

# **ŠKODA AUTO VYSOKÁ ŠKOLA, O.P.S.**

Studijní program: N6208 Ekonomika a management

Studijní obor: 6208T088 Podniková ekonomika a management provozu

## **Internet věcí ve společnosti ŠKODA AUTO a.s.**

**Bc. Sergii Svystula**

Vedoucí práce: prof. Ing. Radim Lenort, Ph.D.



ŠKODA AUTO Vysoká škola

## ZADÁNÍ DIPLOMOVÉ PRÁCE

Zpracovatel: **Bc. Sergii Svystula**

Studijní program: Ekonomika a management

Obor: Podniková ekonomika a management provozu

Název tématu: **Internet věcí ve společnosti ŠKODA AUTO a.s.**

Cíl: Cílem diplomové práce je, na základě rešerše a analýzy aktuálních odborných zdrojů, reálných případových studií, vytvořit návrh strategie implementace Internetu věcí (IoT) v prostředí ŠKODA AUTO a.s.

Rámcový obsah:

1. Literární rešerše nejnovějších poznatků z oblasti IoT a jeho využití v průmyslovém podniku.
2. Návrh základních pilířů strategie implementace IoT v prostředí společnosti ŠKODA AUTO a.s.
3. Rozpracování jednotlivých pilířů navržené strategie.
4. Kritické zhodnocení předloženého návrhu.

Rozsah práce: 55 – 65 stran

Seznam odborné literatury:

1. GREENGARD, S. *Internet of Things*. Dhaka: University Press Group, 2015.
2. MIRRISH, J. – SLAMA, D. – PUHLMANN, F. *Enterprise IoT*. USA: O'Reilly Media, 2015.
3. HAZENBERG, W. – HUISMAN, M. – CORDOBA RUBINO, S. *Meta Products: Building the Internet of Things*. Netherlands: Booreiland and BIS Publishers, 2011. 176 s. ISBN 978-90-6369-251-3.

Datum zadání diplomové práce: květen 2017

Termín odevzdání diplomové práce: květen 2018

L. S.

  
prof. Ing. Radim Lenort, Ph.D.  
Vedoucí práce

  
Mgr. Petr Šulc  
Prorektor ŠAVŠ

  
prof. Ing. Radim Lenort, Ph.D.  
Vedoucí katedry

  
Bc. Sergii Svystula  
Autor práce

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury pod odborným vedením vedoucího práce.

Prohlašuji, že citace použitých pramenů je úplná a v práci jsem neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Mladé Boleslavi dne 17. května 2019

Děkuji prof. Ing. Radimovi Lenortovi, Ph.D. za odborné vedení diplomové práce, poskytování rad a informačních podkladů. Dále bych rád poděkoval pracovníkům odd. PSZ/1 ŠKODA AUTO a.s., a zvláště Bc. Milanovi Kičakovi za ochotnou spolupráci a svým českým kamarádům.

## Obsah

Seznam použitých zkratk a symbolů.....	6
Úvod .....	8
1 IoT a jeho využití v průmyslovém podniku .....	9
1.1 Současný stav trhu IoT .....	13
1.2 Použití IoT v průmyslovém podniku .....	15
1.3 Přehled současných IoT technologií .....	20
1.4 Bezpečnostní rizika při realizaci IoT projektu.....	23
2 ŠKODA AUTO a.s. a IoT.....	26
2.1 ŠKODA AUTO a.s. ....	26
2.2 Oddělení PSZ - Centrální technický servis .....	26
2.3 Laboratoř PSZ - FabLab .....	27
3 Návrh a rozpracování strategie implementace IoT platform a technologií v prostředí společnosti ŠKODA AUTO a.s. ....	29
3.1 Návrh strategie implementace IoT platform a technologií v prostředí společnosti ŠKODA AUTO a.s. ....	29
3.2 Přehled současných IoT platform, fungujících v České republice .....	31
3.3 Porovnávání a výběr vhodné IoT platformy .....	36
3.4 Popis nevýhod použité platformy LoRaWAN .....	37
3.5 Požadavky, přehled a výběr cloudů .....	38
3.6 Přehled dostupných zařízení pro sběr dat .....	44
3.7 Pilotní testovací provoz IoT LoRaWAN .....	46
3.8 Návrh vývoje vlastní IoT platformy typu XNB a přechod na Privátní Cloud .....	51
3.9 Přehled a výběr vhodné BI platformy .....	55
3.10 Zavedení monitorovacího systému MCD .....	56
4 Kritické zhodnocení předloženého návrhu .....	59
Závěr .....	61
Seznam literatury .....	63
Seznam obrázků a tabulek .....	65
Seznam příloh .....	67

## Seznam použitých zkratk a symbolů

AIS	Analytický informační systém
AWS	Amazon Webové Služby
Big Data	Velká data
B2B	Podnik pro podnik
BI	Business Intelligence
BLE	Bluetooth Low Energy
CTU	Český telekomunikační úřad
CNC	Počítačové číslicové řízení
DB	Databáze
ETSI	Evropský ústav pro telekomunikační normy
ECC	Kryptografie nad eliptickými křivkami
GSM	Globální systém pro mobilní komunikace
GPS	Globální polohový systém
IaaS	Infrastruktura jako služba
IoT	Internet věcí
ICT	Informační a komunikační technologie
ISO	Mezinárodní organizace pro normalizaci
IEEE	Institut pro elektrotechnické a elektronické inženýrství
JTC	Společný technický výbor
LPWAN	Globální síť se zařízeními s nízkou spotřebou
NB-IoT	Úzkopásmová síť pro IoT
NFC	Komunikace na krátkou vzdálenost
M2M	Mezi stroji
MDC	Sběr Dat ze Strojů
MQTT	Přenos zpráv telemetrie

PaaS	Platforma jako služba
PdM	Prediktivní údržba
RFID	Radiofrekvenční identifikace
SaaS	Software jako služba
SLA	Smlouvy o úrovni služeb
SOA	Architektura orientovaná na služby
ŠA	ŠKODA AUTO a.s.
UWB	Ultra širokopásmové systémy
UNB	Ultra úzké pásmo
WWAN	Rozsáhlá bezdrátová síť
XNB	Úzkopásmové rozšíření



## Úvod

Internet věcí neboli IoT je zavádění automatizovaných systémů, které propojují různé přístroje, zařízení, čidla, sensory a vyhodnocují získaná data. V dnešní době je jedním z hlavních trendů v oblasti digitalizaci a automatizaci průmyslu, energetiky, dopravy, zdravotnictví, provozu měst a obcí i domácností.

Svět IoT nachází uplatnění v široké škále oblastí a základní principy vždy jsou stejné - založené na autonomním sběru dat, místním nebo vzdáleném zpracování a využití výsledků pro řízení určitého procesu nebo získání přidané hodnoty. Na druhou stranu bohužel platí, že některá konkrétní řešení jdou spíše po povrchu a zdaleka nevyužívají všech výhod IoT. Řada implementací ze světa IoT tak končí pouze na úrovni pasivního sběru údajů bez podrobnějšího analytického využití.

“Obrovským přínosem IoT je možnost převést do praxe princip „řídím to, co měřím“. Čím více informací má firma v rámci daného procesu k dispozici, tím kvalifikovanější rozhodnutí může přijímat. Podstatně rychleji, než při využití tradičních „méně informovaných“ přístupů“ (Topinfo, 2017). Díky neustálému poklesu nákladů spojených s IoT, což platí zejména pro jednotlivá autonomní zařízení (tzv. čidla a sensory), je dnes možné získávat obrovské množství relevantních dat za cenu, která je nižší než přínosy spojené s jejich využitím. A to je zásadní průlom potvrzující, že IoT se dostal do etapy svého vývoje, kdy nemá příliš cenu diskutovat o tom zda, ale proč a jak. Nejde přitom o samozřejmost, stačí si uvědomit, kolik skvělých technologií v minulosti neproniklo do praxe právě z důvodu finanční náročnosti. Česká republika patří z hlediska zavádění IoT mezi nejpokrokovější země střední a východní Evropy.

Cílem práce je, na základě rešerše a analýzy aktuálních odborných zdrojů a reálných případových studií vytvořit a kriticky zhodnotit návrh strategie implementace vybraných IoT platforem v prostředí ŠKODA AUTO a.s.

## 1 IoT a jeho využití v průmyslovém podniku

Rozvoj Internetu věcí je tlačen dostupností technologií, netáhne ho poptávka po řešeních ze strany podnikatelů (Cearley, 2018). Pro podnikatele je přitom třeba propočítat, co jim nové technologie přinesou právě v jejich případě. Ale ukazuje se, že jakmile s podnikem začne někdo probírat možnosti toho, co by se dalo kde snímat jakým čidlem, podnikatelé sami přicházejí často s nejlepšími nápady - vědí sami nejlépe, co je trápí, jen dosud neuvažovali nad řešením pomocí IoT.

Běžný podnik, ať malý, střední či větší, bude jen sotva nasazovat tyto technologie vlastními silami. Proto na trhu působí několik druhů dodavatelů, kteří se vzájemně doplňují:

**Integrátoři** – navrhnu a připraví řešení na míru pro zákazníka. Právě s integrátorem přijde do styku podnik v první řadě. Úlohu integrátora na sebe berou i některé velké společnosti, jako je T-Mobile nebo ČD-Telematika, CRA, SimpleCell Networks.

**Datoví analytici** – vypracují algoritmy pro zpracování dat. Často to není táž firma jako integrátor, datová analýza vyžaduje specializovanou dovednost.

**Provozovatelé komunikačních sítí** – zajišťují komunikaci a přenos dat. S nimi se domluví zpravidla integrátoři.

**Poskytovatelé platform**. Někde něčím je třeba data zpracovávat. Nejjednodušší je to v „cloudu“, jemuž má smysl rozumět jakožto nákupu výpočetního výkonu podle okamžité potřeby, aniž by bylo nezbytné budovat vlastní výpočetní infrastrukturu. Vhodnou platformu a její využití navrhne a domluví integrátor s datovým analytikem. ČD-Telematika je například partnerem Microsoftu a využívá Azure. Příklady jiných možností jsou AWS IoT od Amazonu nebo cloud od Googlu.

**Dodavatelé zařízení**, tedy různých součástí a čidel, jimiž lze vybavit stroje vhodná zařízení vybere a nakoupí integrátor po domluvě se zákazníkem.

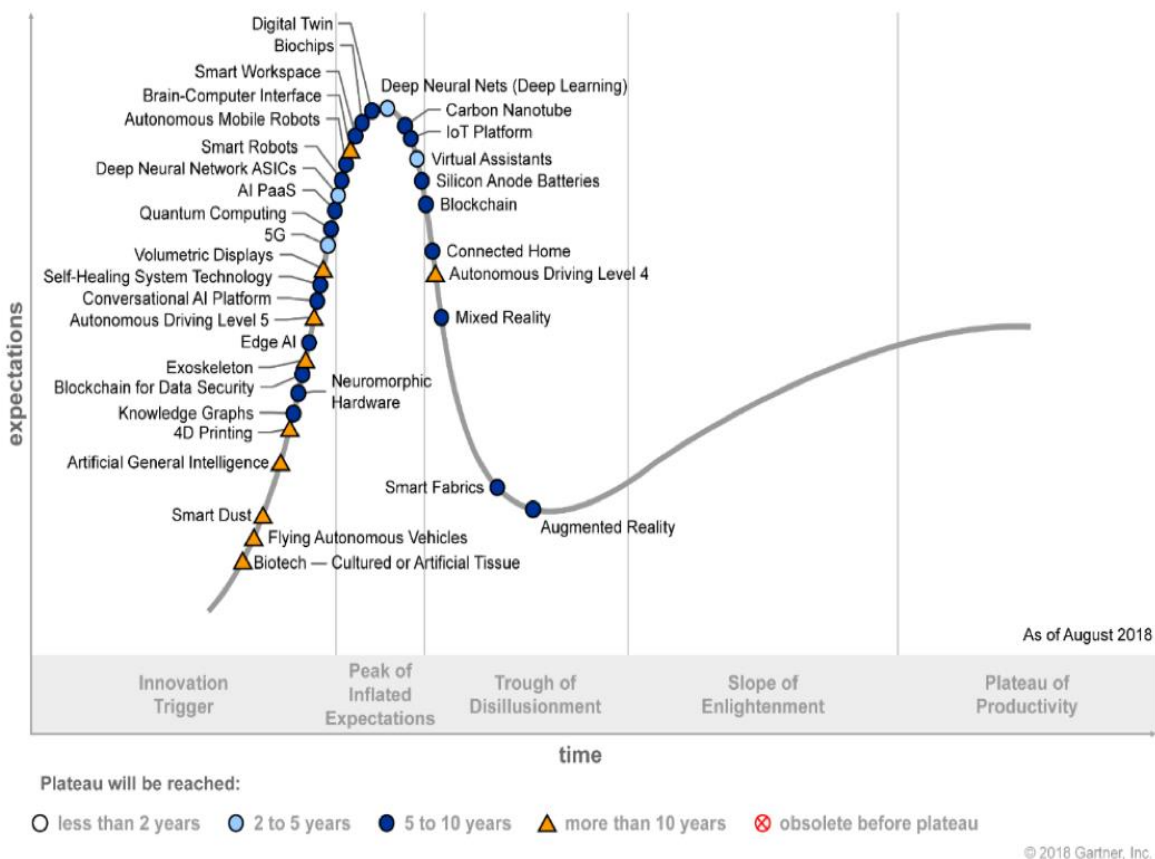
Při uzavírání smluv je potřeba dát pozor na vlastnictví dat. Někteří výrobci nebo dodavatelé rádi považují „provozní data“, posbíraná dodaným strojem, za svoje vlastnictví. Už mnoho let se využívají některá řešení, která by se dala zařadit pod pojem IoT, například sledování polohy vozidel.

O tom, co se vyplatí sledovat, spolurozhoduje dostupnost vhodné bezdrátové sítě a energetická náročnost připojení k takové síti (v některých případech se nabízí i připojení dráty, ale v mnoha jiných by natažení pevných vedení nebylo možné, nebo by vyšlo nesmyslně drahé.). Mobilní síť GSM nebyla navržena pro potřeby IoT (Woodie, 2018), připojení k ní je poměrně energeticky náročné, síť není v některých odlehlých místech spolehlivě dostupná, mimoto ji lze snadno místně rušit (zejména úmyslně). Ani její nástupce, síť LTE, není přednostně vytvořena pro IoT. Různá rozšíření teprve postupně získává, nebo jsou dosud vyvíjena či jen zvažována.

Myšlenka sítě sestávající z inteligentních zařízení začala být diskutována již v roce 1982, kdy se modifikovaný zásobník na nealkoholické nápoje stal prvním zařízením připojeným k internetu na univerzitě Carnegie Mellon University. Přístroj byl schopen přenášet informace o množství založených nápojů, stejně jako o tom, kdy byly nově založené nápoje dostatečně ochlazeny. Příspěvek Marka Weizera z roku 1991 o všudypřítomném počítači "Počítač 21. století", stejně jako akademické konference jako UbiComp a PerCom, vyvinuly moderní vizi IoT. V roce 1994 popsala Reza Raji základní pojetí v časopise IEEE Spectrum jako „přesun malých datových paketů do velké sady uzlů, které integrují a automatizují vše od domácích spotřebičů po celé továrny“. Mezi lety 1993 a 1996 několik společností nabídlo řešení, např. Microsoft at Work nebo NEST Novell. Pak Bill Joy představil komunikaci "Device to Device (D2D)" jako součást svého rámce "Six Webs" během Světového ekonomického fóra v Davosu.

Termín „Internet věcí“ vytvořil Peter T. Lewis v projevu v roce 1985 během zasedání Federální komise pro komunikaci (FCC) podporující bezdrátovou komunikaci. Ve svém projevu uvedl, že „internet věcí je integrace lidí, procesů a technologií s připojenými zařízeními a snímači, aby se zajistilo dálkové sledování, stav, manipulace a hodnocení trendů těchto zařízení“.

Koncepce IoT se stala populární v roce 1999 díky Autoidentifikačnímu centru Massachusetts Institute of Technology a příslušným publikacím v oblasti analýzy trhu. Kevin Ashton (jeden ze zakladatelů autoidentifikačního centra) viděl identifikaci rádiových frekvencí jako předpoklad pro vznik IoT, i když preferoval termín „internet pro věci“.



Zdroj: Gartner Inc.

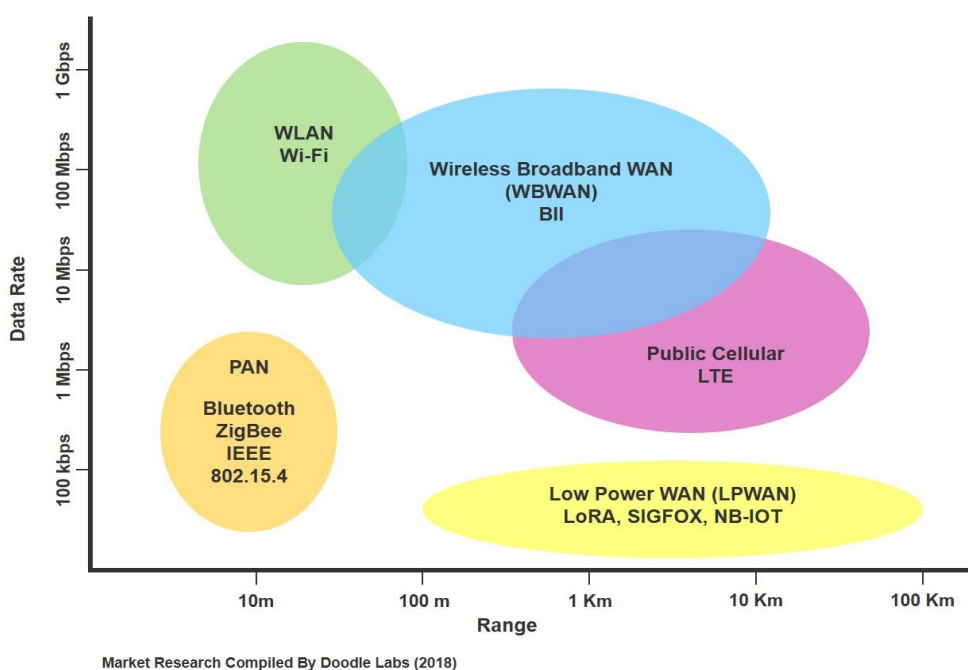
### Obr. 1 Hype cyklus pro vznikající technologie

Na obrázku 1 je zobrazena Hype křivka od společnosti Gartner, která je jednoduchým a přehledným nástrojem pro pochopení technologických cyklů. Umožní odlišit očekávání spojená s novými technologiemi a na základě 5 fází umožňuje rozhodnutí, zda a kdy se o ně začít zajímat a investovat do nich. Dle obrázku se IoT nachází ve třetí fázi – co je na trhu co ještě nepoužíváme? A jak říká viceprezident výzkumu společnosti Gartner Nick Jones „Internet věcí bude přinášet stále nové příležitosti pro digitální inovaci i obchod v celém následujícím desetiletí. Řada z nich bude souviset se zcela novými či modernizovanými technologiemi“.

Existuje mnoho definic pojmu Internetu věcí a je tedy často těžké pochopit význam tohoto pojmu. Za nejužitečnější je však možné považovat následující definici: „Internet věcí“ znamená - síť propojených objektů (věcí), které jsou jednoznačně adresovatelné s tím, že tato síť je založena na standardizovaných komunikačních protokolech umožňující výměnu a sdílení dat a informací, jejichž analýzou bude možné docílit vyšší přidané hodnoty.

**Síť:** Slovo síť nemusí představovat pouze Internet (jak evokuje pojem IoT) – tedy celosvětový systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP, ale může znamenat i lokální síť (LAN), v rámci které mohou věci komunikovat, avšak s přístupem do Internetu pro možnost sdílení výsledků. Síť zajišťuje konektivitu (viz Obr. 2).

