VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

DOPAD BEZPEČNOSTI IIOT NA PROAKTIVNÍ ÚDRŽBU FIREMNÍCH AKTIV

IMPACT OF IIOT SECURITY ON PROACTIVE MAINTENANCE OF COMPANY'S ASSETS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MAXIM CHOMYŠYN
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR SEDLÁK
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Maxim Chomyšyn**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Dopad bezpečnosti IIoT na proaktivní údržbu firemních aktiv

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem diplomové práce je provést průzkum využívaných IIoT zařízení v průmyslových výrobních procesech a na základě výsledku této analýzy vyhodnotit možné finanční a provozní dopady v případě narušení jejich bezpečnosti v kyberprostoru. Ze zjištěných faktů budou následně doporučeny kroky a změny, které zmenší šanci vzniku bezpečnostního incidentu.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2014.

P. DOUCEK, L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato práce zkoumá možná bezpečnostní rizika spojené s provozem IIoT technologií v průmyslové výrobě. Obsahem tohoto dokumentu je analýza používaných IIoT technologií, jejich účel a metoda implementace do výrobních procesů a samotné technologické strategie firmy. Výsledek této analýzy poslouží pro vytvoření možných scénářů rizik a dopadů s nimi spojenými. Na závěr doporučím možné změny, které tyto rizika buď zcela odstraní, nebo je alespoň minimalizují.

Abstract

This work examines possible safety risks associated with the operation of IIoT technologies in industrial production. The content of this document is an analysis of used IIoT technologies, their purpose and method of implementation into production processes and the company's technology strategy. The outcome of this analysis will serve to develop possible risk scenarios and their associated impacts. Finally, I recommend possible changes that either eliminate these risks completely or at least minimize them.

Klíčová slova

kybernetická bezpečnost, IIoT, proaktivní údržba, komunikační IIoT protokoly, technologická strategie

Key words

cybersecurity, IIoT, proactive maintenance, IIoT communication protocols, technology strategy

Bibliografická citace

CHOMYŠYN, Maxim. *Dopad bezpečnosti IIoT na proaktivní údržbu firemních aktiv*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2020. 81 s. Vedoucí bakalářské práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31.05.2020

_____

podpis studenta

Poděkování

Nesmírně děkuji za ochotu, věnovaný čas a odborné rady inženýra Petra Sedláka, který mi věnoval v době vedení mé bakalářské práce. Taktéž chci poděkovat společnosti ŠKODA AUTO a.s. zato, že mi umožnila nahlédnout dovnitř firmy a přímo ze zdroje čerpat informace, které slouží jako podklad pro vypracování této práce. V poslední řadě poděkování patři i mé rodině a kamarádům, kteří mě v této době podporovali a nadále podporují.

OBSAH

ÚVOD

Slavný vědec Gordon Moore jednou prohlásil, že každé dva roky se celkový výpočetní výkon zdvojnásobí. Od roku 1975 zhruba do roku 2018 to byla pravda, ale nyní už sledujeme, jak se trend zpomaluje a my narážíme na hranice výpočetní kapacity silikonu. V takovém stádiu se začíná s masovou digitalizací každodenních věcí, které jsou všude okolo nás. Jako příklad lze uvést hodinky, brýle, auta, ledničky, světla a spoustu jiných věcí u nichž bychom nikdy nečekali, že někdy budou schopni komunikovat s okolním světem. Obecný pojem pro takové věci je Internet of Things (IoT). Už jen obyčejná chytrá LED žárovka má víc výpočetního výkonu než první počítač ENIAC, který vážil 30 tun a zabíral 167 m^2 plochy.

S rostoucí popularitou všudypřítomné digitalizace a tzv. „smart" věcí, se začíná nabývat na významnosti zabezpečení digitálních aktiv. Doposud krádeže, podvody a jiné přestupky či trestné činy byly prováděny zejména v reálném světe. Když někdo chtěl peníze, vyhlídl si potenciální oběť a té ukradl peněženku. Nyní se tyto aktivity překlápí do zcela jiné roviny. Poměr druhů zločinů se již dávno překlopil ve prospěch digitální sféry. Teď se cílí na osobní informace jedinců a jejich přístupy přímo do bankovních systémů. Oběť je pak okradená a ani neví, že se něco takového stalo.

Problémem je, že výrobci nových smart zařízení kolikrát natolik spěchají s vypuštěním svého produktu na trh, že zvolí funkčnost nad bezpečností. Takové věci jsou pak skoro jako tikající bomby jen čekající na signál od správného detonátoru.

Internet věcí se začíná dostávat do všech segmentů, nejen do spotřebitelského. Oblast průmyslu zažívá přechod to tzv. éry Průmyslu 4.0, během níž se výroba razantně modernizuje za pomocí nových digitalizačních technologií. Mezi ně patří i rozsáhlé nasazování internetu věcí pro sběr dat, které jsou následně použity pro zefektivnění práce s aktivy a lepší řízení nákladů. V případě napadení spotřebitelských IoT zařízení hrozí únik osobních dat či ztráta peněz jedinců, ale v případě napadení průmyslových zařízení hrozí podniku opravdu velké finanční ztráty i úniky dat všech osob, které kdy s danou firmou jednali.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

V této kapitole popíšu hlavní cíl, který mě prováděl celým procesem vypracovávání této závěrečné práce. Na něj je navazuji popisem vedlejších cílů a metod, jimiž jsem sbíral potřebné informace pro vypracování této práce.

Hlavní cíle

Hlavním cílem je zhodnotit aktuální stav kybernetické bezpečnosti pro oblast IoT zařízení internetu věcí (IoT) ve společnosti ŠKODA AUTO a.s. a také to, jaký vliv můžou mít nedostatky ochrany těchto technologií na procesy v nichž figurují.

Bezpečnost IoT je hodně podceňována, kdy i pouhý zranitelný monitorovací snímač může vést ke škodám, které nemusí být zřejmé v krátkém časovém měřítku. Proto ze zjištěných poznatků provedu analýzu rizik, které následně ohodnotím a popíšu možné dopady.

Vedlejší cíle

S analýzou rizik souvisí uvedení scénářů, které mohou nastat v případě, že se riziko vyplní. Z tohoto důvodu mým vedlejším cílem jen namodelovat, co by se mohlo stát, pokud se neoprávněně zmanipulují výstupy tzv. Industriálních IoT (IIoT) systémů či snímačů. Mezi to patří odhad možného pozastavení výroby linky a také propočet spojených finanční nákladů. Namodelováním ukázkového případu lze si zajistit podklady proto, aby si společnost vyčlenila dostatečný rozpočet pro zavedení efektivních protiopatření.

Postup vypracování práce

Tato práce je rozdělená do tří tematických celků. V úvodní části popisuji všechny teoretické podklady pro řízení informační bezpečnosti. Průmyslové odvětví se řídí mnohem striktnějšími pravidly pro provoz počítačové sítě i samotných strojů. Liší se taky komunikačními protokoly, které jsou speciálně vytvořené pro řízení výrobních strojů a sběr dat. Nejprve je potřeba popsat jaká je definice IIoT zařízení, pro která zařízení je takové označení validní, jak mezi sebou komunikují a jak je národní organizace

doporučují spravovat. Tyto informace slouží jako základ pro provedení analýzy v následující části

V druhé části představím společnost ŠKODA AUTO a.s., její strukturu a předmět podnikání. Z informací získaných přímo v této společnosti provedu zhodnocení zavedených praktik pro zabezpečení IIoT zařízení, která jsou používaná ve výrobních továrnách. V rámci toho vyjmenuji technologie, které jsou použity ve výrobě, a hlavně co je jejích účel. IIoT produkuje výstupy, které jsou potřebné ve výrobních a údržbových procesech.

V závěrečné části zhodnotím dosavadní stav řízení informační bezpečnosti, vyjmenuji silné a slabé stránky. Z těchto závěru sepíšu analýzu možných rizik, které mohou nastat. U každého z nich odhadnu pravděpodobnost a vážnost možných následků, které může sloužit jako ukázka toho, jaké dopady může mít zranitelná bezpečnost IIoT. Následně zvolím jedno riziko, u něhož názorně namodeluji přesnější finanční újmy.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části představím základní stavební kameny teorie, které jsou použity pro následnou analýzu již implementovaných technologií v společnosti. Teoretické informace nejprve uvádím od nejvíc obecných charakteristik až ke konkrétním vlastnostem a postupům řízení bezpečnosti IIoT.

1.1 Průmysl 4.0

Pro představení kontextu rostoucího významu IIoT nejprve představím koncept Industrie 4.0, který se významně ovlivňuje autoprůmysl. Jeho popisem chci ukázat, jak je IoT jeho nedílnou součástí a proč se považuje za jednoho z jeho čtyř základních pilířů.

V minulosti můžeme najít dvě příčiny, které vedly ke čtvrté průmyslové revoluci, která je stále v plném proudu po celém světě. První z nich bylo představení nových průmyslových řídících architektur, technologií a systémů na konci 90. let minulého století. Místo strojů, které byly doposud řízeny pomocí Programmable Logic Controllery (PLC) se objevily programovatelné automaty pod názvem Programmable Automation Controller (PAC) a industriální počítače (IPC). Tyto technologie umožnily upustit od striktně machine-to-machine (M2M) komunikace a napojit průmyslové stroje na širokou komunikační síť a databáze. Průmyslové stroje se nyní dokážou napojit na sdílené zdroje dat a manipulovat s nimi k tomu, aby se promítly do následného provozu (1, s. 67).

