 11:02	3	0	25	0	1	Alarm
57	77205	12.10.2022 11:01	3	0	25	0	0	Alarm
58	77205	12.10.2022 11:01	3	0	25	0	0	Alarm
59	77205	12.10.2022 11:01	2	0	25	0	0	Alarm
60	77205	12.10.2022 11:01	2	1	25	0	0	Alarm
61	77205	12.10.2022 10:57	2	1	25	1	0	Alarm
62	77205	12.10.2022 10:57	3	1	25	0	1	Alarm
63	77205	12.10.2022 10:56	2	1	25	0	0	Alarm
64	77205	12.10.2022 10:55	2	1	25	0	1	Alarm
65	77205	12.10.2022 10:55	2	1	25	0	0	Alarm
66	77205	12.10.2022 10:54	1	1	25	0	1	Alarm
67	77205	12.10.2022 10:54	2	1	25	0	0	Alarm
68	77205	12.10.2022 10:53	1	0	25	0	0	Alarm
69	77205	12.10.2022 10:53	2	1	25	0	0	Alarm
70	77205	12.10.2022 10:53	2	0	25	0	0	Alarm
71	77205	12.10.2022 10:40	3	1	25	0	0	Čas
72	77205	11.10.2022 22:40	3	1	25	0	0	Čas

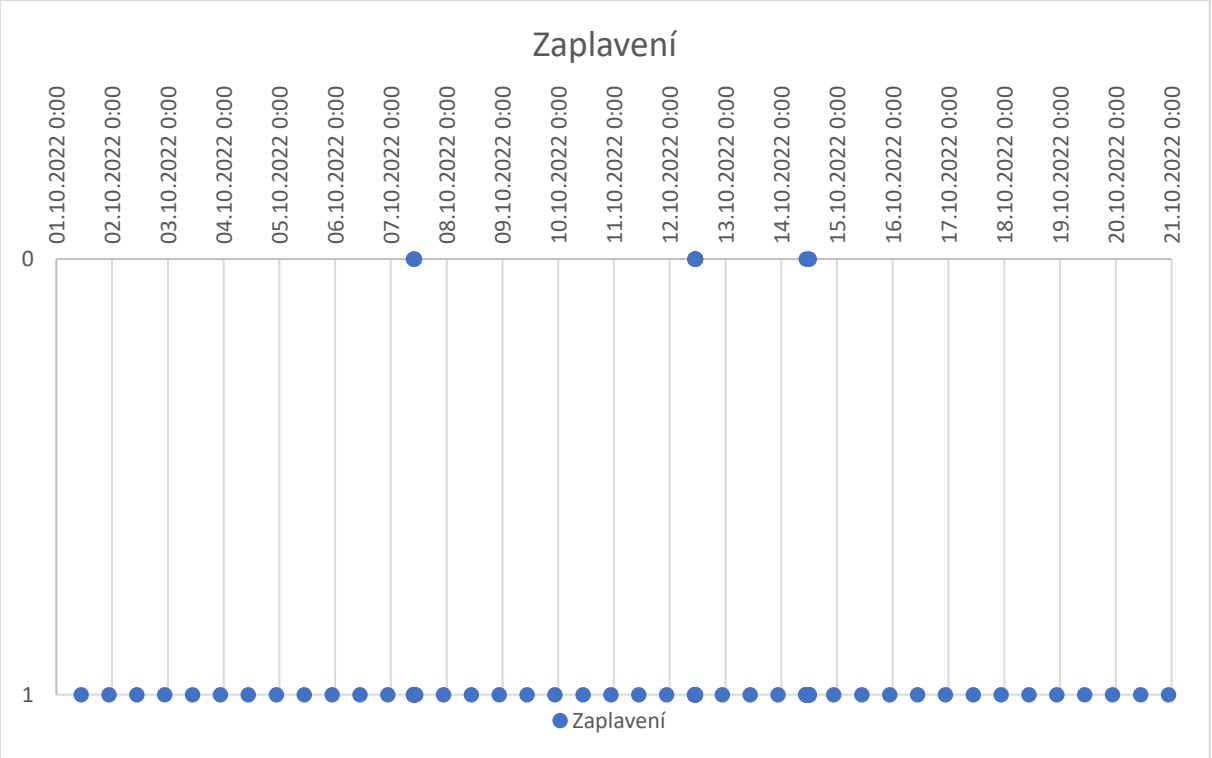
Tabulka 4. Kontrolní testy 12.10.

Posledním kontrolním dnem v měsíci bylo 14.10. Testování probíhalo obdobně jako v předchozí dva dny. Měření je vyobrazeno v následující tabulce.

1	Hardware id	Datum a čas	Úroveň napětí baterie	Zaplavení	Interní teplota [°C]	Požární alarm	Test požárního senzoru	Důvod zprávy
32	77205	15.10.2022 22:40	1	1	25	0	0	Čas
33	77205	15.10.2022 10:40	2	1	25	0	0	Čas
34	77205	14.10.2022 22:40	3	1	25	0	0	Čas
35	77205	14.10.2022 12:02	1	1	25	0	0	Alarm
36	77205	14.10.2022 12:02	3	1	25	1	0	Alarm
37	77205	14.10.2022 12:02	1	0	25	1	0	Alarm
38	77205	14.10.2022 12:01	3	1	25	1	0	Alarm
39	77205	14.10.2022 12:00	2	1	25	0	1	Alarm
40	77205	14.10.2022 12:00	3	1	25	0	0	Alarm
41	77205	14.10.2022 12:00	3	0	25	0	0	Alarm
42	77205	14.10.2022 10:51	2	1	25	0	0	Alarm
43	77205	14.10.2022 10:49	3	1	25	1	0	Alarm
44	77205	14.10.2022 10:49	3	1	25	0	1	Alarm
45	77205	14.10.2022 10:49	3	1	25	0	0	Alarm
46	77205	14.10.2022 10:48	2	1	25	0	1	Alarm
47	77205	14.10.2022 10:47	2	1	25	0	0	Alarm
48	77205	14.10.2022 10:47	2	0	25	0	0	Alarm
49	77205	14.10.2022 10:40	2	1	25	0	0	Čas
50	77205	13.10.2022 22:40	2	1	25	0	0	Čas

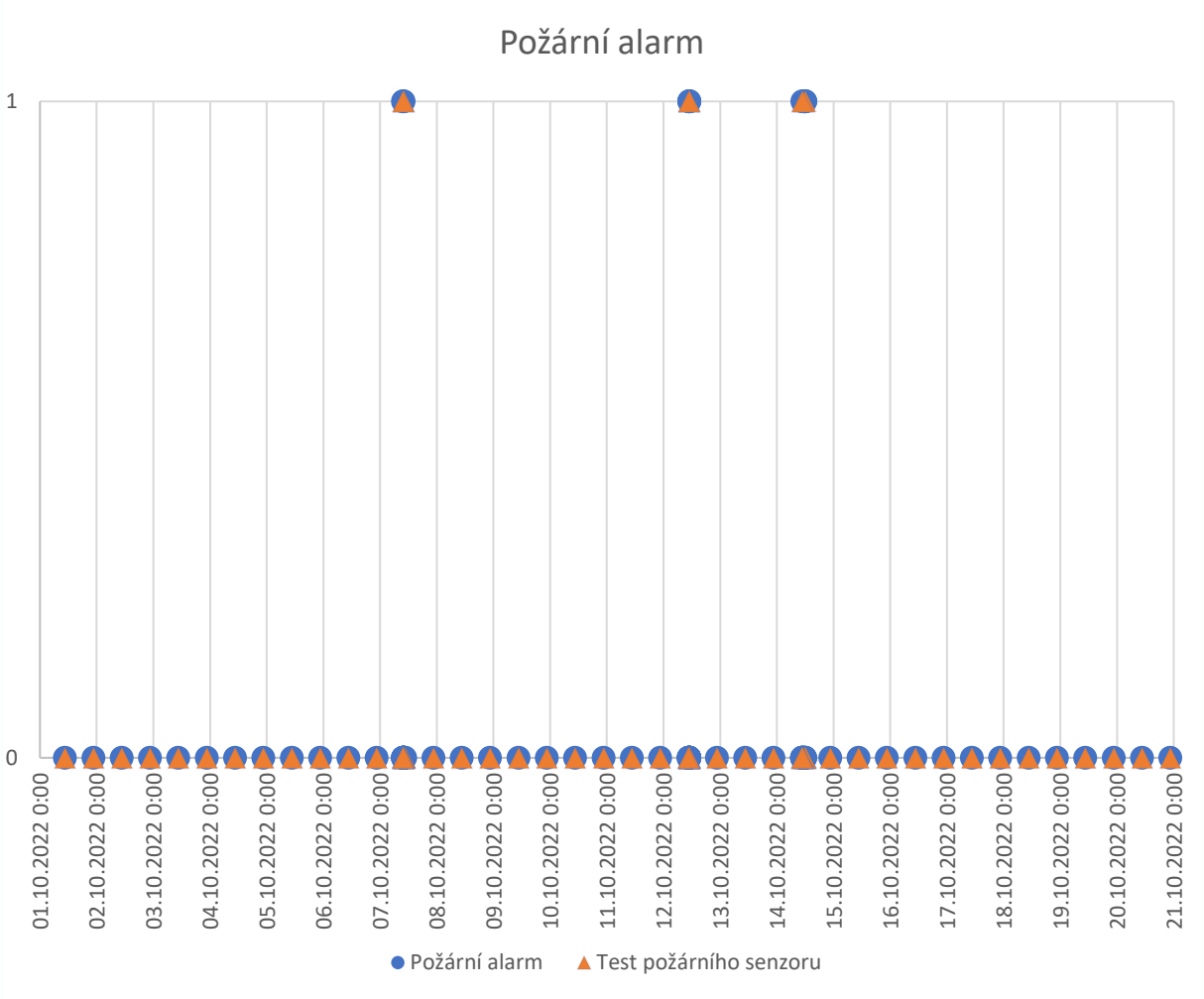
Tabulka 5. Kontrolní testy 14.10.

Následně jsem vytvořil graf, ve kterém je vidět, kdy došlo k testu záplavového senzoru. Test (nadzvednutí plováčku) je vyjádřen hodnotou 0.



