

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

**VYUŽITÍ MOŽNOSTÍ IOT PRO REINŽENÝRING
PODNIKOVÝCH PROCESŮ**
UTILIZING THE INTERNET OF THINGS FOR BUSINESS PROCESS
REENGINEERING

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

VILÉM HUJŇÁK

VEDOUCÍ PRÁCE
SUPERVISOR

Doc. Ing. ONDŘEJ RYŠAVÝ, Ph.D.

BRNO 2017

Zadání bakalářské práce

Řešitel: **Hujňák Vilém**

Obor: Informační technologie

Téma: **Využití možností IoT pro reinženýring podnikových procesů**

Utilizing the Internet of Things for Business Processes Reengineering

Kategorie: Softwarové inženýrství

Pokyny:

1. Seznamte se s problematikou Business Process Reengineering a možnostmi prostředí IoT.
2. Prostudujte existující přístupy při návrhu procesů v prostředí IoT.
3. Definujte metodu návrhu a implementace IoT řešení procesním způsobem.
4. Vyberte vhodný systém, který bude sloužit jako případová studie. Vytvořte či doplňte nezbytnou dokumentaci tohoto systému.
5. Za pomoci vybrané IoT technologie vytvořte systém s použitím navržené metody.
6. Vyhodnoťte zkušenosti a výsledky získané z provedené studie a diskutujte další rozvoj metody.

Literatura:

- Ned Kock: Systems Analysis & Design Fundamentals: A Business Process Redesign Approach, Sage Publications Pvt. Ltd. 2006.
- M. Ferretti, F. Schiavone, Internet of Things and business processes redesign in seaports: The case of Hamburg, Bus. Process Manag. J. 22 (2016) 271-284. doi:10.1108/BPMJ-05-2015-0079.

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 až 3.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese

<http://www.fit.vutbr.cz/info/szz/>

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).


Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT**

Datum zadání: 1. listopadu 2016

Datum odevzdání: 17. května 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2


doc. Dr. Ing. Dušan Kolář
vedoucí ústavu

Abstrakt

Bakalářská práce se zabývá problematikou reinženýringu podnikových procesů s využitím možností Internetu věcí. V práci je navržena metoda implementace IoT procesním způsobem a ověřena na případové studii procesu zajištění pohybu oprávněných osob ve firemních prostorách s využitím vícefaktorové autentizace.

Abstract

The bachelor's thesis deals with the issue of Business Process Reengineering using possibilities of the Internet of Things. The thesis describes a method for implementing IoT solutions in a procedural manner and has been validated in a case study process – ensuring a movement of authorized persons in a company premises using multi-factor authentication.

Klíčová slova

Internet věcí, reinženýring podnikových procesů

Keywords

Internet of Things, Business Process Reengineering

Citace

HUJŇÁK, Vilém. Využití možností IoT pro reinženýring podnikových procesů. Brno, 2016. 55 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ondřej Ryšavý.

Využití možností IoT pro reinženýring podnikových procesů

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Doc. Ing. Ondřeje Ryšavého, Ph.D. Další informace a prostředky mi poskytla společnost Per Partes Consulting, s.r.o., ve které jsem zaměstnán na pozici vývojáře IoT. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Vilém Hujňák
15. května 2017

Poděkování

Děkuji vedoucímu práce Doc. Ing. Ondřeji Ryšavému, Ph.D. za konstruktivní připomínky a podněty k řešení problematice a také společnosti Per Partes Consulting, s.r.o. za poskytnutí IoT zařízení potřebných pro provedení případové studie.

© Vilém Hujňák, 2017

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

Obsah.....	4
Úvod.....	6
1. Cíle práce.....	7
1.1 Hlavní cíl práce.....	7
1.2 Postupové cíle práce.....	7
2. Reinženýring procesů a nové možnosti prostředí IoT.....	8
2.1 Definice pojmu BPR.....	8
2.2 Současné metodické přístupy k provádění BPR.....	9
2.3 Definice pojmu IoT.....	10
2.4 Nové možnosti IoT z hlediska podnikových procesů.....	14
3. Existující přístupy při návrhu procesů v prostředí IoT.....	16
3.1 IoT Analytics.....	16
3.2 Rozšíření BPMN.....	18
3.3 Přístup společnosti Oracle.....	18
3.4 Přístup společnosti IBM.....	19
3.5 Přístup společnosti Mindtree.....	20
3.6 Shrnutí k existujícím přístupům.....	21
4. Návrh metody pro zavedení IoT řešení procesním způsobem.....	22
4.1 Principiální základy navržené metody.....	22
4.1.1 Použité techniky.....	22
4.2 Implementační etapy metody.....	24
4.2.1 Etapa 1: Analýza stávajícího stavu.....	25
4.2.2 Etapa 2: Analýza příležitostí IoT k reinženýringu procesu.....	26
4.2.3 Etapa 3: Návrh reinženýringu procesu s umožněním IoT aktiv.....	27
4.2.4 Etapa 4: Nastavení řídicích pravidel a konfigurace IoT Manažera.....	29
4.3 Role IoT Manažera při provádění procesu.....	29
5. Volba případové studie pro ověření metody v praxi.....	30
5.1 Zvolená případová studie.....	30
5.2 Zvolené IoT technologie.....	31
5.2.1 Zařízení.....	31
5.2.2 Komunikační protokoly.....	31
6. Aplikace navržené metody na reinženýring procesu z případové studie.....	32
6.1 Etapa 1: Analýza stávajícího stavu.....	32
6.2 Etapa 2: Analýza příležitostí IoT k reinženýringu procesu.....	33
6.3 Etapa 3: Návrh reinženýringu procesu s umožněním IoT aktiv.....	35
6.4 Etapa 4: Konfigurace IoT Manažera a nastavení řídicích pravidel.....	39
6.5 Návrh řešení IoT Manažera.....	39
6.5.1 Implementace.....	41
7. Vyhodnocení zkušeností z aplikace metody na případové studii.....	42

7.1 Zkušenosti z aplikace navržené metody pro reinženýring procesů.....	42
7.2 Zkušenosti z fungování IoT technologií.....	42
7.2.1 Chytré auto.....	43
7.2.2 Multisenzor Sens'it.....	44
7.2.3 Z-Wave brána.....	45
7.3 Zkušenosti z řízení procesu IoT Manažerem.....	45
8. Závěr.....	48
8.1 Splnění cílů práce.....	48
8.2 Doporučení dalšího rozvoje.....	49
Literatura.....	50
Přílohy.....	51
Seznam příloh.....	52
A Tabulkové vyjádření procesu.....	53
B Obsah příloženého paměťového média.....	54
C Seznam obrázků.....	55

Úvod

V současné informační éře je kladen stále větší důraz na propojení počítačových systémů větších celků. Vznikla síť sítí internet a téměř veškerá výpočetní a komunikační zařízení jsou jí vzájemně propojena. Trend se stále rozšiřuje a na internet se připojuje čím dál více zařízení veškerého druhu, kterým se říká „věci“. Propojení fyzických či virtuálních objektů vytváří „Internet věcí“ (Internet of Things, IoT). Propojení není limitované pouze pomocí internetu, ale může se jednat o jakoukoli jinou vytvořenou síť. Některé pohledy pracují s pojmem „Internet of Everything[1]“, který kromě věcí spojuje i lidi, procesy a data. Snahou je proměna informací na konání, které vytváří nové schopnosti, bohatší zkušenosti a nebývalé ekonomické příležitosti pro podniky, jednotlivce a státy. Podle Gartnerovy křivky¹ životních cyklů technologií, se nyní IoT nachází na pomezí *vrcholu přehnaných očekávání* a *údolí deziluze* a během pěti až deseti lety by se mohlo dostat na *plošinu produktivity*.

Druhou oblastí, kterou se tato práce zabývá, je reinženýring podnikových procesů (Business Process Reengineering, BPR). Ten poukazuje na analýzu, návrh a přepracování procesů uvnitř organizací nebo při kooperaci mezi organizacemi a právě IoT se jeví jako nová hybná síla, která dokáže zajistit zvýšení produktivity, snížení nákladů a v důsledku i generování vyšších zisků.

Ve spojení výše zmíněných dvou oblastí, tj. Internetu věcí a reinženýringu podnikových procesů, vidím příležitost, jak důsledným využíváním možností nastupujících technologií dosáhnout vyšší výkonnosti a konkurenceschopnosti podnikových procesů. Práce se proto zaměřuje na návrh metody implementace IoT procesním způsobem, tedy je v ní navržen ucelený a obecný postup jak přistupovat k reinženýringu procesů s využitím možností IoT. Dále je v práci popsána aplikace metody implementace IoT na konkrétní případové studii procesu zajišťujícího pohyb oprávněných osob ve firemních prostorách s využitím vícefaktorové autentizace probíhající v pozadí procesu. Stav pohybu osob je monitorován IoT zařízeními a na pozadí procesu běží řídicí software vyhodnocující jejich oprávnění při vstupu do a výstupu z kanceláří daného objektu. Významnou částí práce je návrh a vytvoření tohoto softwaru, který je v práci nazýván IoT Manažer. V práci popisovaná IoT zařízení byla poskytnuta a testována při reinženýringu procesu pohybu oprávněných osob ve společnosti Per Parties Consulting, s.r.o., kde od roku 2014 pracuji na pozici vývojáře a od 6/2016 se specializuji na možnosti využití IoT technologií.

V závěru práce jsou rozebrány zkušenosti z aplikace navržené metody implementace IoT procesním způsobem, výsledky testování využitelnosti IoT zařízení v praxi, zkušenosti z řízení procesu IoT Manažerem a náměty pro další rozvoj řešené oblasti.

1 <http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp>

1. Cíle práce

Cíle práce jsou rozděleny na hlavní cíl a dílčí postupové cíle, kterými bude dosaženo cíle hlavního. Dílčí cíle na sebe těsně navazují a využívají předchozích výsledků. Závěrečná kapitola (8. *Závěr*) hodnotí splnění dílčích cílů a dosažení hlavního cíle.

1.1 Hlavní cíl práce

Hlavním cílem práce je navrhnout metodu implementace IoT řešení procesním způsobem a její ověření na případové studii. Pro dosažení hlavního cíle práce je třeba splnit všechny níže uvedené postupové cíle práce a výsledky případové studie prokázat využitelnost navržené metody.

1.2 Postupové cíle práce

Pro dosažení hlavního cíle byly vytvořeny následující postupové cíle odpovídající zadání bakalářské práce:

1. Seznámit se s problematikou BPR a možnostmi prostředí IoT.
2. Prostudovat existující přístupy při návrhu procesů v prostředí IoT.
3. Definovat metodu návrhu a implementace IoT řešení procesním způsobem.
4. Vybrat vhodnou případovou studii pro ověření navržené metody zavedení IoT procesním způsobem, tj. zvolit vhodný proces a vhodné IoT technologie pro jeho reinženýring. Vytvořit či doplnit nezbytnou dokumentaci výchozího stavu procesu a zvolených IoT technologií.
5. Aplikovat navrženou metodu na reinženýring procesu podporovaného zvolenými IoT technologiemi.
6. Vyhodnotit zkušenosti a výsledky získané z provedené případové studie a diskutovat další rozvoj navržené metody.

2. Reinženýring procesů a nové možnosti prostředí IoT

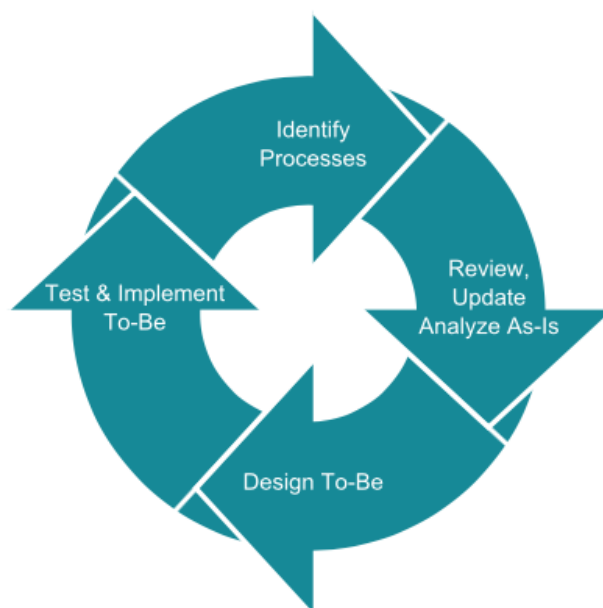
„Business process reengineering“ česky „reinženýring podnikových procesů“ a „Internet of Things“ česky „Internet věcí“ jsou dvě oblasti rozvoje, které mají velký potenciál do budoucna a jejich spojení by mohlo přinést revoluční výsledky v oblastech fungování podniků. V následujících podkapitolách jsou tyto dvě oblasti rozepsány.

2.1 Definice pojmu BPR

BPR, jak je uvedeno v [6], znamená zásadní přehodnocení a radikální rekonstrukci (redesign) podnikových procesů tak, aby mohlo být dosaženo dramatického zdokonalení z hlediska kritických měřítek výkonnosti, jako jsou náklady, kvalita služby a rychlost. Jedná se tedy o zavádění radikálních změn v podniku (procesech) za účelem jejich dramatického zdokonalení.

Zde je důležité uvést, co to podnikový proces [4] je. Definuje se jako množina logicky souvisejících činností, které se provádí za účelem získání definovaných výstupů. Jiná definice [7] říká, že jde o logické uspořádání lidí, materiálů, energie, nástrojů a procedur, které jsou navrženy jako pracovní aktivity tak, aby produkovaly specifický výsledek (produkt). Obě definice se ve své podstatě shodují.

Procesní myšlení [4] se rozšířilo v posledních desetiletích a to hlavně kvůli zvyšování kvality operací v podniku. Vyznačuje se identifikací procesů napříč celou hierarchií společnosti a nikoli zaměřením pouze na jednotlivé konkrétní úkoly nebo funkce.



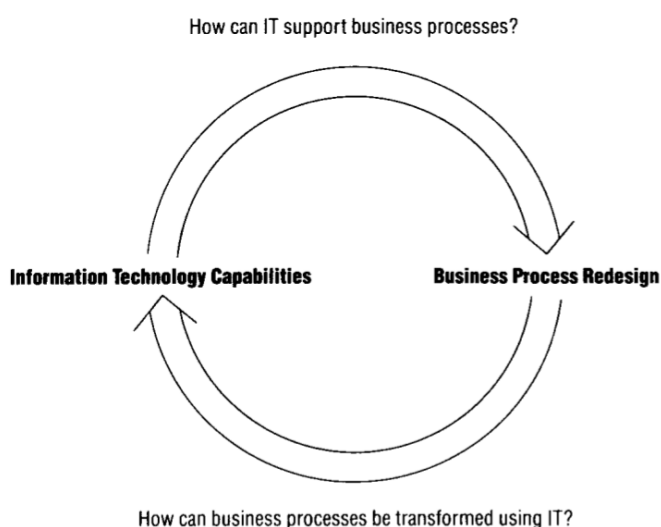
Obrázek 1: Cyklus BPR ²

2.2 Současné metodické přístupy k provádění BPR

Vzniklo mnoho metodických přístupů, jak k reinženýringu přistupovat. Základ má ale většina společný. Jedná se o následující čtyři kroky², které jsou také zobrazeny na obrázku 1:

1. identifikace procesu;
2. analýza stávajícího stavu (as-is);
3. návrh nového stavu (to-be);
4. přechod ze stávajícího do nového stavu.

Reinženýring procesů je z velké části spjatý s informačními technologiemi. Mezi těmito dvěma pojmy existuje rekurzivní vztah [4], který je zobrazen na obrázku 2. Nové informační technologie jsou často podnětem pro přeměnu procesů. A naopak při přeměně procesu, bychom měli vycházet z možností dostupných informačních technologií.



Obrázek 2: Rekurzivní vztah mezi informačními technologiemi a BPR [4]

Jedna z metodik BPR, kterou formuloval Hammer and Champy [8] se vyznačuje použitím přístupu „čistého talíře“ (clean-slate approach), kdy je analýza současného stavu z velké části zanedbána. Další metodika, kterou formuloval T. Davenport [4], zdůrazňuje, že současné zkušenosti a důkladná analýza existujících procesů jsou nutné pro úspěšný reinženýring. Tato metodika má následujících pět kroků:

1. *Rozvoj podnikové vize a procesních cílů* – má-li být společnost dlouhodobě úspěšná, navržení nových procesů musí odpovídat podnikové vizi vrcholového managementu. Procesní cíle jsou nejčastěji: snižování nákladů, úspora času, zkvalitnění výstupů nebo zvýšení kvality pracovního prostředí.
2. *Identifikace procesu, který je potřeba znovu navrhnout* – i když by bylo většinou

² https://en.wikipedia.org/wiki/Business_process_reengineering

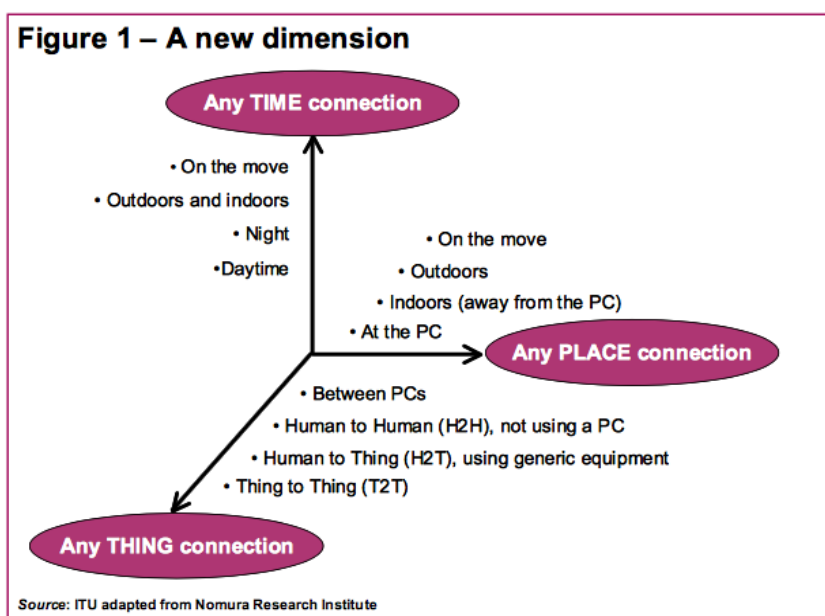
nejlepší znovu navrhnout veškeré procesy s ohledem na nejnovější IT technologie, není to vždy možné a společnosti musí pro začátek vybrat jen některé klíčové procesy.

3. *Pochopení a měření existujícího procesu* – tento krok je důležitý proto, aby se zabránilo opakování minulých problémů a aby bylo možné vyčíslit dosažené zlepšení (např. čas, náklady).
4. *Identifikace nových možností IT* – informační technologie jsou mocným nástrojem, které samy o sobě dokáží vytvořit nové možnosti pro reinženýring procesů.
5. *Vývoj nového procesu* – při vývoj nového procesu by se měl v první řadě vytvořit prototyp, na kterém se nový proces vyzkouší a navrhnou se případná vylepšení. Další výhodou prototypu je možnost seznámení s novým procesem ostatními lidmi ještě před ostrým nasazením.