Druhá událost, která přispěla ke zrychlení zavádění nové filozofie je finanční krize v letech 2008 a 2009. Ačkoliv se jedná o krizi finanční, ne průmyslovou, různých průmyslových odvětví to postihlo v variabilních mírách. Podniky vyrábějící prvotní suroviny pro následovné zpracování byly mnohem méně postižené než ty, které přímo závisí na zájmu koncových kupujících. Mezi ně patří zejména autoprůmysl a výrobci spotřebitelské elektroniky. Díky tomu se tyto dvě oblasti začali usilovat o omezení outsorcingu do Asie a vrácení výroby co možná nejblíže k domácímu trhu (1, s. 67).

Samotný koncept Industrie 4.0 byl představen v roce 2011 zástupci z německých institucí jako strategie, která má podpořit konkurenceschopnost a samostatnost německého průmyslu (2).

Různé zdroje definují Průmysl 4.0 následovně:

„Koncept Industrie 4.0 byl navržen tak, aby splňoval požadavky na rychlost výroby, její automatizaci, ziskovost a efektivitu. Pro dosažení těchto požadavků využívá kyber-fyzické systémy (CPS), tedy systémy, které se skládají z různých objektů s vestavěným zpracováním dat a informací. Objekty mohou být polotovary (vybavené např. čipy RFID), samokonfigurovatelné podsestavy, zařízení nebo stroje.“ (1, s. 67)

„Industry 4.0 should not be approached as a closed system but rather should be considered as one essential part out of several key areas. In a smart, interconnected world based on the Internet of Things and Services the economic key sectors will be transformed into smart infrastructures and constellations.“ (3, s. 35)

“A paradigm shift towards digitalised, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT.” (4, s. 12)

1.1.1 Základy Průmyslu 4.0

Obě definice mají jedno společné. Industrie 4.0 buduje na čtyřech základních kamenech, které umožňují naplnění zamýšlené německé strategie:

Cyber-Physical Systems (CPS)

Tyto systémy mají za úkol propojit výrobní stroje s inteligentními řadiči. Cílem je dosáhnout synchronizace mezi výpočetními a fyzickými procesy. Konkrétněji lze mluvit o monitorování fyzických činností vestavěnými výpočetními jednotkami, v nichž dochází k neustálé kontrole vývoje výrobních činností. Při takovém sledování může výpočetní logika ovlivňovat průběh výroby a naopak (5). K propojení těchto dvou rovin systém používá zejména snímače, ovládače, logické výpočetní jednotky a komunikační zařízení.

Internet of Things

Internet věcí, v průmyslu taktéž známý jako IIoT, se počítá za prvotního spouštěče přechodu firem do Průmyslu 4.0. Porter a Heppelmann představili světu doposud nejpoužívanější, a také nejobecnější, definici internetu věcí:

„Smart, connected products offer exponentially expanding opportunities for new functionality, far greater reliability, much higher product utilization, and capabilities that cut across and transcend traditional product boundaries.“ (5)

Někteří autoři si představují budoucnost IoT jako společnost, kde všichni členové mají kdykoliv a kdekoliv přístup k internetu, v němž se nachází samo-řídící a samo-konfigurující se chytrá zařízení (5). Fleisch klade důraz na rozlišování IoT a obecného internetu. Dle něj je internet věcí naplněn malými až neviditelnými zařízeními, které mají malý výpočetní výkon a jsou energeticky nenáročné. Oproti tomu pod pojmem internet chápe propojení plnohodnotných osobních počítačů. V rámci průmyslu se IoT senzory a ovládače liší od dosavadních průmyslových senzorů a ovládačů tím, že IoT zařízení si mezi sebou vyměňují data pomocí počítačové sítě (6, s. 15).

Pojmy CPS a IoT mají velmi tenkou hranici, protože IoT lze chápat jako jistou podmnožinu CPS. Proto IoT lze definovat jako síť, ve které CPS komunikuji mezi sebou skrze unikátní adresovací schémata (7). Bližší definici IoT se budu zabývat v následující kapitole.

Internet of Services (IoS)

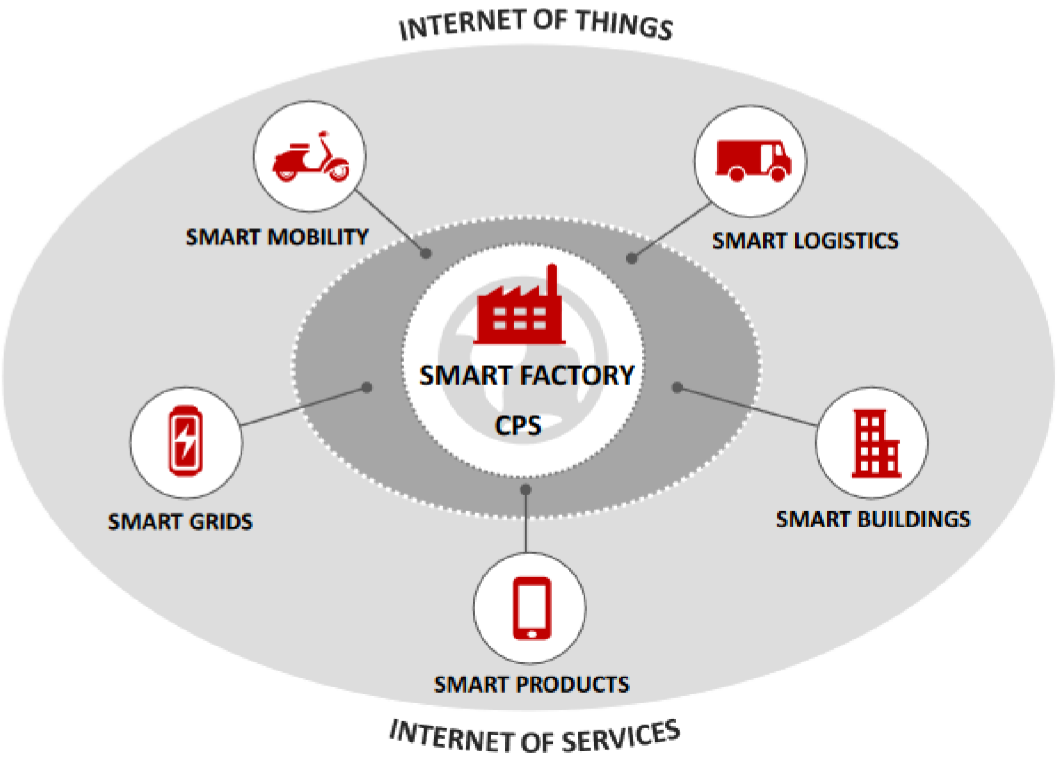
Princip internetu služeb spočívá v možnostech sdílení volných prostředků na internetu za účelem dosažení nového produktu s větší výslednou přídavnou hodnotou. Principy, jako jsou service-oriented architecture, Software as a Service a business process outsourcing, se dají považovat jako součást myšlenky IoS (3). Jako ukázku lze vzít nová mobilní a chytrá zařízení, u kterých se předpokládá, že budou komunikovat minimálně s internetem a v možném důsledku i mezi sebou. Díky tomu výrobci mohou navrhovat integrované služby, které jsou díky tomu uživatelsky přívětivější (7).

„A commercial transaction where one party grants temporary access to the resources of another party in order to perform a prescribed function and a related benefit. Resources may be human workforce and skills, technical systems, information, consumables, land and others. “ (8)

Smart Factory

Tento pilíř pojednává předchozí tři dohromady. Je třeba si uvědomit, že CPS komunikuje za pomocí IoT a IoS. Dle Kagermanna (2011) pokud to vše dáme dohromady získáme tím Smart Factory, která si zakládá na myšlence decentralizovaného produkčního systému, v němž lidi, stroje a prostředky mezi sebou přirozeně komunikují, jako kdyby byli v sociální síti.

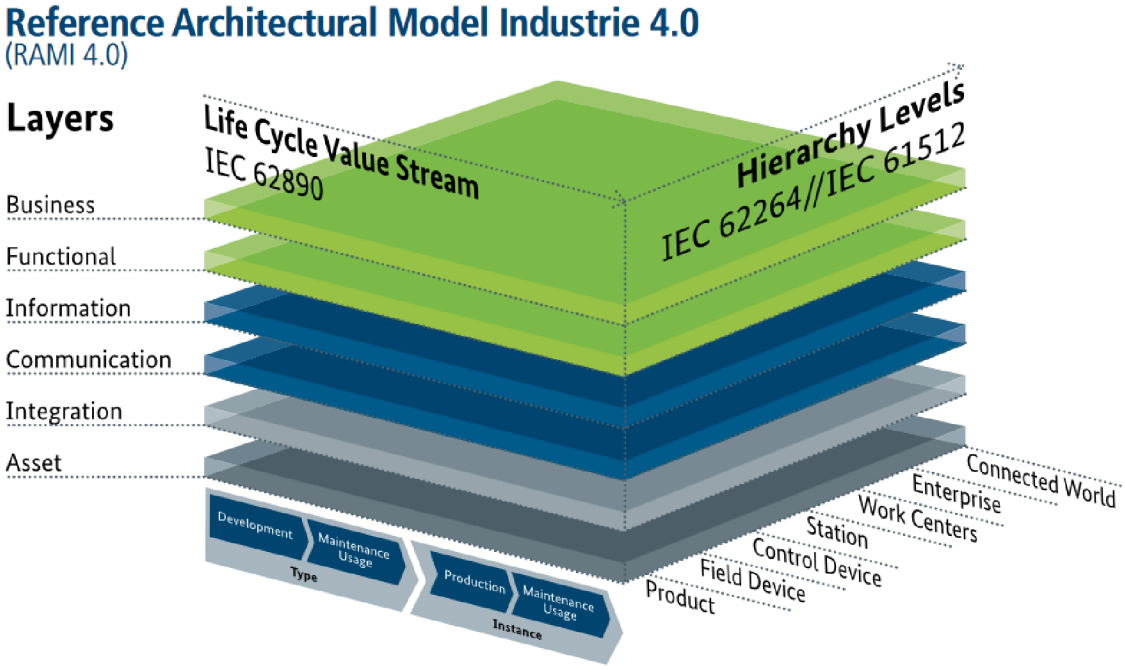
Smart Faktory má za cíl přinést větší automatizaci průmyslové práce, u niž hrozí zaměstnancům zvýšené riziko úrazu nebo která je fyzicky namáhavá a je třeba u ní zajistit vysokou úroveň preciznosti. Nad tímto konceptem jsou často vedené debaty. Na jedné straně větší robotizace některých úkonů zmenší nároky na pracovní kapacity, ale najdou se odpůrci, kteří namítají, že to může zajít do extrému a průmyslové stroje zaměstnance zcela nahradí (5).