Graf 2. Test záplavového senzoru

Druhý graf, který jsem vytvořil zobrazuje dny, kdy byl testován kouřový senzor. Spuštění testu je vyjádřeno hodnotou 1. Samotný test je vyobrazen žlutým trojúhelníkem a požární alarm modrým kolečkem. Z grafu je vidět, že se systém jeví jako funkční, protože se po každém testu kouřového senzoru spustil alarm.



Graf 3. Test kouřového senzoru

Vyhodnocení dat:

Během ověřovacího provozu nebyla zjištěna žádná nefunkčnost či výpadek zařízení. Po dobu ověření nedošlo sice k reálnému výskytu zaplavení ani požáru, nicméně v naměřených datech jsou korektně zaznamenány simulace zaplavení, resp. požáru. Jednotka se tak jeví jako plně funkční a jako zařízení, které je schopné plně zabezpečit funkci záplavového a požární čidla a pomocí technologie NarrowBand IoT tak efektivně předcházet případným škodám způsobeným zaplavením či požárem.

Detekce kouře v tunelu

Jednotka FlexiCube je rozmístěna po několika metrech do tunelu. Je vybavena senzorem, který neustále zaznamenává hustotu kouře. Data jsou neustále posílána přes GateWay do DDTS. Jakmile dojde k zachycení vyšší hustoty vzduchu nad povolenou mez, tunel musí být okamžitě uzavřen a vlaky do něj v žádném případě nesmí vjet. Je povolán hasičský záchranný sbor pro prověření situace. Po navrácení situace do normálu je obnoven provoz v tunelu.

Sledování polohy

Jednotka je osazena na vozidlo např. MUV. Jednotka je napájena bateriově. Zde jsou vypsány sledované funkce:

- Směr posledního pohybu (dopředný, zpětný, zrychlení, zpomalení)
- Orientace vozidla vzhledem k severu
- Poloha
- Teplota

Komunikace probíhá přes GW do DDTS, která data vyhodnocuje.

Obrázek 18. Umístění jednotky ve vozidle MUV [Firma Intesys]

Neoprávněná manipulace

Jednotku lze také využívat při monitorování neoprávněné manipulace se zařízením. Pro detekci je využíván otřesový nebo náklonový senzor. V případě použití náklonového senzoru systém funguje na obdobném principu jak v případě použití zabezpečení trakčního vedení, kdy jsou data o náklonu neustále odesílána přes GateWay do DDTS. Musí zde být určitá tolerance vychýlení, např. vlivem větru. Jakmile dojde k přijetí informace v DDTS o velkém vychýlení jednotky, došlo pravděpodobně k odcizení zařízení a v kombinace se sledováním polohy lze vypátrat, kdo jednotku odcizil. Otřesový, někdy může být zmiňován jako vibrační senzor pracuje na mechanickém, fyzikálním nebo fyzikálně chemickém principu. Ve velké většině se jedná o elektrické principy. Jako u náklonového senzoru jsou data neustále posílána přes GateWay do DDTS. [12]

Počítání lidí/aut

Jednotku lze také využívat při počítání lidí a následně analyzovat tok cestujících. Jednotky jsou umístěny do stanic, nejčastěji ke vchodu, a poté do vlaku. Data o pohybu cestujících jsou neustále přenášena přes Gateway do DDTS. Data jsou vyhodnocována a podle nich mohou být navrhovány úpravy stanic, posílení vlaků apod.

5.2 Návrh využití IoT na železnici

V této podkapitole je podrobněji popsán můj návrh, jak by mohlo být využito IoT v rámci železnice. Návrh je i finančně vyčíslen. Jedná se o monitorování vstupu do tunelů. Systém lze zařadit do kategorie varovných systémů, jelikož cílem je včasné varování dispečera při neoprávněném vstupu do tunelu. Může se stát, že se do tunelu zatoulá divoká zvěř nebo do něj neoprávněně vejde člověk, což může způsobit veliké, někdy až fatální, komplikace při průjezdu vlaku tunelem.

Na obou stranách tunelu budou umístěny jednotky FlexiCube s detektorem výšky. Detektory budou umístěny ve dvou výškách, a to 0,5 m a 2,5 m.

Každá jednotka neustále zaznamenává data o přítomnosti objektů v tunelu. Data jsou neustále posílána přes GateWay na integrační koncentrátor, který je umístěn v nejbližší železniční stanici. Zde jsou data shromažďována a poté posílána na integrační server dálkové diagnostiky. Na integrační servery jsou připojena klientská pracoviště. Veškerý přenos dat

probíhá přes Narrowband. Data jsou posílána v podobě jedniček a nul. Nula udává klidový stav neboli nedochází k narušení tunelu, naopak jednička poukazuje na to, že došlo k narušení a v tunelu se může nacházet nějaký objekt, který může zkomplikovat průjezd vlaku tunelem. V případě, že došlo k narušení prostoru tunelu, musí být vlaky odkloněny na jinou trať, pokud je to možné, v druhém případě musí být zastaven provoz na trati, než dojde k možnosti bezpečného průjezdu tunelu. O bezpečnost průjezdu se starají záchranné složky, které celou situaci řeší.

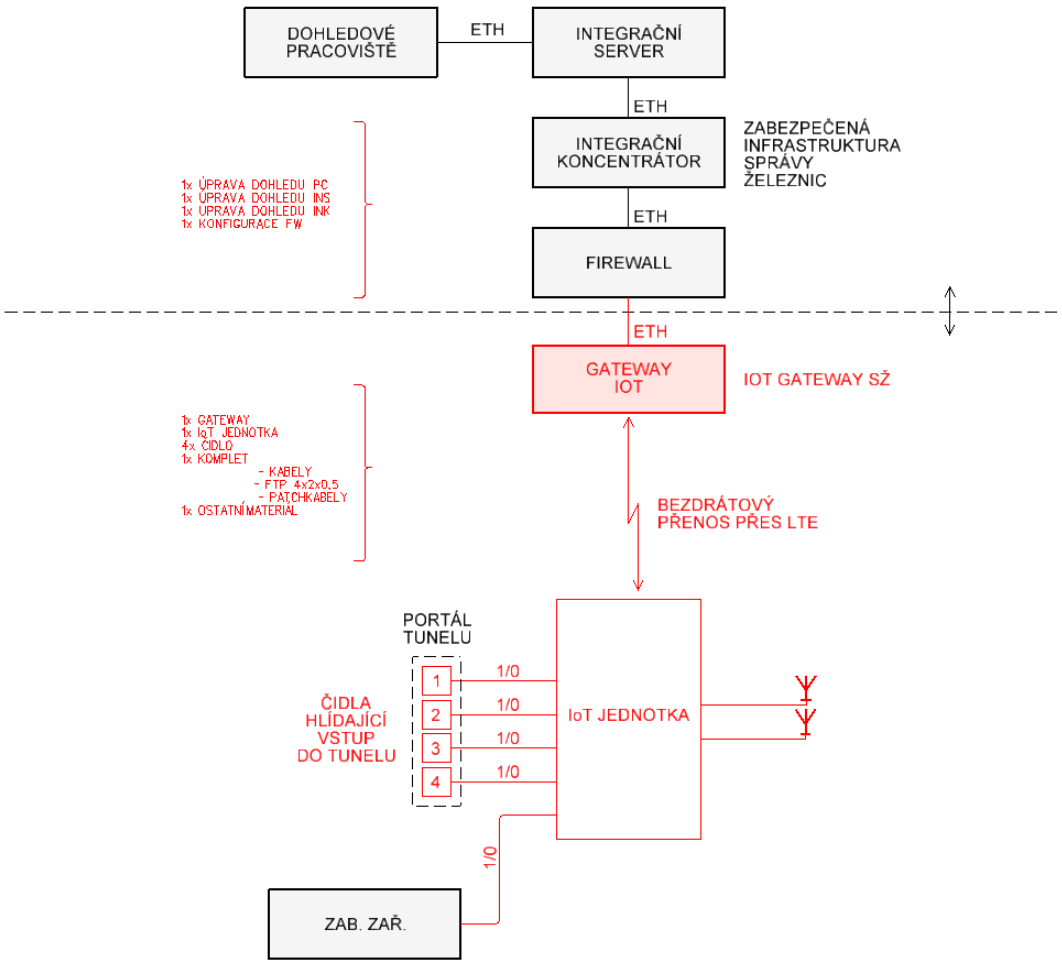
Jednotky jsou také zabezpečeny proti neoprávněné manipulaci. Každá jednotka obsahuje gyroskop, dle kterého lze rozpoznat, že došlo k manipulaci s jednotkou. Data, která jsou přenášena do integračního koncentrátu obsahují také data o poloze jednotlivých os gyroskopu. Když se změny polohy jednotlivých os, došlo k manipulaci s jednotkou. Pokud byla jednotka odcizena, lze ji pomoci GPS modulu vystopovat.

Každá jednotka je napájena bateriově, které vydrží minimálně 2 roky. V případě, kdy nejsou dispečerovi doručována žádná data po delší dobu, tak pravděpodobně došlo k vybití baterie a je potřeba jejího vyměnění.

Systém musí být nastaven tak, aby nedocházelo k falešným poplachům, a to i při samotném průjezdu vlaku tunelem, protože i ten bude zaznamenán detektory, to bude vyfiltrováno pomocí SW filtru. Systém bude nastavený tak, že jednotky budou dostávat data od zabezpečovacího zařízení na trati. Data budou přenášena v podobě jedniček a nul. Nula udává nepřítomnost vlaku a jednička obsazenost trati vlakem.

Postup měření:
Jednotka bude spolu s detektorem výšky umístěna pro účely ověření ve vybraném tunelu. V rámci instalace bude v tunelu zvoleno nejvhodnější umístění pro optimální detekci, což jsou portály tunelu. Během doby ověření budou provedeny kontrolní testy funkčnosti zařízení simulací testovacím tlačítkem výškového senzoru.

Blokové schéma:



Obrázek 19. Blokové schéma návrhu monitorování vstupu do tunelu [vlastní]

Výše je znázorněno schéma propojení jednotlivých prvků v návrhu systému. Černě je vyznačena stávající infrastruktura SŽ, která se bude pouze doplňovat softwarem, kromě zabezpečovacího zařízení. Červeně je vyznačena část, která bude součástí dodávky. Náklady jsou uvedeny níže. Vše, co bude dodáváno je vyznačeno vedle složených závorek.