Studie [4] T. Davenporta dále identifikovala některé problémy, které nastanou v průběhu přeměny procesu. Převážně se jedná o problémy spojené s managementem. Prvním je role managementu během výše zmíněných pěti kroků. Jelikož se proces obvykle týká více částí společnosti, je nutné, aby se přeměny účastnili všichni vedoucí, kterých se proces týká. Druhým praktickým problémem je možná změna organizační struktury, která nový proces podpoří. Dalším problémem může být nutnost naučení se novým dovednostem, které jsou spojené s nasazením a prováděním nového procesu.

2.3 Definice pojmu IoT

Pojem „Internet of Things“ (IoT) poprvé použil roku 1999 Kevin Ashton³, který chtěl svou prezentací přitáhnout pozornost vyššího managementu k nové technologii RFID. Nyní je IoT vnímáno z mnoha úhlů pohledu a neexistuje jednotná a ucelená definice. Ve své podstatě jde o propojení fyzických objektů („věcí“) a umožnění komunikace mezi nimi. Oblast použití není

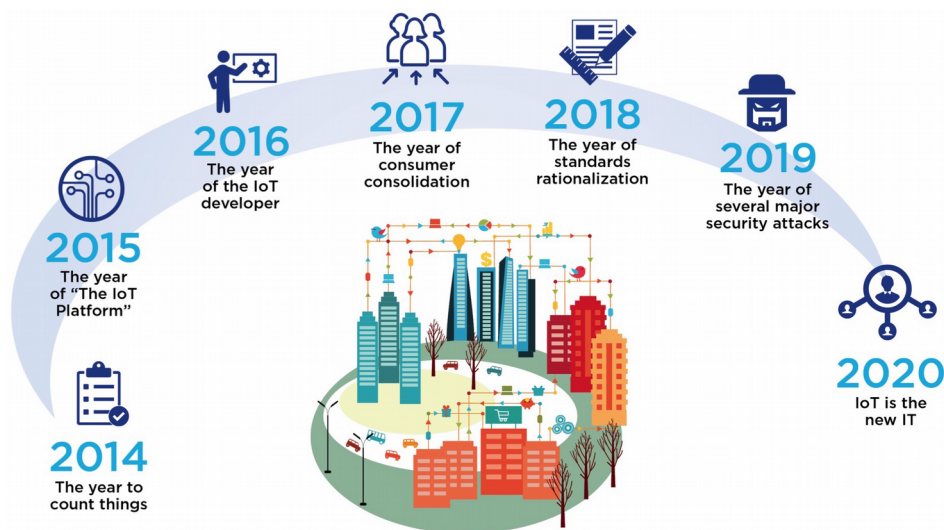


Obrázek 3: Nová dimenze „věc“ [2]

³ <http://www.rfidjournal.com/articles/view?4986>

nijak limitována a jako „věc“ můžou figurovat jakékoli zařízení či předměty z reálného světa. IoT tedy přináší novou dimenzi [2] do světa informačních a komunikačních technologií a to připojení nejen kdykoli a odkudkoli, ale také čehokoli. Obrázek 3 tuto myšlenku ilustruje.

Nástup IoT probíhá postupně a bude nějakou dobu trvat, než se dočkáme dokonalého fungování. Na obrázku 4 je znázorněno, jak odhaduje vývoj IoT společnost IDC⁴. Z tohoto



Obrázek 4: Odhad vývoje IoT podle IDC⁴

obrázku je patrné, že do 3 let, tedy do roku 2020, by se měl Internet věcí stát novým standardem IT a většina organizací bude čerpat nových výhod a příležitostí, který IoT nabízí. Je také nutno uvést, že zavedení IoT může přinést řadu překážek a nevýhod a to především v raných fázích, kdy nebudou použité technologie dostatečně odladěny nebo použity správně. O problematice nových očekávání z využití IoT technologií je napsáno v kapitole 2.4 *Nové možnosti IoT z hlediska podnikových procesů*.

Na Internet věcí je možné se dívat z více pohledů. Následující rozdělení vyplynulo z nastudování různých převážně online zdrojů, které se zabývají Internetem věcí. Následuje výčet s popisem každého z pohledů:

- **fyzický „věcný“ pohled⁵** – propojené (komunikující) fyzické objekty, které mají vestavěné senzory, aktuátory (ovladače) a další zařízení, které sbírají a posílají informace o těchto objektech;
- **infrastrukturní pohled⁶** – globální infrastruktura postavená na interoperabilitě různých sítí a protokolů;
- **výpočetní pohled⁷** – výpočetní schopnosti a konektivita rozšířená na objekty, které nejsou normálně považovány za počítače;

4 <http://connect.zive.cz/clanky/idc-internet-veci-bude-vetsi-trh-nez-smartphony-a-tablety-dohromady/sc-320-a-181851>

5 McKinsey Global Institute, Preparing IT Systems and Organizations for the Internet of Things

6 ITU, Recommendation ITU-T Y.2060. Overview of the Internet of things, 2013

7 The Internet of Things (IoT): An Overview, Karen Rose, et.al. The Internet Society, October 2015

- **cloudový pohled**⁸ – framework, ve kterém jsou všechny věci virtuálně reprezentované v internetu;
- **informační pohled**⁹ – „věci“ je cokoli, co je propojené a schopné shromažďovat současný stav/informace a jednat podle něj nebo jej odesílat jinému systému pro hlubší analýzu;
- **kybernetický pohled**¹⁰ – kyberfyzikální systém, který reprezentuje těsné spojení a spolupráci mezi výpočetními a fyzickými zdroji.

Samotné „věci“ můžeme také rozdělit do více kategorií [3] a to především podle toho, jaké informace jsou schopné poskytovat. Nejjednodušší věci mají pouze nějaký značkovací (tagging) mechanismus, např. RFID. Ten umožňuje nenápadný a nákladově efektivní způsob identifikace objektů. Další kategorií jsou věci, které jsou schopné snímat a ovlivňovat své okolí (mají zabudované smysly). Jako vstupní smysly fungují různé *senzory*, které umožňují vjem okolí a shromažďují o něm informace. Jako výstupní smysly slouží *aktuátory*, které umožňují měnit okolí na základě implementovaného rozhodnutí. Dají se také označit jako *ovladače*. Poslední kategorií jsou věci, které jsou často označovány jako „smart“ (chytré). Tyto věci mají vlastní aplikační logiku s určitou úrovní inteligence a rozšiřují výpočetní výkon na okraj sítě.

Z tohoto popisu se dají odvodit následující základní charakteristiky pro „věci“:

- mají výpočetní kapacitu, přestože nebyly primárně vytvořeny jako počítače;
- jsou připojeny k síti;
- jsou prvoplánově vždy zapnuty;
- generují, vyměňují a využívají data s minimální intervencí lidí;
- data z objektů přecházejí nakonec v nějaké podobě do IP sítí a jsou zahrnuta do produktových vlastností dostupných přes internet;
- uživatelé IoT zařízení nemají přímé informace o tom, kde a kdy byla data využívána zařízením přenesena po síti;
- mohou mít vlastní aplikační logiku a rozhodovací mechanismy, pak se nazývají „smart“;
- představují kyberfyzikální systém.

Internet věcí proniká do mnoha oblastí našich životů. Podle německé společnosti IoT Analytics, která se zabývá sledováním a analýzou trhu Internetu věcí, lze na základě studie [10] rozdělit IoT na dvě základní oblasti. A to spotřebitelský a podnikový Internet věcí. Detailní rozdělení je vidět na obrázku 5. Mezi dnešní hlavní aplikace IoT patří následující:

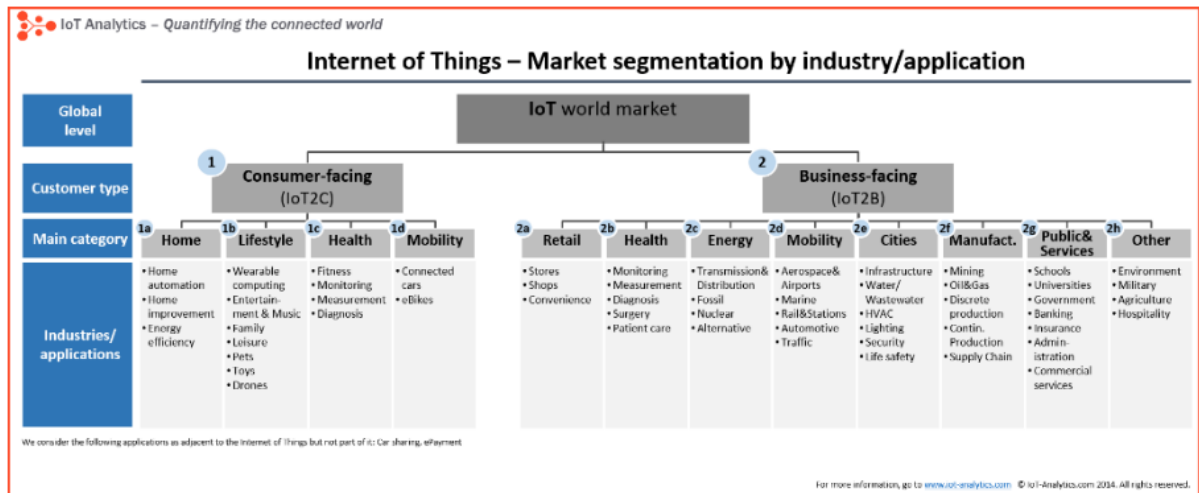
- *Chytrá domácnost* (smart home, domácí automatizace) – popisuje propojení a použití různých prvků IoT uvnitř domovů, jako např. regulátory teploty, detektory kouře, světla, dveřní zámky, spotřebiče a mnoho dalších.
- *Nositelná elektronika* (wearables) – různá zařízení, která lidé nosí na těle. Nejčastěji

8 ISOC, IoT Overview, December 2015

9 ISACA, Security and Privacy Challenges of IoT-enabled Solutions, July 2015

10 National Science Foundation, NSF 10-515 Cyber-Physical Systems (CPS)

se jedná o fitness náramky a chytré hodinky. Patří sem ale i brýle, se kterými se v roce 2013 snažil prorazit Google a nyní se o podobné snaží společnost Snap. Dalším příkladem můžou být chytrá sluchátka od společnosti Bragi, která kromě poslechu hudby měří fitness aktivitu a umožňují komunikaci s chytrým telefonem.



Obrázek 5: Segmentace IoT trhu [9]

- *Chytrá města* (smart cities) – do oblasti chytrých měst spadají různé případy užití, jako například řízení dopravy a parkovišť, distribuce vody a monitoring bezpečnosti nebo životního prostředí.
- *Průmysl* (industrial internet) – oblast s největším celkovým potenciálem. Vzniklo označení Průmysl 4.0 nebo čtvrtá průmyslová revoluce a zahrnuje chytré továrny, propojené stroje a další.
- *Automobily* (connected cars) – nabízí mnoho prostoru pro další vývoj. Může se jednat o samoříditelná auta, propojení mezi automobily, regulaci dopravy nebo platformy pro ovládání auta, jako je například CarPlay od společnosti Apple.
- *Zdravotnictví* (connected health) – zde se nabízí nové možnosti monitorování zdraví v reálném čase nebo např. vylepšení rozhodovacích procesů na základě velkého množství dat o pacientech.
- *Maloobchod* (smart retail) – mezi IoT koncepty maloobchodu patří nové platební metody, cílení reklamy na základě blízkosti nebo analýza chování zákazníků uvnitř obchodů.
- *Dodavatelský řetězec* (smart supply chain) – nové způsoby sledování dodávky zboží jako např. kontrola teploty u potravin nebo nárazů u křehkých předmětů.
- *Farmářství* (smart farming) – např. monitorování dobytku pomocí senzorů nebo sledování půdy.

Z technologického hlediska je IoT rozděleno na tři hlavní vrstvy. Jedná se o hardware, software a komunikaci. Hardware se týká senzorů, aktuátorů, úsporných čipů a dalších fyzických věcí. Software je především o ukládání a analýze dat, logice nad daty nebo

o aplikacích pro koncové uživatele. Pro komunikaci se nejčastěji používají bezdrátové technologie. Ve spojení s Internetem věcí se rozšířily tzv. LPWAN (Low Power Wide Area Networks) sítě [11]. Jedná se o sítě s větším dosahem než např. Wi-Fi nebo Bluetooth. Další klíčovou vlastností je nízká spotřeba energie a nízká cena. Z toho vyplývá, že využití takových sítí je vhodné, pokud je třeba přenášet malé objemy dat (řád desítek bytů) na velkou vzdálenost (cca 10 kilometrů) a udržet dlouhou životnost vysílacího zařízení na baterie (až 10 let). Z praktického hlediska mají tyto sítě využití např. v *chytrých městech* nebo *farmářství*. V České republice se od roku 2016 buduje síť Sigfox a také konkurenční LoRa.

2.4 Nové možnosti IoT z hlediska podnikových procesů

Propojení fyzických věcí, které jsou vybaveny senzory a aktuátory a mají schopnost zachytit a komunikovat informace o sobě i o svém okolí, přináší celou řadu nových možností. Obecná použití IoT byla popsána v kapitole 2.3 *Definice pojmu IoT*, z hlediska podnikových procesů IoT umožňuje:

- efektivnější výrobu a distribuci produktů;
- úsporu času;
- efektivnější ochranu majetku;
- úsporu za energii;
- a další.

Podle studie institutu McKinsey¹¹ by příležitosti vytvořené Internetem věcí měly mít do roku 2025 globální ekonomický dopad ve výši až 11 biliónů dolarů ročně. Příležitosti jsou v této studii definovány jako kolektivní finanční a nefinanční výhody, které mohou získat koncoví uživatelé z používání aplikací Internetu věcí.

Tyto příležitosti jsou velké, ale představují pro firmy mnoho nejistot. Jedou z otázek je, jak vybudovat technologickou strukturu, tj. vrstvy softwaru, hardwaru a síť¹². Tato struktura musí denně podporovat tisíce nezávislých událostí od stovek produktů, zařízení a aplikací a musí pracovat v reálném čase. Další velkou otázkou je interoperabilita IoT systémů. Téměř 40 % výše zmíněného ekonomického dopadu je odhadnuto na základě toho, že různé systémy spolu budou vzájemně spolupracovat a dosáhnou vzájemné součinnosti. Mezi další nejistoty spadá co největší využití nasbíraných dat. Např. ropná plošina se 30 tisíci senzory používá pouze 1% dat, protože pouze detekuje anomálie.¹³ Zabránění vzniku těchto anomálií je možné na základě využití veškerých dat, díky kterým je možná optimalizace a predikce.

Několik příkladů z praxe¹³, jak může IoT změnit (vylepšit) podnikové procesy:

- Prvním je řízení zásobování v podniku Wurth USA. Kamery zde počítají komponenty v kontejnerech podél výrobních linek a řídicí systém automaticky posílá

11 <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>

12 <http://www.mckinsey.com/industries/high-tech/our-insights/preparing-it-systems-and-organizations-for-the-internet-of-things>

13 <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/an-executives-guide-to-the-internet-of-things>

objednávky dodavatelům k naplnění kontejnerů.

- V druhém příkladě jsou použita data ze senzorů k predikci opotřebení nějakého zařízení, nebo stavu, kdy toto zařízení vyžaduje údržbu. Predikce může ušetřit náklady na údržbu o 40 % a snížit neplánované výpadky provozu na polovinu.
- Dalším příkladem je použití samořídících vozidel v těžebním průmyslu. To slibuje zvýšení produktivity o 25 % a také snižuje pravděpodobnost úrazů na pracovišti.
- Poslední uvedený příklad se týká vývoje produktů. Nové produkty sbírají data o své funkčnosti a také o tom, jak jsou používány. Data získaná tímto způsobem umožňují výrobcům modifikovat návrh produktu k lepším výkonům a nebo jim umožní zjistit, které vlastnosti a funkce nejsou využívány a měly by být eliminovány či předělány.

Obecně lze říci, že se IoT v podnicích snaží o zvýšení efektivity, účinnosti, kvality, výkonnosti a bezpečnosti procesů. Jak již bylo uvedeno výše, není to vždy přímočaré a 100% funkční řešení narůstá na komplikovanosti. Řekněme, že chceme mít zautomatizované otevírání vjezdové brány na základě příjezdu konkrétního vozu k této bráně a předpokládejme, že je brána součástí řadové zástavby ulice. Když se vůz přiblíží, vyšle signál řídicí jednotce a ta zařídí otevření brány. Na první pohled je to nová užitečná vlastnost, ale teď si představme, že pojedeme onou ulicí, ale nemáme v úmyslu do brány vjet. Vyšle se signál a brána se otevře. V tomto případě je nutné použít více zdrojů informací, než jen samotný příjezd auta (např. událost z kalendáře osoby v autě, která má přiřazenu lokaci nebo je vhodné ruční potvrzení na telefonu či palubního počítače auta) k rozhodnutí o otevření brány. Je tedy zřejmé, že pro nahrazení klasického ovládacího tlačítka pro otevření brány, bude potřeba vyvinout obsáhlý a do jisté míry inteligentní systém. Další z důležitých požadavků na takový systém je možnost nouzového ručního ovládání. Systém musí uživateli umožnit ruční ovládání v případech, kdy si „neví rady“ nebo uživatel vyžaduje jednorázově výjimku ze zaběhnutých pravidel.

Dalším velkým rizikem IoT, na kterém se shodlo několik expertů¹⁴, je bezpečnost a soukromí. Propojení mnoha zařízení, která sbírají informace o svém okolí představují velkou příležitost pro případné hackery a útočníky. Může jít čistě o nepovolený přístup k datům nebo až o převzetí kontroly nad určitým systémem. Z hlediska soukromí je třeba řešit, kdo vlastní shromážděná data a jak mohou být proti někomu použita.

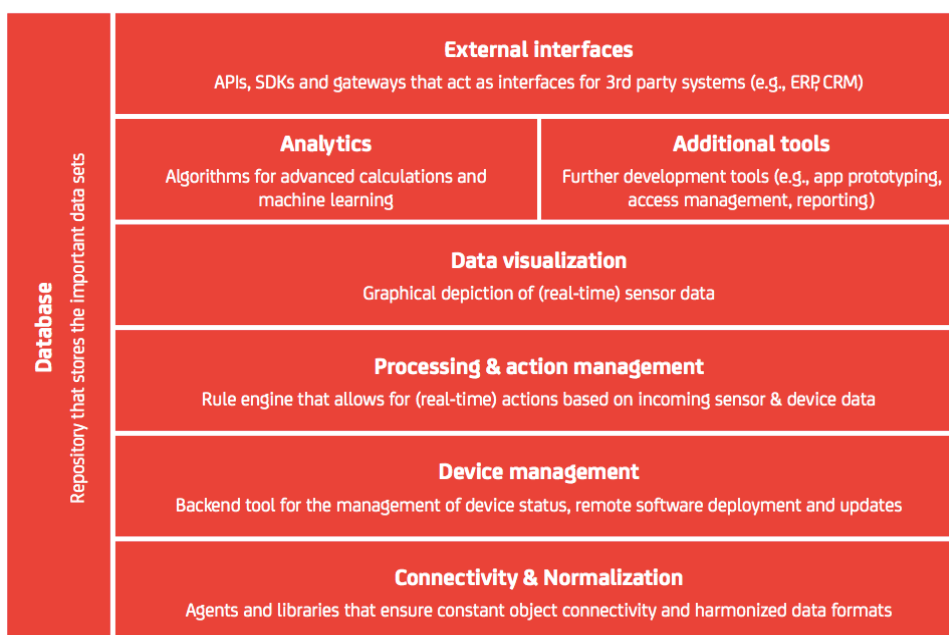
14 <http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-five-critical-questions>

3. Existující přístupy při návrhu procesů v prostředí IoT

Návrh procesů se tradičně týká lidí, obchodních partnerů a podnikových aplikací. Tato skutečnost se ale mění s přicházejícím Internetem věcí. Do návrhu je třeba začlenit „věci“ s jejich senzory a aktuátory, které mohou sami vykonávat určité činnosti. Vzhledem k tomu, že neexistuje jeden ucelený standard zavádění IoT, každá společnost řeší tento problém po svém. Většinou je nakreslen proces jako propojené, graficky ilustrované činnosti bez rozdělení podle jednotlivých technologických vrstev. Společnosti, které si na návrhu specifických procesů pro Internet věcí dávají více záležet, jsou rozebrány v následující kapitole.