Obr. 1: Schéma konceptů Průmyslu 4.0 (Převzato z (3, s. 35))

Dnes Průmysl 4.0 se začíná dostávat do čím dál tím většího počtu firem, proto německý svaz elektroinženýru přišli s doporučením pro produkty vyhovující konceptu Industrie 4.0. V rámci standardizační práce se vytvořil navrhl Referenční Model Architektury

Industrie 4.0 (RAMI 4.0). Tento tříosý model zahrnuje vrstvy architektury, životní cyklus a hodnotový řetězec v hierarchické úrovni. Jeho součásti je i popis toho, jak je výsledný produkt následně vestavěn do sítě Průmyslu 4.0 (9, s. 31).



Obr. 2: RAMI 4.0 model (Převzato z (1, s. 37))

S jeho pomocí firmy mohou rozložit celou problematiku na malé celky, které pak lze snadno přiřadit k modelu a zajistit jejich plnou kompatibilitu s celým konceptem. Vrstvy modelu ukazuji, jak nejvyšší vrstva podnikatelských procesů buduje na sehranosti nižších vrstev, v nichž je obsažená transformace dat pocházejících z fyzických snímačů do informací potřebných pro vykonání strategického rozhodnutí. Lícová osa krychle poukazuje na to, jak každá činnost musí mít pevně stanovený životní cyklus. Boční osa znázorňuje to, jak správné nasazení Průmyslu 4.0 prochází všemi úrovněmi hierarchie, od fyzického produktu po napojení na celosvětovou síť (10). Podrobnější model je znázorněn v Příloha 1.

Tento úvod do konceptu Průmyslu 4.0 slouží jako ukázka toho, jak jsou a budou moderní továrny ovlivněny digitalizací na neustálým propojováním zařízení do sítí. Z tohoto důvodu neustále roste význam kyberbezpečnosti, protože v této sféře se během kybernetického napadení nemusí obejít jen „virtuální“ škodou ale může dojít i k fyzické škodě.

1.2 Definice internetu věcí

V předchozí kapitole jsem představil jednu z definic IoT jako součást Průmyslu 4.0. Tato kapitola je věnována bližšímu představení této technologie a toho, jak operuje.

Definice IoT byla doposud nejednoznačná, neboť bylo těžké nastavit hranice toho, jak komplexní či velká musí být samotná „věc“, aby nebyla považována jako IoT zařízení. V posledních několika letech se toho ujaly národní agentury a organizace. Tyto instituce se snaží přijít s obecnou definici a souvisejícími doporučeními, které jednoznačně určí, co jsou IoT a jak se s nimi má zacházet.

Jednou z nich je Evropská agentura pro bezpečnost sítí a informací (ENISA), která teprve na konci roku 2017 stanovila výchozí definici IoT a jejich význam při použití v chytrých továrnách. Jejich definice zní následovně:

„ENISA defines the Internet of Things (IoT) as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making". Stemming from the definition is the fact that information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision-making, and actions." (11, s. 18)

Jinými slovy ENISA chápe IoT hlavně jako kolekce čidel a ovládači, které jsou specializovaná pouze na specifické účely. Oba druhy zařízení jsou zapojené do cyklu komunikace, během kterého dochází k neustálému vyhodnocování dat pro následné upravení chování ovládačů.

Americký Národní institut standardů a technologie (NIST) také přišel se svou definicí IoT a doporučených praktik zacházení. Podle nich je IoT rychle rozvíjející se a rozšiřující se sbírka různých technologií, které interagují s fyzickým světem. Zařízení IoT jsou výsledkem spojení informačních technologií (IT) a operačních technologií (OT). Mnoho IoT zařízení je výsledkem konvergence cloud computingu, mobilních zařízení, vestavěných systémů, Big Data, levného hardwaru a dalších technologických pokroků (12, s. iv).

Nejsrozumitelnější popis doposud poskytl Institut pro elektrotechnické a elektronické inženýrství (IEEE), který popisuje IoT jako systém obsahující sítě senzorů, ovládačů a

jiných chytrých zařízení jejichž účelem je propojení všech věcí mezi něž patří každodenní i průmyslové objekty takovým způsobem, který je činí sledovatelnými, programovatelnými a dává jim větší schopnost interakce s lidmi i mezi sebou (13, s. 1).

Přesně definovat IoT je velice složitý úkol, neboť je těžké jednoznačně vystihnout širokou škálu možností, která se s každým dnem nadále vyvíjí. Jediné společné vodítko mezi všemi definicemi je zmínka o senzorech a ovládačích, které na základě předdefinované logiky komunikují mezi sebou za pomocí připojení k počítačovým sítím.

Použití IoT zařízení není vázáno pouze na specifické případy a lze je nasadit jak do domácností, tak i do průmyslu. Mezi nejčastější použití IoT patří:

- **Regulace osvětlení**: řízení světelných zdrojů i stínicí techniky jako jsou rolety nebo žaluzie. Logika ovládání přitom může spoléhat na čidlech pohybu nebo také na tom, jaké je aktuální umístění slunce,
- **regulace ventilace**: za pomocí kontroly teploty, vlhkosti vzduchu a obsahu kouře či CO2 ve vzduchu, ovládače mohou regulovat jeho ohřev a (re)cirkulaci,
- **monitoring měřitelných veličin**: IoT snímače dokážou hlídat většinu fyzických veličin jako je vzdálenost, náklon, teplota, světlo, vlhkost, ampéry, odpor, aj.,
- **zabezpečení**: za předpokladu, že samotná IoT zařízení jsou dostatečně zabezpečená, lze použít kamery, pohybová čidla, spínací čidla aj. ke sledování stavu zabezpečení budovy a pozemku,
- **predikce události**: za pomocí naměřených dat a zapojení logiky sledující cyklické vzory lze odhadnout, že něco není v souladu s očekáváním dřív, než dojde k nežádanému stavu,
- **vzdálená kontrola**: díky napojení na internet lze na dálku ovládat a měnit logiku vyhodnocování všech výše zmíněných kategorií (14).

1.3 Definice pojmů

Dřív, než popíšu teoretická východiska související s informační bezpečností, je potřeba nejdříve rozebrat a popsat definice klíčových pojmů, které jsou podstatnou součástí analyzované problematiky.

1.3.1 Data

Data jsou vnímána jako základní stavební prvek všech znalostí, které získáváme ze zažitých zkušeností. Jsou produktem samotného sledování a samy o sobě nemají význam, dokud se mezi nimi nevytvoří vazby a nezformují informace (15, s. 13).

Dle profesorky Rowley mají data tyhle vlastnosti:

- Nemají význam ani hodnotu, protože jsou bez kontextu.
- Jedná se o neuspořádaný výsledek sledování neboli diskrétní objektivní fakta.
- Je to pouhý popis vlastností, objektů a událostí (16, s. 170).

Data jsou vhodná pro skládání do informací za předpokladu, že se zařadí do souvisejícího kontextu, z něhož informace vychází. Samotná data jsou vhodná pro komunikaci, vyhodnocování nebo zpracování (17, s. 12).

1.3.2 Informace

Informace je další stupeň v znalostní hierarchii a nachází se hned nad daty. Informace se skládají z dat a na rozdíl od nich už poskytují příjemci kontext a význam s hodnotou. Informace jsou často přizpůsobována do takové podoby, která je užitečná pro snazší rozhodování lidí. Vznik informací je vždy iniciován se specifickým účelem, aby informace byla relevantní pro očekáváné použití. Z tohoto důvodu jsou informace subjektivní vyjádření jedince, protože každý může ze stejné skupiny dat vytvořit jiné informace (15, s. 14).

1.3.3 Aktiva

Mezi aktiva patří všechen majetek firmy, je to cokoliv, co má pro organizaci nějakou hodnotu (18, s. 2). Pro potřeby této práce se však zaměřím pouze na aktiva spojené s informačními technologiemi.

„Jsou zdroje (HW, SW, služby a informace), které mají být chráněny pomocí bezpečnostních opatření.“ (17, s. 346)

Aktiva lze rozdělit na primární a podpůrná. Primární aktiva jsou informace a služby, které poskytuje nebo zpracovává informační systém. Mezi podpůrná se řadí všechny prostředky, které přichází do styku s primárními aktivy a zajišťují jejich zpracování a zabezpečení (19).

1.3.4 Informační/kybernetická bezpečnost

Informační bezpečnost je zajištění pravidel atributů popsaných níže, tedy důvěrnost, integritu a spolehlivost dat (20). Ačkoliv pojmy informatická a kybernetická bezpečnost jsou často zaměňované, jde o dva různé pojmy s odlišnými definicemi. Zatímco informatická bezpečnost popisuje kredibilitu samotných informací, kybernetická bezpečnost je souhrn právních, organizačních a vzdělávacích prostředků sloužících k zajištění ochrany kybernetického prostoru (17). Pro představu, bezpečnost odeslaného e-mailu je předmětem informační bezpečnosti, ale správa pravidel a technologií potřebných ke zpracování daného e-mailu je už předmětem kybernetické bezpečnosti.

