Univerzita Pardubice

Fakulta ekonomicko-správní

Možnosti zabezpečení prostředků IoT ve výrobním podniku

Radim Ondrůch

Bakalářská práce

2022

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Radim Ondrůch**
Osobní číslo:	**E19131**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Možnosti zabezpečení prostředků IoT ve výrobním podniku**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je vyhledat možnosti a rámcově navrhnout realizaci zabezpečení prostředků *Internet of Things* v provozu výrobního podniku.

Osnova:

- Vyhledání informací o využívání IoT technologií ve sledovaném segmentu podniků.
- Vytipování zranitelnosti využívaných technologií ve vztahu ke specifickým podmínkám daného prostředí.
- Návrh využití odpovídajících forem zabezpečení pro několik vybraných modelových subjektů.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

CHANDANA, Roy, Sudip MISRA a Anandarup MUKHERJEE, 2021. *Introduction to Industrial Internet of Things and Industry 4.0*. Boca Raton: CRC Press. ISBN 9781000283068.
GILCHRIST, Alasdair. *Industry 4.0: the industrial internet of things*. New York: Apress, 2016. ISBN 978--1-4842-2046-7.
LEA, Perry. *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security*. Birmingham: Packt Publishing, 2018. ISBN 9781788475747.
VACULÍK, Juraj. *Od telemetrie k internetu vecí I.* Bratislava: EDIS, 2019. ISBN 9788055415215.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2021**
Termín odevzdání bakalářské práce: **30. dubna 2022**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2021

Prohlašuji:

Práci s názvem Možnosti zabezpečení prostředků IoT ve výrobním podniku jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 11. 2022

Radim Ondrůch v. r.

PODĚKOVÁNÍ

Tímto bych rád poděkoval RNDr. Ing. Oldřichu Horákovi, Ph.D., za odborné vedení, ochotu pomoci a velice cenné rady při zpracování této práce. Dále bych chtěl poděkovat mé rodině a přátelům, kteří mi byli oporou v průběhu studia.

ANOTACE

Cílem této bakalářské práce je vyhledat možnosti a rámcově navrhnout realizaci zabezpečení prostředků Internet of Things v provozu výrobního podniku. První část práce představuje možnosti využití IoT technologií ve výrobním prostředí a definuje koncept Industry 4.0. Dále práce popisuje reálné hrozby při implementaci chytrých řešení a dle architektury IoT jsou vytipována zranitelná místa využívaných technologií. V poslední části práce jsou navrženy implementace IoT technologií do výroby a odpovídající formy zabezpečení pro daná řešení.

KLÍČOVÁ SLOVA

Internet věcí, Průmysl 4.0, Kyberbezpečnost, Návrh zabezpečení, Bezdrátové sítě

TITLE

Options for Securing IoT Assets in the Manufacturing Enterprise

ANNOTATION

The purpose of this bachelor's thesis is to search for possibilities and to propose a framework for the implementation of Internet of Things security in the operation of a manufacturing company. The first part of the thesis presents the possibilities of using IoT technologies in the manufacturing environment and defines the concept of Industry 4.0. Furthermore, the thesis describes the real threats in the implementation of smart solutions and according to the IoT architecture, the vulnerabilities of the used technologies are identified. The last part of the thesis proposes the implementations of IoT technologies in production and the corresponding forms of security for these solutions.

KEYWORDS

Internet of Things, Industry 4.0, Cybersecurity, Security design, Wireless networks

OBSAH

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

ABP – Activation By Personalisation

AES – Advanced Encryption Standard

API – Application Programming Interface

AppSKey – Application Session Key

AQI – Air Quality Index

B2B – Business-to-Business

BLE – Bluetooth Low Energy

CO_2 – Oxid uhličitý

DDoS – Distributed Denial of Service

DoS – Denial of Service

GPRS – General Packet Radio Service

GPS – Global Positioning System

GSM – Global System for Mobile Communication

HTTPS – Hypertext Transfer Protocol Secure

HVAC – Heating, Ventilation and Air Conditioning

ICS – Industrial Control System

IIoT – Industrial Internet of Things

IoE – Internet of Everything

IoMT – Internet of Medical Things

IoT – Internet of Things

IP – Internet Protocol

IT – Information Technology

LoRaWAN – Long Range Wide Area Network

LPWAN – Low Power Wide Area Network

LTE – Long Term Evolution

M2M – Machine-to-Machine

MQTT – Message Queuing Telemetry Transport

NB-IoT – NarrowBand-Internet of Things

NFC – Near Field Communication

NwkSKey – Network Session Key

OT – Operational Technology

OTAA – Over-The-Air Activation

OWASP – Open Web Application Security Project

QoS – Quality of Service

RAT – Remote Access Trojan

RFID – Radio Frequency Identification

TLS – Transport Layer Security

UDP – User Datagram Protocol

USB – Universal Serial Bus

UUID – Universally Unique Identifier

VPN – Virtual Private Network

WLAN – Wireless Local Area Network

WSN – Wireless Sensor Network

ÚVOD

Koncept Internetu věcí v současnosti zažívá velký rozmach a jedná se o prudce rozvíjející se odvětví s velice širokým záběrem, které zasahuje do každé oblasti lidské činnosti. Tento trend našel své uplatnění v oblasti nositelné elektroniky, autonomních vozidel, inteligentních domácností, inteligentních měst. Zároveň je nedílnou součástí moderního zdravotnictví, dopravy a logistiky nebo různých výrobních odvětví. Díky tomu vznikají odvozené definice jako Internet všeho (IoE), Internet zdravotnických věcí (IoMT), Internet energetiky (Internet of Energy), Internet průmyslových věcí (IIoT) a mnoho dalších. Obecně lze říci, že se jedná o mnoho různých druhů senzorů, které sbírají data o svém okolí. Data, která jsou základem konceptu IoT, jsou následně ukládána a analyzována. Pomocí analýzy je možné z dat vytvářet informace, které jsou srozumitelné a užitečné pro člověka. Na základně těchto informací je umožněno například efektivní řízení zdrojů a poskytování služeb, snazší reportování nebo optimalizace každodenních činností.

Využívání těchto zařízení přináší mnoho užitku, ale nese s sebou i jistá bezpečnostní rizika. Jelikož jsou všechna tato zařízení připojena k síti, tak se mohou snadno stát terčem kybernetického útoku. Často se sbírané údaje týkají polohy a jiných citlivých nebo osobních údajů. V případě útoku cíleným na kritickou infrastrukturu mohou vzniknout závažné škody. Právě z tohoto důvodu je klíčové se bezpečností připojených zařízení do sítě podrobně zabývat. Je velice důležité dbát na důvěrnost, integritu a dostupnost informací při jejich přenosu, ukládání a zpracování.

Tato práce se skládá ze třech hlavních bodů. V první části práce jsou vymezeny základní pojmy ohledně IoT technologií a popsány možnosti využití těchto technologií v prostředí výrobního podniku. Na tuto část volně navazuje vytipování zranitelných míst využívaných technologií ve vztahu ke specifickým podmínkám prostředí výrobního podniku. V poslední části práce jsou charakterizovány čtyři výrobní podniky. Pro tyto podniky jsou navrženy implementace technologií Internet of Things a odpovídající formy zabezpečení těchto řešení.

Hlavním cílem této práce je vyhledat možnosti a rámcově navrhnout realizaci zabezpečení prostředků Internet of Things v provozu výrobního podniku.

1 IOT TECHNOLOGIE A JEJICH VYUŽITÍ VE VÝROBĚ

Průmyslový Internet Věcí (IIoT) je jednou ze součástí konceptu Industry 4.0. Jeho zaměření se soustředí především na to jak inteligentní systémy, propojené senzory a analýza dat získaných ze senzorů může přispět ke zlepšení business-to-business (B2B) iniciativy v celé řadě průmyslových odvětví. Celý koncept IIoT se snaží lépe využívat údaje ze senzorů, komunikaci mezi stroji (M2M), strojové učení a automatizační technologie, které existují již delší dobu v průmyslovém odvětví. V oblasti výroby má využití IIoT velký potenciál především při kontrole kvality, sledovatelnosti dodavatelského řetězce, prediktivní údržbě výrobních strojů a jejich vzdáleném monitoringu. [1]

1.1 IoT ve výrobním podniku

V celém IIoT se lze setkat s mnoha způsoby využití chytrých propojených zařízení. V této kapitole jsou popsány vybrané způsoby využití zařízení IoT v prostředí výrobních podniků.

1.1.1 Prediktivní údržba

Senzory IoT připojené k průmyslovým zařízením mohou v reálném čase shromažďovat údaje související s výkonem, včetně tlaku, vibrací atd. Tyto informace se přenášejí do brány nebo přímo do cloudu a kombinují se s údaji o konfiguraci stroje a s historií jeho používání, aby se zachytily jakékoli neobvyklé vzorce. Díky tomu mají manažeři v podniku přístup k analýze a naplánují další kontroly a údržbu tak, aby byl dopad na výrobní proces minimální. Kromě zkrácení prostojů prediktivní údržba zvyšuje životnost zařízení, snižuje náklady a snižuje riziko nehod. Je efektivnější a bezpečnější náhradou tradiční údržby s plánovanými kontrolami. [2]

Jedním z příkladů jsou pneumatiky pro nákladní automobily s technologií IoT, kde senzory shromažďují údaje o využití pneumatik, aby bylo možné naplánovat jejich údržbu a výměnu, a předejít tak situaci, kdy pneumatika během přepravy praskne, zastaví vozidlo a zpozdí dodávku. Společnost Volvo vybavila svá nákladní vozidla senzory IoT, což vedlo ke zkrácení doby diagnostiky o 70 % a zkrácení doby opravy o 25 %. [3]

Velcí výrobci ztratí ročně přibližně 323 výrobních hodin kvůli prostojům zařízení. Pokud by byly sečteny ušlé tržby a případné finanční sankce za nedodržení termínů, mohou náklady spojené s výpadky strojů dosáhnout u velkých výrobních závodů až 532 000 USD za hodinu. [4]

Nasazení Internetu věcí ve výrobě může odhalit poruchy zařízení v rané fázi, minimalizovat prostoje a podle společnosti McKinsey snížit náklady na údržbu přibližně až o 40 %. [5]

1.1.2 Vzdálený monitoring

Senzory IoT monitorují a shromažďují data týkající se provozu a produktivity strojů a následně tyto informace předávají k analýze. Personál podniku má k těmto informacím přístup v reálném čase. Podnik tak má přehled o chodu celé výrobní linky – od výkonu stroje až po případnou hrozící poruchu. Vzdálené monitorování prostřednictvím IoT totiž dokáže předpovídat poruchy, takže lze přijmout nezbytná opatření ke zkrácení prostojů. Výhody, které IoT ve výrobě nabízí prostřednictvím vzdáleného monitoringu, mohou být snížení nákladů, zkrácení prostojů výrobního zařízení, predikce poruch a maximalizace provozuschopnosti stroje. [6]

Například společnost Armal, přední výrobce přenosných toalet, používá k výrobě svého produktu lisovací zařízení. Za účelem sledování a optimalizaci spotřeby energie lisovacího zařízení nasadila do výroby IoT zařízení. [7]

1.1.3 Bezpečnost pracovníků

Bezpečnost pracovníků patří mezi hlavní priority v každém výrobním podniku. Internet věcí ve výrobě může učinit pracovní prostředí mnohem bezpečnějším. Například kvalitu vzduchu ve výrobní hale lze výrazně zlepšit instalací snímačů HVAC. Software Air Quality Index (AQI) je schopen analyzovat data získaná ze snímačů vzduchu a zajistí, aby kvalita okolního vzduchu byla v předepsaných mezích. Stejně tak lze monitorovat a předcházet dalším nebezpečím nebo úrazům, které ohrožují životy pracovníků. [6]

Například společnost FaceMe se specializuje na technologii rozpoznávání obličeje a tento systém lze propojit s IoT prvky. Systém dokáže zjistit, zda má pracovník správně nasazenou obličejovou masku. To pomáhá předcházet šíření nákazy COVID-19 mezi pracovníky. Na obdobném principu lze kontrolovat i předepsanou výstroj na pracovišti. [8]