**Věc:** Věc z pohledu IoT představuje neživý objekt (fyzický nebo virtuální) obsahující elektroniku, software a senzory, pomocí kterých snímá určitou hodnotu nebo hodnoty a poskytuje schopnost sloužit k danému účelu. (Pohanka, 2015)



Zdroj: doodlelabs.com

### **Obr. 2 Druhy sítí – bezdrátové a s velkým dosahem**

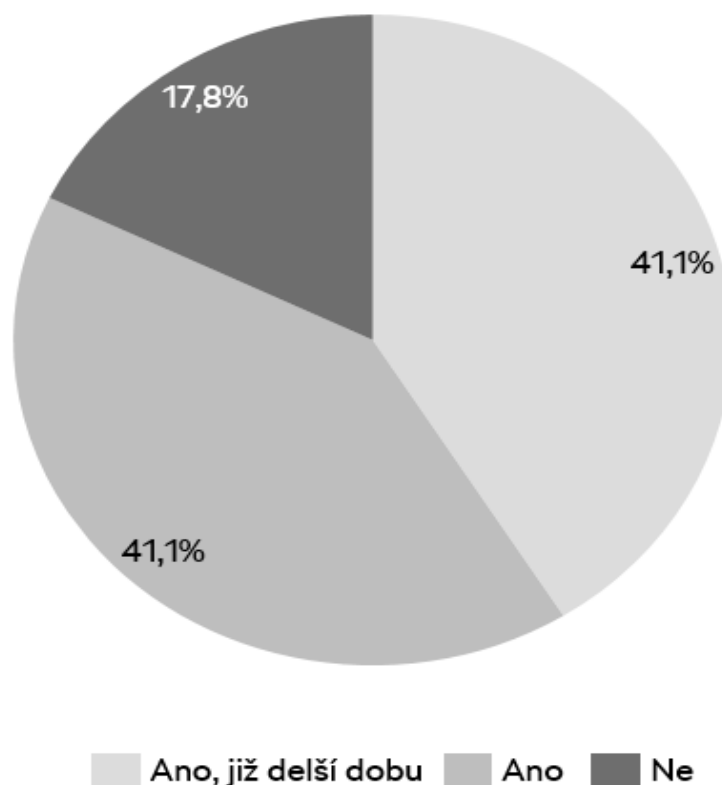
Jedná se tedy o zařízení (systém), které autonomně poskytuje data (osobní počítač, který neposkytuje data, nepředstavuje věc z pohledu IoT), která jsou kabelově nebo bezdrátově sdílena s dalšími věcmi nebo systémy. Paradoxem však je, že v rámci Internetu věcí nejsou základem věci, ale data, která tyto věci poskytují.

Internet věcí tedy představuje koncept, v rámci kterého si fyzické a virtuální objekty (věci) vyměňují data přes síť Internet. Věci (systémy) mohou být v rámci Internetu věcí libovolně pospojovány za účelem dosažení vyšších cílů (nových funkcností, složitějších úloh, apod.). IoT tvoří čtyři základní prvky: vlastní zařízení, konektivita k tomuto zařízení a z něj, data a analytika. Zařízením může být cokoli, od jednoho senzoru až po rozsáhlý řídicí systém. Senzory a systémy potřebují konektivitu k větší síti pro sdílení třetího prvku – dat generovaných senzorem nebo systémem.

Analýza těchto dat generuje prakticky využitelné informace, které pracovníkům ve výsledku dovolují přijímat kvalifikovaná rozhodnutí. Informace tohoto charakteru mají pro podnik velkou hodnotu. Přispívají k vývoji nových provedení produktu, optimalizaci výkonu systému a maximalizaci zisku.

### 1.1 Současný stav trhu IoT

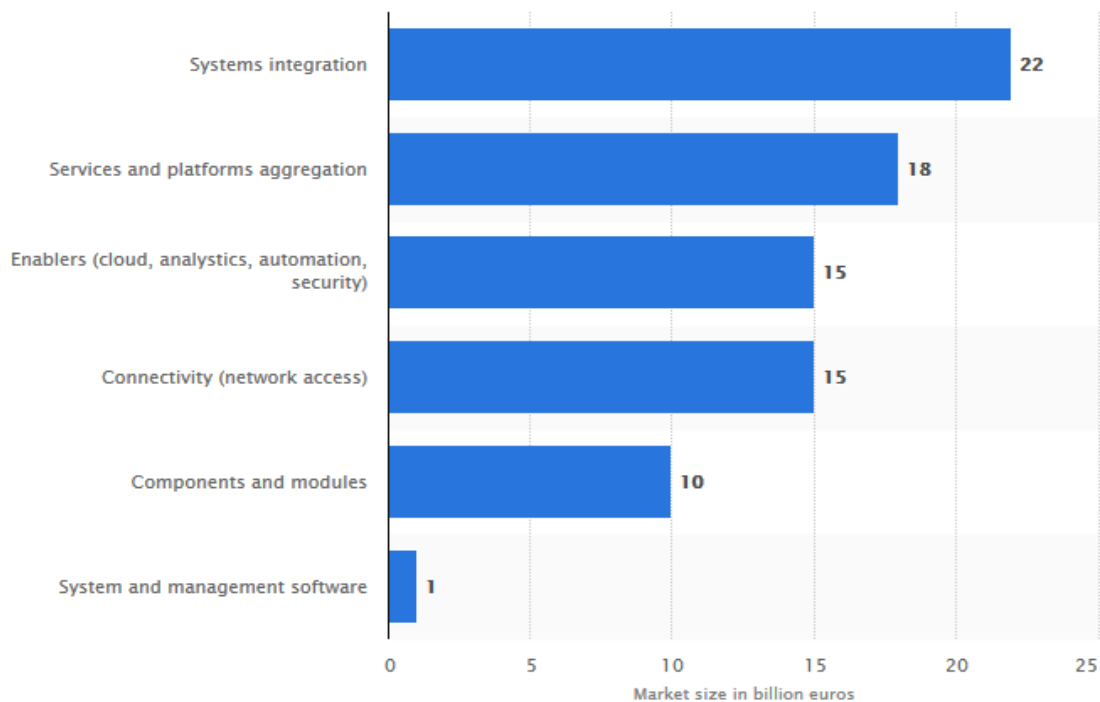
Současná situace na trhu s informačními technologiemi je způsobena vysokým nárůstem popularity IoT (viz Obr. 3). Mnoho podniků projevuje velký zájem o implementaci této technologie, neboť je schopno automatizovat velké množství různých výrobních procesů a nyní se Internet věcí aktivně zavádí do průmyslových zařízení.



Zdroj: Prediktivní údržba 4.0: Nesmysl, nebo nezbytnost?

#### **Obr. 3 Dotazník: dochází ve vaší výrobě k reálnému využití konceptu IoT?**

Podle průmyslových analytiků je dnes k internetu připojeno přibližně 10 - 20 miliard objektů. Tento ekosystém spojených objektů je základem IoT (Lom, 2017). Počet připojených objektů je dnes zanedbatelný ve srovnání s tím, kolik z nich bude připojeno během několika málo let. Podle různých odhadů bude rozsah připojených objektů do roku 2025 od 40 do 50 miliard (viz Obr. 4), a bude obsahovat vše od kelímků a perníků až po domovy, auta a průmyslová zařízení.



Zdroj: <https://www.statista.com/>

**Obr. 4 Trh IoT řešení v Evropské unii (EU 28) v roce 2025 (v miliardách eur)**

Svět Internetu věcí učiní ekonomiku složitější. Pravidla, která průmyslové společnosti a vlády přijaly k podpoře růstu a hospodářské soutěže, nebudou v dlouhodobém horizontu účinná. IoT ovlivní každou zemi a ekonomiku na planetě, dokonce i rozvojové země, které byly historicky zbaveny výhod technologického pokroku. Aby bylo možné zhodnotit obchodní příležitosti, které jsou součástí IoT, je třeba nejprve pochopit jeho makroekonomické důsledky. V politice Evropské komise RAND Europe načrtla horní odhad ekonomického potenciálu IoT ve výši 1,4 bilionů USD ročně (1,09 bilionů EUR) na 14,4 bilionů USD (11,2 bilionů EUR) ve všech sektorech světového trhu. Prodej souvisejících zařízení a služeb navíc dosáhne v roce 2025 přibližně 2,5 bilionu USD, zatímco kumulativní investice z propojení miliard připojených zařízení dosáhnou v běžných cenách nejméně 2 biliony EUR. Například studie RAND uvádí, že Čína již přidělila 625 milionů EUR (775 milionů USD) na investice do IoT.

Lze tvrdit, že za několik let nebude jediný průmysl, který nebude přímo ovlivněn IoT, což je však ovlivňováno určitými stimuly a bariérami (viz Tab. 1).

**Tab. 1 Stimuly a bariéry Internetu věcí**

Stimuly	Bariéry
Rychlý vývoj ICT technologie	Potřeba přechodu na společné standardy
Logistika a řízení dodávek	Nekompatibilita standardu komponent
Zvýšení bezpečnosti a vybavení dopravních prostředků	Problém ochrany osobních údajů a bezpečnosti
Ochrana životního prostředí a snížení nákladů na energii	Poměrně vysoké realizační náklady
Rozvoj kontroly nad padělanými výrobky a ochrana před krádeží	
Státní podpora a akční inovátoři	

Pod vlivem očekávání a požadavků zákazníků bude tempo implementace IoT rychle přeměňovat jakýkoli průmysl nebo společnost, která nepoužívá IoT, bez nadsázky, v „muzejní exponát“. Mnoho průmyslových odvětví má tedy čas pochopit tento jev i to, jak může ovlivnit jejich dlouhodobé strategické cíle.

## 1.2 Použití IoT v průmyslovém podniku

Internet věcí v průmyslu vylepšuje výrobní operace tím, že zlepšuje konektivitu, správu zařízení, monitorování výroby a vztahy se zákazníky. Na obrázku 5 je uvedeno několik přínosů, které má využití IoT v průmyslu (Clemons, 2018).



Zdroj: Actum digital

**Obr. 5 Dotazník: Co firmy od IoT očekávají?**



## **Monitorování výroby**

Protože IoT propojuje chytré stroje, shromažďuje a sdílí velké množství dat, je nyní možné monitorování výroby v reálném čase. To umožňuje okamžitou reakci na narušení, pomáhá eliminovat prostoje a omezit množství zásob rozpracované výroby. IoT umožňuje dokončit výrobu včas a synchronizovaně se zásobami materiálů a surovin.

## **Vzdálená správa zařízení**

Připojení strojů kompatibilních s IoT sítí umožňuje vzdálenou správu zařízení odkudkoli na základě sledování jejich stavu pomocí chytrých senzorů. Lze použít chytré senzory. Je možno nastavit protokoly tak, aby aktivně spravovaly zařízení, šetřily náklady na energii a snižovaly celkové provozní výdaje.

## **Údržba zařízení**

Pomocí IoT je možné snadno implementovat prediktivní údržbu. IoT je klíčovým faktorem umožňujícím realizovat údržbu na bázi spolehlivosti a využívat strojové učení pro podporu prediktivní údržby. To vše se pozitivně odráží ve zvýšeném objemu výroby, omezení odstávek, nižších nákladech na údržbu, vysoké spolehlivosti strojů a větší návratnosti investovaného kapitálu v podobě lepšího využívání stroje a objemu výroby (Raycom, 2018).

## **Průběžné zlepšování díky analýze dat**

Štíhlá výroba, Six Sigma a další koncepce neustálého zlepšování potřebují spoustu dat. Proto je průmyslový IoT tak důležitý. IoT pomáhá agregovat produktová, procesní a další data a pomáhá je dostat k těm správným lidem a na správná místa k analýze. Tato data potřebují pracovníci zabývající se průběžným zlepšováním k tomu, aby identifikovali problémy, dobrali se k hlavní příčině, implementovali vylepšení a ověřili si, že tato zlepšení fungují.

## **Autonomní manipulace s materiálem**

IoT se dokáže připojit v podstatě ke všemu, včetně zařízení pro manipulaci s materiálem, jako jsou automaticky naváděná vozidla (Automated Guided Vehicles - AGV) a automatizované skladovací a vychystávací systémy (Automated Storage and Retrieval Systems). Výrobní linka vyzve AGV k vyzvednutí produktů nebo přivezení materiálu. AGV vyzve systém ASRS k zaslání dalších surovin, což následně přiměje k činnosti vozidlo AGV. To vše běží autonomně a jednotlivě

jednotky spolu komunikují v reálném čase.

### **Zlepšení komunikace s dodavateli**

IoT umožňuje komunikaci s dodavateli tím, že jim poskytuje provozní informace pro vzdálenou automatizaci a optimalizaci procesu. Komunikaci s dodavateli na bázi IoT lze rozšířit o informace jako je objem výroby nebo úroveň skladových zásob, to vše pro podporu dodávek skladových zásob právě včas (just-in-time), systémů zásob řízených dodavatelem a lepšího řízení skladových zásob materiálu.

### **Lepší vztahy se zákazníky**

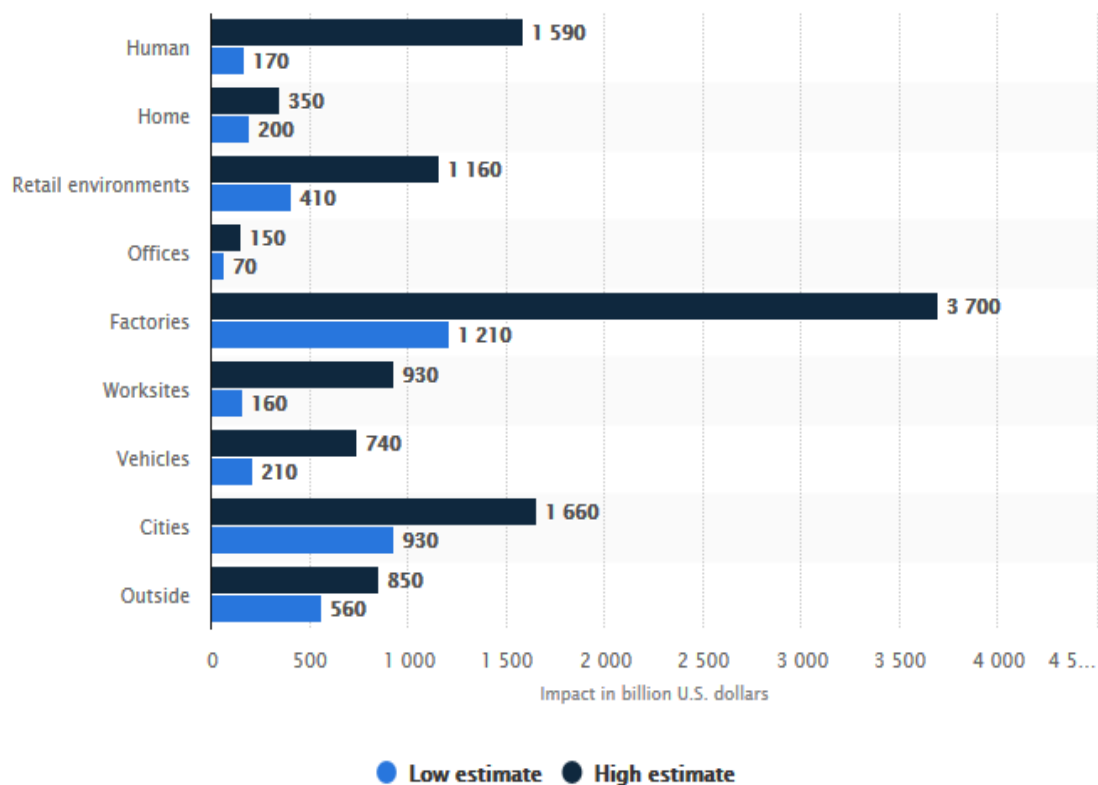
Pokud jde o zákazníky, IoT může odběratelskému řetězci poskytovat přehled o výši skladových zásob dokončených výrobků. To umožňuje snížit úroveň skladových zásob, snížit přepravní náklady, snížit skladovací a distribuční náklady a poskytovat lepší zákaznické služby. Pomáhá to výrobním a distribučním operacím dostat správné produkty na správná místa a ve správný čas, což zvyšuje spokojenost zákazníků.

### **Lepší rozhodování managementu**

Dnes tým managementu musí mít k dispozici informace v reálném čase, aby mohl přijímat rozhodnutí s výrazným dopadem na náklady a zisky firmy. IoT umožňuje managementu dostávat ty správné informace, aby měl přehled o tom, co se děje na výrobní úrovni, aby mohl přijímat rozhodnutí potřebná pro lepší řízení celkových provozních nákladů a zvyšování firemních zisků (Trademedia international, 2018).

Všechna sesbíraná data lze zpracovat a rozdělit konkrétním uživatelům například podle jejich rolí následovně:

- Management – využije přístup z libovolného místa na světě k celkovým přehledům a reportům, potřebuje znát aktuální data i trendy za zvolené období.
- Mistr výroby – sleduje práci zaměstnanců, jejich výkonnost, produkci vadných výrobků, spotřebu materiálu, stav skladových zásob, apod.
- Pracovník údržby – musí mít aktuální informace o stavu výrobní linky, o jednotlivých strojích.
- Pracovník ve výrobě – potřebuje informace o svém úkolu, technické údaje a schéma výrobku, varování před nejčastějšími chybami.



Zdroj: <https://www.statista.com/>

**Obr. 6 Předpokládaný ekonomický dopad internetu věcí v roce 2025 (v miliardách eur)**

IoT propojuje zařízení a osoby, shromažďuje a sdílí velké množství dat, umožňuje a integruje inteligentnější a autonomnější stroje.

Tolik informací, kolik se k nám dostane v dnešní době během jednoho týdne, se k lidem žijícím před 100 lety dostalo za celý jejich život. K internetu se připojuje stále větší počet zařízení, a ačkoliv nikdo není schopen přesné číslo říci, vědci odhadují, že v roce 2025 bude počet zařízení připojených k internetu atakovat hranici 50 miliard zařízení (viz Obr. 6), přičemž každý měsíc se zvýší počet nově připojených zařízení o 328 milionů (Lasse, 2018). Každou minutu se tak připojí více než 7 500 zařízení.

Je důležité si vyjasnit, o jakých typech zařízení je přesně tato diplomová práce. Existuje velké množství různých „internetových“ zařízení a některá z nich jsou „skutečně“ připojena do internetu, což znamená, že mají přidělenou svou vlastní IP adresu, jsou adresovatelné a vzdáleně přístupné. Většina lidí si pod pojmem Internet věcí představí právě taková adresovatelná zařízení jako webkamera nebo komunikující televize či termostat. Ačkoliv lze tato zařízení rovněž zařadit do oblasti

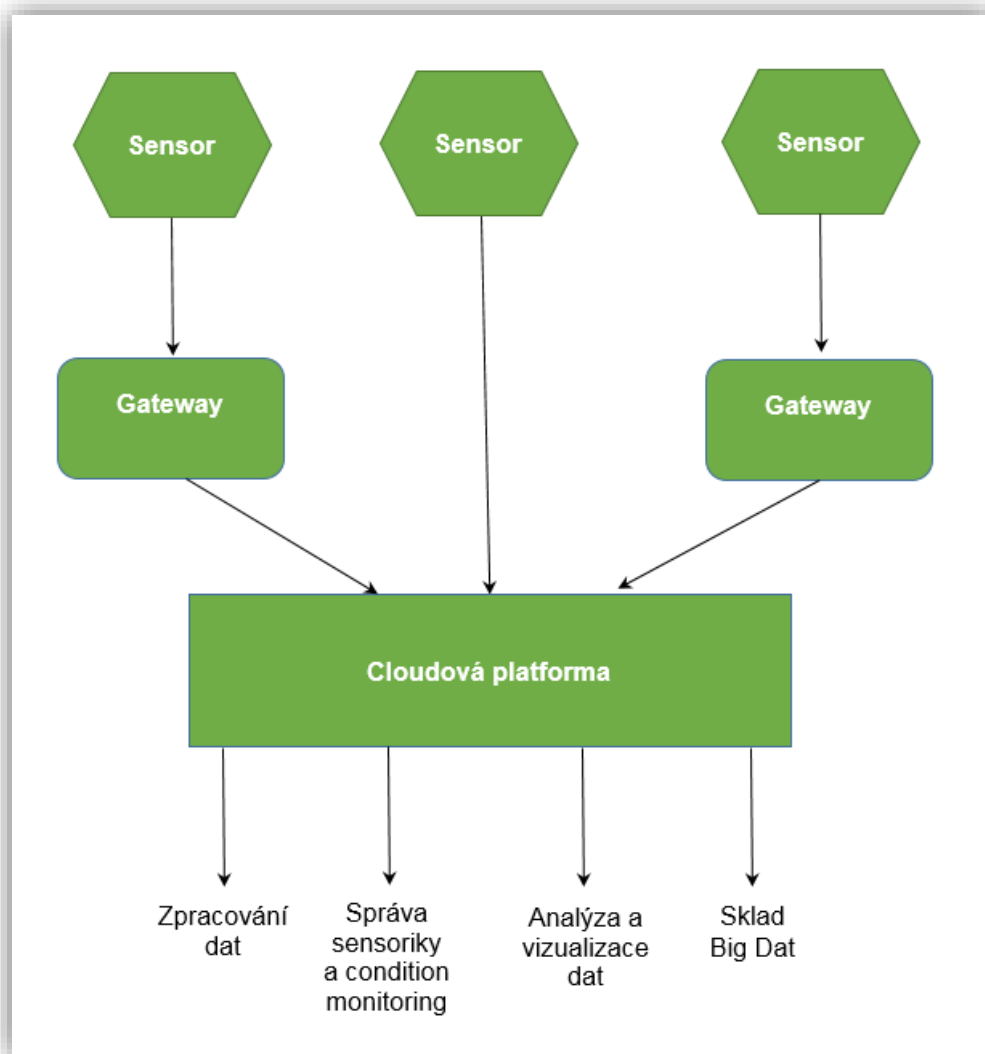
IoT, pravda je taková, že IoT je primárně určen pro vytvoření speciálních datových sítí ze senzorů a čidel, které budou snímat požadovanou veličinu nebo provádět danou akci. Jinými slovy se jedná o zařízení, kterým stačí poslat jen několik zpráv během dne a nepotřebují být stále online, což jim umožní fungovat i několik let pouze s napájením pomocí baterií. Komunikace někdy dokonce probíhá pouze jedním směrem. Tato zařízení nemají žádnou IP adresu a proto je pro ně nutné vybudovat speciální datové komunikační sítě pro Internet věcí.

Zařízení (věc) z pohledu IoT představuje neživý objekt, který v sobě obsahuje elektroniku, software a senzory, pomocí kterých snímá určitou veličinu ( $y$ ). Tyto informace jsou ve formě dat následně přenášeny sítí do cloudu s cílem jejich následné analýzy. Cloud je vzdálený server, na kterém se data ukládají a mohou se s nimi provádět další operace s cílem jejich zpřístupnění koncovému uživateli. Data jsou zpřístupněna koncovým uživatelům nejčastěji pomocí webové stránky nebo mobilní aplikace (Greengards, 2015).

Typickým příkladem aplikace IoT je systém odečtu spotřeb energií (elektřiny, vody, tepla apod.), kde každé měřicí místo nebo výroba je osazeno IoT komunikačním modulem, které odešle například poslední den v měsíci aktuální spotřebu energie (Salazar, 2017). Odpadá tedy nutnost fyzicky obcházet jednotlivá měřicí místa a ručně zapisovat aktuální spotřeby. Jakým způsobem jsou sítě pro IoT koncipovány, je ukázáno na obrázku 7.

Každé IoT zařízení obsahuje komunikační modul, který periodicky vysílá požadované informace ve formě dat k nejbližší základnové stanici (tzv. gateway). Odtud jsou odeslány do vzdáleného serveru / cloudu, kde jsou dále zpracovávány. Data jsou následně zpřístupněna koncovému uživateli většinou pomocí webové stránky či mobilní aplikace, kde se koncový uživatel může v případě měření spotřeby energií podívat na jejich spotřebu v čase.

Dva hlavní důvody, proč je doposud takových aplikací velmi málo, jsou především pořizovací cena jednotlivých čidel a nedostatečná komunikační infrastruktura pro IoT zařízení.



**Obr. 7 Typická architektura IoT**

Samozřejmě lze vybudovat systém, kde bude komunikace řešena fyzickým připojením pomocí kabelů, což je technicky „vyřešené“ a poměrně snadno realizovatelné, ale na druhou stranu velice nákladné a neefektivní.

### 1.3 Přehled současných IoT technologií

Aby bylo možné úspěšně implementovat technologie pro Internet věcí, je nezbytné je znát. Výběr správné technologie připojení je jedním z nejdůležitějších rozhodnutí při vývoji systému na bázi IoT. Přehled těchto technologií je uveden v příloze 1. Pokud aplikace optimálně nevyhovuje, může dojít ke ztrátě výkonu nebo ke zbytečně vysokým provozním nákladům. V případě nejhoršího scénáře se systém nedokáže přizpůsobit změnám technologie bez velkého zásahu do hardware, a to by vedlo k nárůstu nákladů a práce (Topinfo, 2017). V následující části budou představeny výhody a nevýhody různých technologií spadajících do současných IoT

technologií.

## **Základy LPWAN**

LPWAN jsou bezdrátové komunikační sítě, které byly vyvinuty za účelem odstranění mezery mezi mobilními sítěmi a sítěmi krátkého dosahu, jako jsou například Bluetooth a WiFi (Clemons a kol., 2018). Mobilní sítě jsou pro IoT příliš drahé a sítě krátkého dosahu jsou energeticky příliš náročné a mají omezení v dosahu, zejména uvnitř budov. Naproti tomu sítě LPWAN vykazují sice nízké přenosové rychlosti, ale na dlouhé vzdálenosti. Díky tomu jsou ideální pro aplikace, jako je inteligentní měření, průmyslové monitorování a inteligentní města. Vzhledem k tomu, že jejich rychlost přenosu dat je omezená, potřebují podstatně menší výkon než ostatní bezdrátové širokopásmové sítě (WWAN). Díky nízké spotřebě jsou vhodné pro bateriové aplikace.

Všechny analýzy se shodnou na jedné věci - technologie LPWAN se ujme vedení v oblasti konektivity pro IoT. Různé technologie LPWAN se liší v pokrytí, přenosových rychlostech, spotřebě energie, zabezpečení, schopnosti adaptace a interoperability. Z technického hlediska nemůže žádná technologie vynikat ve všech uvedených kritériích. Některé si přímo protiřečí. Je nutné předem provést analýzu, ze které vyplynou kritéria pro výběr optimální technologie.

## **Licenční varianty**

Mezi licenčními a bezlicenčními technologiemi je zásadní rozdíl. Nejznámějšími příkladem bezlicenční technologie je SigFox, reprezentovaný například moduly STMicro nebo Telit a LoRa (např. Murata nebo Telit). Jsou především nákladově efektivnější než licencované technologie: moduly jsou levnější a nepotřebují SIM kartu, takže nevyžadují náklady na jejich správu a výměnu. Jejich hlavním nedostatkem je malé pokrytí. V současné době se sice stále rozšiřuje, ale nějaký čas ještě potrvá, než bude dostatečné. Takže pouze technologie s licencí jsou jasnou volbou pro aplikace, které vyžadují spolehlivé bezdrátové připojení s rozsáhlým pokrytím.

## **Úzkopásmový IoT (NB-IoT nebo Cat-NB1)**

Technologie v licencovaném pásmu nabízejí díky své mobilní komunikační síti lepší adaptaci na změny (tzv. škálovatelnost), kvalitu služeb a bezpečnostní funkce. Ze dvou licencovaných standardů LPWAN NB-IoT a Cat-M1 má NB-IoT pomalejší

přenosovou rychlost: méně než 250 kb/s pro stažení a méně než 20 kb/s pro nahraní. Šířka pásma je 200 kHz. Proto je technologie NB-IoT primárně vhodná pro stacionární aplikace s mimořádně vysokými požadavky na energetickou účinnost. Poskytovatelé sítí v Evropě a Asii (zejména v Číně a Jižní Koreji) používají standard NB-IoT, zatímco USA se rozhodlo pro Cat-M1. V Kanadě a Austrálii jsou rozšířeny oba standardy. Deutsche Telekom rychle rozšiřuje pokrytí celé sítě v Německu a jinde v Evropě. V polovině roku 2017 uvedla na trh dva startovací balíčky pro technologii NB-IoT. V roce 2017 se Nizozemsko stalo první zemí na světě, kde má síť NB-IoT stoprocentní pokrytí. (Schaal a kol., 2018).

Moduly pro aplikace NB-IoT obsahují čip Telit NE910C1, který kombinuje maximální energetickou účinnost s vysoce spolehlivým pokrytím sítě, včetně vnitřků budov. Díky tomu je vhodný pro inteligentní měření, bezpečnost, prodejní stánky či místa a lékařské aplikace.

Čip spadá do formátu xE910 (28 x 28 mm<sup>2</sup>), díky tomu lze jednoduše provést výměnu za čip ve stejném formátu. Čip NE866B1 od společnosti Telit nabízí velmi podobnou funkcionalitu. Jeho menší pouzdro spadá do formátu xE866 (19 x 15 mm<sup>2</sup>) a je ideální pro použití ve velmi malých zařízeních.

### **LTE kategorie M1, Cat M1 nebo LTE-M**

Ve srovnání s NB-IoT má standard Cat M1 vyšší přenosovou rychlost až 1 Mb/s. Na rozdíl od NB-IoT podporuje aplikace zahrnující přenos hlasu - Voice Over LTE (VoLTE). Cat M1 navíc umožňuje přepínání z jedné bezdrátové buňky do další, takže je vhodná pro mobilní a pohyblivé aplikace, jako je telematika a řízení vozového parku. Je nutné dodržet objem dat v rámci přenosové rychlosti.

Telit má ve svém portfoliu následující moduly pro technologii Cat M1. Moduly ME910C1 a ME866A1 mají stejný formát jako moduly NB-IoT. To znamená, že může být nainstalován v zařízení správný modul v závislosti na zemi a podporované bezdrátové technologii bez nutnosti drahého přepracování. Navíc ME910C1 je specifický v tom, že jde o kombinované řešení Cat M1 a NB-IoT.

### **Koncept rodiny Telit**

Unifikovaný design, globální uplatnitelnost je koncept všech modulů ve formátu xE910 a xE866. Členové formátu xE910 podporují různé technologie, datové rychlosti a standardy mobilní komunikace, jako jsou GSM / GPRS, UMTS /

HSPA +, 1xRTT, EV-DO, LTE pro různé kategorie (kategorie 1, 3, 4, NB1 nebo M1). To uživatelům poskytuje potřebnou flexibilitu pro produkty M2M, stejně jako snadnou migraci z 2G na 3G a na 4G. Všechny modely jsou založeny na identickém formátu Land Grid Array (LGA) s rozměry pouhých 28,2 x 28,2 mm<sup>2</sup>. Vysoce kompaktní moduly formátu xE866 v rozměrech 19 x 15 mm<sup>2</sup> pokrývají standardy GSM / GPRS, UMTS / HSDPA, LTE a LoRaWAN v kombinaci s Bluetooth Low Energy.

Na základě tohoto přehledu technologií lze dojít k závěru, že nevhodné k použití pro IoT projekty jsou sítě LTE kategorie M1, Cat M1, LTE-M, nebo Telit, protože mají jinou technologii nebo slabý průnik, či spotřebují hodně elektrické energie.

#### **1.4 Bezpečnostní rizika při realizaci IoT projektu**

Vzhledem k tomu, že průmyslový internet a IoT přináší síťovou inteligenci fyzickým věcem kolem nás, je nutné být opatrný ohledně jejich bezpečnosti. Zvýšení počtu připojených zařízení vede ke zvýšení bezpečnostních rizik: způsobení fyzické újmy lidem v době prostoje a poškození zařízení.

Zabezpečení IoT lze postavit na základě čtyř základních kamenů: zabezpečení komunikace, ochranu zařízení, sledování zařízení a sledování síťových interakcí. Na tomto základě je možné vytvořit silný a snadno nasaditelný bezpečnostní systém, který může zmírnit negativní dopad většiny bezpečnostních hrozeb na internetu, včetně cílených útoků.

##### **Zabezpečení komunikace**

Komunikační kanál musí být zabezpečen, technologie šifrování a autentizace se používají k zajištění toho, aby zařízení věděla, zda mohou důvěřovat vzdálenému systému. Je skvělé, že nové kryptografické technologie, jako je ECC (Elliptic Curve Cryptography), pracují desetkrát lépe než jejich předchůdci v 8 bitových 8MHz čípech s nízkou spotřebou energie 8MHz. Stejně důležitým úkolem je řídit klíče k ověření pravosti dat a autenticity kanálů pro jejich příjem. Vedoucí certifikační autority již vložily certifikáty zařízení do více než miliardy zařízení IoT, které umožňují autentizaci široké škály zařízení, včetně mobilních základnových stanic, televizorů a dalších (Doodle Labs (SG) PTE. LTD., 2018).

##### **Ochrana zařízení**

Ochrana zařízení je primárně zaměřena na zajištění bezpečnosti a integrity kódu



programu. Podepsání kódu je vyžadováno pro potvrzení platnosti jeho spuštění, ochrana je také potřebná při běhu, takže útočníci jej nepřepíší při spuštění. Kód podepisování kryptograficky zajišťuje, že po podpisu nebyl změněný a je pro zařízení bezpečný. To lze provést na úrovni aplikací a firmwaru a dokonce i na zařízeních s monolitickým firmware. Všechna důležitá zařízení, ať již to jsou senzory, regulátory nebo něco jiného, musí být nakonfigurována tak, aby spouštěla pouze podepsaný kód. Zařízení musí být po spuštění kódu chráněna v dalších fázích. To pomůže ochraně založené na hostiteli, která poskytuje kontrolu přístupu k systémovým zdrojům a souborům, kontrole připojení, karanténě, ochraně proti vniknutí, ochraně založené na chování a pověsti. Také tento dlouhý seznam funkcí hostitelské ochrany zahrnuje blokování, protokolování a upozorňování na různé operační systémy IoT (Lea, 2018). V poslední době bylo mnoho nástrojů pro ochranu hostitele přizpůsobeno pro IoT a nyní jsou dobře rozvinuté a laděné, nevyžadují přístup ke cloudu a vyváženě zatěžují výpočetní prostředky zařízení IoT.

### **Sledování zařízení**

Je zřejmé, že zařízení IoT budou stále zranitelná. Dokonce i kód založený na obfuskátoru<sup>1</sup> v kritických systémech je nakonec rekonstruován a útočníci v něm najdou zranitelná místa. Nikdo nechce a často nemůže posílat své zaměstnance na návštěvu každého IoT zařízení, aby aktualizoval firmware, zejména pokud jde například o vozový park nebo o síť monitorovacích senzorů distribuovaných po stovky kilometrů.

### **Sledování interakcí sítě**

Některé hrozby dokážou překonat všechna přijatá opatření bez ohledu na to, jak je vše chráněno. Proto je zásadní, aby byly v oblasti IoT analytické nástroje schopné toto odhalit. Bezpečnostní analytické systémy pomohou lépe porozumět síti, zjistit podezřelé, nebezpečné nebo škodlivé anomálie.

### **Vývoj paradigmatu**

Většina zařízení IoT je „uzavřený systém“. Zákazníci nebudou moci přidat bezpečnostní software poté, co zařízení opustí továrnu. Taková intervence zruší záruku a často jednoduše není možná.

---

<sup>1</sup> je konverzní softwarová pomůcka, která převádí zdrojový kód konkrétního programovacího nebo skriptovacího jazyku do téhož zdrojového kódu v témže jazyku, ale provede v něm několik změn.

Z tohoto důvodu musí být ochranné funkce zpočátku zabudovány do zařízení IoT tak, aby byly v jejich architektuře bezpečné. Pro většinu odvětví bezpečnosti informací je taková „bezpečnost uvnitř“, tedy zabudovaná do výroby zařízení v továrně, nový způsob, jak zajistit ochranu. To platí i pro klasické bezpečnostní technologie, jako je šifrování, ověřování, kontrola integrity, prevence narušení a možnost bezpečné aktualizace. Vzhledem k úzkému vztahu mezi hardwarem a softwarem v modelu IoT je někdy snazší, aby programy ochrany používaly vylepšené hardwarové funkce a vytvořily "externí" úroveň zabezpečení. Je skvělé, že mnoho výrobců čipů již vestavělo bezpečnostní prvky do svého hardwaru. Ale úroveň hardwaru je pouze první vrstvou, která je nezbytná pro integrovanou ochranu komunikací a zařízení. Komplexní zabezpečení vyžaduje integraci správy klíčů a bezpečnostních analýz.

Absence dokonce jednoho ze základních kamenů v pozadí bezpečnosti zanechá široký prostor pro akce vetřelců. Zbývá jen připomenout, že úspěšné zabezpečení systému začíná modelováním rizik.

## **2 ŠKODA AUTO a.s. a IoT**

### **2.1 ŠKODA AUTO a.s.**

ŠKODA AUTO a.s. je největší český výrobce automobilů. Hlavním sídlem společnosti je Mladá Boleslav, ale v České republice soustředí svou výrobní produkci ještě v dalších městech, kterými jsou Kvasiny a Vrchlabí. Tato společnost je nyní vlastněna pouze jediným majitelem a to Volkswagen Finance Luxemburg S.A.

ŠKODA AUTO vyrobila v roce 2018 v České republice celkem 886 100 vozů (2017: 858 100 vozidel) a to odpovídá meziročnímu nárůstu o 3,3 %. Svým obratem, tržbami a počtem zaměstnanců patří k nejdůležitějším článkům české ekonomiky. Automobilka do roku 2025 bude investovat několik miliard eur do elektromobility, digitalizace a nových projektů dle konceptu Průmysl 4.0.

### **2.2 Oddělení PSZ - Centrální technický servis**

Ve ŠKODA AUTO a.s. využívají specialisté Centrálního technického servisu (PSZ) své dlouholeté zkušenosti z oblasti vibrodiagnostiky, tribodiagnostiky a speciálních měření a také IoT v laboratoři ŠKODA FabLab (viz Obr. 8). Jsou schopni nabídnout komplexní řešení od sběru dat přes IoT zařízení, jejich analýzu, až po návrh řešení a podporu při jednání s dodavateli.

Útvar PSZ se zabývá následujícími činnostmi:

- interní opravy a údržba strojních zařízení včetně konstrukčního zajištění,
- externí opravy a rekonstrukce strojních zařízení,
- metodika a standardizace, ITS,
- speciální diagnostika a metrologie,
- systémová podpora údržeb,
- revize a servis vyhrazených technických zařízení (zařízení zdvihací, elektrická, plynová, tlakové nádoby a ocelové konstrukce),
- těžká mechanizace – transport SZ,
- péče o dlouhodobý majetek (vyřazování, prodej),
- technická evidence strojního zařízení,
- správa ploch, metodika a servis úklidu,
- operativní servis infrastruktury budov a staveb,
- **standardizace sběru dat, condition monitoring,**
- **prediktivní údržba, napojení na digitální reporting a dokumentaci.**

## 2.3 Laboratoř PSZ - FabLab

ŠKODA FabLab (FabLab<sup>2</sup>), vedený Centrálním technickým servisem, je testovacím centrem prediktivní údržby, strojních zařízení a komponentů ve ŠKODA AUTO a.s. Probíhá zde aplikovaný výzkum pro potřeby ŠKODA AUTO a.s., jako bezprostřední reakce na konkrétní případy a objednávky ze strany uživatelů ŠKODA AUTO a.s. a potřeby Centrálního technického servisu (např. uvolňování nových komponent do interních technických standardů). FabLab zvyšuje know-how ŠKODA AUTO a.s. v oblasti sběru, analýzy a interpretace dat ze strojních zařízení a komponentů.

ŠKODA FabLab je jednou z reakcí firmy na čtvrtou průmyslovou revoluci (Industry 4.0) a stal se součástí Strategie 2025 ŠKODA AUTO a.s., jako jeden z pilířů pro oblast výroby s cílem zajistit maximální využitelnost strojních zařízení pomocí prediktivní údržby.



Zdroj: Interní dokumentace ŠKODA AUTO a.s.

**Obr. 8 Laboratoř ŠKODA FabLab**

### Hlavní činnosti ŠKODA FabLab

V rámci ŠKODA FabLab řeší specialisté Centrálního technického servisu projekty především v oblasti prediktivní údržby, kde jsou schopni nabídnout komplexní

---

<sup>2</sup> FabLaby po celém světě umožňují přístup k moderním přístrojům a metodám inovací každému, kdo o ně má zájem. Dílny nebo laboratoře tak zároveň dávají prostor pro setkávání s dalšími lidmi, kteří chtějí objevovat a tvořit.

řešení od sběru dat, přes jejich analýzu až po návrh řešení a podporu při jednání s dodavateli. V rámci projektů jsou využívány dlouholeté zkušenosti z oblasti vibrodiagnostiky, tribodiagnostiky a speciálních měření, které Centrální technický servis zajišťuje napříč ŠKODA AUTO a.s.

Specialisté Centrálního technického servisu ve ŠKODA FabLab provádí také měření a testování strojních zařízení a komponentů. Cílem je vybrat strojní zařízení a komponenty, které jsou nejvhodnější pro specifické prostředí provozů ŠKODA AUTO a.s., a zároveň potvrdit parametry udávané výrobcem. Výsledky těchto měření jsou podkladem pro rozhodnutí o doplnění seznamů uvolněných dílů v rámci interních technických standardů.

Na základě zkušeností z výše uvedených činností je možné odborně argumentovat při jednáních s dodavateli, o změně / úpravě jimi dodávaných komponentů / strojů, případně komplexních řešení.

### **3 Návrh a rozpracování strategie implementace IoT platformem a technologií v prostředí společnosti ŠKODA AUTO a.s.**

#### **3.1 Návrh strategie implementace IoT platformem a technologií v prostředí společnosti ŠKODA AUTO a.s.**

Samotná podstata IoT je jen částečně o technologiích. To, co dává těmto neživým technologiím zásadní význam, je vize a odhodlání posunout byznys směrem k novým příležitostem digitálního věku.

Na začátku cesty k úspěšné digitalizaci může pomoci tento jednoduchý dotazník.

Je potřeba se zamyslet a pokusit se co nejpřesněji odpovědět na šest jednoduchých otázek.

1. Co je typický problém, který firmu stojí peníze?
2. Jaká data jsou potřeba, aby bylo problému předejito?
3. Kde je možné je pořídit?
4. V jaké formě mají být, aby byly využitelné?
5. Komu je tyto informace potřeba zpřístupnit?
6. Jak změřit, že se situace zlepšila?

Každé IoT řešení lze rozdělit do následujících kroků:

#### **1. Popis dat**

V této fázi se rozhoduje, jaký typ dat se bude sledovat, pomocí jakých druhů senzorů se tato data pořídí a kde budou tyto senzory umístěny.

#### **2. Připojení senzorů**

Zde se společně s dodavatelem vyhodnotí, zda je možné si vystačit s jednoduchým senzorem, nebo je potřeba posbírat více dat dohromady a navrhnout tak složitější řešení (set senzorů). Je možné, že tyto senzory budou propojeny mikrokontrolérem, který je bude ovládat.

#### **3. Připojení do cloudu**

V této fázi se řeší způsob přenosu dat ze senzoru do cloudu. Dodavatel také vypočítá, jaká kapacita sítě bude potřeba.

## 4. Cloud

Zde se rozhodne, do jakého cloudu se budou data ukládat a jaký budou mít objem. Kromě ukládání jsou klíčové také doplňující funkce, např. rychlost přístupu k datům, protokoly, zabezpečení, geolokace a další.

## 5. Zpracování dat

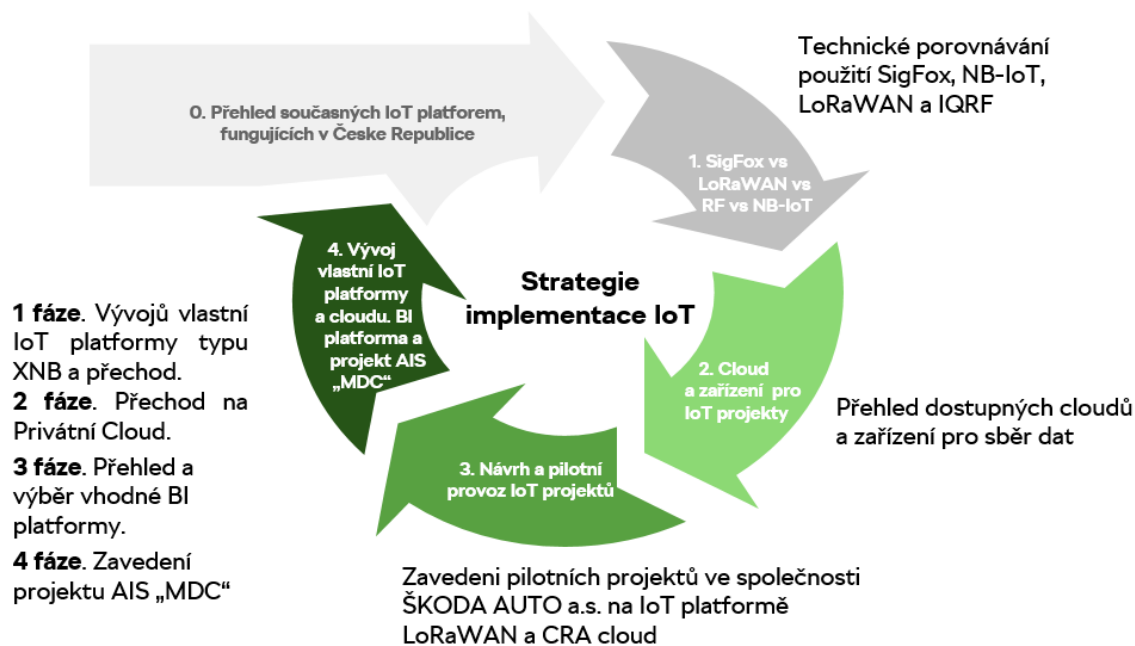
Hrubá data mohou poskytnout první vodítka, ale pro účinnou práci s informacemi je potřeba je zpracovat a podrobně analyzovat. V této fázi je nutné se zaměřit na služby, které cloud nabízí pro zpracování dat.

## 6. Prezentace dat

Data zůstanou jen čísla, pokud nebudou předaná ve správnou chvíli, správným lidem a ve srozumitelné podobě. Zde se musí určit, co, komu, kdy a jak je potřeba prezentovat. Dodavatel může pomoci nastavit reporty tak, aby vyhovovaly přesně potřebám.

## Popis jednotlivých kroků strategie implementace IoT platform

Na obrázku 9 autor přepravil návrh jednotlivých kroků strategie implementace IoT platform a technologií v prostředí společnosti ŠKODA AUTO a.s.



Obr. 9 Postup strategie implementace IoT platform

Autor nultým a prvním krokem (viz Obr. 9) této strategii vytváří přehled současných IoT platform fungujících v České republice a na základě porovnání těchto platform vybírá nejvhodnější z nich pro použití na IoT projekty.

Dalším krokem je přehled dostupných cloudů a zařízení pro sběr dat. Následně je potřeba vyřešit zavedení vyhovujícího cloudu a provést nákup zařízení, které je vhodné pro vybranou platformu.

V další části kapitoly 3 jsou autorem rozpracovány pilíře navržené strategie. Jde o zavedení jednotlivých projektů v provozech společnosti ŠKODA AUTO a.s. a jejich stručný popis a plán postupu realizace budoucích IoT projektů. Poslední krok strategie je rozpracován do tří fází:

1. fáze: Vývoj vlastní IoT platformy typu XNB.
2. fáze: Přejít na privátní cloud.
3. fáze: Přehled a výběr vhodné BI platformy.
4. fáze: Zavedení projektu AIS „MDC“.

### **3.2 Přehled současných IoT platform, fungujících v České republice**

Na základě analýzy literární rešerše je možné říct, že na českém trhu IoT platform působí tyto čtyři hlavní dodavatelé: SigFox, NB-IoT, IQRF a LoRaWAN (Příbyl a kol., 2017). Níže je každá z platform detailněji rozebrána a na základě analýzy je navržen výběr nejvhodnější z nich k použití na IoT projekty ve společnosti ŠKODA AUTO a.s.

#### **Platforma SigFox (uzavřená platforma)**

Společnost SimpleCell se stala prvním českým veřejným operátorem pro Internet věcí. SimpleCell buduje síť v České republice ve spolupráci se společností T-Mobile, která poskytuje svoji infrastrukturu pro umístění základnových stanic. Pro SigFox je tedy nutné vybudovat novou infrastrukturu a k tomu poslouží již stávající stožáry T-Mobile, které se osadí moduly pro komunikaci v síti SigFox.

Zařízení SigFox komunikuje v nelicenčním pásmu. Využití v tomto pásmu je zdarma, ale je nutné dodržovat podmínky stanovené Českým telekomunikačním úřadem o frekvenci 868 MHz. Tato frekvence špatně prochází zeminou a pokrytí budovách jen do suterénu. Pro pokrytí v nižších podzemních patrech bude zapotřebí lokální vykrývač. Každé zařízení musí obsahovat komunikační čip (nazývané také jako modem), který umožňuje komunikaci se SigFox sítí. Modem neobsahuje ani SIM kartu, ani nemá žádnou IP adresu. Každé zařízení je v síti



jednoznačně identifikováno pomocí unikátního 32bitového SigFox ID, které je přiřazeno při výrobě. Vlastnictví daného zařízení se převádí on-line pomocí PAC (Porting Authorization Code) kódu. Tento PAC kód je kupujícímu sdělen při koupi a v okamžiku, kdy si zařízení zaregistruje, je tento kód přegenerován. Pokud by se zařízení mělo převést v budoucnosti na jiného vlastníka, pak stávající vlastník pouze sdělí novému vlastníkovi PAC kód a tím se dostane pod jeho správu a opět se vygeneruje nový PAC kód. Starý vlastník ztrácí veškerý přístup k danému zařízení. Z tohoto principu vyplývá, že v jednu chvíli má k zařízení přístup pouze jeden vlastník, což je především z důvodu zabezpečení a ochrany. Všechny zprávy jsou podepsány privátním klíčem a šifrovány, takže uživatel si může být jist pravostí zprávy.

Rychlost přenosu dat je pouze 100 bit/s. Díky tomu je počet zpráv za den vyslaných zařízeními maximálně 144 a vysílací výkon maximálně 25 mW. Zařízení s technologií SigFox mají velmi malou spotřebu energie a nízké pořizovací náklady (SigFox modem lze pořídit za cenu nižší než 5 dolarů), nese to s sebou omezení přenosu uživatelských dat na 0 - 12 bajtů a dobu přenosu dat od 2 do 5 sekund. Zpětná komunikace je aktivována pouze na vyžádání koncovým zařízením (senzorem).

Samotná komunikace vypadá tak, že zařízení vyšle data k nejbližší základnové stanici, odkud jsou přeposlány pomocí zabezpečeného IP spojení do SigFox cloudu, odkud jsou data dostupná pro vlastníky zařízení pro další zpracování. Jelikož je SigFox globálním operátorem, jsou tato data poslána na jejich servery. Operátor se stará pouze o zajištění pásma a samotné servery, ke kterým aplikace přistupují. Jsou umístěny ve Francii, kde je platforma vyvíjena. Tímto se celý SigFox stává uzavřenou záležitostí a pro koncového zákazníka svým způsobem černou schránkou. Cena za připojení zařízení do sítě SigFox je závislá na počtu připojených SigFox zařízení a na objemu přenesených dat. Technologie SigFox také aktuálně prochází standardizačním procesem.

### **Platforma NB-IoT (uzavřená platforma)**

NB-IoT je nová bezdrátová úzkopásmová LPWAN technologie speciálně vyvinutá pro IoT (Schaal, 2018). Největší její předností je možnost nasazení v pásmech GSM a LTE.

NB-IoT ctí standardy 3GPP (dohoda o spolupráci mezi telekomunikačními asociacemi z roku 1998 s cílem vyvinout a udržovat 3G sítě), následně také LTE a IMS (IP Multimedia Subsystem). NB-IoT bude poskytovat zlepšené pokrytí uvnitř budov, podporu masivního počtu zařízení, velmi nízkou cenu koncových zařízení i jejich spotřebu energie a také optimalizovanou architekturu sítě. Je tak velmi vhodná pro opětovný „refarming“ GSM kanálů.

K dosažení co nejlepšího využití spektra byla NB-IoT navržena s řadou možností nasazení pro GSM, WCDMA nebo LTE:

- standalone – výměna GSM nosiče za NB-IoT nosič (využití hlavně v oblastech se souběžným pokrytím GSM a WCDMA/LTE),
- in-band – skrze flexibilní využití části LTE nosiče,
- guard-band (ochranné pásmo) – ať už v síti WCDMA nebo LTE.

Je předpokládáno, že NB-IoT doplní v budoucnu na trhu již zavedené technologie jako SigFox či LoRaWAN a rozšíří nabídku českých mobilních operátorů.

Nevýhodou je to, že jde o novou technologii a zároveň nejsou zařízení dostupná na českém trhu, i když se předpokládá jejich rychlé rozšíření. Proto v současné době není daná platforma vhodná pro implementaci ve společnosti ŠKODA AUTO a.s.

### **Platforma IQRF (uzavřená platforma)**

Aliance IQRF přináší bezdrátové sítě bez programování. Vstupem do Aliance IQRF získá uživatel přístup k plné funkcionalitě DPA, což nesmírně usnadňuje vývoj a používání bezdrátových modulů IQRF. DPA zajišťuje kompatibilitu všech produktů, využívajících tento protokol a díky tomu lze do produktu přidat funkcionalitu bezdrátové komunikace během několika dnů až týdnů (Sos electronic, 2018).

Pokud však zájemce nepředpokládá tak rychlé využití produktu a poplatek 1 000 Eur za členství v IQRF Alianci je pro příliš mnoho, nabízí se nyní možnost využívat DPA a hardwarové profily i bez vstupu do IQRF Aliance. Jediné, co je potřeba, je vyvíjet s moduly označenými předponou „DC“ (data controlled).

Různé RF moduly IQRF jsou dostupné ve dvou verzích, standardní a „DC“. Pokud je organizace členem IQRF Aliance, postačí standardní moduly (bez označení „DC“). Pokud není členem IQRF Aliance a přesto chce využívat výrazného zjednodušení vývoje v podobě DPA a hardwarových profilů, pak jsou ideální právě moduly s předponou „DC“. Za mírně vyšší cenu tak lze získat možnost vyvíjet a

používat bezdrátovou komunikaci a řízení s maximálním zjednodušením. Používat moduly „DC“ se vyplatí zhruba do množství 400 ks / rok, pak je již výhodnější používat standardní (levnější) moduly a stát se členem IQRF Aliance.

#### **Základní vlastnosti:**

- kompletní technologie pro bezdrátovou komunikaci,
- založeno na modulech transceiverů se zabudovaným OS,
- otevřená funkcionalita, aplikace v jazyce C,
- komunikace v paketech, max 64B,
- dosah několik stovek metrů / skok (hop), až 240 hops/paket,
- velmi malá spotřeba 25  $\mu$ A / příjem,
- nízká rychlost 19,2 kb/s,
- podporuje sítě MESH, IQMESH<sup>3</sup> implementován v OS,
- žádné licenční poplatky,
- snadná implementace.

Za nevýhodu této IoT platformy se považuje zejména malý dosah, cca 700 m.

#### **Platforma LoRaWAN (otevřená platforma)**

LoRa je fyzická vrstva resp. radiová modulace, která se používá pro vytvoření telekomunikačního spojení na velkou vzdálenost. Starší bezdrátové systémy rovněž využívají modulaci založenou na frekvenčním posunu (FSK), neboť se jedná o velmi účinnou a robustní modulaci. Při nízkém vysílacím výkonu lze dosáhnout spolehlivého přenosu informací (IDLAB, 2018).

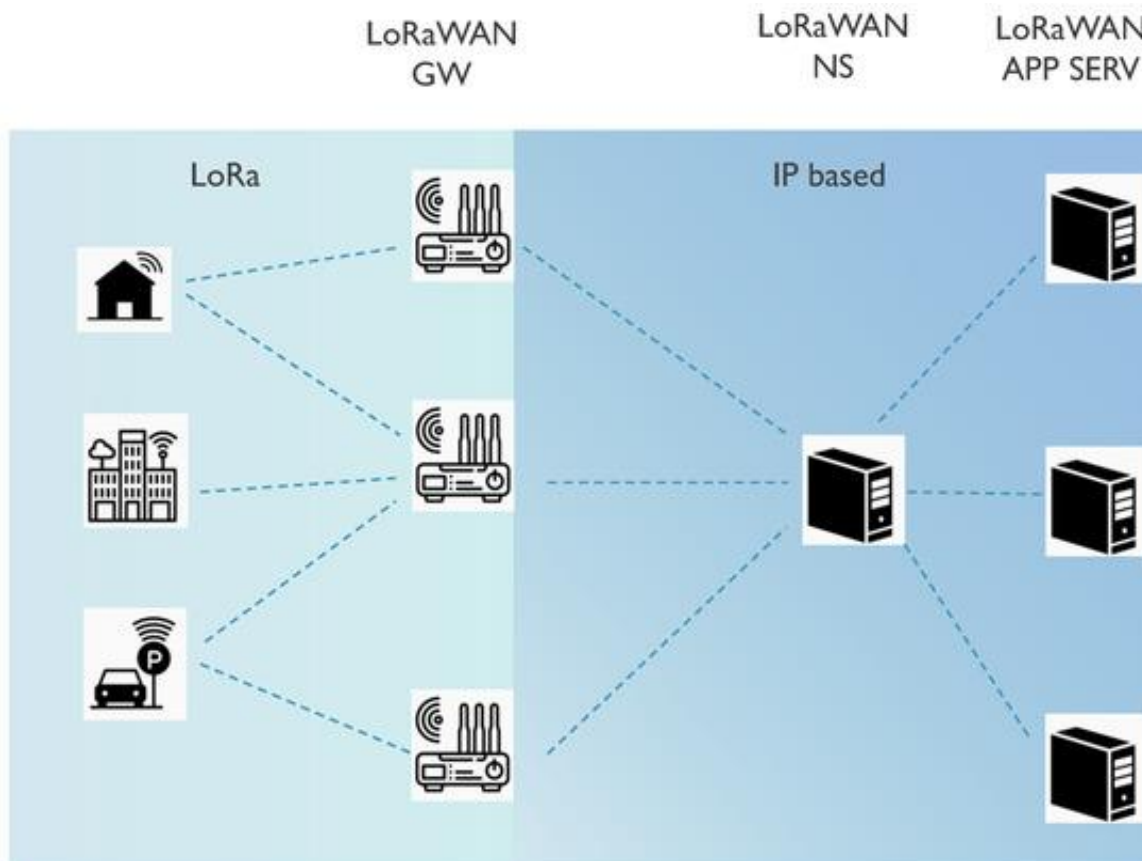
Systém LoRa je založen na modulaci rozprostřeného spektra, která má velmi podobnou charakteristiku jako FSK modulace, avšak na mnohem větší vzdálenost. Provoz v rozprostřeném spektru se začal používat v armádě již před několika desítkami let především z důvodu dlouhého dosahu a odolnosti vůči rušení.

LoRa je prvním komerčním řešením s nízkými investičními i provozními náklady a obrovským obchodním využitím. Hlavní výhodou technologie LoRa je její dlouhý

---

<sup>3</sup> V bezdrátových sítích typu MESH jsou data přenášena pomocí směrovacího mechanismu (s pomocí uzlů sítě). Tento přístup zvyšuje dosah, odolnost, spolehlivost a snižuje pravděpodobnost potenciálních problémů hvězdicové topologie.

dosah. Jedna brána nebo jedna základna může velmi rychle pokrýt i velmi rozsáhlá území, např. celá města nebo stovky kilometrů čtverečních. Celkový dosah této technologie je závislý na překážkách, které musí v prostředí překonat (hustota zastavěnosti, členitost terénu atd.).



Zdroj: <https://www.mdpi.com>

**Obr. 10 LoRaWAN topologie sítě**

LoRa a LoRaWAN mají nejlepší parametry pro navázání spojení ze všech jiných standardizovaných komunikačních technologií (viz Obr. 10). Celková útlumová hodnota na spojení je obvykle uváděna v desítkách decibelů (dB). Díky těmto parametrům lze pokrýt celou zemi s minimálním množstvím infrastruktury.

LPWAN technologie je určena pro čidla a aplikace, které potřebují posílat relativně malé množství dat na velké vzdálenosti vícekrát za hodinu a z různého prostředí. Tato technologie vyžaduje baterii s několikaletou životností.

LoRaWAN sítě používají dvě bezpečnostní vrstvy – jednu vrstvu pro síť, druhou pro aplikace. Síťovou bezpečnost zajišťuje autentifikace koncového zařízení k jednotlivému síťovému uzlu. Na straně aplikační vrstvy se zajišťuje bezpečnost tím, že síťový operátor nemá přístup k aplikačním datům uživatele.

Aplikační data koncového uživatele jsou navíc zakódována pomocí AES metody používající k výměně klíče IEEE EUI64 identifikátor.

### 3.3 Porovnávání a výběr vhodné IoT platformy

Existují tedy tři IoT platformy, které je možné využít pro projekty ve společnosti ŠKODA AUTO a.s. a na základě srovnání je nutné rozhodnout, která z nich je nejvhodnější.

**Tab. 2 IoT platformy podle technologie**

	LoRaWAN	SigFox	IQRF
Systém	CDMA, open	UNB, closed	Krátký dosah, mesh, open
Standardizace	Vlastnická	Vlastnická	Vlastnická
Pokrytí v městě	2-5 km	3-10 km	Stovky metrů
Pokrytí mimo město	5-20 km	30-50 km	Stovky metrů
Způsob komunikace	Pásmo ISM	Pásmo ISM	Pásmo ISM
Bezpečnost	Šifrování klíčem	Šifrování dle LTE	AES-128 encryption
Poskytovatel v ČR	ČRA	Simplecell	IQRF

Z tabulky 2 je patrné, že IoT platforma LoRaWAN je technologicky výhodnější než jiné vybrané platformy. Navíc, LoRaWAN je otevřenou platformou, na rozdíl od její konkurence SigFox a IQRF.

Současně je LoRaWAN mnohem variabilnější, pokud jde o výběr zařízení (viz příloha č. 3). Přestože je Semtech jediným výrobcem čipů pro LoRaWAN, snímače a koncové zařízení mohou být od jiných výrobců. To znovu ukazuje na to, že LoRaWAN je pružnější platforma než SigFox a IQRF (viz Tab. 3).

**Tab. 3 Porovnávání SigFox, LoRaWAN, IQRF**

Vlastnosti	LoRaWAN	SigFox	IQRF
Modulace	SS chip	UNB / GFSK / BPSK	GFSK
Rx Šířka pásma	500-125 KHz	100 KHz	100 kHz
Rychlost přenosu dat	290 bps-50 Kbps	100 bit / sek	1,2 - 115 kbit / s
Max. # zprav / denně	Neomezený	12/8 bytes Max UL: 140 zprav / denně	Typická 19.836 kbit / s 20 kbps
Max. výstupní výkon	79 mW	25 mW	12 mW
Rozpočet propojení	154 dBm	151 dBm	120 dB
Životnost baterie - 2000 mAh	105 měsíců	90 měsíců	Nízký výkon Rx: 1,68 let Extra nízký výkon Rx mód: 11,4 let
Energetická účinnost	Velmi vysoké	Velmi vysoké	Velmi vysoké
Rušení imunity	Velmi vysoké	Nízké	Nízké
Soužití	Ano	Ne	
Bezpečnost	Ano	Ano	
Počet připojeních zařízení	Uplink: >1 mil., Downlink: <100 tis.	<1 mil.	239

■ vhodné  
■ nevhodné

### 3.4 Popis nevýhod použití platformy LoRaWAN

Poskytovatelé řešení LoRaWAN hovoří o otevřenosti technologií a vytvoření otevřeného ekosystému. Pro koncového zákazníka je však tato "otevřenost" podmíněna:

- Koncová zařízení (čítače, snímače) různých výrobců jsou nekompatibilní a neměnná.
- Zařízení mají odlišný firmware, algoritmy pro zpracování datových balíčků (úroveň zobrazení modelu OSI) jsou pro všechny výrobce odlišné. Při přechodu od jednoho poskytovatele LoRaWAN k jinému zákazníkovi je nutné samostatně vyřešit problém kompatibility. Tento úkol bude vyžadovat vývoj aplikace pro zpracování dat ze zařízení.
- Šifrovací klíče jsou uloženy výhradně na serveru poskytovatele řešení, který zákazníkovi dodal zařízení. Pokud dojde k přechodu na jiného poskytovatele LoRaWAN, nebude možné zařízení používat bez šifrovacích klíčů – řešení nebude fungovat. Konečný klient, který používá řešení jednoho poskytovatele LoRaWAN, zůstává pevně spojen s poskytovatelem tohoto

řešení. Při pokusu o přepnutí na jiného poskytovatele LoRaWAN bude muset změnit základní stanice, koncové zařízení a software - tj. celý systém.

- Aby si zákazníka „udrželi“, blokují jednotliví výrobci stanice na úrovni programu, analogicky s mobilními operátory, kteří blokují modemy. Účelem blokování je vývoj jeho sítě a prevence „úniků“ klientské základny z jednoho poskytovatele k druhému.
- Výrobce nastavuje své řešení pro práci na konkrétním frekvenčním pásmu (od 868,7 do 869,2 MHz) na frekvencích, které pracují pouze s jeho základnovými stanicemi.

Díky manipulaci s kódem umožňuje LoRaWAN demodulovat signály až do úrovně -20 dB. Vzhledem k hladině šumu to vyvolává řadu negativních faktorů, které nakonec ovlivňují rozsah sítě.

### **3.5 Požadavky, přehled a výběr cloudů**

#### **Požadavky na poskytovatele dostupných cloudů**

Požadavky na poskytovatele cloudů lze shrnout následovně:

##### 1. Obchodní kondice a procesy:

- Finanční kondice. Poskytovatel by měl vykazovat stabilitu a být v dobré finanční situaci s dostatečným kapitálem pro úspěšný provoz v dlouhodobém horizontu.
- Organizace, zásady správného řízení, plánování a správa rizik. Poskytovatel by měl mít formální řídicí strukturu, ustavené zásady správy rizik a formální proces hodnocení svých externích poskytovatelů služeb a dodavatelů.
- Důvěryhodnost. Je důležité si zkontrolovat reputaci poskytovatele a podívat se, s kým spolupracuje. Potom si zjistit úroveň zkušeností práce s cloudem. Přečíst si recenze a pobavit se se zákazníky, kteří jsou v podobné situaci.
- Obchodní znalosti a technické know-how. Poskytovatel by měl rozumět oboru podnikání a plánům a měl by být schopný se s tím vyrovnat na expertní úrovni.
- Audit dodržování předpisů. Poskytovatel by měl být schopný ověřit dodržování předpisů pro všechny požadavky pomocí nezávislého auditu.

## 2. Administrační podpora:

- Smlouvy o úrovni služeb (SLA). Poskytovatelé by měli být schopní zaručit základní úroveň služeb, která zákazníkovi bude vyhovovat.
- Generování sestav o výkonu. Poskytovatel by měl být schopný dodávat sestavy o výkonu.
- Sledování prostředků a správa konfigurace. Mělo by existovat dost kontrol, aby mohl poskytovatel sledovat a monitorovat služby poskytované zákazníkům a všechny změny provedené v jejich systémech.
- Účtování a fakturace. To by mělo být automatické, aby mohly být sledovány prostředky, které jsou používány, a účtované náklady. Měla by existovat i podpora pro problémy týkající se účtování.

## 3. Technické funkce a procesy:

- Snadnost nasazení, správy a upgradů. Je nezbytné se ujistit, že má poskytovatel mechanismy, které usnadní nasazení, správu a upgrady softwaru a aplikací.
- Standardní rozhraní. Poskytovatel by měl používat standardní rozhraní API a transformace dat, aby organizace mohla snadno budovat připojení ke cloudu.
- Správa událostí. Poskytovatel by měl mít formální systém pro správu událostí, který je integrovaný do jeho systému sledování a správy.
- Správa změn. Poskytovatel by měl mít dokumentované formální procesy pro požadavky na změny, jejich protokolování, schvalování, testování a přijetí.
- Hybridní funkce. I když zákazník nechce od začátku používat hybridní cloud, měl by se přesvědčit, že je poskytovatel tento model schopný podporovat. Má výhody, které může chtít využít později.

## 4. Postupy zabezpečení:

- Infrastruktura zabezpečení. Měla by existovat obsáhlá bezpečnostní infrastruktura pro všechny úrovně a typy cloudových služeb.
- Zásady zabezpečení. Měly by platit obsáhlé zásady zabezpečení a postupy pro řízení přístupu k systémům poskytovatele i zákazníka.



- Správa identit. Změny libovolné aplikační služby nebo hardwarové komponenty by měly být autorizované na úrovni osobní nebo skupinové role a mělo by být vyžadováno ověření pro kohokoli, kdo mění aplikace nebo data.
- Zálohování a uchování dat. Měly by platit a být dodržovány zásady a postupy zajišťující integritu dat zákazníků.
- Fyzické zabezpečení. Měly by platit kontroly zajišťující fyzické zabezpečení, včetně přístupu k hardwaru umístěnému na společném místě. Datová centra by také měla být jištěna, aby byla zařízení a data chráněná před ničivými událostmi. K dispozici by mělo být zdvojené napájení i sítě, a také zdokumentovaný plán zotavení po havárii a kontinuity podnikových procesů.

### **Přehled cloudů pro IoT**

Pro potřeby IoT jsou dostupné následující cloudy (SigFox, 2018):

#### 1. Microsoft Azure

Jeho služeb využívá například Schneider Electric, Rolls-Royce, Thyssenkrupp a další. Pro IoT nabízí Azure tyto služby:

- IoT Hub - připojení, monitoring a kontrola aktivit IoT zařízení.
- Event Hub - určeno pro měření na dálku, tzv. telemetrie.
- Stream Analytics - zpracování datového toku v reálném čase.
- Machine learning - metodika založená na konstrukci automatizovaného modelu, která bude systematizovat Big Data pomocí vestavěných matematických algoritmů. Pomocí ní lze najít skryté závislosti mezi několika faktory. S nejjednodušším příkladem strojového učení se setkáváme v prediktivní údržbě strojů, kde přijímáme data ze senzorů (tzv. hodnoty teploty, vlhkosti, tlaku a vibrací), a ty tvoří základ strojového učení.
- Notification Hubs - škálovatelnost, posílání notifikací.

#### 2. Google Cloud Platform

Google nabízí Seeed Studio pro BeagleBone Green Wireless startovací desku, která představuje základy komunikace s Google Cloud Platform. Mezi uživatele cloudu od Googlu patří - Motorola, Airbus, HTC, Philips, Coca-Cola.

### 3. Oracle Cloud

Nabízí veškeré služby, které se od cloudu dají očekávat. Největší výhodou je, že dokonce umožňuje umístit Oracle Cloud ve svém vlastním datovém centru.

### 4. IBM Bluemix

Využívá IBM Watson IoT Platformu, která umožňuje okamžitý přístup k naměřeným datům. Používá otevřený protokol MQTT nebo HTTP.

### 5. SAP HANA

SAP HANA je řešení od společnosti SAP. Nabízí komplexní portfolio řešení pro IoT. Mezi uživatele cloudu od SAPu patří Siemens.

### 6. Bosch IoT Cloud

Bosch IoT Cloud pomáhá urychlit IoT projekty, zkrátit dobu uvedení na trh nových řešení. Prostřednictvím IoT se získají bezpečnostní mechanismy, které pomohou ochránit data. Bosch IoT Cloud má pevná pravidla pro nakládání s osobními údaji zákazníků – respektování práva zákazníků vědět, co se děje s jejich osobními údaji. Zákazníci si mohou sami zvolit, zda poskytnou své osobní údaje a samy rozhodnou, kdy data vymazat.

### 6. Samsung Artik

Samsung Artik zahrnuje kompletní řešení – hardware, software, cloudové připojení a bezpečnost. Moduly obsahují bezdrátové připojení WIFI, Bluetooth a Zigbee, které poskytují dostatečnou flexibilitu. Díky dostupné a otevřené API SDK lze rychle vytvořit aplikace pro domácí i průmyslové prostředí. Snadné vytvoření komunikace „peer to peer“ až po složitější MESH sítě. Tato platforma v sobě zahrnuje nástroje pro vývoj, nasazení a správu IoT systémů a se skládá z tzv. modulů a cloudu.

### 7. Predix

Specializuje se výhradně na IoT v průmyslu. Dokáže připojit senzory, motory a inteligentní stroje. Predix je průmyslová platforma IoT, která dokáže nasbíraná data zpracovat tak, aby lépe poskytla přehled o provozním chodu celé továrny, podniku atd.

### 8. CRA Cloud Platform

České Radiokomunikace dnes mohou formou služby poskytnout kapacitu cloudu prakticky do druhého dne za vysoce konkurenční cenu, čímž jsou na českém trhu

unikátní. Pro jejich klienty se jedná o výhodné řešení, neboť ušetří náklady na vlastní infrastrukturu, lidské zdroje a zároveň mají díky použité technologii Isilon od EMC zaručenu nejvyšší možnou dostupnost uloženého multimediálního obsahu s dosaženým SLA 99,99 % v případě, že klient využívá replikace dat do obou datových center (viz Obr. 11).

#### 9. Amazon Web Service (AWS)

Síla cloudového řešení nabízeného Amazonem je hlavně ve zpracování dat a šíře nabízených služeb.

#### 10. ThingWorx

Tato platforma se specializuje na shromažďování, analýzy a zpětné využití dat. V ČR její používá na IoT projekty společnost FOXON s.r.o.

### **Přehled vybraného cloudu - CRA Cloud Platform**

Pro pilotní provoz IoT ŠKODA AUTO a.s. nemají ambice realizovat celé projekty od začátku až do konce ve své režii. Cílem je vybudovat telekomunikační infrastrukturu, která zajistí přenos dat formou zpráv přenášených radiovou komunikací od jednotlivých čidel.

A výhodou outsourcingu cloudu CRA pro ŠA mělo by stát to, že kromě robustní infrastrukturní části, CRA nabízejí i prostor a zázemí pro data, která s využitím IoT bezprostředně souvisejí. Pro tuto oblast zpřístupnily IoT cloud, který umožňuje hostování IoT aplikace, ukládání velkého množství dat z IoT zařízení a rovněž správu dat – pro jejich další využití (CRA a.s., 2018).

CRA současně se aktivně podílejí na budování ekosystému partnerů sítě LoRaWAN v České republice, a to nejen na úrovni výrobců, dodavatelů hardwaru a koncových čidel a uživatelských aplikací, ale také na úrovni zákazníků a projektů, které se již zrealizovaly a mohou spolu sdílet zkušenosti, jež přispějí k dalšímu rozvoji této technologie u nás. V rámci budování partnerského prostředí s možností navázání další spolupráce České Radiokomunikace organizují softwarově i hardwarově zaměřené akce a počátkem roku 2017 otevřely unikátní prostor pro spolupráci v oblasti IoT a to stejné mělo by stát výhodou pro ŠKODA AUTO a.s., kvůli výběru IoT platformy od LoRaWAN.

 <b>Snížíte náklady</b> Žádné investiční náklady (CAPEX).	 <b>Zbavíte se starostí</b> Nemusíte se starat o hardware ani software.	 <b>IT pod kontrolou 24/7</b> Ke svým službám máte přístup kdykoliv a odkudkoliv.	 <b>Opravdu vysoký výkon</b> AŽ <b>2THz, 10 TB RAM, 3PB</b> úložiště. Vše si řídíte podle aktuální potřeby.
--	--	--	--

**Vyberte si variantu**

<p><b>1 Virtual Private Centre</b></p> <p>Virtuální datové centrum na infrastruktuře, která se svými parametry přizpůsobí vždy, když potřebujete.</p>	<p><b>2 Private Cloud</b></p> <p>Virtuální datové centrum na dedikované infrastruktuře. Získáte s ním garantovaný výkon a <u>speciální vlastnosti</u>.</p>	<p><b>3 Private Cloud PAYG</b></p> <p>Kombinuje výhody obou předchozích variant. Získáte a platíte jen to, co právě potřebujete, a spolu s tím i garantovaný výkon.</p>
---	--	---

Zdroj: <https://www.cra.cz>

### **Obr. 11 Interní stránky CRA Business Cloudu**

Certifikace:

1. Common Criteria for Information Technology Security Evaluation na úrovni CC EAL 4+.
2. Mezinárodní standard (ISO/IEC 15408) pro certifikaci počítačové bezpečnosti.
3. Bezpečnost provozu a managementu IT služeb podle ISO 27001 a certifikátu ISO 20000-1.
4. Certifikace managementu kvality ISO 9001 a managementu životního prostředí ISO 14001.
5. Technologie provozované v datovém centru DC TOWER s certifikací ANSI-TIA942.

Bezpečnost datových center:

1. Webový aplikační firewall, ochrání webové portály a jejich API před většinou útoků na aplikační vrstvu, webový server a databázovou vrstvu.
2. Datové centrum DC TOWER poskytuje vysokou bezpečnost a dostupnost. Využívá k tomu např. zálohované napájení, nonstop ostrahu a technickou podporu.
3. Každý technologický prvek je v datovém centru instalován v redundanci minimálně N+1.

Vysoká dostupnost (SLA):

- Služba je garantována ve výši 99,99%.

- Variabilní cena – od 999 Kč.

Fixní cena – od 15,83 Kč/měsíc za jedno připojené zařízení.

### **3.6 Přehled dostupných zařízení pro sběr dat**

#### **Microchip**

Microchip spolupracuje s Amazon Web Service. Nabízí vývojový kit AWS Zero touch secure Provisioning kit, který je založen na procesoru Atmel. Byl vyvinut společně s Amazon. Má integrovanou sadu eliptických křivek ECC508, která zaručuje bezpečné připojení k internetu. Vývojový kit IoT Ethernet Kit, je založen na procesoru PIC32MZEF a využívá LAN8740 k připojení k internetu a k Amazon cloudu. Tento kit obsahuje operační systém FreeRTOS™ a dokáže komunikovat pomocí MQTT protokolu. Bluetooth Low Energy Client Module (BLECM) je navržen tak, aby umožnil rychle ovládat přednastavené mobilní aplikace. Pomocí mikroBUS sběrnice dokáže komunikovat s širokou škálou čidel.

#### **Texas instruments**

Na stránkách má přehledně uveden seznam platforem, se kterými spolupracuje. Jsou mezi nimi známá jména jako IBM Watson IoT, či ThingWorx. Mezi méně známá patří například Tago, Sierra Wireless či Vitanet. Pro bezdrátovou komunikaci nabízí integrované čipy a jejich vývojové kity. Mezi ně patří CC3200 (ARM Cortex M4 a WIFI onchip), který komunikuje pomocí Bluetooth ultra low power. CC1350 (Sub-1Ghz a Bluetooth low energy), CC2650 (Bluetooth, ZigBee). Pro drátovou komunikaci nabízí Ethernetové moduly DP83867CR, DP83822I nebo pro RS485 převodník SN65HVD1794. Nelze opomenout mikroprocesory řady Sitara a MSP430. Dále nabízí veškeré podpůrné obvody pro bezdrátové zařízení jako je battery management, různé sensory tlaku, teploty, světla, vlhkosti atd.

#### **StMicroelectronics**

Spolupracuje převážně s IBM Watson a Microsoft Azure. Pro IoT aplikace dokáže IoT nabídnout širokou škálu integrovaných obvodů. Pro bezdrátovou konektivitu nabízí obvody pro komunikaci pomocí Bluetooth low energy, Sigfox, WiFi a Sub 1GHz RF. Používá mikrokontroléry řady Cortex M4, M3 či M0. Důležitou součástí každého bezdrátového zařízení je mít dokonalý power management, o který se postará STC3115. StMicroelectronics je silný v portfoliu sensorů. Mezi ně patří akcelerometry, gyroskopy, teplotní a vlhkostní sensory a mnoho dalších. Neméně

důležitou součástí je zpracování signálů ze senzorů.

### **Intel Edison**

Spolupracuje s Amazon Web Service, Microsoft Azure a IBM Bluemix. Jedná se o populární chip, který s okolím dokáže komunikovat pomocí Bluetooth či WiFi. Nabízí mnoho volně stažitelných zdrojových kódů. Nabízí mnoho senzorů, které se dají připojit k tomuto modulu.

### **Raspberry Pi**

Populární mikropočítač Rapsberry Pi spolupracuje s cloudem. Tento málo známý poskytovatel cloudu nabízí veškeré služby, které jsou dostačující pro aplikace IoT.

### **BeagleBone**

Je oficiálním vývojovým kitem Amazon Web service. AWS IoT Starter Kit obsahuje desku Beaglebone Green.

### **Silicon Labs**

Nabízí hardware platformu Thunderboard, která komunikuje pomocí Bluetooth. Lze k němu jednoduše připojit sensory CO<sub>2</sub>, tlaku, světla, rychlosti, teploty či vlhkosti. K dispozici je také aplikace pro mobilní telefony Android i iOS. Data jsou uložena v uložišti Firebase od Googlu.

### **Arduino**

Velkou výhodou například je, že vývojáři na platformě Arduino Yun nebo Tian mohou pro připojení zařízení od společnosti QNAP kromě rozhraní Ethernet a USB využívat i Wi-Fi a Bluetooth Low Energy. Pro bezpečnější přenos dat je možné využít i technologii LoRa. Kombinace platformy Arduino a funkcionality QNAP umožňuje snadné vytváření a implementaci kreativních IoT řešení. Jejich uživatelé tak mohou využívat jak komerční IoT produkty, tak i widgety přímo navržené pro Arduino. To vše lze snadno propojit s technologiemi QNAP. Platformy Arduino Yun a Tian podporují konektivitu prostřednictvím Wi-Fi a BLE, díky čemuž překonávají předěl mezi bezdrátovými senzory a zařízeními pro IoT na jedné straně a QNAP NAS s podporou rozhraní Ethernet a USB, na straně druhé. Nové platformy Arduino Uno Wi-Fi a Primo lze přímo bezdrátově připojit k Yun nebo Tian, což dává vývojářům celou řadu možností při vývoji komerčních aplikací pro IoT. QIoT Suite Lite nabízí velké množství protokolů a aplikací ovládacího panelu, které vývojářům pro vývoj elektronických desek umožňují používat různé senzory a zároveň možnost

implementovat takové aplikace, jako jsou například Node-RED a Freeboard. Data přijímaná senzory lze pomocí různých protokolů (MQTT, CoAP, atd.) přenášet do QNAP NAS, díky čemuž mohou uživatelé například pomocí ovládacího panelu dálkově monitorovat prostředí ve své domácnosti.

Současné senzory se zlevní a díky tomu se začnou objevovat nové způsoby jejich využití. Trh senzorů se do roku 2025 bude neustále vyvíjet. Nové senzory umožní pokrýt detekci širší škály situací a událostí, díky novým algoritmům bude možné ze stávajících senzorových technologií získat více informací.

### **3.7 Pilotní testovací provoz IoT LoRaWAN**

Autor dále navrhne několik pilotních testovacích projektů pro ŠKODA AUTO a.s. s využitím platformy LoRaWAN a cloud platformy od CRA, které byly zvoleny na základě porovnání dostupných platform a cloudů jako nejvhodnější pro realizaci IoT projektů. V případě, že budou tyto projekty životaschopné a přínosné, měl by být dalším krokem implementace navržené strategie vývoj vlastní IoT platformy a přechod na privátní cloud.

Na základě rešerše a analýzy odborných zdrojů, případových studií a jednání s odborníky ŠKODA AUTO a.s., autor vybral a navrhuje pět pilotních testovacích IoT projektů. Tyto projekty, by měly, podle názorů odborníků, přenést přidanou hodnotu pro výrobu i společnost.

#### **První projekt: Inteligentní osvětlení**

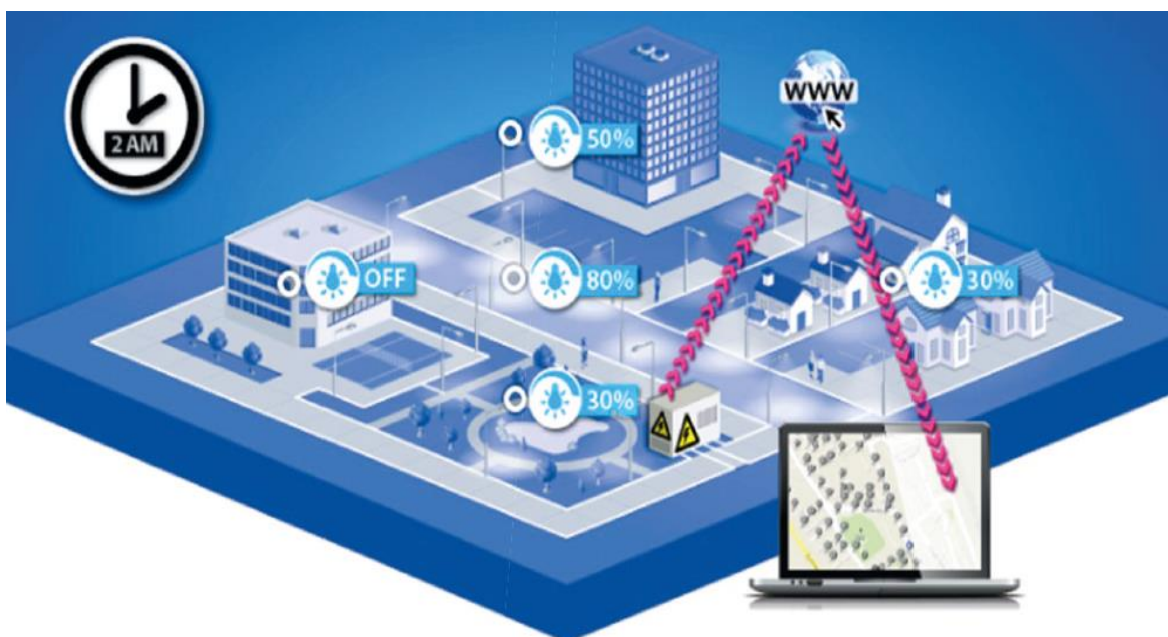
Cíl: chytré využití elektřiny.

Termín realizace projektu – 2020-2021.

Očekávaný přínos: ušetření nákladů na osvětlení až o 40%.

„**INTELILIGHT** je aplikace LoRaWAN umožňující inteligentně řídit osvětlení. Při klasickém provozu se ovládá pro zapnutí/vypnutí osvětlení celá jedna větev sítě osvětlení.

Systém INTELILIGHT (viz Obr. 12) absolutně mění provoz celé sítě. Zásadní změna spočívá v tom, že celá síť osvětlení je stále pod napětím a ovládá se každá jednotlivá lampa.



Zdroj: Raycom s.r.o.

**Obr. 12 INTELILIGHT – inteligentní osvětlení**

Inteligentní pouliční systém osvětlení zajišťuje ovládání každé jednotlivé lampy zvlášť, což umožňuje svítit každé lampě ve stanovenou dobu, přičemž pouliční světla stále poskytují dobré osvětlení komunikace a chodníku pro zajištění bezpečnosti provozu vozidel a pohybu chodců.

**Druhý projekt: Měření dodávek vody, plynu a tepla**

Cíl: měření a kontrola dodávek vody, plynu, tepla.

Termín realizace projektu – 2020-2021.

Očekávaný přínos: ušetření nákladů na vodu, plyn, teplo až o 20%.

Systém LoRaWAN je doslova stvořený i pro inteligentní měření dodávek vody, plynu a elektrické energie, tepelné energie, kvality ovzduší a vzduchu, tlaku, vlhkosti, atd. Vybudování nutné infrastruktury je velmi jednoduché, rychlé a levné, stejně tak i osazení měřičů jednotlivých médií moduly systému LoRa zajišťující přenos dat přímo z měřicího zařízení do systémů dodavatelů jednotlivých komodit.

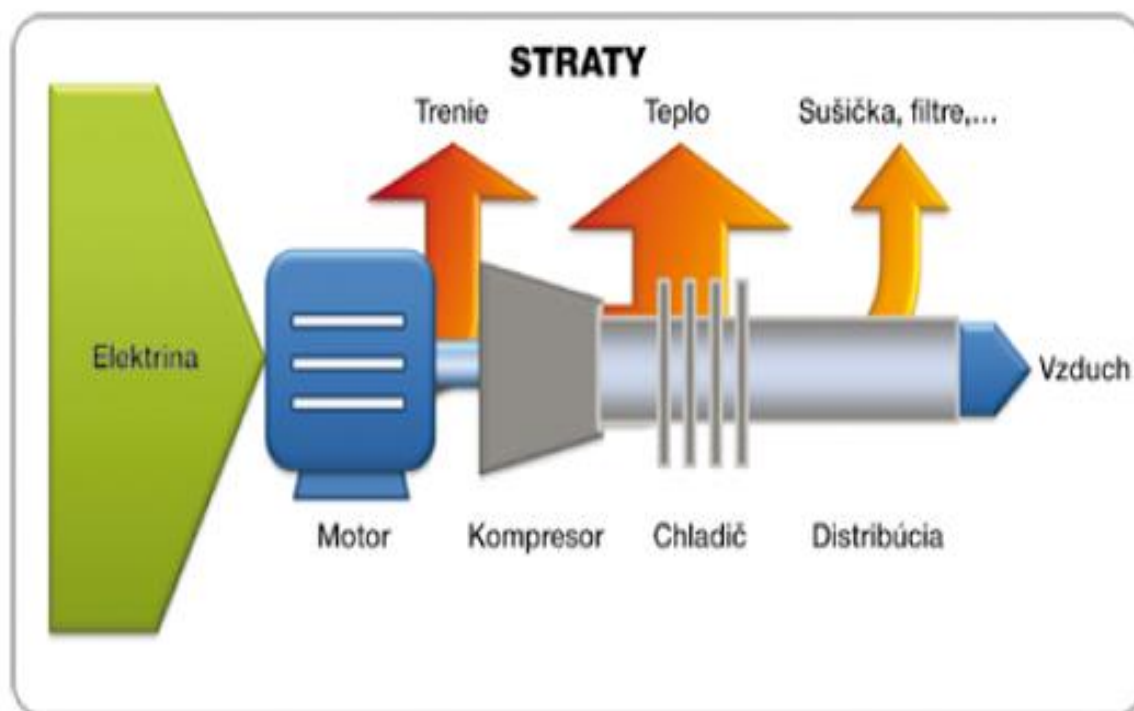
**Třetí projekt: Stlačený vzduch – monitorování ztrát**

Cíl: kontrola a predikce ztrát stlačeného vzduchu.

Termín realizace projektu – 2020-2021.

Očekávaný přínos: zmenšení ztrát stlačeného vzduchu o cca 7 %.





Zdroj: SONOTEC s.r.o.

**Obr. 13 Stlačený vzduch – monitorování ztrát**

Stlačený vzduch je velmi nákladný zdroj energie. Jeho výroba probíhá v kompresoru a pod tlakem. Ztráty jsou způsobeny filtrací a vysušováním (viz Obr. 13). Lze říci, že stlačený vzduch je 10 krát dražší než ekvivalent elektřiny.

Pro oblast tlakového vzduchu a technických plynů je klíčové trvalé monitorování základních parametrů: průtok, tlak a teplota. Na základě těchto dat je možné přesně nasměrovat údržbu a zdroje na místo nejvyšší ztráty a dosáhnout nejvyšší možné úspory s nejnižšími náklady.

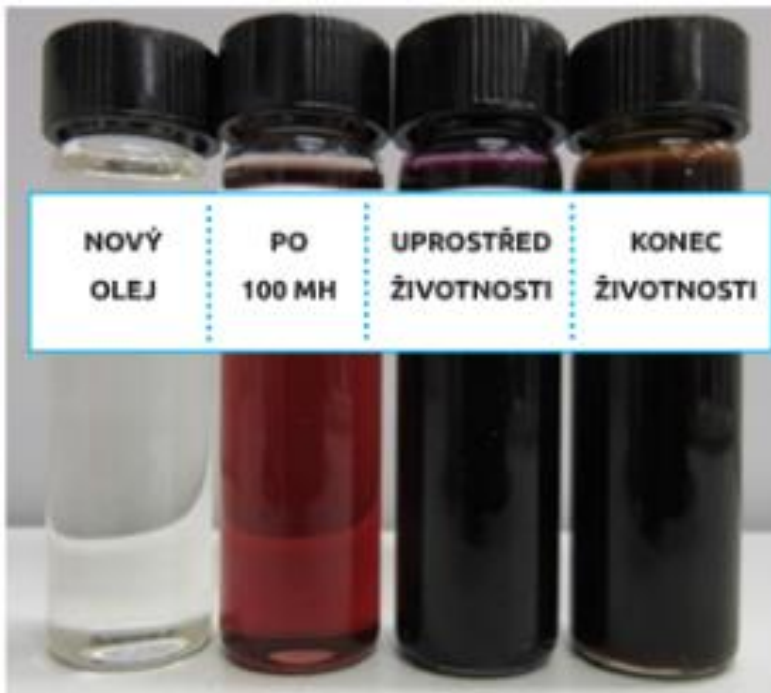
**Čtvrtý projekt: Efektivní analýza mazacího oleje strojního zařízení**

Cíl: detekování jakékoli změny stavu mazacího oleje strojního zařízení.

Termín realizace projektu – 2019-2020.

Očekávaný přínos: efektivnější analýza mazacího oleje.

Projekt je založen na zavádění čidel pro on-line monitorování aktuálního stavu mazacího oleje strojního zařízení, tj. instalaci čidel, která sledují údaje o vibracích, stavu oleje, znečištění a opotřebení.



Zdroj: Interní obrázek oddělení PSZ

#### ***Obr. 14 Životní cyklus mazacího oleje strojního zařízení***

Tato čidla neustále posílají data do cloudu, kde algoritmy pro strojové učení umožňují spouštět alarmy ve chvíli, kdy je detekována jakákoli změna stavu. Po odhalení anomálie ihned následují doporučení, jaká nápravná opatření je nutno provést (viz Obr. 14).

#### **Pátý projekt: Kvalita vzduchu ve vnitřním prostředí průmyslových hal**

Cíl: Monitoring toxických plynů a kvality kyslíku v průmyslových halách pomáhá zajistit bezpečnost pracovníků a zboží.

Termín realizace projektu – 2019-2020.

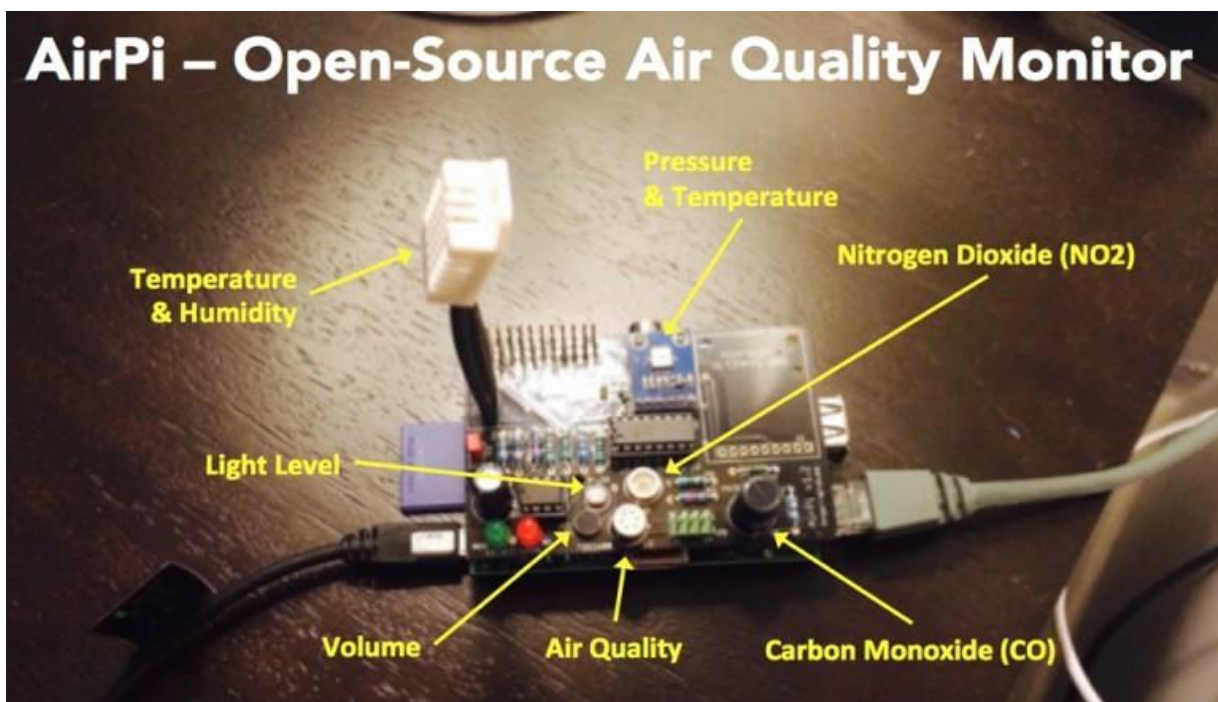
Projekt založen na komunikaci s chytrými budovami. Server, do kterého senzory samy posílají hodnoty, bude přímo napojený na řízení klimatizace budov (viz Obr. 15). Podle množství polétavých částic ve vzduchu dokáže vydat pokyn k nasazení správného filtru do větrání budovy a chránit tak lidi před vnikem škodlivých látek do plic.

Průmyslová výroba má svá specifika při požadavcích na kvalitu vzduchu:

- Čistý, bezprašný prostor, typickým příkladem jsou např. autolakovny, tiskárny atd.
- Udržení konstantní vlhkosti a teploty přiváděného vzduchu.

- Zajištění dostatečné cirkulace vzduchu bránící potenciálnímu znehodnocení vyrobeného produktu například ve skladových halách.
- Likvidace vzniklých výparů či jiné kontaminace vzduchu nežádoucích třeba pro obsluhu strojů.
- Chlazení výrobků při výrobě pro jejich další zpracovávání.

Výsledkem by mělo být vytvoření a udržení komfortního prostředí ve výrobě.



Zdroj: <https://www.tindie.com/products/tmhrtly/airpi-kit-v14-raspberry-pi-weather-shield/>

**Obr. 15 AirPi Kit**

Seznam zařízení, která jsou koupena pro realizaci těchto projektů, je uveden v příloze 2.

#### **Další náměty pro projekty:**

- Příprava pilotních měření pro oblast výrobních strojních zařízení, přenos dat a jejich adekvátní rychlé zpracování, včetně vyhodnocení a zpětné vazby.
- Příprava pilotních měření pro oblast Prediktivní údržby, přenos dat a jejich adekvátní rychlé zpracování, včetně vyhodnocení a zpětné vazby.
- Příprava pilotních měření pro oblasti transportu a logistiky, přenos dat a jejich adekvátní rychlé zpracování, včetně vyhodnocení a zpětné vazby.
- Zaměření na vývoj adekvátních analytických metod, senzorických systémů, systémů s dlouhodobým nezávislým energetickým zdrojem.

### 3.8 Návrh vývoje vlastní IoT platformy typu XNB a přechod na Privátní Cloud

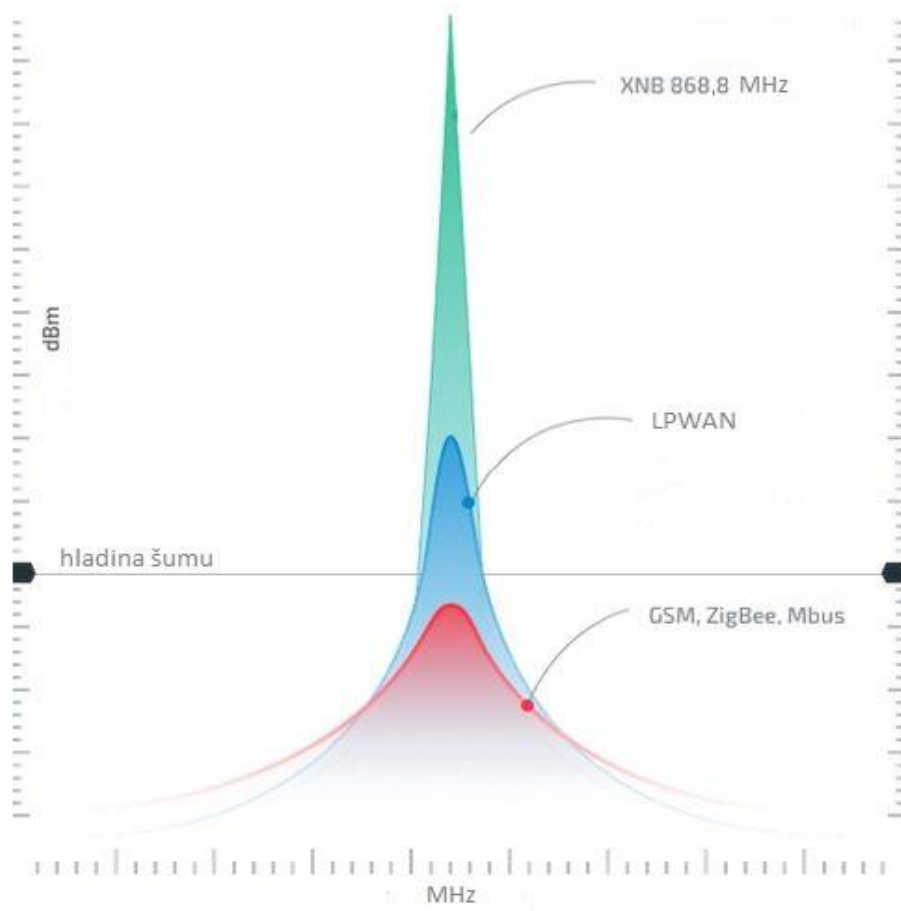
Technologie LoRaWAN má své nevýhody (viz kapitola 3.4), proto autor nabízí, jako východisko z této situace, vývoj vlastní IoT platformy a přechod na privátní cloud. Platforma by měla být typu XNB (Extended Narrowband).

Technologie XNB je podobná technologii LoRaWAN, ale má zásadní rozdíl: zatímco LoRaWAN používá úzkopásmovou modulaci, XNB používá ultraúzké pásmo (viz Obr. 16).

Cíl: nezávislost na externích dodavatelů služeb IoT.

Realizace projektu:

- Vytvoření vlastní soukromé komunikační IoT platformy – min. 6 měsíců.
- TCO (celkové náklady spojené s vlastnictvím) – od 1 mil. Kč.



Obr. 16 IoT platforma typu XNB

Co je pro to nutné udělat:

- Zapojování firem typu Start-Up do procesů vývoje a implementace soukromé IoT komunikační platformy pro ŠA v rámci vzdálené prediktivní analýzy nebo údržby.
- Vzdělávání managementu firmy a jeho seznamování s konceptem IoT v podmínkách výrobních procesů.

#### **Vlastnosti přenosu dat v úzkém pásmu rádiových frekvencí:**

- při pevném vysílacím výkonu generuje modulace s vyšším přenosem dat širší, ale méně energeticky náročný signál,
- rozdíl v energii mezi signálem a hladinou hluku určuje spolehlivost komunikačního kanálu a dosahu,
- problém zvýšení rozsahu je ten, že není možné dosáhnout úzkopásmového signálu snížením přenosové rychlosti na aplikační úrovni - víceúrovňová složitost komunikačního stohu, kódování a další faktory vedou k šíření spektra,
- XNB (Extended Narrowband) je přepracovaný komunikační protokol na nejnižší fyzické úrovni,
- na fyzické úrovni je DBPSK4 modulace použita k přenosu signálu v IoT síti,
- šířka pásma kanálu vysílacího zařízení je v tomto případě 100 Hz, s minimálním datovým tokem 50 zpráv,
- úzkopásmový signál a vysoká energie na každý bit přenášené informace poskytují vynikající energetický potenciál komunikačního kanálu a vysokou odolnost proti šumu.

#### **Výhody IoT platformy typu XNB:**

- XNB je navržena tak, aby vyměňovala data zařízení ve velkých, distribuovaných oblastech s minimální spotřebou energie – ideální pro budování bezdrátových sítí LPWAN pro IoT, telemetrii M2M,
- protokol XNB je přizpůsoben pro přenos signálu s frekvencí 868,8 MHz

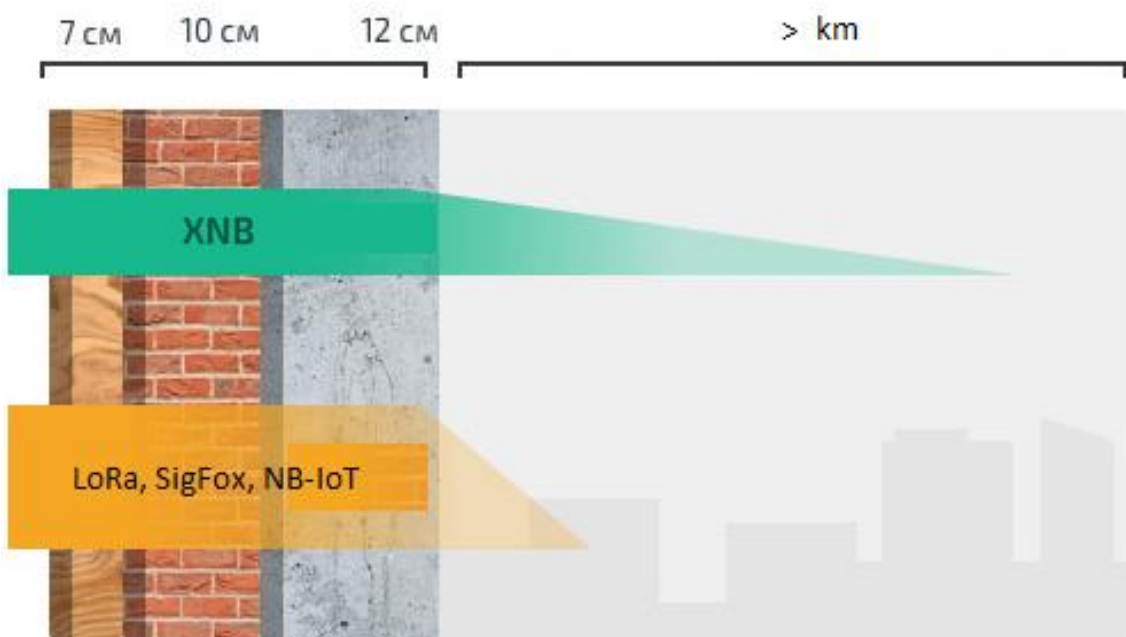
---

<sup>4</sup> Binární – fázové klíčování - je digitální modulace založená na posunutí fáze harmonické nosné o 0° nebo 180° v závislosti na hodnotě binárního modulačního signálu.

(nevyžaduje licenci),

- rozsah přenosu signálu 10-40 km (viz Obr. 17),
- pracuje v ultra-úzkém pásmu a XNB umožňuje vysílání signálu na desítky kilometrů i v obtížných městských podmínkách,
- 5 000 dostupných kanálů,
- šířka pásma vysílacího zařízení je 100 Hz, šířka dostupného spektra je 500 kHz, pro signalizaci XNB je k dispozici až 5 000 úzkopásmových kanálů,
- data jsou šifrována algoritmy XTEA-256, GOST R34.12-2015,
- neomezená škálovatelnost,
- díky službě XNB se kapacita stanice zvýší na 2 000 000 zpráv denně, což stačí k vytvoření superintenzivní bezdrátové sítě IoT,
- sofistikované matematické algoritmy řeší problém efektivního využívání spektra a přenosu dat v úzkém pásmu,
- stavební konstrukce nejsou překážkou a přenos je možný i ze sklepů a silných stěn, kde GSM nedosahuje,

obousměrná komunikace umožňuje dálkově přeprogramovat a spravovat zařízení LPWAN, která pracují s protokolem XNB.



**Obr. 17** Převaha IoT platformy typu XNB

## Přechod na privátní cloud

Cíl: nezávislost od externích dodavatelů služeb cloudu

Realizace projektu:

- Termín realizace – cca 6 měsíců.
- TCO (celkové náklady spojené s vlastnictvím) – cca 2 mil. Kč.

U společností, které uvažují o přechodu z internetu do cloudu, se může stát, že to bude nesnadný úkol. Je možné rozlišit tři klíčové kroky, které popisují, jak lze data shromažďovat z okrajových zařízení a rychle a snadno přenášet na platformy založené na cloudových počítačích (CRA a.s., 2018):

1. Služba dat. První krok spočívá v přípravě na zajištění spolehlivého přenosu dat v síti. Povolení aplikací IoT vyžaduje shromažďování velkého množství dat z mnoha senzorů a zařízení. Obvykle jsou to starší zařízení, která jsou nekompatibilní se sítěmi založenými na protokolu IP. Je proto důležité, aby servery sériových zařízení (které přenášejí data mezi počítačovým sériovým portem a místní sítí Ethernet) a protokolové brány (které umožňují komunikaci zařízení) zajišťovaly interoperabilitu zařízení. To usnadňuje a zefektivňuje sběr dat.

2. Připojení dat. Druhý krok, připojení IoT, se zaměřuje na interní síť společnosti, která zajišťuje, že je spolehlivá a bezpečná. V podstatě je to most mezi koncovými zařízeními společnosti a cloudem.

Pro zajištění spolehlivosti je důležité posoudit šířku pásma sítě. Provozovatelé sítí obvykle potřebují aktualizovat proudové přepínače, přístupové body a směrovače, aby podpořili zvýšení úrovně přenosu dat. Dále je vhodné uvažovat o přidání nebo zlepšení propojení redundance v síti. Tento návrh používá vícenásobné nebo redundantní cesty, aby se zabránilo ztrátě kontroly dat v případě neočekávaných poruch sítě.

Aby bylo možné splnit standardy ochrany počítačové bezpečnosti, je důležité, aby každé síťové zařízení splňovalo standardy průmyslové bezpečnosti IEC 62443. Zařízení, která vyhovují těmto standardům, nabízejí důležité bezpečnostní prvky, jako jsou uživatelská kontrola, autentizace založená na heslech, správa účtů, identifikátor a ověřování, integritu a důvěrnost dat a další. To zajišťuje, že kritické aplikace zůstávají v provozu a zůstávají chráněny před neoprávněným přístupem.

3. Přenos dat. Třetí krok zahrnuje bezpečný přenos dat na cloudovou platformu. Existuje několik způsobů, jak to udělat, a klíčové je určit, který přístup je nejlepší pro podnikání.

### 3.9 Přehled a výběr vhodné BI platformy

Když už bude mít společnost ŠKODA AUTO a.s. sensorickou vrstvu, přenosové technologie a integrační vrstvu, dalším krokem by měla být aplikační vrstva, tj. Business Intelligence. V 2016 roce analytická společnost Gartner zveřejnila poskytovatelů systémů BI (viz Obr. 18). A pak se v tomto roce začalo dvě zjevné vůdce na trhu BI - Microsoft BI a Tableau.



Zdroj: aptude.com

**Obr. 18 Analýza trhu BI platform**

Lže říct, že od samého začátku Tableau byl nejvíce uživatelsky přívětivý nástroj pro vizuální průzkum, ale v současnosti to již pravděpodobně nelze tvrdit. Existuje vysoká úroveň integrace a kompatibility, kterou Tableau nebo jiný nástroj nedokáže poskytnout. Je možné snadno převést existující práci v Excelu na Power BI bez nutnosti přepracování, zatímco s jakýmkoli jiným BI nástrojem musíte začít od nuly.



Dříve byl Tableau jediný nástroj na trhu s možností vytvářet jednoduché výpočty pomocí jednoho kliknutí, ale už i Power BI má podobnou schopnost. Tabulkové diferenciační prvky, jako jsou reportovací nápovědy, již nejsou jedinečným faktorem a konec konců, Power BI je má také. Funkce vyprávění příběhu jsou v Power BI (záložkách) mnohem lepší než u Tableau. V tabulce 4 je možné vidět nákladové srovnání BI Platforem, přičemž lepší dle ceny je MS Power BI.

Na základě technologického a cenového porovnání (viz Příloha 4 a Tab. 4) těchto BI produktů lze říct, že Power BI víc vyhovuje praktickému nasazení.

**Tab. 4 Nákladové srovnání BI Platforem MS Power BI a Tableau**

	Tableau	MSFT Power BI	Difference From Tableau	Savings %
# of Content Creators	197	197	\$0	0%
# of Information Consumers	1,954	1,954	\$0	0%
User Pricing - Monthly Subscriptions	\$2,605,680	\$628,890	<del>-\$1,775,610</del>	-76%
			\$1,976,790	

Zdroj: betterbuys.com

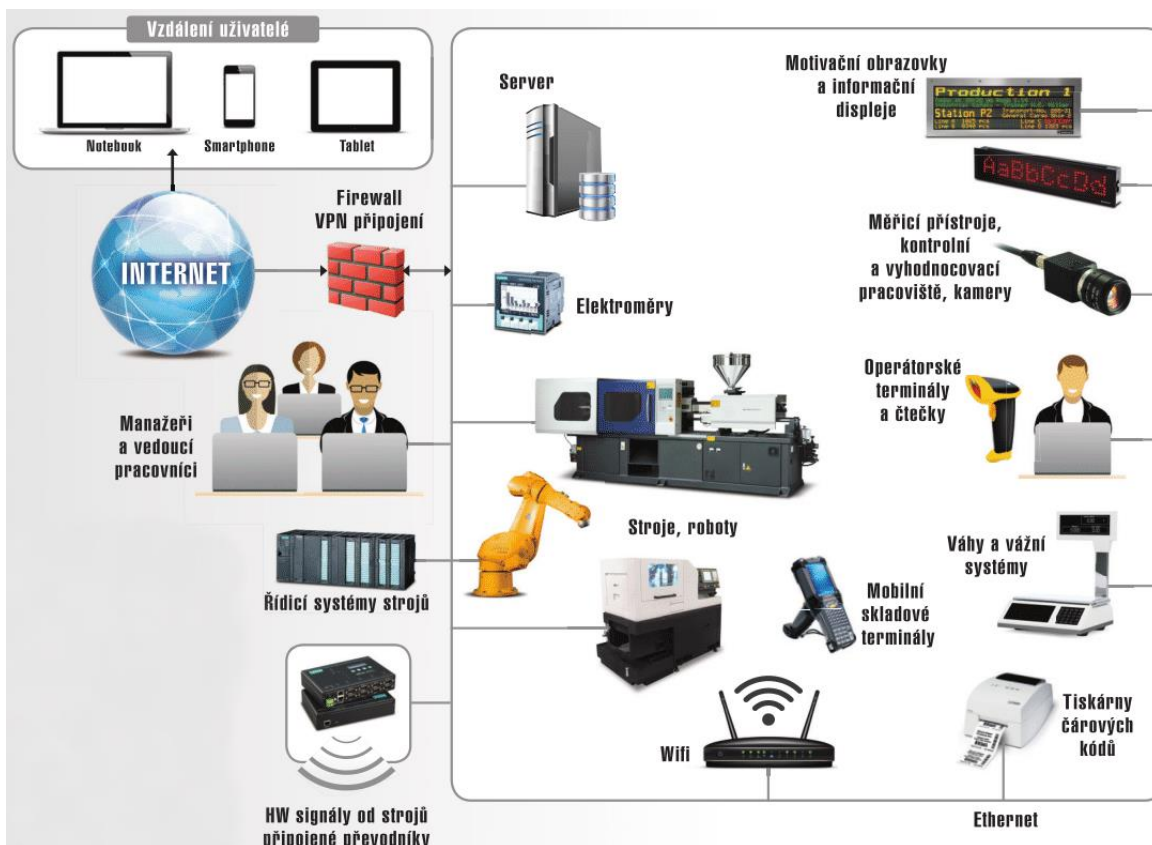
### 3.10 Zavedení monitorovacího systému MCD

Historie pochybu strojů, historie běhu výroby, analytická data pro zjištění, co se ve výrobě stalo a hlídání kvality výroby - toto další témata jsou přesně to, na co bude jednoduché řešení Monitorovací systém „MDC“ (viz Obr. 19).

Monitorovací systém MDC by se tak měl stát dalším krokem v realizaci strategie implementace IoT platforem v prostředí společnosti ŠKODA AUTO a.s.

Předpokládané přínosy zavedení MDC:

- omezení neplánovaných prostojů,
- zvýšení výkonu zařízení,
- minimalizace vadných výrobků,
- průběžné sledování realizace výrobních plánů,



Obr. 19 Monitorovací systém MDC (Machine Data Collection)

- optimalizace výrobního plánu, personálu a vybavení,
- nižší provozní náklady,
- snížení nákladů na elektřinu,
- snížení výrobních nákladů za 1 strojní hodinu,
- pomocí systému MDC se data ze zařízení převedou na správná rozhodnutí.

### Systémové funkce MDC

#### 1. Monitoring zařízení a personálu:

- určení skutečné zátěže zařízení,
- určení skutečné výrobní kapacity stroje, místa, podniku,
- snížení nákladů na jednotku výroby,
- identifikace překážek v procesním řetězci,
- hodnocení skutečných ztrát pracovní doby a výrobních zdrojů, identifikace odpovědných pracovníků,

- zlepšení pracovní kázně,
- optimalizace pracovního plánu (eliminace práce o víkendech, 2. nebo 3. směny),
- zlepšení účinnosti služeb,
- přijetí správných rozhodnutí při nákupu dalšího vybavení nebo modernizace.

## 2. Řízení výroby:

- optimalizace technologických procesů výroby výrobků,
- snížení prostojů výroby,
- snížení výroby vadných výrobků,
- tvorba korektních technologických norem,
- snížení nákladů na jednotku výroby.

## 3. Řízení prostojů:

- snížení neplánovaných prostojů,
- prodloužení životnosti zařízení,
- snížení nákladů na jednotku výroby.

## 4. Správa CNC programů:

- zvýšení využitelnosti a produktivity CNC strojů,
- zabránění poškození nástrojů a zařízení,
- zkrácení času nastavení,
- snížení nákladů na jednotku výroby.

## 5. Kontrola energetické účinnosti:

- analýza energetické účinnosti zařízení,
- snížené náklady na energii,
- plánování spotřeby elektrické energie.

## 4 Kritické zhodnocení předloženého návrhu

V současném konkurenčním prostředí musí mít tým managementu k dispozici informace v reálném čase, aby mohl přijímat rozhodnutí s výrazným dopadem na náklady a zisky firmy. IoT umožňuje managementu dodávat ty správné informace, aby měl přehled o tom, co se děje na výrobní úrovni, aby mohl přijímat rozhodnutí potřebná pro lepší řízení celkových provozních nákladů a zvyšování firemních zisků.

Propojuje zařízení a lidi, shromažďuje a sdílí velké množství dat, umožňuje a integruje inteligentnější a autonomnější stroje. IoT je skvělým nástrojem, který umožňuje výrobcům a zároveň ŠKODA AUTO a.s. zlepšit širokou řadu výrobních operací.

ŠKODA AUTO a.s. už má několik zprovozněných IoT projektů, které, spolu s libereckou firmou Foxon s.r.o., vyvíjely a realizovaly. Jde o projekty (FOXON, 2017):

- Aktivní monitoring PROFINET sítí a jeho potenciál.
- Condition monitoring největších lisů v ČR.
- Bezdrátový monitoring kvality řídicího napětí 24 voltů.
- Pasivní monitoring PROFINET sítě.
- Data z frekvenčních měničů jako ukazatele stavu pohonů.
- Permanentní diagnostika sítí PROFIBUS DP.

Na jedné straně, autor této práce chápe, že implementace navržené strategie a realizace jednotlivých stavebních kamenů této strategie formou IoT projektů, údržba a provoz jednotlivých aplikací jsou činnosti, které jsou velmi náročné jak na kvalifikaci pracovníků, tak na celkový objem lidských a finančních zdrojů. Pro mnohé hospodářské organizace se ukazuje jako finančně a personálně neúnosné nebo dokonce zcela nemožné, aby si všechny činnosti související s vývojem, provozem a údržbou IoT projektu zajišťovaly vlastními silami. Snaží se proto vyčlenit některé, nebo většinu těchto činností mimo podnik - na externí dodavatele komponent a služeb. Jinými slovy, snaží se realizovat outsourcing, aby se podnik mohl soustředit na hlavní činnost.

Na straně druhé se však autor rozhodl najít alternativní řešení a rozpracoval postupy strategie implementace IoT platforem, které by umožnily zůstat společnosti ŠKODA AUTO a.s. konkurenceschopnou a nezávislou organizací. Jednou z největších

překážek implementace nástrojů a technologií z IoT je to, že hodně výrobních firem má nedostatek kvalifikovaného personálu. Autor zároveň ví, že společnost ŠKODA AUTO a.s. má již svou laboratoř FabLab, která je zaměřena na trend Průmysl 4.0. Je jasné, že Internet věcí je součástí tohoto trendu, a v realizaci nabízené strategie by v tom neměl být žádný problém.

## Závěr

Cílem této diplomové práce bylo, na základě rešerše a analýzy aktuálních odborných zdrojů, reálných případových studií, vytvořit návrh strategie implementace vybraných IoT řešení v prostředí ŠKODA AUTO a.s.

Internet věcí začíná novou, doslova pionýrskou éru, která momentálně velký přínos negeneruje. Celkově se dá očekávat, že bude pokračovat nárůst nasazování IoT s velkým přínosem pro ty společnosti, které si dříve potenciálu IoT nevšimly. Protože dodavatelé kladou na zabezpečení důraz a budou vyvíjet další zařízení, přitáhne to pozornost společností k integraci IoT do jejich vybavení, a to začne vytvářet novou přidanou hodnotu.

Masovému rozšíření IoT brání složité technické a organizační problémy, zejména ty, které souvisejí s normalizací a standardizací. Zatím neexistují jednotné standardy pro Internet věcí, což ztěžuje integraci řešení na trhu a v mnoha ohledech brání vzniku nových.

Z rešerše vyplynulo, že na trhu existují některé vhodné nebo univerzálnější IoT platformy pro použití v IoT projektech. Autor z nich doporučuje využít platformu LoRaWAN, jejímž provozovatelem na českém trhu jsou České Radiokomunikace a.s.

Autor navrhl strategii nasazení vybraných IoT řešení ve společnosti ŠKODA AUTO a.s. jako hlavní výstup této diplomové práce. Návrh je zaměřen na dosažení zlepšení současného stavu výroby prostřednictvím realizace navržených IoT projektů, a to ve dvou oblastech. Za první při monitorování, kontrole a predikci stavů ve výrobě a za druhé při snižování výrobních nákladů společnosti ŠKODA AUTO a.s. Postupné zavedení strategie implementace IoT řešení však nutně podléhá dalšímu detailnímu zhodnocení vedoucích a IoT specialistů, převážně s ohledem na ekonomické a strategické cíle společnosti.

## Seznam literatury

BETTER BUYS STAFF. *Tableau vs Power BI: Comparing Pricing, Functionality and Support*. [cit. 2018-12-05]. Dostupné z: <https://www.betterbuys.com/bi/tableau-vs-power-bi/> [online].

CEARLEY D., BURKE B. *Top 10 Strategic Technology Trends for 2019*. [cit. 2018-12-04]. Dostupné z: <https://www.gartner.com/doc/3891569> [online].

CRA A.S. *CRA Business Cloud* [cit. 2018-12-04]. Dostupné z: <https://www.cra.cz/cra-business-cloud> [online].

TOPINFO. *Sítě pro internet věcí v České republice. 2017* [cit. 2019-01-21]. Dostupné z: <https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/16519-site-pro-internet-veci-v-ceske-republice> [online].

DOODLE LABS (SG) PTE. LTD. *Wireless Technologies*. [cit. 2018-11-05]. Dostupné z: <https://doodlelabs.com/solution-gallery/bii-technology-overview/wireless-technologies-2/> [online].

ELKO EP, s.r.o. *Porovnání IoT platform dle zařízení* [cit. 2018-11-05]. Dostupné z: <https://www.elkoep.cz/lora>. [online].

ElektroPrůmysl.cz. *FOXON INTERNET OF THINGS 2015* [cit. 2019-01-20]. Dostupné z: <http://www.elektroprumysl.cz/automatizace/fiot-cz-foxon-internet-of-things> [online].

FOXON S.R.O. *Jaké jsme realizovali projekty?: A jak jsou spokojeni naši zákazníci?* FOXON, 2018 [cit. 2019-03-05]. Dostupné z: <https://www.foxon.cz/projekty-fiot/reference> [online].

GREENGARD S. *Internet of Things*. Dhaka: The MIT Press Essential Knowledge series, 2015. ISBN 9780262527736 [cit. 2018-12-23].

HW SERVER. *All-in-one i jednoúčelové čipy na kterých postavíte IoT*. [cit. 2018-12-10]. Dostupné z: <https://vyvoj.hw.cz/all-in-one-i-jednoucelove-cipy-na-kterych-postavite-iot> [online].

HW SERVER. *Velký přehled cloudů pro IoT* [cit. 2019-05-20]. Dostupné z: <https://vyvoj.hw.cz/velky-prehled-cloudu-pro-iot.html> [online].

HW SERVER. *Výrobci chipů a vývojových kitů* [cit. 2019-05-20]. Dostupné z: <https://vyvoj.hw.cz/velky-prehled-cloudu-pro-iot.html> [online].

IDLAB, DEPARTMENT OF INFORMATION TECHNOLOGY AT GHENT UNIVERSITY. *A Survey of LoRaWAN for IoT: From Technology to Application*. [cit. 2018-11-05]. Dostupné z: <https://www.mdpi.com/1424-8220/18/11/3995/htm>. [online].

IOT PORTÁL. *Velký přehled cloudů pro IoT* [cit. 2018-12-12]. Dostupné z: <http://www.iot-portal.cz/2017/02/23/velky-prehled-cloudu-pro-iot-1-cast/> [online].

IOT PORTÁL. *All-in-one i jednocelové čipy na kterých postavíte IoT* [cit. 2018-12-05]. Dostupné z: <https://www.iot-portal.cz/2017/07/07/all-in-one-i-jednocelove-cipy-na-kterych-postavite-iot/> [online].

JANOUSH M. *Seznamte se s internetem věcí. Může vám automatizací ušetřit v podnikání peníze.* [cit. 2018-12-05]. Dostupné z: <https://www.podnikatel.cz/clanky/seznamte-se-s-internetem-veci-muze-vam-automatizaci-usetrit-v-odnikani-penize/> [online].

LEA P. *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security.* Columbia University: Packt Publishing, 2018. ISBN 1788470591 [cit. 2018-12-17].

LASSE LUETH K. *State of the IoT 2018: Number of IoT devices now at 7B Market accelerating.* [cit. 2018-12-04]. Dostupné z: <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> [online].

LOM M., PŘIBYL O., SODOMKA P., SIMPLECELL. *Sítě pro internet věcí v České republice* [cit. 2018-11-02]. Dostupné z: <https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/16519-site-pro-internet-veci-v-ceske-republice> [online].

LACKO L. *Internet věcí – klasický fenomén s novými možnostmi* . [cit. 2018-12-05]. Dostupné z: <https://www.cad.cz/hardware/78-hardware/6748-internet-veci-klasicky-fenomen-s-novemi-moznostmi.html> [online].

MICHALEC L. *Velký přehled cloudů pro IoT.* [cit. 2018-12-03]. Dostupné z: <https://www.iot-portal.cz/2017/02/23/velky-prehled-cloudu-pro-iot-1-cast/> [online].

M-TECH, S.R.O. *Rekuperace.* [cit. 2018-11-05]. Dostupné z: <https://www.mtech.cz/produkty/rekuperace/prumysl> [online].

POHANKA, P. *Internet věcí.* PP, 2015 [cit. 2018-11-20]. Dostupné z: <http://i2ot.eu/internet-of-things/> [online].

RAYCOM S.R.O. *Internet věcí – bezdrátově a s velkým dosahem: inteligentní veřejné osvětlení.* [cit. 2019-02-04]. Dostupné z: <http://www.raycom.cz/data/article/filemanager/LoRa.pdf> [online].

SLAMA D., PUHLMANN F., MORRISH J., BHATNAGAR. M. *Enterprise IoT: Strategies and Best Practices for Connected Products and Services.* Boston: O'Reilly, 2015. ISBN 9781491924839 [cit. 2018-12-23].

SUDHI S. *Building an effective IoT ecosystem for your business.* New York, NY:



Springer Science+Business Media, 2017. ISBN 9783319573908 [cit. 2018-12-17].

SALAZAR J., SANTIAGO S. *Internet věcí* [online, pdf]. Technická 2, Praha 6: České vysoké učení technické v Praze Fakulta elektrotechnická, 2017 [cit. 2019-01-03]. ISBN 978-80-01-06231-9.

ŠKODA AUTO a.s. *Interní internetové stránky společnosti ŠKODA AUTO a.s.* Dostupné z: <https://eportal.skoda.vwg>.

SCHAAL A., RUTRONIK. *Technologie NB-IoT a LTE Cat M1 jsou krok napřed.* [cit. 2018-12-03]. Dostupné z: <https://vyvoj.hw.cz/technologie-nb-iot-a-lte-cat-m1-jsou-krok-napred.html> [online].

SIGFOX. *Cloud platform providers.* [cit. 2018-12-03]. Dostupné z: <https://partners.SigFox.com/companies/cloud-platform-provider?page=0> [online].

SOS ELECTRONIC. *Vytváření bezdrátových MESH sítí s IQRF nyní ještě efektivněji* [cit. 2019-01-22]. Dostupné z: <https://www.soselectronic.cz/articles/iqrf/iqrf-vytvareni-bezdratovych-mesh-siti-s-iqrf-nyni-jeste-efektivneji-1557> [online].

STATISTA. *Internet of Things (IoT) solutions market in the European Union (EU 28) in 2025 (in billion euros)* [cit. 2018-11-05]. Dostupné z: <https://www.statista.com/> [online].

TRADEMEDIA INTERNATIONAL. *Co dokáže IIoT?* 2018 [cit. 2019-01-17]. Dostupné z: <https://www.vseoprmyslu.cz/digitalizace/prumyslovy-internet-veci/co-dokaze-iiot.html> [online].

TRADEMEDIA INTERNATIONAL. *Realizace Průmyslu 4.0 a IoT v chytrých závodech* [cit. 2019-03-04]. Dostupné z: <http://www.controlengcesko.com/hlavni-menu/artikuly/artikul/article/realizace-prumyslu-40-a-iot-v-chytrych-zavodech/> [online].

THE STATISTICS PORTAL. *Internet of Things (IoT) solutions market in the European Union (EU 28) in 2025 (in billion euros).* [cit. 2019-01-03]. Dostupné z: <https://www.statista.com/statistics/686198/iot-solutions-market-in-the-european-union-eu/> [online].

WOODIE A. *Gartner Sees AI Democratized in Latest Hype Cycle* [cit. 2018-12-04]. Dostupné z: <https://www.datanami.com/2018/08/27/gartner-sees-ai-democratized-in-latest-hype-cycle/> [online].

TOPINFO. *Sítě pro internet věcí v České republice 2017* [cit. 2019-02-14]. Dostupné z: [http://cc.bingj.com/cache.aspx?q=typy+zprav+informacni+types+information&d=4972684856263313&mkt=en-US&setlang=en-US&w=4lwDUYjwIITVUJVw euW2G\\_BMGp7ViVI6](http://cc.bingj.com/cache.aspx?q=typy+zprav+informacni+types+information&d=4972684856263313&mkt=en-US&setlang=en-US&w=4lwDUYjwIITVUJVw euW2G_BMGp7ViVI6) [online].

## Seznam obrázků a tabulek

### Seznam obrázků

Obr. 1 Hype cyklus pro vznikající technologie .....	11
Obr. 2 Druhy sítí – bezdrátově a s velkým dosahem .....	12
Obr. 3 Dotazník: dochází ve vaší výrobě k reálnému využití konceptu IoT? .....	13
Obr. 4 Trh IoT řešení v Evropské unii (EU 28) v roce 2025 (v miliardách eur) .....	14
Obr. 5 Dotazník: Co firmy od IoT očekávají? .....	15
Obr. 6 Předpokládaný ekonomický dopad internetu věcí v roce 2025 (v miliardách eur) .....	18
Obr. 7 Typická architektura internetu věcí .....	20
Obr. 8 Laboratoř ŠKODA FabLab .....	27
Obr. 9 Postup strategie implementace IoT platforem .....	30
Obr. 10 LoRaWAN topologie sítě .....	35
Obr. 11 Interní stránky CRA Business Cloudu .....	43
Obr. 12 INTELILIGHT – inteligentní osvětlení .....	47
Obr. 13 Stlačený vzduch - monitorování ztrát .....	48
Obr. 14 Životní cyklus mazacího oleje strojního zařízení.....	49
Obr. 15 AirPi Kit .....	50
Obr. 16 IoT platforma typu XNB .....	51
Obr. 17 Převaha IoT platformy typu XNB .....	53
Obr. 18 Analýza trhu BI platforem .....	55
Obr. 19 Monitorovací systém "MDC,, (Machine Data Collection) .....	57

## Seznam tabulek

Tab. 1 Stimuly a bariéry Internetu věcí.....	15
Tab. 2 IoT platformy podle technologie.....	36
Tab. 3 Porovnávání SigFox, LoRaWAN, IQRF.....	37
Tab. 4 Nákladové srovnání BI Platforem MS Power BI a Tableau.....	56

## **Seznam příloh**

Příloha č. 1 Srovnání Low-Power WAN alternativ .....	68
Příloha č. 2 Objednávka pro pilotní provoz .....	69
Příloha č. 3 Porovnání IoT platforem dle zařízení .....	70
Příloha č. 4 Plusy a mínusy BI platforem .....	71

# Příloha č. 1 Srovnání Low-Power WAN alternativ

Name of Standard	Weightless-W	Weightless-N	Weightless-P	SigFox	LoRaWAN	LTE-Cat M1 (formerly LTE-Cat M)	LTE-Cat M2 (formerly NB-IoT)	IEEE P802.11ah (low power WiFi)	Dash7 Alliance Protocol 1.0	Ingeniu RPMA	nWave
Frequency Band	TV whitespace (400-800 MHz)	Sub-GHz ISM	Sub-GHz ISM	868 MHz/902 MHz ISM	433/868/780/915 MHz ISM	Cellular	Cellular	License-exempt bands below 1 GHz, excluding the TV White Spaces	433, 868, 915 MHz ISM/SRD	2.4 GHz ISM	Sub-GHz ISM
Channel Width	5MHz	Ultra narrow band (200Hz)	12.5 kHz	Ultra narrow band	EU: 8x125kHz, US 64x125kHz/8x125kHz, Modulation: Chirp Spread Spectrum	1.4MHz	200 kHz	17/14/8/16 MHz	25 KHz or 200 KHz	1 MHz (40 channels available)	Ultra narrow band
Range	5km (urban)	3km (urban)	2km (urban)	30-50km (rural), 3-10km (urban), 1000km LoS	2-5k (urban), 15k (rural)	2.5- 5km	2.5- 5km	Up to 1km (outdoor)	0 – 5 km	>500 km LoS	10km (urban), 20-30km (rural)
End Node Transmit Power	17 dBm	17 dBm	17 dBm	-10 dBm to 20 dBm	EU: <+14dBm, US: <+27dBm	20 dBm	20 dBm	Dependent on Regional Regulations (from 0 dBm to 30 dBm)	Depending on FCC/ETSI regulations	to 20 dBm	14 dBm to 20 dBm
Packet Size	10 byte min.	Up to 20 bytes	10 byte min.	12 bytes	Defined by User	100 - 1000 bytes typical	100 - 1000 bytes typical	Up to 791 Bytes (w/o Aggregation), up to 65,535 Bytes (with Aggregation)	256 bytes max / packet	Flexible (6 bytes to 10 kbytes)	12 byte header, 220 byte payload
Uplink Data Rate	1 kbps to 10 Mbps	100bps	200 bps to 100 kbps	100 bps to 140 messages/day	EU: 300 bps to 50 kbps, US: 900-1000kbps	~375 kbps	~55	150 Kbps ~ 346.666 Mbps	9.6 kb/s, 55.55 kbps or 166.667 kb/s	AP aggregates to 624 kbps per Sector (Assumes 8 channel Access Point)	100 bps
Downlink Data Rate	1 kbps to 10 Mbps	No downlink	200 bps to 100 kbps	Max 4 messages of 8 bytes/day	EU: 300 bps to 50 kbps, US: 900-1000kbps	~300 kbps	~40 kbps	150 Kbps ~ 346.666 Mbps	9.6 kb/s, 55.55 kbps or 166.667 kb/s	AP aggregates to 156 kbps per Sector (Assumes 8 channel Access Point)	--
Devices per Access Point	Unlimited	Unlimited	Unlimited	1k	1k	20k+	20k+	8191	NA (connectionless communication)	Up to 384,000 per sector	1M
Topology	Star	Star	Star	Star	Star on Star	Star	Star	Star, Tree	Node-to-node, Star, Tree	Typically Star, Tree supported with an RPMA extender	Star
End node roaming allowed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Allowed by other IEEE 802.11 amendments (e.g., IEEE 802.11r)	Yes	Yes	Yes
Governing Body	Weightless SIG	Weightless SIG	Weightless SIG	Sigfox	LoRa Alliance	3GPP	3GPP	IEEE 802.11 working group	Dash7 Alliance	Ingeniu (formerly OnRamp)	Weightless SIG
Status	Limited deployment awaiting spectrum availability	Deployment beginning	Standard in development. Scheduled release 4Q 2015	In deployment	Spec released June 2015, in deployment	Release 13 expected 2016	Release 13 expected 2016	Targeting 2016 release	Released May 2015	In Deployment	In Deployment

## Příloha č. 2 Objednávka pro pilotní provoz

NABÍDKA číslo ND-1805008 (2/2)



Dodavatel: **ALTERNETIVO s.r.o.**  
 Žitovnická 2389  
 10600 Praha 10  
 IČ: 25098314  
 Sídlo: Alternetivo s.r.o., Žitovnická 2389/1, Praha - Záběhlice, 10600  
 Tel.: +420 221 771 881  
 Banka: ČSOB Praha 1  
 Účet: 482837603/0300  
 DIČ: CZ25098314  
 Fax: +420 221 771 882  
 E-mail: info@alternetivo.cz

Kód	Název produktu	Počet	Cena/jed.	Měna	DPH %	Základ	DPH	Celkem
WX500-CU	WireXpert 500 Certifikační tester CAT6A, měřicí rozsah 500 MHz	1	161 110,50	Kč	21	161 110,50	33 833,21	194 943,71
GWLoRaWAN	Blumatic GW LoRa WAN	1	28 376,50	Kč	21	28 376,50	5 959,07	34 335,57
MAX21030	LoRa - MiniUNI velmi přesný teploměr SI7051	1	2 109,00	Kč	21	2 109,00	442,89	2 551,89
MAX01001	Abeeway - GPS tracker, Master Tracker	1	6 900,80	Kč	21	6 900,80	1 449,17	8 349,97
MAX06001	CLICKEY Micro T&T - triangulační tracker	1	3 450,40	Kč	21	3 450,40	724,58	4 174,98
MAX21038	SF - mini UNI 50 čítač impulsů s optočlenem 2bat	1	1 892,40	Kč	21	1 892,40	397,40	2 289,80
MAX21035	SF - mini UNI teploměr DS18B20	1	1 824,00	Kč	21	1 824,00	383,04	2 207,04
MAX21043	SF - MINI UNI - TH + Atm tlak	1	2 223,00	Kč	21	2 223,00	466,83	2 689,83
MAX21046	SF - Odečítací jednotka WSD + 2bat	1	2 793,00	Kč	21	2 793,00	586,53	3 379,53
MAX21024	LoRa - SIGFOX GPS tracker s akcelerometrem IP65 (*)	1	2 793,00	Kč	21	2 793,00	586,53	3 379,53
MAX02001	Ascoel - PIR čidlo - detekce pohybu	1	2 070,05	Kč	21	2 070,05	434,71	2 504,76
MAX02002	Ascoel - Magnetické čidlo - detekce otevření	1	2 380,70	Kč	21	2 380,70	499,95	2 880,65
MAX02003	Ascoel - Senzor kvality ovzduší - CO2, Teplota a vlhkost	1	10 098,50	Kč	21	10 098,50	2 120,69	12 219,19
MAX02004	Ascoel - Průmyslové tlačítko	1	3 553,95	Kč	21	3 553,95	746,33	4 300,28
LPN LIGHTING BRIDGE	Kontrolér osvětlení	1	3 519,75	Kč	21	3 519,75	739,15	4 258,90
LT-100E	LT-100E LoRaWAN GPS Tracker	1	2 222,05	Kč	21	2 222,05	466,63	2 688,68
LT-501E	LT-501E LoRaWAN GPS Tracker	1	2 518,45	Kč	21	2 518,45	528,87	3 047,32
MAX16002	Gemtek Smart Parking Sensor	1	2 344,60	Kč	21	2 344,60	492,37	2 836,97
MAX21010	LoRa Tester	1	4 104,00	Kč	21	4 104,00	861,84	4 965,84

## Příloha č. 3 Porovnání IoT platforem dle zařízení

			
 <b>AirIM-100</b> Univerzální modul	✓ AirIM-100S	✓ AirIM-100L	✓ AirIM-100NB
 <b>AirIM-100/M</b> Univerzální modul	✓ AirIM-100S/M	✓ AirIM-100L/M	✓ AirIM-100NB/M
 <b>AirSF-100</b> Záplavový detektor	✓ AirSF-100S	✓ AirSF-100L	✓ AirSF-100NB
 <b>AirWD-100</b> Magnetický detektor	✓ AirWD-100S	✓ AirWD-100L	✓ AirWD-100NB
 <b>AirMD-100</b> Pohybový detektor	✓ AirMD-100S	✓ AirMD-100L	✓ AirMD-100NB
 <b>AirSD-100</b> Detektor kouře	✓ AirSD-100S	✓ AirSD-100L	✓ AirSD-100NB
 <b>AirQS-100</b> Senzor kvality vzduchu (CO <sub>2</sub> )	✓ AirQS-100S	✓ AirQS-100L	✓ AirQS-100NB
 <b>AirQS-101</b> Senzor kvality vzduchu (CO)	✓ AirQS-101S	✓ AirQS-101L	✓ AirQS-101NB
 <b>AirTM-100</b> Převodník pulzů	✓ AirTM-100S	✓ AirTM-100L	✓ AirTM-100NB
 <b>AirDAC-100</b> Ovládací prvek	-	✓ AirDAC-100L	✓ AirDAC-100NB
 <b>AirSLC-100</b> Obousměrný komunikační modul	-	✓ AirSLC-100L	✓ AirSLC-100NB
 <b>AirPS-100</b> Parkovací senzor	✓ AirPS-100S	✓ AirPS-100L	✓ AirPS-100NB
 <b>AirSOU-100</b> Senzor stmívání osvětlení	✓ AirSOU-100S	✓ AirSOU-100L	-

## Příloha č. 4 Plusy a mínusy BI platformem

### *Plusy a mínusy BI Tableau*

Plusy	Mínusy
snadná implementace	cena
vynikající podpora mobilních zařízení	SQL znalost je nutná pro vytvoření datasetů
výborná vizualizace dat	v okamžiku, kdy panely dashboardu a zprávy jsou publikovány na serveru, není možné jít zpět a obnovit stará data
jednoduché řešení pro integraci s většinou populárních datových zdrojů a analytických jazyků	
bohaté on-line zdroje a společenství	
bohatý na funkce, snadné nasazení a upgrade	

### *Plusy a mínusy MS Power BI*

Plusy	Mínusy
nulové investiční náklady	publikování je k dispozici pouze do cloudu a od června 2017 na jeho vlastní server Power BI
jednoduchá tvorba vizuálně kvalitních reportů	aplikace je nutno instalovat každého půl roku, jinak přestane fungovat
mnoho datových konektorů	není možné přímo publikovat na serveru SharePoint a SharePoint Online / Office 365
úprava dat před reportováním	nemožnost připojení datového modelu do souboru aplikace Excel
sdílení reportů v organizaci	produkt je zadarmo, a to znamená, že nejsou žádné SLA s dodavatelem
Power BI komunita si pomáhá	
vhodné pro pilotní projekty	



## ANOTAČNÍ ZÁZNAM

<b>AUTOR</b>	Bc. Sergii Svystula		
<b>STUDIJNÍ OBOR</b>	6208T088 Podniková ekonomika a management provozu		
<b>NÁZEV PRÁCE</b>	Internet věcí ve společnosti ŠKODA AUTO a.s.		
<b>VEDOUCÍ PRÁCE</b>	prof. Ing. Radim Lenort, Ph.D.		
<b>KATEDRA</b>	KLAT - Katedra logistiky, kvality a automobilové techniky	<b>ROK ODEVZDÁNÍ</b>	2019
<b>POČET STRAN</b>	67		
<b>POČET OBRÁZKŮ</b>	19		
<b>POČET TABULEK</b>	4		
<b>POČET PŘÍLOH</b>	4		
<b>STRUČNÝ POPIS</b>	<p>Cílem diplomové práce je, na základě rešerše a analýzy aktuálních odborných zdrojů, reálných případových studií, vytvořit návrh strategie implementace vybraných IoT platforem v prostředí ŠKODA AUTO a.s. Práce je rozdělena na tři části, část teoretickou, praktickou a kritické zhodnocení předloženého návrhu. Teoretická část se zabývá nejnovějšími poznatky z oblasti IoT v průmyslovém podniku, přehledem současných IoT platforem fungujících jak v zahraničí, tak v České republice, dostupných cloudů a zařízení pro sběr dat, vhodných BI platform. Praktická část popisuje technické porovnání použitých IoT platforem, a jednotlivé fáze strategie implementace IoT platforem a technologií v prostředí společnosti ŠKODA AUTO a.s. Závěrečná část kriticky zhodnocuje předložený návrh.</p>		
<b>KLÍČOVÁ SLOVA</b>	IoT, zařízení, IIoT, Business Intelligence, aplikace, sensor, cloud, výpočetní infrastruktura, komunikační síť, komunikační rozhraní, LPWAN, SLA, SigFox, LoRaWAN		

## ANNOTATION

<b>AUTHOR</b>	Bc. Sergii Svystula		
<b>FIELD</b>	6208T088 Production Management and Global Business		
<b>THESIS TITLE</b>	Internet of Things in ŠKODA AUTO a.s.		
<b>SUPERVISOR</b>	prof. Ing. Radim Lenort, Ph.D.		
<b>DEPARTMENT</b>	KLAT Department of Logistics, Quality and Automotive Technology	<b>YEAR</b>	2019
<b>NUMBER OF PAGES</b>	67		
<b>NUMBER OF PICTURES</b>	19		
<b>NUMBER OF TABLES</b>	4		
<b>NUMBER OF APPENDICES</b>	4		
<b>SUMMARY</b>	<p>The aim of this thesis is to create a strategy of implementation of selected IoT platforms in ŠKODA AUTO a.s. The thesis is divided into three parts, the theoretical, practical and critical evaluation of the submitted proposal. The theoretical part deals with the latest knowledge in the field of IoT in an industrial enterprise, an overview of current IoT platforms operating both abroad and in the Czech Republic, available clouds and data collection devices, suitable BI platforms. The practical part describes the technical comparison of used IoT platforms, and the individual phases of the implementation strategy of IoT platforms and technologies in the ŠKODA AUTO a.s. The final part critically evaluates the submitted proposal.</p>		
<b>KEY WORDS</b>	IoT, devices, IIoT, Business Intelligence, application, sensor, cloud, computing infrastructure, communication network, communication interface, LPWAN, SLA, SigFox, LoRaWAN		