3.1 IoT Analytics

Společnost IoT Analytics popisuje v [12] procesy pomocí IoT platformy. Jedná se o zobecněnou, teoretickou platformu, která obsahuje veškeré náležitosti, které by IoT platforma měla mít. Jde o následující softwarové části, které jsou také zobrazeny na obrázku 6:

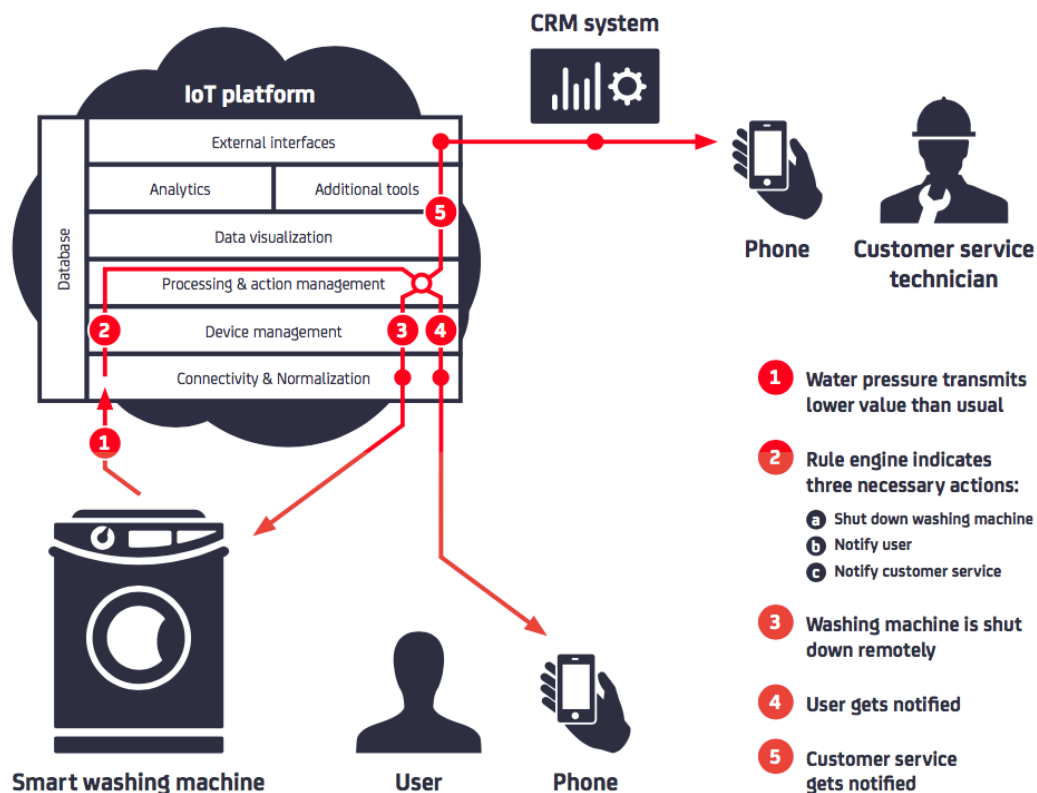


Obrázek 6: Osm základních částí IoT platformy [12]

- *konektivita a normalizace* – agenti a knihovny, které zajistí spojení mezi různými zařízeními a jednotný formát dat;
- *správa zařízení* – sledování statusu jednotlivých zařízení nebo vzdálené nasazení softwaru a aktualizací;
- *databáze* – slouží k ukládání důležitých dat;
- *zpracování a řízení akcí* – pravidlový software, který umožňuje provádět akce

- v reálném čase a to na základě vstupů ze senzorů a zařízení;
- *analytika* – algoritmy pro pokročilé výpočty a strojové učení;
- *vizualizace dat* – grafické znázornění dat v reálném čase;
- *dodatkové nástroje* – další vývojářské nástroje;
- *externí rozhraní* – API, SDK a brány, které slouží jako rozhraní pro systémy třetích stran.

Pomocí takové platformy je možné uspořádat a znázornit činnosti, které je nutné na procesu vykonat. IoT Analytics používají diagram s očíslovaným sledem činností, které jsou propojeny šipkami a mají uvedený popis. Šipky mají na sobě vyplněný kruh podle toho, v jaké části platformy se daná činnost provádí. Dále jsou v diagramu znázorněny jednotlivé prvky (aktéři) procesu. Jako příkladový proces poslouží komunikace „chytré“ pračky za účelem předejití úniku vody. Tato pračka je vybavena senzory, které analyzují spotřebu elektřiny, tlak vody a mechanické vibrace. Data ze senzorů jsou v reálném čase zpracovávána a na základě detekce abnormalit je pračka zastavena ještě před tím, než způsobí škodu. Na



Obrázek 7: Diagram procesu podle IoT Analytics [12]

obrázku 7 je znázorněn tento proces. Začíná tím, že senzor tlaku vody v pračce naměří nižší hodnotu, než je obvyklé a pošle tuto hodnotu skrze bezdrátovou síť do IoT platformy. Následnou činností je označení nezbytných úkonů, které je třeba na základě naměřené hodnoty vykonat. To se děje ve vrstvě *zpracování a řízení akcí*, která je pro správnou funkčnost celého systému klíčová. V tomto případě se jedná o tři činnosti: vypnutí pračky, zaslání upozornění uživateli a upozornění zákaznického servisu. Vypnutí pračky se provede na základě bezdrátového poslání zprávy zpět na pračku skrz vrstvu *konektivita*

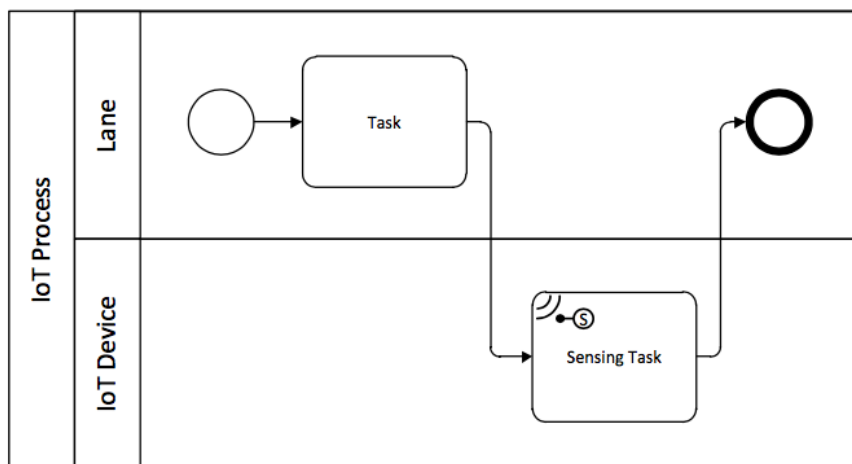
a normalizace. Následně je skrz stejnou vrstvu platformy poslána notifikace do uživatelské aplikace na chytrém telefonu uživatele. Poslední činnost – upozornění zákaznického servisu – obsahuje posláni upozornění do CRM systému dodavatele pračky skrze *externí rozhraní*.

Takovéto schématické znázornění procesů je na první pohled názorné, ale jeví se příliš abstraktně. Některé části jako např. identifikace potřebných činností na základě naměřené hodnoty nejsou zcela objasněny. Proto se v druhé části této kapitoly věnuji notaci BPMN, která umožňuje vytvoření návrhu s různými úrovněmi abstrakce.

3.2 Rozšíření BPMN

Přístup popsáný v [13], využívá notaci BPMN 2.0 a doplňuje ji o nové komponenty pro IoT zařízení a software s nimi spojený. Samotnou notaci BPMN popisují v kapitole 4.1.1 *Použité techniky*. Tento přístup si zakládá na tom, že v současnosti neexistuje standardizovaný způsob zahrnutí IoT zařízení a služeb do procesních diagramů.

Na obrázku 8 je znázorněné rozšířené BPMN schéma podle tohoto přístupu. Jako první byla do procesu přidána plavecká dráha, která je dedikovaná určitému IoT zařízení. Druhé



Obrázek 8: Znázornění činnosti, která je spojená s IoT zařízením [12]

rozšíření diagramu je v podobě činnosti, která je specifická pro IoT zařízení. Ta je zobrazena uvnitř nově přidané plavecké dráhy a je označena charakteristickou ikonou v podobě kolečka s písmenem „s“. Tato ikona znázorňuje, že se jedná o činnost senzoru. V případě, že se by se jednalo o činnost aktuátoru, ikona by měla jinou podobu. Autoři rozšíření však tuto ikonu nevedli, doporučoval bych použít analogickou ikonu s náhradou písmene „s“ (senzor) za „a“ (aktuátor). Tímto způsobem je tedy možné znázornit procesy, které obsahují činnosti spojené s IoT zařízeními.

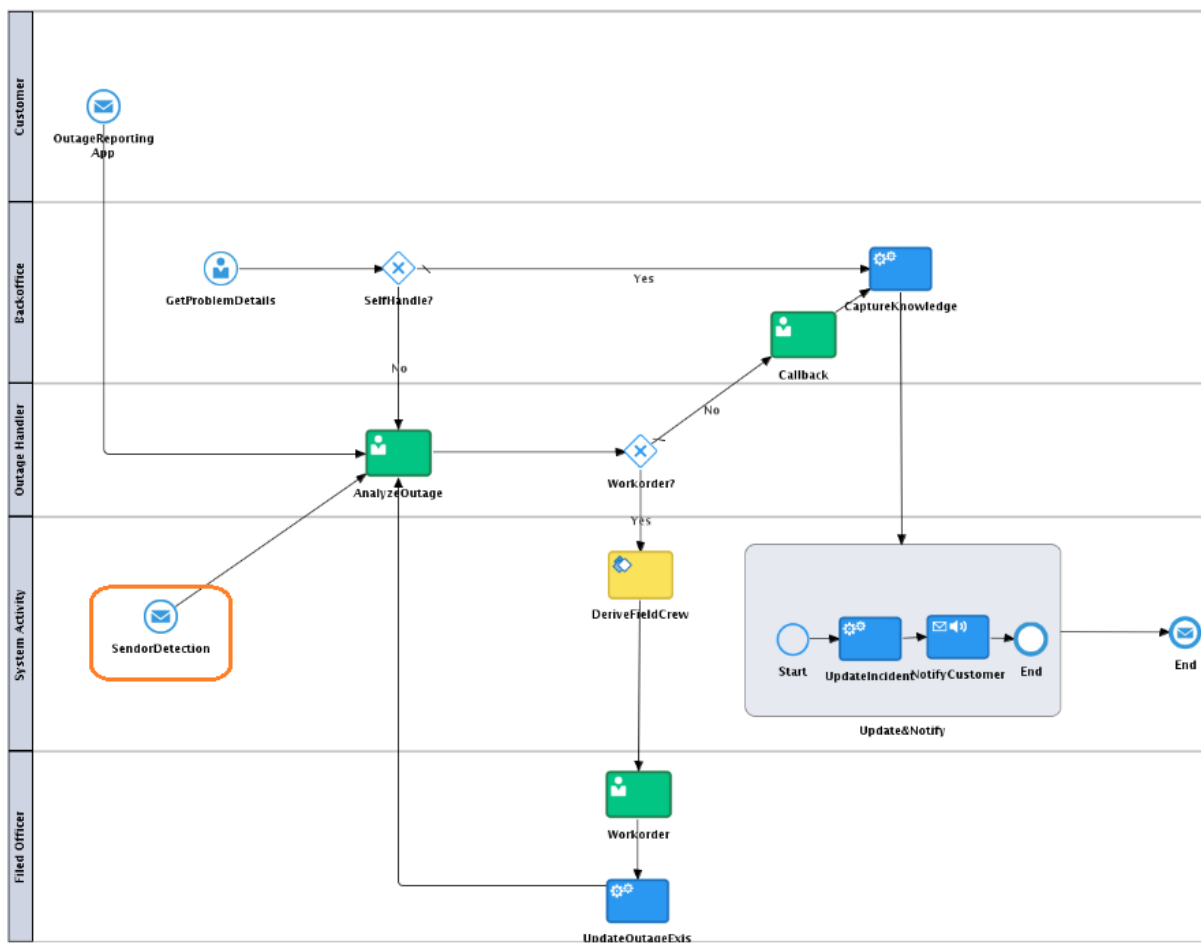
3.3 Přístup společnosti Oracle

Společnost Oracle na svých webových stránkách popisuje¹⁵, jak integruje IoT a řízení podnikových procesů na případu užití „řešení výpadku proudu pomocí IoT“. Tvrdí, že základem všech IoT procesů by měly být následující kroky:

¹⁵ https://blogs.oracle.com/acharyavivek/entry/internet_of_things_and_business

- cítit (sense),
- získat (acquire),
- komunikovat (communicate),
- zpracovat události (event processing),
- integrovat (integrate),
- zviditelnit a analyzovat (visualize and analyze).

Existuje více způsobů, jak takový proces iniciovat. Zákazník může výpadek nahlásit skrze mobilní aplikaci nebo zavolat na příslušnou linku. Nově může být proces zahájen na základě detekce senzorů. Na obrázku 9 je diagram tohoto procesu a detekce pomocí senzorů je oranžově zvýrazněna. Použitá notace je opět BPMN a není využito žádných speciálních entit



Obrázek 9: Znárodnění procesu společnosti Oracle ¹⁵

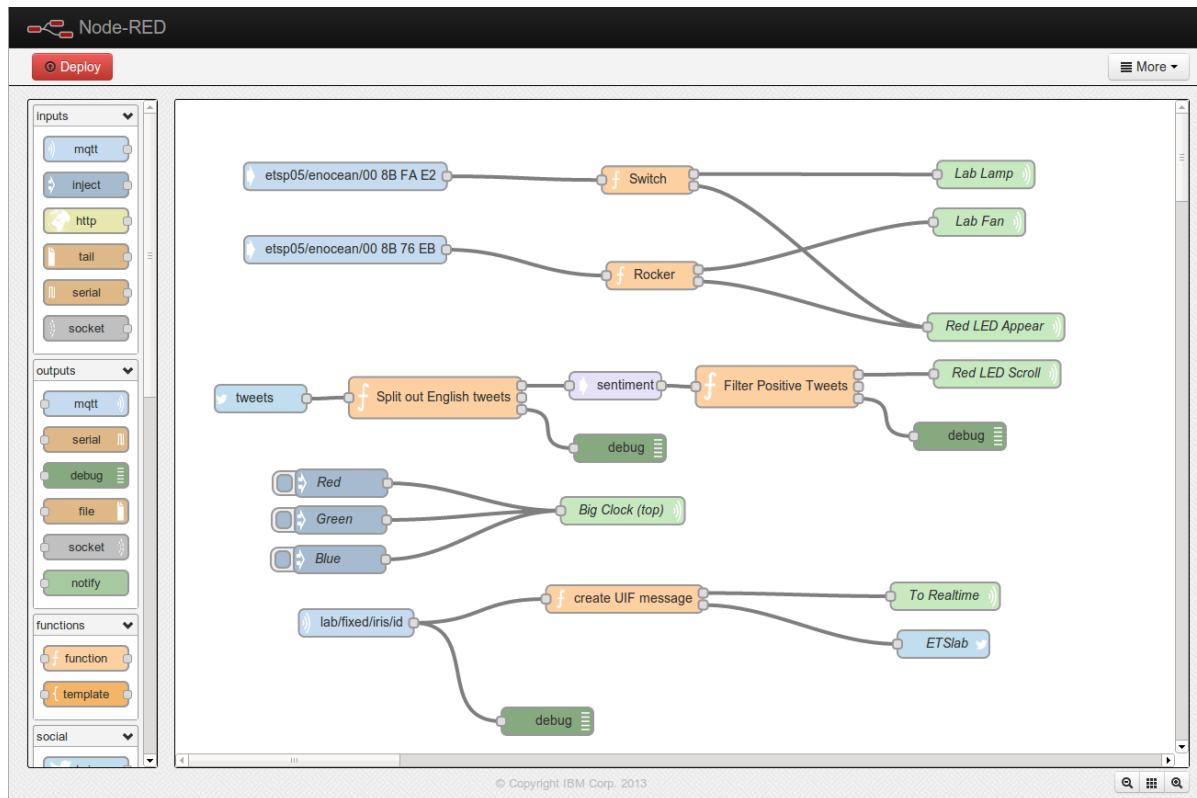
pro odlišení IoT činností. Zvýraznění je v tomto případě pouze ilustrativní. Oracle pro tvorbu procesních diagramů využívá cloudovou aplikaci Process Cloud Service.

3.4 Přístup společnosti IBM

IBM vytvořilo programovací nástroj Node-RED¹⁶, který slouží pro propojování hardwarových zařízení, aplikačních programovacích rozhraní (APIs), online služeb

¹⁶ <https://gigaom.com/2013/09/27/meet-node-red-an-ibm-project-that-fulfills-the-internet-of-things-missing-link/>

a databází. Cílem je, definovat, co mají jednotlivá zařízení dělat. Jak to udělají už je interní věc Node-RED. Jedná se o grafické rozhraní, ve kterém se propojí jednotlivé uzly, které reprezentují výše zmíněné části. Toto rozhraní je zobrazeno na obrázku 10. Dojde tak k vytvoření jakéhosi toku činností, tedy procesu.