Z hlediska bezpečnosti pracovníků nabízí Internet věcí ve výrobě následující výhody – lze předcházet vzniku požáru, lze monitorovat hladinu CO_2, lze rychleji reagovat na mimořádné události nebo jim předcházet. [6]

1.1.4 Kontrola kvality

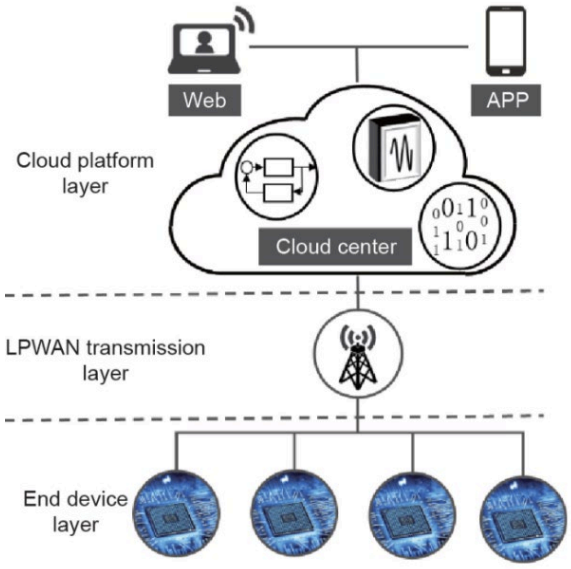
Proces kontroly kvality zajišťuje, že konečný výrobek je bez jakýchkoliv závad a splňuje normy kvality. Pokud je tento proces prováděn správně, přináší výhody jak výrobci, tak zákazníkům. Pokud však proběhne špatně, může poškodit zisky a ohrozit zákazníky. Hlavní přínosy Internetu věcí ve výrobě, pokud jde o kontrolu kvality, může být snadná detekce anomálií v pracovním procesu nebo snadné sledování skladových zásob a skladovacích podmínek po ukončení výroby. [6]

Například katastrofa airbagů Takata vedla k největšímu stažení automobilů z trhu. Týkala se téměř 69 milionů nafukovacích airbagů a společnost přišla o miliardy dolarů. Takovému problému lze předejít účinnou kontrolou kvality. [9]

1.2 IoT technologie a architektura

Koncept IoT propojuje mnoho heterogenních zařízení a systémy prostřednictvím sítě. O architektuře Internetu věcí neexistuje jednotná a obecná shoda, na které by se shodl celý svět a odborníci. Bylo navrženo několik různých architektur, ale podle mnoha odborníků však IoT funguje především na třech vrstvách. Jednotlivé vrstvy se nazývají Fyzická vrstva (také označována jako Perception layer – vrstva vnímaní), Síťová vrstva a Aplikační vrstva. [10]

Tato práce se zabývá právě třívrstvou architekturou, která je popsána v této kapitole. Obrázek 1 zobrazuje jednotlivé vrstvy architektury IoT.



Obrázek 1: Architektura IoT

Zdroj: [11]

1.2.1 Fyzická vrstva

Fyzická vrstva se skládá ze zařízení IoT, která jsou vybavena senzorovými uzly, Bluetooth zařízeními, analogovými senzory, snímači, senzory pro měření a regulaci, digitálními senzory a RFID tagy. Senzorové uzly získávají informace, přenášejí informace v reálném čase a komunikují mezi sebou. Tyto senzorové uzly spotřebovávají málo elektrické energie a vyžadují připojení s nízkou rychlostí přenosu dat. Vytvářejí mezi sebou bezdrátovou senzorovou síť (WSN). Každé zařízení Internetu věcí má svůj univerzální, jedinečný identifikátor (UUID). [12]

1.2.2 Síťová vrstva

Síťová vrstva pomáhá zařízením IoT sdílet informace s ostatními zařízeními. Kromě toho tato vrstva zpracovává velké množství dat generovaných těmito zařízeními IoT. Aby byla zachována komunikace mezi těmito heterogenními zařízeními, měly by být splněny určité požadavky QoS. Síťová vrstva se skládá z mobilních sítí, WLAN, Internetu, databází a WSN. Proto je třeba při návrhu brát v úvahu především latenci, škálovatelnost, požadavky na šířku pásma, energetickou účinnost, bezpečnost a soukromí. [12]

1.2.3 Aplikační vrstva

Aplikační vrstva integruje služby a aplikace v IoT. Tato vrstva vykonává celkový pracovní proces, který zahrnuje výměnu informací, komunikaci, ukládání a správu dat. Kromě toho jsou na této vrstvě prováděny různé formy prediktivní analýzy. Dále tato vrstva udržuje důvěryhodnost dat a využívá informace rozšířené ostatními službami. [12]

1.3 Komunikační technologie LPWAN

V následujících odstavcích jsou popsány komunikační sítě LPWAN, které jsou vytvořeny speciálně pro připojení IoT zařízení. Tyto sítě lze rozdělit na nelicencované a licencované sítě.

Nelicencované sítě jsou volně k dispozici. Jedinou podmínkou je, že uživatelé a připojená zařízení musí dodržovat specifikované podmínky. Hlavní charakteristikou nelicencovaných sítí je absence centrálního řízení. Využívání nelicencované sítě je po finanční stránce méně nákladné oproti využívání licencované sítě. Na druhou stranu uživatelé těchto nelicencovaných sítí nemají záruku, že je po připojení jejich zařízení nebude omezovat rušení signálu. [13]

V případě licencovaných sítí mohou službu využívat pouze její vlastníci. Státy uskutečňují aukce kmitočtů a mobilní operátoři v daném státu kupují určité části frekvenčního spektra.

Dále mobilní operátoři rozdělují určité části frekvenčního spektra svým zákazníkům. Vyžívání licencované sítě bývá zpravidla nákladnější oproti síti nelicencované. [13]

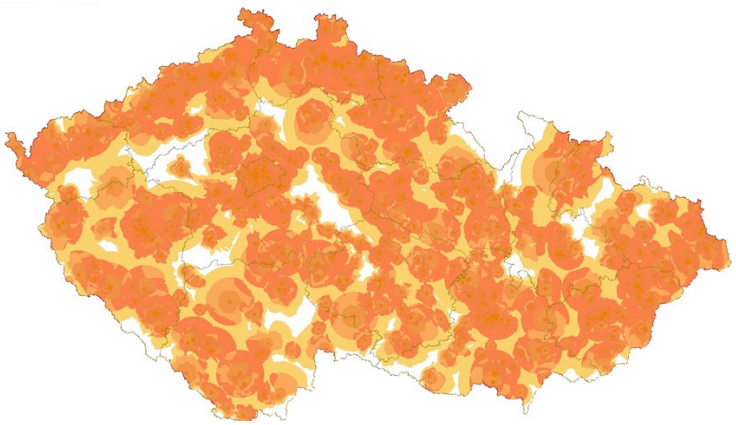
Jako zástupci nelicencovaných sítí jsou dále popsány sítě LoRaWAN společně se sítí Sigfox a jako zástupce licencované sítě je popsáno NB-IoT.

1.3.1 LoRaWAN

LoRaWAN (Long Range Wide Area Network) je síť s nízkými požadavky na spotřebu energie koncových zařízení a podporuje zabezpečenou obousměrnou komunikaci. Pro rádiovou komunikaci využívá, jako ostatní sítě LPWAN, pásmo 868 MHz pro Evropu a přenosová rychlost se pohybuje od 0.3 kb/s do 50 kb/s. Proto se tedy nehodí k přenosu většího objemu dat jako například zvuku nebo videa z IP kamer. Výhodou LoRaWAN sítě je skutečnost, že vznikla za spolupráce více subjektů a díky tomu dokáže spolupracovat se zařízeními od různých výrobců. [14]

IoT síť LoRaWAN v České republice provozuje řada subjektů. Mezi hlavní patří České Radiokomunikace a.s., The Things Network (TTN), Starnet s.r.o. a dále to jsou kraje, města a podniky [15][16][17]. Cena za připojení k LoRaWAN je čistě individuální a závislá na různých faktorech – počet připojených zařízení, počet odchozích zpráv za den, počet příchozích zpráv za den. U České Radiokomunikace lze například zvolit tarifní balíček Pilot s cenou 200 Kč/měsíc, který umožňuje připojení až deseti zařízení v jeden okamžik [18]. Při zvolení celosvětově dostupné platformy The Things Network (TTN) je možné se připojit k již existujícím výchozím bránám v okolí [17].

Obrázek 2 zachycuje stav pokrytí sítí LoRaWAN na území České republiky od společnosti České Radiokomunikace a.s.



Obrázek 2: Stav pokrytí sítě LoRaWAN na území České republiky

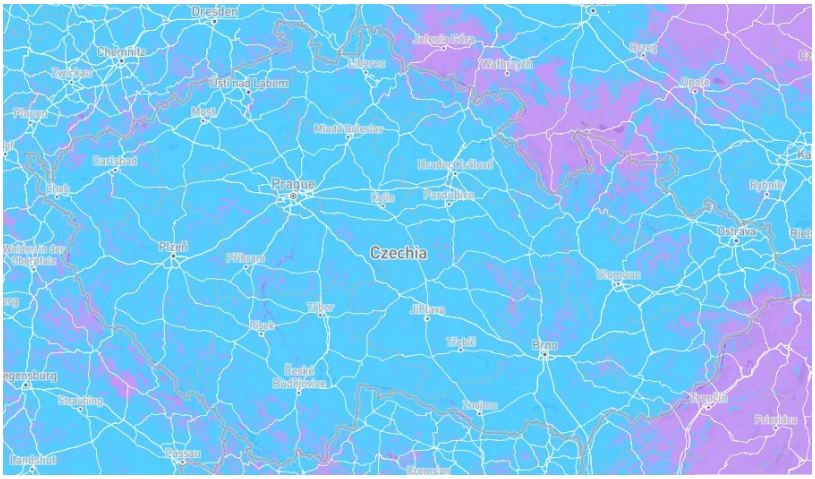
Zdroj: [19]

1.3.2 Sigfox

Přenosovou síť Sigfox vytvořila stejnojmenná francouzská firma. Sigfox využívá, stejně jako LoRaWAN, pásmo 868 MHz pro Evropu. Dle specifikace může zařízení připojeno do této sítě poslat maximálně 144 zpráv za den o délce 0-12 bytů. Kombinací malého objemu dat a nízké přenosové rychlosti se značně snižuje spotřeba energie daného zařízení. Sigfox, stejně jako síť LoRaWAN, není vhodný pro přenos velkého objemu dat z důvodu nízké přenosové rychlosti. Oproti LoRaWAN Sigfox slouží pouze pro jednosměrnou komunikaci. To znamená, že kdyby uživatel obdržel od senzoru informaci o příliš vysoké teplotě ve výrobní hale, tak už není schopen přes síť Sigfox zpět vykonat akci – spustit klimatizaci. [20]

Základní cena připojení do sítě Sigfox, dle webových stránek výrobce, začíná na 140 Kč za jedno zařízení na dobu jednoho roku. Při využití tohoto balíčku zařízení může odeslat maximálně 3 zprávy denně. Maximální počet odeslaných zpráv, tedy 144 zpráv denně, je dostupný až od tarifního balíčku Ultra s cenou 247 Kč za jedno zařízení na dobu jednoho roku. [21]

V České republice síť aktuálně pokrývá 94 % území a zasahuje i do míst bez dosahu GSM signálu mobilních operátorů [22]. Obrázek 3 zachycuje stav pokrytí sítí Sigfox na území České republiky.



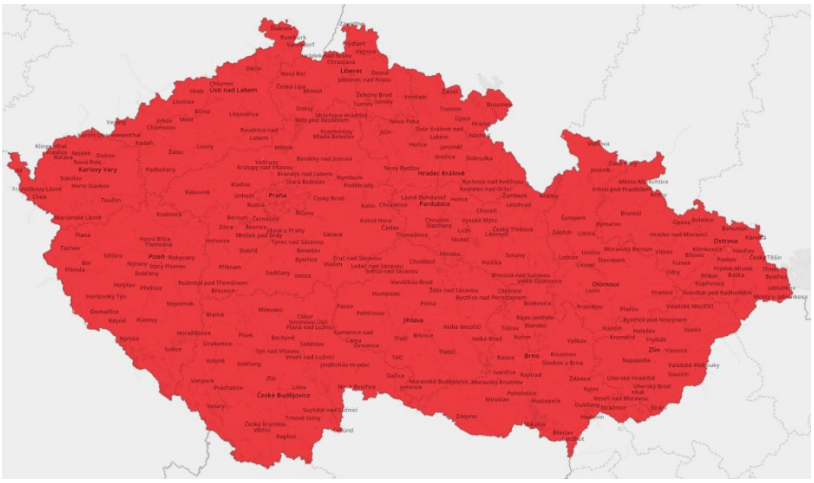
Obrázek 3: Stav pokrytí sítě Sigfox na území České republiky

Zdroj: [23]

1.3.3 NB-IoT

NarrowBand-IoT (NB-IoT) komunikuje v úzkém pásmu LTE, ale v případě této sítě nejsou vyžadovány vysoké přenosové rychlosti jako u LTE. Jelikož síť spadá pod mobilního operátora, tak je její využívání plně zpoplatněno. Na území České republiky je tato síť provozována mobilními operátory Vodafone, O2 a T-Mobile. U NB-IoT je především kladen důraz na maximální pokrytí sítě a maximální kapacitu sítě. NB-IoT je oproti sítím LoRaWAN a SigFox náročnější na spotřebu energie. Stejně jako síť LoRaWAN poskytuje obousměrnou komunikaci. Zařízení podporující NB-IoT musejí pro komunikaci obsahovat SIM kartu. Zákazník takové zařízení při spuštění aktivuje a následně se zařízení propojí s NB-IoT sítí. V případě NB-IoT nelze přesně určit cenu za připojená zařízení bez udání přesného počtu zařízení a objemu přenesených dat. Ceny se budou lišit dle smlouvy klienta s mobilním operátorem. [20]

Obrázek 4 zachycuje stav pokrytí sítí NB-IoT na území České republiky od společnosti Vodafone. Jelikož mobilní operátor Vodafone využívá svou stávající infrastrukturu vysílačů, tak nemusí budovat novou síť a dosáhl téměř 100% pokrytí území České republiky.



Obrázek 4: Stav pokrytí sítě NB-IoT na území České republiky

Zdroj: [24]

2 ZRANITELNOST IOT INFRASTRUKTURY

Se zaváděním Internetu věcí (IoT) do výroby vznikají i nové hrozby. Poznatky získané z dat shromážděných z IoT zařízení se využívají napříč průmyslovými odvětvími. Zejména ke zlepšení produktivity, řešení problémů, vytváření nových obchodních příležitostí a udržení provozní efektivity. Existují však také nemalá rizika. Zejména pro první generace prvků Internetu věcí byla bezpečnost pouze dodatečná myšlenka, což vytvářelo zranitelná místa a potenciál pro narušení průmyslových procesů nebo špionáž. Právě proto by průmyslové podniky společně s výrobci IoT komponent neměli opomíjet, při zavádění Internetu věcí (IoT) do provozu, strategie pro zmírnění a řízení takovýchto kybernetických rizik.

Jedna studie provedená společností Nippon Telegraph and Telephone (NTT) tvrdí, že výrobci zaznamenali v roce 2020 meziroční nárůst hrozeb o 300 %. Útočníci považují závazky výrobního podniku vůči navazujícím partnerům za páku, kterou mohou vymáhat výkupné v případě přerušení provozu výrobního podniku. [25]

Dle studie společnosti Fictiv z roku 2021 91 % výrobců hlásilo zvýšení investic a ještě více (95 %) uvedlo, že digitální transformace je pro jejich budoucí úspěch zásadní [26]. Ta může mít mnoho podob – od systémů Internetu věcí až po cloudovou infrastrukturu, aplikace a služby. Jak zdůrazňuje studie Trend Micro z roku 2020, může to také znamenat sbližování IT a OT systémů s cílem zlepšit efektivitu a rychlost ve výrobní hale – tím se ale také zvyšuje kybernetické riziko [27].

Průzkum magazínu Industry Europe zjistil, že v mnoha výrobních IT/OT prostředích běží ransomware nebo malware pro těžbu kryptoměn. Těžba kryptoměn je náročná na zdroje a mohla by opotřebovávat výrobní zařízení a zároveň zvyšovat náklady na energii. V neposlední řadě ransomware může zablokovat celé výrobní linky. Existuje však také riziko krádeže duševního vlastnictví. [28]

Dopad těchto hrozeb na podnikání by se neměl podceňovat. Průměrné náklady na únik dat v průmyslovém sektoru byly v roce 2021 odhadnuty na více než 4,2 milionu dolarů dle průzkumu společnosti IBM [29]. Některé útoky však mohou způsobit mnohem větší škody. Norský výrobce hliníku Norsk Hydro předpokládal po výpadku provozu způsobeným ransomwarem v roce 2019 ztrátu 75 milionů dolarů [30].

2.1 Zranitelná místa z pohledu architektury IoT

V architektuře systémů IoT čelí jednotlivé vrstvy IoT různým útokům a rizikům. V této kapitole jsou uvedena zranitelná místa s ohledem na jednotlivé vrstvy.

2.1.1 Zranitelná místa fyzické vrstvy

Na fyzické vrstvě může vzniknout hned několik bezpečnostních problémů. Prvky IoT operující na fyzických vrstvách jsou převážně senzory a RFID tagy, které mají omezený výpočetní výkon a úložiště, což je činí náchylnými k mnoha druhům hrozeb a útoků [12]. Pokud senzory IoT pracují ve venkovním prostředí, tak může dojít k fyzickým útokům na senzory a zařízení IoT, při nichž je útočník schopen manipulovat s hardwarovými součástmi zařízení.

Důvěrnost této vrstvy lze snadno zneužít útokem typu Replay Attack, který lze provést podvržením, pozměněním nebo přehráním informací o identitě jednoho ze zařízení v IoT. Dalším možným útokem ohrožujícím důvěrnost může být útok typu Node Capture, při kterém je útočník schopen zachytit všechny informace a data ze zařízení. Zařízení na fyzické vrstvě jsou také náchylná na útok typu DoS. [31]

Bezpečnostní problémy na fyzické vrstvě lze řešit pomocí šifrování (které může být point-to-point nebo end-to-end), autentizací (k ověření skutečné identity odesílatele) a řízením přístupu. [32]

2.1.2 Zranitelná místa síťové vrstvy

Síťová vrstva je zodpovědná za vzájemné propojení IoT prvků, síťových zařízení a celých sítí. Přenos informací získaných z fyzických objektů prostřednictvím senzorů může být realizován pomocí drátové nebo bezdrátové technologie. Proto je tato vrstva velmi citlivá na útoky ze strany útočníků. Mezi největší bezpečnostní problémy patří narušení integrity a důvěrnosti informací, které jsou v síti přenášeny [32].

V síťové vrstvě představují nebezpečí útoky typu Man-in-the-middle, při kterém může útočník odposlechnout přenášené informace po síti a bude tak narušena důvěrnost v síti. Nutná je také prevence proti útokům typu DoS. [31]

Prvky na síťové vrstvě musí mít možnost znát stav sítě a schopnost chránit se před případnými útoky na síť. Toho lze dosáhnout bezpečnostními protokoly a také softwarem, který prvkům umožní reagovat na všechny situace a chování, které lze považovat za abnormální nebo mohou ovlivnit jejich bezpečnost. Jedním z problémů může být

kompatibilita z důvodu velké rozmanitosti prvků IoT. Tato rozmanitost ztěžuje používání současných síťových protokolů. [32]

2.1.3 Zranitelná místa aplikační vrstvy

V případě aplikační vrstvy závisí potřeby zabezpečení na typu aplikace, ale většinou se týkají ochrany soukromí dat a řízení přístupu.

Mezi obvyklé zranitelnosti na této vrstvě patří DoS útok, při kterém může útočník znemožnit přístup do administrace aplikace. Dále to může být útok typu Cross Site Scripting, kdy např. formulářové pole v aplikaci nekontroluje vstup na přítomnost škodlivého JavaScriptového kódu. Tímto způsobem může útočník zcela změnit obsah aplikace podle svých potřeb a zneužít informace v aplikaci ve svůj prospěch. V neposlední řadě zde hrozí typické útoky malwarem. Ke zmírnění hrozeb by měl být využit pro přístup do administrace webové aplikace šifrovaný TLS kanál. [31]

2.2 Specifické hrozby pro výrobní podnik

V následujících odstavcích jsou uvedeny specifické hrozby, kterým mohou čelit výrobní podniky při digitalizaci výroby, zavádění IoT do provozu a jeho dalším využívání.

2.2.1 Používání zastaralého operačního systému

Jedním z problémů může být používání zastaralého operačního systému. Tato situace je s největší pravděpodobností způsobena kombinací mentality „nesahat na fungující systém“ a dlouhého cyklu výměny hardwarového a softwarového vybavení. Ve výrobním odvětví je častým jevem, že softwarové komponenty a ovladače, které podporují specializovaná zařízení, nemusí být kompatibilní s novějšími operačními systémy. [33]

2.2.2 Šíření síťových červů

Jedním z vedlejších účinků starých a nepodporovaných operačních systémů ve výrobním průmyslu je přítomnost velkého počtu zranitelností, které mohou být zneužity starými variantami síťového malwaru. Detekce malwaru jako jsou Downad (alias Conficker), WannaCry (WCry) a Gamarue (Andromeda), jsou na strojích používaných ve výrobních prostředích poměrně časté. Downad (alias Conficker) je červ, který se šíří zneužitím staré zranitelnosti v systémech Windows nebo také prostřednictvím vyměnitelných disků (USB) a síťových sdílení. Downadu se daří ve velkých průmyslových podnicích, protože modernizace systémů může být pro kontinuitu podnikání zádrhelem. [33]

2.2.3 Zranitelnost automatického spuštění prostřednictvím USB

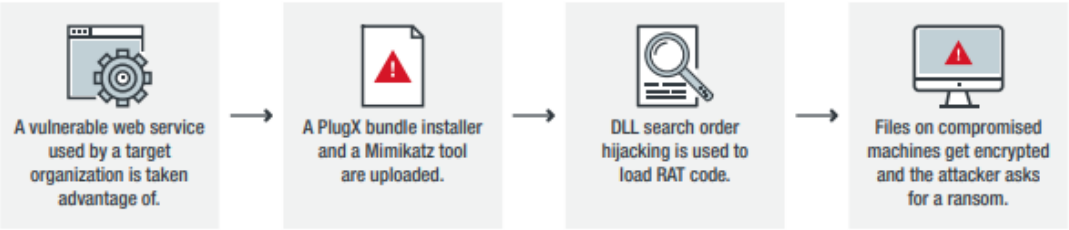
Další zranitelností je šíření škodlivého softwaru prostřednictvím USB. Při takovém útoku je zneužit soubor autorun.inf, pomocí kterého se může automaticky spustit škodlivý kód, kdykoli je připojeno infikované vyměnitelné zařízení. Toto riziko odráží běžnou praxi v tomto odvětví, kdy se ve výrobním prostředí používají jednotky USB ke kopírování a přenosu informací mezi počítači a sítěmi. [33]

2.2.4 Ransomware a software pro těžbu kryptoměn

Výrobní podniky mohou čelit cíleným kampaním za účelem narušení výroby nebo znemožnění dodat službu. Mohou také čelit příležitostným hackerským útokům.

PlugX je pokročilý nástroj pro vzdálený přístup (RAT – Remote Access Trojan), který se běžně používá při cílených útocích za účelem špionáže nebo úniku informací. Od září 2017 útočník kompromitoval několik výrobních společností a na napadené stroje nasadil PlugX RAT, aby si zajistil vzdálený přístup k těmto prostředkům. Ve všech případech došlo k počátečnímu narušení prostřednictvím zranitelné webové služby napadené organizace. Jakmile byl stroj kompromitován, tak v poslední fázi útočník zašifroval soubory na napadených strojích a zanechal majiteli systému vzkaz s žádostí o výkupné. Dále útočník na napadené počítače nasadil a spustil také software pro těžbu kryptoměn. [33]

Obrázek 5 popisuje postup útoku typu PlugX.



Obrázek 5: Postup útoku typu PlugX

Zdroj: [33]

Útok škodlivým softwarem pro těžbu kryptoměn je ve výrobních podnicích poměrně častý. Používáním zastaralého hardwaru a softwaru na zařízeních, může být toto riziko mnohem větší. Další hrozbou jsou útoky ransomwaru, které zasáhnou přímo výrobní linky. To se stalo několika výrobcům automobilů během nákazy ransomwarem WannaCry v květnu 2017 a výrobci čipů, který musel po napadení novou variantou WannaCry v srpnu 2018 uzavřít několik svých továren. Dalším příkladem je ransomware LockerGoga, který zasáhl norského výrobce hliníku a tím donutil podnik přejít na ruční provoz. [33]

V případě ransomwaru může být výrobní podnik postižen nejen náklady na obnovu dat, ale odstávka výroby může mít za následek obrovské finanční ztráty.

2.3 Bezpečnostní doporučení pro zavádění IoT do výrobního podniku

Výrobní podniky se mohou vyhnout zbytečným bezpečnostním problémům a finančním ztrátám zavedením základních osvědčených postupů, jako jsou následující:

- Osoby, kterým je udělen přístup k souborům a systémům, by měly být identifikovány a měla by jim být přidělena co nejomezenější oprávnění. Pokud by neměly mít možnost měnit informace, měl by jim být přidělen přístup pouze pro čtení. [33]
- Měly by být identifikovány IT zařízení a produkční stroje, které mohou vzájemně komunikovat. Měla by být stanovena omezení, která zařízení v síti IT by měla být schopna výměny informací s kterými zařízeními v síti OT. [33]
- Nepotřebné služby v síti by měly být zakázány. Tímto způsobem lze zabránit zneužití zranitelných služeb. [33]

Dalším doporučeným přístupem k zabezpečení výrobních podniků zavádějících IoT do výroby je sladění se s normami kybernetické bezpečnosti IEC 62443. Normy zahrnují několik aspektů, jako jsou požadavky na systém řízení bezpečnosti ICS, bezpečnostní technologie pro ICS a bezpečné životní cykly vývoje produktů. Obecně se označují jako průmyslové normy pro vlastníky majetku, systémové integrátory a výrobce zařízení. [34][35]

Bezpečnost je pro úspěšné zavedení prvků IoT do výroby zásadní. Odolnost výrobních procesů silně závisí na povědomí výrobních podniků o současném prostředí hrozeb a na použitém bezpečnostním rámci pro ochranu před útoky.

2.4 OWASP IoT Top 10

Nezisková nadace OWASP, celým názvem Open Web Application Security Project, pracuje na zlepšení bezpečnosti softwaru. Tato kapitola popisuje základní doporučení projektu OWASP Internet of Things Top 10, který má za cíl pomoci vývojářům, výrobcům, podnikům a spotřebitelům lépe se rozhodovat při vytváření a používání systémů Internetu věcí. Jedná se o deset nejzávažnějších věcí, jichž je třeba se vyvarovat při vytváření, nasazování nebo správě systémů IoT. Dále bude z této metodiky čerpáno při návrhu zabezpečení pro jednotlivé modelové subjekty v další části práce.

Následující seznam zranitelností je převážně čerpán ze zdroje [36].

Slabá, odhadnutelná nebo pevně zakódovaná hesla

Zařízení Internetu věcí se slabými výchozími hesly jsou náchylná ke kybernetickým útokům. Výrobci a uživatelé zařízení IoT musí věnovat pozornost nastavení hesel při spuštění zařízení. Buď zařízení neumožňuje uživatelům změnit výchozí heslo, nebo je uživatelé raději nemění, i když mohou. Úspěšný pokus o získání neoprávněného přístupu do jednoho zařízení navíc zanechává ostatní zařízení v systému zranitelná, protože zařízení IoT často sdílejí stejná výchozí hesla.

Nezabezpečené síťové služby

Síťové služby spuštěné v zařízení mohou představovat hrozbu pro bezpečnost a integritu systému. Pokud jsou tyto služby volně přístupné z Internetu, otevírají cestu k neoprávněnému vzdálenému přístupu a úniku dat. Útočníci mohou úspěšně ohrozit bezpečnost koncového zařízení IoT tím, že využijí slabin v modelu síťové komunikace.

Nezabezpečená rozhraní systému

Existuje několik rozhraní, jako je webové rozhraní, backend API, cloud a mobilní rozhraní, která umožňují interakci uživatele se zařízením. Nedostatečná autentizace, špatné šifrování a filtrování dat však mohou mít negativní dopad na bezpečnost chytrých zařízení. Mezi nejčastější problémy se řadí absence autentizace, slabé nebo vůbec žádné šifrování a v neposlední řadě nedostatek filtrování vstupů a výstupů.

Nedostatek bezpečného aktualizačního mechanismu

Mezi další zranitelnost se řadí neschopnost zařízení bezpečné aktualizace. Mezi příčiny ohrožení bezpečnosti chytrých zařízení Internetu věcí se nejčastěji řadí absence validace firmwaru, absence oznámení o bezpečnostních aktualizacích a nešifrovaný přenos dat.

Používání nezabezpečených nebo zastaralých komponent

Tento bezpečnostní problém se týká především využívání hardwaru a softwaru třetích stran. Ty mohou potencionálně přinést rizika a ohrozit bezpečnost celého systému. Průmyslový Internet věcí (IIoT) je vybaven zejména systémy, které se obtížně aktualizují a udržují. Takové zranitelnosti mohou být využity k útoku a narušení funkčnosti zařízení.

Nedostatečná ochrana soukromí

Zařízení Internetu věcí mohou pro správnou funkci ukládat a uchovávat citlivé informace o uživatelích. Tato zařízení však často nenabízejí bezpečné úložiště, což vede k úniku kritických dat při napadení kyberzločinci. Kromě zařízení jsou k útokům náchylné také

databáze výrobců. Šifrovaný provoz může být zárukou bezpečné komunikace, ale stále je náchylný k hrozbám.

Nezabezpečený přenos a ukládání dat

Nedostatečné šifrování při manipulaci s citlivými údaji, ať už při přenosu, zpracování nebo v klidovém stavu, je příležitostí pro hackery, aby data ukradli a odhalili. Šifrování je nezbytné všude tam, kde dochází k přenosu dat.

Nedostatečná správa zařízení

Jedná se o neschopnost účinně zabezpečit všechna zařízení v síti. Systém je tak vystaven mnoha hrozbám. Bez ohledu na počet zapojených zařízení nebo jejich velikost je třeba každé z nich chránit před narušením dat.

Nezabezpečené výchozí nastavení

Stávající zranitelnosti ve výchozím nastavení vystavují celý systém řadě bezpečnostních problémů. Mohou to být výchozí hesla, neschopnost aktualizace zabezpečení a přítomnost zastaralých součástí.

Nedostatek fyzického zabezpečení

Nedostatečné fyzické zabezpečení, které umožňuje potenciálním útočníkům získat citlivé informace, které mohou pomoci při budoucím vzdáleném útoku nebo převzít místní kontrolu nad zařízením. Nezabezpečení konfiguračních portů nebo vyjmutí paměťové karty může kvůli nedostatečnému fyzickému zabezpečení vystavit systém útokům.

2.5 Ukázka reálných zranitelností

Tato kapitola představuje reálné zranitelnosti zařízení připojených k síti v prostředí výrobních podniků. V rámci vlastního zkoumání těchto zranitelností bylo nalezeno několik případů, které budou v následujících odstavcích blíže popsány.

K nalezení zranitelných míst poslouží vyhledávač Shodan.io, který umožňuje vyhledávat fyzická zařízení připojená k Internetu. Zásadním rozdílem mezi vyhledávačem Shodan.io a vyhledávačem Google je, že Shodan.io prohledává otevřené porty zařízení, zatímco Google prohledává pouze webové stránky. V případě využití vyhledávače Shodan.io je důležité mít vytvořen uživatelský účet, který je s omezenou funkčností dostupný zdarma a porozumět syntaxi vyhledávacího dotazu.

Při zadání vyhledávacího dotazu *screenshot.label:"ics"* jsou zobrazena administrátorská monitorovací rozhraní a síťové servery na nichž běží systémy řízení výroby z celého světa. Využitím tohoto vyhledávacího dotazu je možné volně získat jejich náhledový obrázek. Příloha A, Příloha B a Příloha D slouží jako názorná ukázka nesprávně zabezpečených administrátorských rozhraní systémů řízení výroby.

Na podobném principu je možné zkoumat i nezabezpečené IP kamery. Při zadání vyhledávacího dotazu *has_screenshot: true* jsou zobrazeny volně přístupné a nezabezpečené IP kamery. Příloha C slouží jako názorná ukázka nesprávně zabezpečené IP kamery. Pro přístup k nezabezpečeným IP kamerám z celého světa může být také využita webová stránka Insecam.org jako alternativa vyhledávače Shodan.io.

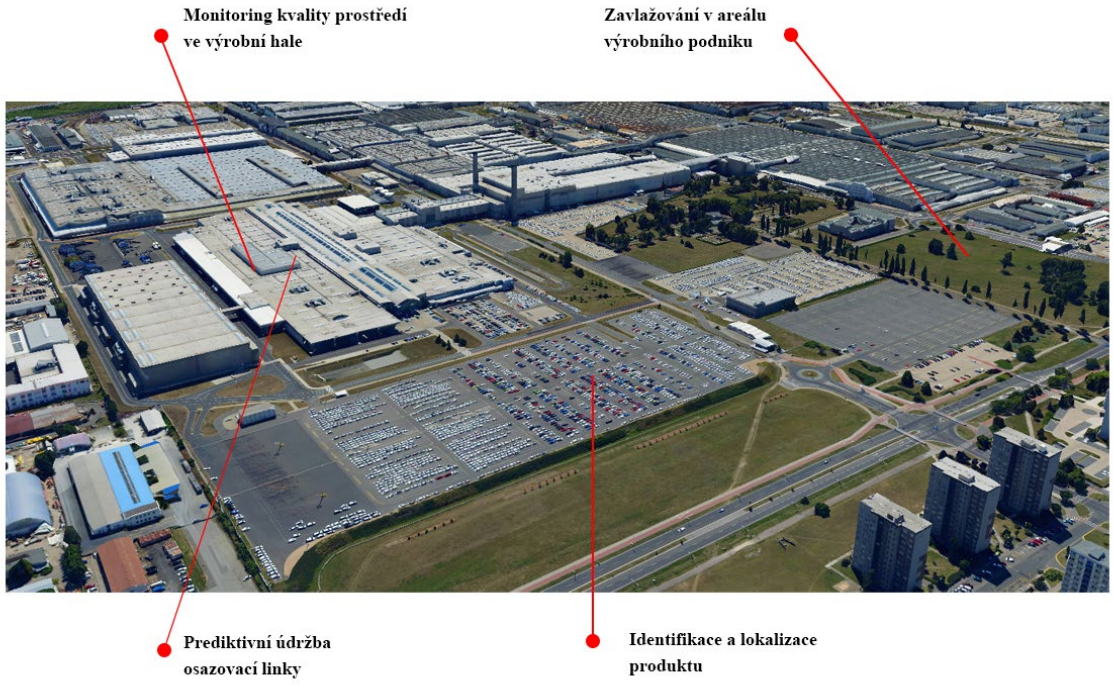
V této práci je zachycen pouze zlomek příkladů, které slouží k názorné demonstraci zranitelností zařízení připojených k Internetu. Jelikož taková nezabezpečená zařízení představují velké riziko pro jejich uživatele, je nutné se jejich zabezpečením podrobněji zabývat.

3 ZABEZPEČENÍ PRO VYBRANÉ MODELOVÉ SUBJEKTY

V této kapitole jsou uvedeny příležitosti využití prostředků Internet of Things v modelových výrobních podnicích. Dále jsou navrženy odpovídající formy zabezpečení jednotlivých prvků IoT a přenosových cest.

Pro potřebu této práce jsou charakterizovány čtyři výrobní podniky, které jsou specifikovány několika vlastnostmi. Tyto podniky poskytnou možnosti pro využití prvků IoT s cílem řešení problémů ve výrobě, sledování ideálních podmínek na pracovišti nebo zajištění bezpečnosti pracovníků.

Obrázek 6 znázorňuje jednotlivé případy užití, které jsou blíže popsány v této kapitole. Konkrétně se jedná o Prediktivní údržbu osazovací linky, Identifikaci a lokalizaci produktu, Monitoring kvality prostředí ve výrobní hale a Zavlažování v areálu výrobního podniku. Obrázek 6 má čistě ilustrativní charakter.



Obrázek 6: Ilustrativní zobrazení využití IoT technologií

Zdroj: vlastní zpracování s využitím Mapy.cz

3.1 Výrobní podnik A

Výrobní podnik A se zabývá výrobou automobilů. Ve výrobních halách podniku, konkrétně v montážním oddělení, se nacházejí tzv. osazovací linky, které jsou neodmyslitelnou součástí výroby. Na lince může dojít k výpadku provozu například z důvodu poruchy motoru. Tyto výpadky následně mají dopad na kompletní proces montáže automobilů a podniku způsobují velké ztráty. Jednou z příčin takového výpadku může být přehřátý motor osazovací linky. Takové situaci lze předcházet pravidelným monitoringem teploty osazovací linky a včasným nahlášením zvýšených teplot personálu podniku.

3.1.1 Návrh implementace IoT zařízení

Prediktivní údržba osazovací linky

Jedním z řešení, jak předejít výpadku, jsou senzory, které budou teplotu výrobní linky snímat a včas zahlásí odchylku od požadovaného stavu. Senzory fungují při nízké spotřebě a s běžnými alkalickými bateriemi. Samotný IoT modul komunikuje v pásmu 868 MHz upraveným rádiovým protokolem sub-GHz. Dále modul obsahuje teplotní senzor pro snímání teploty motoru osazovací linky. Jako brána komunikace zde slouží systém Raspberry Pi. Přijímá data z teplotních senzorů a sítí LoRaWAN je dále zasílá do cloudu k dalšímu zpracování a jejich vizualizaci.

Při překročení teploty osazovací linky odešle notifikační služba e-mail údržbě podniku s touto informací. Údržba následně může provést kroky, které povedou k zachování kontinuity výroby a nedojde k jejímu nečekanému výpadku.

V tomto řešení je využit teplotní senzor s názvem LR TEMP od francouzské společnosti ELA Innovation (Obrázek 7).

Obrázek 7: Teplotní senzor LR TEMP

Zdroj: [37]

3.1.2 Návrh zabezpečení

Fyzické:

Z pohledu fyzické bezpečnosti je důležité senzory zabezpečit proti neoprávněné manipulaci a přístupu. Mohlo by dojít k podvržení dat – například ohřátím tepelného senzoru pomocí zapalovače. Jelikož je v tomto případu modul umístěn uvnitř osazovací linky u jejího motoru, tak se k němu dostane pouze pracovník údržby a takovéto podvržení dat zde nehrozí. Dále musí být zabezpečen servisní port modulu a nastaveno dostatečné silné heslo pro přístup do nastavení systému, aby nemohlo dojít k narušení konfigurace. Samotný modul disponuje stupněm krytí IP68, který je definovaný normou ČSN EN 60529. Je tedy optimálně zabezpečen proti vniknutí cizích těles (prach, nečistota) a také proti vniknutí tekutin.

Síťové:

Po stránce síťové je ke komunikaci využita technologie LoRaWAN, která využívá šifrování AES-128. Každé IoT zařízení může spolupracovat se sítí LoRaWAN až po jeho aktivaci. Aktivace může být provedena dvěma způsoby – buďto dynamicky OTAA (Over-The-Air Activation) nebo staticky APB (Activation By Personalisation). Na úrovni aplikace se k šifrování zpráv využívá klíč aplikační relace (AppSKey) a na úrovni LoRa se využívá klíč síťové relace (NwkSKey). [38]

Klíč aplikační relace (AppSKey) – tento klíč je zodpovědný za end-to-end šifrování uživatelských dat. Jedná se o 128bitový klíč AES, který je pro každé zařízení jedinečný a je sdílen mezi zařízením a aplikačním serverem. Klíč aplikační relace šifruje a dešifruje datové zprávy aplikace a zabezpečuje přenášená data.

Klíč síťové relace (NwkSKey) – se stará o bezpečnostní mechanismus síťové vrstvy. Tento klíč je jedinečný pro každé koncové zařízení a je sdílen mezi koncovým zařízením a síťovým serverem. Klíč síťové relace zajišťuje integritu zpráv během komunikace a zabezpečuje komunikaci z koncových zařízení na síťový server.

Tyto dva klíče (NwkSKey a AppSKey) jsou pro každé zařízení a relaci jedinečné. Pokud je zařízení aktivováno dynamicky (OTAA), jsou tyto klíče generovány znovu při každé aktivaci. Pokud je zařízení aktivováno staticky (ABP), zůstávají tyto klíče zachovány, dokud nejsou ručně změněny.

Tímto mechanismem je zajištěna důvěrnost a integrita při přenosu dat mezi koncovými body. Využití oddělené sítě pro komunikaci IoT zařízení od interní podnikové sítě je

důležitým prvkem bezpečnosti. Díky tomu je komunikace prostředků IoT situována v oddělené síťové vrstvě a je tak odstíněna od interní podnikové sítě.

V tomto řešení je předpoklad, že servery v cloudu jsou optimálně zabezpečeny a splňují normy kvality ISO 9001:2009 a zabezpečení ISO 27001:2014.

Aplikační:

Po aplikační stránce je zde využit MQTT protokol pro zasílání zpráv IoT. Tento protokol využívá pro zasílání šifrovaný TLS kanál a autentizuje klienty pomocí autentizačního protokolu jako například OAuth [39]. Dále by měly být změněny výchozí přihlašovací údaje do aplikace a nastaveno optimálně silné heslo. Formulářová pole v aplikačním prostředí by měla kontrolovat vstup na přítomnost škodlivého Javascriptového kódu a tím by se měl eliminovat útok typu Cross-site scripting.

3.2 Výrobní podnik B

Výrobní podnik B se zabývá, stejně jako Výrobní podnik A, výrobou automobilů. Vyrobené automobily jsou zaparkovány na rozsáhlých parkovištích podniku – tyto parkovací prostory zabírají řádově několik tisíc parkovacích míst. Podnik potřebuje vyrobené automobily expedovat ke koncovému zákazníkovi, uskutečnit jejich pravidelnou servisní prohlídku anebo provést testovací jízdu. V takovém případě nastává problém s jednoznačnou identifikací a lokalizací konkrétního vyrobeného automobilu na takto rozsáhlých parkovacích místech.

3.2.1 Návrh implementace IoT zařízení

Identifikace a lokalizace produktu

Jedním z řešení tohoto problému mohou být lokalizační senzory, které jsou umístěny uvnitř každého vyrobeného automobilu. Senzor posílá do informačního systému podniku přesnou polohu vozidla a tím je docílena dohledatelnost konkrétního vyrobeného kusu. Dále senzor může sledovat teplotu v automobilu, zrychlení, kolizi či opuštění areálu podniku. Díky malým rozměrům lze senzor jednoduše přenášet a lze jej umístit kamkoliv ve vyrobeném automobilu.

Modul nabízí možnost lokalizace vícero metodami a to pomocí LoW Power GPS, WiFi, Bluetooth Low Energy (BLE) anebo LoRaWAN. Pro komunikaci s cloudem je využita síť LoRaWAN. Získaná data jsou dále zpracována a využita v informačním systému podniku.

V tomto řešení je využit senzor s názvem Micro Tracker od francouzské společnosti Abeeway (Obrázek 8).

Obrázek 8: Senzor Micro Tracker

Zdroj: [40]

Inteligentní řešení pro identifikaci a lokalizaci produktu nabízí v České republice například firma reBIT TECH s.r.o. [41].

3.2.2 Návrh zabezpečení

Fyzické:

Jelikož je modul volně umístěn v automobilu, tak by měl být odolný proti otřesům a neopatrnému zacházení ze strany zaměstnanců podniku. Dále modul disponuje servisním Micro USB portem pro jeho konfiguraci. Přístup do konfigurace modulu musí být ošetřen dostatečně silným heslem. Toto řešení počítá s optimálním zabezpečením areálu podniku a jeho parkoviště, a proto by k modulu neměly mít fyzický přístup nepovolané osoby.

Síťové:

K přenosu dat o poloze mezi senzorem a cloudem by mohla být využita síť GSM/GPRS, ale tento standard nezaručuje optimální ochranu přenášených dat. Standard GPRS využívá k zajištění soukromí proudovou šifru A5/1 a v průběhu let byla zjištěna řada vážných slabin v této šifře. Proto je v tomto případu využita pro přenos dat síť LoRaWAN. Zabezpečení sítě LoRaWAN bylo detailně popsáno v kapitole 3.1.2. GPS přijímač v modulu slouží pouze pro příjem signálů z družic GPS, takže není nutné ho dále jakkoliv zabezpečovat.

Aplikační:

Po aplikační stránce je potřeba změnit výchozí přístupové údaje do aplikace a nastavit optimálně silné heslo. V případě citlivých dat by mohla být využita dvoufaktorová autentizace pro přístup do aplikace. Dvoufaktorová autentizace je založena na prokázání dvou faktorů – prvním faktorem bývá jméno a heslo a druhý faktor může být otisk prstu, PIN, elektronický token nebo snímek sítnice oka. Formulářová pole v aplikačním prostředí by měla kontrolovat vstup na přítomnost škodlivého kódu.

3.3 Výrobní podnik C

Výrobní podnik C se zabývá produkcí balených minerálních vod. Jelikož je při výrobě kladen veliký důraz na kvalitu výrobního prostředí, rozhodlo vedení podniku o zavedení monitoringu kvality prostředí ve svých halách. Důraz na kvalitu výrobního prostředí je kladen především kvůli vyráběnému produktu a vhodnému pracovnímu prostředí pro zaměstnance podniku.

3.3.1 Návrh implementace IoT zařízení

Monitoring kvality prostředí ve výrobní hale

Jako ideální a neinvazivní řešení mohou být chytré senzory. Tyto senzory monitorují přítomnost oxidu uhličitého, těkavých organických látek, aktuální teplotu vzduchu a jeho vlhkost. Všechny tyto veličiny jsou důležité pro stanovení kvality prostředí na pracovišti. Senzory se umístí na vytipovaná místa v halách podniku, kde mohou monitorovat aktuální stav prostředí v pravidelných intervalech. Naměřená data se dále odesílají do cloudu. Oprávnění uživatelé tak v aplikaci uvidí aktuální úroveň naměřených hodnot. V případě odchylek od optimálního stavu systém dokáže, na základě dat naměřených ze senzorů, upravit klimatizaci a další výbavu výrobní haly tak, aby byly podmínky pro výrobu v optimální normě.

V tomto řešení může být využit senzor s názvem ModemLabs NB-IoT Air Quality PM2.5 Sensor od společnosti ModemLabs Company (Obrázek 9). Senzor je napájen pouze alkalickými AA bateriemi a díky tomu jejich výrobce deklaruje bezúdržbový provoz po dobu nejméně pěti let. Síťová komunikace probíhá v pásmu 868 MHz a pro přenos naměřených dat na cloudový server je využita komunikační síť NB-IoT. Díky bezdrátové komunikaci je zajištěna i snadná bezdrátová montáž do provozu.

Obrázek 9: Senzor ModemLabs NB-IoT Air Quality PM2.5

Zdroj: [42]

Obrázek 10 zobrazuje praktickou ukázku, jak může vypadat podoba grafické vizualizace naměřených hodnot z chytrých senzorů v praxi. Jsou zde vyobrazeny naměřené teploty z jednotlivých senzorů v prostorech podniku a hodnoty koncentrace CO_2. Tento pohled pochází ze společnosti Ondrášovka a.s.

Obrázek 10: Vizualizace v aplikačním prostředí společnosti Ondrášovka a.s.

Zdroj: [43]

3.3.2 Návrh zabezpečení

Fyzické:

Z hlediska fyzického zabezpečení je senzor třeba umístit do vhodných míst, kde k němu nebude snadný fyzický přístup, ale zároveň senzor musí spolehlivě získávat potřebná data. Omezení fyzického přístupu může zamezit podvržení dat a zkreslení měření. K takovému stavu může dojít úmyslným ohříváním senzoru nebo úmyslným zvýšením koncentrace kouře v jeho blízkosti.

Síťové:

V tomto řešení je použita komunikační síť NB-IoT (NarrowBand-IoT), která přenáší data prostřednictvím rozhraní LTE Cat-NB1. Tato síť využívá licencovaný frekvenční rozsah LTE, vychází ze specifikací 3GPP a zahrnuje bezpečnostní funkce LTE. Mezi tyto bezpečnostní

funkce patří vzájemné ověřování koncových zařízení a sítě. Dále to jsou kryptografické algoritmy jako je AES a vysoká úroveň zabezpečení při vytváření a výměně šifrování. [44]

Úroveň zabezpečení lze zvýšit využitím bezpečnostních tunelů (IP VPN). Jedná se o využití zprostředkujícího serveru, který shromažďuje data ze sítě NB-IoT, aniž by procházela Internetem. Platforma klienta je připojena zabezpečeným připojením VPN k platformě operátora, a díky tomu je celá cesta od zařízení ke cloudovému serveru zabezpečená. [44]

Interní podniková síť je ochráněna, v případě uskutečnění kybernetického útoku na některé z IoT zařízení, díky využití oddělené sítě pro komunikaci IoT zařízení.

Aplikační:

Aplikační část by měla mít možnost bezpečné a pravidelné aktualizace softwaru. V případě využití webového rozhraní by měl být podporován zabezpečený protokol HTTPS, který zajišťuje autentizaci, důvěrnost a integritu dat. Aplikační část by měla podporovat bezpečné zálohování dat. V neposlední řadě je nutnost změnit výchozí přihlašovací údaje do aplikace, nastavit optimálně silné heslo a uživatelům aplikace nastavit pouze nutná přístupová práva, která potřebují při práci s aplikací.

3.4 Výrobní podnik D

Výrobní podnik D je moderní podnik, který se zabývá výrobou zdravotnických potřeb. Tento výrobní podnik má ve svém areálu travnaté okrasné plochy, jelikož vedení podniku klade velký důraz jak na kvalitu vnitřního prostředí v podniku, tak i na vnější prostředí podniku a jeho okolí. Travnaté plochy jsou vybaveny zavlažovacím systémem, který zavlažuje v předem nastavených intervalech nebo po příkazu jeho obsluhy. Vedení podniku vzneslo požadavek na automatizaci zavlažování za účelem šetření zdroje vody. Zavlažování by se mělo automaticky spustit pouze v případě, kdy vlhkost půdy klesla pod určitou hranici a nejsou v brzké době očekávány srážky.

3.4.1 Návrh implementace IoT zařízení

Zavlažování v areálu výrobního podniku

Řešení chytrého zavlažování může být realizováno pomocí senzorů v půdě, které měří vlhkost půdy a teplotu půdy. Získaná data o stavu půdy jsou dále odeslána do systému, kde se předají zavlažovacímu systému. Podle naměřených dat lze rozhodovat, zda spustit zavlažování či nikoliv. Systém lze propojit s předpovědí počasí, a pokud by předpověď predikovala v brzké době srážky, systém se spuštěním zavlažování vyčká. Díky tomu lze v podniku efektivně nakládat se zdrojem vody. Pokud by se předpověď zmýlila a srážky by se nedostavily, systém spustí zavlažování automaticky později. Podle toho jakou míru vlhkosti senzor v půdě naměří, tak potom systém vyhodnotí, kolik závlahy bude třeba. Vždy tedy bude spotřebováno optimálním množstvím vody.

Komunikace je realizována pomocí sítě LoRaWAN. Samotný modul se senzorem je napájen pomocí dvou AAA baterií. V tomto řešení je využit senzor s názvem Soil Sensor od české společnosti HARDWARIO s.r.o. (Obrázek 11).

Obrázek 11: Soil Sensor

Zdroj: [45]

Obrázek 12 zobrazuje modul Sada Sensor od společnosti HARDWARIO s.r.o., ke kterému lze připojit půdní senzor Soil Sensor pomocí 1-Wire sběrnice. Samotný modul v tomto řešení zastává funkci brány komunikace mezi senzorem a cloudem.

Obrázek 12: Sada Sensor

Zdroj: [46]

Podobných IoT řešení stále přibývá. Mezi společnosti, které taková řešení v České republice implementují, patří například společnost Agdata, LESPROJEKT-SLUŽBY s.r.o. nebo HARDWARIO s.r.o. [47]

3.4.2 Návrh zabezpečení

Fyzické:

Z pohledu fyzického zabezpečení je nutné zabezpečit senzor s modulem proti vniknutí vlhkosti a nečistoty z okolí. Měření senzoru je realizováno pomocí měděných pásků ve vnitřních vrstvách PCB. Tímto nejsou samotné kontakty vystaveny vlhkosti přímo a díky tomu neoxidují. Celý senzor je utěsněn, a proto je chráněn před nepříznivými povětrnostními podmínkami a jeho výrobce deklaruje roky provozu. Samotný modul vyžaduje pro bezproblémový provoz voděodolný kryt.

Síťové:

V tomto řešení je k přenosu dat mezi senzorem a cloudem využita komunikační síť LoRaWAN. Tato síť poskytuje zabezpečený šifrovaný přenos dat pomocí šifrovacího algoritmu AES-128. Zabezpečení sítě LoRaWAN již bylo detailně popsáno v kapitole 3.1.2.

Aplikační:

Jelikož aplikační rozhraní je z velké části standardizováno, bude zabezpečení v tomto řešení podobné předchozím řešením. Je důležité, aby aplikace umožňovala proces bezpečné

aktualizace softwaru. S tím se pojí podpora dodavatele, který bude tyto bezpečnostní aktualizace vydávat. Je důležité mít nastaveno optimálně silné heslo pro přístup do aplikace a změněny výchozí přihlašovací údaje. Oprávnění uživatelé aplikace by měli mít přidělena jenom nejnutnější práva, která k práci s aplikací potřebují. Práva role Administrátora by měla být přidělena jenom správci systému.

3.5 Shrnutí

V této kapitole byly navrženy čtyři případy využití Internetu věcí v prostředí výrobního podniku. Konkrétně se jednalo o Prediktivní údržbu osazovací linky, Identifikaci a lokalizaci produktu, Monitoring kvality prostředí ve výrobní hale a Zavlažování v areálu výrobního podniku. Ke každému případu využití byly vytipovány vhodné IoT senzory od různých výrobců, které by mohly být potencionálně využity při implementaci daného řešení. Následně byly navrženy a popsány nejdůležitější principy zabezpečení jednotlivých komponent IoT a přenosových cest.

Po stránce fyzické bezpečnosti velice záleží na prostředí ve kterém daný IoT prvek operuje a také na dodavateli jednotlivých komponent. Je důležité komponenty zabezpečit proti neoprávněné manipulaci a přístupu. Tímto bude zamezeno fyzickému podvržení dat nebo úplného zničení senzoru. Dále by měly být IoT prvky zabezpečeny vůči vnějším vlivům jako jsou prach, nečistota a vlhkost. V neposlední řadě musí být zabezpečen přístup do konfigurace skrz servisní port optimálně silným heslem.

Jelikož v těchto ukázkových případech byla potřeba přenosu pouze malého objemu dat ze senzorů, tak byly zvoleny dvě komunikační sítě typu LPWAN. Konkrétně se jednalo o síť LoRaWAN a síť NB-IoT. Obě tyto sítě zaručují zabezpečený šifrovaný přenos dat. Síť NB-IoT je na území České republiky poskytována mobilními operátory, kteří značně investují do spolehlivé a bezpečné infrastruktury této sítě. Síť LoRaWAN je území České republiky poskytována vícero subjekty a k bezpečnému přenosu dat využívá šifrovací algoritmus AES-128. Bezpečnosti interní podnikové sítě bylo docíleno využitím oddělené síťové komunikace pro IoT zařízení. V případě útoku na některé z IoT zařízení je nezbytné zajistit bezproblémový a bezpečný chod ostatních částí výrobního podniku.

Aplikační rozhraní je z velké části standardizováno, proto si jsou jednotlivé bezpečnostní přístupy v každém případu velice blízké. K úspěšnému zabezpečení na aplikační vrstvě je důležitý výběr vhodného a prověřeného dodavatele. Důležitým faktorem bezpečnosti je zajištění pravidelné údržby a aktualizace aplikace. Pro přístup do aplikace by mělo být nastaveno optimálně silné heslo a pro uživatele aplikace by měla být nastavena jenom nejnutnější oprávnění k jejímu využívání. Administrátorská práva by měla být povelena pouze kvalifikovanému správci systému. V neposlední řadě by aplikace měla podporovat bezpečnou zálohu dat.

Všechny implementované technologie Internetu věcí musejí být pravidelně kontrolovány a testovány. Otestováním bezpečnosti implementace ještě před jejím plným zavedením do provozu lze odhalit zranitelnosti konkrétního řešení a předejít možnému hackerskému útoku. Pro penetrační testování je vhodné zvolit externí agenturu, která disponuje potřebným know-how a týmem certifikovaných etických hackerů.

ZÁVĚR

Cílem této práce bylo vyhledat možnosti a rámcově navrhnout realizaci zabezpečení prostředků Internet of Things v provozu výrobního podniku.

První část práce představuje možnosti využití IoT technologií ve výrobním prostředí a definuje koncept Industry 4.0, ve kterém zastávají IoT technologie důležitou roli. Dále je zde popsána architektura Internetu věcí společně s komunikačními technologiemi LPWAN. Sítě LPWAN jsou v posledních letech hojně využívány právě kvůli rozmachu IoT technologií a v budoucnu lze předpokládat jejich další vývoj.

Druhá kapitola se zabývá zranitelností IoT infrastruktury. Tato kapitola popisuje reálné hrozby při implementaci chytrých řešení a dle architektury IoT jsou zde vytipována zranitelná místa využívaných technologií. Na konci kapitoly jsou uvedena doporučení pro bezpečnou implementaci IoT řešení doplněné o desatero organizace OWASP, které popisuje deset nejzávažnějších a dalo by se říci i nejčastějších chyb, kterých je třeba se vyvarovat při vytváření, nasazování nebo správě systémů IoT.

V poslední části práce jsou charakterizovány čtyři výrobní podniky. Pro tyto podniky jsou navrženy implementace IoT technologií do výroby a odpovídající formy zabezpečení pro dané řešení. Poznatky a bezpečnostní doporučení zmapované v této práci mohou být použity výrobními podniky jako podklad pro bezpečné zavedení IoT technologií do výroby.

Podniky by se v dnešní době měly zabývat otázkami kyberbezpečnosti v mnohem větší míře právě kvůli masivní digitalizaci a rostoucímu počtu hackerských útoků. Kybernetická bezpečnost by v podniku měla být formalizována pomocí dokumentace a měla by se hlouběji začlenit do podnikových procesů. Nezbytnou součástí tohoto procesu mohou být pravidelná školení zaměstnanců firmy, pravidelná penetrační testování a také důsledný výběr dodavatelů IoT technologií. Penetrační testování by mělo být ideálně prováděno externí společností, kdy hrozí menší riziko zkreslení výsledků a manipulace s nimi. Tento přístup může podnik ochránit před neočekávanými výpadky výroby a lze tak předejít značným finančním ztrátám v případě kybernetického útoku.

Tato práce není definitivním návodem pro zavedení IoT technologií do výrobního podniku. V tomto mladém odvětví dochází k dynamickému vývoji například u využití distribuované bezpečnosti v IoT infrastruktuře. Podrobné zkoumání těchto témat už by bylo nad rámec této práce. Může však posloužit jako inspirace pro práce další.

POUŽITÁ LITERATURA

[1] VACULÍK, Juraj. *Od telemetrie k internetu vecí I*. Bratislava: EDIS, 2019. ISBN 9788055415215.

[2] ALKHALDI, Nadejda. Considering using IoT in manufacturing? Read this first. *Itrexgroup.com* [online]. California: Itrexgroup.com, 2022 [cit. 2022-11-20]. Dostupné z: https://itrexgroup.com/blog/iot-in-manufacturing/

[3] VIOLINO, Bob. IoT and AI boost Volvo Trucks vehicle connectivity. *Networkworld.com* [online]. Massachusetts: Network World, 2020 [cit. 2022-11-20]. Dostupné z: https://www.networkworld.com/article/3587404/volvo-trucks-boosts-vehicle-connectivity-with-ai-and-iot.html

[4] World's Largest Manufacturers Lose Almost $1 Trillion a Year to Machine Failures. *Automation.com* [online]. North Carolina: Automation.com, 2021 [cit. 2022-11-20]. Dostupné z: https://www.automation.com/en-us/articles/june-2021/world-largest-manufacturers-lose-almost-1-trillion

[5] BEHRENDT, Andreas, Enno DE BOER, Tarek KASAH, Bodo KOERBER, Niko MOHR a Gérard RICHTER. Leveraging Industrial IoT and advanced technologies for digital transformation. *McKinsey Co*, 2021 [online]. 1-75 [cit. 2022-11-20]. Dostupné z: https://info.sightmachine.com/hubfs/Downloadable%20Resources/Downloads/leveraging-industrial-iot-and-advanced-technologies-for-digital-transformation.pdf

[6] BROWN, Davies. 10 Best Use Cases of the IoT in Manufacturing Sector. *Mytechmag.com* [online]. Texas: MYTECHMAG, 2022 [cit. 2022-11-20]. Dostupné z: https://www.mytechmag.com/iot-in-manufacturing/

[7] IoT monitoring of production and energy consumption. *Zerynth.com* [online]. Pisa: Zerynth, c2015-2022 [cit. 2022-11-20].
Dostupné z: https://www.zerynth.com/customers/case-studies/armal/

[8] AJAO, Esther. How a startup uses a facial recognition engine during COVID-19. *Techtarget.com* [online]. Massachusetts: TechTarget, 2022 [cit. 2022-11-20]. Dostupné z: https://www.techtarget.com/searchenterpriseai/news/252516453/How-a-startup-uses-a-facial-recognition-engine-during-COVID

[9] Japanese airbag maker Takata files for bankruptcy. *Cbc.ca* [online]. Toronto: CBC/Radio-Canada, 2017 [cit. 2022-11-20].
Dostupné z: https://www.cbc.ca/news/business/takata-airbag-bankruptcy-1.4177256

[10] MAHMOUD, Rwan, Tasneem YOUSUF, Fadi ALOUL a Imran ZUALKERNAN, 2015. Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* [online]. IEEE, 2015, 336-341 [cit. 2022-11-20]. ISBN 978-1-9083-2052-0. Dostupné z: http://ieeexplore.ieee.org/document/7412116/

[11] SONG, Yonghua, Jin LIN, Ming TANG a Shufeng DONG. An Internet of Energy Things Based on Wireless LPWAN. *Sciencedirect.com* [online]. China: Elsevier, 2017 [cit. 2022-11-20]. ISSN 2095-8099. Dostupné také z: https://www.sciencedirect.com/science/article/pii/S2095809917306057

[12] CHANDANA, Roy, Sudip MISRA a Anandarup MUKHERJEE. *Introduction to Industrial Internet of Things and Industry 4.0*. Boca Raton: CRC Press, 2021. ISBN 9781000283068.

[13] BEEKMAN, Johannes. Understanding Wireless Technologies: Licensed vs. Unlicensed Spectrum. *Iotmktg.com* [online]. Texas: IoT Marketing, 2022 [cit. 2022-11-20]. Dostupné z: https://iotmktg.com/understanding-wireless-technologies-licensed-vs-unlicensed-spectrum/

[14] LoRaWAN. *IoT portál* [online]. IoT portál, 2016 [cit. 2022-11-20]. Dostupné z: https://www.iot-portal.cz/2016/02/29/lorawan/

[15] IoT – Internet věcí. *Cra.cz* [online]. Praha: České Radiokomunikace, c2022 [cit. 2022-11-20]. Dostupné z: https://www.cra.cz/cra-iot-internet-veci

[16] Internet věcí – IoT. *Starnet.cz* [online]. České Budějovice: STARNET [cit. 2022-11-20]. Dostupné z: https://www.starnet.cz/iot/

[17] Czech Republic: The Things Network. *Thethingsnetwork.org* [online]. The Things Network [cit. 2022-11-20].
Dostupné z: https://www.thethingsnetwork.org/country/czech-republic/

[18] Objednáváte připojení k IoT síti LoRa. *Iotport.cz* [online]. Praha: České Radiokomunikace, c2022 [cit. 2022-11-20].
Dostupné z: https://www.iotport.cz/objednavka-lorawan

[19] LoRaWAN - připojení do sítě IoT. *Iotport.cz* [online]. Praha: České Radiokomunikace, c2022 [cit. 2022-11-20]. Dostupné z: https://www.iotport.cz/lorawan-sit-pro-iot

[20] LoRaWAN, Sigfox nebo NB-IoT?: Srovnání 3 významných typů IoT sítí. *Iotport.cz* [online]. Praha: České Radiokomunikace, 2020 [cit. 2022-11-20]. Dostupné z: https://www.iotport.cz/iot-novinky/lorawan/lorawan-sigfox-nebo-nb-iot-srovnani-3-vyznamnych-typu-iot-siti

[21] Základní ceník konektivity. *Sigfox.cz* [online]. Praha: Sigfox, c2016-2022 [cit. 2022-11-20]. Dostupné z: https://sigfox.cz/cs/o-nas/cenik-vop

[22] Dostupnost sítě. *Sigfox.cz* [online]. Praha: Sigfox, c2016-2022 [cit. 2022-11-20]. Dostupné z: https://sigfox.cz/cs

[23] 0G NETWORK COVERAGE. In: *Sigfox.com* [online]. Francie: Sigfox, c2022 [cit. 2022-11-20]. Dostupné z: https://www.sigfox.com/en/coverage

[24] Mapa pokrytí signálem. In: *Vodafone.cz* [online]. Praha: Vodafone Czech Republic, c2022 [cit. 2022-11-20]. Dostupné z: https://www.vodafone.cz/mapa-pokryti/

[25] NTT Global Threat Intelligence Report: Up to 300% Increase in Attacks from Opportunistic Targeting. *Services.global.ntt* [online]. Londýn: Nippon Telegraph and Telephone, 2021 [cit. 2022-11-20]. Dostupné z: https://services.global.ntt/ja-jp/newsroom/ntt-global-threat-intelligence-report-2021

[26] 2021 State of Manufacturing Report. *Fictiv.com* [online]. California: Fictiv, c2022 [cit. 2022-11-20]. Dostupné z: https://www.fictiv.com/ebooks/2021-state-of-manufacturing

[27] 2020 REPORT: ICS ENDPOINTS AS STARTING POINTS FOR THREATS. *Trendmicro.com* [online]. Texas: Trend Micro Incorporated, 2021 [cit. 2022-11-20]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/2020-report-ics-endpoints-as-starting-points-for-threats

[28] Securing Industry 4.0: How manufacturers can stem the rising tide of cyber risk. *Industryeurope.com* [online]. Industry Europe, 2022 [cit. 2022-11-20]. Dostupné z: https://industryeurope.com/sectors/technology-innovation/securing-industry-4-0-how-manufacturers-can-stem-the-rising-tide-of-cyber-risk/

[29] Cost of a Data Breach Report 2021. *Ibm.com* [online]. New York: IBM Corporation, 2021 [cit. 2022-11-20]. Dostupné z: https://www.ibm.com/downloads/cas/OJDVQGRY

[30] Reputation Intact Despite Projected Cost of $75 Million for Norsk Hydro Cyber Attack. *Cpomagazine.com* [online]. Singapore: CPO Magazine, 2019 [cit. 2022-11-20]. Dostupné z: https://www.cpomagazine.com/cyber-security/reputation-intact-despite-projected-cost-of-75-million-for-norsk-hydro-cyber-attack/

[31] BURHAN, Muhammad, Rana REHMAN, Bilal KHAN a Byung-Seo KIM. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* [online]. 2018, 18(9) [cit. 2022-11-20]. ISSN 1424-8220. Dostupné z: https://www.mdpi.com/1424-8220/18/9/2796

[32] YOUSUF, Tasneem, Rwan MAHMOUD, Fadi ALOUL a Imran ZUALKERNAN. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures.

International Journal for Information Security Research [online]. 2015, 5(4), 608-616 [cit. 2022-11-20]. ISSN 20424639. Dostupné z: https://www.researchgate.net/publication/307945826_Internet_of_Things_IoT_Security_Current_Status_Challenges_and_Countermeasures

[33] BAKUEI, Matsukawa, Ryan FLORES, Vladimir KROPOTOV a Fyodor YAROCHKIN. Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0. *Trendmicro.com* [online]. Texas: Trend Micro Incorporated, 2019 [cit. 2022-11-20].
Dostupné z: https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

[34] KADLAS BLÜMELOVÁ, Kristina. Standard IEC 62443 je pojistkou firemní kybernetické bezpečnosti. *Technickytydenik.cz* [online]. Praha: Business Media CZ, 2021 [cit. 2022-11-20].
Dostupné z: https://www.technickytydenik.cz/rubriky/poutaky/standard-iec-62443-je-pojistkou-firemni-kyberneticke-bezpecnosti_53149.html

[35] IEC 62443 – norma týkající se průmyslové kybernetické bezpečnosti. *Phoenixcontact.com* [online]. Brno: PHOENIX CONTACT, c2022 [cit. 2022-11-20]. Dostupné z: https://www.phoenixcontact.com/cs-cz/iec-62443-norma-tykajici-se-prumyslove-kyberneticke-bezpecnosti

[36] OWASP IoT Top 10 2018. *Owasp.org* [online]. OWASP, 2018 [cit. 2022-11-20]. Dostupné z: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[37] LORA temperature sensor - ELA Innovation. In: *Elainnovation.com* [online]. Montpellier: ELA Innovation [cit. 2022-11-20].
Dostupné z: https://elainnovation.com/en/catalogue/lora-temp-en/

[38] Security in LoRaWAN applications. *Smartmakers.io* [online]. Karlsruhe: SmartMakers, c2021 [cit. 2022-11-20]. Dostupné z: https://smartmakers.io/en/security-in-lorawan-applications/

[39] MQTT: The Standard for IoT Messaging. *Mqtt.org* [online]. MQTT.org, c2022 [cit. 2022-11-20]. Dostupné z: https://mqtt.org/

[40] Micro tracker - Abeeway. In: *Abeeway.com* [online]. Abeeway, c2022 [cit. 2022-11-20]. Dostupné z: https://www.abeeway.com/micro-tracker/

[41] Naši partneři ve světě internetu věcí. *Iotport.cz* [online]. Praha: České Radiokomunikace, c2022 [cit. 2022-11-20]. Dostupné z: https://www.iotport.cz/nasi-partneri/rebit-tech-s-r-o

[42] ModemLabs NB-IoT Air Quality PM2.5 Sensor - Modem Labs. In: *Modemlabs.com* [online]. ModemLabs, c2019 [cit. 2022-11-20]. Dostupné z: https://www.modemlabs.com/product/modemlabs-nb-iot-air-quality-pm2-5-sensor/

[43] HARDWARIO. *Monitoring vnitřního prostředí ve výrobě a skladování | HARDWARIO IoT Webinář* [online]. YouTube video, 2020 [cit. 2022-11-20]. Dostupné z: https://www.youtube.com/watch?v=f9ZdIYVATz0&t=2799s

[44] Security of NB-IoT devices. *Accent-systems.com* [online]. Barcelona: Accent Advanced Systems, c2021 [cit. 2022-11-20]. Dostupné z: https://accent-systems.com/security-of-nb-iot-devices/

[45] Soil Sensor - HARDWARIO obchod. In: *Obchod.hardwario.cz* [online]. Liberec: HARDWARIO, c2022 [cit. 2022-11-20]. Dostupné z: https://obchod.hardwario.cz/soil-sensor/

[46] Sada Sensor - HARDWARIO obchod. In: *Obchod.hardwario.cz* [online]. Liberec: HARDWARIO, c2022 [cit. 2022-11-20]. Dostupné z: https://obchod.hardwario.cz/sada-sensor/

[47] Boj se suchem pomocí chytrého zavlažování. *Iotport.cz* [online]. Praha: České Radiokomunikace, 2020 [cit. 2022-11-20]. Dostupné z: https://www.iotport.cz/iot-novinky/zemedelstvi-a/iot-a-boj-proti-suchu-pomoci-chytreho-zavlazovani

[48] 188.116.126.158. In: *Shodan.io* [online]. Shodan [cit. 2022-11-27]. Dostupné z: https://www.shodan.io/host/188.116.126.158

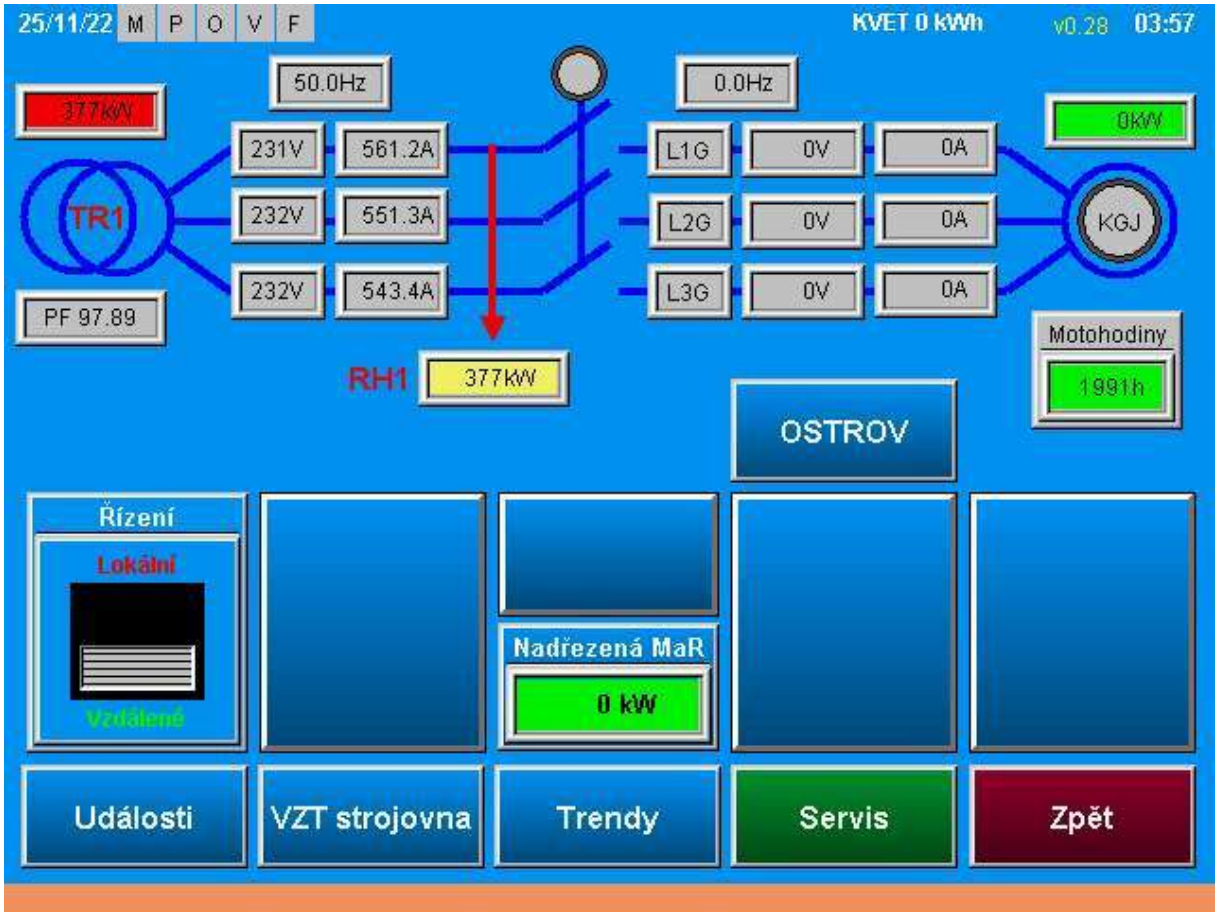
[49] 90.179.168.48. In: *Shodan.io* [online]. Shodan [cit. 2022-11-27]. Dostupné z: https://www.shodan.io/host/90.179.168.48

[50] 189.15.204.207. In: *Shodan.io* [online]. Shodan [cit. 2022-11-27]. Dostupné z: https://www.shodan.io/host/189.15.204.207

[51] 217.247.150.118. In: *Shodan.io* [online]. Shodan [cit. 2022-11-27]. Dostupné z: https://www.shodan.io/host/217.247.150.118

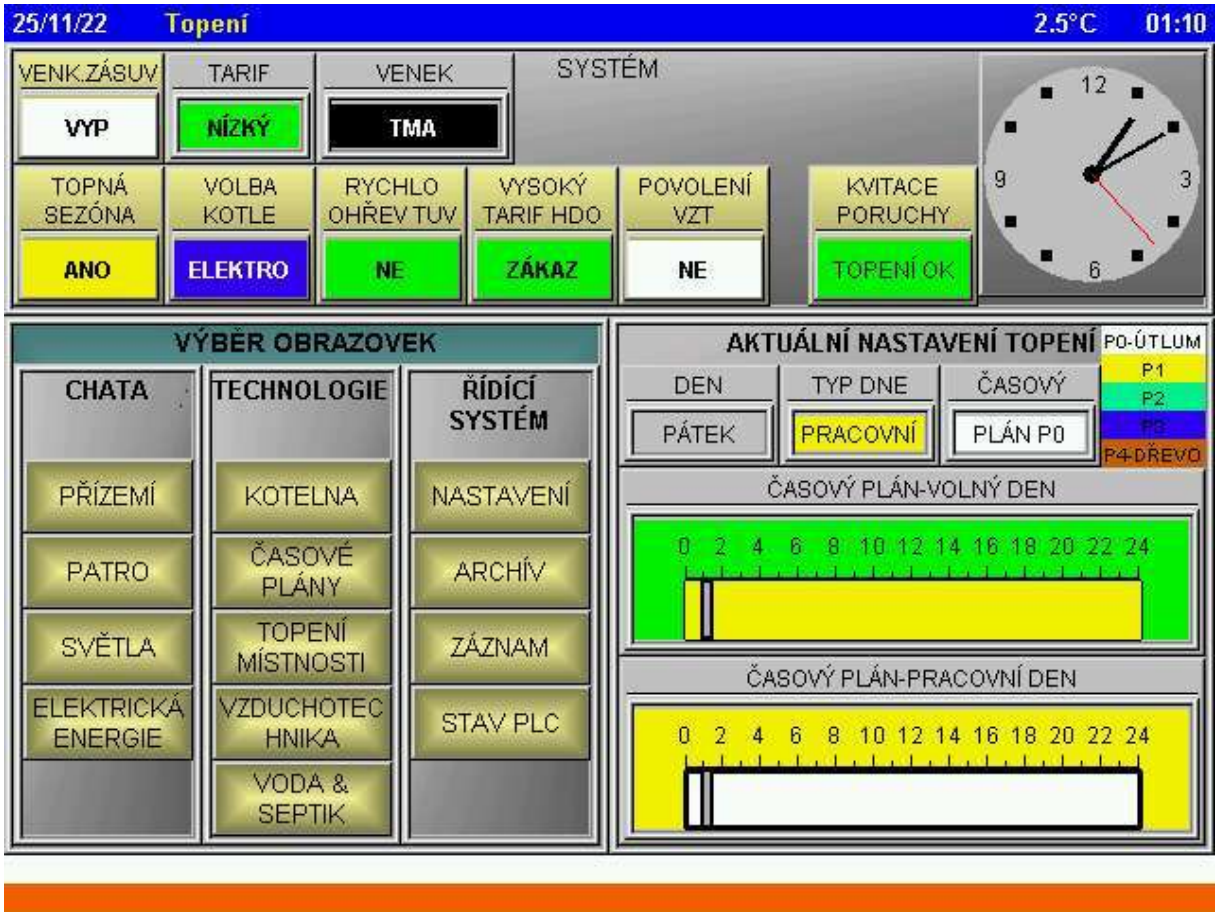
SEZNAM PŘÍLOH

Příloha A: Administrátorské monitorovací rozhraní z adresy 188.116.126.158



Zdroj: [48]

Příloha B: Administrátorské monitorovací rozhraní z adresy 90.179.168.48

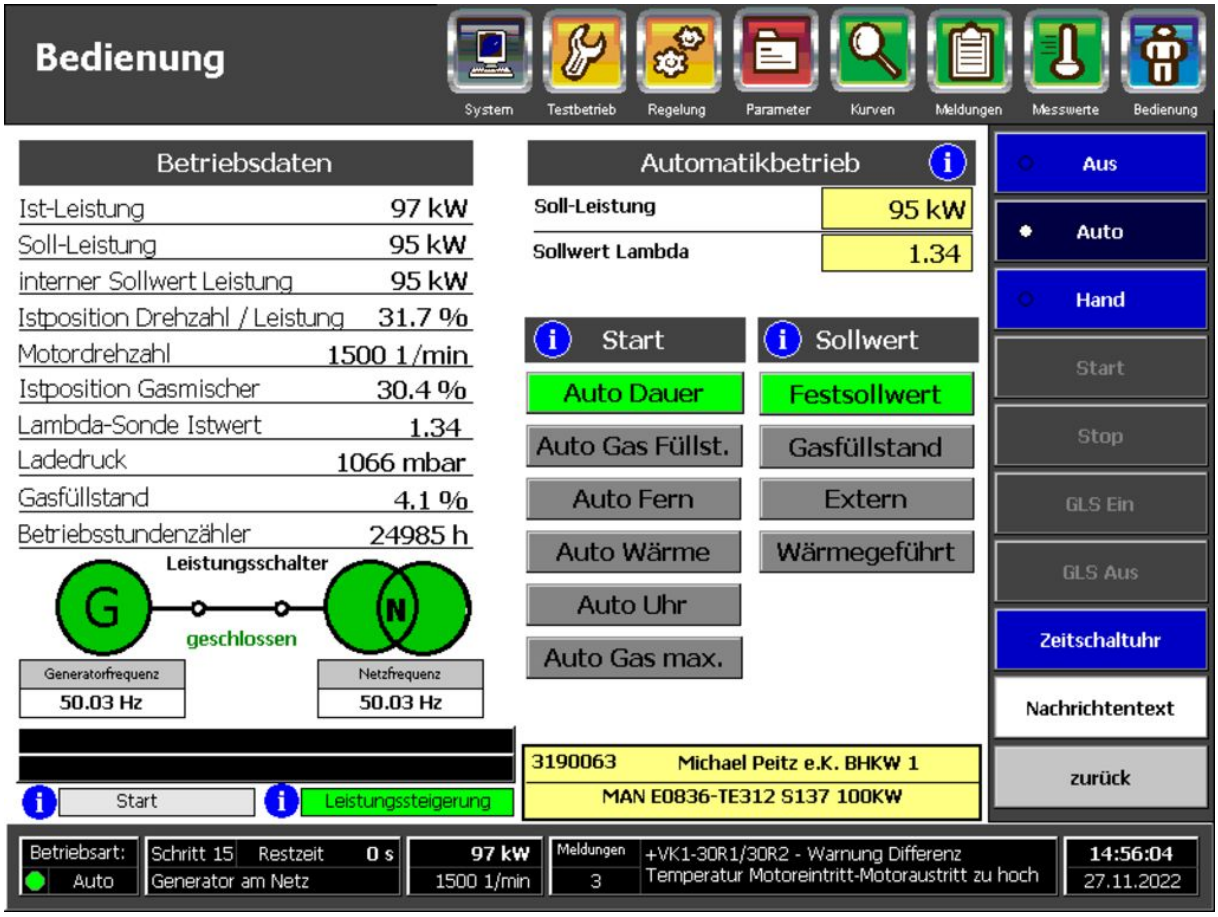


Zdroj: [49]

Příloha C: IP kamera z adresy 189.15.204.207

Zdroj: [50]

Příloha D: Administrátorské monitorovací rozhraní z adresy 217.247.150.118



Zdroj: [51]