1.3.5 Hrozba

„*Hrozbou potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu.*“ (19)

Hrozbou tedy rozumíme jakékoliv nežádoucí působení na aktiva, které může způsobit poškození, zneužití nebo nedostupnost aktiva. Hrozby se vztahují zejména na primární aktiva, neboť právě ony mají největší hodnotu. Všechna podpůrná aktiva jsou zaváděná k odvrácení hrozeb. Jsou to však často složité a nedokonalé systémy, které mají slabá místa tzv. zranitelnosti.

1.3.6 Zranitelnost

Zranitelností se rozumí slabé místo aktiva nebo samotného bezpečnostního opatření, které může být zneužito jednou a více hrozbami (19). Cílem systému řízení informační bezpečnosti je vyhledávat a odstraňovat tato slabá místa. Úroveň bezpečnosti informací je dána mírou úspěšností, se kterou jsou zranitelnosti napravovány.

1.3.7 Riziko

„Rizikem se rozumí možnost, že určitá hrozba využije zranitelnosti informačního systému a způsobí poškození aktiva.“ (19)

Riziko je spojení hrozby a zranitelnosti. Hrozba sama o sobě nemusí být nebezpečná, pokud neexistuje zranitelnost, kterou lze zneužít. Až v momentě, kdy se identifikuje hrozba a související zranitelnost, pak lze je tento stav označován jako riziko.

1.3.8 Vlastnosti IoT

Na rozdíl od plnohodnotných zařízení se IoT věci liší v několika zásadních aspektech. Nejdůležitějším faktem je, že ve většině případů je IoT věc tzv. „černá skříňka“. To znamená, že správce IoT nevidí, jak interní procesy dané věci fungují. Z pravidla se jedná o malé zařízení s nízkou energetickou spotřebou vykonávající pouze malé množství předem nadefinovaných operací. Oproti obyčejnému IT zařízení se IoT liší hlavně v:

- **Nedostatku možností pro správu**. U IoT nelze jednoduše spravovat nainstalovaný software či firmware. Zároveň se věc může sama rekonfigurovat dojde-li ke ztrátě napájení nebo připojení k síti.
- **Chybí uživatelská rozhraní**. IoT často neposkytuje uživateli přehledné rozhraní, ve kterém lze sledovat všechna interní nastavení a stavy zařízení. Výrobci nejsou jednotní ve struktuře vysílaných dat a paletě podporovaných příkazů.
- **Problémy při správě velkého množství zařízení.** V průmyslové aplikaci IoT se předpokládá s velkým množstvím IoT zařízení, které nemají standardizované mechanizmy pro centrální správu.
- **Různorodost softwaru.** Velké množství zařízení od různorodých výrobců se také promítá v rozmanitosti operačního softwaru i firmwaru.
- **Různé délky životnosti zařízení.** Výrobce může stanovit dobu životnosti svých zařízení. Pokud uživatel bude chtít toto zařízení používat déle, musí tak činit na své vlastní nebezpečí, protože zařízení již nebude podporováno ze strany výrobce. V průmyslu to může znamenat obzvlášť velké riziko, protože dané zařízení má přímý vliv na chování výrobního stroje.

- **Omezený servis**. IoT zařízení často nelze opravit, upravit či jinak interně zkontrolovat.
- **Krátké a časté datové zprávy**. IoT zařízení podle potřeby posílají zprávy s měřenými hodnotami. Tyto zprávy jsou často v řadech kilobajtů, ale zato se opakovaně posílají v řádech sekund. V průmyslu se tyto zprávy posílají téměř nepřetržitě, aby byl zajištěná real-time komunikace. Četné množství IoT věcí má za výsledek velkou zátěž na přenosnou síť (12, s. 8).

1.3.9 Protokoly IoT

Z důvodu své odlišnosti od ostatních IT zařízení, se začaly vytvářet speciálně optimalizované protokoly pro komunikaci mezi IoT věcmi. Zásadní vývoj zaznamenaly síťové a datové protokoly, v nichž začaly vznikat energeticky a datově nenáročné varianty protokolů.

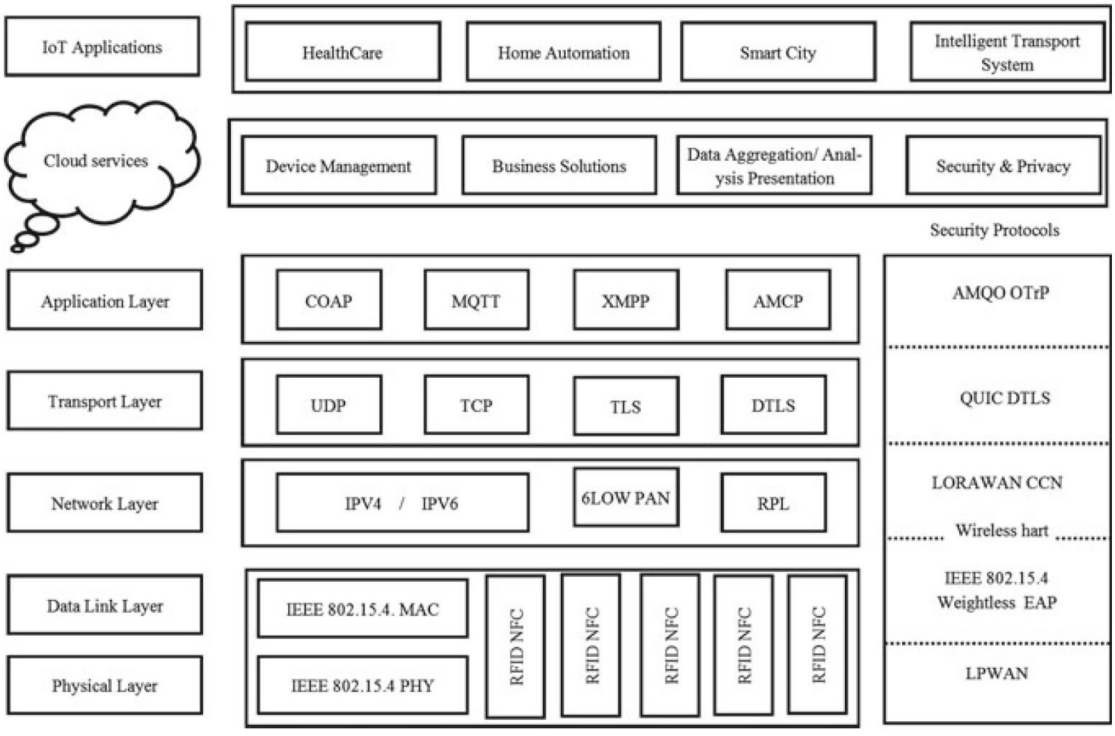
Z hlediska infrastruktury IoT dokáže využívat obecně přijaté IPv4/IPv6 internetové protokoly. Speciálně pro IoT byl vytvořen IPv6 over Low – Power Wireless Personal Area Networks (6LoWPAN) protokol, který je modifikací IPv6 určený pro i ty nejmenší zařízení (21).

Pro přenos dat IoT mohou použít pevné kabelové připojení, ale z důvodu své malé konstrukce se ve většině případů volí bezdrátové technologie. Základními technologiemi jsou Radio-frequency Identification (RFID) a Near-field Communication (NFC), které vysílají přenosové vlny do 4 cm. Pro jejich použití se předpokládá, že komunikující zařízení jsou v těsné blízkosti. Tyto technologie se z pravidla používají pro předání jednorázové zprávy jedním směrem – zejména pro potřeby identifikace. Technologií pro středně velkou vzdálenost se používá technologie Bluetooth, WiFi a ZigBee. Problémem posledních dvou technologií je to, že používají 2,4 GHz frekveční pásmo, které je v hustě obydlených oblastech beznadějně přeplněné a dochází v něm k rušení. Nejoptimálnější bezdrátová technologie pro IoT jsou IQRF, Z-Wave, LoRa nebo Weightless využívající bezlicenční evropské pásmo 868 MHz, které má dosah až 100 metrů (22).

Charakteristikou IoT je fakt, že často je potřeba z jednoho zdroje poslat příkaz zároveň několika příjemcům a naopak. Proto se pro IoT vytvořily speciální protokoly pro rozesílání zpráv pomocí konsolidačního bodu – tzv. brokeru. Ukázkovým příkladem je protokol MQTT i jeho modifikace MQTT Sensor Network, který je navržen tak, aby co nejvíce zmenšil objem přenášených dat. Jeho binární HTTP alternativa Constrained Application Protocol (CoAP) byla na svém začátku koncipována stejným způsobem, avšak při zavedení volitelných doplňků protokol nabobtnal a s tím zmizela jeho hlavní výhoda malé datové náročnosti (23). Mezi další často používané protokoly patří například Extensible Messaging and Presence Protocol IoT (XMPP IoT) a Lightweight M2M (22).

Z popsaných protokolů je zřejmé, že takzvaný protocol stack je pro IoT zcela odlišný než

Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular Bands	10 Mbps	Several Miles	High	High
Bluetooth/BLE	2.4Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz, 2.4GHz	40, 250 kbps	> 100 square miles	Low	Low



Obr. 4: Bezpečný IoT protocol stack (Zdroj: Převzato z (24, s. 9))

pro ostatní IT zařízení. Podrobněji to popisují autoři vědeckého článku Security protocols for IoT, kde se podrobněji zkoumají hrozby, zranitelnosti, vektory útoků IoT. Na Obr. 4

lze vidět, jak popisují i složení IoT stacku, který je zabezpečen napříč většiny vrstev ISO OSI modelu (24, s. 8-10).