Obrázek 10: Rozhraní nástroje Node-RED ¹⁶

3.5 Přístup společnosti Mindtree

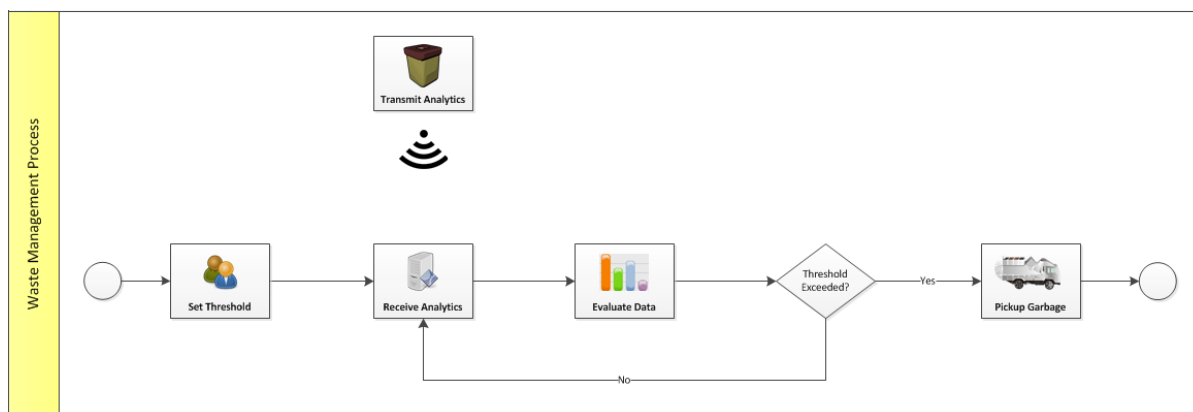
Softwarový architekt Adeel Javed ze společnosti Mindtree publikoval sérii článků¹⁷ na serveru bpmleader.com o využívání Internetu věcí k vylepšení podnikových procesů. V druhé části série¹⁸ vysvětluje na procesu, jaké výhody může IoT přinést do řízení odpadního průmyslu. Konkrétně se jedná o proces svozu odpadu. Ve výchozím stavu procesu musí popelářské auto projet naplánovanou trasu a vybrat odpad nehledě na to, jestli jsou popelnice plné či prázdné. Přidáním senzorů a umožněním bezdrátové komunikace lze docílit toho, že popelářské auto nemusí jezdit k prázdným či poloprázdným popelnicím a tím optimalizovat svou cestu. To dále povede ke snížení nákladů a znečištění ovzduší. Na obrázku 11 je tento proces nakreslen. Skládá se z následujících činností:

- *Nastavení prahu* (Set treshold) – v systému je nastaven práh, kdy už se popelnice považuje za plnou.

¹⁷ <http://www.bpmleader.com/2014/12/23/business-process-improvement-using-internet-of-things-part-1/>

¹⁸ <http://www.bpmleader.com/2015/02/11/business-process-improvement-using-internet-of-things-part-2/>

- *Příjem dat* (Receive analytics) – popelnice bezdrátově posílá data ze senzoru.
- *Vyhodnocení dat* (Evaluate data) – data jsou vyhodnocena a v případě, že je dosaženo zvoleného prahu plnosti, přechází se na poslední činnosti.
- *Sběr odpadu* (Pickup garbage) – tato činnost v sobě ukrývá plánování optimální trasy a samotný výjezd popelářského auta.



Obrázek 11: Znárodnění procesu svozu odpadu ¹⁸

Procesní diagram nevyužívá žádnou ze standardních notací a je nakreslen velice abstraktně. Pro ilustraci činností jsou použity barevné ikony a přenos zpráv je naznačen ikonou pro bezdrátovou komunikaci. Je patrné, že autor nakreslil procesní diagram pouze pro ilustraci problému a nepoužil žádnou metodu pro implementaci IoT řešení procesním způsobem.

3.6 Shrnutí k existujícím přístupům

Vzhledem k tomu, že je IoT relativně mladá oblast informačních technologií a zatím nepronikla do většiny podnikových procesů, není zcela běžné tyto procesy modelovat se zaměřením na požadavky IoT. Také se doposud neujal žádný standardizovaný přístup návrhu procesů v prostředí IoT. Jednotlivé společnosti přistupují k návrhu procesů po svém a znázorňují procesy různými způsoby. První popsany přístup (3.1 *IoT Analytics*) je zajímavý tím, že využívá užitečné rozdělení na jednotlivé vrstvy IoT platformy, která je v nějaké podobě nezbytná pro fungování a komunikaci IoT zařízení. Silnou stránkou druhého přístupu (3.2 *Rozšíření BPMN*) je, že vychází ze standardizované notace BPMN a doplňuje ji o specializované prvky pro IoT. Třetí přístup (3.3 *Přístup společnosti Oracle*) využívá specializovaný software pro návrh procesů, které jsou následně implementovány vývojáři. Společnost IBM (3.4 *Přístup společnosti IBM*) vyvinula specifický nástroj Node-RED, který je velice inovativní ve způsobu, jakým popisuje a implementuje procesy. Slouží k naprogramování věcí, aby dělaly to, co chceme a to bez napsání jediného řádku kódu. Poslední přístup (3.5 *Přístup společnosti Mindtree*) jen potvrzuje absenci ucelené metody pro zavádění IoT procesním způsobem. V další části se zabývám vlastním návrhem metody pro zavedení IoT řešení procesním způsobem.

4. Návrh metody pro zavedení IoT řešení procesním způsobem

V této kapitole je popsána metoda, která slouží k návrhu a implementaci IoT řešení procesním způsobem.

4.1 Principiální základy navržené metody

Metoda vychází ze čtyř základních kroků reinženýringu procesů, který je popsán v kapitole 2.3 *Definice pojmu IoT*. Jedná se o identifikaci procesu, analýzu stávajícího stavu (as-is), návrh nového stavu (to-be) a přechodu do (implementaci) nového stavu. První krok – identifikaci procesu – navržená metoda neobsahuje, protože se předpokládá použití této metody ve chvíli, když už známe proces, který je třeba přetvořit. Analýza stávajícího stavu je provedena pomocí sepsání činností s jejich vstupy a výstupy do tabulky, která slouží jako podklad pro nakreslení procesního diagramu. Tato tabulka může také obsahovat podrobnější popis činností, který se do procesního diagramu nevejde.

Pro návrh nového stavu procesu je klíčová analýza příležitostí, které jsou umožněny Internetem věcí. IoT nabízí mnoho nových možností, ale jen některé mají opravdový smysl (viz příklad s bránou v kapitole 2.4 *Nové možnosti IoT z hlediska podnikových procesů*). Možnosti, které mají pozitivní dopady, jsou nazývány příležitostmi a jejich analýza se snaží najít takové změny, které povedou k efektivnějším, kvalitnějším a bezpečnějším výstupům. Implementace nového stavu je závislá na použitých IoT technologiích a díky nízké úrovni interoperability současných IoT řešení neexistuje ucelený, obecný postup, jak nový stav procesu implementovat. Vesměs je nutné propojit data z různých zdrojů a na jejich základě provádět akce. K tomu byl v rámci této práce vyvinut software, na který bude dále odkazováno jako na IoT Manažera a jeho popis je uveden v kapitole 4.3 *Role IoT Manažera při provádění procesu*.

Navržená metoda je tedy rozdělena na čtyři po sobě jdoucí etapy. Podrobný popis každé z nich je dále uveden v následující kapitole 4.2 *Implementační etapy metody*.








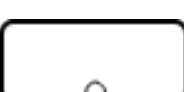



4.1.1 Použité techniky






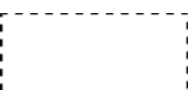
Metoda využívá tabulkových popisů a notace BPMN. Ta je použita pro zápis a znázornění procesů a informací o nich. Tabulkové popisy jsou použity pro prvotní utřídění činností na procesu s příslušnými vstupy a výstupy a později je tato tabulka doplněna o tři nové prvky, které vyplývají z analýzy příležitostí díky IoT možnostem. Jedná se o IoT aktiva, IoT věci a IoT aktivity. Tyto prvky jsou popsány v kapitole 4.2.2 *Etapa 2: Analýza příležitostí IoT k reinženýringu procesu*.

Notace BPMN 2.0 (Business Process Model and Notation) [9] je soubor principů a pravidel, který slouží pro grafické znázorňování podnikových procesů pomocí procesních diagramů. Hlavním cílem je poskytnout snadno pochopitelnou notaci pro všechny zaměstnance, kteří se na procesu podílí. Ať už jsou to obchodní analytici, kteří vytváří prvotní návrh procesu, vývojáři, kteří jsou zodpovědní za implementaci, nebo manažeři, kteří

řídí a dohlíží na provádění procesu. BPMN je současným standardem pro modelování podnikových procesů a jeho vývoj a správu zjišťuje Object Management Group (OMG).

V následující tabulce 1 jsou vysvětleny a popsány použité prvky BPMN.

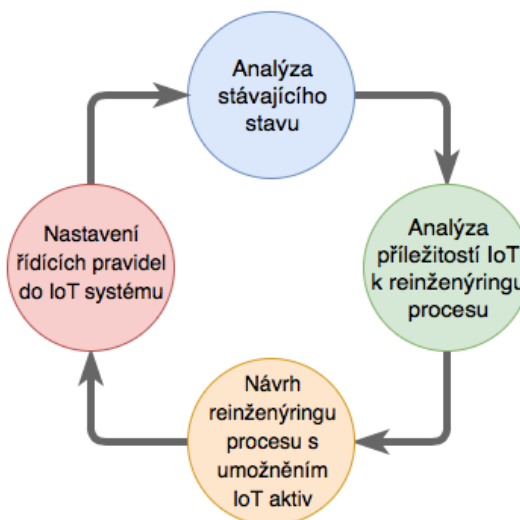
Název prvku	Grafický symbol	Popis	
Událost		Počáteční událost (nespecifikovaná)	K událostem dochází během procesu. Může se jednat o počáteční událost, která proces spustí nebo průběžné události, ke kterým dochází během procesu nebo koncová událost, kterou proces končí.
		Počáteční událost vyvolaná zprávou	
		Koncová událost (nespecifikovaná)	
		Průběžný odkaz	
		Koncový odkaz	
Činnost		Atomická činnost – úloha (nespecifikovaná)	Činnost či práce v procesu. Může být dále nedělena nebo v sobě může obsahovat samostatný proces nazývaný subprocesem.
		Činnost obsahující subproces	
		Opakující se činnost	
Rozhodovací brána		Exkluzivní brána – křižovatka v procesu, pokračuje se jen jednou cestou na základě podmínky	Brána slouží k řízení rozbíhání či souběhu toků procesu.
		Paralelní brána – všechny činnosti vstupující do brány musí být dokončeny, aby byla volána činnost z brány vystupující, rep. činnost vstupující do brány vyvolá všechny činnosti z brány vystupující.	
		Komplexní brána – v případě, že předchází dvě brány nevystihují situaci, je použita tato brána.	

Tok		Sekvenční tok – určuje pořadí činností.	Toky znázorňují návaznost (pořadí)
		Předdefinovaný sekvenční tok – určuje implicitní činnost, která následuje po větvení.	
		Tok zpráv – určuje předání zprávy mezi bazény.	
Data		Datový objekt	Posílání dat mezi aktéry procesu.
		Zpráva	
Textová poznámka		Poznámka k činnosti, větvení nebo jinému prvku procesu.	Textová poznámka objasňuje či doplňuje prvky diagramu.

Tabulka 1 – Vysvětlení prvků BPMN 2.0

4.2 Implementační etapy metody

Metoda byla rozdělena do čtyř navazujících etap (obrázek 12). První etapa slouží k analýze



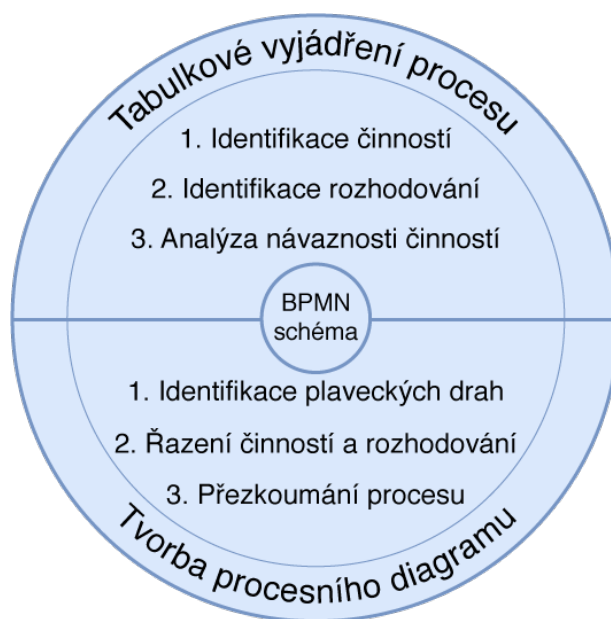
Obrázek 12: Etapy navržené metody

stávajícího stavu procesu pomocí tabulkového vyjádření, které je následně překresleno do BPMN schématu. V druhé etapě se zanalyzují příležitosti IoT, tedy jakého vylepšení můžeme pomocí IoT docílit. V další etapě se navrhne nový proces s využitím IoT příležitostí

a v poslední etapě se provede nastavení pravidel do softwaru IoT Manažer včetně konfigurace senzorů do systému.

4.2.1 Etapa 1: Analýza stávajícího stavu

Nejprve je nutno řešený proces pochopit ve všech jeho souvislostech. První etapa má proto za cíl zjistit co nejvíce informací o stávajícím procesu (tzv. as-is). Na obrázku 13 jsou znázorněny jednotlivé kroky etapy. První skupina kroků této etapy se týká **vypracování tabulkového vyjádření procesu**. Jde o sepsání prvotních myšlenek a informací o procesu. Tato tabulka má čtyři sloupce: činnost, vstup, výstup, popis. Tvorba tabulky se skládá ze tří kroků:



Obrázek 13: Kroky první etapy – analýza stávajícího stavu procesu

1. **Identifikace činností procesu** – do tabulky jsou napsány prováděné činnosti s jejich vstupy, výstupy a popisem. Činností může být například odeslání určitého dokumentu nebo například vytvoření ceníku služeb atd.
2. **Identifikace rozhodování na procesu a podmínek pro rozhodování** – v procesu je obvyklé vykonávání různých činností na základě podmínek. Toto větvení je třeba pochopit a identifikovat. Může jít například o odeslání různých dokumentů různými prostředky nebo odeslání dokumentu jen v případě, že splňuje určitá kritéria.
3. **Analýza návaznosti činností na procesu** – jedná se o seřazení činností v procesu. Vychází se z rozhodovacích podmínek a také platí pravidlo, že výstup jedné činnosti se zpravidla stává vstupem do činnosti navazující.

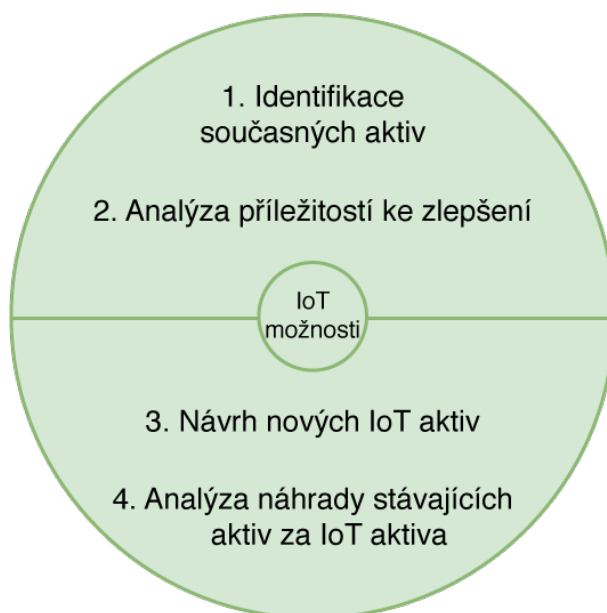
Ve druhé skupině kroků první etapy je **zpracován procesní diagram**. Jde o zobrazení procesu jako sledu činností identifikovaných v první skupině kroků tabulkového vyjádření stávajícího stavu procesu s doplněním o rozhodovací brány a události. Rozhodovací brány implementují větvící podmínky a události jsou jednorázové akce, ke kterým dochází v průběhu procesu (např. příchod zprávy). Jak bylo napsáno v kapitole 4.1.1 *Použité techniky*, k tvorbě procesního diagramu je využito schematické znázornění procesu pomocí BPMN notace.

Tvorba procesního diagramu stávajícího stavu procesu se skládá ze tří dílčích kroků:

1. **Identifikace bazénů a plaveckých drah** (*swimlanes, kontextů*) – jedná se o velmi důležitou část tvorby diagramu. Na základě charakteru řešeného problému je třeba identifikovat důležité prvky (aktéry) procesu. Každý takový prvek by měl mít svůj bazén a v případě, že lze tento prvek dále vnitřně rozdělit, vytvoří se uvnitř bazénu více plaveckých drah příslušící jednotlivých částem. Jako příklad samostatného bazénu může sloužit administrativní oddělení v podniku, které by se dalo dále rozdělit do plaveckých drah: tisk a sken dokumentů, vyřizování podpisů nebo zpracování mezd.
2. **Řazení činností a rozhodování do průběhu procesu s kreslením procesního diagramu** – jednotlivé činnosti z tabulkového popisu procesu se přenesou do příslušných plaveckých drah a spojí se pomocí šipek na základě analýzy návaznosti činností. Dále jsou mezi činnosti vloženy rozhodovací brány, které zajistí větvení na procesu podle stanovených podmínek. Dalšími prvky diagramu, které jsou většinou nezbytné, jsou datové objekty a zprávy. Ty znázorňují komunikaci mezi jednotlivými prvky procesu (tj. mezi bazény). Může jít například o znázornění toho, že IoT Manager dá pokyn určitému aktuátoru na provedení akce.
3. **Přezkoumání navrženého procesu jako celku** – tento krok slouží ke kontrole správnosti diagramu. Je třeba zkontrolovat jednotlivé části procesu, správnou návaznost, správné rozhodovací podmínky a datové toky. V případě nějakých nesrovnalostí je třeba diagram upravit a typická je i zpětná úprava tabulky z prvního kroku první etapy.

4.2.2 Etapa 2: Analýza příležitostí IoT k reinženýringu procesu

Druhá etapa má za cíl zanalyzovat příležitosti, které může Internet věcí umožnit. Zde je nutné zavedení následujícího nového pojmu:



Obrázek 14: Kroky druhé etapy – analýza příležitostí IoT

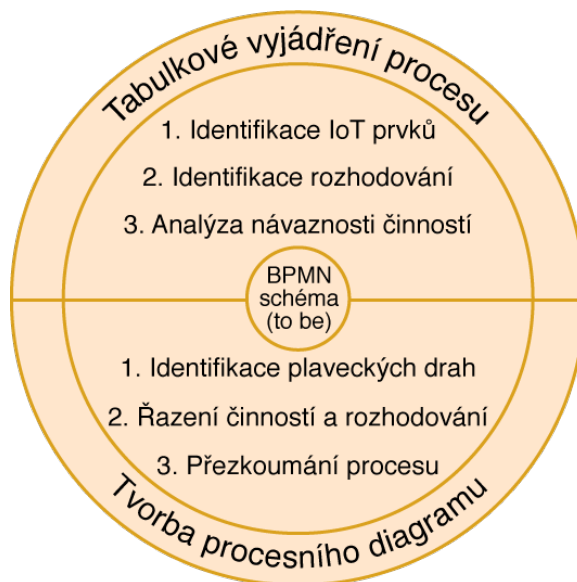
- **IoT aktivum** – název pro nová aktiva, která jsou umožněna Internetem věcí. Aktivum je to, co se na procesu sleduje (co má smysl řídit), např. informace o tom, že někdo je v budově nebo zda je prázdná garáž.

Nalezení nových aktiv, které bude možné sledovat díky IoT je klíčové pro celou metodu. Tato etapa se drží následujících kroků (obrázek 14):

1. **Identifikace současných aktiv procesu** – identifikace toho, co se v současnosti sleduje na procesu. Aktiva jsou napsána do nové tabulky do sloupce *aktiva*. Může jít například o informaci o tom, jestli je správně vyplněn formulář, který je tvořen v průběhu procesu.
2. **Analýza příležitostí ke zlepšení procesu** – tato část metody představuje jakési zamyšlení nad IoT příležitostmi, které lze využít pro dosažení lepších výsledků. Může jít o přidání různých senzorů, úplné nahrazení současných fyzických věcí věcmi se zabudovanými senzory či aktuátory, využití nových komunikačních kanálů atd. Dále je nutné porovnání těchto možností a rozhodnutí, které jsou nejvíce výhodné. V tomto kroku může být vytvořen rizikový scénář nebo prostý expertní názor.
3. **Návrh nových IoT aktiv procesu** – na základě předchozího kroku se navrhnou nová aktiva procesu. Půjde o informace, které jsou nově dostupné díky IoT technologiím. Aktiva jsou zapsána do druhého sloupce – *IoT aktiva* – tabulky z kroku 1.
4. **Analýza náhrady stávajících aktiv za IoT aktiva** – porovnání původních a nově získaných aktiv. Zamyšlení se nad tím, jestli jejich přínos převyšuje vynaložené úsilí na realizaci.

4.2.3 Etapa 3: Návrh reinženýringu procesu s umožněním IoT aktiv

Třetí etapa, jejíž kroky jsou znázorněny na obrázku 15, má za cíl navrhnout nový,



Obrázek 15: Kroky třetí etapy – návrh reinženýringu procesu

reinženýringovaný proces (tzv. to-be). Tato etapa má shodné kroky s první etapou, ale tvorba tabulky a diagramu je rozšířená o *IoT aktiva* z předchozí etapy a další dva nové

prvky:

- **IoT věci** – nově přidané zařízení nebo stávající zařízení obohacené o nové senzory, aktuátory či funkce, které přinese nové možnosti do procesu.
- **IoT aktivity** – činnosti, které vykonávají IoT věci nebo IoT Manager.

V první skupině kroků této etapy je doplněno a rozšířeno tabulkové vyjádření procesu z první etapy a ve druhé skupině kroků je zpracován nový procesní diagram zahrnující navržené změny. Diagram vychází z doplněného tabulkového vyjádření a má nové bazény a plavecké dráhy na základě architektury IoT prvků. Mnohdy se stane, že je nový proces natolik složitý, že je vhodnější jej rozdělit na několik subprocesů. V tomto případě se nakreslí první celkový diagram, který bude obsahovat jen jakousi kostru celého procesu a bude zcela bez bazénů a plaveckých drah. Činnosti tohoto diagramu budou znázorněny jako subprocesy a budou podrobněji rozkresleny v samostatných diagramech. Z praktického hlediska je výhodnější nejprve nakreslit celý proces ve vší obsáhlosti do jednoho diagramu a ten poté rozdělit na jednotlivé subprocesy. A na základě tohoto rozdělení vytvořit obecný diagram bez bazénů.

Opět zde následuje podrobnější popis jednotlivých kroků etapy. První skupina kroků zahrnuje **zpracování tabulkového vyjádření procesu** a postup je následovný:

1. **Identifikace činností procesu a IoT prvků** – rozšíření tabulkového vyjádření procesu o nově identifikované činnosti a jejich popis, vstupy, výstupy, IoT věci, IoT aktiva a IoT aktivity. Samotné IoT aktivity mohou figurovat jako plnohodnotné činnosti a může se tedy stát, že buňka řádku tabulky ve sloupci *činnost* bude prázdná.
2. **Identifikace rozhodování na procesu a podmínek pro rozhodování** – pochopení a identifikace nových rozhodovacích podmínek na procesu vycházejících z předešlých změn.
3. **Analýza návaznosti činností na procesu** – stejné zamyšlení nad pořadím činností jako v první etapě.

V momentě, kdy je hotová tabulka, opět následuje zpracování procesního diagramu a to v rámci druhé skupině kroků:

1. **Identifikace bazénů a plaveckých drah** – nově přidané IoT prvky vyžadují nové bazény a plavecké dráhy na základě své architektury. Jako příklad může sloužit obecná IoT „věc“, která by tvořila samostatný bazén a plavecké dráhy by byly následující: senzory, aktuátory, data, logika a uživatelské rozhraní.
2. **Řazení činností a rozhodování do průběhu procesu s kreslením procesního diagramu** – stejně jako v první etapě se nakreslí činnosti z tabulkového popisu do příslušných drah procesního diagramu.
3. **Přezkoumání navrženého procesu jako celku** – i zde se stejně jako v první etapě provede kontrola správnosti diagramu. Je třeba zkontrolovat logiku jednotlivých částí procesu, správnou návaznost, správné rozhodovací podmínky a datové toky. V případě nějakých nesrovnalostí je třeba diagram upravit a typická je i zpětná úprava tabulky z prvního kroku první etapy.

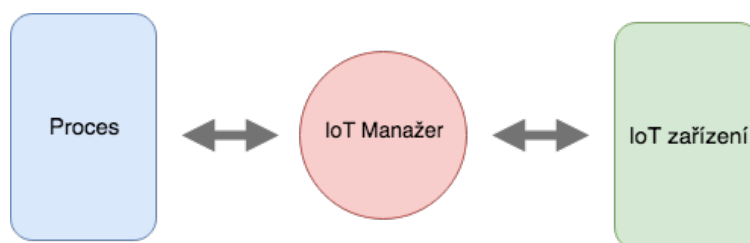
4.2.4 Etapa 4: Nastavení řídicích pravidel a konfigurace IoT Manažera

Poslední etapa je klíčová pro nasazení nového procesu do ostrého provozu. Nezbytnou součástí reinženýringu podnikových procesů s využitím IoT zařízení je řídicí software IoT Manažer, který byl naprogramován v rámci této práce. V první řadě je nutné do systému přidat jednotlivé IoT zařízení (čidla a ovladače), které se v procesu vyskytují. Toho se docílí přidáním informací o zařízení do konfigurační databáze.

Dále je třeba nastavit řídicí pravidla, které celý proces zautomatizují. Tato pravidla musí být nejprve identifikována. Musí zahrnovat všechny činnosti IoT Manažera z předešlých etap. Nastavení probíhá přes uživatelské rozhraní.

4.3 Role IoT Manažera při provádění procesu

Jakmile je reinženýring procesu úspěšně hotový, je třeba zasadit nový proces do ostrého provozu. V této fázi proti sobě stojí proces jako takový a jednotlivá IoT zařízení, která realizaci procesu umožňují. IoT Manažer je řídicí software, který představuje spojovací vrstvu mezi procesem a IoT zařízeními (znázorněno na obrázku 16). Jeho hlavní úlohou je



Obrázek 16: Role IoT Manažera

přijímat data z IoT zařízení co nejbližně reálnému času, vyhodnocovat je a na jejich základě dávat pokyny k automatizovaným akcím, které jsou základem nově navrženého procesu. Vyhodnocení se děje pomocí pravidel typu „IF THEN“ a jednou z hlavních částí programu je inferenční mechanismus, který tato pravidla prochází a vyhodnocuje.

IoT Manažer je nezbytnou vrstvou mezi procesy a IoT zařízeními, která je propojuje a řídí.

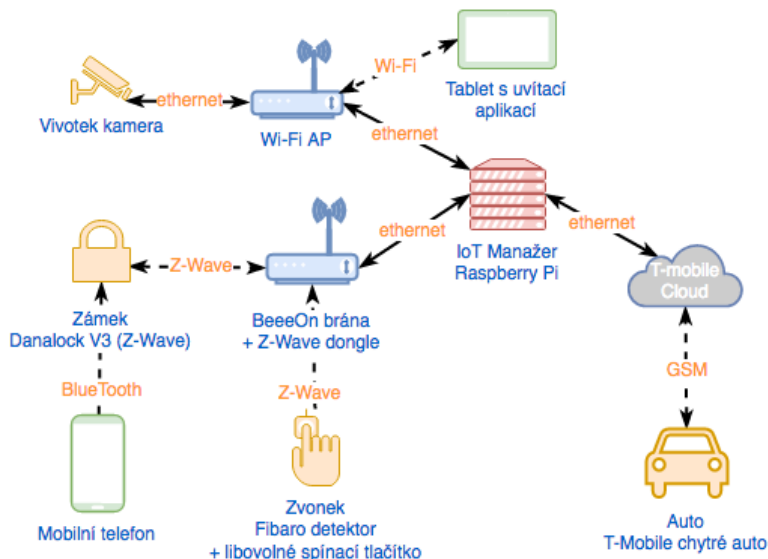
5. Volba případové studie pro ověření metody v praxi

Tato kapitola je věnována výběru a popisu případové studie, na které bude ověřena navržená metoda implementace IoT. Bylo třeba vybrat vhodný proces a vhodné IoT technologie pro jeho reinženýring.

5.1 Zvolená případová studie

Zvolenou případovou studií je proces zajištění pohybu oprávněných osob ve firemních prostorách s využitím vícefaktorové autentizace. Proces je realizován v rámci společnosti s cca 10 zaměstnanci, která sídlí v samostatně stojící budově s kanceláři. Klíčovým prvkem je umožnění vstupu pouze autorizovaným osobám, neumožnění vstupu nepovoleným osobám, identifikace pokusů o nežádoucí vniknutí a vedení záznamů o příchodech a odchodech zaměstnanců.

Dnešní dveře bývají často zabezpečeny pouze klíčem, který může majitel lehce ztratit či mu může být odcizen. V takovém případě má případný lupič vcelku snadný přístup do důležitých prostor, což může mít za následek velké škody. Dále v menších společnostech většinou nebývá veden záznam docházky zaměstnanců, což zaměstnavateli znesnadňuje kontrolu přítomnosti pracovníků.



Obrázek 17: Zvolené IoT technologie

Základní činností procesu je odemknutí dveří zaměstnanci a zaznamenání jeho příchodu. Odemknutí se musí dít na základě více faktorů ověření totožnosti konkrétní povolené osoby. Takové ověření je možné s využitím IoT technologií, které jsou popsány v následující podkapitole.

Dokumentace výchozího stavu případové studie reinženýringu procesu zajištění pohybu

oprávněných osob ve firemních prostorech s využitím více-faktorové autentizace je prvním krokem navržené metody implementace IoT procesním způsobem (viz kapitola 6. *Aplikace navržené metody na reinženýring procesu z případové studie*).

5.2 Zvolené IoT technologie

V této podkapitole jsou uvedeny jednotlivé použité IoT technologie a jejich popis. Výběr vycházel z analýzy příležitostí, která je součástí druhé etapy navržené metody. Na obrázku 17 jsou vyobrazena použitá zařízení („věci“) a příslušná propojení komunikačními protokoly. Centrem řízení systému je lokální serverová aplikace (IoT Manažer).

5.2.1 Zařízení

Zde je uveden popis jednotlivých IoT zařízení.

Zámek Jde o přídatný prvek k současnému zámku, který umožňuje otáčení západkou z vnitřní strany dveří. Toto zařízení se připojuje k mobilnímu telefonu přicházejícího zaměstnance pomocí Bluetooth a provádí jeho autentizaci. Zařízení také komunikuje s bránou, která je připojená na server. Pro tuto komunikaci je vyhrazen protokol Z-Wave.

Kamera Snímá dění přede dveřmi a v případě příchodu člověka posílá snímek obličeje na identifikaci osoby na server.

Zvonek Jedná se o tlačítko připojené pomocí Z-Wave protokolu k bráně, která záznam o zvonění posílá na server. Další z možných použití je při zazvonění zachytit osobu přede dveřmi na kameru a v případě rozpoznání obličeje osoby se tato informace přiřadí k záznamu o zvonění. Signál tlačítka také spustí zvukovou signalizaci zvonku uvnitř objektu.

Automobil Automobilem se myslí zařízení připojená do ODB portů firemních automobilů, která bezdrátově posílají informace o daném vozidle. V současnosti je sledována poloha vozu pro identifikaci příjezdu konkrétního zaměstnance. To slouží jako jeden z faktorů autentizace a také k případnému otevření vjezdové brány.

Výběr těchto zařízení je dán charakterem konkrétního procesu a existuje mnoho jiných zařízení, která by mohla být použita. Některá zařízení, jako například kamery určené pro identifikaci obličeje, nejsou v současnosti snadno dostupná a obvykle nemají požadovanou technologickou úroveň a spolehlivost a jejich využitelnost je spíše ve fázi zkoušení (tzv. „proof of concept“). Mohlo být použito více dalších zařízení, ale pro splnění současných požadavků je tato sestava zcela dostačující.

5.2.2 Komunikační protokoly

Pro komunikaci mezi prvky systému bylo použito následujících bezdrátových protokolů.

Bluetooth Využit pro připojení mobilního telefonu jako jeden z faktorů autentizace.

Z-Wave Určen pro komunikaci mezi prvky, které vyžadují větší dosah, než Bluetooth, ale mají menší nároky na přenos dat.

Wi-Fi Pro zařízení, které budou přenášet větší objemy dat a jsou v kratším dosahu.

Tyto protokoly byly vybrány na základě požadovaných vlastností a s ohledem na jejich cenovou a technologickou dostupnost.

6. Aplikace navržené metody na reinženýring procesu z případové studie

Cílem této kapitoly je popsat aplikaci navržené metody na reinženýring procesu zajištění pohybu oprávněných osob ve firemních prostorách s využitím vícefaktorové autentizace, podporovaného zvolenými IoT technologiemi.

6.1 Etapa 1: Analýza stávajícího stavu

První etapa odpovídá dokumentaci výchozího stavu procesu. Jedná se o přístup osoby do firemního objektu s využitím vstupních dveří a klíče. Jako první krok této etapy je **zpracování tabulkového vyjádření procesu**. To se skládá z dílčích kroků, které jsou níže uvedeny v tabulce 2 a zde je také uveden slovní popis:

1. **Identifikace činností procesu** – byly identifikovány tyto tři činnosti:
 - *Příchod osoby ke vstupním dveřím* – vstupem této činnosti je kontakt se dveřmi a výstupem vložení klíče do zámku.
 - *Odemčení dveří klíčem* – vstup je zde vložený klíč v zámku a výstup odemčené dveře.
 - *Průchod dveřmi* – odemčené dveře jsou vstupem a výstupem je překročení perimetru firemního objektu osobou.

Činnost	Vstup	Výstup	Popis
Příchod osoby ke vstupním dveřím	Kontakt se dveřmi (trigger, spouštěč procesu)	Vložení klíče do zámku	
Osoba odemyká klíčem	Vložení klíče do zámku	Odemčené dveře	
Osoba prochází dveřmi	Odemčené dveře	Překročení perimetru objektu	Jakákoli osoba s klíčem pronikne do objektu

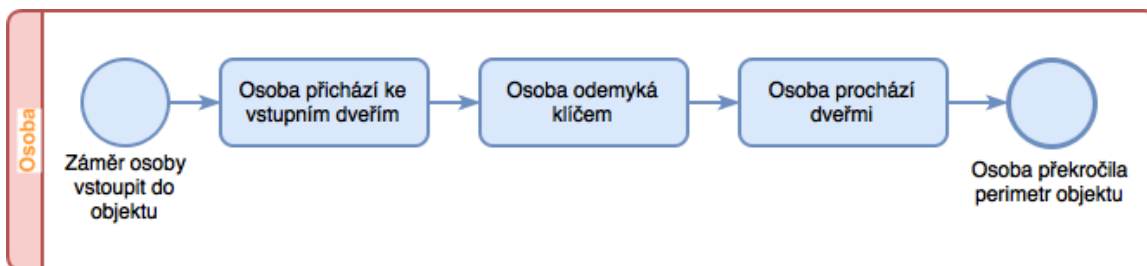
Tabulka 2 – tabulkové vyjádření procesu

2. **Identifikace rozhodování na procesu a podmínek pro rozhodování** – výchozí stav procesu neobsahuje žádné rozhodování a rozhodovací podmínky.
3. **Analýza návaznosti činností na procesu** – u výchozího stavu procesu je patrné, že je nejprve nutné přijít ke dveřím, poté odemknout klíčem a následně projít dveřmi.

Druhý krok – **zpracování procesního diagramu**, se skládá z následujících tří dílčích kroků:

- 1) **Identifikace bazénů a plaveckých drah** – bazény a plavecké dráhy obvykle kopírují aktéry na procesu. Je zřejmé, že zde figuruje pouze osoba se záměrem vstoupení do dveří, tudíž zde bude pouze jeden bazén o jedné plavecké dráze.

- 2) **Řazení činností a rozhodování do průběhu procesu s kreslením procesního diagramu** – díky nízkému počtu činností a nulového rozhodování je nakreslení diagramu výchozího stavu triviální. Výsledek je na obrázku 18. Osoba nejprve přichází ke vstupním dveřím, následně dveře odemýká a nakonec vchází dovnitř.



Obrázek 18: Výchozí proces (as-is)

- 3) **Přezkoumání navrženého procesu jako celku** – proces je jednoznačný a neobsahuje žádnou nepřehlednou pasáž. Není zde větvení ani čekání na nějakou událost. Z uvedeného popisu procesu vyplývá, že jeho současný stav má bezpečnostní riziko spojené se vstupem neoprávněné osoby do objektu. Kdokoli s klíčem od budovy může vstoupit dovnitř a není o tomto vstupu žádný záznam. Logickým motivem na zlepšení procesu je zvýšení jistoty, že osoby vstupující do firemního objektu mají oprávnění ke vstupu.

6.2 Etapa 2: Analýza příležitostí IoT k reinženýringu procesu

V této etapě je klíčové najít nová aktiva, která budou umožněna Internetem věcí. Ta vychází z analýzy příležitostí, která je součástí této etapy.

Identifikace současných aktiv procesu

Ve stávajícím stavu (výchozí proces) není nic sledováno. Osoba pouze vejde do dveří bez jakékoli identifikace nebo záznamu o tomto vstupu. Z pohledu reinženýringu je to výhodné, protože proces nabízí spoustu prostoru pro vylepšení. Za jediné aktivum stávajícího stavu procesu by se dalo považovat *odemčení dveří zámekem* osobou, která se autentizuje klíčem.

Analýza příležitostí ke zlepšení procesu

Jako první zjevná příležitost se jeví **automatické umožnění vstupu** osobě (odemknutí dveří), která bude ověřena jako povolená. Kvůli zvýšení bezpečnosti bude nutné zavést dvoufaktorovou autentizaci. Zde se naskýtá více možností, jak tuto autentizaci provést. V současnosti jsou na trhu různé „chytré“ zámky, které umožňují odemknutí dveří pomocí mobilního telefonu. Jelikož u sebe každý zaměstnanec nosí firemní mobilní telefon, ten může sloužit jako první z faktorů pro autentizaci.

Další příležitost ke zlepšení stávajícího stavu procesu se naskýtá jako **automatický záznam příchodu** zaměstnance. Jestliže zámek umožní komunikaci s vnitřní sítí domu (např. Technologií Z-Wave), bude možné při každém odemknutí dveří poslat signál na server, který záznam uloží do databáze.

Jako **druhý faktor autentizace** je možné použít nějakou z biometrických metod ověření osoby. Může jít například o otisk prstu nebo rozpoznání obličeje kamerou u vstupu. Dle mého názoru má kamera větší potenciál do budoucna, protože zaprvé osoby rozpoznává bez

jejich aktivní účasti (naproti tomu u otisku prstu musí osoba aktivně přiložit prst na čtečku) a zadruhé je možné do budoucna vylepšit úroveň rozpoznání zlepšením algoritmů, které zpracovávají obraz z kamery (např. rozpoznání na základě chůze osoby). Kamera může také vyhodnocovat, zda se před objektem neděje něco neobvyklého a v případě, že se bude někdo pokoušet o vniknutí do objektu, může být udělán záznam se snímkem dané osoby.

V případě, že bude i vstupní prostor objektu pokryt kamerami, bude možné automaticky identifikovat i odchody zaměstnanců. Alternativní řešení, které je v současnosti více dostupné, je umístit do vstupní chodby tablet, na kterém poběží aplikace spojená s IoT Manažerem. Ta bude zobrazovat karty jednotlivých zaměstnanců a v případě, že někdo opouští objekt, označí svou kartu na tabletu a systém udělá o této události záznam do databáze. Stejně tak může mít tablet využití v případě, kdy s jednou povolenou osobou přijde více lidí (např. host nebo další povolené osoby). Na základě první povolené osoby se dveře odemknou a následně se na tabletu označí další příchozí osoby a tím se provede záznam o jejich příchodu.

Jako další příležitost se jeví **připojení automobilu** zaměstnance do systému. Společnost T-Mobile v současné době nabízí řešení „Chytré auto“, které poskytuje informace (GPS poloha, rychlost, stav nádrže atp.) o vozidle skrze GSM síť. V případě, že zaměstnanec přijede autem a zaparkuje na firemním parkovišti, systém může považovat tuto skutečnost jako jeden z faktorů autentizace. Může nastat situace, kdy zaměstnanec nebude mít k dispozici auto (např. bude v servisu) a také bude mít vybitý mobil. V takovém případě nelze splnit podmínku dvoufaktorové autentizace a zámek by se neměl nikdy odemknout. Lze jej ale nouzově odemknout klíčem a i o této události zámek posílá informace, takže je možné navrhnout různá opatření, jak se má systém zachovat v případě odemknutí klíčem.

Návrh nových IoT aktiv procesu

Z předchozích částí analýzy příležitostí jsou patrné některé nové a užitečné informace, o které stojí v rámci zlepšení procesu usilovat. Především jde o následující:

- Ověření konkrétní osoby, která se chystá vstoupit do objektu.
- Informace o vstupu konkrétní osoby do objektu.
- Informace o nepovoleném pokusu o přístup.
- Informace o vstupu dalších osob do objektu.

Aktivum *vstup ověřené osoby do objektu* přináší mnohé možnosti budoucího využití. Jestliže řídicí software uvnitř domu ví, kdo je uvnitř, může podle toho provádět různé akce. Například regulovat teplotu v konkrétní kanceláři nebo přizpůsobit pracovní místo zaměstnanci, který zrovna přišel (zapnout oblíbenou hudbu, nastavit osvětlení atd.). Podobné příležitosti se naskýtají při odchodu zaměstnance. Jestliže je známa informace, že zaměstnanec opouští kancelář, vše nepotřebné se vypne a jestli je osoba poslední osobou v objektu, tak se zapne zabezpečení objektu či se provedou jiné akce.

Analýza náhrady stávajících aktiv za IoT aktiva

Vzhledem k tomu, že na stávajícím stavu procesu bylo identifikováno jediné triviální aktivum *odemčení dveří zámekem* s tím, že jeho stav není mimo okamžik otevření dveří dále využíván, je možné uvažovat pouze přidání aktiv nových. Nová IoT aktiva stávající aktivum nahrazují a přinášejí další užitečné informace, na jejichž základě lze automatizovat spoustu činností na procesu. A také je dosaženo vyšší úrovně bezpečnosti.

6.3 Etapa 3: Návrh reinženýringu procesu s umožněním IoT aktiv

Když jsou známa IoT aktiva, tedy to, co se bude na procesu sledovat a řídit, je třeba zpracovat nové tabulkové vyjádření a procesní diagram. Oproti tabulce z první etapy je tato tabulka rozšířená o IoT aktiva, IoT věci a IoT aktivity. IoT aktiva byla identifikována v předchozí etapě a IoT věci a aktivity z těchto aktiv vycházejí. Jednotlivá zařízení, která jsou pro nový proces k dispozici, byla popsána v kapitole 5.2 *Zvolené IoT technologie*.

Zpracování tabulkového vyjádření procesu

Tabulka je kvůli své obsáhlosti uvedena jako příloha A. Jsou v ní napsány činnosti s příslušnými vstupy a výstupy, dále jsou připsány IoT aktivity a IoT věci, které tyto aktivity vykonávají a také IoT aktiva, která jsou sledována. V tabulce je také znázorněno větvení činností a rozhodovací podmínky. Následuje slovní popis tabulky dle jednotlivých kroků.

- 1) **Identifikace činností procesu a IoT prvků** – seznam činností se nyní rozšiřuje o činnosti, které vykonávají IoT věci a IoT Manažer. Činnosti jsou tedy následující:
 - *Příchod/příjezd osoby k objektu.*
 - *Rozpoznání konkrétní osoby ze seznamu povolených osob (tzv. whitelistu) – rozpoznání se děje na základě dvou faktorů, které jsou porovnány s vnitřní databází povolených a nepovolených osob IoT Manažera. Jako faktory slouží:*
 - nasnímání obličeje kamerou a jeho následné rozpoznání,
 - mobilní telefon (připojení přes Bluetooth k zámku),
 - automobil příslušného zaměstnance (zastavení na parkovišti firmy).
 - *Porovnání dvou faktorů na shodu – dva autentizační faktory musí být porovnány, jestli ověřily stejnou osobu.*
 - *Záznam do databáze – v případě úspěšného i neúspěšného vstupu do objektu je vytvořen záznam do databáze o tomto vstupu (popř. pokusu o vstup). Záznam vstupu by měl být proveden pro všechny vstupující osoby (v případě, že jich vstupuje více najednou) na základě označení osob na tabletu za vstupními dveřmi. Automatické rozpoznání se současnými technologickými prvky není zcela možné.*
 - *Odemčení dveří – IoT věc zámek na základě signálu z IoT Manažera odemkne dveře.*
 - *Vstup osoby.*
 - *Zobrazení uvítání – na tabletu za vstupními dveřmi se zobrazí uvítání pro konkrétního zaměstnance a jiné, pro něj důležité, údaje.*
 - *Volba dalších osob – po úspěšném vstupu povolené osoby tato osoba označí na tabletu za vstupními dveřmi ostatní příchozí osoby.*
- 2) **Identifikace rozhodování na procesu a podmínek pro rozhodování** – na procesu byla identifikována následující rozhodování:
 - *Shodují se oba faktory autentizace? – jestliže dva faktory ověří stejnou osobu, dochází k postupu na další činnost procesu. V opačném případě je přístup odepřen a do databáze je udělán záznam o této skutečnosti.*
 - *Je automobil v blízkosti firemního objektu? – cloudová služba musí implementovat funkcionalitu geofence, díky které je možné určit, zda automobil vjel do předem*

vytyčené oblasti.

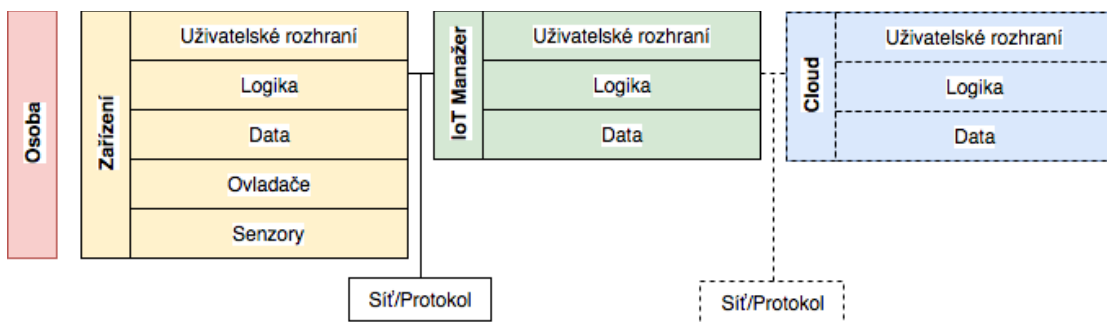
- *Je autentizace na zámku úspěšná?* – zámek sám provádí autentizaci a v případě neúspěchu se tento faktor považuje za negativní a musí být použity ostatní dva faktory.
- *Přichází více osob?* – v případě, že do objektu vstupuje více než pouze jedna (rozpoznaná) osoba, musí být ostatní osoby také identifikovány. Současné technologie toto spolehlivě neumožňují a tak je třeba zadat příchod osob ručně.

3) **Analýza návaznosti činností na procesu** – z výše uvedeného popisu činností je návaznost z velké části zřetelná. Osoba se musí první přiblížit k objektu, následně je provedena autentizace a poté je povolen či odepřen přístup se zaznamenáním této události do databáze.

Zpracování procesního diagramu

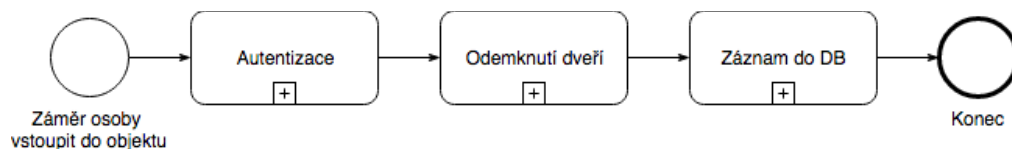
Dalším krokem je zpracování procesního diagramu. To je opět popsáno v jednotlivých krocích metody.

1) **Identifikace bazénů a plaveckých drah** – nejprve je nutné najít jednotlivé aktéry procesu. Jako zjevný aktér se jeví osoba, která chce vstoupit do objektu. Vedle osoby zde budou



Obrázek 19: Návrh bazénů s plaveckými dráhami

také figurovat IoT zařízení a IoT Manažer s případným napojením na nějaké cloudové služby. Každý z těchto aktérů bude mít svůj bazén a některé bazény budou dále rozděleny na plavecké dráhy. Rozdělení je vidět na obrázku 19. Osoba není dále nijak dělena. Zařízení může mít až 5 plaveckých drah podle typu tohoto zařízení. Například uvažovaný „chytrý“ zámek má senzory v podobě příjmu Bluetooth signálu z mobilního

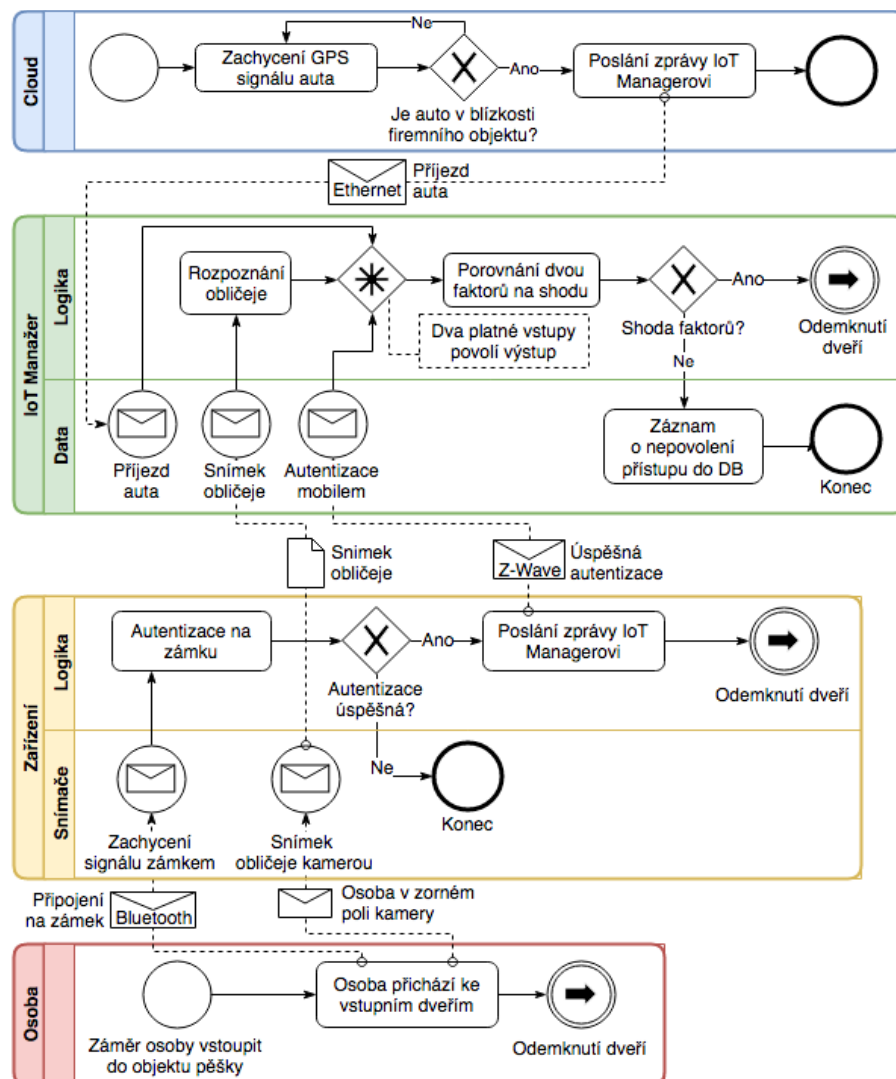


Obrázek 20: Celkový diagram procesu složený z jednotlivých subprocessů

telefonu, ovladačem je mechanický motůrek, který otáčí západkou zámku a dále má zámek vlastní logiku s datovým úložištěm pro provádění autentizace jednotlivých uživatelů. IoT Manažer má také více drah. Jako vhodné rozdělení se jeví na data, logiku

a uživatelské rozhraní. Posledním bazénem je cloud, kterým je v případě tohoto procesu služba, které zprostředkovává informace o automobilech zaměstnanců. Má stejné plavecké dráhy jako IoT Manažer a je možné připojení více takových cloudových služeb.

- 2) **Řazení činností a rozhodování do průběhu procesu s kreslením procesního diagramu** – nyní je třeba uspořádat činnosti do příslušných plaveckých drah s využitím rozhodovacích bran, komunikace mezi bazény a dalších BPMN prvků. Jak bylo popsáno v kapitole 4.2.3 *Etapa 3: Návrh reinženýringu procesu s umožněním IoT aktiv*, je vhodné proces rozdělit do několika subprocesů a nakreslit celkový diagram se subprocesy, které se dále rozkreslí v samostatných diagramech. Z praktického hlediska je ale výhodnější jako první vytvořit celkový diagram s detailně rozkreslenými procesy a ten následně rozsekat na dílčí subprocesy. Na obrázku 20 je diagram, který znázorňuje celý proces v podobě jednotlivých subprocesů, které budou dále detailně zpracovány. Jako první musí proběhnout autentizace, následně odemknutí dveří a nakonec záznam do databáze.

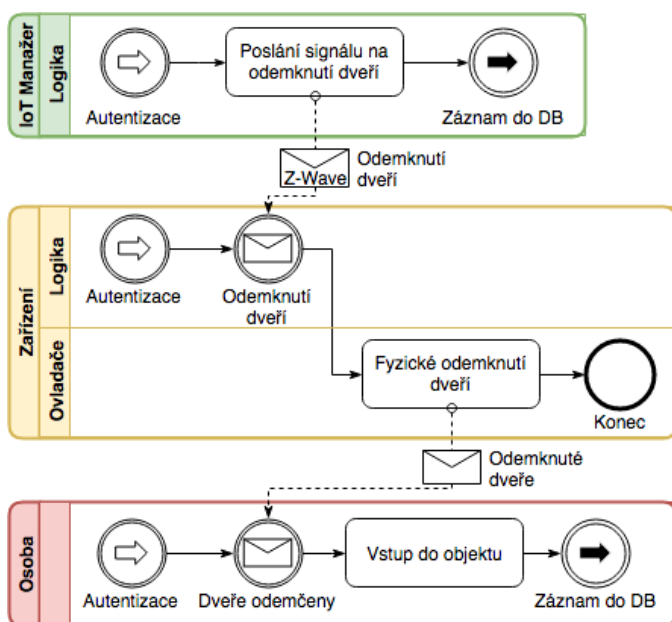


Obrázek 21: Subproces autentizace

Nyní budou popsány jednotlivé subprocesy. Na obrázku 21 je zobrazen subproces

autentizace. Proces začíná záměrem osoby vstoupit do objektu. Aby byla autentizace úspěšná, je zapotřebí, aby alespoň dva faktory rozpoznaly tutéž osobu. Přiblížení osoby k zámku na dosah Bluetooth způsobí připojení na tento zámek s následnou autentizací uživatele. Jestliže je autentizace úspěšná, pošle zámek zprávu IoT Manažerovi (skrze Z-Wave), který čeká ještě na další faktor. Tím může být informace o příjezdu konkrétního automobilu nebo rozpoznání obličeje před vstupními dveřmi. V případě, že alespoň faktory identifikují stejnou osobu, pokračuje se na další subproces – *odemknutí dveří*. V opačném případě je proveden záznam do databáze o tomto pokusu o přístup a proces a v procesu není povoleno pokračovat a je ukončen.

Obrázek 22 znázorňuje další navazující subproces – *odemčení dveří*. Osoba čeká na

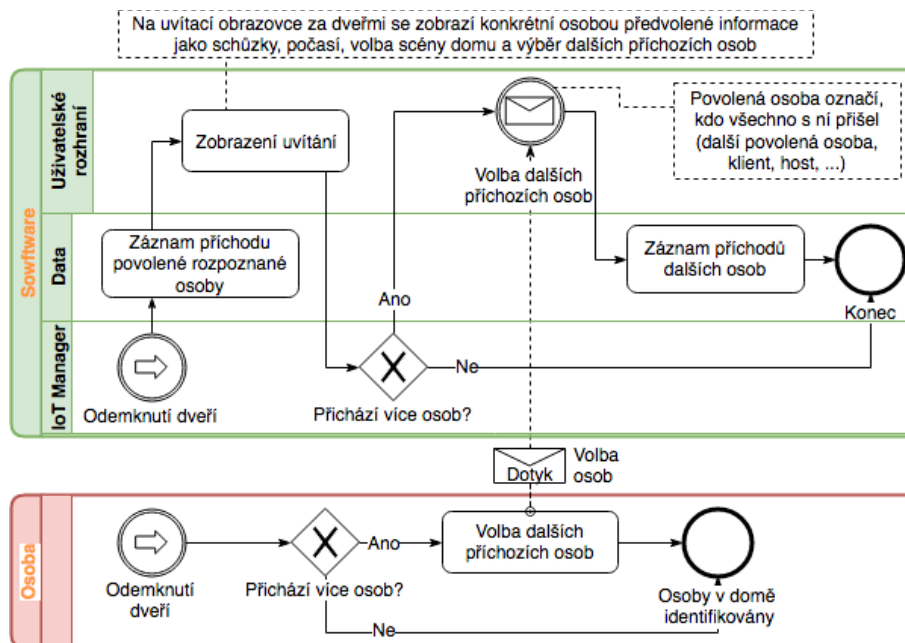


Obrázek 22: Subproces odemčení dveří

odemčení dveří, vstupuje do objektu a přechází na další část *záznam do databáze*. IoT Manažer posílá zprávu zámku, aby dveře odemkl a pokračuje na další subproces. Zámek po obdržení zprávy *odemčení dveří* dveře odemyká a pro něj činnost na procesu tímto končí.

Další navazující subproces je *záznam do databáze* a je zobrazený na obrázku 23. Jako první je automaticky zaznamenán příchod rozpoznané osoby a je zobrazeno uvítání na obrazovce tabletu za vstupními dveřmi. V případě, že rozpoznaná osoba vstupuje sama, proces je u konce. V opačném případě ještě osoba zvolí, které další povolené osoby (popřípadě klient, host, atd.) přicházejí, tedy v tomto případě musí být oprávnění vstupu dalších osob provedeno rozpoznanou (autentizovanou) osobou.

- 3) **Přezkoumání navrženého procesu jako celku** – v tomto kroku druhé etapy došlo k největším změnám na vytvořeném diagramu. Na základě přezkoumávání celého procesu došlo k mnoha úpravám. Tvorba diagramu probíhala iterativně v několika cyklech. Z výše uvedeného popisu diagramů tento postup není vidět, protože uvádím pouze výsledný stav a nikoli všechny předešlé iterační verze, které k tomuto stavu vedly.



Obrázek 23: Subproces záznam do databáze

6.4 Etapa 4: Konfigurace IoT Manažera a nastavení řídicích pravidel

V první řadě je třeba přidat jednotlivá zařízení do systému. Jedná se o tato zařízení:

- zámek Danalock V3,
- připojení automobilu skrze platformu „Chytré auto“ od T-Mobile,
- kamera Vivotek.

Přidání zařízení se docílí vytvořením záznamů v konfigurační databázi s příslušnými údaji o zařízeních.

Dále je nutné identifikovat řídicí pravidla typu IF THEN pro automatizovaný běh procesu. Musí zahrnovat všechny činnosti IoT Manažera identifikované v předešlé etapě.

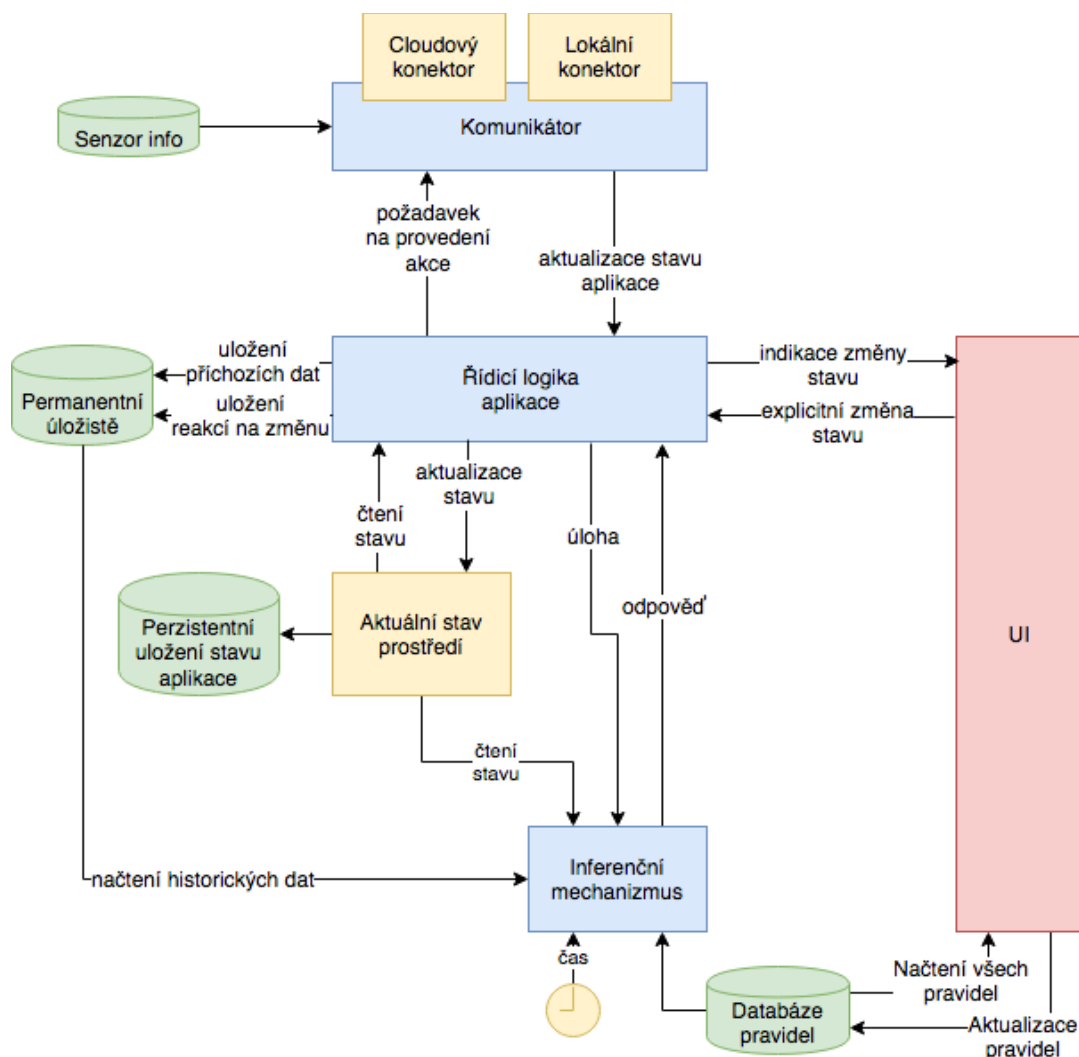
- **IF** automobil na firemním parkovišti **THEN** příslušná osoba faktor autentizace 1.
- **IF** autentizace na zámku v pořádku **THEN** příslušná osoba faktor autentizace 2.
- **IF** kamera rozpozná obličej **THEN** příslušná osoba faktor autentizace 3.
- **IF** alespoň dva faktory u stejné osoby **THEN** odemknout dveře.
- **IF** odemčeny dveře **THEN** zobrazit uvítání osoby.

6.5 Návrh řešení IoT Manažera

IoT Manažer je program, který zpracovává příchozí data z IoT zařízení a reaguje na podněty ze senzorů těchto zařízení pomocí zavedených pravidel. Program byl navržen jako modulární a vícevláknový systém. Vysokourovnová architektura softwaru je vidět na obrázku 24. Následující popis objasňuje účel jednotlivých modulů a komunikaci mezi nimi.

Konektor Zajišťuje vstupně-výstupní operace s čidly a ovladači. Každý typ čidla má svůj konektor a k jednomu konektoru může být připojeno více čidel stejného typu. Jsou rozlišovány dva základní typy konektorů a to *cloudové*, které se připojují na vzdálené

služby třetích stran a *lokální*, které komunikují s čidly napřímo. Cloudové se dále dělí na REST konektory a WebSocket konektory. Každý konektor běží ve svém vlákně, aby svými vstupně-výstupními operacemi nebrzdil ostatní moduly programu.



Obrázek 24: Architektura IoT Manažera

Komunikátor Modul *komunikátor* zastřešuje jednotlivé *konektory* a unifikuje přijatá data na společnou datovou strukturu, která je na obrázku 25. Společná datová struktura obsahuje identifikátor senzoru, identifikátor konektoru, typ, popis, čas přijetí dat a data samotná, které se liší u každého typu senzoru. Od *řídící logiky* přijímá požadavky na provedení akcí, které přeposílá na příslušný *konektor*. *Komunikátor* posílá řídicí logice přijatá data z *konektorů*.

Senzor info Jedná se o konfigurační databázi čidel na jejímž základě je vytvořen *komunikátor* s *konektory*.

Řídící logika aplikace Tento modul zajišťuje celkový běh aplikace a datové toky mezi moduly. *Komunikátoru* posílá požadavky na provedení akcí a přijímá unifikovaná data z čidel, která ukládá do databáze. Dále také čte a aktualizuje *aktuální stav prostředí*, informuje *inferenční mechanismus* o změnách stavu prostřednictvím jednotlivých úloh a přijímá

odpovědi na tyto úlohy. S modulem *UI* (uživatelské rozhraní) si vyměňují změny stavu.

Permanentní úložiště Úložiště historických dat ze sensorů a provedených akcí.

Aktuální stav Slouží k reprezentaci aktuálního stavu sensorů, ovladačů a dalších objektů (např. osoby).

```
SensorData = {
  'id': 'a234-b792',
  'connectorId': 'conn01',
  'type': 'MojjoConnector',
  'description': 't-mobile chytře auto',
  'timestamp': '17-05-2017 23:59',
  'data': {
    'arrived': 'True',
    'location': 'Brno'
  }
}
```

Obrázek 25: Společná struktura přichozích dat

Perzistentní uložení stavu Průběžně aktualizovaná kopie stavu aplikace v databázi.

Inferenční mechanismus Přijímá úlohy s nově změněnými daty od řídicí logiky a na základě pravidel, která jsou uložena v *databázi pravidel* odvozuje reakce na změnu stavu. Má přístup k *aktuálnímu stavu prostředí* a k historickým datům z *permanentního úložiště*. Reakce na změnu stavu může odvodit i na základě uplynutí času.

Databáze pravidel Úložiště pravidel.

UI Uživatelské rozhraní slouží k zobrazování aktuálního stavu systému, který lze v některých případech i měnit. Dále slouží k nastavování řídicích pravidel.

6.5.1 Implementace

Program byl realizován v programovacím jazyce Python3 s využitím OOP (objektově orientovaného programování). Každý modul je tvořen vlastním objektem a moduly *řídicí logika*, *inferenční mechanismus*, *komunikátor* a *konektory* běží ve vlastních vláknech. Toho bylo docíleno použitím knihovny *threading* a také bylo zapotřebí využít synchronizačních zámků. Komunikace mezi jednotlivými objekty je zajištěna pomocí FIFO front, kdy každý datový tok má svoji frontu. Moduly, které čtou data z více vstupů (*řídicí logika* a *komunikátor*) využívají volání *select* pro přepínání těchto vstupů. Inferenční mechanismus se spouští na základě nově přijatých dat (buď ze senzoru, nebo na základě použitého pravidla, které mění aktuální stav) a prochází pravidla týkající se pouze nových dat. Program běží na počítači Raspberry Pi s operačním systémem Raspbian Jessie.

7. Vyhodnocení zkušeností z aplikace metody na případové studii

Aplikací navržené metody jsem získal nové zkušenosti z oblastí:

- reinženýring procesů,
- fungování technologií IoT a
- programové řízení procesu.

Následně pokračuji podrobným popisem těchto zkušeností.

7.1 Zkušenosti z aplikace navržené metody pro reinženýring procesů

Navržená metoda pro reinženýring procesů se v praxi osvědčila a ukázala jako dobře využitelná. Její klíčovou charakteristikou je orientace na účelnost využitých IoT technologií, tedy všechna IoT zařízení mají své místo na novém procesu a nejsou pořizována bez znalosti jejich konkrétního využití. Metoda přímo k orientaci na účelnost pořízení IoT technologií vede svými kroky.

Prvním předpokladem pro úspěšné navržení metody bylo porozumění notaci BPMN pro znázorňování procesů. S touto notací se mi pracovalo velice dobře, ovšem počáteční pochopení dělbý procesu do jednotlivých bazénů a komunikace mezi nimi nebylo úplně jednoznačné. S každým bazénem vzniká nový dílčí proces a komunikace mezi těmito procesy musí být realizována jako zasílání zpráv.

Jednotlivé etapy metody a jejich kroky jsem volil co možná nejvíce jednoznačně, abych tím předešel zbytečnému nedorozumění a především obrázkové znázornění etap bylo nápomocné k orientaci v krocích metody.

Před samotným kreslením procesu je výhodné sepsat tabulku, která slouží jako dobrý start k utřídění myšlenek o navrhovaném procesu. Ke konci zpracování procesu je výhodné opětovně se vrátit k tabulce a doplnit ji o různé detaily, které se do BPMN diagramu nevezou nebo jej doplňují.

Rozdělení procesu na jednotlivé bazény podle architektury výsledného systému napomohlo k jasné představě o komunikaci mezi všemi prvky. Vnitřní rozdělení bazénů na plavecké dráhy již není tak důležité, ale zvyšuje přehlednost diagramů na úkor jejich velikosti.

Dále je třeba zmínit, že většina IoT zařízení je teprve v technologických začátcích a analýza příležitostí může vést ke v současnosti nereálným představám, jak uvádím v následující kapitole.

7.2 Zkušenosti z fungování IoT technologií

IoT technologie jsou v současnosti velkým trendem a většina výrobců elektroniky se snaží dělat „chytrá“ zařízení. Většinou jde o uzavřené systémy, kdy je zařízení připojeno nějakou bezdrátovou technologií (nejčastěji Wi-Fi, Bluetooth, Sigfox) či jejich kombinací na server konkrétní společnosti, kde jsou data dále zpracována a poskytnuta koncovému uživateli skrze

mobilní nebo webovou aplikaci. Také je dobrým zvykem, že pro vývojáře je dostupné rozhraní (REST API), díky kterému je možné získat data v přímé (surové) podobě. Záleží ovšem na konkrétním výrobci, jak toto rozhraní zpracuje a jestli k němu vytvoří podpůrné vývojářské nástroje (SDK) a technickou dokumentaci. Konkrétní SDK je spjaté zpravidla jen s jedním programovacím jazykem a tudíž jsou kladeny další nároky na výrobce, aby pokryl co možná největší spektrum vývojových prostředí. Používání takových zařízení se stává vysoce nespolehlivým, protože není zaručeno, že nedojde k neohlášeným změnám ze strany výrobce a celková důvěra v taková zařízení je nízká, protože závisí na rozhodnutí třetích stran.

Dále není seriózně vyřešena otázka bezpečnosti, zejména jak se chovat v případě, pokud někdo odcizí zařízení a začne posílat data jeho jménem. Řídicí software typu IoT Manažer proto bude muset být schopen reagovat na situace, kdy dojde k poruše přísunu dat z IoT zařízení. Bezpečnost IoT je samostatnou oblastí, kterou je třeba v budoucnu řešit v součinnosti s výrobcí jednotlivých zařízení zavedením schopnosti identifikace situace spojené s neoprávněným odcizením zařízení.

Pro realizaci procesu jsem použil dvou cloudově připojených zařízení. Prvním je malá krabička zapojená do ODB portu automobilu, kterou zastřešuje služba „Chytré auto“ od společnosti T-Mobile. Druhé zařízení je multifunkční senzor Sens‘it, který komunikuje po nově vybudované mezinárodní síti Sigfox (LPWAN). Chytrý zámek Danalock V3, který jako jediný splňuje požadavky na nároky procesu, bude dle výrobce dostupný až v červnu tohoto roku a tudíž musel být pro účely ověření navržené metody implementace IoT dočasně nahrazen jiným způsobem. Pro autentizaci využívám notificačního signálu zařízení Sens‘it, které je popsáno níže a samotné otevření dveří zatím simulují softwarově. Třetí z autentizačních faktorů – rozpoznání obličeje kamerou – je zatím také pouze simulováno z důvodu nedostupnosti spolehlivého software pro rozpoznání obličeje.

V rámci práce jsem vyzkoušel ještě další zařízení:

- BeeeOn brána + Z-Wave adaptér
- Fibaro Door Sensor

Následuje podrobnější popis jednotlivých zařízení a zkušenosti s nimi.

7.2.1 Chytré auto

Chytré auto je služba kterou v České republice poskytuje mobilní operátor T-Mobile, ale ve skutečnosti se jedná o zařízení firmy Mojio (obrázek 26), které posílá data na cloud také této firmy. Díky dostupnosti otevřeného API je možné se k datům o automobilu dostat buď skrze REST API nebo pomocí otevřeného WebSocket spojení, kdy jsou data při změnách posílána v reálném čase. Výrobce slibuje zasílání notifikací v případě příjezdu automobilu na předem určené místo, ovšem reálně tato služba nefunguje. Kontaktoval jsem autory platformy Mojio, kteří mi sdělili, že si musím aktuální polohu kontrolovat sám. Do IoT Manažera jsem proto naprogramoval *konektor*, který přijímá polohu z jedoucího automobilu a počítá, zda se nachází v předem vymezené oblasti.



Obrázek 26: Zařízení Mojio

7.2.2 Multisenzor Sens'it

Sens'it je malé kapesní zařízení (zobrazené na obrázku 26), které obsahuje 5 senzorů měřící:

- teplotu,
- vlhkost,
- pohyb (3osý akcelerometr),
- magnet (magnetometr),
- světlo.



Obrázek 27: Zařízení Sens'it

Dále je možné na základě stisku tlačítka poslat notifikační signál. Zařízení je připojené na síť Sigfox a umožňuje poslat až 8 12bytových zpráv za hodinu. V procesu jsem ho využil jako jeden z faktorů autentizace a to tak, že místo připojení mobilního telefonu na zámek posílám notifikační signál z tohoto zařízení. Po stisku tlačítka dojdou data do IoT Manažera do 2-4 sekund, což je dáno vlastnostmi sítě Sigfox.

7.2.3 Z-Wave brána

Některá lokální zařízení (např. zámek Danalock V3) komunikují prostřednictvím protokolu Z-Wave a proto jsem pořídil BeeeOn¹⁹ bránu (obrázek 28) a k ní Z-Wave adaptér. Z-Wave



Obrázek 28: BeeeOn brána

protokol byl bohužel začleněn do podporovaných protokolů bránou až v době odevzdání této práce a tak jsem ji nestačil plně využít. Jakmile bude brána správně nastavena, použiji ji jako centrální bod pro komunikaci s lokálními senzory a ovladači. Ve stejném období byla pořízena i komerční brána Vera Plus (obrázek 29), která kromě Z-Wave podporuje i Zig-Bee a Bluetooth a která rozšíří portfolio připojitelných IoT zařízení. Výhodou brány BeeeOn je, že se na ní dají spustit další doprovodné skripty, což komerční brána neumožňuje.



Obrázek 29: Brána Vera Plus

Jako další zařízení jsem vyzkoušel Fibaro Door Sensor, který komunikuje také protokolem Z-Wave a umožňuje poslání signálu při sepnutí obvodu. Sepnutí může být realizováno na základě oddálení magnetu nebo na základě dvou připojených vodičů. Připojil jsem spínač zvonku k tomuto zařízení a slouží tedy jako tlačítko, které může spouštět více věcí, než jen zvukový signál. Zvonek není součástí navrženého procesu a proto se jím dále nezabývám.

7.3 Zkušenosti z řízení procesu IoT Manažerem

Tato kapitola začíná popisem řízení konkrétního procesu IoT Manažerem a následně jsou shrnuty dosažené zkušenosti. Na obrázku 30 je výpis z běhu programu. Znak na začátku

¹⁹ Projekt, který vznikl na půdě Fakulty informačních technologií, VUT.

každého řádku značí modul, který je za konkrétní výpis zodpovědný. Legenda je následující:

- pomlčka „—“ značí komunikátor;
- dvě pomlčky „—“ značí konektor;
- dolar „\$“ značí řídicí logiku;
- mřížka „#“ značí inferenční mechanismus.

Po spuštění je provedena inicializace konektorů a program čeká na vstupní data ze senzorů. Jako první přichází data o příjezdu automobilu na firemní parkoviště. K těm je přidán identifikátor konektoru, na který data přišla a časová značka. Takto zabalená data jsou poslána do řídicí jednoty, která je zabalí jako úlohu (přidán identifikátor a stav úlohy) pro inferenční mechanismus. Na základě vytvoření této úlohy 1 je spuštěn inferenční mechanismus a ten prochází jednotlivá pravidla, která jsou spjatá s novými daty, která přišla v rámci úlohy. V tomto případě se aplikuje pravidlo, které říká, že se má nastavit první faktor autentizace a inferenční mechanismus pošle v rámci odpovědi na úlohu akci „nastavení faktoru“.

```
- Found new connector [conn01]: MojioConnector (moj.io car location)
- Found new connector [conn02]: Sensit (SigFox testing sensor)
- Found new connector [conn04]: Danalock (simulated door lock)
— Connector data: {'id': 'mojio01', 'car': 'Dev Simulator', 'timestamp': '2017-05-08 17:58:51', 'arrived': True}
- Communicator: {'id': 'mojio01', 'car': 'Dev Simulator', 'timestamp': '2017-05-08 17:58:51', 'arrived': True, 'conn
$ Manager: Sensor data: {'id': 'mojio01', 'connectorId': 'conn01', 'timestamp': '2017-05-08 17:58:51', 'data': {'id'
# Automation: Job 1 - STARTED, changed entity: mojio01
# processing rule 1
# RULE 1 used - car auth factor
$ Manager: Control data: {'jobId': 1, 'action': 'update', 'id': 'person01', 'data': {'authCar': True}}
$ Manager: Sensor data: {'jobId': 1, 'action': 'update', 'id': 'person01', 'data': {'authCar': True}}
$ Manager: Control data: {'jobId': 1, 'action': 'done', 'entity': <model.entity.Mojio object at 0x10345b6a0>}
$ updating... arrived: True
# Automation: Job 2 - STARTED, changed entity: person01
# processing rule 4
$ Manager: Control data: {'jobId': 2, 'action': 'done', 'entity': <model.entity.Human object at 0x10345bb38>}
$ updating... authCar: True
— Connector data: {'id': 'sensit01', 'alert': True, 'temperature': 23}
- Communicator: {'id': 'sensit01', 'alert': True, 'temperature': 23, 'connector': 'conn02'}
$ Manager: Sensor data: {'id': 'sensit01', 'connectorId': 'conn02', 'timestamp': '2017-05-08 17:58:57', 'data': {'ic
# Automation: Job 3 - STARTED, changed entity: sensit01
# processing rule 2
# RULE 2 used - mobile auth factor
$ Manager: Control data: {'jobId': 3, 'action': 'update', 'id': 'person01', 'data': {'authMobile': True}}
$ Manager: Sensor data: {'jobId': 3, 'action': 'update', 'id': 'person01', 'data': {'authMobile': True}}
$ Manager: Control data: {'jobId': 3, 'action': 'done', 'entity': <model.entity.Sensit object at 0x10345b3c8>}
$ updating... temperature: 23
$ updating... alert: True
# Automation: Job 4 - STARTED, changed entity: person01
# processing rule 4
# RULE 2 used - unlocking doors
$ Manager: Control data: {'jobId': 4, 'action': 'do', 'id': 'danalock01', 'data': {'status': 'unlocked', 'person': '
$ Manager: Sensor data: {'jobId': 4, 'action': 'do', 'id': 'danalock01', 'data': {'status': 'unlocked', 'person': 'p
- Communicator: {'jobId': 4, 'action': 'do', 'id': 'danalock01', 'data': {'status': 'unlocked', 'person': 'person01'
— Connector action: {'jobId': 4, 'action': 'do', 'id': 'danalock01', 'data': {'status': 'unlocked', 'person': 'pers
$ Manager: Control data: {'jobId': 4, 'action': 'done', 'entity': <model.entity.Human object at 0x10345b240>}
$ updating... authMobile: True
# Automation: Job 5 - STARTED, changed entity: danalock01
$ Manager: Control data: {'jobId': 5, 'action': 'done', 'entity': <model.entity.Danalock object at 0x10345bcf8>}
$ updating... status: unlocked
$ updating... person: person01
```

Obrázek 30: Výpis z běhu IoT Manažera

Obecně je posláno tolik odpovědí, kolik akcí je třeba provést a před ukončením úlohy se pošle poslední odpověď, která zajistí aktualizaci stavu prostředí. Zde se pošlou dvě odpovědi – nastavení faktoru a aktualizace stavu. Řídicí logika přijímá první odpověď, která říká, že má být u osoby nastaven první faktor autentizace. Jedná se o změnu stavu prostředí a proto

vytváří novou úlohu 2 pro inferenční mechanismus, která má za úkol odpovědět, jestli tato změna spustí nějaké další akce. Následně řídicí logika přijímá druhou odpověď a aktualizuje stav automobilu, který přijel. Nově vytvořená úloha 2 nezpůsobí žádné změny a je pouze poslána koncová odpověď pro aktualizaci stavu. Řídicí logika aktualizaci provede.

Dále na konektor přichází data ze zařízení Sens'it, která informují o stisku notifikačního tlačítka. Data jsou stejným způsobem jako předtím zabalena a přeposlána inferenčnímu mechanismu jako nová úloha 3. Aplikuje se pravidlo nastavení druhého faktoru obdobně jako u prvního faktoru a v rámci úlohy 4 je splněna podmínka dvou platných faktorů autentizace a je poslána odpověď s akcí „odemknutí dveří“. Řídicí logika akci přepoše komunikátoru, který ji dále přepoše správnému konektoru. Vytvoří se ještě úloha 5, která zjišťuje, zde se má stát ještě něco v důsledku odemknutí dveří. Žádné takové pravidlo není nalezeno a je odeslána pouze koncová odpověď pro aktualizaci stavu.

Kvůli dočasné nedostupnosti klíčového IoT zařízení pro realizaci procesu (Danalock V3) jsem byl nucen proces simulovat a není ještě reálně nasazen. Už teď je ale jasné, že klíčovou vlastností řídicího softwaru je vypořádání se s heterogenitou prostředí. Výkonnostní nároky na inferenční mechanismus porostou s množstvím připojených zařízení a používaných pravidel.

8. Závěr

Závěrečná kapitola bakalářské práce Využití možností IoT pro reinženýring podnikových procesů shrnuje dosažení cílů stanovených v kapitole 1. Nejdříve je vyhodnoceno dosažení šesti postupových cílů práce, které jsou předpokladem pro navazující vyhodnocení splnění hlavního cíle bakalářské práce. Na závěr kapitoly jsou uvedena doporučení pro další rozvoj řešené oblasti vycházející z dosažených výsledků.

8.1 Splnění cílů práce

Všechny dílčí cíle práce byly dosaženy a výsledky jsou popsány v níže uvedených bodech:

1. Seznámit se s problematikou BPR a možnostmi prostředí IoT – výsledky uvedeny v kapitole 2. *Reinženýring procesů a nové možnosti prostředí IoT.*
2. Prostudovat existující přístupy při návrhu procesů v prostředí IoT – výsledky uvedeny v kapitole 3. *Existující přístupy při návrhu procesů v prostředí IoT.*
3. Definovat metodu návrhu a implementace IoT řešení procesním způsobem – výsledky uvedeny v kapitole 4. *Návrh metody pro zavedení IoT řešení procesním způsobem.*
4. Vybrat vhodnou případovou studii pro ověření navržené metody zavedení IoT procesním způsobem, tj. zvolit vhodný proces a vhodné IoT technologie pro jeho reinženýring. Vytvořit či doplnit nezbytnou dokumentaci výchozího stavu procesu a zvolených IoT technologií – vybraná případová studie je uvedena v kapitole 5. *Volba případové studie pro ověření metody v praxi* a dokumentace výchozího stavu je uvedena na začátku kapitoly 6. *Aplikace navržené metody na reinženýring procesu z případové studie.*
5. Aplikovat navrženou metodu na reinženýring procesu podporovaného zvolenými IoT technologiemi – výsledky uvedeny v kapitole 6. *Aplikace navržené metody na reinženýring procesu z případové studie.*
6. Vyhodnotit zkušenosti a výsledky získané z provedené případové studie a diskutovat další rozvoj navržené metody – výsledky uvedeny v kapitole 7. *Vyhodnocení zkušeností z aplikace metody na případové studii.*

Hlavním cílem práce bylo navrhnout metodu implementace IoT řešení procesním způsobem a metodu ověřit na případové studii. Pro dosažení hlavního cíle práce bylo třeba splnit všechny postupové cíle práce a výsledky případové studie prokázat využitelnost navržené metody. Navržená metoda implementace IoT řešení procesním způsobem byla ověřena na procesu zajištění pohybu oprávněných osob ve firemních prostorech s využitím více-faktorové autentizace. Výsledky získané z provedené případové studie prokazují reálnou využitelnost navržené metody v konkrétních podmínkách firemní praxe společnosti Per Partes Consulting, s.r.o., kde pracuji jako vývojář IoT, ve které byla metoda testována a úspěšně ověřena.

8.2 Doporučení dalšího rozvoje

Jsem přesvědčen, že navržená a ověřená metoda implementace IoT procesním způsobem zdůvodňuje účelnost pořízení moderních IoT zařízení a jejich využitelnost v podnikové praxi. Otevřenou otázkou zůstává zkoumání u kterých podnikových procesů bude reinženýring pomocí IoT zařízení nejvíce přínosný. Navazující úsilí by proto mohlo směřovat do hledání vhodných procesů pro aplikaci navržené metody.

V průběhu zpracování bakalářské práce jsem došel ke zjištění, že reinženýring podnikových procesů s využitím IoT zařízení musí být doprovázen vývojem řídicího softwaru. V práci jsem jej nazval IoT Manažer. Navrhl jsem jeho architekturu a programové zpracování, které mi umožnilo úspěšně ověřit navrženou metodu v rámci bakalářské práce. IoT Manažer je navržen jako modulární systém, zpracovává příchozí data z IoT zařízení v samostatných vláknech a reaguje na podněty ze senzorů těchto zařízení pomocí zavedených pravidel. Rád bych se v diplomové práci zabýval implementací pravidlové logiky a návrhem většího množství pravidel (stovky) pro rozsáhlou aplikaci IoT Manažera při reinženýringu složitějších procesů.

Trendy vývoje IoT mluví o tom, že budeme obklopeni velkým množstvím IoT zařízení, která budou zasílat do řídicího softwaru typu IoT Manažer velké množství vstupních dat a to bude klást další nároky na výkonnost řídicího softwaru. Jak jsem zjistil a zpracovával na případové studii, některá data vstupují přímo z lokálně připojených zařízení, jiná jsou však získávána výhradně prostřednictvím cloudů výrobců těchto zařízení přes internet. Řídicí software se tak bude muset vypořádat i s heterogenitou prostředí a s problémy bezpečnosti a důvěryhodnosti obdržených dat. Další oblastí, kterou bude proto potřeba se zabývat, je nové pojetí bezpečnosti při masivním využívání IoT zařízení.

Literatura

- [1] FERRETTI, M., F. SCHIAVONE. Internet of things and business processes redesign in seaports: The case of Hamburg. *Business Process Management Journal*, 2016, 22(2), 271–284.
- [2] International Telecommunication Union. Internet Reports 2005: The Internet of Things – Executive Summary [online]. 2015 [cit. 2016-12-5]. Dostupné z: https://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf
- [3] Institute of Electrical and Electronics Engineers (IEEE). Towards a definition of the Internet of Things [online]. 2015 [cit. 2016-12-7]. Dostupné z: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
- [4] DAVENPORT, T., J. SHORT. The New Industrial Engineering: Information Technology And Business Process Redesign, *Sloan Management Review*, 1990, 31(4), 11.
- [5] MANSAR, S., H. REIJERS. Best practices in business process redesign: use and impact. *Business Process Management Journal*, 2007, 13(2), 193–213.
- [6] HAMMER, M., J. CHAMPY. Reengineering - radikální proměna firmy: manifest revoluce v podnikání. 3. vyd. Praha: Management Press, 2000. s. 38.
- [7] PALL, Gabriel A. *Quality process management*. Englewood Cliffs, N.J.: Prentice-Hall, c1987. ISBN 9780137450275.
- [8] EFTEKHARI, A., P. AKHAVAN. Developing a Comprehensive Methodology for BPR Projects by Employing IT Tools, *Business Process Management Journal*, 2013, 19(1), 4–29.
- [9] Object Management Group, Inc. Business Process Model and Notation (BPMN) [online]. 2011-01-03 [cit. 2017-1-14]. Dostupné z: <http://www.omg.org/spec/BPMN/2.0/>
- [10] IoT Analytics. IoT basics: Getting started with the Internet of Things [online]. 2015 [cit. 2017-3-7]. Dostupné z: <https://iot-analytics.com/product/whitepaper-iot-basics-getting-started-with-the-internet-of-things/>
- [11] LinkLabs, Inc. A Comprehensive Look at Low Power, Wide Area Networks [online]. 2016 [cit. 2017-3-7]. Dostupné z: <https://www.link-labs.com/lpwan>
- [12] IoT Analytics. IoT platforms: The central backbone for the Internet of Things [online]. 2015 [cit. 2017-3-8]. Dostupné z: <https://iot-analytics.com/product/iot-platforms-whitepaper/>
- [13] MEYER, S., A. RUPPEN, C. MAGERKURTH. Internet of Things-aware Process Modeling: Integrating IoT Devices as Business Process Resources [online]. 2013 [cit. 2017-3-9]. Dostupné z: <https://diuf.unifr.ch/drupal/softeng/sites/diuf.unifr.ch.drupal.softeng/files/file/caise.pdf>

Přílohy

Seznam příloh

- A Tabulkové vyjádření procesu
- B Obsah přiloženého paměťového média
- C Seznam obrázků

A Tabulkové vyjádření procesu

Činnost	Vstup (podmínka před)	Výstup (podmínka po)	Popis	IoT věc	IoT aktivum	IoT aktivita (činnost)
Příchod/příjezd osoby k objektu.	Kontakt se dveřmi (trigger, spouštěč procesu) (kamera vidí osobu)	Identifikace osoby, přiřazení statusu „povolená“ nebo „nepovolená“. V případě povolení identifikace jména. U nepovolené jméno „Anonym“.	Kontaktem se rozumí přiblížení 30 cm ke vstupním dveřím a natočením obličeje do zorného úhlu kamery.	Kamera Software pro rozpoznání obličeje	Identifikace osoby	Software rozpozná konkrétní osobu z whitelistu nebo uloží novou osobu „Anonym“ – blacklist.
	Mobil osoby je v dosahu Bluetooth	Dtto výše (z jiného vstupu)	Mobil slouží k jednoznačné identifikaci osoby	Mobil (Bluetooth zařízení), Zámek	Identifikace osoby	Software rozpozná konkrétní osobu z whitelistu.
	Automobil osoby je na firemním parkovišti	Dtto výše (z jiného vstupu)	Poloha automobilu slouží jako jeden z faktorů autentizace	Automobil	Identifikace osoby	Software rozpozná konkrétní osobu z whitelistu.
	Identifikace osoby pomocí dvou faktorů	Shoda faktorů → konkrétní povolená osoba Neshoda → nepovolená osoba „Anonym“	IoT systém porovná výstupy dvou faktorů na shodu	řídící software (IoT Manažer)	Identifikace osoby	Porovnání identifikací z předchozích dvou kroků na shodu
Neshoda – pokus o přístup nepovolenou osobou						
	Neshoda porovnání dvou faktorů autentizace	Záznam pokusu o přístup nepovolenou osobou (ID „Anonym“, datum a čas, vstupní dveře)		IoT Manažer, Zámek	Nepovolený pokus o přístup	Záznam do DB
Shoda – povolená osoba						
	Shoda porovnání dvou faktorů autentizace	Záznam příchodu povolené rozpoznané osoby (ID osoby, datum a čas, vstupní dveře)		IoT Manažer, Zámek	Vstup osoby do objektu	Záznam do DB, Odemknutí (otevření) dveří
Průchod dveřmi	Osoba je povolena	Uvítací oznámení na obrazovce (= IoT Manažer – uživatelské rozhraní)	Uvítací oznámení na obrazovce zveřejní jméno vstupující osoby. A nabídne volbu dalších přichozích osob a volby scény chování domu.	IoT Manažer, Zámek		Uvítací oznámení, Rozsvícení vstup. světla, deaktivace zastřežení, a další...
Volba dalších přichozích osob	S povolenou osobou přišlo více lidí	Záznam příchodu dalších povolených osob (ID osoby, datum a čas, vstupní dveře), či jiných osob	Povolená osoba označí, kdo všechno s ní přišel (další povolené osoby, klient, host, ...)	IoT Manažer (uživatelské rozhraní)	Vstup dalších osob do objektu	Záznam do DB

B Obsah přiloženého paměťového média

<code>bakalarska-prace.pdf</code>	Bakalářská práce ve formátu PDF
<code>bakalarska-prace.odt</code>	Zdrojový soubor bakalářské práce (Libre Office)
<code>source/</code>	Zdrojové soubory aplikace IoT Manažer

C Seznam obrázků

Obrázek 1: Cyklus BPR 2.....	8
Obrázek 2: Rekurzivní vztah mezi informačními technologiemi a BPR [4].....	9
Obrázek 3: Nová dimenze „věc“ [2].....	10
Obrázek 4: Odhad vývoje IoT podle IDC 4.....	11
Obrázek 5: Segmentace IoT trhu [9].....	13
Obrázek 6: Osm základních částí IoT platformy [12].....	16
Obrázek 7: Diagram procesu podle IoT Analytics [12].....	17
Obrázek 8: Znázornění činnosti, která je spojená s IoT zařízením [12].....	18
Obrázek 9: Znázornění procesu společností Oracle 15.....	19
Obrázek 10: Rozhraní nástroje Node-RED 16.....	20
Obrázek 11: Znázornění procesu svozu odpadu 18.....	21
Obrázek 12: Etapy navržené metody.....	24
Obrázek 13: Kroky první etapy – analýza stávajícího stavu procesu.....	25
Obrázek 14: Kroky druhé etapy – analýza příležitostí IoT.....	26
Obrázek 15: Kroky třetí etapy – návrh reinženýringu procesu.....	27
Obrázek 16: Role IoT Manažera.....	29
Obrázek 17: Zvolené IoT technologie.....	30
Obrázek 18: Výchozí proces (as-is).....	33
Obrázek 19: Návrh bazénů s plaveckými dráhami.....	36
Obrázek 20: Celkový diagram procesu složený z jednotlivých subprocesů.....	36
Obrázek 21: Subproces autentizace.....	37
Obrázek 22: Subproces odemčení dveří.....	38
Obrázek 23: Subproces zápisu do databáze.....	39
Obrázek 24: Architektura IoT Manažera.....	40
Obrázek 25: Společná struktura příchozích dat.....	41
Obrázek 26: Zařízení Mojio.....	44
Obrázek 27: Zařízení Sens'it.....	44
Obrázek 28: BeeeOn brána.....	45
Obrázek 29: Brána Vera Plus.....	45
Obrázek 30: Výpis z běhu IoT Manažera.....	46