Čidla, která budou umístěna u portálů tunelu jsou napojena na vstup IoT jednotek. Jako další vstup do jednotky slouží zabezpečovací zařízení. Z jednotek jsou data přes Narrowband posílána do IoT Gateway. Z Gateway jsou data posílána skrz Firewall a Integrační koncentrátor do Integračního serveru. V serveru jsou data archivována. Do integračního serveru má náhled pracovník dohledového pracoviště.

Náklady:

Náklady za návrh tohoto systému jsou uvedeny na jeden portál tunelu.

Cena zahrnuje kompletní dodávku IoT, která obsahuje 1x Gateway, 1x IoT jednotku, 4x čidlo hlídající vstup do tunelu, kabelizaci, materiál (např. chráničky) a konfiguraci stávajících zařízení, což je znázorněno ve schématu.

V nákladech jsou uvedeny i další položky, jako je školení zaměstnanců, prohlídky, zkoušky, dodávky materiálu a montáž systému.

Do budoucna už nebudou nutné žádné dodávky IoT, v případě potřeby dojde pouze k doplnění softwaru.

Celková cena za tento návrh činí cca 200 000 Kč.

Monitorování vstupu do tunelu, může být kontrolováno i pomocí jiných technologií, které ale jsou výrazně dražší. Prvním způsobem může být monitorování pomocí infrazávor. Závory jsou umístěné většinou ve třech různých výškách na začátku tunelu (v případě tří závor). Cena tohoto způsobu monitorování vstupu do tunelu se pohybuje mezi 390 000 Kč a 450 000 Kč, závisí na počtu infrazávor. V ceně je zahrnuta integrace do DDTS (InK, InS, klientská pracoviště). Cena je uvedena za jeden portál tunelu.

Druhým způsobem můžou být laserové skenery, které umožňují detekovat vstup osoby po chodnících, i při průjezdu vlaku tunelem. Velkou výhodou laserového skeneru je, že umí monitorovat v celé detekční rovině. Laserové skenery také umí detekovat rozměr objektu a mohou tedy být umístěné výše v tunelu, tím se zvýší odolnost vůči vandalismu. Cena toho způsobu monitorování vstupu do tunelu se pohybuje kolem 900 000 Kč za jeden portál tunelu. Cena zahrnuje 2ks skenerů, převodník, kabelizaci, ostatní materiál a integraci do DDTS (InK, InS, klientská pracoviště).

6 Implementace IoT pro dopravní objekty

V této kapitole jsou uvedeny příklady systémů ze světa, kde bylo IoT využito v rámci dopravy a dopravních objektů. Systémy nemusí souviset přímo se železnicí, ale mají, co dočinění s dopravou, jako takovou.

6.1 Systém monitorování bezpečnosti mostu založený na IoT

Tento systém byl vyvinut na Tchaj-wanu z důvodu velmi častého poškození mostů nebo mostních pilířů způsobené tajfunovými záplavami nebo zemětřeseními. Kromě záplav, tajfuny a zemětřesení mohou také způsobit katastrofální havárie požárů, únik výbušných plynů a únik kapalných chemikálií. Různé katastrofy a poškozená místa vyžadují různé odborné znalosti a vybavení pro záchranu při katastrofách, aby bylo dosaženo optimálních výsledků záchrany. Nedostatek informací o místě poškození však může bránit správě informací v záchranném středisku a záchranné operaci, což má za následek špatnou efektivitu záchrany nebo dokonce kauzalitám, kterým lze předejít. Tradiční metody řízení bezpečnosti mostů mají následující problémy: (1) selhání při sběru dat nebo monitorování podmínek na místě v reálném čase a neschopnost komplexně zaznamenat nebo analyzovat shromážděná data o podmínkách na místě v reálném čase, což má za následek špatnou účinnost záchrany při katastrofě; a (2) sběr dat prostřednictvím vizuálního hodnocení nebo použití velkého elektronického zařízení, což často vede k nepřesným výsledkům monitorování nebo vyšším nákladům a vyšší spotřebě energie. Proto byl v této studii vyvinut systém monitorování bezpečnosti mostů založený na internetu věcí s cílem vyřešit výše uvedené zmíněné problémy.

Systém se skládá z pěti hlavních subsystémů: (1) monitorovacích jednotek; (2) fotovoltaické jednotky; (3) bezdrátový komunikační systém; (4) serverový systém pro monitorování bezpečnosti mostu. Následuje úvod do každého subsystému:

1) Monitorovací jednotky

Monitorovací jednotky jsou senzorovou vrstvou v tomto IoT systému. V tomto systému existují čtyři druhy monitorovacích jednotek pro monitorování bezpečnosti mostů: (1) Jednotky pro monitorování hladiny říční vody: monitorování hladin řek a upozornění na anomálie hladiny; (2) jednotky pro monitorování tlaku vody v řece: monitorování hladin říční vody a upozorňování na anomálie tlaku vody; (3) jednotky pro monitorování potrubí: monitorování stavu potrubí a upozorňování na anomálie v potrubích; a (4) jednotky monitorování plynu: monitorování podmínek několika plynů a upozornění na anomálie v plynech. Monitorovací jednotky jsou navrženy tak, aby byly energeticky účinné, levné, malé a schopné snímat okolní prostředí. Každá monitorovací jednotka je jako mikropočítač, vybavena senzorem, výpočetním zařízením

a bezdrátovým přenosovým zařízením. Jednotky mohou monitorovat a shromažďovat data o podmínkách čtyř důležitých faktorů v prostředí mostu: hladina vody, tlak vody, potrubí a plyn, a poté zpracovat data pomocí jednoduchého výpočtu před odesláním zpracovaných dat na server pro ukládání dat prostřednictvím bezdrátového přenosu.

2) Fotovoltaické jednotky

Fotovoltaické (PV) jednotky přeměňují sluneční energii na elektrickou energii prostřednictvím FV panelů instalovaných na mostě. Solární energie je uložena v bateriích a slouží jako doplněk k elektrické síti pro napájení bezpečnostního monitorovacího systému mostu a lamp mostu. Kromě toho je v systému mechanismus sledování slunce, který dokáže automaticky sledovat slunce a podle toho upravit úhly naklonění FV panelů, aby byl zajištěn optimální sběr solární energie.

3) Bezdrátový komunikační systém

Hlavní funkcí bezdrátového komunikačního systému je propojit všechny komponenty v systému monitorování bezpečnosti mostu, včetně senzorů, výpočetního systému a signálových receptorů. Bezdrátový komunikační systém je založen na protokolu ZigBee, který se vyznačuje především nízkou rychlostí přenosu, nízkou spotřebou energie, vysokou bezpečností a podporou velkého množství síťových uzlů a více typologií sítí. Ve srovnání s Bluetooth může ZigBee podporovat více síťových uzlů s širší pracovní šířkou pásma. ZigBee má navíc nižší náklady na vývoj a delší přenosové vzdálenosti než Bluetooth.

4) serverový systém pro monitorování bezpečnosti mostu

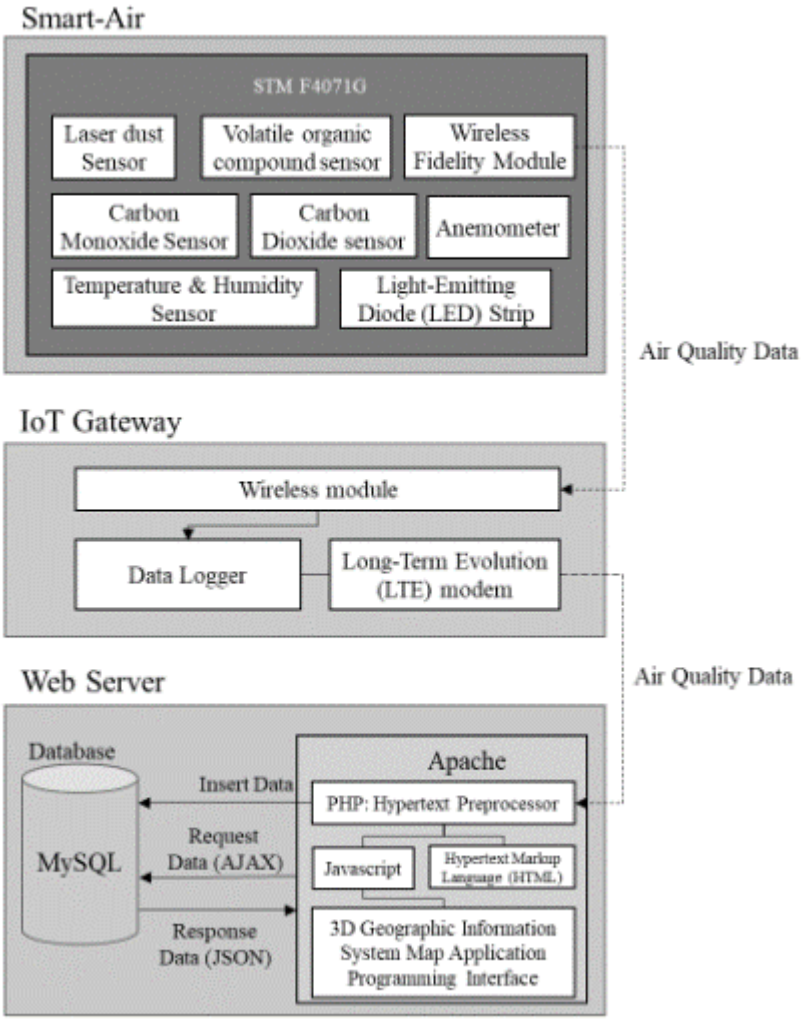
Data shromážděná výše uvedenými čtyřmi typy monitorovacích jednotek jsou přenášena pomocí technologie ZigBee do tohoto serverového systému pro další výpočty a rozhodování. Rozhodnutí učiněná systémem, související obsah analýzy a varovné zprávy jsou všechny přenášeny serverovým systémem přes internet do řídicího centra a mobilních zařízení vedoucích pracovníků, aby mohli v reálném čase a komplexně porozumět okolnímu prostředí mostu a udržovat záznamy údajů pro vhodné reakce, když dojde ke katastrofě. [16]

6.2 Implementace systému monitorování kvality ovzduší založeného na internetu věcí pro zkoumání částic (PM10) v tunelech metra

V této studii byl vyvinut systém monitorování kvality ovzduší založený na internetu věcí (IoT) pro monitorování pevných částic a byl implementován v tunelu metra v Incheonu v Jižní Koreji. Hlavním účelem tohoto systému bylo monitorování pevných částic v reálném čase a analýza stavu PM_{10}. V této studii byla k měření a přenosu dat o kvalitě ovzduší použita technologie IoT, zatímco k analýze a ukládání dat byla použita technologie cloud computingu. Kromě toho byl

vyvinut systém okamžitého varování, který informuje personál, aby okamžitě zasáhl, když byla zjištěna změna kvality ovzduší.

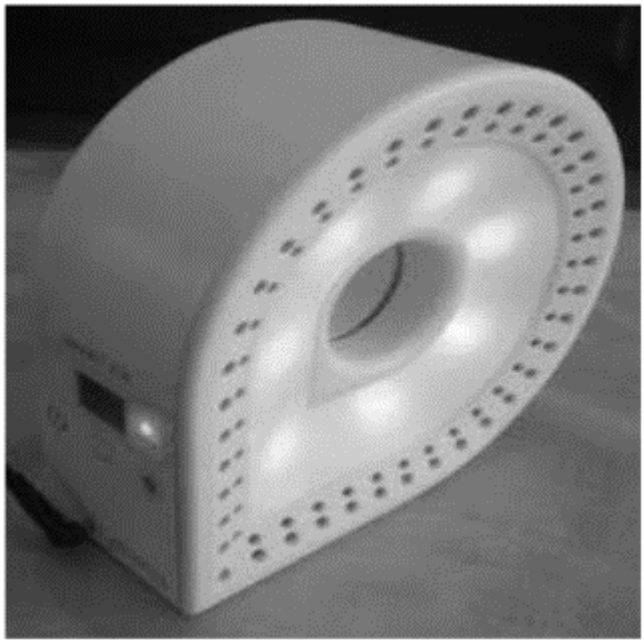
Systém byl primárně rozdělen do tří částí: zařízení Smart-Air, IoT gateway a webový server založený na cloud computingu. Rozdělení je uvedeno na obrázku č.19. Zařízení Smart-Air pro měření PM_{10} bylo použito ke sledování a zjišťování kvality ovzduší v tunelech metra. Gateway byla použita jako most, bezdrátově propojující zařízení Smart-Air s webovým serverem. Webový server umožnil analyzovat a zjišťovat podmínky kvality ovzduší. Má schopnost vypočítat index kvality ovzduš pro částice, vizualizovat koncentrace každé znečišťující látky a ukládat data pro další analýzu.



Obrázek 20. Schéma konfigurace systému monitorování kvality ovzduší založeného na IoT. [17]

1) Smart-Air zařízení

Zařízení Smart-Air je zařízení pro sledování kvality vzduchu od společnosti Smart-Is, které je navrženo tak, aby přesně a spolehlivě monitorovalo kvalitu vnitřního vzduchu pomocí rozšiřitelného rozhraní. Proto lze snadno nainstalovat nebo upravit více senzorů podle požadavků na monitorování. Kromě toho pásek LED namontovaný v zařízení zobrazuje různé barvy, aby indikoval stav kvality vzduchu v reálném čase. Barevný kód pro tento displej je definován indexem kvality ovzduší.



Obrázek 21. Zařízení Smart-Air [17]

2) IoT Gateway

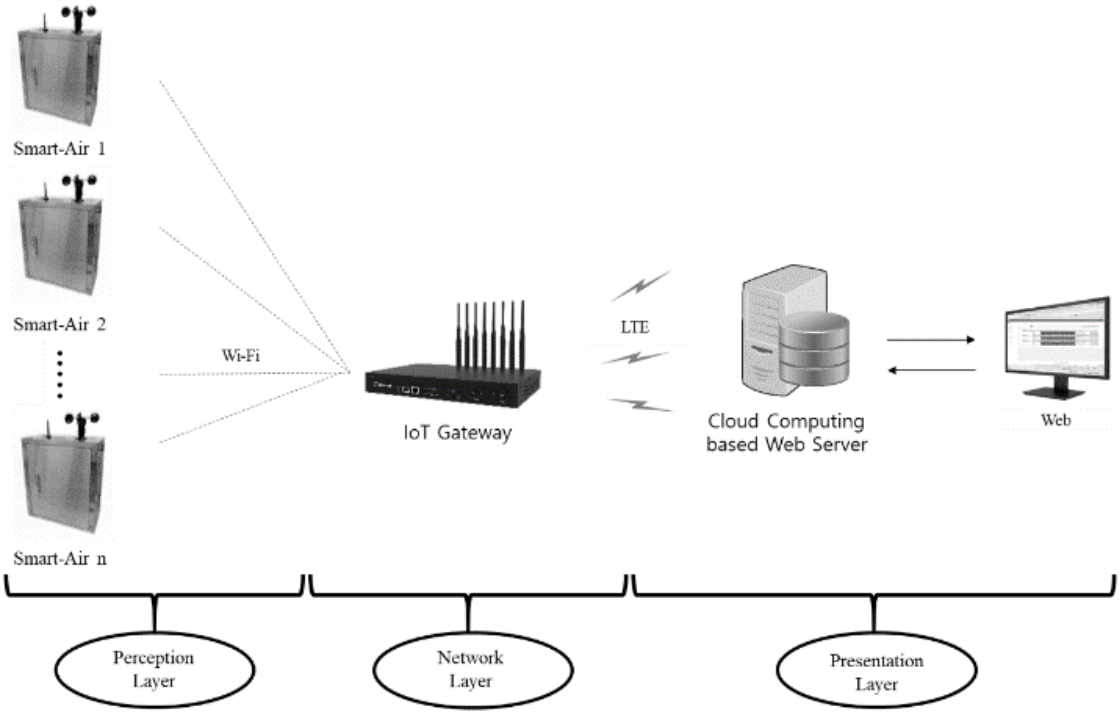
IoT brána shromažďuje data z více zařízení a přenáší data na webový server pro účely monitorování. Brána se skládá z bezdrátového modulu a dataloggeru pro přenos a sběr snímaných dat. V bráně jsou namontovány dva typy bezdrátových modulů: modul Wi-Fi a modul Long-Term Evolution (LTE). Data z každého zařízení jsou shromažďována přes Wi-Fi a přenášena ve formě paketů Transmission Control Protocol/Internet Protocol (TCP/IP) na webový server prostřednictvím LTE. Poté jsou data analyzována prostřednictvím webového serveru pro vizualizaci a zároveň jsou uložena v databázi.

3) Webový server

Webový server je navržen tak, aby vizualizoval koncentrace každé znečišťující látky a vypočítal index kvality ovzduší pro částice. Webový server ukládá data do databáze pro podporu budoucích analýz, které mohou být vyžadovány, například pro měsíční nebo roční analýzu monitorování kvality ovzduší. V tomto výzkumu byl k efektivnímu a efektivnímu řízení měření kvality ovzduší použit webový server založený na cloud computingu od Amazon Web Services (AWS). AWS je certifikovaná komerční platforma cloud computingu, která nabízí knihovny s otevřeným zdrojovým kódem pro různé aplikace, jako je alarmová služba a služba cloudového úložiště. Použití AWS tak snižuje čas a náklady potřebné k vytvoření přizpůsobených verzí těchto aplikací. AWS navíc poskytuje nejvyšší standard zabezpečení pro ochranu dat uložených v databázi.

Pro výzkum byl navržen webový server Apache s webovým programovacím jazykem nazývaným hypertextový preprocesor, zatímco jako databáze bylo použito MySQL

Metoda monitorování v této studii byla založena na platformě monitorování IoT. Platforma IoT je síť fyzických zařízení, která propojuje objekty v rámci systémů pomocí síťových technologií k inteligentnější interakci mezi každým objektem. Díky integraci technologie IoT do monitorovací platformy jsou senzory přímo propojeny s monitorovacím systémem, aby poskytovaly analýzu částic v tunelu v reálném čase. Platforma IoT se skládá ze tří hlavních komponent: vrstva vnímání, síťová vrstva a prezentační vrstva. Pro vrstvu vnímání bylo použito více zařízení Smart-Air k detekci kvality vzduchu se zaměřením na částice. Měření shromážděná ze zařízení Smart-Air byla přenášena do gateway přes Wi-Fi. Brána byla síťová vrstva platformy a zařízení Smart-Air byla připojena k webovému serveru cloud computingu prostřednictvím LTE. Poté webový server analyzoval přijatá data, aby určil kvalitu vzduchu a vizualizoval AQI pro částice. Pomocí cloudového serveru mohou manažeři nebo příbuzní pracovníci kdykoli a odkudkoli sledovat úrovně pevných částic.



Obrázek 22. Systémový diagram systému monitorování kvality ovzduší založeného na IoT. [17]

Index kvality ovzduší (AQI)

Hodnota AQI pro částice byla vypočtena pomocí dat ze zařízení Smart-Air připojených k webovému serveru. AQI je hodnota definovaná Agenturou pro ochranu životního prostředí Spojených států (EPA) k charakterizaci kvality vzduchu. Koncentrace PM_{10} byly použity k výpočtu AQI, který je popsán v rovnici:

$$I = (C - C_l)\frac{I_h - I_l}{C_h - C_l} + I_l$$

kde I = Index kvality ovzduší, C = zaokrouhlená koncentrace znečišťující látky (PM_{10}), C_h = mez koncentrace, která je větší nebo rovna C, C_1 = mez koncentrace, která je menší nebo rovna C, I_h = hodnota AQI odpovídající C_h a I_1 = hodnota AQI odpovídající C_1.

AQI hodnoty	Úrovně obav o zdraví	Kódy barev
0-50	Dobrá	Zelená
51-100	Mírná	Žlutá
101-150	Nezdravé pro citlivé skupiny	Oranžová
151-200	Nezdravé	Červená
201-300	Velmi nezdravé	Fialová
301-500	Hazardní	Hnědá

Tabulka 3. Hodnoty AQI

Cílem této studie bylo implementovat systém monitorování kvality ovzduší založený na IoT v tunelu metra za účelem prozkoumání stavu pevných částic. Hodnoty AQI pro částice byly postupně analyzovány a zobrazeny na webovém serveru s 95 % úrovní spolehlivosti. Výsledky ukázaly, že AQI a koncentrace částic se lišily v závislosti na místě a čase, a to i ve stejném tunelu. Údaje o AQI pro částice (údaje AQI z let 2017 a 2018) navíc prokázaly, že se podmínky kvality ovzduší zlepšily po provedení národního projektu údržby. [17]

6.3 Systém vizuální detekce defektů na železničních tratích založený na IoT

V dopravních systémech jsou bezpečnost a spolehlivost hlavními faktory, které jsou vždy zpochybňovány, zejména v systémech železniční dopravy. Systémy včasné kontroly jsou zásadní pro udržení bezpečných železničních tratí, které zajistí bezpečnou jízdu. Statistiky ukazují, že 60 % železničních nehod je způsobeno vykolejením a 90 % je způsobeno prasklinami na železnici. Praskliny na železničních tratích mohou být kontrolovány lidským personálem; to je však nejen časově náročné, ale také přesnost je subjektivní, protože ne všechny trhliny jsou rozpoznatelné pouhým okem. Vzhledem k tomu, že společnost Qatar Rail nedávno zahájila provoz prvních vlaků v Kataru, je velmi důležité hledat systémy údržby, které vyhovují katarskému klimatu pro kontroly železničních tratí. Tento požadavek vyžaduje kontrolní systémy, které budou nepřetržitě kontrolovat stav všech tratí nad Katarem a vydávat okamžitá upozornění na údržbu, aby se předešlo nehodám. V průběhu let se ukázalo, že strojně řízené kontrolní systémy nabízejí řešení pro rychlejší kontrolu a údržbu. Tyto inspekční systémy jsou běžné ve své schopnosti najít trhliny v železničních kolejích, stejně jako umístění trhliny, což pomáhá týmu údržby dosáhnout a opravit trhlinu v kratším čase.

Byl navržen nový automatizovaný systém, který se skládá z robota, který provádí kontrolu pomocí nedestruktivní metody kontroly založené na vizuální kontrole s místním zpracováním

obrazu, cloudové úložiště informací, které se bude skládat ze snímků železničních tratí s defektem a lokalizace robota v rozsahu 3 palců.

Vady železniční trati

Vady železniční tratě se dělí na dvě hlavní části: vnitřní vady a povrchové vady. Tyto defekty se mohou vyskytovat v hlavě, svaru nebo základní části dráhy. Nejběžnější defekty objevující se na kolejích jsou známé jako RCF (Rolling Contact Fatigue), česky: „únava z valivého kontaktu,‘‘ které jsou výsledkem tření na vysokorychlostních železnicích. Další běžnou sadou závad je ta, která vyplývá z místních klimatických podmínek a zvláštností infrastruktury. Vysoká teplota a vlhké podnebí, jako v Kataru, způsobuje vybočení a tepelné zlomy – známé také jako sluneční zlomy – na železničních tratích. Závady, jako jsou rozbité železniční tratě nebo sluneční zlomy, jsou důležitější než uvolněný balast nebo růst vegetace.

Metody inspekce železničních tratí jsou buď kontaktní, které jsou známé jako nedestruktivní testování, nebo bezkontaktní metody, které jsou založeny na analýze snímků nebo videí kolejových tratí.

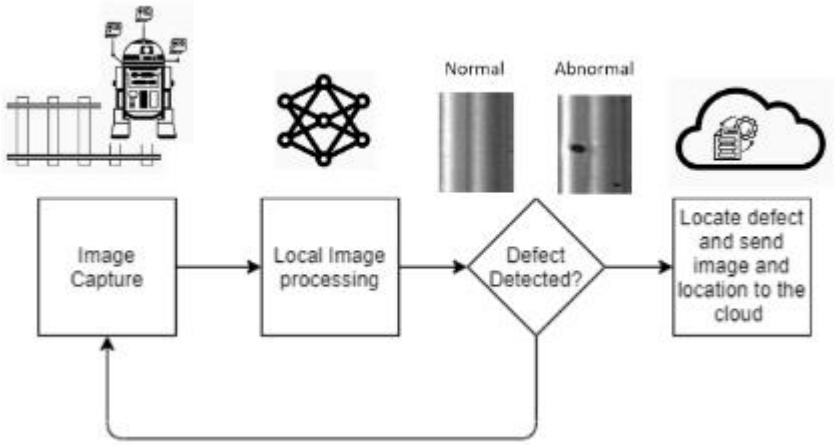
Navrhovaná systémová architektura

V této kapitole jsou popsány detaily navrhovaného řešení.

1) Blokové schéma

Systém se skládá ze tří hlavních částí:

- Robot, který je nasazený na kolejnici a vytváří snímky z obou stran koleje
- Modul pro místní zpracování obrazu zabudovaný v robotu
- Cloudová komunikace a ukládání poškozených úseků koleje



Obrázek 23. Blokové schéma systému [18]

2) Zpracování obrazu

Většina řešení vizuální kontroly je založena na zpracování obrazu, které se provádí po zachycení celých snímků železniční trati nebo po nahrání videa, které je odesláno do cloudu nebo uloženo na místních zařízeních. To znamená, že zpracování obrazu se provádí v řídicí stanici mimo kolejiště. V této práci se však zpracování obrazu provádí na kolejích během kontroly a pouze poškozené obrazy kolejí se ukládají a odesílají do cloudu. Díky tomu je kontrola rychlejší a nezahlcuje cloud zbytečnými daty.

Lokální zpracování obrazu je založeno na klasifikaci pořízených snímků na normální nebo abnormální pomocí konvoluční neuronové sítě. Jakmile je snímek klasifikován jako abnormální, jeho umístění je zmapováno a odesláno spolu s obrázkem do cloudu, kde bude později zpracováno. Následné zpracování spočívá v lokalizaci defektu v obraze; tato část se však provádí v pozdější fázi.

Navržená síť se skládá z 24 vrstev. Síť má 5 vrstev konvoluce o velikosti 5 x 5. Vstupní obrázek o velikosti 160 x 120 má celkem 19200 pixelů. První konvoluční vrstva má 8 filtrů. Počet filtrů se zvyšuje v každé konvoluční vrstvě. Druhá konvoluční vrstva má 25 filtrů, třetí konvoluční vrstva má 50 filtrů, čtvrtá konvoluční vrstva má 75 filtrů a pátá konvoluční vrstva má 100 filtrů. Filtry ve všech konvolučních vrstvách mají velikost 5x5.

Metoda byla implementována a testována v programu MATLAB.

Tento dokument představil nový automatizovaný systém pro inspekci kolejí, který integruje robotiku s vizuální inspekcí pro detekci a lokalizaci povrchových defektů. Novinkou této práce je poskytování místní detekce založené na IoT za chodu při kontrole pomocí 2DCNN. Zatímco

robot provádí inspekci, zachycené snímky jsou odesílány do neuronové sítě k detekci. Jakmile je detekována jakákoli povrchová vada, bude sdělena přímo do cloudu s odpovídajícím místem pro další kontrolu později. Navrhovaný systém dosáhl míry přesnosti 97 %. [18]

6.4 Systém pro včasné varování založený na IoT pro monitorování kolejnicových styků

Monitorování kolejnicových styků je v železničním komunikačním systému nanejvýš důležité, aby se zabránilo nehodám. K železničním nehodám obecně dochází v důsledku vykolejení vlaků z trati. Jedním z hlavních důvodů vykolejení vlaku je ztráta souososti kolejnic v důsledku uvolněných styků. Pro zajištění bezpečnosti a zabezpečení železnic je tedy vyžadováno monitorování vyrovnání kolejnice a polohy šroubu kolejnicového styku. Navržený systém sleduje polohu každého šroubu styku a varuje centrální železniční monitorovací centrum, stejně jako blízké stanice a strojvedoucí, pokud se některý šroub uvolní. Tento systém využívá GSM komunikaci a je schopen pracovat v oblastech, kde je dostupná mobilní síť alespoň 2G. Vestavěný systém detekuje místo poruchy pomocí mechanického převodu a podá varování, jakmile je detekováno jakékoli vychýlení šroubu. Navrhovaný systém je srovnatelně mnohem levnější. Kromě toho v testu přesnosti varování založeném na simulaci výsledky systému vykazují vysokou přesnost, což ukazuje na účinnost systému.

V tomto navrhovaném systému byl pro přenos varovného signálu použit elektrický pulzní generátor (EPG) založený na detekci chyb a bezdrátový komunikační systém založený na GSM. GSM modul je součástí vestavěného systému, který řídí celý systém. Systém také nepřetržitě vysílá fiktivní signál, aby byla zajištěna dostupnost systému. Tento systém funguje jako kontinuální monitorovací systém tím, že podá varování, jakmile dojde k významnému pohybu šroubu, a předchází tak nehodám včasným varováním.

Zařízení shromažďuje informace o stavu kolejnicových styků a odesílá je do základnové stanice prostřednictvím modulu GSM. Ze základní stanice jsou informace odesílány do centrálního dispečinku, nejbližší stanice a blízkého vlaku (v případě potřeby).

1) Detekce rotace pomocí EPG

Byl navržen nový nástroj, který dokáže zohlednit rotaci šroubů. Vědci přišli s nápadem spojit ozubené kolo se šroubem a vytvořte spínač, který se zavře, když se šroub pootočí o významné množství. Toto zařízení se nazývá elektrický pulzní generátor (EPG). Když se šroub otáčí, otáčí se také mechanické ozubené kolo, které je připevněno ke šroubu. Je navržen tak, že

když dojde k významnému otočení, jeden konec spínače spojený s ozubeným kolem je zkratován s druhým koncem. Nyní bude protékat proud a napětí bude klesat přes rezistor.

2) Zpracování dat vestavěným systémem

Ve vestavěném systému jsou uloženy podrobné informace o rotaci šroubu a počtu otáček, umístění šroubu, kde došlo k rotaci. Vestavěný systém také řídí, ovládá další zařízení k němu připojená. Jako vestavěný systém se používá Arduino Uno. Je nakódován tak, aby přijímal impuls z EPG, analyzoval data, a nakonec přikázal GSM modulu, aby odeslal informace konkrétnímu cíli. Stručně řečeno, vestavěný systém funguje jako mozek celého systému.

3) Přenos dat přes GSM

Po zpracování dat vestavěný systém přikáže GSM modulu odeslat textovou zprávu. Tento úkol se provádí pomocí SIM karty nastavené uvnitř GSM modulu a příkazem kódu nahraného do mikrokontroleru. Textová zpráva obsahuje informace o čísle zařízení, počtu otáček, jak moc je šroub uvolněn. Kromě přenosu dat pro upozornění na uvolnění šroubu je také po určité době nepřetržitě zasílána výchozí zpráva, aby se zajistilo, že snímač je stále na místě.

GSM modul slouží k navázání komunikace mezi dvěma mobilními zařízeními. Služba GSM je poměrně dostupná. Lze tak snadno zajistit nepřetržitý a nepřerušovaný výkon systému. Přenos dat je také spolehlivější a flexibilnější prostřednictvím GSM než jiné komunikační zařízení, jako je bluetooth a wifi. GSM modul je také levný, což snižuje náklady na projekt. Pro tuto výhodu je GSM preferován před jiným způsobem komunikace. Provádí bezdrátový přenos informací. GSM modul se aktivuje příkazem kódu nahraného na desce Arduino uno. Když je modul zadán, je na cílové telefonní číslo odeslána dříve napsaná textová zpráva. Při každém otočení šroubu a pokud je jeho množství riskantní, systém odešle zprávu do blízké stanice, centrálního dispečinku a blízkému strojvedoucímu.

4) Výpočet pro generování varování

Každá odpověď není nutná k odeslání varování. Varování by mělo být zasláno, když se šroub povolí o značné množství. Výpočet se pro generování varování provádí následovně: Ozubené kolo použité v systému má 32 zubů. Za účelem vytvoření pulzu, pokud se jeden zub otáčí a cestuje na stejné místo, kde byl jeho další zub před rotací, pak je jeho úhlové posunutí $\frac{360}{32} = 11.25$. Úhlové posunutí šroubu bude stejné, $\theta = (11.25°)$. Pokud předpokládáme, že je použit šestihranný šroub třídy 10,9 o průměru 14 mm, pak rozteč šroubu je $p = 2mm$. Pro 11,25° rotace bude lineární posunutí šroubu $d = \left(\frac{p}{360} x\theta\right) = 0.0625mm$. To je velmi malý posun a nemusí stačit k vytvoření varování. Můžeme tedy nastavit práh posunutí šroubu o 0,5 mm a vygenerovat varování. To by vyžadovalo posunutí zubů $\frac{0,5}{d} =$ 8krát nebo vytvoření 8 pulzů,

které by vygenerovaly varování, že šroub je dostatečně uvolněný, aby byl považován za riskantní.

5) Distribuce dat přes základní stanici

GSM modul odesílá data do blízké základnové stanice. Základnová stanice funguje jako konečný distributor datového paketu. Základnová stanice posílá informace do blízké stanice, centrálního dispečinku. Centrální dispečink nahrává informace do cloudu přes internet. Tyto informace jsou odeslány strojvedoucímu vlaku v okolí, pokud existuje riziko nehody. [19]

7 Zajištění kyberbezpečnosti IoT technologie

Když bylo IoT jako technologie inovováno a když byly plány na jeho použití k propojení zařízení a sítí v primitivní fázi, možná se bezpečnosti nevěnovala velká pozornost. Podniky tuto technologii využívaly k získávání obchodních výhod nebo vytvářely produkty založené na internetu věcí pro koncové uživatele a spouštěly je ve spěchu. Bezpečnostní hledisko se rozjelo, a než s tím mohli něco udělat, přišly jim do rukou nové příležitosti.

Avšak s ohledem na bezpečnostní výzvy internetu věcí, souběžnou úroveň narušení dat a neustále rostoucí kyberkriminalitu je nutné, aby podniky přijaly bezpečnostní protokoly a techniky internetu věcí, které zajistí úplnou ochranu cenných dat. [20]

I když se zmíněné systémy liší ve způsobu detekce, princip zabezpečení je pro všechny systémy stejný, tudíž níže uvedené způsoby zajištění kyberbezpečnosti platí pro všechny zmíněné systémy.

1) Vytvoření jedinečných přihlašovacích údajů pro každé zařízení

Odesílání chráněných dat je základní funkcí jakéhokoli zařízení IoT. Aby byla tato funkce účinná, musí uživatelé i výrobci důvěřovat, že data, která obdrží, jsou autentická a určená jim. Nejlepším způsobem, jak tohoto cíle dosáhnout, je vydání jedinečných přihlašovacích údajů ve formě digitálních certifikátů pro každé zařízení IoT.

Poskytnutí jedinečného digitálního certifikátu každému zařízení pomáhá zlepšit autentizaci a nabízí obrovskou ochranu oproti běžným dnešním postupům používání výchozích hesel nebo dokonce sdílených klíčů pro symetrické šifrování. Je to proto, že hesla s sebou nesou vysoké riziko kompromitace a symetrické šifrovací klíče, které nabízejí větší ochranu než výchozí hesla, neposkytují žádný druh rozlišení mezi zařízeními. Tento nedostatek diferenciace znemožňuje sdílet jedinečné informace s konkrétním připojeným zařízením nebo určit konkrétní zařízení, ze kterého jednotlivá data pocházejí.

Naproti tomu digitální certifikáty mohou pro každé zařízení vytvořit vysoce bezpečnou, jedinečnou autentizační metodu, která nabízí výrazně vyšší bezpečnost. Tento přístup například umožňuje výrobcům bezpečně sdílet aktualizace a data s konkrétními zařízeními a pomáhá lépe ověřovat autenticitu příchozích informací ze samotných zařízení. [20]

2) Používání aktuálního softwaru

Aktualizace softwaru nejsou jen pro elegantnější uživatelské rozhraní nebo přidané funkce. Často opravují staré chyby a opravují bezpečnostní zranitelnosti a rizika. [21]

Jedním z významných bezpečnostních rizik IoT je schopnost hackerů dodávat aktualizace škodlivého softwaru do připojených zařízení. Výrobci se mohou před tímto rizikem chránit tím, že požadují, aby zařízení před instalací ověřila pravost nového firmwaru nebo softwaru. To vyžaduje, aby vývojové týmy výrobců podepsaly svůj kód digitálním podpisem, čehož lze dosáhnout pomocí páru veřejného/soukromého klíče.

V tomto případě by každé připojené zařízení vyžadovalo veřejný klíč, který odpovídá soukromému klíči drženému vývojovým týmem výrobce. Pokud vývojáři používají soukromý klíč k „podepsání svého kódu“, jakékoli zařízení s veřejným klíčem může (a) ověřit, že aktualizace byla skutečně odeslána od výrobce (nebo kohokoli, kdo má soukromý klíč) a (b) potvrdit, že aktualizace nebyla při přenosu změněna. V důsledku toho vyžadování podepisování kódu pomáhá chránit před připojenými zařízeními, která instalují poškozený software odeslaný škodlivou třetí stranou. [20]

3) PKI – Public Key Infrastructure

PKI je důvěryhodný rámec složený z hardwaru, softwaru, zásad a postupů potřebných ke správě důvěryhodných digitálních certifikátů a šifrování veřejného klíče. Pomáhá ověřovat digitální identity a zabezpečit data, což splňuje kritické potřeby zabezpečení IoT v oblasti ověřování, šifrování a podepisování kódu. Důležité je, že je také škálovatelný tak, aby vyhovoval milionům identit zařízení s pouze minimální stopou na každém zařízení.

PKI nabízí několik zásadních výhod, pokud jde o posílení bezpečnosti IoT, včetně:

- Jedinečné identity: PKI umožňuje výrobcům zařízení IoT vložit kryptograficky ověřitelnou identitu prostřednictvím digitálního certifikátu do každého zařízení, aby byl zajištěn bezpečný přístup a poskytování softwaru v průběhu času. Důležité je, že výrobci mohou tyto certifikáty na jednotlivých zařízeních také aktualizovat nebo zrušit podle potřeby.
- Flexibilita: PKI je vysoce flexibilní přístup, který výrobcům umožňuje používat různé možnosti pro odvolávání a registraci a nasazení certifikátů.
- Škálovatelnost: Výrobci mohou vydávat digitální certifikáty od jediné důvěryhodné certifikační autority, což umožňuje zařízením IoT vzájemně se bezpečně ověřovat bez jakéhokoli centralizovaného serveru.
- Robustní zabezpečení: Za předpokladu, že je PKI dobře spravováno, poskytují digitální certifikáty výrazně vyšší zabezpečení než jiné metody ověřování, zahrnující výchozí hesla a symetrickou kryptografii.

- Minimální dopad: Asymetrické klíče používané v PKI mají minimální dopad, což znamená, že nepředstavují zátěž k uložení informací pro připojená zařízení s nízkým výpočetním výkonem.

Osvědčený přístup: PKI se již dlouho používá k získání bezpečné metody pro digitální autentizaci a datovou komunikaci. Je uznáváno jako praktické a škálovatelné řešení pro ochranu před krádeží dat. [20]

8 Životní cyklus IoT zařízení

Modely životního cyklu byly vytvářeny a zkoumány po mnoho let pro různé aplikační účely. Tyto různé pohledy musí být také jasně odděleny při zvažování aplikací IoT, zejména životního cyklu produktu a životního cyklu zařízení.

Životní cyklus může být rozdělena do tří fází: začátek života (anglicky Begin of Life (BoL)), průběh života (anglicky Middle of Life (MoL) a konec života (anglicky End of Life (EoL Fáze BoL zahrnuje výrobu zařízení. Přechod do fáze MoL zahrnuje prodej a instalaci v místě použití. Ve fázi MoL je zařízení v nominálním používání uživatelem. Kromě toho jsou ve fázi MoL zapojeny další role, protože musí proběhnout mnoho různých činností, aby se zařízení udrželo ve funkčním stavu a fungovalo v užitečném nastavení. Fáze EoL zahrnuje odinstalaci a vyřazení zařízení, když zařízení již nenabízí zákazníkovi dostatečnou hodnotu. Příčina klesající hodnoty může pocházet z různých hledisek. Zařízení může být například technicky rozbité, uživatelské požadavky se v průběhu času měnily, byla k dispozici lepší řešení nebo jednoduše poskytovatel služby zastavil službu potřebnou k provozu zařízení.

1) Aktivity fáze výroby zařízení

Výroba a montáž: Mechanická výroba IoT zařízení z jednotlivých komponent a podsestav. Přestože ještě nebyl vyroben žádný koncový produkt, v tomto kroku již musí být zaznamenány informace o zařízení. Zejména musí být zaznamenána sériová čísla a identifikační prvky sestav s vyšší hodnotou, jako jsou CPU, modemy, síťové komponenty.

Závěrečné testy hardwaru, počáteční konfigurace: Jako jeden z nejkritičtějších kroků ve výrobním procesu se provádějí závěrečné testy zařízení na úrovni hardwaru. K tomuto účelu se používá specifický firmware nebo specifický režim standardního firmwaru zařízení. Pokud jsou tyto testy úspěšné, nainstaluje se nebo aktivuje standardní firmware a nakonfiguruje se s továrním nastavením.

První komunikace: První komunikace zařízení se systémem správy dokončí testy zařízení. Tato první komunikace zajišťuje dva aspekty: Za prvé, že bezdrátová komunikace funguje správně. Za druhé je zajištěno, že v komunikační službě jsou dostupné všechny potřebné informace o zařízení. Používanou komunikační službou může být i bootstrap komunikační služba, která je při následném použití nahrazena službou specifickou pro aplikaci.

Přiřazení individuálních přihlašovacích údajů (automatický proces): Zařízení jsou přiřazena jednotlivá pověření pro vytvoření zabezpečeného komunikačního kanálu. V zařízení jsou k dispozici veřejné klíče pro ověření komunikačního partnera nebo ověření aktualizací softwaru.

Konkrétní výběr identifikačních a autentizačních funkcí závisí na konkrétní aplikaci a implementaci.

Převod právního vlastnictví: Zařízení je výrobcem prodáno novému majiteli, který chce zařízení uvést do aplikace a používat. Při této činnosti může zařízení také několikrát změnit vlastníka.

Přenos do místa použití: Zařízení IoT se fyzicky přenese do místa použití.

2) Aktivity při nominálním používání

Instalace v místě použití: Umístění a fyzická instalace zařízení v místě použití. V závislosti na povaze zařízení a aplikace může být místo použití pevné nebo mobilní. Po instalaci potřebuje instalační technik jasnou zpětnou vazbu k ověření správné instalace zařízení.

Použití konfigurace nominálního použití: Překonfigurování zařízení s konfigurací nominálního použití, která se liší od továrního nastavení. Konfigurace jmenovitého využití závisí na potřebách koncových uživatelů a je individuální pro každé zařízení, i když je hardware a firmware zařízení stejný. Jelikož je každé zařízení používáno v individuálním prostředí, musí být propojeny i aplikační služby, které zpracovávají aplikační aspekty konkrétního zařízení.

Přiřazení zařízení ke kontextu: Zařízení je přiřazeno kontextu aplikace. Všechna smyslová data jsou relativně bezvýznamná, pokud je nelze dát do kontextu. Aplikační služba odpovědná za zpracování dat zařízení IoT si tedy musí být vědoma kontextu aplikace zařízení.

Zpracování/analýza shromážděných aplikačních dat: Zatímco zařízení pracuje nominálně, data jsou shromažďována a odesílána prostřednictvím komunikační služby do aplikační služby. Vzhledem k tomu, že tato data souvisejí s aplikací, nejsou tato data zpracovávána správou zařízení ani službou připojení. Zpracovaná data používá koncový uživatel způsobem specifickým pro aplikaci. Uvnitř aplikační služby lze uplatnit diferenciaci uživatelů do konkrétních rolí.

Spouštění činností zařízení: Uživatel spouští funkci zařízení související s aplikací. Funkci lze spustit přímo na zařízení, přes místní komunikační linku nebo vzdáleně. Funkce zařízení může být velmi jednoduchá, také může jít o složitější interakci mezi uživatelem a zařízením. Vzhledem k tomu, že aplikační služby a samotné zařízení IoT mohou nabízet aplikační programovací rozhraní (API) pro interakci s funkcemi zařízení, činnost zařízení může být také spuštěna jinou externí aplikací nebo službou.

Změna řídicích hodnot: Uživatel změní řídicí hodnotu související s aplikací na zařízení prostřednictvím místní komunikační linky nebo vzdáleně. Zařízení musí přijmout novou hodnotu, přijmout samo sebe a vykonávat vnitřní funkce autonomně. Kontrolní hodnotu může

změnit uživatel i interagující externí aplikace nebo služba. Tato řídicí hodnota souvisí s aplikací a nesouvisí s provozem zařízení.

Monitor provozu zařízení: Zařízení IoT shromažďuje data zaměřená na zařízení a přenáší je do služby monitorování zařízení k dalšímu sběru a zpracování. Data zaměřená na zařízení jsou jako stav vnitřní baterie, spotřeba energie, indikátory kvality, chybové kódy související s hardwarem a softwarem, protokolování. Data se nevztahují k aplikaci zařízení, ale pouze k zařízení samotnému. Která data je třeba přenášet a sledovat, závisí na zařízení a jeho konstrukci.

Překonfigurování zařízení: Konfigurace zařízení se musí přizpůsobit změněnému prostředí, jako je změněné nastavení externí konektivity nebo interní optimalizované nastavení správy energie a napájení. Konfigurace souvisí se zařízením a nepatří přímo do aplikace zařízení IoT.

Výměna interního firmwaru zařízení: Probíhá výměna interního firmwaru. Tento proces mohou spustit dvě základní situace: Oprava chyb nebo další vývoj firmwaru při zachování funkčnosti. Při výměně firmwaru může být nutná také rekonfigurace zařízení.

Aktualizace komunikační služby: Náhrada nainstalované a používané komunikační služby. I když tato činnost přímo nesouvisí se zařízením samotným, může mít na zařízení významný dopad. V závislosti na nastavení a provozu systémů IoT lze realizovat hladký přechod zařízení IoT z jedné instance komunikační služby do druhé. V menších sestavách dojde k okamžitému přechodu všech připojených zařízení IoT na aktualizovanou komunikační službu. Protože jsou aplikační služby propojeny s komunikační službou je nutné toto propojení a datové toky zkontrolovat.

Aktualizace aplikační služby: Nahrazení nainstalované verze aplikační služby novou verzí. Vzhledem k tomu, že IoT zařízení nekomunikuje přímo s aplikační službou, nemělo by dojít k žádné změně pro samotné zařízení. Jelikož je aplikační služba propojena s komunikační službou, je nutné toto propojení ověřit při aktualizaci jedné z těchto služeb. Ve spojení s aktualizovaným firmwarem lze realizovat nové funkce aplikace.

3) Aktivity ve fázi konce zařízení

Smazání interních dat o používání zařízení: Když bude zařízení vyřazeno z provozu, musí být ze zařízení vymazána všechna data, osobní údaje a údaje o používání. Tento proces by mělo být možné spustit přímo na zařízení a vzdáleně.

Uvolnění oprávnění: Protože zařízení již není aktivně používáno, musí být uvolněny všechny již nepotřebné prostředky a oprávnění. To zahrnuje přístupová práva ke komunikační

infrastruktuře i přidělené kapacity u komunikačních a aplikačních služeb. Rovněž musí být odstraněno sledování činnosti zařízení.

Přiřazení/přidružení kontextu uvolnění: Musí být uvolněno přidružení aktivního kontextu mezi zařízením IoT a kontextem aplikace.

Odstranění zařízení z místa použití: Zařízení je fyzicky odstraněno z místa použití. Všechny vratné mechanismy pro provoz zařízení musí být demontovány.

Zahájení procesu reaktivace: V některých případech použití a za zvláštních okolností může být nutná reaktivace téměř vyřazeného zařízení. V tomto procesu opětovné aktivace musí být znovu nastavena víceméně veškerá požadovaná konfigurace komunikace. Proces opětovné aktivace zahrnuje obnovené vydání autentizačních a autorizačních tokenů a také opětovnou aktivaci přiřazení fyzických a logických prostředků. Pokud proces počátečního nastavení zahrnoval stále dostupnou službu bootstrap, může být reaktivace snadnější.

Zničení zařízení: Konečný konec životnosti tohoto zařízení. V závislosti na částech zařízení a konstrukci lze některé prvky znovu použít a renovovat. S největší pravděpodobností bude většina dílů zlikvidována nebo recyklována jako surovina. [22]

9 Doporučení pro používání IoT na železnici

IoT získává v dnešním světě na oblibě a jinak tomu není ani na železnici. Je to jedním z řešení, jak zabezpečit železniční síť a získávat data v reálném čase. Toto doporučení může také sloužit pro případného konzumenta obsahu, kterým může být např. Správa železnic.

IoT jednotky jsou skvělým způsobem, jak zabezpečit trakční vedení proti případným krádežím a ušetřit náklady na obnovu trakčního vedení po krádeži. Jelikož v případě krádeže musí dojít k výlukám, než se obnoví trakční vedení, jsou s tím spojené i náklady právě na tyto výluky. Když bude trakční vedení vybaveno IoT jednotkami, bude mít správce trati informace o jakékoliv manipulaci s trakčním vedením a výrazně se sníží náklady, které musel vydávat za obnovu trakčního vedení a vytváření výluk.

V případě zabezpečení technologického domku u přejezdu se můžou ušetřit náklady na rekonstrukci domku po vyhoření nebo záplavě. V případě rekonstrukce technologického domku musí být omezena doprava na trati, tyto náklady mohou být ušetřeny, pokud k vyhoření nebo záplavě vůbec nedojde, a to díky IoT jednotkám, které neustále posílají data o situaci v technologickém domku.

V případě detekce vstupu do tunelu mohou jednotky IoT ušetřit náklady na obnovení provozu na trati nebo náklady vydané za výluky. Pokud dojde k nehodě v tunelu, musí být všechny vlaky projíždějící daným tunelem vedeny odklonem, dokud nedojde v obnově provozu v tunelu. Pokud bude Správa železnic používat v tunelech IoT jednotky, bude získávat data o pohybu v tunelu a může zabránit nehodám, které můžou mít také škody na lidských životech.

Jsou zde samozřejmě i další způsoby, jak monitorovat neoprávněný vstup do tunelu, ale žádný není, tak cenově dostupný jako technologie IoT. Je tedy pouze na konzumentovi, jaký způsob si zvolí a kolik je ochotný za systém zaplatit.

Při navrhování systému, který bude pracovat na technologii IoT je důležité ověření navrženého systému. Systém mohu ověřit v reálném provozu, jako to bylo v případě zabezpečení trakčního vedení nebo testy, které budou probíhat v určité dny, viz případ u zabezpečení technologického domku u přejezdu. Data vidí klient ve webovém rozhraní, a tak má přehled o všech svých jednotkách, zda aktivně komunikují nebo ne. Po určitém časovém úseku testování je vhodné si vytvořit přehledný graf za to dané časové období a zhodnotit, jestli došlo k nějakým výpadkům komunikace a zda jednotka předávala pravdivé informace. Někdy může docházet k falešným alarmům, viz zabezpečení trakčního vedení, kde byly alarmy způsobeny průjezdem vlaku nebo silnějším větrem. Tyto alarmy mohou být odstraněny nasazením vhodného filtru SW nástroje.

10 Závěr

Tato diplomová práce představuje způsoby využití technologie IoT na železnici. Tato technologie má potenciál více zabezpečit železniční síť a zlepšit poskytování informací v reálném čase. Velikou výhodou této technologie je cena, která je v porovnání s lidarovými technologiemi velmi nízká.

Nejdříve byla provedena rešerše, která se skládala z popisu technologie a jakým způsobem funguje. Následně zde byly vypsány senzory, které se spolu s touto technologií využívají. A v neposlední řadě zde byly uvedeny typy sítí, které jsou využívány, jak ve světě, tak v České republice.

V další kapitole byla zhodnocena aktuální situace IoT na železnici v České republice. IoT na naší železnici bohužel není moc využíváno, ale bylo už několikrát testováno.

Následovala kapitola týkající se architektury, kde byly podrobněji rozepsány všechny části, které se používají v rámci systému založeného na IoT.

Pátá kapitola se týkala konkrétních možností využití technologie IoT na železnici. Je zde vypsáno několik způsobů. Systémy jsou stručně popsány, je zde uveden i postup měření a u některých jsou doložena data i jejich vyhodnocení. Během ověřovacího provozu nebyla zjištěna žádná nefunkčnost či výpadek zařízení. Jednotka se tak jeví jako plně funkční a jako zařízení, které je schopné plně zabezpečit železniční síť a pomocí technologie NarrowBand IoT tak efektivně předcházet případným škodám a nehodám.

Dále je zde podkapitola, která obsahuje můj vlastní návrh systému, který je založený na technologii IoT. Systém je zaměřen na kontrolu vstupu do tunelu a měl by předcházet nehodám vzniklých v tunelu. Systém je i následně finančně ohodnocen. IoT technologie je z finančního hlediska porovnána s jinými způsoby, kterými se dá monitorovat vstup do tunelu.

Šestá kapitola je zaměřená na implementaci IoT technologie pro dopravní objekty. Kapitola je výčtem zajímavých implementací technologie IoT použité ve světě a není použita přímo na dráze.

Sedmá a osmá kapitola jsou rešeršní. Popisují, jak zabezpečit IoT technologii proti kybernetickým útokům, resp. Životní cyklus IoT zařízení. Obě kapitoly byly převzaty z odborných článků.

V rámci deváté kapitoly byly vypsány doporučení pro případné konzumenty, kterým může být např. Správa železnic. Důvodem používání IoT jednotek je zejména zabezpečení železniční sítě, ať už se jedná o trakční vedení, monitorování vstupu do tunelu nebo zabezpečení

technologického domku u přejezdu. IoT jednotky mohou ušetřit náklady vynaložené za obnovu po poruchách nebo nehodách na železnici. Ušetřeny budou také náklady vynaložené za výluky po dobu oprav.

ZDROJE

[1] What is internet of things (IoT)? [online]
Dostupné z: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[2] What is IoT? The Internet of Things defined and explained [online]
Dostupné z: https://www.i-scoop.eu/internet-of-things-iot/internet-of-things-what-definition/

[3] What technologies are used in IoT – technology behind Internet of Things [online]
Dostupné z: https://www.avsystem.com/blog/iot-technology/

[4] How IoT Works? [online]
Dostupné z: https://techvidvan.com/tutorials/how-iot-works/

[5] LoRaWAN, Sigfox nebo NB-IoT? Srovnání 3 významných typů IoT sítí [online]
Dostupné z: https://www.iotport.cz/iot-novinky/lorawan/lorawan-sigfox-nebo-nb-iot-srovnani-3-vyznamnych-typu-iot-siti

[6] DOROBANTU, Octavia Georgiana a Simona HALUNGA. Security threats in IoT [online]
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9301127

[7] Top 15 Sensor Types Being Used Most By IoT Application Development Companies [online]
Dostupné z: https://www.finoit.com/blog/top-15-sensor-types-used-iot/

[8] TECHNICKÉ SPECIFIKACE systémů, zařízení a výrobků: Dálková diagnostika technologických systémů železniční dopravní cesty. In: . 2018, TS 2/2008 – ZSE

[9] KONÍČEK, Jakub. Ověřovací provoz FlexiCube Gateway: Popis komunikace IoT

[10] KOVAŘÍK, MBA, Mgr. Martin. TECHNICKÉ PODMÍNKY: Zařízení FlexiCube

[11] KOVAŘÍK, MBA, Mgr. Martin. TECHNICKÉ PODMÍNKY: Zařízení FlexiCube Gateway

[12] Edukační materiál pro prvky, zařízení a technologie využívané v elektrických zabezpečovacích systémech – vibrační detektory [online]
Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/1353/%C5%A1t%C4%9Brba_2006_bp.pdf?sequence=1&isAllowed=y

[13] Jak funguje kouřový požární hlásič [online]
Dostupné z: https://www.zabezpecovaci-zarizeni.cz/pozarni-detektory/jak-funguje-kourovy-pozarni-hlasic-%5Bb062%5D

[14] Fire Detector Types And Their Working Principle
Dostupné z: https://shipfever.com/fire-detector-types-working-principle/

[15] What is a Humidity Sensor? [online]
Dostupné z: https://www.fierceelectronics.com/sensors/what-a-humidity-sensor

[16] LEE, Jin-Lian a Yaw-Yauan TYAN. Development of an IoT-based Bridge Safety Monitoring System [online]
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7988352

[17] JO, ByungWan, Jun Ho JO a Ian CHOI. Implementation of IoT-Based Air Quality Monitoring System for Investigating Particulate Matter (PM10) in Subway Tunnels [online]
Dostupné z: https://www.mdpi.com/1660-4601/17/15/5429/htm

[18] ALNAIMI, Noora a Uvais QIDWAI. IoT Based on-the-fly Visual Defect Detection in Railway Tracks [online]
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9089560

[19] , Md. Mizanur Rahaman Nayan, Suaib Al Sufi, Abir Kallayan Abedin, Rizwan Ahamed a Md. Farhad Hossain. An IoT Based Real-time Railway Fishplate Monitoring System for Early Warning [online]
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9393036

[20] IoT Device Security: 7 Ways to Secure your IoT Devices [online]
Dostupné z: https://www.kelltontech.com/kellton-tech-blog/iot-device-security-7-ways-secure-your-iot-devices

[21] How to Secure IoT Devices [online]
Dostupné z: https://www.iotforall.com/how-to-secure-iot-devices-2

[22] SPÄTHE, Steffen. Conception of a Generic IoT Device Life Cycle Model [online]
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9628736

[23] LoRaWAN, Sigfox nebo NB-IoT? Srovnání 3 významných typů IoT sítí [online]
Dostupné z: https://www.iotport.cz/iot-novinky/lorawan/lorawan-sigfox-nebo-nb-iot-srovnani-3-vyznamnych-typu-iot-siti

SEZNAM OBRÁZKŮ

Obrázek 1. Definování internetu věcí pomocí 7 charakteristik [2]
Obrázek 2. Detektor kouře [14]
Obrázek 3. Fungování IoT [4]
Obrázek 4. Pokrytí v ČR v roce 2019 [23]
Obrázek 5. Pokrytí v ČR [23]
Obrázek 6. Pokrytím NB-IoT dosáhne k 96 % obyvatelům v ČR [23]
Obrázek 7. Schéma komunikace [9]
Obrázek 8. Jednotka FlexiCube [10]
Obrázek 9. Struktura a protokoly dálkové diagnostiky TLS [8]
Obrázek 10. Schéma provedení detekce pádu vozidla do kolejiště [vlastní]
Obrázek 11 a 12. Umístění jednotky na trakčním vedení [Firma Intesys]
Obrázek 13 a 14. Umístění jednotky v elektroměru [Firma Intesys]
Obrázek 15 a 16. Umístění jednotky s požárním čidlem [Firma Intesys]
Obrázek 17. Umístění jednotky se záplavovým senzorem [Firma Intesys]
Obrázek 18. Umístění jednotky ve vozidle MUV [Firma Intesys]
Obrázek 19. Blokové schéma návrhu monitorování vstupu do tunelu [vlastní]
Obrázek 20. Schéma konfigurace systému monitorování kvality ovzduší založeného na IoT [17]
Obrázek 21. Zařízení Smart-Air [17]
Obrázek 22. Systémový diagram systému monitorování kvality ovzduší založeného na IoT [17]
Obrázek 23. Blokové schéma systému [18]

SEZNAM TABULEK

Tabulka 1. Náhled na data získaná při měření zabezpečení trakčního vedení
Tabulka 2. Náhled na data získaná z jednotky umístěné v technologickém domku u přejezdu v ŽST Podivín
Tabulka 3. Hodnoty AQI