1.4 Řízení IoT bezpečnosti

Česká republika v roce 2014 zavedla zákon č. č. 181/2014 Sb. o kybernetické bezpečnosti jehož cílem je zlepšit opatření i reakce na kybernetické incidenty. Součástí zákona je i výčet přestupků, pokud některé ustanovení není dodrženo (25). Tím se každý poskytovatel digitální služby stal odpovědným za ochranu dat, které má v rámci svých služeb pod správou. Následné vyhlášky č. 315 až 317/2014 Sb. stanovily, obsah a strukturu bezpečnostních opatření, dokumentace, typy incidentů a správné likvidace dat (19). Zjednodušeně lze říct, že zákon stanoví, jak je potřeba zajistit ochranu dat a informací, a až vyhlášky určují, kdo je povinen tak činit.

Už v roce 2013 Mezinárodní organizace pro standardizaci (ISO) vydala sadu norem pro systém řízení informační bezpečnosti (ISMS). Normy jsou výsledkem zkušeností z praxe, které byly sepsány jako soubor doporučení přijaté širokou odbornou komunitou. V tomto případě normy přesně popisují, jak firmy mají postupovat pro zavedení aktivních opatření a firemních procesů pro zajištění ochrany informací.

O několik let později vydala ENISA příručky pro zajištění bezpečnosti IoT ve všech dotčených odvětvích. Za zmínku stojí hlavně dedikovaná příručka pro použití IoT v kritických informačních infrastrukturách a příručka pro použití IoT v moderní průmyslové výrobě.

1.4.1 ČSN ISO/IEC 27000

Norma ISO 27000 představuje pouze terminologii používanou ostatními normami ve skupině norem 27000. Mezi hlavní popisované části patří popis ISMS, proč je důležitý a také struktury požadavků proto, aby informace byla považována za bezpečnou. Do této struktury patří:

- **Důvěrnost:** zajištění, že informace není dostupná neoprávněné třetí straně (20, s. 9).

- **Integrita:** zajištění, správnosti, přesnosti a úplnosti informace a že informace během přenosu nebyla pozměněná neoprávněnou třetí stranou (20, s. 11).
- **Autenticita:** zajištění, že všechny strany zapojené do zpracovávání informací jsou opravdu ty, za koho se vydávají (20, s. 8).
- **Dostupnost:** zajištění, že informace bude dostupná a použitelná entitou, která si o ni zažádá (20, s. 8).
- **Spolehlivost:** zajištění souladu mezi zamýšleným chováním a výsledky (20, s. 14).
- **Nepopiratelnost:** zajištění schopnosti prokázat pravost a výskyt údajné události entitami, které je vyvolali (20, s. 13).

První tři požadavky se považují jako nezbytné minimum i mimo ISMS a často je k nim referováno pod zkratkou CIA – Confidentiality, Integrity, Authenticity.

1.4.2 ČSN ISO/IEC 27001

Norma 27001 je považována za hlavní dokument ISMS. Jejím obsahem je návod pro všechny organizace bez ohledu na jejich velikost či pole působnosti, jak mají postupovat při implementaci bezpečnostní politiky.

Norma má 10 kapitol z nichž pouze posledních 6 přesně popisují ISMS požadavky. Pokud organizace nesplní, byť jeden požadavek, pak nemůže získat příslušnou certifikaci (26, s. 1).

Z normy vyplývá, že ISMS má za cíl zavést, provozovat, monitorovat, udržovat a zlepšovat bezpečnost informačních aktiv (26, s. 2). K tomu je z pravidla použit Demingův model Plan, Do, Check, Act (PDCA). Jedná se o nekonečný cyklus, který v každé své iteraci vychází z předešlých poznatků proto, aby v další iteraci se dokázal adekvátně přizpůsobit pro dosažení lepších výsledků (17, s. 24).

Souhrn klíčových kapitol:

- **Kontext organizace**

  Kontext organizace je povinný dokument, ve kterém organizace popisuje své

činnosti, potřeby a také své okolí. Dokument je rozdělen na interní a externí aspekty. Interními se rozumí aspekty, které firma dokáže sama přímo ovlivnit. Externí jsou naopak takové, které organizace může ovlivnit pouze nepřímo (26, s. 1-2).

- **Vůdčí role**

  Organizace musí definovat základní bezpečnostní politiku a také stanovit odpovědnosti svých zaměstnanců za dodržování bezpečnosti informací. Vedení společnosti se musí také zavázat, že budou prosazovat ISMS prostřednictvím integrace bezpečnostních požadavků do činnosti organizace společně s poskytováním potřebných zdrojů (26, s. 2-3).

- **Plánování**

  Stejně tak jak i s ostatními podnikatelskými činnostmi, organizace musí plánovat bezpečnostní opatření na základě identifikovaných rizik. Na základě výstupu z předchozích dvou částí firma posoudí, která rizika jsou relevantní s ohledem na kontext činností a zainteresované strany. Je potřeba definovat jednotný postup identifikace, posuzování a akceptace rizik (26, s. 3-5).

- **Podpora**

  K tomu, aby organizace dokázala efektivně řídit bezpečnost svých informací, musí se zavázat k poskytování potřebných zdrojů pro zavedení, správu a neustále zlepšování ISMS. S tím souvisí zajištění kompetence osob, šíření povědomí o bezpečnosti mezi své zaměstnance, stanovení pravidel pro interní i externí komunikaci a styl, jakým je bude pořizována dokumentace (26, s. 5-7).

- **Provoz**

  Kroky popsané v předešlých částech normy jsou pojednávány během provozu firmy. Plánování je nezbytnou součástí všech procesů nutných pro splnění požadavků na bezpečnost informací. Každé přijaté rozhodnutí je potřeba dokumentovat, aby existoval důkaz, že společnost zvážila všechny možné hrozby a přijala preventivní a nápravná opatření (26, s. 7).

- **Hodnocení výkonnosti**

  Organizace musí průběžně sledovat a hodnotit efektivnost zavedeného ISMS. K tomuto stanoví jednoznačné procesy, během kterých bude docházet k měření a monitorování pro následné vyhodnocení efektivity. Dalším nástrojem ověření

kvality je interní audit, jehož účelem je ověřovat soulad interního ISMS s požadavky normy (26, s. 7-9).

- **Zlepšování**

  V případě, že během monitoringu dojde k neshodnému stavu, kdy reálný stav neodpovídá interním požadavkům, musí být organizace schopná identifikovat příčiny a provést přiměřená nápravná opatření. Jejich výsledkem má být obnovení souladu s požadavky a snížení rizika opakování neshodného stavu (26, s. 10).

1.4.3 ČSN ISO/IEC 27002

Na rozdíl od normy 27001, kde se popisují základní myšlenky ISMS a toho, jak je firma má zařadit do svých procesů, norma 27002 už přímo uvádí tzv. „implementační návody" bezpečnostních opatření. Norma obsahuje 14 bezpečnostních oblastí obsahujících celkem 35 hlavních bezpečnostních kategorií a 114 opatření. U každé kategorie je napsané odůvodnění a cíl, kvůli nimž je kategorie vytvořená. Pod kategorii spadají související opatření, kde u každé z nich je napsaný základní souhrnný popis, návod implementace daného opatření a další doplňková doporučení (27).

Mezi oblasti patří obecná bezpečnostní politika, která je zavedena vedením společnosti jako jasná pravidla a směrnice, jimiž jsou spravována a chráněna všechna informační aktiva. Následným krokem je organizace bezpečnosti informací, která určuje sadu bezpečnostních opatření v případě, že se jedná buď o interní, nebo o externí subjekty. Zkoumá taky zajištění bezpečného výkonu informační práce zaměstnanci ve všech stádiích pracovního poměru. Dalšími oblastmi jsou řízení informačních aktiv a přístupových práv (27, s. 2-28).

Zbylé oblasti řeší technologické části bezpečnosti a pravidla, jak postupovat s jejich výběrem, správou a vylepšováním. Norma řeší zejména kryptografické technologie, fyzické zabezpečení, zálohování, nástroje pro monitoring, řízení síťové bezpečnosti a nástroje k tomu potřebné. Dále řeší vztahy s dodavateli, řešení bezpečnostních incidentů a dopad informační bezpečnosti na kontinuitu činností organizace (27, s. 28-74).

Důležitou oblastí je sledování souladu s požadavky, které souvisí s právními nařízeními. Mezi ně patří například ochrana osobních údajů, duševního vlastnictví, interního know-

how aj. Oblast také řeší posuzování bezpečnostní politiky skrze dodržování interních předpisů nebo provádění auditu informačních systémů (27, s. 74-77).

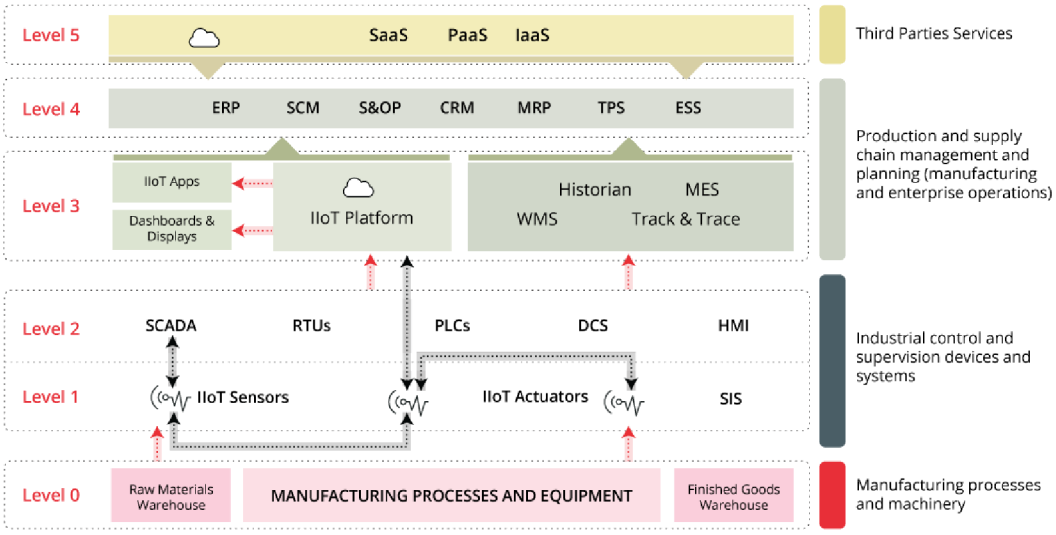
1.4.4 Doporučení ENISA pro IoT v průmyslové výrobě

Studie instituce ENISA si klade za cíl metodologicky prozkoumat moderní IIoT architekturní vzory a posbírat zkušenosti expertů daného oboru za pomoci strukturovaných dotazníků. Výsledkem tohoto průzkumu je sada nezbytných doporučení pro co možná nejsnazší řízení bezpečnosti IIoT v továrnách (6).

V předmluvě studie popisuje, že IoT technologie doposud nemá jednotnou definici. Jedním z důvodu je chybějící standardizace, která vede k četnosti heterogenních architektur. Mezi nimi jsou například FP7-ICT – IoT – A Architectural reference model nebo také NIST Network of Things. ENISA se snažila přijít s architekturou, která vyzdvihne klíčové elementy s důrazem na interoperabilitu napříč různými aktivy (11, s. 24).

Studie dále popisuje bezpečnostní výzvy, které vznikají zavedením IIoT zařízení do výroby, mezi něž patří například zranitelné komponenty, zvýšená konektivita, konvergence IT a OT, nezabezpečené protokoly aj. (6, s. 17)

Pro snadnější vytvoření taxonomie aktiv, byl vytvořen tzv. High-level referenční model založený na Purdue Modelu vyvinutý T. J. Williamsem.

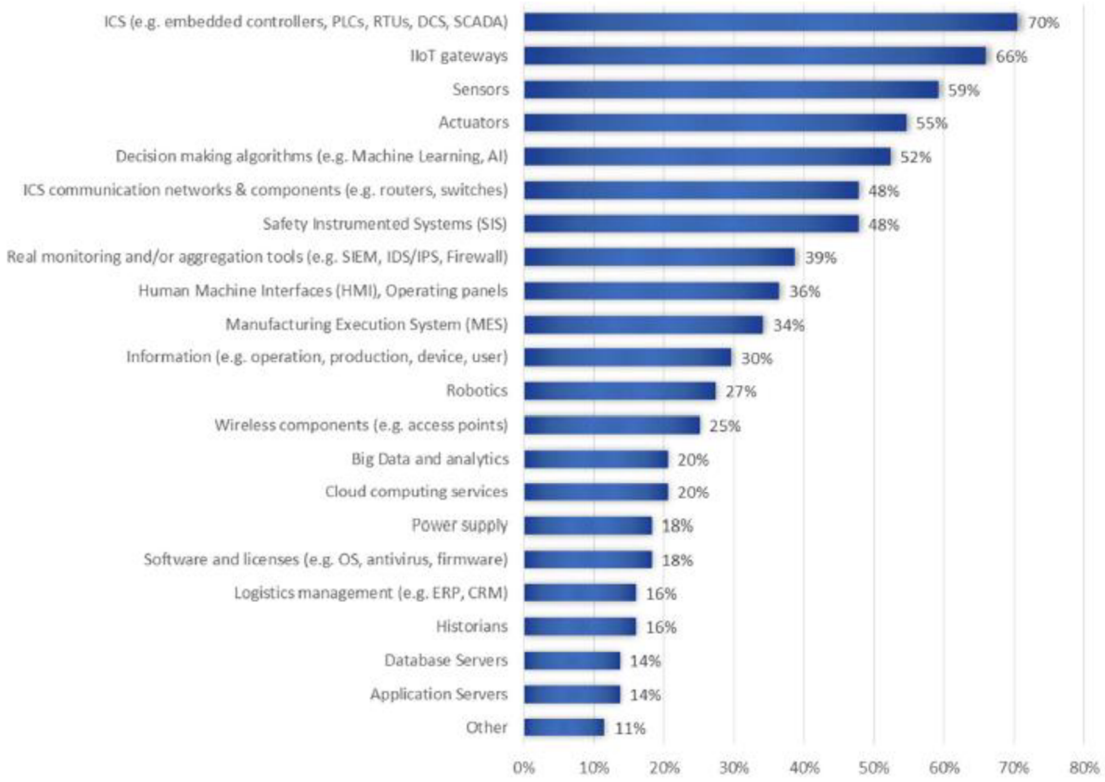


Obr. 5: High-level reference model (Převzato z (6, s. 18))

Tento model názorně ukazuje, jak IoT platforma vstupuje mezi OT a IT systémy. Slouží tím jako pojítko mezi oblastmi, které fungují real-time a systémy, které slouží k plánování.

Taxonomie aktiv

Proto, aby firma dokázala efektivně spravovat bezpečnost svých informací, je potřeba si nejdříve zmapovat všechna dostupná aktiva, která mají vliv na bezpečnost. ENISA vytvořila přehledný soupis všech aktiv, které se často vyskytují v Průmyslu 4.0. V Příloha 2 je znázorněno schéma všech dostupných aktiv. K tomuto schématu je v studii sepsána tabulka, která blíže popisuje každé aktivum a do které úrovně High-level referenčního modelu patří (6, s. 22-24). Daný soupis aktiv byl následně předložen expertům k tomu, aby určili ta aktiva, která považují za nejdůležitější z hlediska kyberbezpečnosti IIoT systému. Výsledek je zobrazený v Obr. 6. Z nej vidíme, že za nejkritičtější části se považují Industriální kontrolní systémy (ICS), za nimiž jsou vzápětí IIoT brány, čidla a ovladače.



Obr. 6: Výsledek hodnocení kritičnosti aktiv (Převzato z (6, s. 25))

Taxonomie hrozeb

Za pomocí rozčlenění aktiv a obecné taxonomie hrozeb, sestavila ENISA specializovanou taxonomii pro prostředí Průmyslu 4.0. Obdobně jak u aktiv, i zde bylo vytvořeno schéma viz. Příloha 3 a korespondující tabulka. Hrozby jsou rozděleny do kategorií podle jejich charakteru. V každé kategorii jsou pak vypsané možné hrozby a aktiva, kterých se to týká. Obdobně jak i u aktiv, se sepsané hrozby představili expertům, kteří následně hrozby ohodnotili a určili scénáře které mohou k hrozbám vést a jejich dopady (6, s. 27-35).

Kategoriazce bezpečnostních opatření

Autoři studie provedli extenzivní průzkum nejčastěji probíraných témat ohledně IoT bezpečnostních opatření. Ze zkoumaných materiálu byly pak agregováno 20 bezpečnostních domén, které mají zásadní vliv na zabezpečení IoT sítě. Pro přehlednost a logické rozčlenění se domény rozdělily do 3 skupin – obecná opatření, organizační postupy a technické postupy.

Obr. 7: Skupiny bezpečnostních domén (Převzato z (6, s. 36))

Obecnými opatřeními se rozumí celofiremní procesy, které při zavedení v organizaci zajistí dobrou úroveň kybernetické bezpečnosti (6, s. 37). Organizační praktiky popisují doporučené postupy, které se mají zavést mezi své zaměstnance a smluvní strany pro efektivní řízení zranitelností, zvládání incidentů a zajištění bezpečnosti IIoT v průběhu celého životního cyklu zařízení (6, s. 38). Technické postupy jsou pak opatření a nařízení týkající se bezpečné integrace, provozu a likvidace podpůrných aktiv (6, s. 40). Příklady jednotlivých domén jsou znázorněné v Obr. 7.

2 ANALÝZA SOUČASNÉHO STAVU

V této části práce představím zkoumanou organizaci. Motivací analýzy je snaha odkrýt možný dopad zranitelnosti bezpečnosti IIoT na proaktivní správu aktiv. Proaktivní správou se myslí nepřetržité vyhodnocování výrobního procesu za pomocí IIoT monitoringu, s cílem odhalit degradující kvalitu či výkon výrobního stroje k tomu, aby se dalo naplánovat jeho preventivní údržba.

Z důvodu velikosti organizace, bylo potřeba hned při rozpracovávání této práce postupně upřesňovat rozsah zkoumaných technologií. Daná firma mi umožnila si samotnému určit, co chci zkoumat, jelikož v každém oddělení firmy je velké množství oblastí, o kterých se dá psát závěrečná práce. Během úvodního průzkumu nastala komplikace v podobě vyhlášení národního nouzového stavu a zavedení státní karantény. To vedlo k razantní redukci zamýšlených analýz.

Sbírané informace byly tedy shromážděny pouze vyšetřováním veřejné dostupných materiálů a dotazování na dálku, protože dotyčná firma se uzavřela na větší část doby, kterou jsem měl k dispozici na vypracování této práce. Pokud bude v rámci této firmy poskytnutá příležitost, rád v budoucnu splním své prvotní zamýšlené plány.

2.1 Přestavení společnosti ŠKODA AUTO a.s.

ŠKODA AUTO a.s. je již 125letá firma vyrábějící automobily a je jedinou českou automobilkou, která přetrvala nejen druhou světovou válku ale i komunistický režim. Počátky této firmy můžeme najít v momentě, kdy zakladatelé Laurin a Klement se rozhodli vyrábět kola. Za nedlouho poté se tito pánové rozhodli motorizovat svá kola a začali vyrábět motocykly. Začátek výroby automobilů v roce 1905 byl pak jedině logickým krokem této společnosti, která se tím zabývá doteď (28). Díky tomu je se jedná o 4. nejstaršího výrobce aut na světě (29) a tvoří majoritní část průmyslu českého hospodářství. Pouze tato společnost odpovídá za skoro 5 % HDP (30) zejména díky tomu, že již pátým po sobě jdoucím rokem vyrábí víc než milion aut ročně a v průměru 3600 aut denně dohromady ve svých českých továrnách (31).

Základní údaje o společnosti:

Obchodní firma: ŠKODA AUTO a.s.

Právní forma: Akciová společnost

Sídlo společnosti: tř. Václava Klementa 869, Mladá Boleslav II, 293 01

Identifikační číslo: 001 77 041

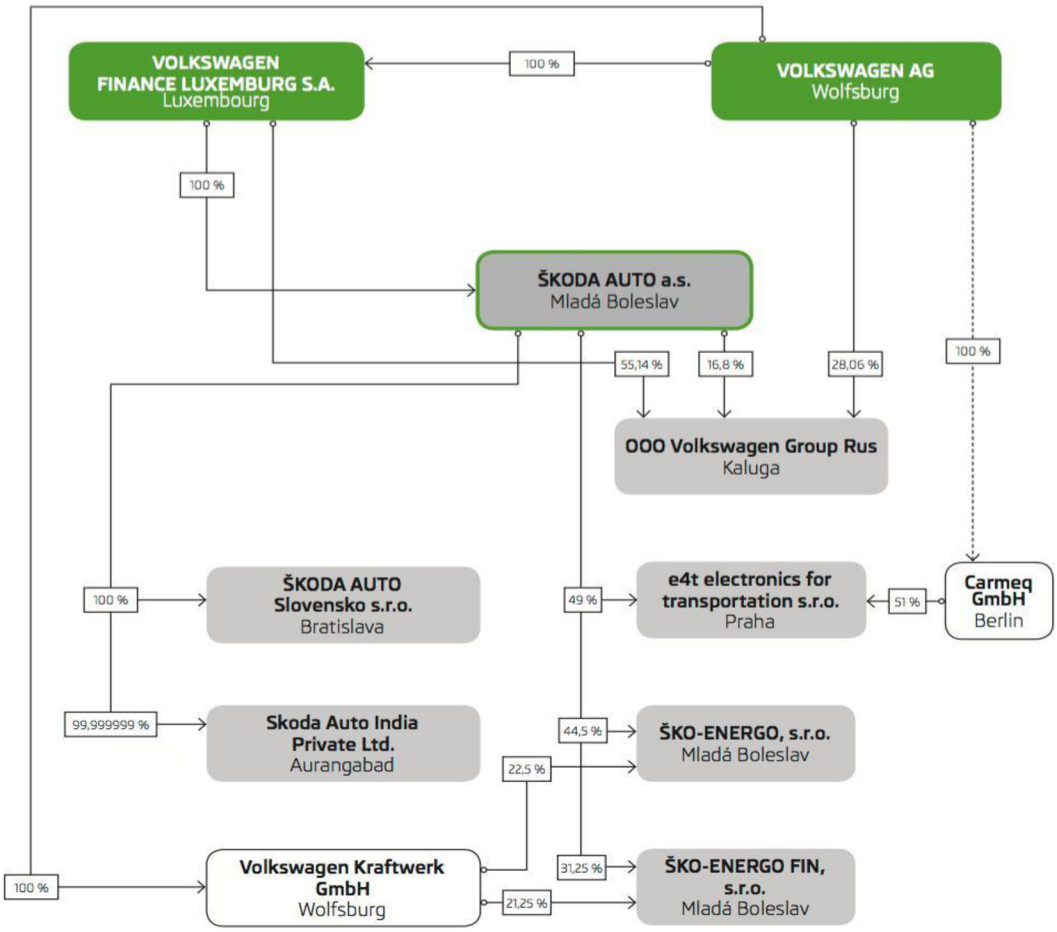
Základní kapitál: 16 708 850 000,- Kč

Roční obrat (v roce 2018): 416 700 000 000,- Kč (32)

Obr. 8: Logo firmy SKODA AUTO a.s. (Zdroj: Převzato z (48))

2.1.1 Obchodní skupina

V roce 1991 se stává ŠKODA AUTO a.s. součástí koncernu Volkswagen, čímž se stává čtvrtou značkou po boku Volkswagen, Audi a SEAT. Koncern si zpočátku pořídil 11 % podíl, ale v následujících letech tento podíl neustále navyšoval a od roku 2000 vlastní 100 % podíl společnosti. Prvotní záměr koncernu byl zajištění výrobce aut v blízkosti Německa, který by se stal strategickým konkurentem v cenovém segmentu aut, do kterého patří automobilky Renault, Peugeot, Fiat a Volvo. Toto strategické umístění továren Škody umožnilo sdílet autodíly napříč sesterskými automobilkami a tím i snižovat své náklady (33).



Obr. 9: Schéma obchodní skupiny ŠKODA AUTO a.s. (Zdroj: Interní dokumenty ŠKODA AUTO a.s.)

2.1.2 Výrobní továrny

ŠKODA AUTO má tři domácí výrobní závody. První a největší z nich se nachází v Mladé Boleslavi, které zároveň slouží jako centrální středisko společnosti. Druhá se nachází ve Vrchlabí a poslední v Kvasinách. Mimo to má továrny téměř po celém světě s primární koncentrací ve slovanských zemích a na dálném východě, kde jenom v Číně má o továrnu víc než v České republice. Mezi další země produkující vozy Škoda patří Ukrajina, Rusko, Kazachstán, Alžírsko, Indie, Slovensko a Německo (34).

Mladá Boleslav

Tento závod je epicentrem všech činností ŠKODA AUTO. Právě zde se nachází středisko technologického pokroku značky ŠKODA. V tom čísle jsou veškeré nové designy, nápady a inovace, které značka přináší s každou novou iterací modelů svých aut.

V daném momentě se v této továrně vyrábí modely FABIA, OCTAVIA, RAPID a KAROQ. Mimo to se zde produkují moderní maloobjemové TSI motory, které jsou následně použité v autech napříč koncernem. Společně s nimi si ŠKODA AUTO vyrábí i své vlastní převodové skříně typu MQ/SQ 100 a MQ 200 s dalšími příslušnými díly (35).

V mladoboleslavském výrobním komplexu sídlí i další administrativní celky mezi něž patří vedení společnosti, technický vývoj, výroba a logistika, prodej a marketing, obchodní oddělení, správa lidských zdrojů a muzeum. To je otevřeno pro širokou veřejnost a obsahuje reprezentanty naprosté většiny historicky významných modelu této značky. Příznivci značky Škoda si také mohou domluvit prohlídku výrobních prostor s průvodcem.

Kvasiny

Kvasinský závod je nejmladší továrnou v České republice, která na začátku vyráběla karoserie pro JAWA 700, ale po druhé světové válce se stala součásti mladoboleslavské továrny. Tato továrna v aktuálním výrobním programu vyrábí modely KAROQ, KODIAQ a SUPERB. Společnost nedávno zainvestovala téměř 7 miliard korun na nejrozsáhlejší modernizaci továrny za celou svou historii (36).

Vrchlabí

Druhá nejstarší továrna společnosti byla na začátku nezávislým výrobcem, který vyráběl těla vozů Škoda. V roce 1946 se stala plnohodnotnou součástí ŠKODA AUTO a její prvním oficiálním vypuštěným modelem pod střechou nového majitele byl koncept auta ŠKODA Tudor, po kterém následovali zejména modely speciálních edicí luxusních a užitkových vozů.

V dnešní době primárním produkčním plánem tohoto závodu je výroba sofistikovaných DSG převodovek typu DQ 200 pro celý koncern Volkswagen. Sedmistupňová automatická převodovka, která se vyrábí od roku 2012, patří mezi nejmodernější převodovku svého druhu (35).

2.1.3 Dodavatelé

Dle výroční zprávy ŠKODA AUTO z roku 2015, společnost prosazuje celosvětový nákup ve vztazích se svými dodavateli i nadále hlavní principy koncernového projektu „Udržitelnost v dodavatelských vztazích“, který byl zaveden nejdřív výrobcem Volkswagen a následně postupně zaváděn do všech firem stejnojmenného koncernu. Tento projekt prověřuje, zda dodavatelé fungují v souladu s těmito zásadami, které se dělí do dvou kategorií a je jich celkově dvanáct. Nákup je rovněž spoluzodpovědný za modely značky ŠKODA a spolupráci s dodavateli v zahraničí. Vážnou výzvou bylo udržení evropských dodavatelů na ruském trhu. Situace, okolo hrozícího odchodu dodavatelů z Ruska, způsobená ruskou krizí a extrémním oslabením ruského rublu, již byla stabilizována. Ve spolupráci s kolegy z čínského regionu probíhají intenzivní snahy o oboustrannou optimalizaci materiálových nákladů jednotlivých modelů značky ŠKODA (37).

Výroční zpráva z roku 2018 rovněž napovídá, že společnost aktivně buduje vztahy ve svém dodavatelském řetězci a vede s nimi diskuze o jejich plánech do budoucna. K tomu slouží každoroční inovační akce TechDays, kdy jak sama ŠKODA, tak i její dodavatele prezentují své plány do budoucna a chystané inovace. Společnost si vybírá strategické dodavatelé jsou rozmístění po celém světě. V daném momentě 80 % všech dodavatelů tvoří importéři, zato když se podíváme na výdaje spojené s dodavateli, vidíme, že ač domácí dodavatelé tvoří pouze pětinu dodavatelské struktury, připadá na nich 45 % z celkových 215 mld. Kč výdajů. Hned za nimi jsou němečtí dodavatelé s čtvrtinovým podílem na této statistice (38).

2.1.4 Zákazníci

Statistiky v poslední výroční zprávě ukazují, že se automobilce podařilo za rok 2018 udržet rostoucí trend z hlediska prodejů. Celkové meziroční prodané kusy aut se zvedly o 4,4 % na 1 253 741 vozů. Společnost se dokázala rychle přizpůsobit novým WTLP emisním certifikacím a obhájit si svůj pozitivní rozvoj z hlediska prodejů. Jiné automobilky museli projit re-certifikačním procesem proto, aby nově představené modely mohli být vypuštěni na evropské silnice. S tím souvisely i opožděné dodávky objednaných vozů novým kupcům, čemuž se společnost dokázala vyhnout (38).

Výroční zpráva rozepisuje jednotlivé země a jak se změnily prodeje v každé z nich. Největším posunem společnost zaznamenala v Rusku, kde prodeje stouply o úctyhodných 30,7 %. V absolutních číslech to ovšem znamenalo umístění Ruska na 4. místo z hlediska celkových prodejů. Hned nad nim se umístil domácí trh, který zaznamenal pokles o 1,5. Druhé místo patří Německu a prvenství si znovu připsala Čína, která má třínásobně větší prodeje než v Německu a meziročně se ji zvedly prodeje o 4,5 % (38).

Díky přísnějším emisním nařízením, automobilka od roku 2019 postupně uvádí auta s plně elektrickým pohonem, například CITIGO IV, nové plug-in hybrid verze svého vlajkového modelu SUPERB a sportovní varianty OCTAVIA RS. V roce 2020 se také chystá odhalit podobu plně elektrického SUV modelu ENYAQ. Díky spojení se společností ŠKODA Financial Services lze vozy ŠKODA zakoupit v České republice i on-line na operativní leasing.

2.1.5 Technický vývoj

ŠKODA AUTO v roce 2018 investovala téměř 22,5 mld Kč na technologický vývoj. Není v plánu, aby se tato částka se v následujících letech zmenšovala, jelikož moderní automobily se neustále digitalizují. Mezi možné důvody patří tlak poptávky, nebo samotných zákonodárců, kteří zavádějí stále přísnější nařízení na bezpečnostní prvky aut jako jsou povinné aktivní upozorňování o překročené povolené rychlosti, nouzové udržování jízdního pruhu aj. (38).

Společnost otevírá nové testovací a výrobní objekty mezi které patří nová zkušebna převodovek v Motorovém centru nebo vývojové centrum v Indii, které je speciálně dedikované pro vývoj produktů určené pro tento trh (38).

V roce 2019 ŠKODA AUTO představila své vize budoucnosti v podobě konceptu VISION X, který kombinuje dva zdroje pohonu CNG a elektrickou energii. Během provozu tento vůz má kombinovat oba zdroje a tím snížit emise až o 20 % oproti čistě spalovacímu pohonu. V případě, že by vůz využíval syntetický plyn, nebo bioplyn, dosahoval by nulové uhlíkové stopy. Nový koncept představil i nové digitální služby, které jsou možné díky technologii ŠKODA Connect. Jmenovitě se jedná o chytré

navádění na volné parkovací místo, možnost sdílení jízdy nebo také pronájem vozu, když zrovna není v aktivním provozu (38).

Je nutné podotknout, že nové technologické pokroky se sebou nesou i řadu rizik, která už zmíněná nejsou veřejnosti. Tím, že auta jsou čím dále tím více digitalizována a napojována na internetovou síť, stávají se dalším velice atraktivním vektorem pro kybernetické napadení. Tím se pro společnost představuje zcela nová dimenze odpovědnosti za své produkty.

2.2 Řízení informačních technologií a aktiv

Pro potřeby této práce je nutné si u tak velké společnosti vytyčit vhodnou část k analýze, která odpovídá dostupným prostředkům. Společnost má šestnáct továren v devíti zemích a je rozdělená do sedmi organizačních jednotek (34). Společnost disponuje velkým IT oddělením, který se stará o zavádění, servis a údržbu všech IT i OT technologií a systémů.

Samotné IT oddělení je dále segmentováno do osmi sekcí dle pole jejich působnosti, z nichž každá je dál rozdělená do jednotlivých týmů. Z tohoto důvodu není možné zkoumat společnost jako celek a je potřeba si vybrat jenom její úzkou specifickou část – v mém případě jediný projekt zaměřený na zavedení technologií, které umožňují lépe sledovat výrobní linky a díky tomu předvídat, kde může dojít k poruše.

Jelikož se jedná o velkou mezinárodní společnost, je jeden segment z IT oddělení vyhrazen pouze na IT governance a bezpečnost. Tento segment dohlíží na to, aby provoz IT technologií byl efektivním pomocníkem při dosahování obchodních cílů. Starají se o zavádění změn IT podpory, kontrolují technické koncepty nově zaváděných řešení pro to, aby splňovali provozní a bezpečnostní požadavky interních i národních IT pravidel. Jedním z nejvýznamnějších činností tohoto segmentu je pravidelné vyhodnocování bezpečnostních rizik a neustálé vyšetřování bezpečnostních incidentů. Jenom tento segment odpovídá za dodržování celkem 44 firemních směrnic, norem a pokynů. Většina z nich je spjatá právě se systémem řízení informační bezpečnosti.

2.2.1 Zkoumaná část firmy

ŠKODA AUTO má již několik projektů spojené se zavedením technologií v souladu s Průmyslem 4.0. Používá již například autonomní transportní vozíky, které přepravují součástky ze skladů k místu jejich zpracování, dále používá chytré snímací rukavice, které kontrolují obrázkové kódy a hapticky dává nositeli vědět, zda pracuje se správnými díly. Jedním z dalších projektů stojících za zmínku jsou kolaborativní roboti, tzv. coboti, sloužící pro skládání převodovek DQ 200 (39).

Pro tuto práci je zásadní projekt pro chytrou údržbu. Projekt pod názvem FIOT si klade následující cíle:

- Vytvoření jednotného systému k podpoře prediktivní a chytré údržby
- Vytvořený systém je dostupný na všech zařízeních se zobrazovacími schopnostmi (počítače, mobilní zařízení a televize)
- Integrace klíčových dat s dalšími aplikacemi pro zlepšení procesu chytré údržby
- Zavedení moderních nástrojů po vzoru Industrie 4.0
- Zajistit budoucí rozvoj této platformy a zajistit dostatečnou reakční schopnost na nové požadavky (40)

Tento systém pak má následně monitorovat veličiny jako je stav sítě PROFINET, trend stavu klíčových zařízení, tlak a spotřeba vzduchu, lisovací síly, teploty hlavních motorů aj.

2.3 Analyzovaná aktiva

Projekt FIOT byl spuštěn v roce 2018 a stále probíhá. Společnost postupně testuje a integruje IIoT zařízení do oddělení, kde je to žádané a přínosné. Projekt pojednává na míru složené SW i HW nástroje, které vzájemně řeší většinu současných požadavků společnosti a jsou dostatečně flexibilní v případě budoucích změn. Zatím se v rámci projektu zavedly nové technologie pouze do tří výrobních oddělení v továrně v Mladé Boleslavi.

Lisovna

Lisovna již měla zavedený systém pro monitorování stavů lisovacích strojů. Tento systém však přestal vyhovovat potřebám firmy z důvodu své chybovosti, špatné odezvy systému a také malou flexibilitou pro zavádění nových změn. Chyběl také monitoring sítě PROFINET a jednotnost s dobrou dostupností výkazů a možnost integrace s nadřazenými systémy, které sbírají výrobní data z lisoven a sledují stav skladů.

Projekt FIOT v tomto případě přináší náhradní SW řešení, které řeší výše zmíněné nedostatky a také přináší další benefity plynoucí z okamžitého vyhodnocování sbíraných dat. Hlavním přínosem je možnost pokročilé prediktivní údržby, při které se uživateli zobrazují trendy a generují výstražná hlášení pomáhající efektivněji naplánovat servisní intervaly (41).

Nářaďovna

V tomto oddělení byly stejné komplikace se stávajícím řešením pro monitoring. Tady vzniká další problém v letních měsících, kdy teploty v rozváděčích mohou vystoupat tak vysoko, že může dojít k poškození PLC a jiných komponent. V rámci FIOTu se proto zavedly bezdrátové senzory s vestavěným čidlem teploty. Ty pak slouží k snímání teplot v nejčastěji zastoupených zařízení od výrobců Heidenhain, Fidia a Siemens. Kromě těchto dodatečných zařízení bude projekt poskytovat stejné výstupy jak i v případě lisovny (42).

Montáž

V případě montáže hraje klíčovou roli stabilní napájecí napětí 24 VDC, které zajišťuje celá řada zdrojů. Ty během své životnosti začínají chátrat a ztrácejí požadovaný příkon. Pro údržbáře je těžké najít ve velkém počtu zdrojů ten, který je vadný. Proto se i zde zavedly tytéž senzory, co i v případě nářaďovny k tomu, aby každých 5 sekund snímaly napětí na každém ze zapojených zdrojů. Dispečink pak může téměř v reálnem čase sledovat jejich stav. Mimo snímání napětí je systém připraven sledovat i další trendy jako je využití většiny provozních utilit (43).

2.3.1 Použité softwarové služby

Celý systém se skládá ze tří hlavních SW komponent – hlavního systému, v němž se uchovává celá business logika, SW propojovací adaptér a sběrných databází. Tyto tři komponenty následně využívají již zavedené služby pro autentizaci a autorizaci.

Systém ThingWorx

Systém ThingWorx je hlavním vyhodnocovacím systémem celého projektu. Jedná se o tzv. skladatele, v němž si správci mohou vytvořit informační panely dle svých potřeb. Výzkumná a konzultační společnost Forrester zařadila vydavatele systému PTC mezi leadery na trhu IoT řešení společně s Microsoftem, Siemensem a C3.ai.

Obr. 10: Forrester srovnání IoT platforem (Zdroj: Převzato z (49))

Tento aplikační serveru má jen jednu centrální instanci, ke které se pak připojují uživatelé a sledují aktuální stavy výrobních zařízení.

Služba KEPServerEX

Tato služba vždy běží na industriálním počítači, který je vždy umístěn na oddělení, ze kterého jsou sbíraná data. Úkolem této služby je být adaptérem mezi industriálními protokoly a centrálním systémem ThingWorx. