Propojení prvků komunikace internetu věcí (IoT) a 5G sítí

Připraveno pro Ministerstvo průmyslu a obchodu

30.9.2024

Grant Thornton

Obsah

Definice pojmů

Definice základních pojmů je důležitým odrazovým můstkem pro další části studie i pro praktické implikace.[1]

IoT (internet věcí): Internet věcí je systém jednoznačně identifikovaných zařízení, která sbírají data, jež jsou dále přenášena přes internet, analyzována a vyhodnocována a na základě kterých může být realizována akce v rámci systému nebo mimo něj. Tento systém má jasně daný účel, kterým je typicky zvyšování efektivity procesů, výkonnosti, informovanosti apod.

IIoT (Industry IoT/ Průmyslový internet věcí): IIoT je podmnožinou IoT zaměřenou na průmyslové aplikace. Zahrnuje propojení průmyslových strojů a senzorů pro sledování, sběr a analýzu dat v reálném čase. IIoT se široce využívá ve výrobě, energetice a logistice ke zlepšení provozu, bezpečnosti a prediktivní údržby.

mMTC (massive Machine-Type Communication): mMTC označuje typ komunikace v IoT, který podporuje velké množství nízkoenergetických zařízení, jež potřebují být připojena současně. Tato technologie je navržena pro aplikace, které vyžadují mnoho připojených zařízení, jako jsou chytrá města, zemědělství a monitorování životního prostředí.

Mission Critical IoT (kritické IoT): Mission Critical IoT se vztahuje na IoT aplikace, které vyžadují extrémně vysokou spolehlivost, nízkou latenci a zaručený výkon. Tyto aplikace se obvykle používají ve scénářích, kde by selhání mohlo mít vážné následky, jako jsou autonomní vozidla, průmyslová automatizace a dálkové zdravotní služby.

Massive IoT (masivní IoT): Massive IoT se zaměřuje na nasazení velkého počtu jednoduchých, nízkonákladových a nízkoenergetických zařízení, která generují malé množství dat. Tato kategorie IoT je vhodná pro aplikace jako chytré měření, environmentální senzorika a sledování, kde zařízení potřebují fungovat dlouhodobě bez údržby a obvykle na baterii.

Mid-Range IoT (IoT střední úrovně): Mid-Range IoT představuje aplikace, které se nacházejí mezi kritickým a masivním IoT. Tyto systémy vyvažují výkon, spolehlivost a náklady. Jsou vhodné pro případy užití, jako je automatizace budov, chytré osvětlení a propojené spotřebiče.

IoT systém: Systém zajišťující funkcionality Internetu věcí. IoT systém může mimo jiné zahrnovat IoT zařízení, IoT brány, senzory a aktuátory (akční členy).

IoT Zařízení: Koncový bod, který interaguje s fyzickým světem prostřednictvím snímání nebo ovládání. Zařízení IoT může být senzor nebo aktuátor (akční člen).

Aktuátor (akční člen): Typicky část mechatronické soustavy (strojů kombinujících elektroniku a mechaniku), která převádí informační část procesu na technickou – např. příkaz o změně směru je aktuátorem převeden na mechanickou energii potřebnou k vychýlení ze současného směru pohybu stroje. V kontextu IoT je aktuátor koncovým zařízením, které umožňuje oboustrannou interakci (nikoli jen jednostranné snímání jako u senzoru).

[1] Poznámka: české vs. anglické pojmy. Tak jako v mnoha odborných oblastech, také v oblasti IoT, 5G a navazujících řešeních existuje řada pojmů, pro které není ukotvený vhodný český ekvivalent. Z principu budou také nově přicházející pojmy v angličtině. Stejně jako většina odborné literatury. Někdy je proto nezbytné použít původní anglický pojem, případně použít anglický i český ekvivalent. Dalším důvodem pro použití anglických pojmů je možnost uživatele vyhledávat k tématu další informace. Pod původním anglickým termínem je to přímočaré, při použití neukotveného českého ekvivalentu by to mohlo být problematické.

Senzor: IoT zařízení se schopností snímání stavu okolí či okolních jevů.

IoT brána (gateway): Entita IoT systému, která propojuje jednu nebo více blízkých sítí a zařízení IoT v těchto sítích navzájem a s jednou nebo více přístupovými sítěmi s různými protokoly.

Další pojmy:

Use case / Případ užití	Obecná definice případu užití je následující: Výraz "případ užití" odkazuje na konkrétní situaci nebo scénář, ve kterém lze produkt nebo službu použít. Pro potřeby této studie je případ užití definován takto: „Úkol, který firma potřebuje realizovat za účelem dosažení určitého výsledku.“ Tato definice je vhodná už toho pohledu, že zvýrazňuje skutečnost, že případ užití slouží k dosažení konkrétního výsledku, respektive řadě různých požadovaných výsledků (například zvýšení efektivity procesu, minimalizace nebezpeční pro zaměstnance, minimalizace odpadu apod.).
Case Study/ Případová studie	Konkrétní realizace Use Case/ případu užití. V rámci případové studie je použito konkrétní řešení pro splnění úkolu definovaného v Use Case. Tedy určitá technologie, produkty a služby specifického poskytovatele. Bez ohledu na to, zda tato realizace již slouží v komerčním provozu, nebo jde o demo realizaci či Proof of Concept.
Digitalizace	• Digitalizace se obvykle zaměřuje na konkrétní procesy nebo operace v rámci podniku. • Cílem digitalizace je nahradit tradiční, analogové a papírové postupy digitálními technologiemi za účelem zvýšení efektivity, snížení nákladů a zlepšení operativního řízení. • Digitalizace může zahrnovat automatizaci, přechod na digitální systémy a procesy, eliminaci papírové práce a optimalizaci konkrétních oblastí podniku.
Digitalizace podniků	Digitalizace využívá digitální technologie ke změně podnikových procesů a poskytuje nové příležitosti pro vytváření hodnoty. Zahrnuje digitalizaci stávajících analogových informací do digitálních formátů a určité procesy, které mohou společnosti provádět lépe pomocí nejnovějších technologií a nástrojů. Cílem digitalizace je: • zvýšení produktivity, • zlepšení kvality služeb a tím vytvoření konkurenční výhody pro podnik pomocí využití informačních a komunikačních technologie (ICT) k zefektivnění procesů.
Digitální transformace	• Digitální transformace je širší a komplexnější koncepce, která se týká celkové změny podnikové strategie, kultury a operací pomocí digitálních technologií. • Jedná se o strategický přístup, který může zahrnovat restrukturalizaci firemních modelů, změny v obchodních procesech, implementaci nových technologií a transformaci firemní kultury. • Digitální transformace nemusí být omezena pouze na konkrétní operace; může zahrnovat radikální změny v celém podnikovém ekosystému, aby byl podnik lépe přizpůsoben digitálnímu prostředí a inovačním trendům.
Edge Computing	Edge computing označuje praxi zpracování dat poblíž okraje sítě, kde se data generují, namísto v centralizovaném skladu pro zpracování dat. „Okraj“ v tomto kontextu může znamenat jakékoli výpočetní a síťové zdroje na cestě mezi datovými zdroji (jako jsou zařízení IoT) a cloudovými datovými centry. Edge computing snižuje potřebu posílat data tam a zpět na centrální server, čímž se snižuje latence a využití šířky pásma.
MEC (Multi-access Edge Computing)	Multi-access Edge Computing (MEC) je koncept síťové architektury, který umožňuje cloud computing a prostředí IT služeb na okraji sítě. MEC přivádí výpočetní zdroje blíže k místu, kde se generují a spotřebovávají data, snižuje latenci, zlepšuje rychlost zpracování a zlepšuje uživatelské zkušenosti. Často je spojován s mobilními sítěmi, zejména 5G, kde může zpracovávat data v blízkosti mobilních základnových stanic nebo jiných přístupových bodů sítě. Rozdíl mezi MEC a Edge Computing: MEC je podmnožina edge computingu, speciálně navržená pro optimalizaci síťových architektur a zlepšování výkonu aplikací v mobilních sítích, včetně 5G. Zaměřuje se především na mobilní okraj, rozšiřující služby v prostředí mobilních sítí. Naproti tomu edge computing je širší koncept použitelný v různých sítích a odvětvích, včetně IoT, výroby, zdravotnictví a dalších, bez ohledu na to, zda se jedná o mobilní nebo pevné sítě. Integrace s mobilními sítěmi: MEC je ze své podstaty navržena tak, aby se úzce integrovala s provozem mobilních sítí, zejména 5G, což usnadňuje služby, jako je ukládání obsahu do mezipaměti, zpracování v reálném čase a kontextové služby. Edge computing, i když může fungovat v mobilních sítích, nemá vlastní design vázaný na tyto sítě a může být implementován v jakémkoli místním prostředí. Jak MEC, tak edge computing jsou klíčové v digitalizaci společností, zejména s příchodem 5G.
Vertikála	V obchodním kontextu se termín "vertikály" používá k popisu kategorizace obchodních společností nebo odvětví podle jejich specializace nebo zaměření na určitý segment trhu. Vertikály jsou obvykle odvětví nebo sektory, které zahrnují podniky, které se specializují na konkrétní typ produktů, služeb nebo tržních segmentů.

Manažerské shrnutí

IoT (Internet věcí) je nesmírně široký pojem. Jedná se o oblast, která má a bude mít obrovský dopad na naše životy v mnoha směrech. Z tohoto pohledu je možné najít málo tak zásadních technologií.

Využití Internetu věcí je nezbytným pomocníkem digitalizace firem, zvyšování efektivity výroby, vede ke zvýšení úrovně a dostupnosti zdravotní péče, zefektivnění dopravy a kvality života ve městech nebo zvýšení výnosů v zemědělství. IoT je součástí nepřeberného množství případů užití v různých vertikálách, z nichž řada je uvedena v této studii.

O významu IoT svědčí také velikost a růst trhu. Podle predikcí má počet IoT připojení vzrůst ze současných cca 15 miliard na 40 miliard připojených zařízení v roce 2033. Globální velikost trhu firemního IoT má vzrůst z 300 miliard USD na více než dvojnásobek do roku 2030.

Tato studie přináší kompletní přehled oblasti internetu věcí. Věnuje se způsobu fungování IoT systémů jeho vrstvám a prvkům, oblastem využití IoT, výzvám spojeným s využitím internetu věcí a také jeho budoucnosti.

5G technologie má na oblast IoT zásadní vliv. Může být přímo aplikována v komunikační (síťové) vrstvě IoT systému, přímo ovlivňuje percepční vrstvu (zařízení) a edge vrstvu. Velký vliv má ovšem také na bezpečnost a ekonomiku IoT systému.

Proto studie věnuje značný prostor různým IoT komunikačním technologiím, jejich možnostem i slabinám. Přináší v tomto směru ucelený záběr zahrnující všechny rozšířené technologie krátkého a dlouhého dosahu.

5G technologie pro IoT existuje v několika zásadně odlišných variantách, které jsou vhodné pro různé případy užití. Z původně 4G ekosystému jsou do 5G ekosystém převzaty a dále rozvíjeny technologie NB-IoT a Cat-M. Aktuální 5G NR technologie není technologií specificky určenou pro IoT. Může být využita pro business kritické aplikace. Ovšem je poměrně nákladná zejména z pohledu koncových zařízení a také není optimalizována z pohledu spotřeby energie koncových zařízení. Právě proto byla pro využití v IoT oblasti standardizována technologie NR-light, neboli RedCap. Velká očekávání jsou spojena také s další variantou 5G technologie v podobě Passive IoT, jejíž standardizace ještě není ukončena.

Z pohledu způsobu vyžití přináší studie členění IoT systémů na kritické IoT, IoT středního typu a masivní IoT. Tyto 3 typy IoT systémů se liší svými požadavky. Kritické IoT vyžaduje typicky vysoký výkon, zabezpečení, vyšší datové rychlosti a velmi vysokou spolehlivost přenosu. Masivní IoT naproti tomu vyžaduje nízkou spotřebu energie koncových zařízení, nízké náklady na zařízení a poměrně nízké přenosové rychlosti. IoT středního typu pak stojí svými požadavky mezi kritickým a masivním IoT.

Studie přináší poměrně unikátní systematický postup výběru vhodné IoT technologie pro různé způsoby využití IoT.

Pro IoT technologie je v rámci studie určeno, pro jakou kategorii IoT systému je vhodná. Každý případ užití je zařazen do IoT kategorie. Díky tomu je možné orientačně určit, jaké IoT technologie jsou vhodné pro daný případ užití.

Přesnější volba technologie je možná na základě definování celé sady klíčových požadovaných vlastností IoT systému. Pro tento účel je ve studii připraven formulář. Získané požadavky je možné porovnat s parametry technologií, které jsou také uvedeny v této studii. Z porovnání požadavků a parametrů je pak možné určit jednu či více vhodných IoT technologií pro daný IoT systém a jeho případy užití.

Mezi hlavní výzvy spojené s oblastí internetu věcí a jeho rozvojem patří kybernetická bezpečnost a stále omezená interoperabilita a vysoká fragmentace protokolů a technologií. Posilování bezpečnosti a další standardizace proto jistě patří k budoucím směrům vývoje IoT.

Kromě toho vidíme tyto zásadní trendy pro budoucnost IoT:

- Nové komunikační technologie v rámci 5G ekosystému, zejména RedCap a Passive IoT. Nové technologie pomohou překonat slabiny stávajících technologií, a to nejen technické, ale také komerční (nákladové). Díky tomu umožní realizace nových business modelů a mnohem masivnější nasazení IoT.

- Využití AI/ML pro pokročilou analýzu dat. To přinese značnou přidanou hodnotu do oblastí jako prediktivní údržba, detekce anomálií a obecně automatizace.

- Cloudové IoT produkty. Sofistikované, a přitom relativně dostupné (také díky modelu PayGo) cloudové produkty umožní rychlé nasazení IoT systémů firmám všech velikostí. A to s trochou nadsázky na několik kliknutí. Cloudové produkty zpřístupní pokročilou analýzu s využitím AI/ML všem uživatelům bez nutnosti specifické expertízy.

Management summary

IoT (Internet of Things) is an extremely broad concept. It is an area that has and will continue to have a massive impact on our lives in many ways. From this perspective, few technologies are as fundamental.

The use of the Internet of Things is an essential tool for the digitalization of companies, increasing production efficiency, improving the level and availability of healthcare, streamlining transportation and the quality of life in cities, and increasing yields in agriculture. IoT is part of a vast array of use cases across different verticals, many of which are highlighted in this study.

The importance of IoT is also demonstrated by the size and growth of the market. According to predictions, the number of IoT connections is expected to increase from the current approximately 15 billion to 40 billion connected devices by 2033. The global market size of enterprise IoT is projected to grow from USD 300 billion to more than double by 2030.

This study provides a comprehensive overview of the Internet of Things. It addresses the functioning of IoT systems, its layers and components, areas of IoT application, challenges associated with the use of the Internet of Things, and its future.

5G technology has a significant impact on IoT. It can be directly applied in the communication (network) layer of the IoT system and directly influences the perception layer (devices) and the edge layer. It also has a substantial effect on the security and economics of the IoT system.

Therefore, the study dedicates significant space to various IoT communication technologies, their capabilities, and weaknesses. It provides a comprehensive view, covering all widespread short- and long-range technologies.

5G technology for IoT exists in several fundamentally different variants, suitable for various use cases. Technologies NB-IoT and Cat-M are derived from the original 4G ecosystem and are further developed within the 5G ecosystem. The current 5G technology is not specifically designed for IoT. It can be used for business-critical applications but is relatively costly, especially regarding end devices, and is not optimized for energy consumption. This is why the NR-light technology, or RedCap, has been standardized for use in the IoT field. High expectations are also associated with another variant of 5G technology in the form of Passive IoT.

From the perspective of utilization, the study divides IoT systems into critical IoT, mid-range IoT, and massive IoT. These three types of IoT systems differ in their requirements. Critical IoT typically requires high performance, security, higher data speeds, and very high transmission reliability. In contrast, massive IoT requires low power consumption of end devices, low device costs, and relatively low transmission speeds. Mid-range IoT requirements lie between those of critical and massive IoT.

The study offers a relatively unique systematic approach to selecting the right IoT technology for various IoT use cases. For IoT technologies, the study determines which category of the IoT system they are suitable for. Each use case is categorized into an IoT category, allowing for an approximate determination of which IoT technologies are suitable for that specific use case.

A more precise technology choice can be made based on defining the key required features of the IoT system. For this purpose, the study includes a form. The acquired requirements can be compared with the technology parameters, which are also outlined in the study. By comparing requirements and parameters, it is then possible to identify one or more suitable IoT technologies for a given IoT system.

Among the main challenges associated with the field of the Internet of Things and its development are cybersecurity, still limited interoperability, and high fragmentation of protocols and technologies. Strengthening security and further standardization will undoubtedly be key directions for the future of IoT.

Additionally, we see the following crucial trends for the future of IoT:

- New communication technologies within the 5G ecosystem, especially RedCap and Passive IoT. These new technologies will help overcome the weaknesses of existing technologies, not only technically but also commercially (in terms of cost). This will enable new business models and much more widespread deployment of IoT.
- Utilization of AI/ML for advanced data analysis. This will bring significant added value to areas such as predictive maintenance, anomaly detection, and automation in general.
- Cloud IoT products* Sophisticated yet relatively affordable (thanks to the PayGo model) cloud products will enable rapid deployment of IoT systems for companies of all sizes—almost literally with a few clicks. Cloud products will make advanced AI/ML analytics accessible to all users without the need for specific expertise.

1 Představení IoT

1.1 Cíle studie

Cílem studie je podpořit další rozvoj IoT řešení v České republice vzhledem k jejich vysokému přínosu pro řadu aspektů ekonomiky i kvality života, a to zejména s využitím 5G technologií, které do IoT přináší nové možnosti a otvírají cestu dalším případům užití.

Tohoto cíle chce dosáhnout tím, že zainteresovaným stranám přinese celostní obrázek oblasti internetu věcí, s důrazem na oblast 5G technologií v IoT systémech. Studie seznámí čtenáře s parametry řady komunikačních technologií pro IoT, s jejich výhodami i nedostatky a pomůže zorientovat se ve vhodném využití jednotlivých technologií pro různé kategorie IoT systémů a případy užití.

Porozumění IoT, jeho možnostem a potenciálu, je nutnou podmínkou pro firmy, které chtějí udávat směr v digitalizaci, zefektivnit své procesy či výrobu, pro města, která se chtějí poskytovat větší komfort svým obyvatelům a udržitelným způsobem se rozvíjet, pro zdravotní zařízení, která chtějí zvyšovat úroveň zdravotní péče a současně překonat problém s nedostatkem kvalifikovaného personálu. A tak by bylo možné pokračovat dále v řadě oblastí, kde využití IoT přináší vysokou přidanou hodnotu.

Porozumění IoT je ovšem důležité také pro firmy, které se pohybují v dalších částech hodnototvorného řetězce. Pro systémové integrátory, poskytovatele managed služeb, poskytovatele komunikačních služeb a konektivity, výrobce zařízení či vývojáře platforem. IoT přináší zajímavé obchodní příležitosti všem těmto subjektům.

Je proto pro ně podstatné chápat internet věcí v celé šíři, rozumět výzvám, se kterými se ekosystém potýká a vidět trendy budoucího vývoje.

1.2 IoT jako komplexní systém

Internet věcí (Internet of Things) je dost obecný a také široký pojem. Díky tomu mohou být pod pojmem IoT v různých materiálech a v různém kontextu zahrnuty (nebo naopak nezahrnuty) odlišné technologie, řešení a případy užití.

Podívejme se proto na některé definice pojmu Internet věcí:

„Internet věcí (IoT) je síť fyzických objektů, které obsahují zabudovanou technologii pro komunikaci a snímání nebo interakci s jejich vnitřními stavy nebo s vnějším prostředím."[2]

„Internet věcí (IoT) je systém vzájemně propojených výpočetních zařízení, mechanických a digitálních strojů, objektů, zvířat nebo lidí, kteří jsou vybaveni unikátními identifikátory (UID) a schopností přenášet data přes síť bez nutnosti interakce přímo mezi lidmi nebo mezi lidmi a stroji."[3]

[2] Gartner IT Glossary, https://www.gartner.com/en/information-technology/glossary/internet-of-things

[3] IEEE Xplore Digital Library, https://ieeexplore.ieee.org

„IoT zahrnuje propojení více zařízení nebo systémů s internetem, což jim umožňuje sbírat, sdílet a analyzovat data. To může zahrnovat širokou škálu zařízení, včetně senzorů, akčních členů (aktuátorů) a chytrých zařízení, které společně poskytují vylepšené služby nebo zvyšují provozní efektivitu."[4]

„Internet věcí (IoT) označuje fyzická zařízení, která jsou nyní připojena k internetu, shromažďují a sdílejí data. Tato transformace má potenciál zlepšit efektivitu v různých odvětvích tím, že umožňuje chytřejší procesy a rozhodování."[5]

„Internet věcí neboli IoT je síť vzájemně propojených zařízení, která si vyměňují data s jinými zařízeními internetu věcí a cloudem. Zařízení internetu věcí jsou obvykle vybavena technologií, jako jsou senzory a software, a mohou zahrnovat mechanické a digitální stroje a další objekty."[6]

Tyto definice zdůrazňují základní aspekty IoT: propojení, výměnu dat, automatizaci a integraci fyzických objektů do digitálního rámce. Každý zdroj vyzdvihuje různé prvky, což odráží širokou použitelnost a různé interpretace IoT.

Zajímavá je jistě také skutečnost, že za součást Internetu věcí jsou považováni lidé či zvířata. Není to omyl. Ovšem lidé či zvířata jsou součástí systému IoT v tom smyslu, že nemusí realizovat žádnou aktivní interakci. Například wearables snímají určité životní funkce a parametry (lidí, ale i zvířat) a přenášejí je dále ke zpracování a vyhodnocení.

Pro účely této studie jsme sumarizovali definici IoT takto:

Internet věcí je systém jednoznačně identifikovaných zařízení, která sbírají data, jež jsou dále přenášena přes internet, analyzována a vyhodnocována a na základě kterých může být realizována akce v rámci systému nebo mimo něj. Tento systém má jasně daný účel, kterým je typicky zvyšování efektivity procesů, výkonnosti, informovanosti apod.

Většina výše uvedených definic internetu věcí se shoduje na tom, že IoT je systém. Podívejme se proto nejprve na obecnou definici systému. Můžeme proto použít definici systému, tak jak ji přináší Donella Meadows v knize Thinking in Systems[7]:

Systém je soubor prvků nebo komponentů, které jsou vzájemně propojeny tak, že vytvářejí určitý vzorec chování v průběhu času. Systém skládá ze tří hlavních prvků:

1. Elementy: To jsou jednotlivé části nebo komponenty systému. Prvky mohou být fyzické objekty (např. stroje v továrně) nebo nehmotné komponenty (např. pravidla nebo informační toky).

2. Propojení: Tím se rozumí vztahy nebo interakce mezi prvky. Tyto interakce určují, jak prvky spolupracují a jak reagují na vnější podněty nebo změny uvnitř systému.

3. Účel nebo funkce: Každý systém má svůj účel, který nemusí být vždy výslovně uveden, ale lze jej odvodit z chování systému. Účel je cílem nebo výsledkem, ke kterému systém přirozeně směřuje v důsledku interakcí jeho prvků.

Systém je více než jen součet svých částí; je definován způsobem, jakým tyto části spolupracují a fungují společně, aby dosáhly společného účelu. Systémy mohou být jednoduché nebo složité, ale vždy se vyznačují zpětnými vazbami, kde výstup jednoho prvku ovlivňuje chování ostatních prvků v rámci systému.

[4] ISO/IEC 20924:2024, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:20924:ed-3:v1:en

[5] McKinsey Digital, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things

[6] TechTarget IoT Agenda, https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[7] Donella Meadows, *Thinking in Systems* (Chelsea Green Publishing, 2008)

Jak IoT zapadá do definice systému?

Internet věcí (IoT) lze chápat jako systém podle výše uvedeného rámce:

1. Elementy:

- **Zařízení**: Patří sem senzory, akční členy (aktuátory), chytré spotřebiče a další připojený hardware, který sbírá a přenáší data.
- **Sítě**: Komunikační infrastruktura, která umožňuje zařízením se připojovat a vyměňovat si data (např. 5G).
- **Elementy pro zpracování dat:** Cloudové služby, edge computing zařízení a AI algoritmy, které zpracovávají a analyzují data získaná zařízeními.
- **Uživatelé**: Lidská obsluhy, automatizované systémy nebo rozhodovatelé, kteří využívají informace generované systémem IoT.

2. Propojení:

- **Datové toky**: IoT zařízení neustále generují data, která jsou přenášena přes sítě, zpracovávána v datových centrech nebo na edge zařízeních a poté dostupná pro další analýzu nebo akci.
- **Zpětné vazby**: Informace získané z analýzy dat jsou často vráceny zpět do systému, aby se přizpůsobilo chování zařízení, optimalizovaly operace nebo spustily automatizované reakce.
- **Řídicí mechanismy**: Patří sem protokoly, standardy a API, které určují, jak různá IoT zařízení a platformy spolupracují.

3. Účel nebo funkce:

Primárním účelem systému IoT je umožnit efektivnější, informovanější a automatizované rozhodovací procesy. IoT systémy jsou navrženy tak, aby zlepšily provozní efektivitu, zvýšily uživatelské zážitky, optimalizovaly využití zdrojů a podpořily inovace v různých odvětvích, včetně výroby, zdravotnictví, dopravy a chytrých měst.

Stručně řečeno, IoT je systém, který integruje různé fyzické a digitální komponenty za účelem vytvoření ucelené sítě schopné snímání, analýzy a reakce na data. Jeho účel je v souladu se zvyšováním funkčnosti, efektivity a rozhodovacích schopností napříč různými odvětvími, což z něj činí typický příklad složitého, propojeného systému.

1.3 Stručná historie IoT

Internet věcí (IoT) se vyvinul z konceptu propojení zařízení do technologie, která transformuje průmyslová odvětví, ekonomiky i každodenní život. Ačkoli byl termín „Internet věcí“ poprvé použit v roce 1999, základní myšlenky IoT se objevily již o několik desetiletí dříve. Tato kapitola poskytuje přehled klíčových událostí a milníků, které formovaly vývoj IoT od jeho počátků až po současnost.

Počátky a základy (70. – 90. léta).

Myšlenka propojení zařízení a umožnění jejich komunikace bez lidského zásahu předchází moderní internet. V 70. a 80. letech se začaly objevovat rané koncepty jako „pervazivní výpočetní technika“, které položily základy pro vznik IoT.

1982 – První propojené zařízení: Jedním z prvních příkladů propojeného zařízení byl automat na Coca-Colu na Carnegie Mellon University na počátku 80. let. Programátoři automat připojili k síti, což jim umožnilo zkontrolovat jeho zásoby a zjistit, zda jsou nápoje studené. Tímto se zapsal do historie propojených zařízení a stal se jedním z prvních případů IoT – zařízení poskytující data do sítě pro vzdálené monitorování a správu.

M2M komunikace: Na konci 20. století se objevila komunikace mezi stroji (M2M), kde zařízení komunikovala prostřednictvím sítí bez lidského zásahu. M2M poskytl základní rámec konektivity, který se později vyvinul do IoT, umožňující zařízení komunikovat přes drátové i bezdrátové sítě. Klíčovými příklady jsou telemetrické systémy v odvětvích jako je ropný a plynárenský průmysl, kde zařízení mohlo zasílat data o výkonu zpět do centrálního řídicího systému.

SCADA (Supervisory Control and Data Acquisition): SCADA systémy, které vznikaly od 60. let a rozvíjely se v 80. a 90. letech, byly také ranými předchůdci IoT. Tyto systémy shromažďovaly data v reálném čase z vzdálených lokalit pro monitorování a řízení zařízení a procesů. Vývoj SCADA směrem k síťovým systémům s integrovaným hardwarem a softwarem byl klíčovým krokem k první generaci IoT systémů.

Vznik pojmu a oblasti IoT (1999–2000s).

Termín „internet věcí“ byl oficiálně poprvé použit Kevinem Ashtonem, spoluzakladatelem Auto-ID Center na Massachusettském technologickém institutu (MIT), **v roce 1999**. Ashton použil tento termín během prezentace pro Procter & Gamble (P&G), aby zdůraznil potenciál RFID (radiofrekvenční identifikace) technologie pro propojení fyzických objektů s internetem a zlepšení řízení dodavatelského řetězce.

Ashton chtěl upozornit vedení P&G na technologii RFID, o které věřil, že může způsobit revoluci ve sledování a řízení zásob. Aby byla jeho prezentace zajímavá, nazval ji „internet věcí“ a spojil tehdejší trend internetu s fyzickými objekty, čímž poprvé formálně použil tento termín.

Ve stejné době vyšla také kniha MIT profesora Neila Gershenfelda „When Things Start to Think“ (Když věci začnou myslet), která sice termín IoT přímo nepoužila, ale popisovala svět, ve kterém by běžné předměty měly výpočetní sílu a konektivitu, což se úzce shodovalo s Ashtonovou vizí.

Oficiální uznání IoT: Mezinárodní telekomunikační unie (ITU) vydala v roce 2005 svou první zprávu o Internetu věcí, čímž oficiálně uznala IoT jako významný technologický koncept. Zpráva představila potenciál světa, ve kterém by prakticky všechny objekty mohly být propojeny a vzdáleně řízeny.

Technologická konvergence IoT (2010–2015).

Jak IoT nabývalo na síle, konvergence bezdrátových technologií, mikromechanických systémů (MEMS), mikroservisů a internetu začala odstraňovat bariéry mezi provozními technologiemi (OT) a informačními technologiemi (IT). Tato konvergence umožnila sběr a analýzu nestrukturovaných dat generovaných stroji k dosažení provozních vylepšení.

V roce 2010 koncept IoT ekosystému získal významný impuls, když čínská vláda oznámila, že IoT bude strategickou prioritou v jejím pětiletém plánu. Tento krok zvýraznil potenciál IoT na globální úrovni a inspiroval další země a průmysly k investicím do výzkumu a vývoje IoT.

V letech 2010 až 2019 technologie IoT rychle rostla díky rozšíření spotřebitelských zařízení, jako jsou chytré telefony, chytré televize a propojené domácí spotřebiče. Tato zařízení mohla komunikovat mezi sebou a připojovat se k internetu, což rozšířilo IoT i mimo průmyslové použití.

Růst cloud computingu a analýzy velkých dat poskytl infrastrukturu potřebnou k sběru, ukládání a zpracování obrovských objemů dat generovaných IoT zařízeními. Společnosti jako IBM, Cisco a GE vedly rané iniciativy k využití dat z IoT pro prediktivní údržbu, provozní efektivitu a nové obchodní modely.

Rozšíření, standardizace a další růst (2016–současnost).

Rychlé zavádění IoT zařízení zdůraznilo potřebu standardizace, zvýšené bezpečnosti a vylepšené infrastruktury pro podporu miliard propojených zařízení. V tomto období proběhly významné průmyslové iniciativy k řešení těchto výzev.

Organizace jako Open Connectivity Foundation (OCF) a Industrial Internet Consortium (IIC) byly založeny s cílem vyvinout standardy, které zajistí interoperabilitu mezi IoT zařízeními od různých výrobců.

Zavedení 5G sítí a vzestup edge computingu transformují IoT prostředí. 5G poskytuje vyšší šířku pásma, nízkou latenci a schopnost připojit obrovské množství zařízení, což umožní rozšíření IoT aplikací do oblastí, jako jsou autonomní vozidla, chytrá města a pokročilá průmyslová automatizace. Edge computing přiblížil zpracování dat k zařízením, čímž se sníží latence a umožní se rozhodování v reálném čase.

Koncept digitálních dvojčat – virtuálních modelů fyzických objektů nebo systémů – získal na významu po roce 2020, přičemž IoT senzory poskytují reálná data, která udržují digitální dvojče v souladu se skutečným protějškem. Tato technologie postupně nachází uplatnění ve výrobě, zdravotnictví a urbanismu, kde byla klíčová pro rozhodování.

V roce 2023 vydala aliance Connectivity Standards Alliance standard Matter, jehož cílem bylo řešit fragmentaci na trhu chytrých domácností. Matter usnadňuje bezproblémovou interakci mezi chytrými zařízeními od různých značek a zdůrazňuje pokračující snahu zlepšit interoperabilitu v IoT ekosystému.

2 Jak IoT funguje

2.1 Architektura IoT řešení.

Architektura internetu věcí (IoT) označuje strukturovaný rámec, který umožňuje integraci, zpracování a komunikaci dat z připojených zařízení. Efektivní IoT architektura se skládá z několika vrstev, z nichž každá je zodpovědná za různé logické funkce v celkovém systému.[8] Jednotlivé vrstvy znázorňuje následující obrázek:

Obrázek 1: Vrstvy IoT systému. Zdroj: vlastní zpracování.

1. Vrstva zařízení (percepční vrstva)

Komponenty: Senzory, akční členy (aktuátory), kamery a další chytrá zařízení.

[8] Simmons, Adam. "Internet of Things (IoT) Architecture: Layers Explained." Dgtl Infra, January 24, 2023.

Funkce: Vrstva zařízení je zodpovědná za sběr dat a interakci s fyzickým prostředím. Senzory detekují změny v prostředí (např. teplota, vlhkost, pohyb), zatímco akční členy provádějí akce na základě přijatých příkazů (např. zapnutí světla, nastavení ventilu).

Příklad: V chytré domácnosti monitoruje teplotní senzor (vrstva zařízení) teplotu v místnosti. Kamera ve výrobní hale monitoruje chování stroje a odchylky od normálu.

2. Síťová vrstva (Vrstva konektivity či také komunikační vrstva)

Komponenty: komunikační sítě a protokoly (např. Wi-Fi, Bluetooth, Zigbee, 5G), směrovače (routers).

Funkce: Tato vrstva zajišťuje přenos dat z vrstvy zařízení do vrstvy zpracování. Zahrnuje komunikační infrastrukturu a protokoly, které umožňují zařízením připojit se k internetu nebo místním sítím, což umožňuje výměnu dat.

Příklad: Teplotní senzor v chytré domácnosti odesílá svá data přes Wi-Fi do centrálního hubu. Senzor znečištění ovzduší zasílá informaci přes NB-IoT.

3. Edge vrstva (Vrstva edge computingu)

Komponenty: Edge zařízení, brány (gateways), lokální zpracovatelské jednotky, mikrokontroléry.

Funkce: Vrstva edge zpracovává data blíže ke zdroji (tj. k zařízením). Prováděním počátečního zpracování a filtrování na edge zařízení snižuje latenci a využití šířky pásma, což umožňuje rychlou reakci a efektivní správu dat.

Příklad: Data z výrobní linky jsou lokálně zpracována pro okamžitou identifikaci zmetkových výrobků. Data jsou dále zaslána do cloudu pro zpracování trendů a dalších analýz.

Poznámka: Edge vrstva může, ale nemusí být součástí IoT architektury. V některých případech jsou data zasílána přímo do centrálních prvků.

4. Zpracovatelská vrstva (Vrstva správy dat, nebo také middleware layer)

Komponenty: Cloudové servery, systémy pro ukládání dat, analytické nástroje.

Funkce: Tato vrstva se zabývá rozsáhlým zpracováním dat, jejich ukládáním a analýzou. Obvykle se nachází v cloudu, kde mohou být na data aplikovány složité výpočty a algoritmy strojového učení.

Příklad: Data o činnosti výrobní linky jsou agregována a analyzována v cloudu za účelem identifikace dlouhodobých vzorců, což umožňuje prediktivní údržbu nebo optimalizaci spotřeby energie.

IoT systém obvykle zpracovává obrovské objemy dat, které generuje množství edge zařízení na různých místech na okrajích sítě. „Middleware“ ve vrstvě zpracování využívá třífázový přístup k přípravě těchto dat pro aplikační vrstvu:

- Akumulace dat: middleware identifikuje a přiřazuje různé typy dat k odpovídajícímu úložišti. Nestrukturovaná data, jako jsou audio a video streamy a obrázky, obvykle vyžadují více úložného prostoru a jsou uchovávána v datových jezerech (data lakes). Naopak strukturovaná data, která zahrnují například hodnoty logů a telemetrická data, jsou efektivnější z hlediska prostoru a jsou ukládána v datových skladech (data warehouses).

- Abstrakce dat: Zahrnuje agregaci dat z více zdrojů a také zajištění toho, aby byla data převedena do formátu, který může být „čten“ softwarem aplikační vrstvy.

- Analýza dat: Využívá algoritmy strojového učení (ML) nebo hlubokého učení, které jsou specializovány na detekci vzorců v rozsáhlých a zdánlivě náhodných datových sadách.

5. Aplikační vrstva

Komponenty: Softwarové aplikace, uživatelská rozhraní, dashboardy.

Funkce: Aplikační vrstva poskytuje rozhraní, prostřednictvím kterého uživatelé interagují se systémem IoT. Interpretuje a prezentuje data uživatelsky přívětivým způsobem a umožňuje uživatelům ovládat zařízení, monitorovat výkon systému a činit informovaná rozhodnutí.

Příklad: Mobilní aplikace, která umožňuje majiteli domu na dálku monitorovat a upravovat nastavení teploty v chytré domácnosti.

6. Bezpečnostní vrstva

Komponenty: Šifrovací protokoly, autentizační mechanismy, firewally.

Funkce: Tato vrstva je zodpovědná za zajištění bezpečnosti a soukromí dat při jejich toku v rámci architektury IoT. Zahrnuje opatření na ochranu dat před neoprávněným přístupem, prevenci narušení a zajištění toho, aby komunikace v IoT síti byla bezpečná.

Příklad: Šifrovaná komunikace mezi teplotním senzorem a centrálním hubem zajišťuje, že data nemohou být zachycena nebo změněna neoprávněnými stranami.

7. Obchodní vrstva

Komponenty: Obchodní logika, nástroje pro řízení pravidel, nástroje pro správu politik.

Funkce: Obchodní vrstva interpretuje data v kontextu cílů a záměrů organizace. Pomáhá při rozhodovacích procesech aplikací obchodních pravidel a politik pro data. Tato vrstva zajišťuje, že systém IoT je v souladu s obchodní strategií a přináší hodnotu.

Příklad: V komerční budově může systém IoT analyzovat data o spotřebě energie, aby optimalizoval provoz, čímž snižuje náklady a podporuje dosažení cílů v oblasti udržitelnosti.

Jednotlivé vrstvy IoT architektury tedy představují logické funkce IoT systému. V reálné implementaci ovšem jednotlivé elementy řešení pokrývají jednu čí více logických vrstev. Například IoT platforma pokrývá typicky zpracovatelskou vrstvu, aplikační vrstvu a obchodní vrstvu, přesah má také bezpečnostní vrstvy.

IoT architektura a 5G

Potenciální využití 5G technologie ovlivňuje několik vrstev IoT architektury:

Percepční vrstva – v této vrstvě budou využita 5G zařízení. Tedy senzory a další koncové prvky obsahující 5G modem. Může jít o standardní 5G NR, nebo o varianty určené pro IoT, tedy RedCap a Passive IoT, stejně tak technologie převzaté do 5G ekosystému Cat-M a NB-IoT.

Síťová vrstva – v této vrstvě bude využita 5G síť pro transport dat z koncových prvků na edge a/nebo do centrální platformy.

Edge vrstva – jednou z klíčových vlastností 5G technologie je oddělení control plane a user plane (CUPS), které umožňuje zpracování uživatelských dat na edge, tedy blízko zdroje. Bez nutnosti je přenášet do vzdáleného jádra sítě. Díky tomu je možné při využití 5G technologie využít funkcí a výhod edge vrstvy.

Bezpečnostní vrstva – technologie 5G je nativně vysoce bezpečná, na rozdíl od řady jiných alternativ, které mohou být v rámci IoT systému také využity. Autentizace s využitím fyzických či v případě IoT řešení spíše e-SIM a pokročilé šifrování přispívají k celkové bezpečnosti IoT systému založeného na 5G.

Zpracovatelská, aplikační a obchodní vrstva jsou naopak v principu nezávislé na využití 5G technologie.

2.2 IoT (přenosové) technologie

2.2.1 Popis a charakteristika IoT přenosových technologií

IoT přenosová technologie zajišťuje přenos dat z koncových prvků (senzorů, aktuátorů) na edge rozhraní a/nebo do centrálních prvků IoT systému (na servery, kde jsou data zpracována) a případně také v opačném směru.

IoT přenosová technologie a její volba tedy hraje klíčovou roli v:

- percepční vrstvě (ovlivňuje, jaké typy koncových zařízení mohou být použité),
- síťové vrstvě.

Má ovšem také vliv na edge vrstvu, obchodní vrstvu a bezpečnostní vrstvu.

Z tohoto výčtu je zřejmé, jak důležitou roli hraje IoT přenosová technologie v celém IoT systému, jak důležité je znát různé varianty technologií a zvolit tu nejvhodnější pro daný IoT systém.

Dále je uveden popis nejpoužívanějších přenosových technologií používaných pro IoT řešení.

Některé z těchto technologií byly navrženy už přímo s tím, že budou pro IoT používány. Jiné jsou technologie využívané pro obecné účely, například interpersonální komunikaci nebo připojení k internetu, ovšem současně s úspěchem slouží také pro IoT projekty.

1. GPRS (General Packet Radio Service)

GPRS je raná služba pro mobilní přenos dat, která byla vyvinuta na konci 90. let jako součást sítě druhé generace (2G), často označovaná jako 2,5G. Byla navržena pro zajištění středních rychlostí přenosu dat, což umožnilo mobilním zařízením odesílat a přijímat data přes mobilní síť. GPRS používá technologii paketového přepínání, což znamená, že data jsou přenášena v malých balíčcích místo kontinuálního toku, což umožňuje efektivnější využití síťových zdrojů ve srovnání se systémy s okruhovým přepínáním, jako je GSM. I když jsou rychlosti dat poměrně nízké, typicky v rozmezí 56 až 114 kbps, GPRS bylo revoluční technologií své doby, umožňující mobilní prohlížení internetu, e-mail a základní multimediální zprávy. V kontextu IoT bylo GPRS používáno v prvních generacích aplikací, jako je sledování vozidel, dálkové monitorování a základní telemetrie, zejména v oblastech s omezenou infrastrukturou sítě. S nástupem novějších a rychlejších technologií je však GPRS pro většinu moderních IoT aplikací považováno za zastaralé.

2. 4G/5G

4G (čtvrtá generace) a 5G (pátá generace) jsou nejnovější generace mobilních sítí. 4G, uvedená na trh kolem roku 2010, přinesla vysokorychlostní mobilní připojení s datovými rychlostmi až 100 Mbps pro mobilní komunikaci, což umožnilo pokročilé aplikace jako je streamování HD videa a online hraní. Také podporovala IoT případy použití, které vyžadovaly vyšší datové rychlosti a spolehlivé připojení, například propojená vozidla, chytrá města a průmyslovou automatizaci. 5G, která se začala celosvětově nasazovat v roce 2019, staví na schopnostech 4G a nabízí mnohem vyšší datové rychlosti (až 10 Gbps), ultra nízkou latenci a schopnost připojit masivní počet zařízení současně. Klíčové vlastnosti 5G zahrnují rozšířené mobilní širokopásmové

připojení (eMBB), ultra spolehlivou komunikaci s nízkou latencí (URLLC) a masivní strojovou komunikaci (mMTC), což ji činí ideální pro širokou škálu IoT aplikací, od chytrých měst a autonomních vozidel po průmyslové IoT a zdravotnictví.

4G ani 5G nejsou specificky IoT technologie. Obě generace se vyznačují tím, že podporují více než dostatečné přenosové rychlosti z pohledu IoT, naproti tomu mají poměrně drahá a energeticky náročná koncová zařízení. 5G má oproti 4G výhodu také v tom, že z pohledu architektury je vhodnější pro privátní sítě.

Detailní popis 5G technologie, architektury a vlastností včetně jejich dostupnosti, je součástí studie „**Využívání 5G a jiných sítí elektronických komunikací pro potřeby digitalizace podniků včetně využití moderních informačních systémů.“**

3. NB-IoT (Narrowband IoT)

NB-IoT je technologie pro nízkoenergetické širokopásmové sítě (LPWAN) standardizovaná organizací 3GPP v rámci Release 13, která byla navržena speciálně pro IoT aplikace. Funguje v rámci stávajícího spektra LTE, ale vyžaduje pouze úzké pásmo o šířce 180 kHz, což ji činí velmi efektivní pro přenos malého množství dat na dlouhé vzdálenosti. NB-IoT podporuje hluboký vnitřní průnik signálu, což je významná výhoda pro případy použití, jako je chytré měření, environmentální monitorování a sledování majetku, kdy jsou zařízení často umístěna v suterénech nebo jiných těžko přístupných místech. Technologie se vyznačuje nízkou spotřebou energie, což umožňuje zařízením fungovat až 10 let na jednu baterii. NB-IoT je díky své jednoduchosti, spolehlivosti a širokému přijetí mobilními operátory populární volbou pro IoT nasazení, zejména tam, kde se jedná o masivní počet zařízení s nízkými datovými nároky.

4. LTE-M (Long Term Evolution for Machines)

LTE-M je další technologie LPWAN vyvinutá v rámci standardů 3GPP, specificky pro IoT aplikace, které vyžadují větší šířku pásma a mobilitu než NB-IoT. Funguje na stávající LTE infrastruktuře, ale s důrazem na snížení složitosti zařízení a spotřeby energie. LTE-M podporuje hlasové služby prostřednictvím VoLTE, což z něj činí vhodnou volbu pro IoT aplikace, které vyžadují jak datovou, tak hlasovou komunikaci, jako jsou nositelná zařízení, monitorování zdravotního stavu a sledování majetku. Podporuje také vyšší datové rychlosti (až 1 Mbps), mobilitu a přechody mezi buňkami, což umožňuje kontinuální pokrytí v mobilních scénářích, jako je sledování vozidel nebo připojené dopravní systémy. Zařízení LTE-M mohou pracovat v režimech spánku, což dále prodlužuje životnost baterie, a nabízí dobrou rovnováhu mezi výkonem, náklady a pokrytím, což ho činí ideálním pro širokou škálu IoT případů použití.

5. LTE Cat 1 bis

LTE Cat 1 bis je evolucí technologie LTE Cat 1, což je kategorie LTE navržená pro IoT aplikace, které vyžadují střední datové rychlosti. Zatímco standardní LTE Cat 1 vyžaduje full-duplex komunikaci, LTE Cat 1 bis je navržena pro half-duplex komunikaci, což zjednodušuje design zařízení a snižuje náklady. Podporuje datové rychlosti až 10 Mbps, což ho činí vhodným pro IoT aplikace jako terminály prodeje (POS), bankomaty a telematiku, kde je vyžadována jak datová, tak hlasová komunikace, ale nejsou nutné ultra vysoké rychlosti. LTE Cat 1 bis je obzvláště ceněna pro svou schopnost vyvažovat spotřebu energie a výkon, nabízející dobrý střed mezi vyššími rychlostmi LTE kategorií a energeticky úspornějšími technologiemi LPWAN, jako je NB-IoT. Tato technologie je obzvláště relevantní pro trhy, kde je již LTE infrastruktura zavedena a je potřeba cenově efektivní IoT řešení.

6. NR-Light/ RedCap (Reduced Capability)

RedCap, nebo Reduced Capability New Radio, je funkce zavedená v sítích 5G na podporu IoT zařízení, která vyžadují střední datové rychlosti a nízkou složitost, ale přesto těží z výhod 5G, jako je nízká latence a vysoká spolehlivost. RedCap je v podstatě zjednodušenou verzí 5G standardu, navrženou pro IoT aplikace, jako jsou průmyslové senzory, nositelná zařízení a infrastruktura chytrých měst, která nepotřebují plné schopnosti 5G, ale stále vyžadují vyšší výkon než technologie LPWAN. Snížením složitosti zařízení RedCap snižuje náklady a spotřebu energie, což z něj činí vysoce efektivní řešení pro středně náročné IoT případy použití. Jak se

budou sítě 5G nadále vyvíjet, očekává se, že RedCap bude hrát významnou roli v rozšiřování dosahu IoT napříč různými odvětvími.

7. 5G Passive IoT

5G Passive IoT představuje novou hranici v IoT technologiích, kde jsou zařízení napájena výhradně energií získávanou z okolních zdrojů, jako jsou rádiové frekvence, tepelné gradienty nebo mechanické vibrace. Tento přístup eliminuje potřebu tradičních baterií, což výrazně snižuje náklady na údržbu a umožňuje nasazení masivního množství senzorů na široké ploše. 5G Passive IoT se integruje s 5G sítěmi, aby poskytoval komunikaci dlouhého dosahu, vysokou spolehlivost a schopnost připojit obrovské množství zařízení současně. Tato technologie je obzvláště vhodná pro aplikace jako environmentální monitorování, chytré zemědělství a řízení dodavatelských řetězců, kde mohou být senzory nasazeny v odlehlých nebo těžko přístupných místech. Standardizace 5G Passive IoT se očekává v rámci 3GPP Release 19, s nasazením očekávaným v nadcházejících letech.

8. LoRa (Long Range)

LoRa je proprietární technologie LPWAN vyvinutá společností Semtech, známá svou schopností poskytovat dlouhodobou komunikaci (až 15-20 km ve venkovských oblastech) při velmi nízké spotřebě energie. Funguje v nelicencovaných frekvenčních pásmech (například 868 MHz v Evropě a 915 MHz v Severní Americe), což jí poskytuje vysokou flexibilitu a možnost nezávislého nasazení mimo mobilní sítě, což ji činí populární volbou pro IoT aplikace tam, kde chybí infrastruktura konektivity. Klíčové charakteristiky LoRa zahrnují dlouhou životnost baterie, dobrou penetraci signuálu a škálovatelnost, což podporuje rozsáhlé sítě s tisíci zařízeními. Je široce využívána v chytrých městech, chytrém zemědělství, environmentálním monitorování a měření spotřeby. Otevřený protokol LoRaWAN poskytuje síťovou architekturu a bezpečnostní funkce potřebné pro rozsáhlé nasazení, což z ní činí nejčastější volbu pro necelulární IoT aplikace.

9. ZigBee

ZigBee je bezdrátová komunikační technologie s krátkým dosahem a nízkou spotřebou energie, založená na standardu IEEE 802.15.4. Byla vyvinuta po roce 2000, aby reagovala na potřebu jednoduché, nízkonákladové a nízkoenergetické komunikace mezi zařízeními v síti. ZigBee funguje v pásmu 2,4 GHz ISM a je navržena pro síťování typu mesh, kde zařízení mohou přímo komunikovat mezi sebou, což rozšiřuje dosah a spolehlivost sítě. To činí ZigBee ideální pro aplikace v domácí automatizaci, chytrém osvětlení, správě energie a automatizaci budov. Klíčové vlastnosti ZigBee zahrnují nízkou spotřebu energie, která umožňuje zařízením fungovat po celé roky na malých bateriích, a podporu hustých sítí až s 65 000 uzly. I když čelí konkurenci jiných bezdrátových standardů, jako jsou Wi-Fi a Bluetooth, ZigBee zůstává populární volbou pro IoT aplikace, které vyžadují spolehlivou, nízkonákladovou komunikaci na krátké vzdálenosti.

10. Bluetooth

Bluetooth je bezdrátová komunikační technologie s krátkým dosahem, která byla široce přijata od svého zavedení na konci 90. let. Původně byla vyvinuta pro bezdrátové propojení osobních zařízení, jako jsou sluchátka a klávesnice, ale Bluetooth se vyvinul tak, aby podporoval různé IoT aplikace, zejména s uvedením Bluetooth Low Energy (BLE) v roce 2010. BLE je optimalizován pro nízkoenergetická zařízení, což jim umožňuje fungovat po dlouhou dobu na malých bateriích, což ho činí ideálním pro použití v nositelných zařízeních, zdravotnických monitorovacích zařízeních, majících a chytrých domácích aplikacích. Bluetooth funguje v pásmu 2,4 GHz ISM a podporuje datové rychlosti až 2 Mbps. Jednou z klíčových silných stránek Bluetooth je jeho široké přijetí a interoperabilita, což umožňuje zařízením od různých výrobců komunikovat bezproblémově. Schopnost podporovat jak bod-bod, tak síťování mesh činí Bluetooth všestrannou technologií v oblasti IoT.

11. WiFi

WiFi je dobře zavedená bezdrátová síťová technologie, která poskytuje vysokorychlostní přístup k internetu a přenos dat na krátké až střední vzdálenosti. Na základě standardů IEEE 802.11 funguje WiFi primárně v

pásmech 2,4 GHz a 5 GHz a nabízí datové rychlosti, které mohou v posledních verzích přesahovat 1 Gbps. Schopnost WiFi zvládat velké objemy dat ji činí ideální pro IoT aplikace, které vyžadují vysokou šířku pásma, jako je video dohled a chytré spotřebiče. WiFi však typicky spotřebovává více energie než technologie LPWAN, což může omezit její použití v bateriově napájených IoT zařízeních. Navzdory tomu je WiFi díky své všudypřítomnosti v domácnostech, kancelářích a veřejných prostorech a solidním bezpečnostním protokolům (nových verzí WiFi6 či WiFi7) klíčovým prvkem ekosystémů IoT, zejména pro aplikace, kde jsou zařízení připojena k napájení a vyžadují vysokorychlostní připojení.

Shrnutí parametrů technologií využívaných pro IoT:

Technologie pro IoT	Dlouhý/ Krátký dosah	Přenosová rychlost	Obousměrná komunikace (vhodnost a frekvence)	Latence (ms)	Podpora mobility
GPRS	Dlouhý	40-171 kbps	Vhodné, nízká frekvence	Vysoká (500+)	Ano
4G/5G	Dlouhý	1 Mbps - 1 Gbps+	Vysoce vhodné, vysoká frekvence	Nízká (<10)	Ano
NB-IoT	Dlouhý	do 250 kbps	Omezená vhodnost, nízká frekvence	Střední (100-1500)	Ne
Cat-M	Dlouhý	375-1000 kbps	Vhodné, střední frekvence	Nízká (50-100)	Ano
LTE Cat 1 bis	Dlouhý	5-10 Mbps	Vhodné, střední frekvence	Nízká (<50)	Ano
RedCap	Dlouhý	50-150 Mbps	Vysoce vhodné, střední až vysoká frekvence	Nízká (<20)	Ano
5G Passive IoT	Dlouhý	<100 kbps	Omezená vhodnost, nízká frekvence	Nízká (<50)	Ne
LoRa	Dlouhý	<50 kbps	Vhodné, nízká frekvence	Vysoká (1000-10000)	Omezená
ZigBee	Krátký	20-250 kbps	Vhodné, vysoká frekvence	Nízká (<50)	Ne
Bluetooth	Krátký	1-3 Mbps	Vysoce vhodné, vysoká frekvence	Nízká (<50)	Ne
WiFi	Krátký	až 1 Gbps	Vysoce vhodné, vysoká frekvence	Nízká (<50)	Omezená

Technologie pro IoT	Podpora mezinárodního roamingu (ano/ne)	Spotřeba energie UE (nízká/střední/vysoká)	Vhodné pro kritickou komunikaci	Úroveň kybernetické bezpečnosti (nízká/střední/vysoká)	Náklady (nízké/střední/vysoké)
GPRS	Ano	Vysoká	Ne	Střední	Střední
4G/5G	Ano	Střední až vysoká	Ano	Vysoká	Střední až vysoké
NB-IoT	Omezená	Nízká	Ne	Střední až vysoká	Střední
Cat-M	Ano	Nízká	Ano	Střední až vysoká	Střední
LTE Cat 1 bis	Ano	Nízká až střední	Ano	Vysoká	Střední
RedCap	Ano	Nízká až střední	Ano	Vysoká	Střední
5G Passive IoT	Omezená	Velmi nízká	Ne	Vysoká	Nízké
LoRa	Ne	Nízká	Ne	Střední	Nízké
ZigBee	Ne	Nízká	Ne	Střední	Nízké
Bluetooth	Ne	Nízká	Ne	Střední až vysoká	Nízké
WiFi	Ne	Střední až vysoká	Ne	Střední až vysoká	Nízké až střední

2.2.2 Kategorizace IoT přenosových technologií.

Kategorizaci je možné udělat podle několika různých kritérií, která vždy dávají určitou informaci ohledně možnosti a vhodnosti využití dané IoT technologie.

V souvislosti s IoT přenosovými technologiemi se často mluví o mMTC a LPWAN. Podívejme se blíže na tyto pojmy a to, které technologie do daných kategorií patří.

mMTC (massive Machine Type Communications)

mMTC je klíčovou funkcí technologie 5G, navrženou pro podporu velkého počtu připojených zařízení, která obvykle přenášejí malé množství dat přerušovaně. Je ideální pro aplikace, jako jsou chytrá města, průmyslový IoT a rozsáhlé senzorové sítě, kde je vysoká hustota připojených zařízení a kde je důležitá energetická účinnost. mMTC se zaměřuje na poskytování škálovatelné konektivity a podporuje potenciálně miliony IoT zařízení na kilometr čtvereční.

LPWAN (Low-Power Wide-Area Network)

LPWAN je kategorie bezdrátových komunikačních technologií navržená pro komunikaci na dlouhé vzdálenosti s nízkou spotřebou energie, což je ideální pro IoT zařízení, která potřebují fungovat na baterie po mnoho let. LPWAN technologie se obvykle používají pro aplikace, které vyžadují dlouhodobou konektivitu, nízké datové přenosy a méně častou komunikaci, jako jsou chytré měření, monitorování životního prostředí a sledování majetku. LPWAN technologie pracují v licencovaných i nelicencovaných frekvenčních pásmech. Následujícící tabulka obsahuje přehled rozřazení technologií do těchto kategorií:

IoT technologie	**mMTC**	**LPWAN**
GPRS	Ne	Ne
4G/5G	Ano	Ne
NB-IoT	Ano	Ano
Cat-M	Ano	Ano
LTE Cat 1 bis	Ano	Ano (!)
RedCap	Ano	Ano (!)
Passive IoT	Ano	Ano
LoRa	Ne	Ano
ZigBee	Ne	Ne
Bluetooth	Ne	Ne

WiFi	Ne	Ne

Cat-M (LTE-M) a NB-IoT vs. mMTC/5G

Trochu paradoxně jsou za mMTC technologie oficiálně označovány také Cat-M (nebo také Cat-M1 či LTE-M, jsou to vzájemně zaměnitelné pojmy) a NB-IoT, což jsou technologie 4G. Počítá se s nimi ovšem i v 5G ekosystému a v principu jsou určeny k machine type communication a připojení velkého počtu zařízení.

Ačkoli je mMTC formálně součástí standardu 5G, NB-IoT a LTE-M byly vyvinuty v rámci 4G (LTE), aby splnily rostoucí potřeby pro masivní IoT konektivitu. Tyto technologie se zaměřují na poskytování nízkoenergetické, širokoplošné konektivity pro obrovské množství zařízení, což je v souladu s cíli mMTC.

Obě technologie, NB-IoT a LTE-M, jsou začleněny do širšího ekosystému 5G. Tato integrace je součástí specifikací 3GPP (3rd Generation Partnership Project) Release 15 a Release 16, které zajišťují, že tyto technologie mohou koexistovat s dalšími komponentami 5G.

V rámci 5G mohou být NB-IoT a LTE-M nasazeny buď jako samostatné sítě, nebo jako součást 5G sítě pomocí dynamického sdílení spektra (DSS). To jim umožňuje pokračovat v provozu ve svých stávajících frekvenčních pásmech a zároveň využívat vylepšení, která přináší 5G, jako je lepší latence a podpora masivního nasazení zařízení.

Průmysl se zavázal k dlouhodobé podpoře technologií NB-IoT a LTE-M, což zajišťuje, že zůstanou relevantní a široce používané i v nadcházejících desetiletích. Tato dlouhodobá podpora je zásadní pro odvětví, která již výrazně investovala do těchto technologií.

Existují snahy o další vylepšení NB-IoT a LTE-M v rámci 5G. To zahrnuje zlepšení energetické účinnosti, rozšíření pokrytí a zvýšení kapacity. Tato vylepšení jsou klíčová pro podporu rostoucího počtu IoT zařízení, která se očekává, že budou připojena v nadcházejících letech.

GPRS: Není klasifikováno jako mMTC nebo LPWAN, protože se jedná o starší technologii primárně používanou pro základní mobilní komunikaci.

4G/5G: Spadá pod mMTC díky své schopnosti podporovat velké množství zařízení, zejména s technologií 5G.

NB-IoT: Podporuje jak mMTC, tak LPWAN, je navrženo pro masivní konektivitu s nízkou spotřebou energie.

LTE-M: Podporuje jak mMTC, tak LPWAN, vhodné pro IoT zařízení vyžadující střední přenosové rychlosti a mobilitu.

LTE Cat 1 bis: Podporuje mMTC. Není vždy klasifikováno jako LPWAN – jde o poměrně hraniční případ, protože má funkcionality podporující snížení spotřeby energie.

RedCap: Patří do rodiny 5G podporující mMTC. Není specificky navrženo jako LPWAN, ale opět jde o hraniční případ, kdy má určité vlastnosti vedoucí k nižší spotřebě energie.

5G Passive IoT: Navrženo tak, aby podporovalo vlastnosti jak mMTC, tak LPWAN.

LoRa: Čistá LPWAN technologie, navržena pro dlouhodobou, nízkoenergetickou komunikaci.

ZigBee: Není klasifikováno jako mMTC nebo LPWAN; jedná se o krátkodosahovou technologii.

Bluetooth: Není klasifikováno jako mMTC nebo LPWAN; jedná se primárně o krátkodosahovou osobní síťovou technologii.

WiFi: Není klasifikováno jako mMTC nebo LPWAN; používá se pro vysokorychlostní přenosy dat na krátké vzdálenosti.

2.2.3 Další možnosti kategorizace IoT přenosových technologií

Dle šířky pásma:

Ovlivňuje možnost využití pro různé aplikace dle datové náročnosti.

Úzkopásmonové, pro přenost malých datových objemů: GPRS, LoRa, NB-IoT

Širokopásmové, které zvládnou i vysoké či střední rychlosti a objemy dat: klasické 4G/5G, 5G RedCap, LTE-M

Dle spotřeby energie:

Ovlivňuje vhodnost pro případy užití, kde není možné napájení z elektrické sítě.

LPWAN (Low Power WAN) – specificky s nízkou spotřebou: NB-IoT, LTE-M, 5G Passive IoT, LoRa, RedCap (hraniční případ).

Ostatní – bez speciálního řešení, které by vedlo k nízké spotřebě energie koncového zařízení: klasické 4G/5G, GPRS.

Dle dosahu:

Dosah technologie ovlivňuje vhodnost použití pro čistě lokální případy užití, nebo pro případy užití na velké ploše, celonárodní či dokonce mezinárodní.

Technologie s krátkým dosahem: NFC, Bluetooth. Zigbee, RFID (podle některých zdrojů nejsou jednoduché technologie RFID do IoT počítány).

Technologie s dlouhým dosahem: LoRa (zkratka ostatně znamená „Long Range“, tedy dlouhý dosah), NB-IoT, LTE-M a další klasické 4G/5G technologie.

Dle využití licencovaného pásma:

Některé technologie jsou určeny k využití na licencovaném pásmu. To má své výhody i nevýhody. Mezi výhody patří odolnost vůči rušení a bezpečnost. Nevýhodou je nutnost řešit projekt výhradně s vlastníky pásma, obvykle mobilními operátory a s tím spojené vyšší náklady. Jiné technologie naopak využívají nelicenovaná pásma.

Technologie na licencovaném pásmu: GPRS, 4G/5G, RedCap, NB-IoT, LTE-M.

Technologie na nelicencovaném pásmu: LoRa, Bluetooth, Zigbee, NFC.

Dle standardizace

Způsob standardizace může mít vliv na způsob dalšího vývoje technologie. Z toho pohledu má smysl členit technologie zejména na 3GPP, za kterými je obrovský ekosystém mobilních operátorů a ostatní, jejichž ekosystém je typicky skromnější. Výhodou 3GPP technologií je téměř jistota, že technologie není slepou vývojovou uličkou a bude mít dlouhodobou kontinuitu. Nevýhodou je obvykle vyšší nákladnost.

3GPP technologie: GPRS, 4G/5G, RedCap, NB-IoT, LTE-M.

Ostatní: LoRa, SigFox.

2.3 5G technologie pro IoT – vývoj a využití

2.3.1 NR-Light (5G RedCap) je řešením pro mid-range IoT.

Existuje velmi široká škála IoT případů užití, které se liší svými požadavky na IoT systémy. Tím pádem se podstatně liší to, jaké parametry by měla mít technologie podporující dané případy užití. V detailu jsou případy užití a jejich požadavky rozebrány v kapitole 3.

Lze ovšem sumarizovat, že na jedné straně (jedním extrémem) je tady **mission critical IoT**. To jsou případy užití vyžadující ultra vysokou spolehlivost komunikace, nízkou latenci a obvykle také vysoké přenosové rychlosti. Naopak obvykle nevyžadují energetickou úspornost koncových zařízení. Příkladem mission/business critical IoT jsou monitorovací a řídící systémy v rámci průmyslového internetu věcí, provoz různého typu robotů jakou jsou AMR a cobots, autonomní systémy v zemědělství nebo řada případů užití ve zdravotnictví spojených s monitoringem životních funkcí atd.

Pro mission/business critical IoT je možné s úspěchem využít bezpečnou a spolehlivou 5G technologii. V některých případech může jít dokonce o síť podporující URLLC (ultra spolehlivou komunikaci a nízkou latenci).

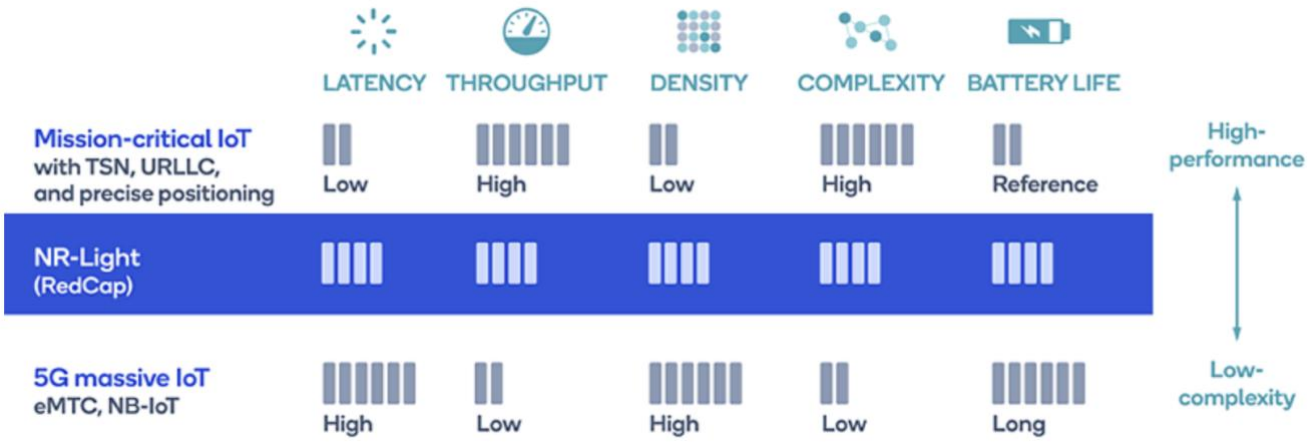
Na druhé straně (druhým extrémem) je tzv. **massive IoT**. To jsou případy užití, které naopak nevyžadují specificky vysokou spolehlivost komunikace a nízkou latenci. Většinou jsou spojeny s přenosem nízkých datových objemů s nízkou frekvencí komunikace s koncovými zařízeními. A často (ne vždy) vyžadují nízkou spotřebu energie ze strany koncových zařízení, která musí být v provozu na baterii. Příkladem massive IoT případů užití jsou měření energií, sledování přírodního prostředí či moniring dostupnosti parkovacích míst.

Pro massive IoT jsou již nyní využívány technologie NB-IoT a eMTC (neboli LTE cat-M). Ač původně 4G technologie (viz výše), počítá se s jejich evolucí v rámci 5G ekosystému.

Pak je tedy ovšem řada IoT případů užití, které se pohybují někde mezi těmito extrémy v podobě mission critical IoT a massive IoT. Je možné je charakterizovat jako tzv. **mid-range IoT**, tedy případy užití se střední úrovní požadavků. Je vyžadována dobrá spolehlivost komunikace, střední rychlosti datových přenosů, latence nemusí být ultra nízká.

Pro tyto případy užití by teoreticky mohla být využita klasická 5G technologie (eMBB/ URLLC). Ale ta je poměrně nákladná, a to zejména z pohledu koncových zařízení. Pro mid-range je očekávána také příznivá nákladovost, která umožní funkční business model pro tyto případy užití.

Právě pro tyto IoT mid-range případy užití vznikla ReCap technologie. Pro překlenutí značné propasti mezi massive IoT technologiemi NB-IoT a LTE-M (eMTC) a mission kritickým 5G, jak názorně ukazuje následující obrázek.



Obrázek 2: NR-light/ RedCap jako můstek mezi 5G pro mission ciritcal IoT a NB-IoT/eMTC (cat-M) pro massive IoT. Zdroj: [9]

V rámci 5G NR Release 17 představila organizace 3GPP novou kategorii zařízení s nižšími schopnostmi (RedCap), známou také jako NR-Light. Jedná se o novou platformu zařízení, která překonává propast v schopnostech a složitosti mezi extrémy současného 5G a je optimalizována pro případy užití střední třídy. Ve srovnání se zařízeními pro 5G enhanced mobile broadband (eMBB), která mohou podporovat rychlost přenosu v downlinku a uplinku až několik gigabitů za sekundu, mohou zařízení NR-Light díky navrženým optimalizacím efektivně podporovat rychlosti 150 Mbps v downlinku a 50 Mbps v uplinku:

- užší šířky pásma, např. 20 MHz v pásmech pod 7 GHz nebo 100 MHz v pásmech milimetrových vln (mmWave),
- jedna vysílací anténa,
- jedna přijímací anténa, s možností volby dvou antén,
- volitelná podpora pro half-duplex FDD,
- nižší řád modulace, přičemž 256-QAM je volitelná, a
- podpora pro nižší vysílací výkon.

Snížená složitost přispívá k cenově efektivnějším zařízením NR-Light, delší životnosti baterie díky nižší spotřebě energie a menšímu rozměru zařízení.

První verze standardu 5G NR, 3GPP Release 15, podporovala dvě úrovně zařízení pro masivní IoT, konkrétně eMTC (Cat-M1) pro kanály o šířce 1,4 MHz a NB-IoT pro kanály o šířce 200 kHz. Díky vylepšením zavedeným v 3GPP Release 16 mohou zařízení obou těchto technologií koexistovat s 5G zařízeními ve stejném 5G NR kanálu.

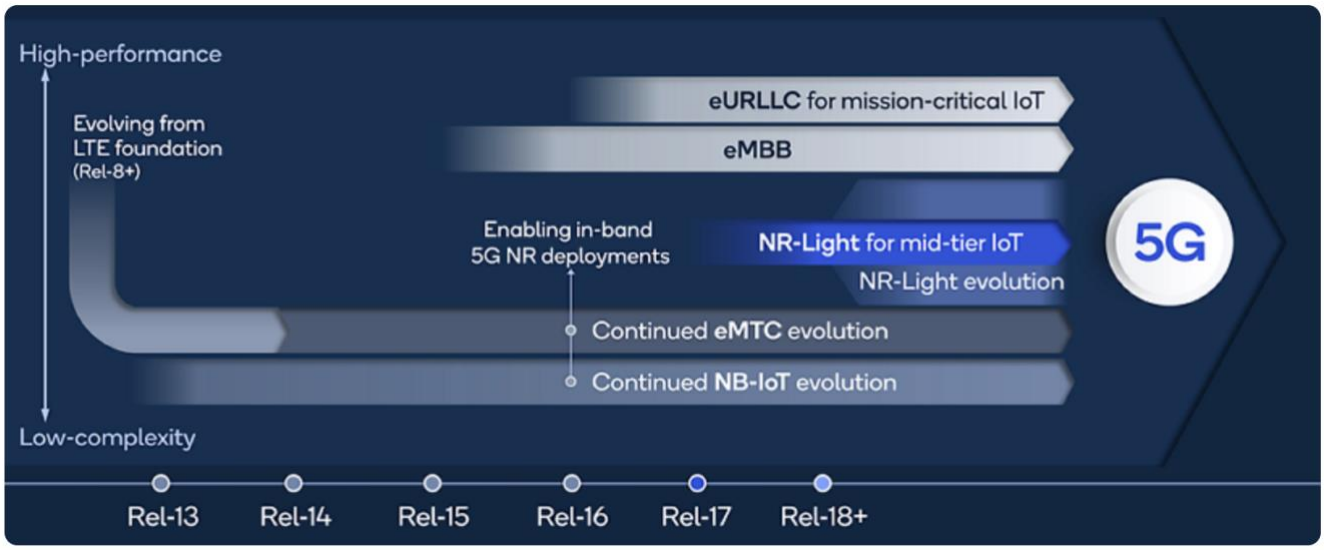
Release 16 také zavedl další úroveň 5G zařízení pro eURLLC, která splňuje přísné požadavky pro mise kritické IoT, s podporou latence v řádu milisekund a 99,9999% spolehlivosti.

[9] "5G NR-Light (RedCap): Revolutionizing IoT | Qualcomm," n.d. https://www.qualcomm.com/news/onq/2022/07/what-is-5g-nr-light--a-k-a--redcap--and-how-will-it-accelerate-t.

NR-Light v 3GPP Release 17 může koexistovat s těmito úrovněmi IoT zařízení a eMBB zařízení ve stejném 5G NR kanálu. Navíc, stejně jako se bude standard 5G NR nadále vyvíjet, NR-Light se plánuje dále rozvíjet v Release 18, se zaměřením na požadavky na polohování a jejich vylepšení.

Komunikace mezi zařízeními prostřednictvím 5G sidelink rozhraní by mohla být další evoluční cestou pro NR-Light v Release 18 a dále.

Tento vývoj rodiny 5G technologií spolu s evolucí původně 4G technologií, názorně zobrazuje následující obrázek.



Obrázek 3: Roadmapa 5G technologií dle 3GPP releasů. Zdroj: [10]

V současnosti se IoT projekty střední třídy spoléhají na technologie LTE Cat-1bis (a částečně LTE Cat-4, která není specificky IoT technologií) pro širokoplošnou bezdrátovou konektivitu a mobilitu. I když se očekává, že LTE sítě budou koexistovat s 5G sítěmi v dohledné budoucnosti, 5G NR-Light může nabídnout novou úroveň schopností, efektivity a flexibility. NR-Light může poskytovat vyšší propustnost, nižší latenci, delší životnost baterie, lepší bezpečnost sítě a optimalizovanou nákladovou strukturu pro takové aplikace. Jak bude evoluce 5G pokračovat, přijde doba, kdy poskytovatelé komunikačních služeb začnou přecházet z 4G na 5G. S ohledem na to se 5G NR-Light bude stávat preferovanou platformou pro zajištění realizace IoT projektů střední třídy (mid-range IoT).

[10] "5G NR-Light (RedCap): Revolutionizing IoT | Qualcomm," n.d. https://www.qualcomm.com/news/onq/2022/07/what-is-5g-nr-light--a-k-a--redcap--and-how-will-it-accelerate-t.

Následující obrázek přináší srovnání parametrů technologií pro mid-range IoT. Těmi jsou LTE Cat 1bis v současnosti a 5G NR-Light do budoucna. Naproti tomu LTE Cat-4 je LTE technologie bez optimalizace pro IoT projekty, pokud jde například o nižší komplexitu a spotřebu energie u koncových zařízení.

	LTE Cat-1bis	LTE Cat-4	5G NR-Light (Rel-17)
Bandwidth	20 MHz	20 MHz	20 MHz (sub-7 GHz)
Peak data rate DL/UL	10/5 Mbps	150/50 Mbps	150/50 Mbps or higher
Duplexing	FD-FDD, TDD	FD-FDD, TDD	HD-FDD, FD-FDD, TDD
Tx/Rx chain	1 Tx, 1 Rx	1 Tx, 2 Rx	1 or 2 Tx, 1 or 2 Rx
MIMO layers DL/UL	1/1	2/1	1 or 2/1
Maximum coupling loss	140 dB	144 dB	140 dB

Obrázek 4: Srovnání parametrů IoT mid-range technologií. Zdroj: [11]

K jakým IoT případům užití se tedy NR-Light (5G RedCap) hodí?

5G NR-Light přináší kombinaci parametrů jako je rychlost datového přenosu, životnosti baterie, a hustoty připojených zařízení, která je potřebná k nákladově efektivnímu zajištění různých případů užití.

Celou řadu uplatnění nalezne v rámci **Smart city**: environmentální senzory, měření spotřeby, ale i kamerové systémy s vysokým rozlišením. Rozhodně je řešením pro **průmysl 4.0**, včetně možnosti využití v rámci **5G privátních sítí**.

NR-Light přináší spolehlivou bezdrátovou konektivitu a bezproblémovou mobilitu. A to při nákladové efektivitě, zejména z pohledu koncových zařízení, což může hrát v ekonomice daného případu užití velkou roli. Příkladem může být náhrada kabeláže, monitoring procesů, chytré kamerové systémy, ale i nositelná zařízení.

Malá velikost zařízení, dlouhá životnost baterie a vysoká propustnost NR-Light zařízení je činí do budoucna zajímavou volbou i pro mnohé mobilní spotřebitelské aplikace (tedy v rámci **Consumer IoT**), jako jsou chytré hodinky, zdravotní monitory, širokopásmový přístup pro základní zařízení jako tablety, brýle pro rozšířenou realitu (AR) apod.

2.3.2 Passive IoT otevírá nové možnosti pro IoT

Technologie Passive IoT/ Pasivní IoT (P-IoT) je spojována s velkými očekáváními. Zejména třetí fáze, neboli P-IoT III, která má být standardizována v rámci 3GPP Release 19 a která propojí P-IoT s celulárními sítěmi.

P-IoT je systém navržený tak, aby řešil omezení tradičních IoT systémů v oblasti spotřeby energie, nákladů a škálovatelnosti. Na rozdíl od aktivních IoT zařízení, která spoléhají na baterie nebo externí zdroje energie, pracují pasivní IoT zařízení tím, že získávají energii ze svého okolí, například z rádiových vln, tepelné energie nebo mechanických vibrací. Tato energie se používá k napájení zařízení, která poté komunikují pomocí technik zpětného rozptylu. To znamená, že odrážejí signály vysílané čtečkou nebo základní stanicí a vkládají svá data do těchto odrazů, která jsou následně dekódována přijímačem.

[11] "5G NR-Light (RedCap): Revolutionizing IoT | Qualcomm," n.d. https://www.qualcomm.com/news/onq/2022/07/what-is-5g-nr-light--a-k-a--redcap--and-how-will-it-accelerate-t.

Fáze Standardizace a nasazení P-IoT

Vývoj Pasivního IoT lze rozdělit do tří hlavních fází:

1. P-IoT I: Tato fáze se vyznačuje architekturou s jediným bodem, která primárně využívá technologii UHF RFID. V tomto nastavení jsou pasivní značky aktivovány RF signálem čtečky a používají zpětný rozptyl k přenosu svých dat zpět do čtečky. Hlavním omezením této fáze je krátká komunikační vzdálenost, obvykle méně než 10 metrů, což ji činí vhodnou pro aplikace, jako je řízení malých skladových zásob.

2. P-IoT II: Tato fáze zavádí síťovou architekturu, kde je RFID systém rozdělen na pomocné zařízení a přijímač. Pomocné zařízení aktivuje pasivní značky, zatímco přijímač sbírá a zpracovává data. Toto rozdělení zlepšuje citlivost systému a prodlužuje komunikační vzdálenost na více než 100 metrů, což umožňuje řízení velkých aktiv a regionální pokrytí.

3. P-IoT III: Poslední fáze zahrnuje integraci s mobilními sítěmi, které využívají rozsáhlou infrastrukturu 5G. Pasivní IoT v této fázi těží z pokročilých schopností mobilních sítí, jako je potlačení interferencí, adaptivní kódování a komunikace na dlouhou vzdálenost. Tato fáze si klade za cíl poskytovat komplexní pokrytí a konektivitu, podporující širokou škálu aplikací napříč odvětvími.

Typické případy užití Passive IoT:

1. Lokální řízení skladů: Pasivní IoT může automatizovat inventarizaci ve skladech, kancelářích a maloobchodních prostředích. Značky umístěné na zboží nebo aktivech jsou čteny strategicky umístěnými přijímači, což umožňuje sledování a řízení v reálném čase. To snižuje náklady a chyby spojené s ruční inventarizací, zvyšuje efektivitu a zlepšuje bezpečnost.

2. Sledování ve velkých oblastech: V tomto scénáři se Pasivní IoT používá ke sledování pohybu osob, vozidel nebo aktiv na velkých plochách. Aplikace zahrnují logistiku, kde se sledování zboží v dodavatelských řetězcích stává plynulým, nebo městskou správu, kde lze efektivně monitorovat a řídit aktiva, jako je dopravní vybavení nebo veřejné bezpečnostní zařízení.

3. Komplexní řízení a správa: Tato kategorie zahrnuje komplexní správu napříč celými procesy nebo dodavatelskými řetězci. Pasivní IoT může sledovat položky od výroby přes logistiku až po konečný prodej, což zajišťuje transparentnost a sledovatelnost. To je zvláště cenné v odvětvích, jako je výroba, logistika chlazeného zboží a správa vysoce hodnotných komodit.

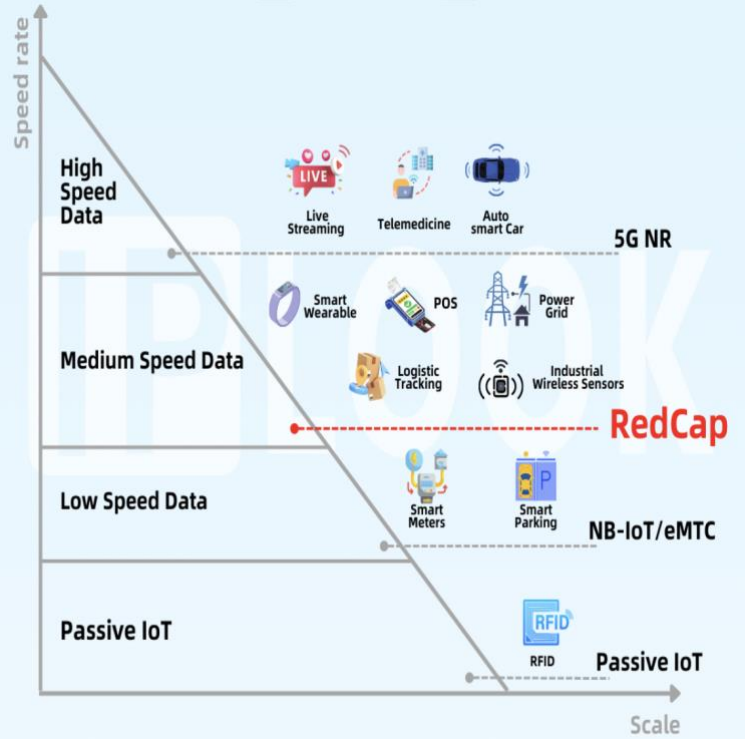
Pozice P-IoT mezi dalšími IoT technologiemi

Pasivní IoT se v rámci dalších IoT technologií profiluje jako ultra-nízkonákladová a snadno implementovatelná technologie s nízkou spotřebou energie. Zatímco tradiční IoT zařízení jsou omezená výdrží baterie a energetickými nároky, Pasivní IoT zařízení mohou být nasazena v masovém měřítku bez potřeby časté údržby nebo doplňování energie.

Ve srovnání s aktivními IoT řešeními je Pasivní IoT vhodnější pro aplikace vyžadující masivní nasazení senzorů nebo značek, kde je energetická účinnost a cena klíčová. Navíc, jak se budou sítě 5G nadále rozšiřovat, integrace Pasivního IoT do těchto sítí umožní nové použití, které vyžaduje rozsáhlé pokrytí a spolehlivou konektivitu, což dále zlepší schopnosti IoT ekosystémů.

Pasivní IoT se stane důležitým prvkem budoucnosti IoT, zejména v scénářích, kde jsou tradiční IoT řešení nepraktická nebo příliš nákladná. Jeho vývoj prostřednictvím fází P-IoT úzce souvisí s rozvojem 5G.

Následující obrázek ukazuje positioning 5G technologií pro IoT a to, pro jaké typy aplikací jsou vhodné:



Obrázek 5: Aplikace 5G technologií v IoT. Zdroj: [12]

2.4 IoT zařízení

2.4.1 Typy a kategorie IoT zařízení

IoT zařízení tvoří klíčovou část každého IoT ekosystému. V obecné rovině se jedná o fyzické objekty vybavené senzory, softwarem a dalšími technologiemi, které jim umožňují připojit se k internetu, vyměňovat si data a komunikovat s jinými zařízeními nebo systémy. IoT zařízení hrají klíčovou roli při sběru dat v reálném čase.

IoT zařízení nejen tvoří percepční vrstvu IoT systému, ale ovlivňují podstatným způsobem všechny ostatní vrsty. Pochopitelně komunikační vrstvu – ta určuje typ použité přenosové technologie a tedy také typ konektivity, který musí být součástí koncových zařízení.

Koncová zařízení ovšem také determinují, jaké informace dokáže IoT systém získávat a ovlivňuje tak také zpracovatelskou vrstvu. Mohou tvořit také podstatnou nákladovou položku a ovlivňují tak obchodní vrstvu IoT sytému.

S příchodem technologie 5G mohou být IoT zařízení výkonnější, ale jsou také nákladnější. Z tohoto pohledu bude pro IoT ekosystém velmi žádoucí příchod 5G verze NR-light.

IoT zařízení v první řadě dělí na senzory a aktuátory (akční členy). Zatímco senzory snímají data ze svého okolí a posílají je dále do systému, aktuátory slouží k ovládání fyzických prvků. Podle toho, zda systém

[12] Iplook. “IPLOOK,” January 5, 2024. https://www.iplook.com/info/redcap-cellular-iot-technology-for-the-5g-era-i00354i1.html.

obsahuje senzory a/nebo aktuátory se dají IoT systémy dělit na jednosměrné nebo interaktivní, viz jejich bližší charakteristika v kapitole 3.1.1.

Existuje ovšem celá řada dalších IoT zařízení. Typicky jde o větší a komplexnější zařízení, jehož součástí je zabudovaný jeden či více senzorů, případně aktuátorů.

Dále jsou charakterizovány ty nejdůležitější a nejrozšířenější kategorie IoT zařízení.

1. Senzory

Senzory shromažďují data z prostředí nebo systému, ve kterém jsou zabudovány. Tato data mohou zahrnovat teplotu, vlhkost, pohyb nebo složitější metriky, jako je vibrace nebo chemické složení.

Senzory fungují jako „oči a uši“ IoT systému. Poskytují kritická vstupní data, která jsou základem pro analytiku, rozhodování a spouštění automatizovaných reakcí.

Příklady: Teplotní senzory, senzory vlhkosti, akcelerometry, senzory kvality vzduchu.

2. Akční členy (Aktuátory)

Akční členy přeměňují elektrické signály na fyzickou akci. Ovládají zařízení, stroje nebo systémy na základě pokynů z IoT systému.

Akční členy jsou „ruce“ IoT systému. Umožňují interakce s reálným světem úpravou fyzických stavů nebo podmínek na základě dat přijatých ze senzorů a zpracovaných centrálními systémy.

Příklady: Elektrické motory, čerpadla, chytré zámky, robotické ramena.

3. Edge zařízení

Edge zařízení provádějí zpracování dat blíže místu, kde jsou data generována, často přímo v zařízení nebo v lokální síti.

Edge zařízení snižují potřebu přenosu velkého množství surových dat do centralizovaných cloudových systémů tím, že provádějí analytiku lokálně, čímž se snižuje zátěž sítě a latence. Jsou zásadní pro aplikace vyžadující rychlé reakční časy nebo offline provoz.

Příklady: Průmyslové brány (gateways), edge servery, chytré kamery.

4. Nositelná zařízení (wearables)

Nositelná zařízení jsou zařízení, která se nosí na těle a shromažďují data týkající se uživatele nebo jeho okolí.

Nositelná zařízení poskytují nepřetržité datové proudy týkající se osobního zdraví, aktivity nebo environmentálních faktorů, což je zásadní pro odvětví, jako je zdravotnictví, fitness a bezpečnost pracovníků.

Příklady: Chytré hodinky, fitness trackery, AR/VR brýle, zdravotní monitory.

5. Připojená spotřebitelská zařízení

Jsou to běžné domácí spotřebiče, které ovšem byly vylepšeny o IoT funkce pro zlepšení uživatelského zážitku, automatizaci nebo nabídku pokročilých funkcí. Může jít například o automatizaci nebo vzdálené ovládání prostředí domácnosti nebo spotřebitelských produktů.

Příklady: Chytré ledničky, chytré reproduktory, domácí bezpečnostní systémy, chytré osvětlení.

6. Průmyslová IoT zařízení (IIoT)

Tato zařízení jsou určena pro použití v průmyslovém prostředí, kde monitorují, řídí a optimalizují stroje a procesy.

Průmyslová IoT zařízení jsou základem Průmyslu 4.0, umožňují chytré továrny, prediktivní údržbu a optimalizaci výrobních procesů v reálném čase.

Příklady: Připojení roboti, průmyslové senzory, automatizované systémy kontroly kvality, průmyslové routery.

7. Vozidla a dopravní zařízení

Tato zařízení zahrnují připojená vozidla, autonomní vozidla a další chytré dopravní systémy. V dopravě hrají IoT zařízení klíčovou roli v zajištění bezpečnosti, umožnění autonomních funkcí, monitorování stavu vozidel nebo zlepšení řízení dopravy.

Příklady: Autonomní vozidla, připojené nákladní vozy, systémy správy vozových parků, chytré semafory.

2.4.2 IoT zařízení a protokoly

IoT zařízení používají pro komunikaci různé protokoly. Ty jsou přizpůsobené potřebám IoT systémů, jako je například nízká energetická náročnost, různé úrovně QoS nebo kritičnosti systému. A také celkově typ komunikace, který není svých charakterem point-to-point, ale zahrnuje velké množství koncových bodů, které odesílají informace do centrálního místa pro zpracování.

Je proto vhodné rozumět principům fungování IoT protokolů a jejich využití. Nejznámější je v současné době MQTT protokol, má však také různé alternativy.

MQTT (Message Queuing Telemetry Transport) je lehký komunikační protokol speciálně navržený pro komunikaci v IoT systémech. Jeho účelem je umožnit efektivní výměnu dat s nízkou latencí mezi zařízeními, často přes nespolehlivé nebo šířkou pásma omezené sítě. MQTT je v IoT široce používán díky své jednoduchosti, nízké režii a schopnosti fungovat v prostředí s přerušovanou konektivitou.

Hlavním účelem MQTT je umožnit komunikaci mezi stroji (M2M). IoT zařízení často potřebují odesílat a přijímat malé datové balíčky, jako jsou například údaje ze senzorů nebo kontrolní příkazy, přes nespolehlivé nebo omezené sítě. Lehký design MQTT umožňuje efektivní zpracování těchto komunikací, minimalizuje spotřebu šířky pásma sítě a výkon zařízení. To je zvláště důležité pro IoT zařízení s omezenými zdroji, která fungují na baterii nebo na sítích s omezenou šířkou pásma, jako jsou mobilní sítě.

MQTT pracuje na modelu publish/subscribe (vydavatel/odběratel), který se liší od tradičních modelů point-to-point, jako je HTTP. Tato architektura je výhodná pro prostředí IoT, protože odděluje producenty zpráv (vydavatele) od konzumentů zpráv (odběratelů), což umožňuje škálovatelnou a flexibilní komunikaci. Funguje to následujícím způsobem:

- Broker (server): Broker je centrem komunikace MQTT. Je zodpovědný za příjem zpráv od vydavatelů a jejich distribuci odběratelům. Broker funguje jako zprostředkovatel, což usnadňuje správu více zařízení v komplexních systémech.

- Vydavatelé (producenti): Zařízení nebo aplikace, která odesílají zprávy brokerovi. Vydavatel nemusí vědět, kdo jsou odběratelé – pouze pošle svá data brokerovi.

- Odběratelé (konzumenti): Zařízení nebo aplikace, které projevují zájem o konkrétní typy zpráv (témata). Odběratel se přihlásí k odběru témat, která ho zajímají, a broker mu doručí relevantní zprávy, jakmile jsou publikovány.

- Témata (Topics): Zprávy jsou brokerovi odesílány v rámci specifických témat (např. `senzory/teplota/obyvak`). Odběratelé se přihlásí k odběru témat, která je zajímají, a broker zajistí, aby dostali pouze relevantní zprávy.

- Úrovně kvality služby (QoS): MQTT podporuje tři úrovně QoS, které zajišťují spolehlivost doručování zpráv:

- QoS 0 (maximálně jednou): Zprávy jsou doručeny jednou bez potvrzení.

- QoS 1 (alespoň jednou): Zprávy jsou doručeny alespoň jednou, přičemž se vyžaduje potvrzení.

- QoS 2 (přesně jednou): Zaručuje, že zprávy budou doručeny přesně jednou, což je nejvyšší úroveň spolehlivosti.

- Uchovávané zprávy: Vydavatelé mohou odesílat uchovávané zprávy, což znamená, že broker uchová poslední zprávu pro budoucí odběratele, kteří se přihlásí později.

- Závěť a poslední projev (LWT): MQTT podporuje možnost informovat odběratele v případě, že zařízení neočekávaně ztratí spojení, tím, že broker odešle předem nastavenou zprávu (LWT).

Vztah mezi MQTT a IP Protokolem

MQTT je aplikační protokol, který spoléhá na podkladové transportní protokoly pro komunikaci. Nejčastěji běží nad TCP/IP, využívajíc TCP pro spolehlivý přenos zpráv. Protože TCP/IP je základem internetové komunikace, MQTT může fungovat na různých typech sítí, jako jsou Ethernet, Wi-Fi, 4G/5G nebo dokonce satelitní komunikace. I když MQTT používá TCP pro spolehlivost, konkrétní transportní vrstva je v MQTT abstraktní. Použití IP protokolu zajišťuje interoperabilitu mezi různými zařízeními a systémy na různých typech sítí.

Pro prostředí, kde může být TCP příliš těžkopádné nebo pomalé, může MQTT běžet také nad jinými transportními vrstvami, jako jsou WebSockets, což umožňuje komunikaci přes HTTP porty.

Měla by tedy IoT zařízení Podporovat MQTT?

Ano, IoT zařízení často těží z podpory MQTT, zejména pokud potřebují komunikovat s jinými zařízeními nebo cloudovými platformami efektivním a lehkým způsobem. Přináší to řadu výhod, zejména:

- Nízká spotřeba energie a šířka pásma: Mnoho IoT zařízení pracuje s omezenou energií (např. na baterii) nebo na sítích s omezenou šířkou pásma (např. 2G, LoRaWAN). MQTT je optimalizováno pro tyto podmínky díky minimální velikosti paketů a nízké režii.

- Oddělená architektura: Model publish/subscribe odděluje zařízení, což umožňuje snadné přidávání nebo odebírání zařízení, aniž by došlo k narušení systému. To je užitečné v dynamickém prostředí, kde zařízení mohou často připojit nebo odpojit ze sítě.

- Spolehlivost a flexibilita: Díky úrovním QoS a funkci Závěti a posledního projevu MQTT zajišťuje spolehlivé doručování zpráv a umožňuje notifikace, pokud zařízení ztratí spojení.

- Škálovatelnost: MQTT podporuje modely komunikace mnoha vydavatelů a mnoha odběratelů, což znamená, že více zařízení může publikovat do stejného tématu a více zařízení se může přihlásit k odběru stejného tématu. To z něj činí vysoce škálovatelný protokol pro velká IoT nasazení, jako jsou chytrá města nebo průmyslové prostředí.

Alternativy k MQTT

I když je MQTT v oblasti IoT velmi populární, existuje několik alternativ, z nichž každá má své výhody v závislosti na konkrétním použití:

- CoAP (Constrained Application Protocol):

- Webový protokol optimalizovaný pro použití v omezených sítích a zařízeních (podobně jako MQTT).

- Používá UDP místo TCP, což je lehčí, ale méně spolehlivé. CoAP se často používá v prostředích, kde je latence kritická, například v senzorových sítích.

- Vhodné pro nízkoenergetická zařízení, ale není tak široce přijímáno jako MQTT.

- AMQP (Advanced Message Queuing Protocol):

- Protokol s více funkcemi ve srovnání s MQTT, s vestavěnou podporou front, směrování, zabezpečení a spolehlivosti.

- AMQP se obvykle používá v podnikovém prostředí, kde je vyžadováno sofistikovanější zpracování zpráv (např. ve finančních službách nebo logistice).

- Je těžší než MQTT, což ho činí méně vhodným pro IoT zařízení s omezenými zdroji.

- HTTP/REST:

- Tradiční webový protokol, který je někdy používán v IoT, zejména pro jednoduchou, jednosměrnou komunikaci (např. odesílání dat do cloudové platformy).

- HTTP je bezstavový, což znamená, že zařízení musí při každém požadavku odesílat kompletní data, což je neefektivní pro nízkoenergetická a nízkopásmová IoT zařízení. Nicméně, je jednoduchý a široce podporovaný.

- DDS (Data Distribution Service):

- DDS je navržen pro systémy v reálném čase, které vyžadují deterministickou, vysoce výkonnou výměnu dat.

2.4.3 Správa IoT zařízení

Ve všech IoT systémech je efektivní správa zařízení zásadní pro zajištění dlouhodobé funkčnosti, bezpečnosti a škálovatelnosti. Správa IoT zařízení zahrnuje soubor procesů, nástrojů a platforem, které umožňují firmám (či jiným uživatelům IoT systémů) na dálku monitorovat, řídit, aktualizovat a zabezpečovat jejich IoT zařízení. Jak sítě IoT rostou v komplexnosti a rozsahu – někdy zahrnují tisíce či miliony zařízení – stává se schopnost centrálně spravovat tato zařízení klíčovou.

Pro potenciální zákazníky IoT systémů je pochopení správy zařízení nezbytné, aby jejich nasazení nebylo jen funkční, ale také bezpečné, efektivní a škálovatelné spolu s růstem jejich podnikání, respektive s růstem IoT systémů. Účelem správy IoT zařízení je zjednodušit dohled a kontrolu rozsáhlých IoT prostředí, což umožňuje podnikům soustředit se na využívání dat a funkcí, které tato zařízení poskytují.

Hlavní činnosti a funkce správy IoT zařízení jsou následující:

- Zprovoznění a konfigurace zařízení.

Když jsou do systému přidávána nová IoT zařízení, musí být správně nakonfigurována pro komunikaci se sítí. Zprovoznění zajišťuje, že zařízení jsou autentizována, připojena a nastavena správně s předdefinovanou konfigurací pro komunikaci.

- Monitorování a diagnostika.

  Průběžné monitorování IoT zařízení je důležité pro zajištění, že fungují podle očekávání. Platformy pro správu zařízení umožňují podnikům v reálném čase sledovat stav a výkon zařízení a diagnostikovat problémy, jako jsou potíže s připojením, nízké úrovně baterie nebo nefunkční senzory.

- Aktualizace firmwaru a softwaru.

  Aktualizace "over-the-air" (OTA) jsou klíčovou součástí správy IoT zařízení. Jak jsou zařízení používána po delší dobu, je nezbytné aktualizovat jejich firmware nebo software pro přidávání nových funkcí, opravy chyb a zajištění bezpečnostních oprav. Správa zařízení zajišťuje, že aktualizace mohou být nasazeny efektivně po celé síti bez nutnosti fyzického přístupu k jednotlivým zařízením.

- Bezpečnost a řízení přístupu.

  Správa bezpečnosti napříč rozsáhlou flotilou IoT zařízení je poměrně náročnou výzvou. Řešení pro správu zařízení zajišťují bezpečnostní konfigurace, včetně nastavení oprávnění, rotace přihlašovacích údajů a zajištění šifrovacích protokolů. Pravidelné aktualizace také pomáhají zmírnit bezpečnostní rizika, jako jsou zranitelnosti a neoprávněný přístup.

- Řízení životního cyklu zařízení.

  Každé IoT zařízení má svůj životní cyklus, od nasazení až po vyřazení z provozu. Platformy pro správu zařízení poskytují nástroje pro sledování zařízení v průběhu jejich životního cyklu, což umožňuje snadnou výměnu nebo vyřazení zařízení, která již nejsou funkční nebo jsou zastaralá. To zajišťuje efektivní provoz a snižuje celkové náklady na údržbu IoT infrastruktury.

  Správa IoT zařízení obvykle funguje prostřednictvím centralizovaných platforem, které poskytují řadu nástrojů pro řízení a monitorování zařízení napříč sítí. Tyto platformy fungují jako most mezi IoT zařízeními (která jsou často geograficky rozptýlená) a centrálním řídicím systémem (obvykle hostovaným v cloudu nebo lokálně).

Příklady řešení pro správu IoT zařízení

Existuje mnoho platforem, které pomáhají podnikům efektivně spravovat jejich IoT zařízení. Některé z významných příkladů jsou uvedeny dále:

- AWS IoT Device Management:

- Součást Amazon Web Services. AWS IoT Device Management nabízí komplexní sadu nástrojů pro registraci, organizaci, monitorování a správu zařízení ve velkém měřítku. Zahrnuje funkce, jako je hromadná registrace, seskupování zařízení a automatizované zprovoznění.

- Klíčové funkce: OTA aktualizace, monitorování zařízení, logování a řešení problémů.

- Microsoft Azure IoT Hub:

- Azure IoT Hub je platforma společnosti Microsoft pro IoT, která nabízí plně vybavenou správu zařízení. Podporuje obousměrnou komunikaci cloud-to-device i device-to-cloud a umožňuje uživatelům monitorovat stav zařízení a bezpečnost.

- Klíčové funkce: Digitální dvojče zařízení (digitální kopie stavu zařízení), integrace s dalšími službami Azure, správa bezpečnosti.

- Google Cloud IoT Core:

- Google Cloud IoT Core nabízí škálovatelné služby pro správu připojených zařízení. Umožňuje zprovoznění, monitorování a aktualizace zařízení a integruje se s analytickými nástroji a strojovým učením společnosti Google.

- Klíčové funkce: Monitorování v reálném čase, bezpečnostní protokoly, integrace s BigQuery a nástroji pro umělou inteligenci.

- Cisco IoT Operations Dashboard:

- Cisco poskytuje řešení pro správu zařízení se zaměřením na bezpečná IoT nasazení v průmyslových odvětvích, jako je výroba, energetika a doprava. Nabízí náhledy v reálném čase, diagnostiku a bezpečnou správu IoT zařízení.

- Klíčové funkce: Prediktivní údržba, detekce anomálií, bezpečné nasazení zařízení.

- Bosch IoT Suite:

- Bosch nabízí kompletní řešení pro správu IoT zařízení v průmyslových prostředích. Poskytuje nástroje pro OTA aktualizace, diagnostiku, dálkový přístup a bezpečnou komunikaci.

- Klíčové Funkce: Zaměření na průmyslový IoT, komplexní monitorování a správa životního cyklu.

Pro potenciální zákazníky je výběr správného řešení pro správu IoT zařízení klíčový pro úspěšné nasazení IoT systému. Dobrá platforma pro správu by měla poskytovat škálovatelnost, bezpečnost, možnost automatizace. Platforma by měla podporovat širokou škálu typů zařízení a komunikačních protokolů (např. MQTT, HTTP, CoAP), aby byla zajištěna flexibilita a kompatibilita s různými hardwarovými a softwarovými prostředími.

Platforma pro správu zařízení může být samostatná, nebo může být součástí celkové IoT platformy, která je popsána v detailu v další kapitole.

2.5 IoT platformy

IoT platforma je komplexní řešení, které poskytuje nezbytné nástroje a infrastrukturu pro připojení, správu a řízení IoT zařízení a datových toků. Slouží jako centrální bod v IoT ekosystému, který umožňuje interakci mezi zařízeními, cloudem, aplikacemi a koncovými uživateli. IoT platformy usnadňují integraci hardwaru, softwaru, analýzy dat a síťové konektivity.

Ve své podstatě fungují IoT platformy jako middleware, tedy vrstva, která propojuje fyzický svět zařízení a senzorů s digitálním světem zpracování a analýzy dat.

Funkce IoT platforem

IoT platformy poskytují širokou škálu funkcí, které umožňují efektivní nasazení a správu IoT systémů. Pro přehlednost je možné rozdělit funkce IoT platformy do 2 hlavních oblastí:

1. Datové služby – pro zpracování, ukládání a analýzu dat.

2. Služby pro správu a řízení IoT zařízení a systémů.

Služby pro správu a řízení

- Připojení a správa zařízení:

- IoT platformy usnadňují připojení zařízení, jejich konfiguraci, autentizaci a monitorování. Umožňují bezpečnou komunikaci mezi zařízeními a cloudem pomocí různých komunikačních protokolů (např. MQTT, HTTP, CoAP).

- Správa zařízení zahrnuje monitorování v reálném čase, diagnostiku, aktualizace softwaru a over-the-air (OTA) aktualizace firmwaru, stejně jako řešení problémů na dálku.

- Automatizace:

- Některé platformy podporují automatizační funkce, jako je nastavení spouštěčů nebo pravidel, která aktivují zařízení na základě určitých podmínek (např. zapnutí topení, pokud teplota klesne pod určitou hranici).

- Bezpečnost:

- Bezpečnost je klíčová v každém IoT systému. IoT platformy poskytují nástroje pro šifrování, bezpečný přenos dat, autentizaci a řízení přístupu, aby byla chráněna integrita jak zařízení, tak datových toků.

Datové služby

- Sběr a zpracování dat:

- Platformy shromažďují data z IoT zařízení (senzory, akční členy) a zajišťují spolehlivý přenos dat do centrálního úložiště nebo analytických služeb.

- Nabízejí také předzpracování dat (např. čištění a agregaci dat) před jejich předáním vyšším aplikacím pro pokročilou analytiku.

- Ukládání dat:

- Shromážděná data z IoT zařízení mohou být uložena v databázích, které jsou často součástí cloudových služeb pro dlouhodobé ukládání, analýzu a vizualizaci.

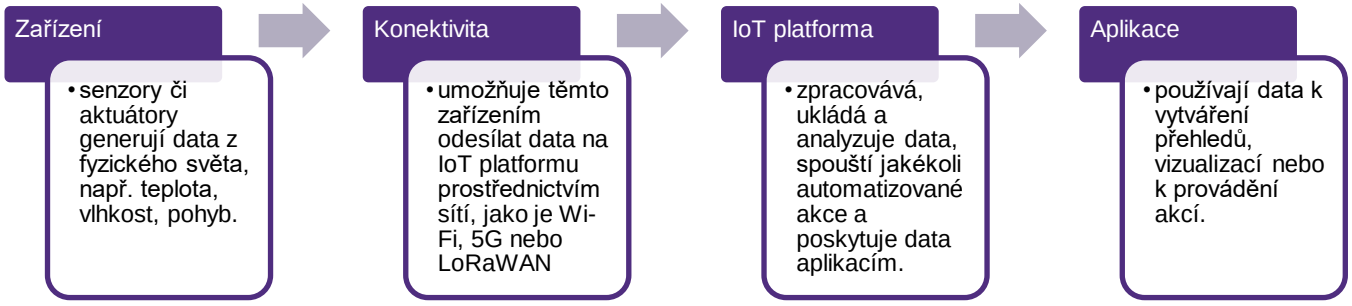
- Analytika a přehledy:

- IoT platformy se často integrují s analytickými nástroji, aby generovaly použitelné přehledy z dat, která shromažďují zařízení. Tato analytika může zahrnovat integraci s algoritmy strojového učení.

- Integrace s aplikacemi třetích stran:

- Mnoho IoT platforem nabízí API (aplikační programovací rozhraní), které umožňuje integraci s externími aplikacemi, podnikovými systémy (např. ERP, CRM) nebo jinými cloudovými službami pro analýzu dat, vizualizaci nebo automatizaci.

IoT platforma je prvkem, které spojuje všechny komponenty IoT systému. Nachází se mezi vrstvou zařízení (senzory, akční členy, brány atd.) připojených komunikační vrstvou a aplikační vrstvou (uživatelská rozhraní, dashboardy, podnikové systémy). IoT platforma řídí komunikaci mezi těmito vrstvami a zajišťuje, aby data plynula hladce a bezpečně ze zařízení do aplikací a zpět. V typickém IoT systému lze tento komunikační proces popsat následujícími kroky:



Obrázek 6: Proces komunikace v rámci IoT systému s IoT platformou. Zdroj: Vlastní zpracování.

Dále jsou uvedeny některé z předních IoT platforem

AWS IoT (detailní popis AWS IoT platformy viz příloha):

- AWS IoT Core je komplexní IoT platforma poskytovaná Amazon Web Services. Nabízí správu zařízení, zpracování dat v reálném čase a pokročilou analytiku. AWS IoT Core se bezproblémově integruje s dalšími službami AWS, jako jsou Lambda (serverless computing) a S3 (datové úložiště).

Microsoft Azure IoT Hub:

- Azure IoT Hub je součástí většího balíčku Azure IoT. Nabízí robustní nástroje pro zprovoznění, monitorování a obousměrnou komunikaci mezi zařízeními a cloudem. Azure IoT Hub se integruje s datovými službami Azure, což umožňuje výkonnou analytiku a schopnosti AI.

Google Cloud IoT Core:

- Google Cloud IoT Core umožňuje bezpečné připojení a správu zařízení ve velkém měřítku. Integruje se s nástroji Google pro velká data a strojové učení, což z něj činí ideální volbu pro firmy, které chtějí aplikovat AI na svá IoT data.

ThingWorx:

- ThingWorx je průmyslová IoT platforma od PTC, která se zaměřuje na rychlý vývoj a nasazení IoT řešení, zejména ve výrobních a průmyslových odvětvích. Nabízí funkce pro správu zařízení, analytiku a rozšířenou realitu (AR).

Bosch IoT Suite:

- Bosch IoT Suite je komplexní IoT platforma navržená pro rozsáhlé podnikové IoT projekty, zejména v průmyslových prostředích. Poskytuje širokou škálu služeb od správy zařízení až po analytiku dat a edge computing.

IoT platformy ovšem vyvíjení a nabízejí české a slovenské firmy. Mezi příklady lokálních IoT platforem patří Heliotics CORE, nebo Multi-tech Cloud společnosti České Radiokomunikace. Bližší informace k této platformě jsou uvedené v příloze 2.

2.6 Mezinárodní IoT pokrytí

Řada případů užití pro IoT systém, a tedy i zákazníků, vyžaduje mezinárodní konektivitu. Může se jednat o požadavek statický, nebo dynamický. V případě statického požadavku jde o izolované řešení, například využití IoT technologií v nemocnici, které chce zákazník replikovat v dalších zemích. Dynamický požadavek je náročnější – předpokládá plynulé (seamless) poskytování služby nejen na celém národním území, ale také napříč hranicemi.

Pro řešení požadavků na mezinárodní konektivitu je tradičně využíván roaming mobilních operátorů. Jde o osvědčený a standardizovaný proces. Je za ním dlouhý technologický vývoj a ekosystém, který kromě samotných operátorů zahrnuje také různé typy brokerů, kteří usnadňují výměnu roamingových dat a jejich vyúčtování, stejně jako technologických firem, které pomáhají s realizací služeb s přidanou hodnotou nebo ošetřením možného fraudu (zneužití služeb).

Kromě řady technologií, standardizací a celého ekosystému vyžaduje vytvoření mezinárodního pokrytí mnoho let úsilí při uzavírání a implementaci roamingových smluv.

Z tohoto důvodu je pro nového mobilního operátora obtížné globální roamingové pokrytí v krátkém čase vybudovat. Řešením je proto využití tzv. roamingových brokerů. Jedná se často o mobilních či integrované operátory, kteří nabízejí řešení na bázi dual (nebo multi) IMSI. IMSI znamená International Mobile Subscriber Identity (Mezinárodní identifikace mobilního účastníka). Je to jedinečný identifikátor, který používají mobilní sítě k identifikaci jednotlivých účastníků. IMSI je uloženo na SIM kartě účastníka a je odesíláno do sítě k ověření a autorizaci přístupu uživatele ke službám sítě, včetně při mezinárodním roamingu. Roamingový broker tedy možní využít své IMSI (identitu) uživatelům svého zákazníka.

Toto řešení (multi-IMSI) je ovšem možné použít nejen pro nového mobilního operátora. Může ho využít také poskytovatel IoT služeb (v roli MVNO) a zajistit tak mezinárodní pokrytí pro své IoT zákazníky.

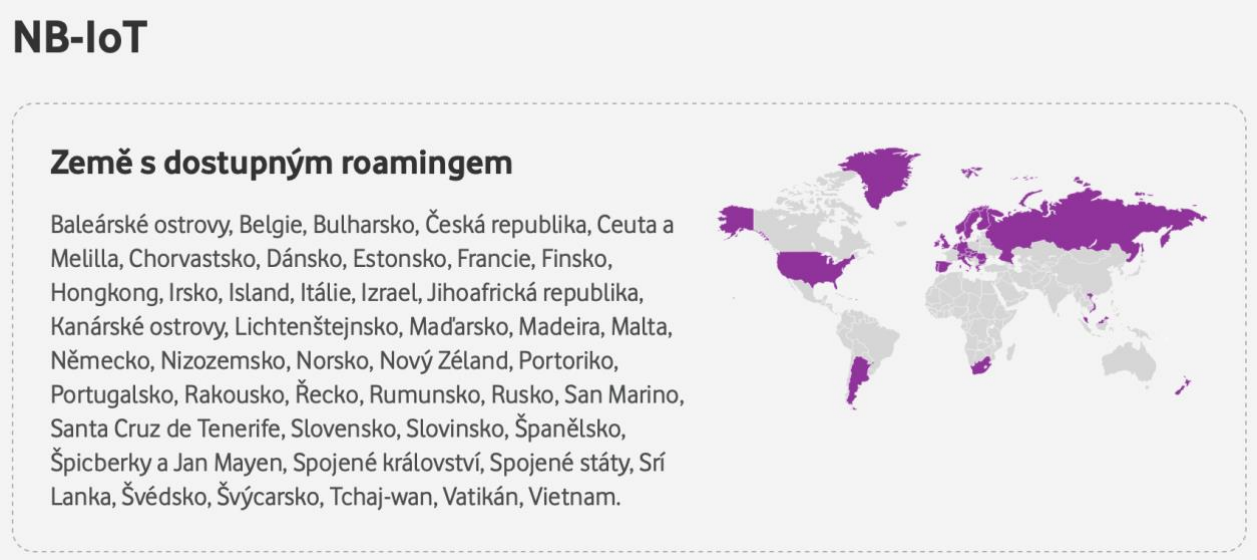
Mezinárodní roaming funguje pro 2G, 3G, 4G i 5G technologie využívané mobilními operátory v souladu s 3GPP standardy.

Jak je to ovšem s přenosovými technologiemi, které jsou specifické pro IoT?

V případě 3GPP ekosystému se jedná především o LPWAN technologie NB-IoT a LTE-M. I pro technologie LTE-M a NB-IoT existuje roamingové řešení a je tedy možné získat mezinárodní pokrytí. Je ovšem zatím výrazně menší než v případě „standardních“ 3GPP technologií. Například společnost emnify uvádí, že pro LTE-M zajišťuje pokrytí v 51 zemích na pěti kontinentech.

Pro NB-IoT je situace ještě složitější. Přestože standardizace technologie proběhla už v roce 2016, její nasazení probíhá pomalu (o tom svědčí ostatně i situace v ČR). Dosud je NB-IoT dostupná jen v cca 1/3 zemí, kde je jinak dostupné pokrytí 3GPP technologiemi. Pro mezinárodní IoT projekty tak například emnify doporučuje použít zařízení, která mohou komunikovat i jiným přístupovými technologiemi, než jen NB-IoT.

Poznámka: Je ovšem potřeba připomenout, že technologie NB-IoT nepodporuje mobilitu, a tedy stejně není vhodná pro případy užití typu mezinárodní doprava apod.



Obrázek 7: NB-IoT pokrytí v roamingu. Zdroj: Vodafone ČR.

Obrázek 8: Cat-M pokrytí v roamingu. Zdroj: Vodafone ČR.

Mimo 3GPP ekosystém jde pak zejména o technologii LoRA. Protože pro technologie krátkého dosahu typu WiFi či Bluetooth nemá smysl mezinárodní pokrytí řešit.

Síť LoRa pro internet věcí také dokáže realizovat mezinárodní roaming. O jeho standardizaci a rozšíření se stará LoRa Alliance. Oproti 3GPP technologiím jde ovšem o pokrytí zatím skromnější. Například LoRa provozovaná Českými Radiokomunikacemi umí mezinárodní roaming. Je k dispozici ve 26 zemích v rámci LoRa Alliance a týká se to i satelitu.

Řešení založené na mezinárodním roamingu má určité výzvy a limitace pro IoT:

- Restrikce permanentního roamingu: v některých zemích a některými operátory je omezen permanentní roaming. To znamená, že není možné roamingovou službu využívat nepřetržitě déle než stanovenou dobu (typicky 60 až 90 dnů). Pro některé IoT případy užití to problém není – například sledování vozidel v zahraničí. Ale znamená to, že na bázi roamingu není možné realizovat IoT případy užití s trvalým místem realizace v zahraničí.

- Datová suverenita: některé země vyžadují, aby data (v rámci IoT případů užití) neopustila jejich teritorium. To může být v rozporu s některými typy roamingových řešení.

- Komerční podmínky: velkoobchodní podmínky spojené s roamingem mohou být natolik nevýhodné, zejména při dlouhodobém roamingu, že se IoT služby nevyplatí poskytovat.

Řešení, jak omezení vyplývající z roamingu překonat, jsou:

Přímá dohoda s lokálním mobilním operátorem. IoT poskytovatel pak využije IMSI místního operátora v rámci multi-IMSi řešení. Získat takové dohody ovšem není snadné a je to tedy cesta schůdná spíše pro velké IoT poskytovatele, jako je například Wireless Logic či KORE.

Vylepšením multi-IMSI je pak řešení na bázi eUICC. Vestavěná univerzální integrovaná obvodová karta (eUICC) je programovatelná technologie SIM (Subscriber Identity Module), která umožňuje změnu profilu uživatele u mobilního operátora (MNO) zařízení bez nutnosti měnit fyzický čip. Tam, kde roaming není možný, tato schopnost otevírá takové trhy pro globální IoT společnosti mnohem jednodušším způsobem než fyzickou výměnou hardwaru v jejich zařízeních. Protože eUICC je přeprogramovatelná, může v paměti typu flash současně hostit několik profilů MNO. Proces změny profilů také zahrnuje software pro vzdálené nastavení SIM karty (RSP - Remote SIM Provisioning). Hardware eUICC spolupracuje s RSP na provedení procesu změny profilů. Nicméně, v jeden okamžik může být aktivní pouze jeden profil a proces přepínání mezi sítěmi může stále vyžadovat značný čas a zdroje.

Další možností je pak vybudování lokální prezence (PoP), případně založení lokálního MVNO. To jsou ovšem řešení značně nákladná. Z pohledu firem, které chtějí realizovat své IoT projekty v globálním prostoru, je tedy důležitá informace, že je možné zajistit mezinárodní IoT pokrytí. Jeho rozsah, omezení a komerční podmínky jsou ovšem do velké míry závislé na typu zvolené IoT technologie a poskytovateli připojení.

Je proto důležité věnovat velkou pozornost tomu, zda má IoT projekt mezinárodní přesah. Pokud ano, je to jeden z podstatných faktorů výběru IoT technologie. Případně může jít právě z důvodů mezinárodního dosahu o potřebu využít více IoT technologií. A s tím je potřeba počítat také při volbě koncových zařízení. V neposlední řadě je vhodné zvážit různé poskytovatele globální IoT konektivity. Může se jednat o mobilní operátory, ale také o specializované společnosti, které poskytují globální IoT konektivitu v režimu MVNO (virtuálních operátorů). Kromě již zmíněných příkladů Wireless Logic a KORE je v příloze 3 v detailu popsána platforma Conexa jako možné řešení požadavku na mezinárodní konektivitu.

3 K čemu je možné IoT využít

3.1 Typy případů užití a IoT systémů.

3.1.1 IoT případy užití a systémy dle interaktivity

Pro popis různých možností využití IoT systémů je důležité IoT systémy kategorizovat. Různé typy IoT totiž nabízí velmi odlišné způsoby využití.

Důležitým členěním IoT z pohledu využití (a tedy různých use cases – případů užití) je členění v závislosti na tom, zda IoT systém umožňuje pouze jednosměrný tok informací, které jsou zpracovávány a vyhodnocovány, nebo obousměrný tok, který umožňuje přímo v rámci IoT systému řídit určité procesy a tedy je i automatizovat.

V prvním případě jsou jako koncové zařízení využity senzory, v druhém případě aktuátory.

Členění IoT na kategorie dle směru/interaktivity komunikace (jednosměrný/ obousměrný systém), přináší 2 základní způsoby využití IoT systémů:[13]

- Informace a analýza
- Automatizace a řízení

Tyto 2 kategorie IoT se tedy liší tím, že první kategorie (Informace a analýza) využívá jednosměrnou komunikaci s využitím senzorů jako koncových bodů, zatímco druhá kategorie využívá obousměrnou komunikaci a koncové body v podobě aktuátorů. Díky tomu může tento obousměrný IoT systém realizovat akce. Pro tyto dvě kategorie IoT jsou pak identifikovány 3 typy aplikací.

Informace a analýza	**Automatizace a řízení**
1. Sledování chování	**1. Optimalizace procesů**
Monitorování chování osob, věcí nebo dat v prostoru a čase.	Automatizované řízení uzavřených (samostatných) systémů
Příklady: Senzory sledující opotřebení materiálů v letadlech. Sledování zásob a dodavatelského řetězce, např. s využitím RFID.	Příklady: Maximalizace průchodnosti vápenné pece pomocí bezdrátových senzorů. Nepřetržité, přesné úpravy ve výrobních linkách.
2. Zlepšené situační povědomí	**2. Optimalizovaná spotřeba zdrojů**

[13] Chui, Michael, Markus Löffler, and Roger Roberts. “The Internet of Things.” McKinsey & Company, March 1, 2010. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-internet-of-things#/.

Dosahování reálného časového povědomí o fyzickém prostředí.	Řízení spotřeby pro optimalizaci využití zdrojů v síti
Příklad: Přehled o stavu zabezpečení areálu.	Příklady: Inteligentní měřiče a energetické sítě, které přizpůsobují zátěže a výrobní kapacitu ke snížení nákladů. Správa datových center pro optimalizaci využití energie, úložiště a procesoru.
3. Analytika rozhodování na základě senzorů	**3. Komplexní autonomní systémy**
Pomáhání při rozhodování prostřednictvím hluboké analýzy a vizualizace dat	Automatizované řízení v otevřených prostředích s velkou nejistotou
Příklady: Plánování ropných polí s 3D vizualizací a simulací Nepřetržité monitorování chronických onemocnění, které pomáhá lékařům určit nejlepší léčbu	Příklady: Systémy pro předcházení kolizím, které snímají objekty a automaticky aplikují brzdy. Úklid nebezpečných materiálů pomocí robotů.

3.1.2 Požadavky případů užití na parametry IoT technologie

Různé IoT případy užití mají velmi odlišné požadavky. Některé vyžadují přenos velkého množství dat v reálním čase pro další zpracování, například s pomocí analytických nástrojů posílených o AI. Jiné naopak přenos velmi malých dat, ale za to je nutné, aby zařízení vydržela celé roky v provozu na baterii bez možnosti připojení k elektrické síti. Některé případy užití jsou business kritické a případný výpadek by měl dalekosáhlé dopady pro uživatele IoT systému, pro jiné případy užití je zase klíčová nízká cena celého řešení. A tak by bylo možné dlouho pokračovat. V rámci širokého pojmu IoT se nacházejí řešení, která mají prakticky o 180 stupňů odlišné požadavky na technické řešení a pro realizaci tedy vyžadují mimo jiné odlišnou komunikační technologii. V málokteré oblasti bychom nalezli tak vysokou diverzitu požadavků jako v IoT.

Je proto klíčové požadavky správně definovat na začátku projektu. Ve výsledku vedou požadavky daného případu užití k volbě vhodné technologie.

Přes velkou různorodost požadavků jednotlivých IoT případů užití je možné rámcově kategorizovat IoT systémy do 3 odlišných skupiny, jak bylo definováno již v kapitole 2:

1. Mission/business critical IoT (kritické IoT)

2. Mid-range IoT (IoT střední třídy)

3. Massive IoT (masivní IoT)

Pro rámcové určení vhodného typu IoT technologie pro danou kategorii IoT můžeme použít tabulku, která ukazuje vhodnost jednotlivých technologií pro Critical, Mid-range a Massive IoT:

IoT technologie	Critical IoT	Mid-Range IoT	Massive IoT
GPRS		✓	

4G/5G	✓	✓	
NB-IoT			✓
Cat-M		✓	✓
LTE Cat 1 bis		✓	
RedCap		✓	
5G Passive IoT		✓	✓
LoRa			✓
ZigBee		✓	✓
Bluetooth		✓	✓
WiFi		✓	

Přesnější výsledek ovšem získáme, pokud se podíváme v detailu na klíčové požadavky IoT případů užití na parametry IoT technologie:

Požadavek případu užití	Definice požadavku
Přenosová rychlost	Je nutné definovat požadovanou rychlost přenosu v uplinku i downlinku, ovšem také typickou či maximální velikost datových paketů.
Směr a frekvence komunikace	Je pro náš případ užití důležitá rovnocenná obousměrná komunikace, nebo jde typicky o jednosměrný sběr dat. Jaká je potřebná frekvence komunikace s koncovými zařízeními?
Latence	Vyžaduje náš případ užití specificky nízkou latenci, nebo latence prakticky nehraje roli (jako například u odečtů energií)?
Podpora mobility	Zahrnuje náš případ užití pohybující se koncové zařízení…a pokud ano, v jakém perimetru? Nebo budou koncová zařízení naopak staticky umístěna?
Perimetr	Na jakém území má náš IoT případ užití fungovat – jde o lokální řešení, například ve výrobní hale či nemocnici? Nebo potřebuje pokrytí na území celé České republiky?

	Nebo má náš případ užití fungovat v zahraničí, ve vybraných zemích nebo dokonce globálně? A pokud v zahraničí, jde o statické fungování, nebo potřebujeme kontinuální připojení pohybujícího se zařízení?
Spotřeba energie	Vyžaduje náš případ užití velmi nízkou nebo nízkou spotřebu energie ze strany koncových zařízení, protože je není možné připojit k napájení? Nebo budou koncová zařízení připojená k napájení a spotřeba tedy nehraje podstatnou roli?
Kritičnost systému	Představuje případ užití business/mission kritickou komunikaci? Pokud ano, jaké jsou požadované parametry pro service level?
Kybernetická bezpečnost	Má daný případ užití vysoké nároky na kybernetickou bezpečnost, dané jeho povahou, standardy firmy, nebo přímo regulačními požadavky?
Nákladovost	Případ užití může být realizován jen pokud má funkční business model. V tom hrají podstatnou roli náklady. Vyžaduje daný případ užití nízkonákladovou technologii, nebo to není rozhodující faktor?

Pokud definujeme požadavky na IoT případ užití dle výše uvedené struktury/formuláře, můžeme tyto požadavky srovnat s parametry jednotlivých IoT technologií uvedených v kapitole 2.2 (IoT technologie) a vyjde nám nejvhodnější IoT technologie pro náš případ užití. Ať už jedna, nebo užší výběr možností k další analýze.

Tabulka níže ilustruje příklady případů užití, které jsou vhodné či naopak nevhodné pro dané IoT technologie.

Technologie pro IoT	Vhodné typy případů užití (use cases)	Nevhodné typy užití (use cases)
GPRS	Základní sledování vozidel, SMS notifikace, jednoduché M2M aplikace.	Přenosy velkých objemů dat, aplikace vyžadující nízkou latenci (např. real-time videostreaming).
4G/5G	Průmyslová automatizace, autonomní vozidla, chytrá města, real-time videostreaming.	Dlouhá životnost baterie u statických senzorů, velmi nízká rychlost přenosu dat.
NB-IoT	Chytré měření (smart metering), sledování životního prostředí, senzory kvality ovzduší.	Aplikace vyžadující vysokou přenosovou rychlost, aplikace s potřebou real-time komunikace a obousměrné komunikace. Mobilní případy užití.
LTE-M	Sledování zásilek, mobilní zdravotní zařízení, chytré hodinky, wearables.	Přenosy velkých objemů dat, aplikace vyžadující velmi nízkou latenci (např. autonomní řízení)
LTE Cat 1 bis	Městské dohledové kamery, hlasové služby v IoT zařízeních, telematika.	Aplikace s velmi nízkou spotřebou energie, velmi dlouhá životnost baterie.
RedCap	Průmyslové IoT aplikace, zdravotnická zařízení, bezpečnostní systémy.	Aplikace vyžadující extrémně nízkou spotřebu energie, statické senzory s nízkou frekvencí přenosu.

5G Passive IoT	Pasivní senzory ve skladech, sledování zásilek, chytré obaly.	Aplikace vyžadující vysokou přenosovou rychlost, mobilní aplikace s vysokou mobilitou.
LoRa	Chytré zemědělství, monitorování prostředí, sledování vodoměrů.	Aplikace vyžadující vysokou přenosovou rychlost, aplikace s potřebou nízké latence.
ZigBee	Domácí automatizace, chytré osvětlení, monitorování zdravotního stavu na krátkou vzdálenost.	Přenosy na dlouhé vzdálenosti, aplikace vyžadující vysokou rychlost dat.
Bluetooth	Wearables, přenos souborů na krátké vzdálenosti, lokalizační služby uvnitř budov	Aplikace s dlouhým dosahem, aplikace vyžadující vysokou bezpečnost přenosu dat.
WiFi	Chytré domácnosti, videostreaming, IoT zařízení v domácím prostředí	Aplikace vyžadující dlouhou životnost baterie, případy užití mimo omezený perimetr, s vysokým požadavkem na bezpečnost.

3.1.3 IoT systémy dle oblasti využití.

Kategorizace podle oblasti využití je dobře uchopitelná a používá se proto také v různých studiích a reportech o IoT trhu, jeho velikosti a dynamice.

Prakticky jde o členění založené na jednotlivých vertikálách. S tím, že jsou zdůrazněny vertikály, které mají klíčový podíl na IoT trhu. To je zejména:

- **Průmysl** – často se hovoří o tzv. industry IoT. Mezi známé případy užití patří prediktivní údržba. Moderní Industry IoT zahrnující pokročilou analytiku a cloudové technologie postupně transformuje tradiční uzavřené a proprietární SCADA systémy.

- **Automotive** – součást průmyslu, ale v IoT hraje tak velkou roli, že je často reportován samostatně. Zahrnuje například fleet management, připojený infotainment, prediktivní údržbu, V2X komunikaci a podporu autonomního řízení, nouzové připojení v případě nehody atd.

- **Zdravotnictví** – zahrnuje zejména monitoring pacientů, ať už lokálně v rámci zdravotních zařízení, nebo vzdálený monitoring.

- **Finance** – řadí se sem pojišťovací telematika, například pojištění založené na užívání, ale také připojené bankomaty.

- **Energetika** – zahrnuje sledování spotřeby energií. A také aktivní opatření na sledování navázané.

- **Vládní sektor a municipality** – patří sem zejména široká oblast smart city, ve kterém existuje široká škála případů užití od monitoringu životního prostředí přes řízení dopravy, energetický monitoring až po odpadové hospodářství.

- **Ostatní vertikály** – IoT najde využití prakticky v každé představitelné vertikále. Byť z hlediska objemu počtu zařízení či výnosů nemusí zatím patřit k největším. K ostatním vertikálám s velkým potenciálem patří zemědělství, doprava a logistika nebo retail.

K vertikálám je pak přiřazena oblast IoT pro koncové spotřebitele (consumer IoT). Tato oblast zahrnuje zejména wearables (nositelnou elektroniku), inteligentní domácnosti, připojené kamery či televizory.

Samotné členění IoT systémů podle oblastí užití/ vertikál nedeterminuje použitou IoT technologii a typ IoT systému (jednosměrný/obousměrný). Například LTE-M technologie může být stejně úspěšně využita pro monitoring v energetice, ve zdravotnictví, nebo v oblasti smart city.

3.2 Případy užití IoT

Dále jsou uvedeny vybrané IoT případy užití v jednotlivých vertikálách.

Případy užití jsou vybrané zejména s potenciálem využití 5G technologií při jejich realizaci. To ovšem neznamená, že by zde uvedené případy užití nemohly být v některých případech realizovány i s využitím jiných než 5G technologií – vždy záleží na konkrétních požadavcích daného případu užití.

Řada případů užití typu IoT je současně případem užití pro digitalizaci podniků s využitím 5G technologie, které byly uvedeny ve studii „**Využívání 5G a jiných sítí elektronických komunikací pro potřeby digitalizace podniků včetně využití moderních informačních systémů.“** Je to logický překryv, protože nemalá část digitalizace firem je spojena právě s IoT technologiemi. Kromě toho pochopitelně existují případy užití digitalizace s 5G, které charakter IoT nemají, protože jsou spojené s komunikací iniciovanou lidmi – například skupinová komunikace, nebo využití AR (rozšířené reality) pro vzdálenou asistenci či trénink pracovníků. A naopak samozřejmě existuje řada případů užití IoT, které nesouvisí s digitalizací podniků. V první řadě takové, jejichž subjektem nejsou podniky ale například orgány státní správy a samosprávy, nebo koncoví uživatelé (consumer IoT).

Některé IoT případy užití bude velmi vhodné a efektivní řešit s využitím 5G technologie Network Slicing (plátkování). Tyto případy jsou uvedené ve studii „**Využití systému plátkování 5G sítí pro veřejné a neveřejné sítě”.** V této studii je také možné najít přednosti a výzvy spojené s využitím Network Slicingu, které jsou tedy relevantní také pro oblast IoT.

U jednotlivých případů užití je uvedeno, na jakém perimetru má být IoT systém realizován. Tedy zda je o lokální případ s jasným ohraničením (například továrna, nemocnice, město), nebo případ užití vyžaduje celonárodní pokrytí (například vnitrostátní doprava, služby poskytované v rámci ČR), nebo případ užití vyžaduje dokonce mezinárodní pokrytí (například trackování zásilek či připojení vozidel).

Dále je uvedeno, do jaké ze 3 kategorií IoT daný případ užití spadá svými požadavky na kritičnost, spolehlivost a další parametry. Tedy zda jde o Critical IoT, Mid-range IoT, nebo Massive IoT. Jde o rámcové zařazení. Pokud bychom chtěli vybrat ideální IoT technologii pro daný případ užití, museli bychom definovat požadavky na všechny klíčové parametry – jak je uvedeno v kapitole 3.1.2.

3.2.1 Průmysl a výroba (Industry IoT)

Průmyslový Internet věcí (IIoT) představuje zásadní posun v tom, jak průmyslové odvětví funguje, propojuje stroje, senzory a systémy za účelem zvýšení efektivity, produktivity a bezpečnosti. Integrací pokročilé datové analýzy, monitorování v reálném čase a automatizace umožňuje IIoT organizacím optimalizovat procesy, minimalizovat prostoje a přijímat rozhodnutí založená na datech. Od prediktivní údržby a chytré výroby po optimalizaci dodavatelského řetězce a řízení energií, příklady použití IIoT ukazují obrovský potenciál propojených technologií v revoluci průmyslových operací napříč různými sektory. Následující příklady poskytují pohled na praktické případy užití IIoT.

Název UC	Popis	Perimetr	Kategorie IoT
Lonely worker protection	Ochrana pracovníků v případě ztráty vědomí, pádu apod. Využívá senzory koncového zařízení a lokalizaci. Člověk je tedy součástí systému, ale komunikace probíhá bez jeho aktivní interakce (proto patří do IoT)	Lokální/ národní	Cricital
Připojené nástroje	Nejen pracovníci, ale přímo jejich ruční nástroje mohou být připojené pro zvýšení efektivity práce. Kromě diagnosticky je možné využít také pro zjišťování polohy nářadí.	Lokální	Mid-range
Kontrola kvality výstupů z výroby	Tento případ použití využívá kamery s podporou 5G a systémy počítačového vidění (machine vision) pro kontrolu v reálném čase a detekci chyb ve výrobních procesech. Vysoká šířka pásma a nízká latence 5G umožňují rychlé zpracování vizuálních dat a identifikaci vad nebo nesrovnalostí na výrobní lince. V rámci řešení bývá využita analýza obrazu s AI.	Lokální	Mid-range
Prediktivní údržba (monitoring strojů)	Automatizované sledování stavu aktiv (strojů) umožňuje výrobcům optimalizovat údržbu a zajistit, aby nedocházelo k prostojům z důvodu nedostatečné údržby. Sníží se také spotřeba náhradních dílů a omezí zbytečná rutinní práce zaměstnanců. Neplánované prostoje jsou pro výrobce jednou z největších překážek dosažení maximální produktivity. Studie ukázaly, že neplánované prostoje stojí průmyslové výrobce každoročně přibližně 50 miliard USD, přičemž příčinou 42 % těchto prostojů jsou poruchy zařízení.	Lokální	Mid-range
Provoz AMR (autonomous mobile robots)/ AGV	5G usnadňuje provoz AMR (Autonomous Mobile Robots) ve výrobních zařízeních. Tyto roboty mohou efektivně a bezpečně přepravovat materiály a přizpůsobovat se měnícím se dispozicím a provozním potřebám. Využití (privátní) 5G konektivity je obzvlášť přínosné při přenosu dat za kamer AMR pro jejich zpracování pomocí edge computingu. A také při potřebě teleoperace AMR.	Lokální	Critical
Bezpečnost areálu a pracovníků ve výrobě	Zvyšování bezpečnosti je často realizováno využitím kamerového systému s vysokým rozlišením spolu s AI analytikou, která zjistí nežádoucí jevy (chybějící ochranné pomůcky, výskyt v zakázané zóně apod.) Další možností je zajištění vyšší bezpečnosti pomocí řešení bránícím kolizím mezi zaměstnanci a roboty, díky využití senzorů apod.	Lokální	Critical
Kolaborativní roboti (cobots)	Kolaborativní roboty neboli koboty pracují po boku operátorů a provádějí výrobní úkoly, jako jsou provozní práce, vrtání nebo montáž, a také automatické kontroly kvality výrobků, které jsou ještě na výrobní lince. Tímto způsobem lze automaticky kontrolovat všechny díly, nejen vzorky. Díky cobotům mohou továrny dosáhnout kontroly každého dílu, aniž by se prodloužila doba potřebná k jejímu provedení, což zvyšuje celkovou kvalitu a spokojenost zákazníků.	Lokální	Critical
Digital twins ve výrobě	Efektivní využití digitálního dvojčete vyžaduje zpracování a správu obrovského množství dat. A to jak při vytváření, tak při provozování digitálního dvojčete. Senzory zabudované ve strojích přenášejí údaje o výkonu do digitálního dvojčete v reálném čase. Využití je pro modelování efektivních výrobních postupů, konfigurace výrobních linek apod., ale také pro plány servisu a snížení nákladů na údržbu.	Lokální	Mid-range

Přenos datových souborů do strojů či produktů ve výrobě	V rámci výrobního procesu je potřeba přenášet datové soubory - s vysokou spolehlivostí a s vysokou rychlostí. Může se jednat o soubory s výrobním programem pro jednotlivé stroje, nebo také o firmware, který má být nahraný do produktů na výrobní lince - příkladem jsou vozidla v oblasti automotive.	Lokální	Mid-range

3.2.2 Automotive (Automobilový průmysl)

Automobilový průmysl je dynamické a technologicky zaměřené odvětví, které zahrnuje návrh, vývoj, výrobu, marketing a prodej motorových vozidel. Jde sice v principu o součást průmyslu, ale jde o odvětví natolik významné, a to i z pohledu IoT a poměrně unikátních a specifických IoT případů užití, že dává smysl představit IoT případy užití v automotive samostatně.

Tato vertikála zahrnuje nejen osobní automobily, ale také komerční vozidla, motocykly a výrobu náhradních dílů. Automobilový průmysl je na špičce technologických inovací, což je spojené s pokroky v autonomním řízení, elektrických vozidlech a technologiích propojených automobilů. Rostoucí poptávka spotřebitelů po vyšší bezpečnosti, efektivitě a pohodlí vedla k integraci sofistikované elektroniky a technologií IoT do vozidel. Tento vývoj přeměňuje vozidla na komplexní, propojené systémy. Do budoucna je možné očekávat posun komunikace vozidel mezi sebou a s externí infrastrukturou, čímž se otevírá cesta pro chytřejší, bezpečnější a efektivnější dopravu.

Automotive IoT umožňuje výměnu dat v reálném čase mezi vozidly, infrastrukturou a řidiči, což vede ke zvýšení bezpečnosti, efektivity a uživatelského zážitku. Od správy vozového parku a propojených infotainment systémů po komunikaci mezi vozidly (V2X) a automatizovanou reakci na nouzové situace, aplikace IoT mění automobilový průmysl.

Název UC	Popis	Perimetr	Kategorie IoT
Fleet management (správa vozového parku)	IoT systémy pro správu vozového parku využívají GPS sledování, telematiku a analýzu dat v reálném čase k monitorování polohy vozidel, optimalizaci tras a řízení spotřeby paliva. Tím se zvyšuje provozní efektivita, snižují náklady a zlepšuje bezpečnost díky dodržování údržby a sledování chování řidičů.	Mezinárodní	Mid-range
Připojený infotainment	Připojené infotainment systémy poskytují cestujícím přístup k zábavě, navigaci a komunikačním službám prostřednictvím integrovaných displejů ve vozidle. Tyto systémy využívají IoT k připojení k internetu, což umožňuje aktualizace v reálném čase, streamování služeb a integraci se smartphony, čímž zlepšují zážitek v autě.	Mezinárodní	Mid-range
Komunikace mezi vozidly (V2X)	V2X komunikace umožňuje vozidlům komunikovat mezi sebou (V2V), s infrastrukturou (V2I), s chodci (V2P) a sítěmi (V2N). Tato technologie zvyšuje bezpečnost na silnicích tím, že vozidla sdílejí informace o podmínkách na silnici, dopravě a možných nebezpečích, což usnadňuje chytřejší rozhodování a vyhýbání se kolizím.	Mezinárodní	Critical

Nouzové volání v případě nehody (eCall)	Systémy eCall automaticky iniciují nouzové volání na místní záchranné služby v případě vážné nehody. Systém poskytuje důležité informace, jako je poloha vozidla, čas nehody a detaily vozidla, což snižuje dobu odezvy a potenciálně zachraňuje životy.	Mezinárodní	Critical
Vzdálená diagnostika a prediktivní údržba vozidel	Nástroje pro dálkovou diagnostiku využívají IoT senzory ke sledování stavu a výkonu vozidel v reálném čase. Data z různých senzorů mohou být analyzována pro diagnostiku problémů dříve, než se stanou vážnými, což umožňuje včasnou údržbu a opravy a zvyšuje spolehlivost a bezpečnost vozidel. Prediktivní údržba upozorňuje řidiče nebo správce vozového parku na potřeby servisu, což snižuje neočekávané poruchy, minimalizuje prostoje a prodlužuje životnost vozidla.	Mezinárodní	Mid-range
Vzdálená aktualizace SW ve vozidlech (OTA)	OTA(Over-the-air) aktualizace umožňují výrobcům vozidel vzdáleně aktualizovat software v automobilových systémech. Nejen infotainmentu a navigaci, ale také bezpečnostních funkcí nebo funkcí autonomního řízení. To snižuje potřebu fyzických svolávacích akcí a zajišťuje, že vozidla zůstávají aktuální s nejnovějšími funkcemi a bezpečnostními záplatami.	Mezinárodní	Mid-range

3.2.3 Zdravotnictví

Integrace IoT ve zdravotnictví podstatně mění způsob, jakým je péče o pacienty poskytována a řízena. Díky možnosti sběru dat v reálném čase, vzdálenému monitorování a automatizovaným procesům IoT ve zdravotnictví zlepšuje výsledky pacientů, zvyšuje provozní efektivitu a snižuje náklady. IoT zařízení a systémy transformují vše od správy chronických onemocnění a provozu nemocnic až po personalizovanou péči a pohotovostní zásahy. Tyto technologie poskytují poskytovatelům zdravotní péče cenné informace, které jim umožňují činit informovaná rozhodnutí, poskytovat včasné intervence a nakonec zlepšovat kvalitu péče. Následující příklady ukazují způsoby, jakými je IoT aplikováno ve zdravotnictví.

Název UC	Popis	Perimetr	Kategorie IoT
Monitoring pacientů pomocí wearables a dalších zařízení	Vzdálené monitorování pacientů je považováno za klíčový faktor pro efektivnější a proaktivnější poskytování zdravotnických služeb a řízení chronických onemocnění. Pomocí senzorů, nositelných zařízení a zařízení elektronického zdravotnictví lze shromažďovat a analyzovat atributy pacientů, aniž by pacienti museli cestovat do zařízení primární péče a mít osobní schůzku s lékařem.	Národní/ Mezinárodní	Mid-range
Connected ambulance	Připojená sanitka a její posádka fungují jako prostředek ke shromažďování a přenosu informací o pacientovi, ať už prostřednictvím nositelných zařízení, senzorů nebo streamování HD video/tělesných kamer, zpět do nemocniční pohotovosti, zatímco je pacient převážen. Nemocniční personál tak lépe porozumí pacientovi před jeho příjezdem. Pro tento případ užití je ideálním řešením network slicing.	Národní	Critical

Monitoring chování pacientů v zařízení pomocí video analýzy.	V nemocnicích, pečovatelských domech, psychiatrických centrech atd. lze videoanalytiku použít na chodbách k identifikaci pacientů, kteří se chovají nestandardně, měli incident, jako je pád, nebo se stávají nebezpečím pro sebe nebo pro ostatní. Hostování analytiky na zařízení pomocí chytrých kamer může vést k neúměrně drahému hardwaru, a proto by se analytika měla odehrávat v cloudu (nebo ideálně pomocí edge-computing pro udržení lokalizace a zabezpečení dat).	Lokální	Mid-range
Přenos a zpracování diagnostických a dalších dat	Ve zdravotnictví existuje mnoho obrázků a souborů s vysokým rozlišením, které mohou vyžadovat vysoce výkonné výpočetní zpracování pro diagnostiku a návrh. S 5G, například po obdržení MRI nebo CT skenu, mohou být snímky odeslány v reálném čase tam, kde je třeba je analyzovat, aby bylo možné stanovit diagnózu. Navíc je možné využít připojení přístrojů k 5G také pro jejich lokalizaci v rámci nemocnice.	Lokální	Mid-range
Monitorování životních funkcí pacientů na lůžku	Multifunkční podložky, samozřejmě s konektivitou, přenášejí nejen informace o životních funkcích pacientů, ale také kontrolují polohování kvůli vzniku proleženin. V nemocnicích mají často problémy s velmi zarušenými wifi sítěmi. Proto takto kritická komunikace rozhodně patří na privátní 5G. To zároveň zachovává potřebnou mobilitu pro přemisťování lůžek.	Lokální	Critical
Chytré dávkovače léků a implantáty	Chytré dávkovače léků připomínají pacientům, aby si vzali léky včas, a dávkují správné množství. Tento proces může být automatizován jako například u inzulínové pumpy. Tato zařízení mohou také upozornit pečovatele nebo poskytovatele zdravotní péče, pokud byla dávka vynechána, což zlepšuje dodržování léčby a snižuje riziko komplikací.	Národní/ Mezinárodní	Mid-range

3.2.4 Finance a pojišťovnictví

Vertikála **Finance a Pojišťovnictví** zahrnuje širokou škálu aktivit, včetně bankovnictví, finančních služeb, pojišťovnictví a správy investic. Tento sektor je klíčový pro globální ekonomiku, protože zajišťuje transakce, řídí rizika a poskytuje finanční ochranu a růstové příležitosti pro jednotlivce i podniky. Jak se toto odvětví stává stále více digitálním, integrace IoT technologií mění způsob poskytování finančních a pojišťovacích služeb. IoT umožňuje sběr dat v reálném čase, personalizované služby a efektivnější řízení rizik, což nakonec zlepšuje zákaznickou zkušenost a provozní efektivitu.

Následující příklady ukazují, jak IoT mění finanční a pojišťovací průmysl tím, že nabízí inteligentnější, propojenější a rychlejší služby.

Název UC	Popis	Perimetr	Kategorie IoT
Pojištění podle skutečné úrovně rizika	IoT zařízení, jako je telematika ve vozidlech nebo nositelná zařízení, sbírají data o chování uživatelů (např. jízdní návyky nebo zdravotní metriky) k přizpůsobení pojistného podle skutečné úrovně rizika. Tento přístup nabízí personalizovanější a spravedlivější ceny, které odměňují bezpečnější chování nižšími pojistnými.	Národní/ Meziárodní	Mid-range

Pojištění při užívání (Pay as You Go)	Na základě automaticky přenášených informací je účtováno pojištění při skutečném užívání. Příkladem může být vozidlo, nebo také cestovní pojištění, které je automaticky aktivováno při překročení hranic.	Mezinárodní	Mid-range
Řízení bankomatů s využitím IoT	IoT technologie se používají k monitorování a správě bankomatů (ATM) v reálném čase. Senzory a připojená zařízení mohou sledovat úrovně hotovosti, detekovat potenciální problémy, jako jsou poruchy nebo pokusy o manipulaci, a dokonce předpovídat potřebu údržby před výskytem selhání. Kromě toho může IoT pomoci optimalizovat plány doplňování hotovosti, snížit provozní náklady a zajistit, aby bankomaty byly vždy funkční a bezpečné pro zákazníky.	Národní	Mid-range

3.2.5 Energetika a utility

Vertikála **Energie a utility** zahrnuje průmyslová odvětví zabývající se výrobou, distribucí a správou základních zdrojů, jako jsou elektřina, zemní plyn, voda a obnovitelné zdroje energie. Tento sektor je nezbytný pro moderní život, napájí domácnosti, podniky a průmysl a zároveň zajišťuje efektivní a udržitelné využívání přírodních zdrojů. S rostoucí poptávkou po energii a potřebou udržitelných praktik se integrace IoT technologií stává stále důležitější. IoT umožňuje monitorování v reálném čase, chytré řízení sítí, prediktivní údržbu a zlepšení energetické účinnosti, což je klíčové pro modernizaci infrastruktury v oblasti energie a utilit.

Název UC	Popis	Perimetr	Kategorie IoT
Smart metering	Smart metering (chytré měřiče) využívá IoT technologie k monitorování spotřeby elektřiny, plynu nebo vody v reálném čase. Nabízí podrobné přehledy o vzorcích spotřeby, umožňuje vzdálené odečty a podporuje dynamické cenové modely, což pomáhá jak spotřebitelům tak utilitním společnostem efektivněji řídit zdroje.	Národní	Massive
Smart grid	Chytrá síť (Smart Grid) je pokročilá elektrická síť, která využívá IoT technologie, analýzu dat a automatizaci k efektivnějšímu a spolehlivějšímu řízení výroby, distribuce a spotřeby elektřiny. Na rozdíl od tradičních energetických sítí, které fungují staticky a jednosměrně, umožňuje chytrá síť obousměrnou komunikaci mezi utilitou a spotřebiteli, stejně jako mezi různými částmi sítě. To umožňuje monitorování v reálném čase, dynamické vyvažování zátěže a lepší integraci obnovitelných zdrojů energie.	Národní	Mid-range
Správa utilit - vody	IoT zařízení monitorují distribuční sítě vody na úniky, změny tlaku a problémy s kvalitou. Data v reálném čase pomáhají utilitám rychle identifikovat a řešit problémy, snižovat ztráty vody, zajišťovat kvalitu vody a optimalizovat její využití.	Národní	Massive
Chytré budovy a HVAC (Heating, ventilation, and air conditioning) systémy	IoT zařízení v domácnostech a budovách pomáhají řídit spotřebu energie řízením systémů HVAC (topení, větrání a klimatizace), osvětlení a spotřebičů na základě dat v reálném čase a uživatelských preferencí. Tyto systémy optimalizují využití energie, snižují náklady a přispívají k udržitelnějšímu energetickému ekosystému.	Národní	Massive
Chytré pouliční osvětlení	Chytré systémy pouličního osvětlení s podporou IoT automaticky přizpůsobují úroveň osvětlení podle podmínek prostředí, denní doby nebo obsazenosti. Tyto systémy snižují spotřebu energie, snižují náklady na údržbu a zvyšují bezpečnost veřejných prostor poskytováním dostatečného osvětlení tam, kde je to potřeba.	Lokální/ Národní	Massive

3.2.6 Municipality a Chytrá města

Vertikála **Municipality a Chytrá města** zahrnuje veřejné sektory zodpovědné za správu a poskytování služeb komunitám a občanům, včetně infrastruktury, veřejné bezpečnosti, dopravy, správy životního prostředí a utilit. Tento sektor stále více využívá IoT technologie k vytváření efektivnějších, udržitelnějších a obyvatelnějších městských prostředí. Integrací propojených zařízení, analýzy dat v reálném čase a automatizace mohou vlády a municipalitní orgány zlepšit poskytování služeb, efektivněji spravovat zdroje a lépe zapojovat občany. Koncept chytrých měst, kde IoT hraje klíčovou roli, se zaměřuje na využívání technologií k zlepšení kvality života, zvýšení efektivity a podpoře udržitelného rozvoje v městských oblastech.

Některé případy užití jsou fakticky společné pro oblast Energetika a pro Chytrá města. Jedná se zejména o:

- Chytré budovy a HVAC systémy.
- Chytré pouliční osvětlení.
- Smart metering.

Chytrá města jsou totiž velkým spotřebitelem energie a náklady na energie tvoří podstatnou část městského rozpočtu. Je proto v bytostném zájmu municipalit přijímat moderní technologická řešení, která jim pomohou optimalizovat spotřebu energií. A IOT systémy jsou klíčovou částí těchto řešení.

Název UC	Popis	Perimetr	Kategorie IoT
Řízení dopravy	Monitorování a řízení dopravy s podporou IoT systémů v reálném čase může snížit dopravní zácpy a zlepšit městskou mobilitu. Další aplikací je monitoring parkovacích míst a dynamické navádění vozidel v závislosti na obsazenosti. 5G poskytne vhodnou konektivitu pro tento případ užití všude tam, kde není možné či efektivní využít pevnou konektivitu.	Lokální/ Národní	Critical
Připojení vozidel hromadné dopravy	Připojení vozidel hromadné dopravy je potřebné z řady důvodů. Optimalizace vytížení hromadné dopravy, komunikace s dispečinkem a řídícími systémy, přenos dat z kamer, poskytování informačních služeb cestujícím, případně i konektivita pro cestující atd. Některé z těchto scénářů spadají do kategorie IoT.	Lokální	Mid-range
Environmentální monitorování	Existuje široká škála parametrů prostředí, které je přínosné sledovat s využitím různých typů senzorů - monitorování kvality ovzduší, kvality vody, koncentrace CO2, vlhkost, odpady atd. Typicky se jedná IoT scénář a nabízí se tedy využití 5G typu mMTC.	Lokální/ Národní	Massive
Bezpečnost města	O bezpečnost města se starají dohledové systémy a také aplikace využívané městskou policií. V těchto případech je opět důležitá garantovaná dostupnost služby s definovanými parametry.	Lokální	Mid-range
Energetika a utility pro chytré město	Výdaje za energie tvoří často podstatnou nákladovou položku v rozpočtu města. Moderní přístupy k řízení energetických zdrojů a spotřeby mohou náklady výrazně snížit. Patří sem například pokročilý facility management městských budov včetně smart meteringu a řízení veřejného osvětlení. Pro všechna tato moderní řešení jsou IoT systémy a spolehlivá konektivita nutným předpokladem.	Lokální	Massive

Řízení odpadů	IoT senzory instalované v odpadkových koších a kontejnerech monitorují úroveň naplnění a optimalizují trasy sběru odpadu. To snižuje provozní náklady, minimalizuje dopad na životní prostředí a zajišťuje efektivnější sběr odpadu, což zabraňuje přeplnění a zlepšuje čistotu veřejných prostor.	Lokální	Massive

3.2.7 Zemědělství a potravinářství

Vertikála **Zemědělství** je zásadní pro globální produkci potravin a zahrnuje činnosti související se zemědělstvím, chovem hospodářských zvířat, pěstováním plodin a celkovou správou zemědělských zdrojů. Tento sektor stále více využívá technologie ke zvýšení produktivity, efektivity a udržitelnosti tváří v tvář výzvám, jako jsou změny klimatu, nedostatek zdrojů a rostoucí světová populace. IoT technologie hrají klíčovou roli v modernizaci zemědělství tím, že poskytují data v reálném čase, umožňují přesné zemědělství a automatizaci procesů. Tyto pokroky pomáhají zemědělcům činit informovaná rozhodnutí, optimalizovat využití zdrojů, a nakonec zvyšovat výnosy při snižování dopadů na životní prostředí.

Název UC	Popis	Perimetr	Kategorie IoT
Autonomní traktory a zemědělské stroje	Autonomní traktory a další zemědělské stroje využívají 5G k příjmu a přenosu dat v reálném čase, což jim umožňuje efektivněji provádět úkoly, jako je sázení, plení a sklízení, s minimálním zásahem člověka. 5G podobně jako u jiných autonomních vozidel umožňuje v případě potřeby efektivní teleoperaci a přenos dat z kamer na strojích pro okamžité vyhodnocení.	Lokální	Critical
Automatizované sklízecí systémy	Automatizované sklízecí systémy využívají robotické stroje k autonomní sklizni plodin. Tyto systémy se obvykle skládají ze samořídících vozidel vybavených senzory, kamerami a robotickými rameny, které dokážou identifikovat zralé plodiny, přesně je nakrájet nebo sbírat a sbírat produkty. Efektivita těchto systémů závisí na jejich schopnosti zpracovávat obrovské množství dat v reálném čase, činit rychlá rozhodnutí a pracovat s vysokou přesností na velkých plochách zemědělské půdy.	Lokální	Mid-range
Chytré zavlažovací systémy	Inteligentní zavlažovací systémy využívají síť senzorů rozmístěných po celém zemědělském poli. Tyto senzory měří různé parametry prostředí a půdy, jako je úroveň vlhkosti, teplota a dokonce i stav živin v půdě. Senzory odesílají data do centrálního systému k analýze. Může jít o edge server. Na základě analýzy jsou vyslány příkazy do zavlažovacího systému, aby se podle potřeby upravil plán zavlažování. To může zahrnovat zapnutí/vypnutí sprinklerů, úpravu průtoku nebo změnu načasování zavlažování. Systém se může zaměřit na konkrétní zóny v rámci pole, aby bylo zajištěno, že každá oblast dostane přesné množství potřebné vody.	Lokální	Massive
Monitorování hospodářských zvířat	Monitoring se zaměřuje na sledování polohy a zdravotního stavu zvířat. Nositelná IoT zařízení shromažďují data o poloze, zdraví a chování hospodářských zvířat. 5G zajišťuje nepřetržitý přenos těchto dat, která lze použít k monitorování zdraví v reálném čase, předpovídání nemocí a optimalizaci chovných cyklů.	Lokální	Massive

Monitorování stavu zemědělských plodin a půdy	Systémy monitorování plodin využívají různé senzory rozmístěné po celém poli. Patří mezi ně senzory půdní vlhkosti, senzory hladiny živin a senzory klimatu, které měří parametry jako teplota, vlhkost a hladiny CO2. Drony poskytují další data, která jsou zásadní pro posouzení zdraví plodin ve větším měřítku. Tyto snímky dokážou detekovat odchylky v barvě, velikosti a vývoji plodiny, které svědčí o zdravotním a nutričním stavu. Data shromážděná z pozemních senzorů a leteckých snímků jsou integrována a přenášena do centrální jednotky, kde se provádí pokročilá analýza dat. Systém poskytuje užitečné informace, které ihned využít. Pokud je například zjištěno možné zamoření škůdci, systém může doporučit konkrétní oblasti pro aplikaci pesticidů.	Lokální	Massive
Trackování produktů z farmy k místu prodeje	Tento UC řeší důležitý aspekt zemědělského dodavatelského řetězce: zajištění transparentnosti, sledovatelnosti a účinnosti od místa původu až ke spotřebiteli. Produkty se označují na úrovni farmy pomocí čárových kódů, RFID tagů nebo chytrých senzorů, které dokážou zachytit a zaznamenat různá data včetně času sklizně, původu, ošetření a hodnocení kvality. Zúčastněné strany mohou sledovat stav a postup zboží, jak se pohybuje v dodavatelském řetězci. Toto monitorování pomáhá při řízení logistiky, optimalizaci tras, reakci na zpoždění a zajištění souladu s bezpečnostními a kvalitativními standardy.	Národní/ Mezinárodní	Massive
Monitoring podmínek při přepravě zemědělských produktů	UC se zaměřuje na zachování integrity a kvality zemědělského zboží při přepravě z farem na trhy nebo ke zpracovatelům. Senzory jsou integrovány do přepravních vozidel nebo jednotlivých balení produktů. Tyto senzory monitorují během přepravy různé parametry prostředí, jako je teplota, vlhkost, vibrace a atmosférický tlak – faktory, které jsou rozhodující pro udržení kvality produktu. Data jsou přenášena do centrálního prvku, vyhodnocena a následně jsou zdrojem pro generování příslušných reportů.	Národní/ Mezinárodní	Massive
Automatizované skleníky	Skleníky s podporou IoT používají senzory a automatizaci k řízení teploty, vlhkosti, osvětlení a větrání. Tyto systémy vytvářejí optimální podmínky pro růst, zlepšují výnosy plodin a snižují potřebu manuálního zásahu.	Lokální	Massive

3.2.8 Doprava a logistika

Vertikála **Doprava a logistika** je klíčová pro globální obchod a pohyb zboží, zahrnuje správu dopravních sítí, přepravu, skladování a operace v dodavatelském řetězci. Tento sektor je zodpovědný za to, aby produkty dorazily na své cíle efektivně, bezpečně a včas. Integrace IoT technologií do dopravy a logistiky transformuje toto odvětví tím, že umožňuje sledování v reálném čase, optimalizaci tras, zlepšení správy vozového parku a zlepšení celkové viditelnosti v dodavatelském řetězci. Tyto pokroky pomáhají společnostem snižovat náklady, zvyšovat efektivitu a efektivněji reagovat na dynamické požadavky trhu, a to vše při zlepšování kvality služeb a spokojenosti zákazníků.

Některé případy užití vertikály Doprava se překrývají s případy užití v oblasti Automotive, konkrétně:

- V2X komunikace mezi vozidly a infrastrukturou
- Fleet management.

Název UC	Popis	Perimetr	Kategorie IoT
Digital twin organizace v logistice	Digital twin komplexního systému, jakým je logistické centrum - v řadě případů přístav, v našich podmínkách například železniční terminál, umožňuje zvyšovat efektivitu celého uzlu díky modelování "what if" scénářů a využití analýzy obrovského množství dat sbíraného senzory a kamerami z reálného prostředí do digitálního dvojčete.	Lokální	Mid-range
Inventory management	Sledování a řízení zásob. Ideálně v reálném čase. Například v podobě tzv. chytrého regálu. A/nebo s využitím RFID a čteček čárových kódů. V každém případě všechny informace je potřeba mít v digitální formě a data přenášet do centrálního prvku, který může být umístěn na edge. Vše je pak řízeno s využitím Warehouse management system SW.	Lokální	Massive
Asset tracking	Sledování položek při dopravě je důležitou součástí řízení celého dodavatelského řetězce a nutnou podmínkou jeho efektivity. Je vyžadována celoplošná technologie, a to z kategorie LP-WAN. V případě 5G by se tedy mohlo jednat o RedCap, nebo Passive IoT.	Národní/ Mezinárodní	Massive
Balení produktů s computer vision	Využití "computer vision" pro kontrolu kvality balení v logistice. Počítačové vidění je obor umělé inteligence, který trénuje počítače k interpretaci a porozumění vizuálnímu světu. Pomocí digitálních snímků z kamer a videí a modelů hlubokého učení mohou systémy počítačového vidění přesně identifikovat a klasifikovat objekty a poté reagovat na to, co „vidí“.	Lokální	Mid-range

4 Business modely IoT

Řešení v oblasti IoT musí mít funkční business model. IoT řešením je v tomto kontextu soubor produktů a služeb na nich založených, které jsou přizpůsobené řešení potřeb zákazníků v dané vertikále.

Právě absence funkčního či vhodného buiness modelu byla historicky jednou z příčin toho, že růst IoT služeb většinou nenaplňoval velmi ambiciózní prognózy.

Podívejme se nejdříve na to, co vlastně business model je a z čeho se skládá. Obecná definice business modelu je následující:

Business model definuje, jak firma tvoří hodnotu, doručuje ji zákazníkům a získává od nich zpět protihodnotu.

Business model má tedy 3 hlavní oblasti:

1. **Vytváření hodnoty** – jaké problémy zákazníka řešíte, jaké potřebu uspokojujete svými produkty a službami, které poskytujete zákazníkovi. Díky tomu zákazník získává hodnotu. Tato hodnota je definovaná jako Value Proposition. A pokud možno je odlišná od hodnoty poskytované konkurencí, je unikátní, tedy Unique Value Proposition.
2. **Doručování hodnoty** – jaká je nákladová struktura produktů a služeb, jak jsou distribuovány k zákazníkovi a zpřístupněny mu k užívání.
3. **Zachycení hodnoty** – způsob, jakým firma získává hodnotu zpět pro sebe. To je dané jejím výnosovým modelem.

Aby business model fungoval, musí v něm platit následující pravidla:

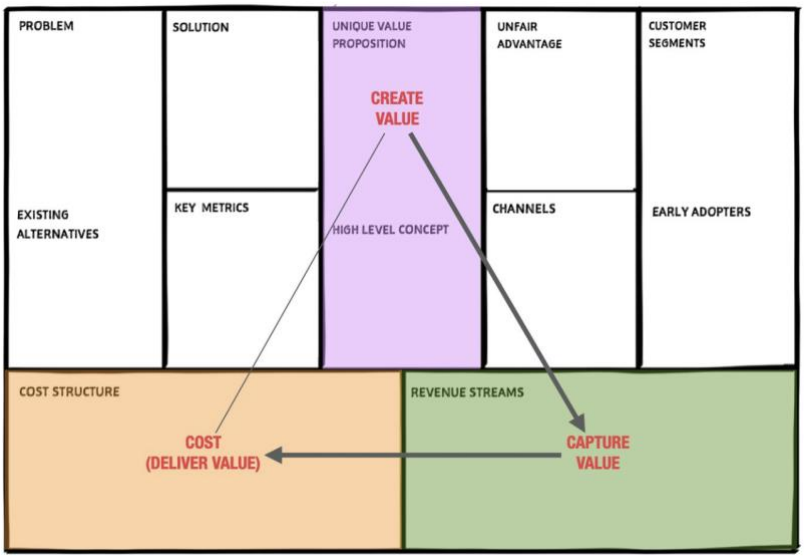
- Hodnota vnímaná zákazníkem musí být vyšší než hodnota, kterou nám vrací zpět. To je podstata správné Value Proposition.
- A současně musí být hodnota, kterou firma získá zpět, vyšší než náklad na doručení této hodnoty.

Tato obecná pravidla budou pochopitelně platit také pro internet věcí a nabídku řešení v této oblasti.

Znamená to tedy, že pokud má být IoT řešení úspěšné, musí zákazník jasně vnímat přínosy IoT systému a být ochoten za ně zaplatit.

Podívejme se nejdříve na obecný business model IoT řešení. Využít při tom můžeme Lean Canvas,[14], Value Proposition Canvas a zaměřit se na to, jak je hodnota vytvářena, doručována a získávána zpět.

[14] Maurya, A. (2012, February 28). *Running Lean*. (O'Reilly Media, Inc.).



Obrázek 9: Lean Canvas. Zdroj: [15]

1. Hodnota, kterou přináší IoT řešení (Value Proposition)

IoT systémy typicky vytvářejí a přinášejí jako **hodnotu informace**. Jak je rozvedeno v kapitole 3.1.1, existují dva hlavní typy IoT systémů:

- Jednosměrné systémy přinášejí informace pro další analýzu.

Sledování zásob, opotřebení strojů, informace o zdravotním stavu, stav ovzduší a nepřeberné množství dalších příkladů. Tyto informace musí být dále analyzovány a mohou vést k určitým akcím a opatřením, která však už probíhají mimo systém.

- Interaktivní systémy přímo využívají informace pro automatizaci a řízení.

Na základě informací generovaných v IoT systému jsou aktivními prvky systému (atkuátory) realizovány přímo akce vedoucí k optimalizaci procesů ve výrobě, optimalizaci spotřeby energií či dalším akcím.

Je zřejmé, že v obou těchto typech IoT systémů může mít informace a její využití pro zákazníka IoT systému obrovskou hodnotu. Na čem tato hodnota záleží? **Výstup z IoT systému musí řešit skutečně podstatný problém/potřebu zákazníka. A zároveň tento problém/potřeba není dostatečně uspokojena jiným stávajícím řešením.**

Například: pro firmu, která trpní vysokými náklady na servis strojů a/nebo jejich častými odstávkami z důvodu poruchy, může být prediktivní údržba s využitím IoT systému výborným řešením s vysokou hodnotou. Pokud ale firma používá stroje prakticky bez poruch a s jednoduchou údržbou, nebude ochota firmy investovat do IoT systému pro prediktivní údržbu vysoká.

Při vytváření hodnoty, tedy návrhu IoT systému, který bude hodnotu generovat, je nutné primárně se zaměřit na nalezení a definici problému/potřeby zákazníka a uživatelů IoT systému a navržení způsobu jeho řešení.

K definici Value Proposition je možné a vhodné využít Value Proposition Canvas. Ten obsahuje oblast zákazníka a oblast produktu.

Oblast zákazníka:

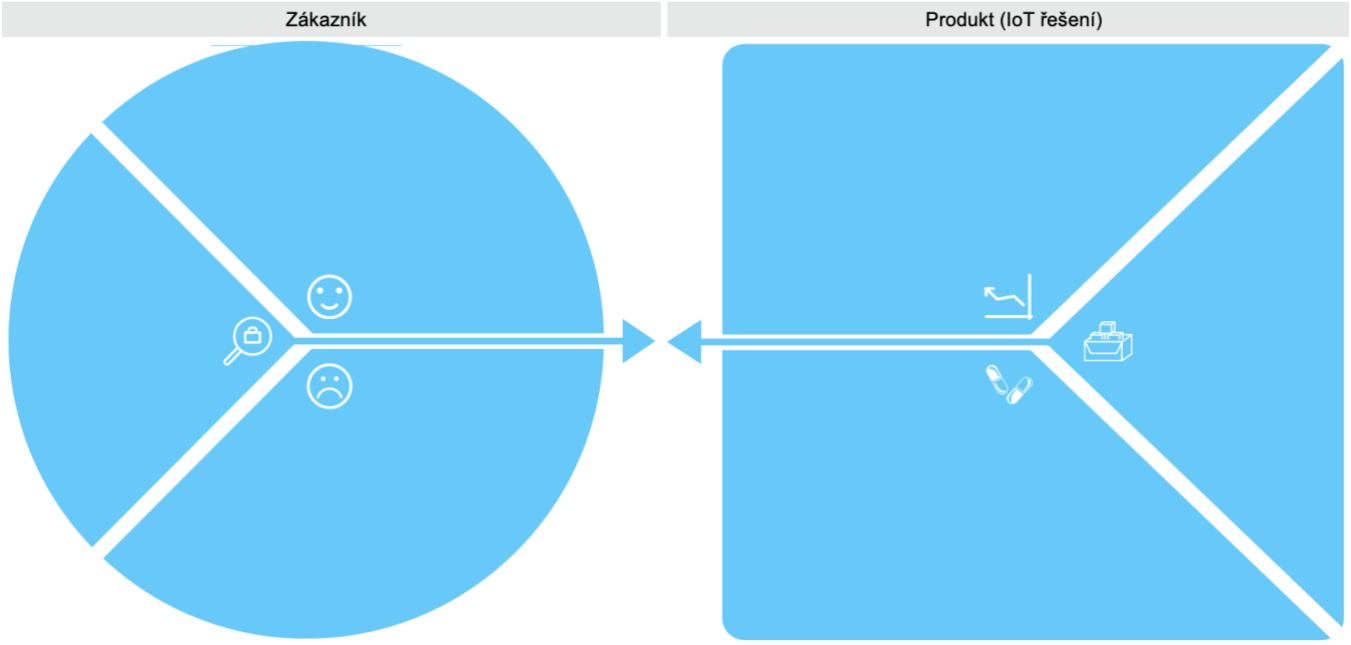
- Vlevo: úkoly, které zákazník potřebuje realizovat („jobs to be done“).
- Dole: Pains/Pain points, tedy problémy, které zákazníka trápí.

[15] Maurya, A. (2012, February 28). *Running Lean*. (O'Reilly Media, Inc.).

- Nahoře: Gains, tedy zákazníkem očekávané zlepšení.

Oblast produktu (v tomto případě IoT řešení):

- Vpravo: Funkcionality produktu či služby, které umožní zákazníkovi realizovat jeho úkoly.
- Dole: Painkillers, tedy vlastnost produktu či služby, které odstraní zákazníkovi jeho jednotlivé pain points.
- Nahoře: Vitamins, tedy vlastnosti produktu či služby, které přinesou zákazníkovi očekávaná zlepšení.



Obrázek 10: Šablona Value Proposition Canvas. Zdroj: Vlastní zpracování.

Technické aspekty jako je typ koncových zařízení, přenosová technologie atd. přijdou na řadu v další fázi.

2. Doručení hodnoty a nákladová struktura.

Hodnota je v IoT oblasti doručena pomocí komplexního systému. Jak je uvedeno v kapitole 1.2, prvky IoT systému tvoří zejména:

- Zařízení: Patří sem senzory, akční členy (aktuátory), chytré spotřebiče a další připojený hardware, který sbírá a přenáší data.
- Sítě: Komunikační infrastruktura, která umožňuje zařízením se připojovat a vyměňovat si data (např. 5G).
- Elementy pro zpracování dat: Cloudové služby, edge computing zařízení a aplikace, které zpracovávají a analyzují data získaná zařízeními.
- Uživatelé: Lidská obsluha, automatizované systémy nebo rozhodovatelé, kteří využívají informace generované systémem IoT.

IoT systémy často využívají standardizovaná zařízení, technologie a služby. Na druhou stranu, s výjimkou Consumer IoT, jsou tyto systémy typicky designovány na míru zákazníkům, jako jsou výrobní firmy, energetické firmy, nemocnice nebo například města. Jedná se o technologicky komplexní řešení, která často

vyžadují účast několika dodavatelů a systémového integrátora, které dokáže spojit jednotlivé prvky řešení do funkčního systému.

Z pohledu nákladové struktury jde také o komplexní systém, který může obsahovat různé nákladové kategorie. Například:

- Jednorázové náklady spojené s koncovými zařízeními, poskytnutím profesionálních služeb atd.
- Průběžné náklady spojené s užíváním komunikačních technologií, dohledem systému atd.
- Náklady dle užívání spojené s využitím cloudových služeb.

3. Získání hodnoty – výnosový model.

V obecné rovině existuje řada výnosových modelů. Například:

- Jednorázový prodej produktu.
- Jednorázový poplatek za poskytnuté služby.
- Předplatné/pronájem - opakovaný měsíční/roční poplatek za užívání produktu či služby.
- Transakční poplatky (ve srovnání s předplatným je klíčové, že poplatek nemusí být nutně opakující se, ale transakční.)
- Měřené služby (PayAsYouGo) - měřené služby se účtují podle skutečného využití po určitou dobu.
- Marketplace/tržiště – model založený na zprostředkování transakce mezi kupujícím a prodávajícím.
- Big data – model založený na využití a monetizaci vygenerovaných dat.

A samozřejmě také kombinace různých výnosových modelů.

V případě IoT je situace komplikovaná tím, že na nákladové straně typicky figurují různé nákladové kategorie a je tak obtížné nastavit jednoduchý výnosový model. Například v podobě jedné pevné měsíční částky. To by s sebou mohlo nést rizika pro poskytovatele IoT řešení. Častější proto bude kombinace několika výnosových modelů v rámci jednoho IoT systému.

Například:

- Jednorázová cena za IoT HW (koncová zařízení – senzory).
- Opakující se měsíční cena za každé připojené IoT zařízení. Celková částka tedy bude záviset na počtu zařízení.
- Měsíční cena dle skutečně spotřebovaných zdrojů za cloudové služby – výpočetní zdroje, úložiště a další služby.

Nicméně také v oblasti IoT se začíná prosazovat model „as a service“. To znamená model založený na tom, že poskytovatel IoT řešení se o danou oblast stará a poskytuje ji zákazníkovi jako službu za jasně definovaných podmínek (nejde tedy o jednorázový transakční business v podobě prodeje produktu). Tyto modely se snáze prosadí v situaci, kdy oblast nepokrývá celý IoT systém. Například:

- Model „Zařízení jako služba“ (Device-as-a-Service): IoT hardware je nabízen v rámci modelu předplatného, kdy uživatel platí za hodnotu, kterou zařízení přináší (např. chytré osvětlení, propojené průmyslové vybavení). Předplatné zahrnuje jak HW, tak konektivitu.
- Model „Data jako služba“ (Data-as-a-Service): Firmy shromažďují a prodávají (anonymizovaná) data generovaná IoT zařízeními. To je možné v odvětvích jako zemědělství, kde lze data ze senzorů zpeněžit. V principu firmy platí za obdržená data, v ceně je již zahrnutý celý ekosystém, který byl potřeba pro jejich generování.
- Model „Platforma jako služba“ (Platform-as-a-Service): IoT platformy poskytují softwarovou infrastrukturu pro správu, analýzu a integraci datových toků ze zařízení, často na bázi předplatného. K ceně platformy bude obvykle zapotřebí počítat s náklady na ostatní části IoT ekosystému v podobě zařízení, konektivity atd.

- Modely založené na výsledcích (Outcome-based Models): Poskytovatelé účtují zákazníkům na základě výsledků či efektů dosažených pomocí IoT řešení, jako jsou zlepšení efektivity nebo snížení nákladů ve výrobě nebo řízení energií.

Role 5G v rámci IoT business modelu

Jak již bylo uvedeno, 5G technologie má vliv jak na komunikační a percepční vrstvu, tak také na bezpečnostní a obchodní. Proto logicky hraje podstatnou roli i v nastavení IoT business modelu.

5G technologie je v principu poměrně nákladná, jednak vzhledem k pokročilým vlastnostem vyžadující pokročilá technická řešení, tak také vzhledem k vysokým nákladům vývoje, které dodavatelé musí do cen promítnout. Navíc je typicky poskytována na licencovaném, a tedy vysokými náklady zatíženém pásmu.

Na druhé straně přináší 5G potenciál vysoké efektivity a vlastnosti, které mohou umožnit řešení, které by na inferiorní technologii nebylo možné. Zejména IoT řešení v kategorii “Critical IoT”. To znamená, že IoT řešení postavené na 5G technologii může přinést vysokou hodnotu vnímanou zákazníkem. To umožní i při účtování relativně vysoké ceny představit funkční business model.

Role poskytovatele a uživatele IoT řešení

V rámci vývoje nového produktu, respektive řešení, je standardní postup takový, že firma vyvíjející produkt definuje Value Proposition na základě znalosti potřeb svých zákazníků.

V případě IoT řešení je situace potenciálně ještě složitější v tom směru, že poskytovatel IoT řešení je expertem na technologický stack, který je potřeba pro realizaci IoT systému. Nicméně tím, kdo dokáže definovat způsob využití informací získaných v rámci IoT systému, je typicky jeho uživatel. Z tohoto pohledu je důležité, aby uživatel IoT systému byl součástí jeho návrhu. Jen tak mu IoT systém můžem přinášet maximální hodnotu v podobě těch správných informací potřebných pro získání hlubokého vhledu do problematiky, či přímo pro řízení a automatizaci procesů.

5 Stávající stav a budoucnost IoT

5.1 Přehled trhu IoT

5.1.1 Globální trh IoT a jeho vývoj

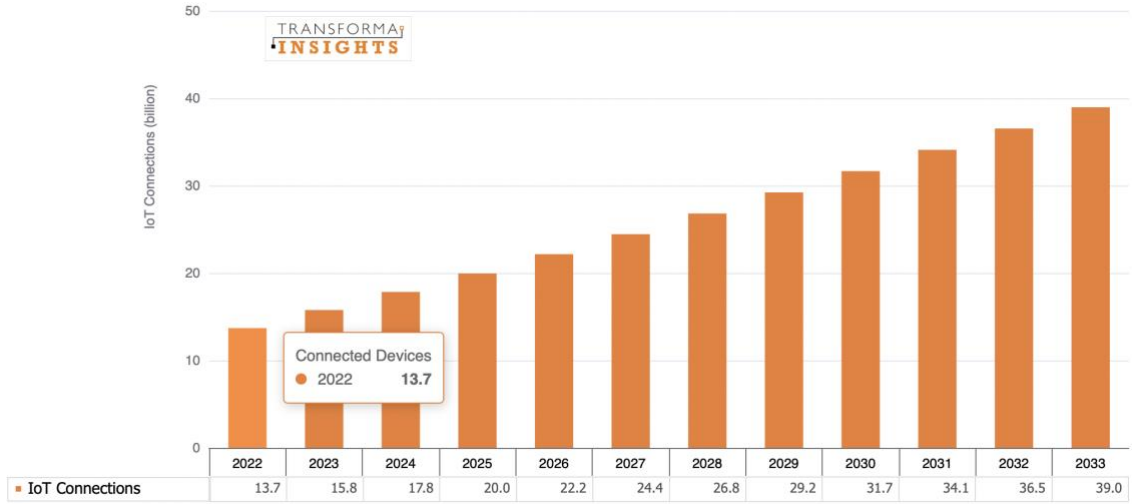
Měření IoT trhu je velmi náročné, protože zahrnuje obrovské množství různých případů užití, vertikál, technologií a řešení. IoT je skutečně široký pojem a de facto neexistuje jednotná metodika, která by umožnila jednotnou klasifikaci. Proto se čísla prezentovaná různými agenturami a analytickými společnostmi mohou poměrně lišit.

Příklad: pokud je součástí řešení připojená kamera, má být do trhu IoT počítána celá hodnota kamery, nebo jen určitá část odpovídající hodnotě bezdrátového modulu?

Čísla o IoT trhu je proto nutné brát s vědomím těchto specifik. Nicméně i tak poskytují užitečnou informaci jak o celkové velikosti, struktuře a dynamice vývoje trhu IoT. A ukazují, že se jedná o skutečně významnou oblasti.

Na následujícím grafu můžeme vidět předpověď počtu připojení IoT mezi roky 2022 až 2033 od společnosti Transforma Insights[16], který má lineárně stoupat až k počtu 39,6 miliardám připojení.

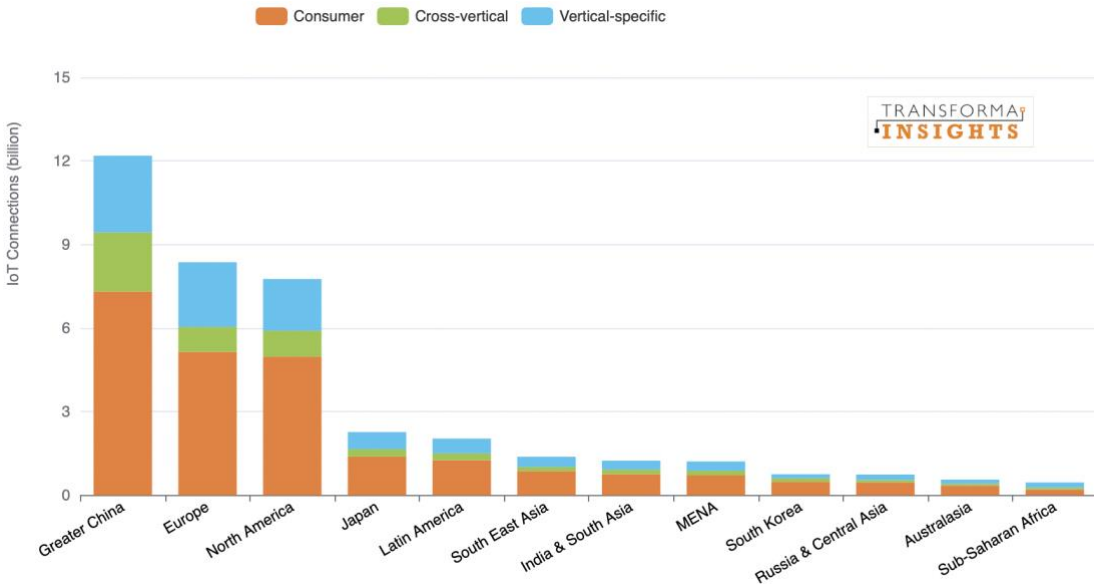
Společnost definuje připojení k internetu věcí jako připojení ke vzdáleným snímacím a ovládacím zařízením a zahrnuje i související agregační zařízení.



Graf 1: Počet IoT připojení 2022-2033. Zdroj: "Current IoT Forecast Highlights - Transforma Insights."

[16] "Current IoT Forecast Highlights - Transforma Insights," Transforma Insights, n.d., https://transformainsights.com/research/forecast/highlights.

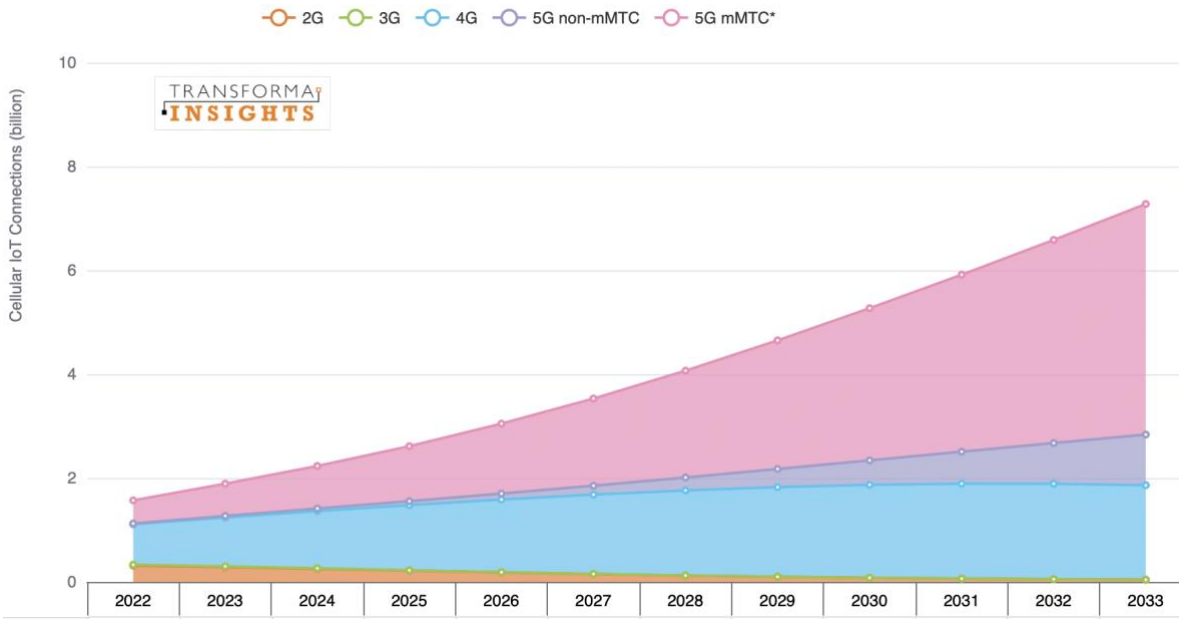
Vzhledem k velikosti spotřebitelského trhu budou v roce 2033 podle prognóz dominovat consumer IoT, včetně zařízení, jako jsou chytré televizory a chytré hodinky. Specifické vertikální trhy jsou mnohem roztříštěnější, ale zahrnují také aplikace inteligentního měření (smart metering), které představují významný počet připojení a který by se měl jen v Evropě v období 2024 až 2028 zvýšit o dalších 88 milionů připojení[17]. Mezi vertikální (podnikové) trhy patří vertikálně agnostické aplikace (vertical-agnostic applications), jako jsou připojené systémy vytápění, větrání a klimatizace a připojené bezpečnostní systémy nasazené v podnikovém kontextu. Největším regionem je Čína (a Taiwan), následovaná Evropou a Severní Amerikou.



Graf 2: Prognóza IoT připojení v roce 2033 dle oblastí. Zdroj: "Current IoT Forecast Highlights - Transforma Insights."

Pokud se podíváme specificky na celulární IoT připojení (tj. technologie poskytované v rámci mobilních sítí), ukazuje prognóza očekávaný vysoký nárůst 5G mMTC technologií. V rámci tohoto přehledu jsou do mMTC počítány nejen RedCap a Passive IoT, ale také původní 4G technologie NB-IoT a LTE-M. Naopak lze očekávat postupné vypínání 2G a 3G sítí.

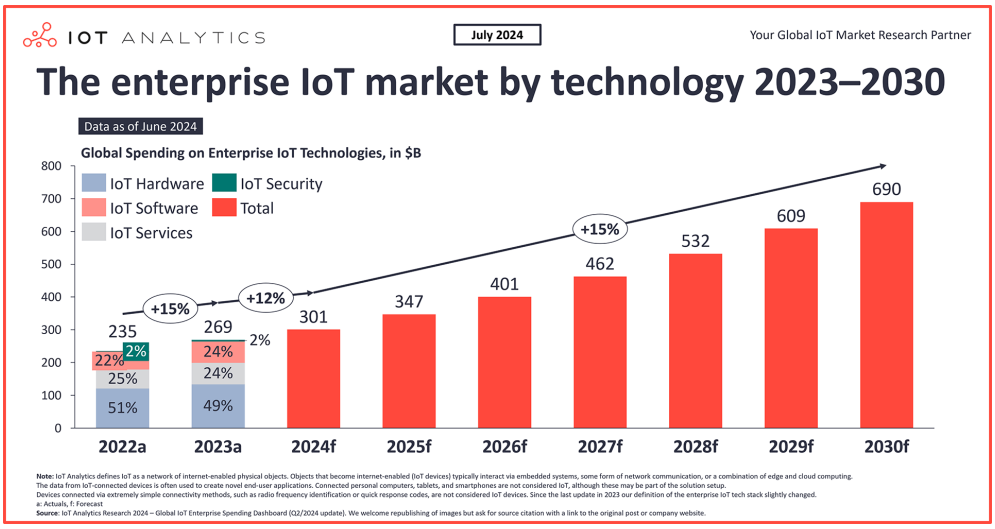
[17] https://www.smart-energy.com/industry-sectors/smart-meters/326-million-smart-meters-across-europe-by-2028-report/



Graf 3: Celulární IoT připojení dle technologií. Zdroj: "Current IoT Forecast Highlights - Transforma Insights."

Dle společnosti IoT Analytics dosáhl trh podnikových IoT řešení v roce 2023 velikosti 269 miliard USD představující meziroční nárůst o 15 %. Je nutno podotknout, že v tomto případě je trh definován dle podnikových výdajů. Největší podíl těchto výdajů, dle technologií, dosahovali IoT hardware se 49 %, následovány IoT softwarem a IoT službami, v obou případech s 24 %. Nejmenšího podílu opět dosáhly se 2 % náklady na IoT zabezpečení jakožto součástí řešení. V příštím roce společnost odhaduje, s ohledem na globální ekonomický vývoj, zpomalení tohoto růstu na 12 % a opětovné zrychlení v roce 2025 až na hodnotu 690 miliard USD v roce 2030. Společnost definuje IoT jako síť fyzických objektů s připojením k internetu. Data ze zařízení připojených k internetu věcí se často používají k vytváření nových aplikací pro koncové uživatele. Připojené osobní počítače, tablety a chytré telefony nejsou považovány za IoT, i když mohou být součástí nastavení řešení (solution setup). Zařízení připojená pomocí extrémně jednoduchých metod připojení, jako je radiofrekvenční identifikace nebo kódy rychlé odezvy, se nepovažují za zařízení internetu věcí. Vertikály rozděluje do jedenácti kategorií jako automotive nebo procesní výroba (process manufacturing), které mají zaznamenat v budoucnu nejvyšší růst, především díky přechodu k elektromobilitě, autonomnímu řízení nebo zvýšení provozní efektivity a modernizace provozu v případě procesní výroby. Ke globálnímu růstu má také přispět zvyšující se počet společností dosahujících pozitivního ROI z adopce IoT.[18]

[18] Joaquin Fernandez, "IoT market update: Enterprise IoT market size reached $269 billion in 2023, with growth deceleration in 2024," IoT Analytics, July 9, 2024, https://iot-analytics.com/iot-market-size/.



Graf 4: Enterprise IoT trh. Zdroj: https://iot-analytics.com/iot-market-size/

Složitost měření velikosti **trhu 5G IoT** dokreslují rozdílné hodnoty výzkumných agentur. Do trhu 5G IoT se v tomto případě počítají všechna zařízení, a také ostatní součásti řešení, jež využívají technologií 5G Stand Alone nebo 5G Non-standalone – jinými slovy využívá kompletně či alespoň částečně architektury 5G. Zatímco SkyQuest odhadoval jeho velikost na 8,53 miliard USD v roce 2022[19], společnost Precedence Research počítala se 4 miliardami USD[20]. Rovněž se liší prognózy velikosti trhu (např. pro rok 2031 136,18 miliard USD a 481,93 miliard USD) i míra růstu (34,12 % a 70,4 %), ačkoliv obě společnosti mají shodně rozřazené vertikály do osmi kategorií:

- výroba – Manufacturing (např. průmyslová automatizace, prediktivní údržba, monitorování majetku),
- zdravotnictví – Healthcare (např. vzdálené sledování pacientů, propojené ambulance, propojená zdravotnická zařízení)
- energetika a veřejné služby – Energy and Utilities (např. inteligentní sítě/Smart Grid, inteligentní měření/Smart Meter, správa potrubí),
- automobilový průmysl a doprava – Automotive and Transportation (např. systémy pro správu vozového parku/Fleet Management, propojená vozidla, autonomní vozidla),
- dodavatelské řetězce a logistika – Supply Chain and Logistics (např. sledování majetku, správa zásob, logistika a automatizace skladů),
- státní správa a veřejná bezpečnost – Governemnt and Public Safety (např. chytré parkování, chytré pouliční osvětlení, monitorování životního prostředí),
- zemědělství – Agriculture (např. precizní zemědělství, sledování hospodářských zvířat, sledování majetku),
- ostatní (např. retail, chytré budovy a vzdělávání).

Celosvětová velikost trhu spotřebitelského internetu věcí byla v roce 2022 oceněna na 75,10 miliardy USD a očekává se, že do roku 2030 vzroste na přibližně 193,58 miliardy USD při tempu růstu přibližně 12,71 % v letech 2023-2030. Vlády a soukromý sektor zvyšují penetraci internetu a infrastruktury, což vede k širokému

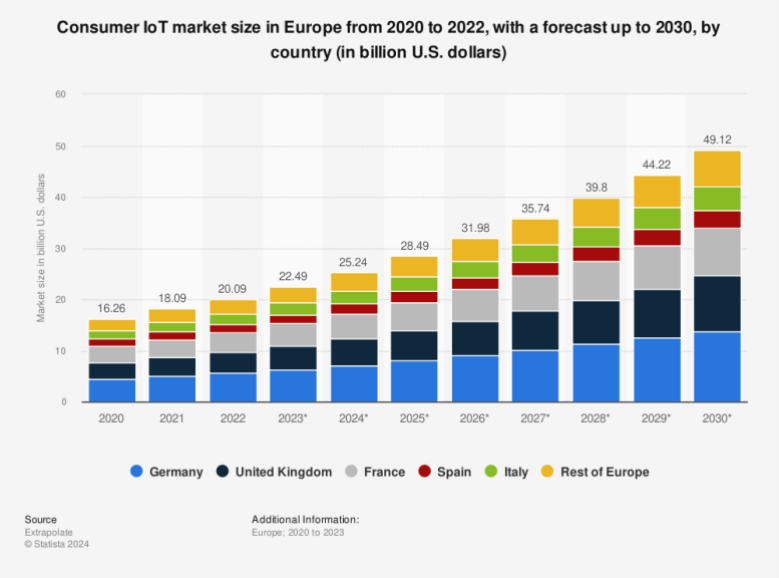
[19] "5G IoT Market Size, Share, Trends, Analysis and - Industry Growth | 2031," n.d., https://www.skyquestt.com/report/5g-iot-market.

[20] Precedence Research, "5G IoT Market Size To Hit USD 823.14 Bn By 2032," August 23, 2023, https://www.precedenceresearch.com/5g-iot-market.

využívání hlasových asistentů a zařízení pro inteligentní domácnost. Hlavními segmenty tohoto trhu budou i nadále pokročilé domácí spotřebiče a wearables.[21]

Statista předpokládá, že tržby na evropském trhu s IoT budou v letech 2024 až 2029 neustále růst, a to celkem o 107,2 miliardy amerických dolarů, což představuje nárůst o 60,55 %. Tržby by měly, podle grafu výše, kulminovat v roce 2029 na hodnotě 284,3 miliardy amerických dolarů. Zásadním faktorem ovlivňujícím trh internetu věcí je dle společnosti penetrace připojení k internetu. Rozšířené a spolehlivé internetové připojení je nezbytné pro bezproblémové fungování zařízení internetu věcí, které jim umožňuje komunikovat, přenášet data a přijímat aktualizace. Současnými trendy, které ovlivňují vývoj IoT jsou 5G sítě, artificial intelligence of things (AIoT), bezpečnost IoT a edge computing.[22] V souvislosti s bezpečností se sluší podotknout rostoucí trend kyberútoků na zařízení internetu věcí, který v roce 2022 dosáhl 112,3 milionů, což představuje meziroční nárůst o 87 %.[23]

Mimo tržeb se také zvyšují investice do řešení souvisejících s IoT. Společnost International Data Corporation předpokládá, že evropské organizace investují v roce 2024 přibližně 260 miliard dolarů a rovněž předpovídá, že růst výdajů na internet věcí bude v roce 2024 se bude kontinuálně zvyšovat s oživením evropské ekonomiky, zaznamená pětiletou složenou roční míru růstu (CAGR) ve výši 11,8 % a do roku 2027 dosáhne téměř 368 miliard dolarů.[24]



Graf 5: předpověď velikosti evropského trhu IoT pro spotřebitele v období 2020-2030. Zdroj: https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe.

Statista přináší i podrobnější pohled na evropskou velikost trhu s IoT pro spotřebitele v roce 2022 na 20,9 miliard USD a očekává jeho růst na 49,12 miliard USD v roce 2030. Největšími evropskými hráči mají být Velká Británie, Francie a Německo. Právě Německo má dosáhnout v roce 2030 13,8 miliard USD při tempu růstu 11,7 %.

[21] https://www.extrapolate.com/information-technology-communication-iot/consumer-iot-market/87454

[22] "Revenue of the internet of things industry in Europe 2019-2029," Statista, July 5, 2024, https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe.

[23] "Global annual number of IoT cyber attacks 2018-2022," Statista, May 3, 2023, https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/.

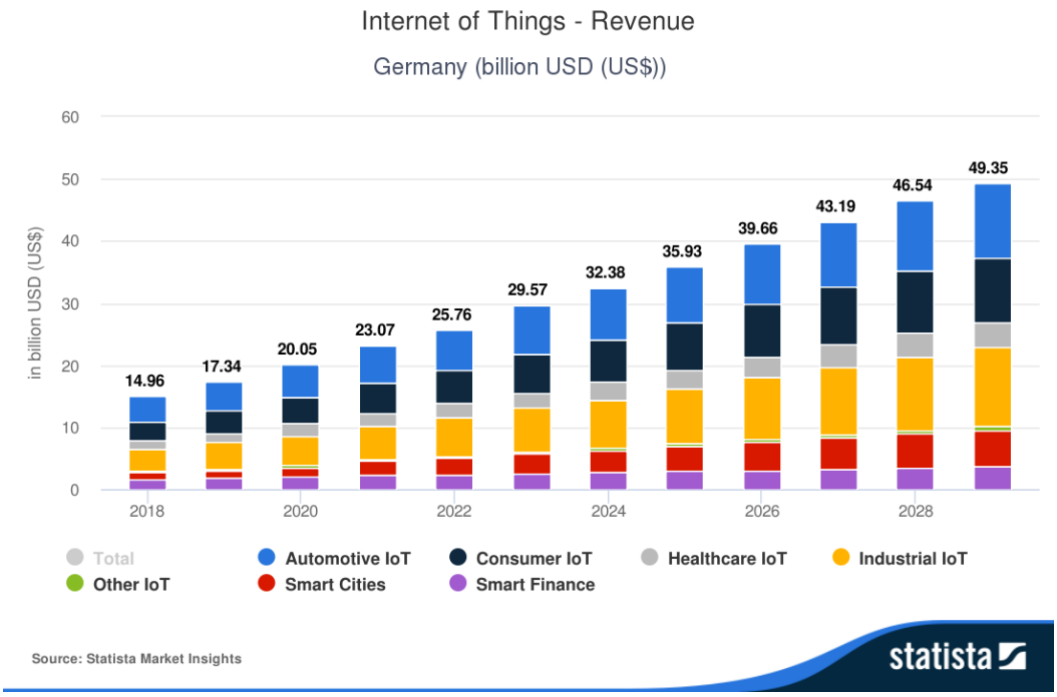
[24] https://www.idc.com/getdoc.jsp?containerId=prEUR251780724

5.1.2 Trh IoT v Německu

Německý trh v oblasti 5G i v oblasti IoT patří k nejvyspělejším na světě, a to i díky silnému průmyslovému zázemí. Průmyslový komplex vyžaduje digitalizaci pro zachování konkurenceschopnosti na globální úrovni. A to zase vede k potřebě pokročilých komunikačních technologií a konkrétně IoT řešení, zejména v oblasti Industry IoT a vertikály automotive. Dá se říci, že německý trh 5G a IoT je o několik let napřed. Je tedy dobrým předobrazem toho, jak se bude s velkou pravděpodobností vyvíjet trh v České republice.

Současně je německý trh dobře zmapovaný, protože je díky své velikosti atraktivní pro dodavatele ze všech částí hodnototvorného řetězce.

Následující graf ukazuje strukturu německého trhu IoT připojení z pohledu vertikál.[25]



Graf 6: IoT trh v Německu podle vertikál. Zdroj: Statista.

Sektor utilit má největší počet připojení

Sektor utilit bude mít v roce 2032 celkem 51,6 milionu IoT připojení, což představuje 27 % z celkového počtu IoT připojení v Německu. Tento sektor je podporován vládními iniciativami; cílem je dosáhnout 95% nasazení chytrých měřičů do roku 2030. Část z 28 miliard EUR, které Německo obdrželo z Fondu obnovy a odolnosti EU po pandemii COVID-19, byla vyčleněna na podporu tohoto úsilí.

[25] Revenue of the internet of things industry in Europe 2019-2029," Statista, July 5, 2024, https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe.

Automobilový průmysl je největším sektorem z hlediska příjmů z IoT

51 % příjmů z IoT v roce 2032 bude generováno automobilovým sektorem. Německo je domovem některých z největších světových automobilových továren, jako jsou BMW, Daimler a Volkswagen, které mají všechny smlouvy na propojená vozidla. Výrobci automobilů obvykle mají smlouvy na mezinárodní konektivitu, protože mnoho vozidel je vyráběno v Německu, ale prodáváno jinde (SIM karta je aktivována mimo Německo). Následující tabulka ukazuje celkovou velikost trhu IoT konektivity, z pohledu počtu připojení, výnosů a tempa růstu.

	2015	2022	2032	CAGR 22-32
Počet bezdrátových připojení	4.8 m	43.1 m	142.0 m	12.7%
Výnosy z konektivity	74.9 m EUR	381 m EUR	686 m EUR	6.0%
ARPU z konektivity	1.6 EUR	0.73 EUR	0.39 EUR	–6.1%

S podstatným růstem počtu připojení se bude snižovat průměrná cena za jedno připojení. Nicméně tempo růstu bude natolik vysoké, že celkové výnosy porostou solidním ročním tempem 6%.

Pokud jde o strukturu IoT konektivity, většinu trhu budou obsluhovat technologie, které bychom mohli souhrnně nazvat 3GPP či operátorské. Zajímavý je očekávaný vysoký podíl NB-IoT. Domníváme se přitom, že ve středním a delším horizontu tuto technologii mohou nahradit novější technologie RedCap a Passive IoT.

Mobilní operátoři působící v Německu jsou současně největší poskytovatelé IoT konektivity v Evropě: Deutsche Telekom, Telefónica a Vodafone.

Kromě nich poskytuje konektivitu pro IoT několik velkých hráčů. Část z nich na bázi technologie LoRa WAN a tedy s využitím vlastní sítě, zatímco další část formou MVNO, kdy využívají sítě různých mobilních operátorů. Jejich služby běží podle potřeby a možností na technologiích 2G, 3G, 4G, LTE-M a NB-IoT.

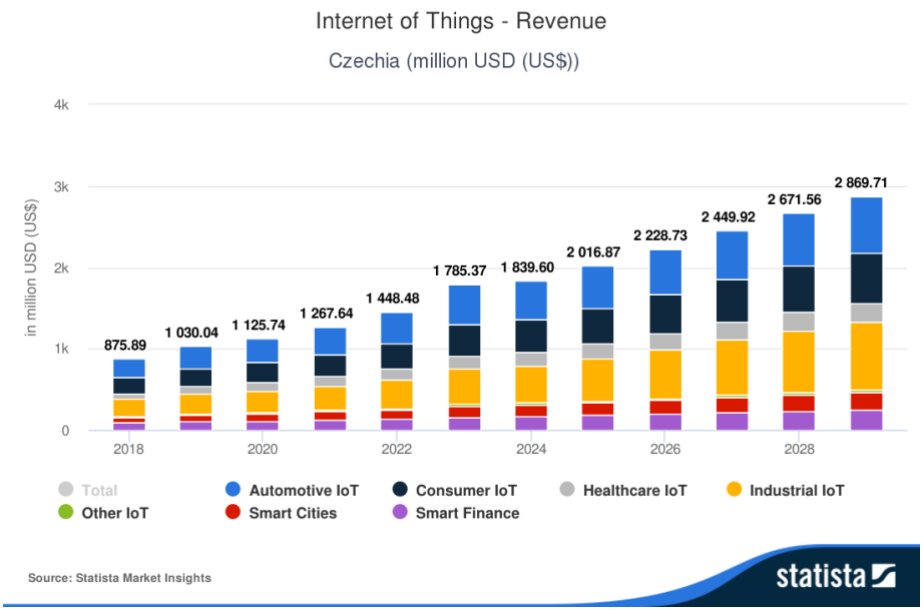
Přehled poskytovatelů je zajímavý také z toho důvodu, že řada z nich poskytuje služby IoT konektivity v evropském i globálním rozsahu a mohou být tedy také volbou pro české firmy hledající globální konektivitu pro své IoT projekty.

Poskytovatel IoT konektivity	**Typ poskytovatele**
1NCE	MVNO
emnify	MVNO
InsideM2M	MVNO
Things Mobile	MVNO
Wireless Logic	MVNO
Digimondo	LPWAN
komro	LPWAN

Minol Zenner	LPWAN
Sigfox Germany (Heliot)	LPWAN
Netze BW	Enterprise

5.1.3 Trh IoT v České republice

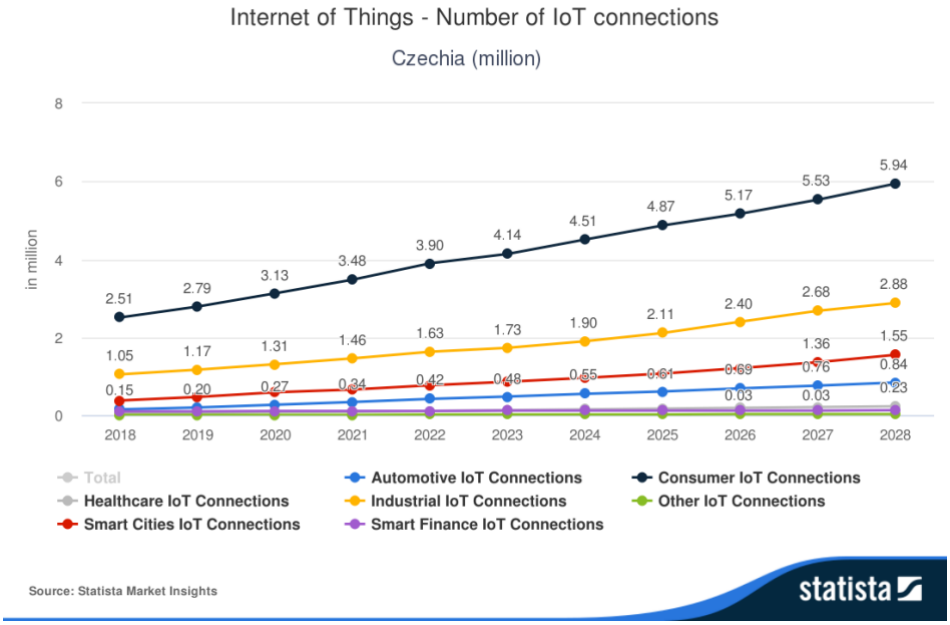
Pro makro pohled na trh IoT v České republice se podíváme na data společnosti Statista[26]. Tržby na trhu internetu věcí v ČR budou v letech 2024 až 2029 vykazovat složenou roční míru růstu 9,30 % (CAGR 2024-2029). Tato trajektorie růstu by měla do roku 2029 vyústit v objem trhu ve výši 2,87 miliard USD. Mezi jednotlivými vertikálami bude dominovat automobilový (automotive) a průmyslový (industrial) IoT. Prognóza vychází z různých ukazatelů trhu, jako jsou výdaje spotřebitelů, penetrace internetu, pokrytí 4G a současný a historický vývoj.



Graf 7: Trh IoT v ČR z pohledu výnosů dle vertikál. Zdroj: Statista.

Pokud se na trh IoT podíváme z pohledu počtu připojení a jejich struktury, největší celkový počet zařízení připojených k technologiím IoT (jak v oblasti internetu věcí s velkým, tak s malým dosahem) pochází ze spotřebitelského segmentu internetu věcí. Na dalších místech z pohledu počtu připojení jsou vertikály průmysl, smart cities a automotive. Z pohledu struktury je tedy trh IoT v České republice srovnatelný s dalšími průmyslově vyspělými státy, včetně Německa.

[26] Statista. "Internet of Things - Czechia | Statista Market Forecast," n.d. https://www.statista.com/outlook/tmo/internet-of-things/czechia.



Graf 8: předpověď počtu IoT připojení v ČR v období 2018-2028 dle vertikál

Hlavní subjekty na trhu IoT v České republice

Hodnotový řetězec IoT zahrnuje celou řadu typů hráčů, z nichž každý hraje důležitou roli při poskytování komplexních IoT řešení. Výrobci a dodavatelé IoT zařízení poskytují hardwarový základ, poskytovatelé konektivity umožňují komunikaci, poskytovatelé platforem a analytici nabízejí správu dat, analytiku a jejich interpretaci. Systémoví integrátoři zajišťují, že všechny IoT komponenty tvoří funkční systém. O provoz IoT systémů se pro zákazníky mohou starat poskytovatelé služeb (managed service providers). Svoji roli mají také poskytovatelé kyberbezpečnostních řešení a regulační úřady.

Někteří hráči zastávají několik rolí současně, například přinášejí kompletní IoT řešení zahrnující koncová zařízení, vyřešenou konektivitu a platformu pro zpracování dat.

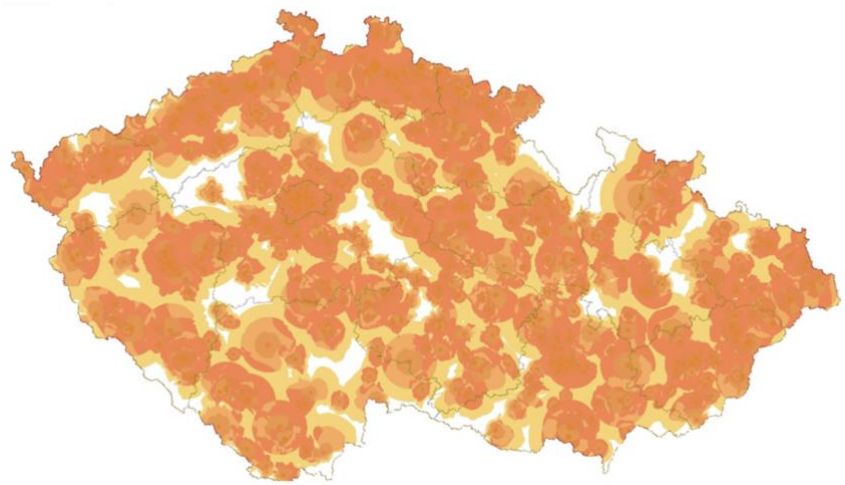
Při pohledu na IoT optikou nastupující 5G technologie je klíčová role poskytovatelů IoT konektivity.

Ty lze rozdělit na 2 hlavní skupiny:

1. Mobilní operátoři: poskytují přenosové technologie na licencovaném pásmu.

2. Poskytovatelé komunikačních služeb, kteří poskytují IoT přenosové technologie na nelicencovaných pásmech.

Do první skupiny patří mobilní operátoři T-Mobile, O2 a Vodafone. Poskytují technologie založené na 3GPP standardech. Pro IoT jsou využívané 2G, 4G, 5G, LTE-M a NB-IoT. Do druhé skupiny patří subjekty poskytující technologie dlouhého dosahu jako LoRa, SigFox a také technologie krátkého dosahu jako WiFi. Celoplošnou LoRa síť, navíc s možností mezinárodního roamingu, poskytují České Radiokomunikace.



Obrázek 11: Porkytí sítí LoRaWAN společnosti České Radiokomunikace. Zdroj: ČRa.

Síť SigFox byla v rámci francouzské franšízy provozována společností SimpleCell. Nyní je ovšem tato síť již v ČR nefunkční a společnost SimpleCell je v konkurzu. Kromě toho existuje celá řada lokálních poskytovatelů konektivity. V případě IoT projektů nabízí především technologii LoRa. Tu si může relativně snadno na nelicenčním pásmu 868 MHz provozovat například město pro vlastní potřeby. Mobilní operátoři v České republice v současnosti provozují jak sítě NB-IoT, tak LTE-M (cat-M). Zatímco síť NB-IoT byla společností Vodafone spuštěna již v roce 2017, ke spuštění cat-M sítí došlo později (v případě O2 a Vodafone až v roce 2023). Nyní je tedy již nabídka připojení z pohledu NB-IoT a Cat-M kompletní a sítě poskytují prakticky celoplošné pokrytí.

5.2 Výzvy spojené s IoT

Celá oblast IoT se dynamicky rozvíjí a podle optimistických předpovědí má tento trend nejen dále pokračovat, ale dokonce zrychlovat, viz data a grafy výše.

Tyto optimistické předpovědi trochu kontrastují s realitou zažívanou účastníky IoT ekosystému, protože ti čelím mnoha výzvám a překážkám, které v důsledku vedou k tomu, že rozvoj IoT projektů je pomalejší než plánovaný. IoT projekty tak nepřinášejí očekávané výnosy na jedné straně a dostatečnou hodnotu pro zákazníky na straně druhé. Podívejme se proto blíže na hlavní výzvy IoT ekosystému.

5.2.1 Kybernetická bezpečnost IoT

S velkým množstvím zařízení připojených k internetu jsou IoT systémy náchylné ke kyberútokům. Mnoho IoT zařízení má slabé bezpečnostní protokoly, což z nich dělá snadné cíle pro hackery. IoT zařízení navíc často zpracovávají citlivé údaje, což představuje významné riziko pro soukromí. Jedno narušení bezpečnosti v síti IoT může ohrozit klíčové systémy, což vede k finančním ztrátám, krádeži dat a poškození reputace značky. Právem je tedy možné označit kybernetickou bezpečnost IoT systémů za jednu z hlavních výzev jak pro uživatele IoT systémů, tak pro jejich poskytovatele.

Kybernetické bezpečnostní výzvy v IoT jsou mnohostranné, počínaje zajištěním bezpečnosti přenosu dat pomocí šifrovacích protokolů až po zajištění toho, že bezpečnost je základním kamenem návrhu systému. Šifrování hraje zásadní roli při ochraně důvěrnosti a integrity dat, ať už prostřednictvím nativního šifrování v protokolech, jako jsou AES a ECC, nebo jako dodatečná vrstva (např. TLS/SSL) pro nechráněné protokoly, jako je MQTT. **Přechod na 5G výrazně posiluje šifrovací standardy a bezpečnost sítě v IoT systémech.**

Hlavní bezpečnostní aspekty IoT systémů jsou:

- Security by Design: zahrnout kyberbezpečnost a tedy i odborníky na ni již do návrhu IoT řešení.

- Šifrovací protokoly: Zavést šifrování pro všechny přenosy dat IoT.

- Pravidelné aktualizace softwaru: Zajistit, aby zařízení IoT mohlo přijímat aktualizace firmwaru a softwaru, aby byla chráněna před nově vznikajícími zranitelnostmi. Ideální je možnost vzdálené aktualizace FW a SW vzduchem (tzv. Over-the-air). Ovšem ne všechny IoT technologie jsou pro tento případ vhodné. To se týká zejména úzkopásmových technologií jako je NB-IoT. Dalším předpokladem efektivní aktualizace FW a SW je potom vyspělá IoT device management platforma, která to umožňuje.

Bezpečnost jako základní prvek - Security by Design v IoT systémech

„Security by Design“ znamená přístup, při kterém jsou bezpečnostní úvahy a mechanismy zabudovány do architektury a návrhu IoT systémů od samého počátku. Místo toho, aby byla bezpečnost řešena dodatečně (kdy jsou zranitelnosti opravovány později), je bezpečnost integrována během celého životního cyklu řešení IoT, včetně hardwaru, softwaru, síťových protokolů a celkové systémové architektury.

Klíčové prvky Security by Design v IoT:

- Zabezpečené hardwarové komponenty: Hardwarové bezpečnostní mechanismy, jako je zabezpečené spouštění (secure boot), důvěryhodná prostředí pro zpracování (trusted execution environment, TEE) nebo hardwarové bezpečnostní moduly (HSM), mohou zajistit, že zařízení se spustí bezpečně a že kritické operace (např. generování kryptografických klíčů) jsou izolovány od ostatních funkcí.

- Integrita firmwaru a aktualizace: IoT zařízení by měla mít mechanismy k ověření integrity svého firmwaru během spouštění a podporovat zabezpečené aktualizace over-the-air (OTA). Tyto aktualizace by měly být autentizovány a šifrovány, aby se zabránilo instalaci škodlivého firmwaru.

- Zabezpečené komunikační protokoly: Vybrat komunikační protokoly, které podporují šifrování a autentizaci nativně, nebo které lze doplnit o další bezpečnostní prvky, jako je TLS pro MQTT nebo DTLS pro CoAP.

- Autentizace a řízení přístupu: Každé IoT zařízení musí mít silnou, jedinečnou identitu. Tam, kde je to relevantní, je vhodné používat vícefaktorovou autentizaci (MFA), aby se zabránilo neoprávněnému přístupu. Role-based Access Control (RBAC) může také omezit rozsah přístupu na základě rolí uživatelů.

Mělo by být navrhování IoT systémů prováděno s odborníky na kybernetickou bezpečnost?

Rozhodně ano. Kybernetická bezpečnost by neměla být ponechána pouze na obecných systémových návrhářích nebo inženýrech, kteří nemusí mít konkrétní odborné znalosti v oblasti bezpečnosti. Je to zejména z těchto důvodů:

- Specializované znalosti: Odborníci na kybernetickou bezpečnost přinášejí hlubší znalosti o modelování hrozeb, šifrovacích standardech, správě zranitelností a bezpečné systémové architektuře. Mohou identifikovat vektory útoků a potenciální zranitelnosti již v rané fázi návrhu, které by jiní členové týmu mohli přehlédnout.

- Shoda s normami a osvědčenými postupy: Odborníci na kybernetickou bezpečnost zajišťují, že návrh odpovídá osvědčeným postupům a splňuje požadavky nařízení, jako je NIS2, GDPR, HIPAA nebo jiné místní a mezinárodní normy. Mohou také vést návrháře IoT systémů k implementaci nejnovějších doporučení pro bezpečný návrh, jako jsou ta od NIST (National Institute of Standards and Technology) a ENISA (European Union Agency for Cybersecurity).

- Průběžné monitorování: V rámci přístupu „Security by Design“ odborníci pomáhají nastavit průběžné monitorovací systémy, které dokážou detekovat a reagovat na bezpečnostní incidenty v reálném čase, čímž zajišťují stálou ochranu i po nasazení.

Jak implementovat Security by Design:

- Modelování hrozeb: Je důležité provést analýzu hrozeb již v rané fázi návrhu. Zmapovat potenciální hrozby pro systém a identifikovat kritické oblasti, které potřebují silnější bezpečnostní opatření.

- Bezpečný vývojový životní cyklus (SDLC): Součástí implementace je vývojový cyklus SDLC, který zahrnuje bezpečnostní kontrolní body v každé fázi, od návrhu až po kódování, testování a nasazení. Je potřebné zajistit, aby veškerý software byl před vydáním otestován na zranitelnosti.

- Spolupráce napříč týmy: Je vhodné přivést dohromady specialisty na bezpečnost, vývojáře, produktové designéry a síťové inženýry už v rané fázi návrhu. Tato multidisciplinární spolupráce zajistí, že bezpečnostní problémy budou řešeny ve všech vrstvách – hardwaru, softwaru a síťové infrastruktuře.

Security by Design zajišťuje, že IoT řešení jsou od základu odolná vůči útokům. Tento přístup vyžaduje úzkou spolupráci s odborníky na kybernetickou bezpečnost, jejichž znalosti v oblasti modelování hrozeb, bezpečného kódování a shody s normami jsou zásadní pro minimalizaci rizik.

Šifrovací protokoly v IoT

Šifrovací protokoly jsou algoritmy a techniky používané k zakódování dat tak, aby je mohly číst nebo k nim přistupovat pouze oprávněné strany. V IoT je šifrování zásadní pro ochranu dat přenášených mezi zařízeními, branami a backendovými systémy.

Standardně používané šifrovací protokoly v IoT:

- TLS/SSL (Transport Layer Security / Secure Sockets Layer): Používá se k zabezpečení přenosu dat přes internet. Zajišťuje šifrování od konce ke konci mezi IoT zařízeními a servery, chrání proti odposlechům, manipulacím a podvržení zpráv. TLS je široce používán v IoT zařízeních, zejména v těch, která jsou připojena ke cloudovým službám.

- DTLS (Datagram Transport Layer Security): Varianta TLS navržená pro datagramové protokoly, jako je UDP. DTLS je vhodnější pro případy použití IoT, kde zařízení spoléhají na komunikaci s nízkou latencí a bez nutnosti připojení, což je zvláště efektivní v omezených prostředích.

- AES (Advanced Encryption Standard): AES je symetrický šifrovací algoritmus běžně používaný v IoT zařízeních pro místní šifrování (např. ukládání dat na zařízení). Je lehký a efektivní, což ho činí ideálním pro zařízení s omezeným výpočetním výkonem.

- ECC (Elliptic Curve Cryptography): ECC je technika asymetrického šifrování, která poskytuje silné zabezpečení při kratších délkách klíčů ve srovnání s tradičními metodami, jako je RSA. To je důležité pro IoT zařízení s omezenými výpočetními schopnostmi, protože jim to umožňuje udržet silné šifrování bez nadměrného využívání zdrojů.

- MQTT s TLS: MQTT, populární komunikační protokol v IoT, je často kombinován s TLS pro zajištění bezpečného přenosu dat mezi zařízeními a brokery. MQTT je lehký, ale sám o sobě nemá nativní šifrování, proto se obvykle používá TLS jako dodatečná vrstva pro zabezpečení komunikace. Šifrování není tedy vždy nativní součástí IoT komunikace. Záleží na technologii a způsobu využití.

Nativní šifrování v protokolech:

Některé IoT protokoly (jako MQTT nebo CoAP) nemají nativně zahrnuto šifrování, ale spoléhají na dodatečnou vrstvu, jako je TLS/SSL, pro zabezpečení. Jiné protokoly, jako Zigbee, LoRaWAN a Z-Wave, mají vestavěné šifrovací mechanismy, většinou založené na AES, které zajišťují důvěrnost během komunikace mezi zařízeními nebo mezi zařízeními a sítí.

5G a šifrování pro IoT:

V sítích 5G je šifrování nedílnou součástí architektury sítě. 5G využívá 128bitové a 256bitové šifrování k zabezpečení komunikace, což je výrazně silnější než šifrovací metody používané ve 4G. Navíc 5G zavádí síťové segmenty (network slicing), které umožňují různým IoT aplikacím mít izolované virtuální sítě, což zajišťuje, že i když je jeden segment ohrožen, ostatní zůstanou bezpečné. Standard 5G také podporuje IPsec a šifrování od konce ke konci (end-to-end), čímž zvyšuje bezpečnost aplikací IoT, které spoléhají na mobilní sítě.

Doporučení pro šifrování v IoT:

- Používat šifrování od konce ke konci (E2EE): Zajistit, aby data byla šifrována od IoT zařízení až po backendový server. To pomáhá předcházet útokům typu man-in-the-middle (MitM) nebo odposlechům, které by mohly nastat, pokud by data byla během přenosu vystavena možnému zneužití.

- Lehké šifrovací algoritmy: Vzhledem k omezeným zdrojům mnoha IoT zařízení (např. omezená baterie, paměť a výpočetní výkon) je nezbytné používat lehké, ale silné šifrovací algoritmy, jako je ECC a AES s kratšími délkami klíčů.

5.2.2 Interoperabilita a fragmentace v ekosystému IoT

Ekosystém IoT se skládá z široké škály zařízení, platforem a komunikačních protokolů, z nichž mnohé nejsou vzájemně kompatibilní. Nedostatek standardizace vytváří fragmentaci, což ztěžuje komunikaci mezi zařízeními od různých výrobců. To brání škálovatelnosti, zvyšuje náklady na integraci a omezuje schopnost vyvíjet skutečně interoperabilní řešení.

Interoperabilita označuje schopnost různých systémů, zařízení a platforem komunikovat a bezproblémově spolupracovat. V ideálním prostředí IoT by si zařízení od různých výrobců měla být schopna vyměňovat data, interpretovat příkazy a fungovat jako součást jednotného ekosystému. Toto však v současné situaci často nefunguje.

Fragmentace znamená roztříštěnost různých technologií, standardů a protokolů, které nejsou vzájemně kompatibilní. Tato diverzita se může objevit na různých vrstvách IoT, včetně hardwaru (různá zařízení), konektivity (různé komunikační protokoly) a softwaru (různé platformy nebo datové formáty). Fragmentace může vytvářet „sila“ dat a funkcionalit, kde si zařízení nebo systémy nemohou efektivně vyměňovat informace nebo spolupracovat.

Mezi hlavní problémy patří:

- Nedostatek standardizace: Zařízení IoT využívají řadu protokolů, jako jsou MQTT, CoAP, Zigbee a LoRa. Navíc ovšem dodavatelé IoT zařízení historicky často přistupovali k implementaci proprietárních protokolů, mezi nimiž často neexistuje kompatibilita. To vede k obtížím při integraci zařízení od různých dodavatelů.

- Závislost na dodavateli (vendor lock-in): Mnoho poskytovatelů IoT vytváří proprietární systémy, které omezují křížovou kompatibilitu. To vytváří izolované systémy, kde jsou firmy vázány na konkrétní ekosystém dodavatele, což snižuje flexibilitu a zvyšuje dlouhodobé náklady.

- Nekonzistence dat: Bez společných datových formátů a standardů nemusí různé systémy IoT data interpretovat nebo používat jednotně. To může vést k nedorozumění mezi zařízeními nebo platformami, což snižuje přesnost a efektivitu provozu řízených IoT.

- Zvýšená komplexita: Čím více je ekosystém roztříštěný, tím složitější je pro firmy integrovat, spravovat a škálovat své IoT řešení. To zvyšuje celkové náklady na vlastnictví (TCO) a snižuje návratnost investic (ROI) do IoT projektů.

Pro zmírnění problémů spojených s interoperabilitou a fragmentací je možné doporučit následující kroky:

- Požadovat otevřené standardy a interoperabilitu: Firmy implementující IoT řešení by měly upřednostňovat dodavatele, kteří dodržují otevřené standardy, a vyhýbat se závislosti na proprietárních ekosystémech. To zajistí větší flexibilitu a ochrání jejich investice do IoT v budoucnu.
- Investovat do middleware řešení: V situacích, kde je nutné, aby různé systémy koexistovaly, může middleware pomoci překonat rozdíly mezi odlišnými zařízeními a protokoly. Investice do middleware platforem podporujících multi-protokolovou interoperabilitu může zjednodušit provoz a snížit složitost integrace.
  Poznámka: příkladem platformy, která umožňuje integrovat různé protokoly a různá zařízení, je IoT platforma Multi-tech Cloud společnosti ČRa, která je představena v příloze 2.
- Spolupracovat s průmyslovými stakeholdery: Zákazníci IoT by měli spolupracovat s průmyslovými skupinami a fóry, které prosazují větší standardizaci a interoperabilitu. Aktivní zapojení do těchto komunit poskytne firmám hlas při utváření budoucích standardů a zajistí, že jejich požadavky budou zohledněny.
- Pilotní provoz v prostředí s více dodavateli: Pro zabránění závislosti na jednom dodavateli, firmy by měly testovat IoT řešení v prostředí s více dodavateli před tím, než přistoupí k rozsáhlejšímu nasazení. To pomůže včas identifikovat případné problémy s interoperabilitou a zajistí hladší škálování IoT řešení.

5.2.3 Výběr a implementace komunikační IoT technologie

S komplexitou a určitou roztříštěností IoT souvisí i další výzva, které čelí nejen potenciální uživatelé IoT systémů, ale trochu paradoxně také poskytovatelé IoT řešení. Protože obě tyto skupiny stojí v případě volby přenosové technologie před náročným úkolem.

Volba přenosové technologie ovlivní vlastnosti celého IoT systému. Kromě toho determinuje typ a dostupnost koncových IoT zařízení. V případě nevhodné volby může jít opravdu o velký problém, protože změna komunikační technologie si případně vyžádá výměnu koncových zařízení, kterých mohou být v IoT systému stovky, nebo také tisíce. To je nákladné a může to být také časově velmi náročný proces. Typicky může být změna komunikační technologie větší výzva než výměna centrálního prvku, jako jde datové úložiště nebo analytické nástroje.

Přenosových technologií je poměrně velké množství, jak ostatně ukazuje kapitola 2.2. Mají objektivně různé výhody a nevýhody, není možné definovat technologii jednoznačně lepší či horší. Výběr navíc stěžuje skutečnost, že dodavatelé technologií často přináší ne zcela objektivní data ohledně jejich vlastností, dostupného pokrytí apod.

Pro výběr lze proto doporučit následující kroky:

- Seznámit se s celou škálou technologií a jejich vlastnostmi. Nápomocna v tomto směru může být i tato studie.
- Důsledně definovat případy užití, které bude IoT systém realizovat. Díky tomu je následně možné definovat požadavky těchto případů užití na IoT systém. Toto je detailně popsáno v kapitole 3.1.2.
- Pro každý případ užití je vhodné dle formuláře definovat celou sadu požadavků na IoT systém. A tyto požadavky následně porovnat s vlastnostmi technologií, které jsou popsané v kapitole 2.
- Vlastnosti a vhodnost technologie ověřit pomocí Proof of concept. V rámci PoC může být vhodné vyzkoušet a porovnat více technologií.
- Vyžadovat transparentnost poskytovatele z pohledu dlouhodobé podpory vybrané technologie. IoT projekty jsou typicky realizované s časovým horizontem 10-15 let.

Kromě technických vlastností přenosové technologie je pro uživatele IoT systémů pochopitelně důležitá také komerční, respektive nákladová stránka zvolené technologie.

Náklady spojené s používáním příslušné technologie jsou dané nejen technologií samotnou. Velkou roli hraje objem datových toků, které jsou v rámci IoT systému přenášeny. V případě IoT jsou poplatky účtovány právě v závislosti na objemu přenesených dat. Velkou roli tak hraje **optimalizace komunikace v rámci IoT systému.** Využití edge computingu a vhodné architektury může vést až k řádově odlišným datovým objemům, které jsou přenášeny, a tím i dramaticky odlišným nákladům. Při chybějící optimalizaci tak mohou provozní náklady IoT systému vést až k tomu, že celé řešení nedává ekonomický smysl, respektive business model není funkční.

5.3 Budoucnost IoT

Prostředí internetu věcí (IoT) se rychle vyvíjí a budoucí růst pohánějí četné technologické inovace. Mezi klíčové trendy patří rozvoj nových komunikačních technologií založených na 5G standardech, integrace umělé inteligence (AI) a strojového učení (ML) a rostoucí role pokročilých cloudových služeb. Tyto prvky mění způsob, jakým mohou firmy využívat IoT k dosažení vyšší efektivity a nových obchodních modelů.

Níže představujeme klíčové oblasti a další vznikající trendy, které budou definovat budoucnost IoT.

5.3.1 Nové komunikační technologie (RedCap, Passive IoT)

Přestože je už nyní k dispozici poměrně široká nabídka komunikačních technologií pro IoT, dochází i v této oblasti k neustálému vývoji, který se snaží eliminovat slabé stránky stávajících technologií a přinést technologie, které uspokojí všechny požadavky uživatelů IoT systémů.

Jedním vývojovým směrem je potřeba poskytnout technologii, která:

- bude plně kompatibilní s 5G ekosystémem,
- zajistí vysokou bezpečnost,
- poskytne dostatečně rychlé datové přenosy,
- bude tak vhodná i pro business kritické aplikace a případy užití,
- a to při nákladech, které nebudou omezovat realizaci IoT projektů.

Tento vývojový směr přináší technologii **RedCap** a její evoluci.

RedCap je funkce 5G, která poskytuje kompromis mezi vysoce výkonnými 5G zařízeními a nízkonákladovými IoT zařízeními. Podporuje datové rychlosti a funkce optimalizované pro IoT aplikace, jako jsou chytré nositelné zařízení, průmyslové senzory a další použití, která nevyžadují plnou šířku pásma 5G. RedCap nabízí sníženou složitost zařízení a nižší spotřebu energie, což z něj činí nákladově efektivní možnost pro nasazení IoT ve velkém měřítku, přičemž stále těží z nízké latence a spolehlivosti sítí 5G.

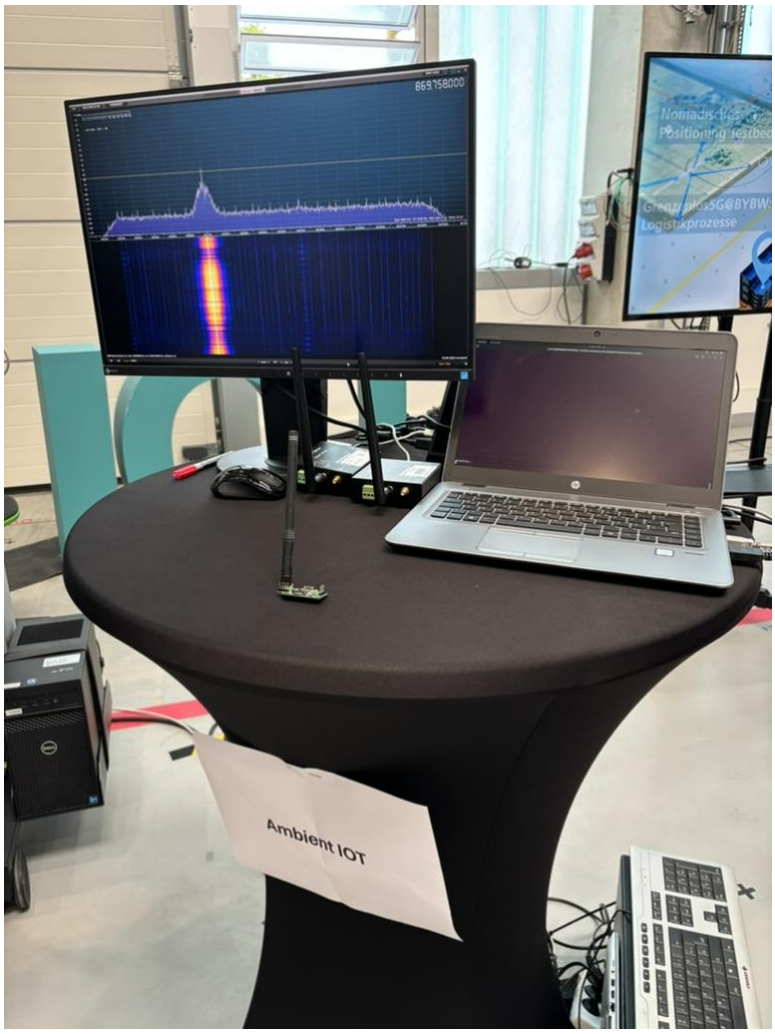
Technologie RedCap je v tuto chvíli (k datu vydání této studie) již v omezené míře dostupná. Někteří asijští dodavatelé již nabízejí možnost implementace RedCap na úrovni privátních 5G sítí. Existuje jen omezený ekosystém zařízení. Lze ovšem očekávat, že šíře ekosystému RedCap se bude plynule rozšiřovat v následujících měsících a letech.

Na další straně vývoje je potřeba ještě nižších nákladů a ještě nižší spotřeby energie zejména na straně koncových zařízení, což by umožnilo mnohem masivnější nasazení IoT a díky tomu digitalizaci oblastí, pro které je stále příliš nákladná. Tento směr vývoje reprezentuje **Passive IoT**.

Pasivní IoT zařízení, jako jsou pasivní tagy a senzory bez baterií, mohou fungovat bez tradičních zdrojů energie, místo toho využívají energii ze svého okolí (např. elektromagnetické vlny, světlo nebo teplo). Tato technologie výrazně snižuje náklady na nasazení a údržbu, což umožňuje propojení velkého množství malých, nízkonákladových zařízení v odvětvích, jako je logistika, výroba, maloobchod, zdravotnictví a zemědělství. Pasivní IoT může být revoluční v aplikacích, kde jsou kritické požadavky na velikost, spotřebu energie a náklady.

Passive IoT, jak je popsáno v kapitole 2.3, bude přicházet v několika fázích. V tuto chvíli tato technologie není v Evropě dostupná, první experimentální implementace běží v Číně.

Nicméně ani evropské výzkumné organizace a výrobci nechtějí zůstat pozadu. Například německý Fraunhofer IIS pracuje na vlastní koncepci Passive IoT, kterou nazývá Ambient IoT. Podstata technologie je stejná, pracuje s technikou zpětného rozptylu signálu. Snaží se ovšem vyjít vstříc evropskému regulačnímu prostředí a pro zpětný rozptyl využít stávající zdroje signálu, místo aktivně generovaného signálu. Řešení je ještě v poměrně rané fázi výzkumu, zařízení zatím pracuje s malou baterií, cílem je dosáhnout zcela pasivního zařízení.



Obrázek 12: Experimentální zařízení pro Ambient IoT využívající „back scattering“. Zdroj: Fraunhofer IIS, 5G Connect Advanced (19.9.2024).

5.3.2 AI/ML pro pokročilou analýzu dat

Integrace umělé inteligence (AI) a strojového učení (ML) proměňuje prostředí IoT díky možnosti pokročilé analýzy dat. Tu je možné využít například k prediktivní údržbě, detekci anomálií a obecně automatizaci. AI a ML algoritmy zpracovávají velké množství dat generovaných IoT zařízeními, čímž převádějí surová data na akční informace, které přinášejí podnikům skutečnou hodnotu.

Jakkoli jsou AI/ML modely nesmírně komplexní záležitostí, pro poskytovatele i uživatele IoT služeb je k dispozici stále více produktů, které umožňují prakticky využít AI/ML nástroje v rámci IoT systémů, aniž by bylo nutné disponovat specifickým know-how. To nepochybně povede k rychlému rozšíření těchto nástrojů. Jejich použití přinese značnou přidanou hodnotu například v následujících oblastech:

- Prediktivní údržba: AI modely dokáží předpovědět poruchy zařízení před jejich skutečným výskytem, což snižuje prostoje a náklady na údržbu. To je zvláště cenné v odvětvích, jako je výroba, energetika a doprava, kde mohou neplánované výpadky být velmi nákladné.

- Detekce anomálií a kontrola kvality: ML algoritmy dokážou v reálném čase detekovat vzory a odchylky, což umožňuje okamžité korektivní zásahy ve výrobních linkách nebo dodavatelských řetězcích. Díky tomu je dosaženo lepší kontroly kvality a snížení odpadu, což přímo ovlivňuje provozní efektivitu.

- Automatizace a rozhodování: Automatizace řízená AI umožňuje IoT systémům rozhodovat autonomně, od optimalizace spotřeby energie v chytrých budovách po úpravu výrobních parametrů v reálném čase ve výrobních závodech. To snižuje potřebu lidského zásahu a výrazně zlepšuje procesní efektivitu.

5.3.3 Cloudové služby (AWS IoT, Azure IoT, Google Cloud IoT)

Cloudové platformy hrají stále důležitější roli v IoT tím, že poskytují robustní a škálovatelnou infrastrukturu, která zjednodušuje nasazení a správu IoT řešení. Služby nabízené platformami jako AWS IoT, Microsoft Azure IoT a Google Cloud IoT poskytují výkonné nástroje, které umožňují vyvíjet, připojovat a spravovat IoT zařízení s minimálním úsilím.

Cloudové platformy umožňují firmám flexibilně škálovat své IoT systémy bez nutnosti výrazných počátečních investic (CAPEX). Nabízejí flexibilní modely cen podle využití, díky čemuž je IoT dostupné pro podniky všech velikostí.

Poznámka: Určitá investice je pochopitelně nutná do HW v podobě koncových zařízení.

Moderní cloudové IoT platformy nabízejí pokročilé funkce, jako je analýza dat v reálném čase, správa zařízení a monitorování bezpečnosti prostřednictvím uživatelsky přívětivých rozhraní. To demokratizuje přístup ke sofistikovaným IoT schopnostem, což umožňuje firmám nasazovat komplexní IoT řešení na několik kliknutí.

Pokročilé cloudové IoT platformy nyní nemusí fungovat jen jako centrální prvky, ale podporují Edge computing, který přináší zpracování dat blíže ke zdroji jejich generování. To snižuje latenci, náklady na šířku pásma a zvyšuje ochranu dat, což činí IoT aplikace více responzivními a efektivními.

Bližší popis sady cloudových IoT produtků AWS je jako příklad tohoto typu služeb uveden v Příloze 1.

5.3.4 Zvýšená bezpečnost a ochrana soukromí

S tím, jak se sítě IoT rozšiřují, se stává důležitějším zajištění robustní bezpečnosti a ochrany soukromí. Kybernetické hrozby se vyvíjejí souběžně s technologií IoT, což vyžaduje pokročilé přístupy k ochraně integrity, důvěrnosti a dostupnosti dat.

Kromě již výše uvedených přístupů (viz kapitola Výzvy spojené s IoT) jako „Security by Design“ a důraz na end-to-end použití šifrovacích protokolů, je možné kybernetickou bezpečnost IoT systémů do budoucna posílit využitím pokročilých technologií jako blockchain a moderním přístupem „Zero Trust“.

- Využití blockchain pro bezpečnost IoT: Blockchain technologie je předmětem zkoumání pro svůj potenciál zvýšit bezpečnost IoT díky poskytování decentralizovaných, nezměnitelných záznamů IoT transakcí a interakcí zařízení. Tato technologie může snížit rizika spojená s úniky dat a neoprávněným přístupem.

- Modely Zero Trust bezpečnosti: Přijetí architektur Zero Trust, které vyžadují nepřetržité ověřování zařízení a datových toků, může významně zlepšit bezpečnostní postavení IoT ekosystémů. Tento přístup předpokládá, že hrozby mohou přijít jak zevnitř, tak zvenčí sítě, a klade důraz na přísné procesy autentizace a autorizace.

5.3.5 Zlepšení v oblasti interoperability a standardizace IoT

Nedostatek interoperability mezi různými IoT zařízeními a platformami stále představuje významnou překážku pro rozšíření adopce. Ostatní proto je interoperabilita a fragmentace IoT ekosystému uvedena mezi hlavními výzvami pro IoT

Budoucnost IoT pravděpodobně přinese, kromě využití různých middleware platforem, větší snahy o standardizaci a vývoj univerzálních protokolů, které umožní bezproblémovou integraci napříč různými IoT ekosystémy.

V průmyslovém prostředí bude hrát důležitou několik protokolů, které mají význam pro IoT a pokročilou automatizaci a robotizaci. Jedná se zejména o **MQTT, OPC UA, průmyslový Ethernet a TSN**.

V případě spotřebitelského IoT je dobrým příkladem úsilí o interoperabilitu projekt **Matter**.

Matter je open-source standard pro konektivitu chytrých domácích zařízení, vyvinutý aliancí Connectivity Standards Alliance (CSA), dříve známou jako Zigbee Alliance. Cílem Matter je zlepšit interoperabilitu mezi IoT zařízeními tím, že jim umožní komunikovat bez ohledu na výrobce, platformu nebo komunikační protokol. Matter usiluje o zjednodušení ekosystému chytré domácnosti tím, že zajistí, aby zařízení od různých značek mohla spolehlivě a bezpečně spolupracovat.

Matter zavádí společný jazyk pro IoT zařízení, což umožňuje jejich spolupráci napříč ekosystémy, jako jsou Apple HomeKit, Google Home, Amazon Alexa a Samsung SmartThings. Toho dosahuje definováním univerzální aplikační vrstvy pro chytrá domácí zařízení. Matter zahrnuje robustní bezpečnostní protokoly, včetně autentizace zařízení a šifrování, což zajišťuje integritu dat a chrání soukromí uživatelů.

Matter také zjednodušuje nastavení a provoz zařízení, což uživatelům usnadňuje přidávání zařízení do jejich chytrých domácích sítí. Zařízení lze snadno nastavit pomocí QR kódů nebo NFC štítků, což zjednodušuje onboarding. Protokol je navržen tak, aby fungoval napříč různými komunikačními technologiemi, včetně Wi-Fi, Thread a Ethernet, což poskytuje flexibilitu v tom, jak zařízení v chytré domácnosti komunikují. Je založen na open-source principech, což umožňuje vývojářům a výrobcům přispívat k rozvoji standardu a podporovat inovace a široké přijetí.

Matter zařízení komunikují prostřednictvím sdíleného protokolu, což jim umožňuje vzájemně se objevovat, interagovat a fungovat společně. Například Matter certifikovaná chytrá žárovka může spolupracovat s Matter kompatibilní chytrou domácí aplikací, bez ohledu na to, zda je žárovka od Philipsu a aplikace od Apple, Google nebo Amazonu. Tato kompatibilita napříč značkami představuje významnou změnu oproti minulosti, kdy chytrá domácí zařízení často vyžadovala specifické huby nebo aplikace spojené s danou značkou.

Příklad použití Matter: Chytré HVAC systémy.

Matter kompatibilní termostat, teplotní senzory a chytré větráky se používají pro řízení vytápění a chlazení domácnosti. Tato zařízení mohou koordinovat akce automaticky. Například když termostat detekuje změnu teploty, může signalizovat větrákům, aby upravily průtok vzduchu, i když jsou tato zařízení od různých výrobců.

Zásadní je, že Matter získal významnou podporu od hlavních technologických společností, včetně Apple, Google, Amazon a Samsung, stejně jako od výrobců zařízení, jako jsou Philips, Yale a IKEA. Tyto společnosti aktivně pracují na certifikaci svých stávajících i budoucích produktů s Matter, což urychluje přijetí standardu.

Matter řeší jeden z největších problémů v odvětví chytré domácnosti, tedy fragmentaci. Nabídkou univerzálního standardu Matter výrazně snižuje složitost pro spotřebitele i vývojáře, což činí chytrá domácí zařízení přístupnějšími a spolehlivějšími. Jak se jeho přijetí rozrůstá, očekává se, že Matter se stane de facto standardem pro konektivitu v chytrých domácnostech, což zjednoduší způsob, jakým interagujeme s IoT zařízeními a využíváme jejich výhody v našem každodenním životě.

Matter tak představuje významný krok vpřed v IoT ekosystému, zlepšuje interoperabilitu zařízení, bezpečnost a uživatelskou zkušenost. Otevírá nové příležitosti pro podniky a spotřebitele a činí technologii chytrých domácností více soudržnou a praktickou než kdy dříve.

Budoucnost IoT je formována technologickými inovacemi zejména v oblasti komunikačních technologií, AI/ML a cloudových služeb. Spolu se zlepšováním bezpečnosti a interoperabilty tyto inovace pohánějí vývoj inteligentnějších, nákladově efektivnějších a škálovatelnějších IoT řešení, která mohou pomoci transformovat průmyslová odvětví a odemykat nové obchodní modely. Díky tomu budou firmy a poskytovatelé služeb moci plně využít potenciál IoT.

Příloha 1 - AWS IoT: sada cloudových produktů pro oblast IoT

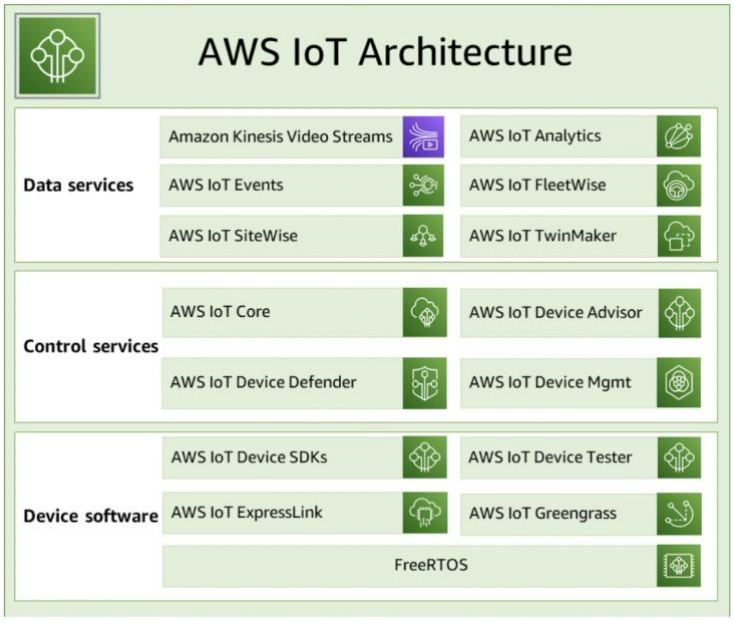
Základní informace o poskytovateli služeb – Amazon Web Services

Amazon Web Services (AWS), divize společnosti Amazon, je globálním lídrem v poskytování cloudových řešení. AWS poskytuje široké portfolio služeb, které zahrnují výpočetní výkon, úložiště, databáze a analytické nástroje, ale také komplexní služby pro Internet věcí (IoT). AWS díky své flexibilitě, globální infrastruktuře a bezpečnostním standardům umožňuje firmám rychle digitalizovat své procesy a využívat nejmodernější technologie pro IoT.

Zákazníci a jejich potřeby

Zákazníci AWS IoT služeb jsou podniky z různých odvětví, jako je průmysl, energetika, zemědělství, zdravotnictví nebo logistika. Tito zákazníci hledají řešení, která jim umožní efektivněji spravovat své procesy pomocí automatizace, monitorování a analýzy dat v reálném čase. Potřebují robustní a bezpečné prostředí pro připojení, správu a analýzu dat z velkého počtu IoT zařízení, a to často v globálním měřítku.

Popis produktu (AWS IoT)



Obrázek 13: Přehled AWS IoT architektury. Zdroj: [27]

AWS IoT zahrnuje několik klíčových produktů, které společně tvoří komplexní platformu pro IoT řešení. Produkty je možné rozdělit do 3 oblastí (viz obrázek výše):

- Datové služby – pro zpracování, ukládání a analýzu dat.
- Kontrolní služby – pro správu zařízení a bezpečnost.
- Software zařízení – pro připojení a interoperabilitu IoT zařízení.

[27] https://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html

Níže jsou uvedeny hlavní produkty a jejich podrobnější popis:

1. AWS IoT Core

AWS IoT Core je základní služba, která umožňuje připojení IoT zařízení ke cloudu AWS a vzájemnou komunikaci mezi těmito zařízeními. IoT Core podporuje komunikační protokoly jako MQTT, HTTPS a LoRaWAN. Výhodou je bezpečné připojení zařízení pomocí certifikátů X.509 a pravidelné aktualizace bezpečnostních standardů.

IoT Core umožňuje snadnou integraci s ostatními službami AWS, jako jsou Amazon DynamoDB, AWS Lambda nebo Amazon S3, což znamená, že data ze zařízení mohou být analyzována nebo uložena bez nutnosti manuálních zásahů.

2. AWS IoT Greengrass

AWS IoT Greengrass přináší výpočetní výkon blíže k zařízením – tedy na tzv. "edge" úrovni. To znamená, že IoT zařízení mohou zpracovávat data lokálně a reagovat v reálném čase, aniž by musela neustále komunikovat s cloudem. Tento model snižuje latenci a náklady na přenos dat a je ideální pro aplikace, kde je rychlá reakce klíčová, například v průmyslové automatizaci nebo zdravotnictví. Greengrass podporuje také offline provoz a automatické synchronizování dat, jakmile je připojení obnoveno.

3. AWS IoT Device Management

Tato služba usnadňuje správu velkého množství zařízení, jejich monitorování, aktualizaci a diagnostiku. S AWS IoT Device Management mohou organizace snadno organizovat zařízení do skupin, monitorovat jejich zdravotní stav, spravovat softwarové aktualizace a nastavovat bezpečnostní zásady pro jednotlivá zařízení nebo jejich skupiny.

To umožňuje efektivní řízení celé flotily IoT zařízení, což je zásadní pro velké organizace, které nasazují tisíce zařízení v různých lokalitách.

4. AWS IoT Device Defender

AWS IoT Device Defender je bezpečnostní služba, která neustále monitoruje IoT zařízení a zajišťuje jejich bezpečný provoz. Kontroluje, zda nastavení zařízení splňuje bezpečnostní standardy, a upozorňuje na potenciální hrozby, jako je neoprávněné použití certifikátů nebo podezřelé aktivity zařízení.

Výhodou této služby je, že organizace mohou rychle reagovat na bezpečnostní problémy a chránit svá data a zařízení před kybernetickými útoky.

5. AWS IoT Analytics

AWS IoT Analytics umožňuje snadnou analýzu dat z IoT zařízení. Automatizuje kroky, jako je filtrování, transformace a obohacení dat, aby byla připravena pro analýzu. Analytická data jsou ukládána v časových řadách, což umožňuje pokročilé analýzy a predikce. K analýze lze využít jak standardní SQL dotazy, tak i nástroje strojového učení.

To umožňuje firmám lépe pochopit své operace, identifikovat trendy a anomálie a optimalizovat procesy.

6. AWS IoT Events

AWS IoT Events monitoruje data ze senzorů a automaticky detekuje předdefinované události nebo anomálie. Příkladem může být detekce pohybu nebo změny teploty, které spustí další akce, jako je aktivace alarmu nebo spuštění stroje. Tato služba je klíčová pro aplikace, které vyžadují okamžitou reakci na změny v reálném čase.

7. AWS IoT SiteWise

AWS IoT SiteWise je služba zaměřená na průmyslové firmy, která usnadňuje sběr, strukturování a analýzu dat z průmyslových zařízení a senzorů. Pomocí SiteWise mohou podniky snadno monitorovat a analyzovat provozní data z různých zařízení, což umožňuje optimalizaci výroby a snížení prostojů.

Proč zvolit AWS IoT řešení?

AWS IoT nabízí několik klíčových výhod oproti jiným možnostem:

- Škálovatelnost a globální dostupnost: AWS má jednu z nejrozsáhlejších globálních sítí datových center, což znamená, že zákazníci mohou snadno škálovat svá IoT řešení a zajistit jejich dostupnost po celém světě.

- Bezpečnost: AWS je známý svými vysokými bezpečnostními standardy. IoT řešení AWS nabízí integrovanou bezpečnost na úrovni zařízení i cloudu, včetně end-to-end šifrování a bezpečného ověřování zařízení pomocí certifikátů.

- Integrace s dalšími AWS službami: Jednou z největších výhod AWS je hluboká integrace s dalšími cloudovými službami, jako je strojové učení, analýza dat nebo databázové systémy. To umožňuje snadné rozšíření IoT řešení o pokročilé analytické a prediktivní funkce.

- Flexibilita a podpora různých protokolů: AWS IoT podporuje různé komunikační protokoly, včetně MQTT, HTTPS, LoRaWAN a dalších, což umožňuje firmám snadno integrovat různá zařízení do jednoho IoT ekosystému.

Podstatnou výhodou je možnost analyzovat data s využitím pokročilého Machine Learning. IoT Analytics umožňuje připravit data tak, aby šla snadno analyzovat pomocí AWS nástroje SageMaker.

Amazon SageMaker je cloudová platforma pro vývoj, trénování a nasazení modelů strojového učení (ML). U IoT projektů lze SageMaker použít k analýze velkého množství nestrukturovaných dat generovaných zařízeními IoT. SageMaker umožňuje firmám:

- Vytvářet prediktivní modely: Na základě historických dat může SageMaker identifikovat vzory, anomálie nebo trendy, které napomáhají predikci budoucích událostí (například prediktivní údržba strojů).

- Zpracovávat a analyzovat data v reálném čase: SageMaker v kombinaci s Amazon Kinesis dokáže analyzovat IoT data v reálném čase, což je klíčové pro aplikace, jako je monitorování zdravotního stavu zařízení nebo predikce havárií.

- Automatizace strojového učení: SageMaker podporuje nasazení modelů ML přímo do edge zařízení (např. pomocí AWS IoT Greengrass), což umožňuje rychlé zpracování dat bez nutnosti odesílat je do cloudu .

Kompatibilita 5G zařízení s AWS IoT

AWS IoT podporuje připojení 5G zařízení a umožňuje využití pokročilých komunikačních protokolů pro efektivní správu a přenos dat. Základní protokoly, které by měla 5G zařízení používat pro bezproblémovou integraci s AWS IoT, zahrnují:

- MQTT (Message Queuing Telemetry Transport): Tento lehký protokol je ideální pro zařízení IoT s omezenými zdroji a přenos dat přes 5G sítě, poskytuje nízkou latenci a spolehlivou komunikaci.

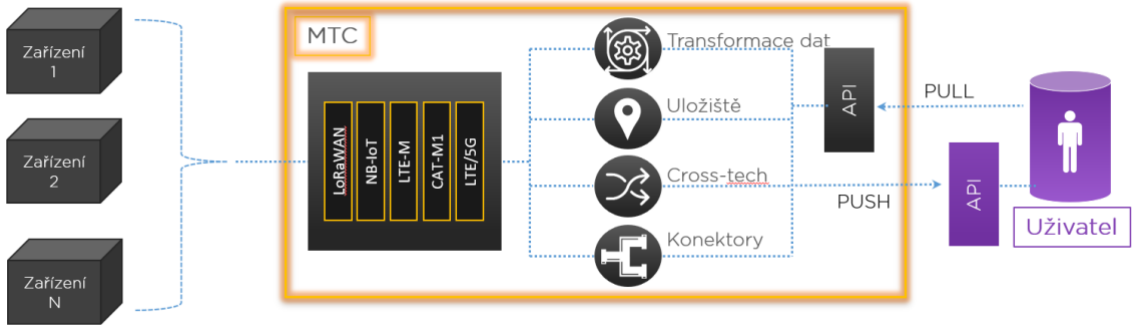
- HTTPS: Používá se pro přenosy dat mezi zařízeními IoT a službami AWS IoT s vysokou úrovní zabezpečení.

- TLS (Transport Layer Security): Verze TLS 1.3 se používá k zabezpečení komunikace mezi 5G zařízeními a AWS IoT .

AWS IoT ve spojení s 5G sítěmi a výkonnými analytickými nástroji jako je SageMaker umožňuje firmám vytvářet robustní IoT řešení s vysokou spolehlivostí, rychlou odezvou a bezpečnou správou dat.

Příloha 2 - Multi-tech Cloud společnosti České Radiokomunikace

MTC je srdcem IoT služeb ČRa. Každý zákazník, který využívá jak LoRaWAN tak SIM služby ČRA tak dostane přístup do platformy, kde si může své služby spravovat a řídit si tak všechny své IoT technologie a IoT zařízení z jednoho místa. Díky pokročilým funkcím MTC se může veškerý datový tok ze všech IoT zařízení agregovat v MTC a je doručován uživateli ve standardizovaném formátu na produkční server zákazníka. MTC není samostatnou službou, ale je standardní součástí jakékoliv IoT komunikační služby CRA – Připojení k IoT síti LoRa, Připojení přes MQTT, Připojení přes UDP, Připojení přes Data SIM. Tato prémiová nadstavba, jež se standardní součástí IoT služeb, dává zákazníkům novou úroveň přidané hodnoty, kdy kromě přenosu dat z IoT zařízení dojde k pokročilému processingu dat, aby se data ze všech technologií doručila ve stejném formátu a na stejný server zákazníka.



Obrázek 14: Schéma integrační platformy MTC. Zdroj: ČRa.

Jak to funguje

Jedná se o platformu, jejíž primární účel je směrování a transformace dat z IoT zařízení, device management, user management, ukládání dat a service management. Data přirozeně procesuje jak z LoRaWAN zařízení využívajících IoT síť CRA, ze zařízení připojených k internetu prostřednictví lokální sítě anebo ze SIM karet u zařízení využívajících technologii NB-IoT, LTE-M, CAT-M1 a LTE/5G. Podporuje nejpoužívanější komunikační protokoly LoRaWAN, MQTT, http a UDP.

Výhody

- Výrazně sníží potřebu transformace dat na straně zákazníka
- Jedno místo, kde spravuji svoje IoT, jedno SLA, jeden dodavatel
- SIM komunikaci rozšiřuje i o směrování dat na straně platformy
- Možnost individuálních transformací dle vlastních podmínek
- Možnost přeposílat data ze SIM na LoRa zařízení a naopak
- Konektory na napojení na nejpoužívanější datové nástroje
- Otevřené, dokumentované API
- Ukládání dat

Kdo je zákazník

- Dodavatelé IoT řešení
- ICT Integrátoři
- IoT operátoři
- Každý, kdo kombinuje LoRaWAN a další technologie

Funkce řešení MTC

- Směrování dat – Stejně jako u LoRaWAN, lze data z NB-IoT zařízení nasměrovat do MTC, kde se data zpracují a doručí se na jedno REST API zákazníka
- Transformace dat – data ze všech technologií se transformují do stejného formátu
- Uložiště dat – data se ukládají v interní databázi MTC
- Cross Tech – zprávy z LoRaWAN lze doručit na NB-IoT, CAT-M1, LTE-M zařízení a naopak
- Konektory – konektory na více než 250 renomovaných platforem jakou jsou AWS, Azure, Microsoft, Google, Oracle, Snowflake, MySQL, Databricks atd.
- Device management – správa IoT zařízení, evidence nastavení, popisy
- User management – vytváření projektů, uživatelů, hierarchie a oprávnění
- Service management – doobjednávání SIM karet, správa tarifů,

Příloha 3 - Platforma Conexa pro mezinárodní IoT pokrytí

Společnost Wireless Logic patří mezi leadery v oblasti zajištění konektivity pro internet věcí (IoT). Zajišťuje propojení fyzického a digitálního světa bezproblémovými, bezpečnými a škálovatelnými řešeními pro podniky v jakémkoli sektoru.

Globální nasazení IoT řešení představuje značné výzvy pro výrobce zařízení, poskytovatele řešení a také firmy, které IoT řešení chtějí a potřebují využívat. Složitost provozu v různorodých obchodních, technologických a regulačních prostředích vyžaduje robustní řešení, která dokážou tyto výzvy bez problémů zvládnout. Conexa, komplexní řešení od společnosti Wireless Logic, splňuje tyto požadavky tím, že využívá pokročilé SIM technologie—eSIM, iSIM a multi-IMSI—k optimalizaci globální IoT konektivity, snížení provozních nákladů a zvýšení celkové efektivity.

Výzvy v globálním nasazování IoT:

Mezinárodní nasazování IoT zařízení vyžaduje orientaci v komplexním prostředí mobilních operátorů (MNO), z nichž každý má své vlastní obchodní zájmy, regulační omezení a různé úrovně kvality služeb. Tradiční roamingové SIM karty, i když jsou běžně používány pro globální konektivitu, přinášejí omezení, jako je omezená kontrola nad výběrem sítě, vyšší latence a potenciální omezení v důsledku místních předpisů. Kromě toho obavy o suverenitu a bezpečnost dat dále komplikují prostředí, protože různé země ukládají různé požadavky na ukládání a přenos dat.

Problém zvládnutí globálního nasazení IoT pomůže vyřešit platforma Conexa:

Conexa je škálovatelná platforma enterprise úrovně, která integruje silné stránky technologií multi-IMSI a eSIM/iSIM a poskytuje komplexní službu pro své uživatele. Podporuje celý životní cyklus IoT zařízení—od počátečního továrního testování přes nasazení, průběžnou správu až po případné opětovné nasazení. Conexa zajišťuje, že zařízení zůstávají v souladu s místními předpisy, dosahují optimální konektivity a minimalizují provozní náklady, což z ní činí ideální řešení pro nadnárodní nasazení IoT.

Technologie eSIM a iSIM:

Conexa využívá technologie eSIM (embedded SIM) a iSIM (integrated SIM), které umožňují vzdálený provisioning SIM karet (RSP). Tyto technologie umožňují správu SIM profilů přes vzduch (OTA), což umožňuje bezproblémové přepínání mezi sítěmi bez nutnosti fyzické výměny SIM karet. eSIM a iSIM zvyšují flexibilitu a škálovatelnost IoT nasazení tím, že umožňují zařízení vzdáleně rekonfigurovat, čímž zajišťují nepřetržitou konektivitu a dodržování místních předpisů.

Funkce multi-IMSI SIM:

Funkcionalita multi-IMSI SIM v rámci Conexa umožňuje, aby jedna SIM karta uchovávala více mezinárodních mobilních identit účastníků (IMSI), což umožňuje zařízením přepínat mezi různými sítěmi podle potřeby. To zajišťuje optimální pokrytí, redundanci a dodržování místních předpisů, které mohou omezovat trvalý roaming. Applet na SIM kartě pro správu profilů autonomně vybírá vhodné IMSI na základě předem definovaných pravidel, čímž optimalizuje konektivitu napříč různými regiony bez nutnosti ručního zásahu.

Výhody platformy a SIM karty Conexa:

Využitím více předinstalovaných IMSI zajišťují SIM karty Conexa maximální pokrytí a redundanci sítě, což zvyšuje spolehlivost napříč různými geografickými regiony.

Soulad s regulací: Conexa umožňuje bezproblémové přepínání na místní sítě, čímž zajišťuje dodržování zákonů o suverenitě dat a dalších regulačních požadavků v různých zemích.

Optimalizace nákladů: Díky možnosti aktualizace profilů přes vzduch umožňuje Conexa dynamický výběr nejvýhodnější sítě, čímž snižuje celkové provozní náklady.

Flexibilita a škálovatelnost: Conexa podporuje různé formáty (SIM karty, eSIM, iSIM), Conexa je přizpůsobitelná specifickým obchodním potřebám a regulačním prostředím, což z ní činí řešení odolné vůči budoucnosti pro globální IoT operace.

Conexa od Wireless Logic nabízí robustní řešení pro globálního nasazování IoT. Integrací nejmodernějších SIM technologií s komplexní platformou pro správu usnadňuje Conexa bezproblémovou mezinárodní konektivitu, optimalizuje využívání sítě a zajišťuje dodržování místních předpisů. Toto řešení umožňuje firmám překonat tradiční výzvy mezinárodní konektivity IoT a zajišťuje efektivní, spolehlivé a nákladově efektivní provoz po celém světě.

Příloha 4 - Případová studie: virtuální IoT senzory od InovecTech

Základní informace o poskytovateli řešení

InovecTech je globálním průkopníkem technologie virtuálních IoT senzorů ve výrobě, což je přístup využívající umělou inteligenci k flexibilnímu sběru dat z výrobních prostor, skladů a dopravy. Edge zařízení s kamerami je rychle nasazeno a okamžitě začne sbírat vizuální data. Umělá inteligence s člověkem ve smyčce, rozdělena do více vrstev mezi edge a cloud, analyzuje tato data do snadno interpretovatelných a ověřitelných signálů, které mohou pohánět digitální dvojčata v reálném čase a být využity k optimalizaci procesů a rozhodování.

Zákazníci, uživatelé a jejich potřeby

Výroba je proces neustálého boje s variabilitou. Zdánlivě malá konkurenční výhoda optimalizace konverzních nákladů pomocí vylepšování procesů může znamenat rozdíl mezi úspěchem a zánikem. Pro zlepšování výroby jsou potřebná vhodná, jednoduše interpretovatelná a dostupná data, což dosahujeme digitalizací výroby. Konvenční metody pro digitalizace výroby jsou velmi pomalé, nákladné a neefektivní. Zapojení fyzických (neboli hardwarových) senzorů vyžaduje dlouhé plánování, testování a zahrnutí expertů do interpretace, co omezuje a zpomaluje implementaci, a tím znemožňuje digitalizaci malých podniků, pro které flexibilita je klíčová. Pro úspěšné zavedení digitalizace je klíčové, aby byla realizována rychle, bez nutnosti vysokých vstupních investic a s rychlou návratností, která nenaruší cashflow firmy. Virtuální senzory umožňují digitalizovat výrobu mnohem rychleji a lépe se přizpůsobí potřebám podniku. InOEE, MES na bázi virtuálních senzorů umožňuje sbírání a vyhodnocování dat z výrobních zařízení, což vede k vyšší efektivitě díky rychlejšímu odstraňování problémů, zlepšení statistických analýz a zvýšení transparentnosti výrobních procesů.

Případ užití:

Firma má většinu biznisu jako Tier2 automotive dodavatel. Společnost má 6 hlavních velkých výrobních prostředků - lisy o tonáži nižší stovky tun. Každý lis měl svůj řídící systém, ale žádný lis neměl zaveden systém sběru relevantních dat do centrálního úložiště, což komplikovalo možnost začít rychle analyzovat a zvyšovat efektivitu výroby. OEE jednoho ze strojů dosahovalo pouhých 40 % a bez dostupných dat se nedařilo tuto hodnotu zvýšit.

Produkt/řešení a jeho implementace

Produkt InOEE, MES pro MSP na bázi umělé inteligence instalovatelný za 1 den, funguje na principu sběru dat pomocí kamer umístěných ve výrobních halách, které nahrávají výrobní zařízení. Tyto záznamy jsou následně zpracovány výpočetní kapacitou přímo na místě (on-premises). Technologie virtuálních senzorů transformuje obrazová data na signály, jež odpovídají výstupům hardwarových senzorů, například, signál odpovídající, zda je lis otevřený nebo zavřený. Tato data jsou dále zpracována na užitečné informace pro lidi, jako jsou časy cyklů, vytíženost strojů a rozpad ztrát, což umožňuje detailní analýzu efektivity výrobních zařízení. Na cloudu probíhá monitoring a trénování umělé inteligence, která se postupně zlepšuje a učí z dat, tím zvyšuje přesnost, spolehlivost a rozšiřuje aplikovatelnost tradičních i pokročilých analýz. Výsledky jsou zákazníkovi prezentovány prostřednictvím přehledných webových dashboardů nebo online tabulek podle jeho potřeb. Například pareto analýza nebo OEE vodopád s rozpadem ztrát, přehled počtu vyrobených kusů a OEE za posledních několik směn atd. Systém je navržen tak, aby komunikoval s cloudem, přičemž data zůstávají u zákazníka, kromě jednotlivých obrázků z videí, které jsou potřebné pro trénování neuronových sítí. Důležitou součástí řešení je umělá inteligence s člověkem ve smyčce, kde anotátor připojený na cloud klasifikuje situace, kdy umělá inteligence nesprávně vyhodnotila stav, což zajišťuje neustálé zlepšování systému a jeho rychlé nasazení, neboť není třeba sbírat týdny kamerových záznamů, ale stačí hodiny. Tento monitoring spolehlivosti

umožňuje rychlé prakticky okamžité nasazení, a zároveň vysokou spolehlivost a nízké náklady. Kromě samotných kamerových záznamů je vhodný mít vstup od operátora, který například na tabletu nainstalovaném ve výrobě může klasifikovat důvody zastavení výrobního zařízení.

První den až dva jsme se instalovali HW, kamery, výpočetní kapacitu a instalovali ethernetovou kabeláž. Třetí den začal první sběr dat, který sloužil jako základ pro kalibraci systému a identifikaci klíčových bodů výrobního procesu. Během prvního až druhého měsíce probíhalo ladění sběru dat, přizpůsobování zákaznického rozhraní a definování konkrétních typů dat, která měla být sbírána a vyhodnocována, například detailní měření OEE po minutě. Po této fázi následoval ostrý provoz, který byl zahájen od třetího měsíce, kdy byl systém plně připraven na standardní výrobu a analýzy. Jednalo se o první implementaci svého druhu, proto bylo nutné pečlivě vyladit všechny parametry. Při dalších implementacích očekáváme, že ostrý provoz bude zahájen již od 5. dne, a to zejména u standardních typů analýz, kde jsme schopni rychle přejít na plně funkční systém.

5G/P5G

5G není zcela nevyhnutné pro digitalizaci pomocí virtuálních senzorů. Ale vzhledem k tomu, že virtuální senzory přenáší obraz s vysokým rozlišením, představuje využití privátní 5G sítě zajištění skutečně stabilní a dostatečně kvalitní služby. Další velkou výhodou využití privátní 5G sítě je možnost flexibilního umisťování a přemísťování virtuálních senzorů.

Proč bylo toto řešení vybráno

Řešení bylo vybráno díky své rychlosti nasazení, která umožňuje rychlý sběr a analýzu dat již během několika dní od instalace. Flexibilita systému zaručuje snadné přizpůsobení různým typům výrobních zařízení a procesů bez nutnosti složitých úprav. Důležitým přínosem je také zamezení tzv. data waste, kdy systém sbírá pouze relevantní data, která jsou nezbytná pro zvýšení efektivity, a minimalizuje tak zbytečný objem nepotřebných informací. Navíc je řešení cenově dostupné, což umožňuje nasazení i v menších podnicích bez nutnosti vysokých vstupních investic.

Status projektu

Projekt ve aktuálně v provozu. Plánuje se rozšíření na další méně důležité stroje.

Hodnocení a přínosy projektu

Klasické MES systémy obvykle přinášejí zhruba 10% zvýšení produkce pouze jejich zavedením, avšak vzhledem k sezónním výkyvům, jako je například letní období, je zatím předčasné hodnotit konkrétní přínosy. Mezi hlavní výhody patří správný přepočet času, úprava standardního cyklu a zvýšení produktivity. Systém také umožňuje identifikaci problémových forem a přispívá k redukci chybovosti týmu.

Možnost využití a budoucí aplikace

InOEE byl nasazen v široké škále provozů, InovecTech již instaloval přes 100 tisíc virtuálních senzorů. Největší výhoda oproti konvenčním metodám je pro digitalizaci diskrétní výroby podniků s širokým záběrem používaných strojů, typicky s časem cyklu stroje od 10ms po 1h, a s hodinovou sazbou (závisí od typu výpočtu od rozpočtu odpisů, přes celkové konverzní náklady na hodinu výroby po marži na hodinu provozu stroje) v rozmezí od 10 do 1000 EUR. To obnáší zhruba 5,000 dosud nedigitalizovaných podniků v ČR. Analýza podobného průmyslu v SR odhaduje potenciál zvýšení HDP ekonomiky v důsledku odemčené možnosti digitalizace v řádu vyšších desetin procenta.

Příloha 5 - Případová studie: Platforma pro geolokační data od Mapotic a Hardwario

Základní informace o poskytovateli řešení

Mapotic je česká technologická společnost zaměřená na vývoj platformy pro zpracování a vizualizaci geolokačních dat, včetně zpracování senzorických dat z IoT zařízení. Spolupracuje například s firmou Hardwario na vývoji platformy pro bateriové online IoT sčítače Chester Motion, které jsou využívány především v oblasti turismu. Nabízí nástroje pro interaktivní mapy, správu IoT dat a mobilní aplikace. Jejím cílem je poskytovat jednoduchá a uživatelsky přívětivá řešení založená na geolokačních technologiích.

Zákazníci, uživatelé a jejich potřeby

Zákazníci se pohybují napříč různými odvětvími, včetně environmentálního monitoringu, udržitelného turismu nebo logistiky a veřejné správy. Potřebují snadné a rychlé způsoby, jak sledovat a analyzovat data z IoT zařízení v reálném čase, a efektivně je vizualizovat pro rozhodování nebo veřejnou prezentaci.

Případy užití tohoto řešení

Mapotic a IoT zařízení na bázi Chester je využíván v různých oblastech, jako je wildlife tracking (sledování pohybu zvířat v divoké přírodě), kde jsou IoT senzory a GPS zařízení nasazovány pro sledování zvířat v oceánech nebo chráněných oblastech. Dalším příkladem je environmentální monitoring, který se zaměřuje na dlouhodobé sledování parametrů, jako jsou kvalita ovzduší, vlhkost půdy nebo úroveň znečištění, pro optimalizaci environmentálních strategií.

V oblasti logistiky a plánování je Mapotic využíván například při zimní údržbě silnic, kde senzory monitorují stav povrchu vozovek a pomáhají optimalizovat plánování zimní údržby na základě aktuálních a historických dat.

Efektivní plánování infrastruktury, jako je rozvoj cest, umístění odpadkových košů a odpočívadel. Tento systém poskytuje přesná data o pohybu návštěvníků, čímž odstraňuje nutnost spoléhat na nepravidelné manuální sčítání nebo odhady.

Dalším projektem bylo nasazení monitoringu silnic v Libereckém kraji, kde bylo implementováno IoT zařízení pro monitorování teploty vozovek. Tento systém poskytuje přesnější údaje než tradiční meteorologické stanice, což umožňuje lepší plánování zimní údržby.

Společnost se podílí také na testovacím projektu v Praze, zaměřeném na sledování turismu. Sčítače jsou umístěny jak v exteriérech, tak interiérech historických budov, kde umožňují zadavatelům sledovat pohyb turistů. Data pomáhají zlepšovat plánování marketingu a úpravy infrastruktury.

Popis produktu

Hardwarová část – HARDWARIO CHESTER

Rozšiřitelné edge zařízení pro průmysl 4.0, chytrá města, e-metering a zemědělské aplikace. Připojuje senzory, akční členy, řídicí jednotky PLC a další zařízení k internetu. Flexibilní napájení a komunikační technologie LPWAN umožňují spolehlivé a stabilní připojení i ze vzdálených a těžko dostupných prostor. Zprávy jsou zprostředkovány pomocí technologií NB-IoT/LTE-M nebo LoRaWAN, aktuální poloha GNSS.

Proces implementace

Proces implementace začíná sběrem požadavků od klienta, identifikací vhodných míst pro instalaci senzorů a samotným nasazením. Naše zařízení jsou bateriově poháněná a, v závislosti na frekvenci odesílání dat a podmínkách, vydrží v provozu několik let. Konektivitu zajišťujeme jako součást řešení. Data jsou pravidelně aktualizována, obvykle v půlhodinových intervalech. Během provozu probíhá kalibrace a kontrolní měření, aby byly výsledky co nejpřesnější. Testujeme také novou generaci zařízení, která bude schopna sledovat směrovost pohybu a umožní vzdálené nastavení a kalibraci senzorů.

5G/P5G

Společnost využívá 5G síť díky jejímu rozšíření a spolupráci s operátory, což nám umožňuje dosáhnout co nejlepšího pokrytí a široké kompatibility nejen v ČR, ale i po celé Evropě a USA. Tato síť je pro společnost do budoucna klíčová, protože naše řešení často pracují v místech bez přístupu k elektrické síti a vyžadují spolehlivou bezdrátovou komunikaci.

Zařízení jsou vybavena komunikačními čipy, které umožňují nejen využití 5G, ale i dalších technologií jako NB-IoT a LORAWAN. Tyto technologie jsou zvláště výhodné pro přenos menších objemů dat, což je pro tyto aplikace dostatečné, a zároveň umožňují výrazně šetřit baterii. Vzhledem k tomu, že zařízení společnosti často pracují v outdoorových podmínkách, kde není přístup k elektrické síti, je efektivní spotřeba energie zásadním faktorem.

Tato kombinace technologií umožňuje efektivní provoz IoT řešení společnosti i na vzdálených místech, čímž poskytujeme spolehlivé výsledky i v nejnáročnějších podmínkách.

Proč bylo toto řešení vybráno

V případě veřejné správy společnost uspěla v tendru, kde jedním z hlavních kritérií byla cenová dostupnost. Zařízení jsou navržena tak, aby poskytovala maximální kvalitu za co nejdostupnější cenu, což je důležité pro zákazníky, kteří potřebují efektivní a spolehlivá řešení pro monitoring v reálném čase.

Dalším klíčovým kritériem je bateriový provoz a možnost online komunikace, což umožňuje zadavatelům přijímat data v reálném nebo téměř reálném čase. Na trhu je stále relativně málo zařízení, která by dokázala nabídnout tuto kombinaci cenové dostupnosti, kvality a spolehlivosti. Konkurenční řešení jsou buď výrazně dražší, nebo mají technické nedostatky, například problémy s fungováním v extrémních podmínkách, jako jsou mrazy.

Zařízení zvládají extrémní teploty, což dokazují například projekty v Tatrách, kde teploty klesaly až k -30 °C, a baterie stále fungovaly bez výrazného poklesu výkonu. Tato odolnost vůči extrémním podmínkám je jednou z klíčových výhod, které naše řešení poskytují oproti konkurenci.

Status projektu

Aktuálně je testována nová generace zařízení, která přináší výrazná technická vylepšení. Mezi hlavní novinky patří vyšší přesnost díky dvěma senzorům, což umožňuje nejen lepší měření, ale také určování směru pohybu. Další důležitou inovací je možnost vzdálené konfigurace zařízení, což znamená, že lze měnit parametry měření, četnost odesílání telemetrických dat a další nastavení bez nutnosti fyzického zásahu.

Tuto novou generaci plánuje společnost testovat ve spolupráci s vybranými partnery na českém trhu během následujících měsíců. Cílem je plná komercializace od roku 2025, kdy plánujeme intenzivní propagaci hlavně v segmentu udržitelného turismu, a to nejen v České republice, ale i na zahraničních trzích.

Hodnocení a přínosy projektu

Některé údaje a měření na case study projektu zde. Zde několik výstupů přímo od klienta (Tatranský národní park – Region Vysoké tatry)

- Turistické informační kanceláře – umí informovat návštěvníky o méně či více navštěvovaných místech a podle toho vyhodnocovat, jaké túry mohou absolvovat s ohledem na tato data
- Ochrana přírody – Správa TANAP provádí jednou ročně sčítání návštěvníků na nejnavštěvovanějších místech, ovšem tímto způsobem má celoroční přehled o pohybu
- Je dobrý argumentační nástroj v případech, kdy dochází k dohadům kolik lidí, která místa navštěvuje
- I s ohledem na zvyšující se ceny elektřiny je to dobrý nástroj na vyhodnocení, na kterých místech může samospráva vypínat, resp. regulovat veřejné osvětlení podle pohybu návštěvníků
- V zimním období jsou sčítače umístěné i na trasách běžeckého lyžování, což je důležité pro sledování, které úseky jsou navštěvované, s čímž souvisí i vyhodnocování údržby tras, na které správa TANAP získává dotační prostředky z Ministerstva dopravy SR

Toto řešení je ideální zejména zaměřených na udržitelný turismus, národní parky a monitoring pohybu osob. Díky agregaci dat z našich senzorů s dalšími kanály, jako jsou mobilní nebo webové aplikace, mohou organizace efektivně řídit turistický ruch na základě přesných a aktuálních dat. Může se jednat o parky ale také distribuci turismu mimo exponovaná místa nebo využití těchto dat spolu s dalšími datovými kanály (mobilní aplikace, kampaně) a následné informovanější rozhodování. Tato řešení tak umožňují lepší plánování infrastruktury, rozložení návštěvnosti a ochranu přírodních oblastí. Díky těmto výhodám je řešení vhodné pro široké spektrum aplikací, od turismu po veřejnou správu a průmyslové monitorování.

Obrázek 15: Ukázka výstupů platformy Mapotic. Zdroj: Mapotic.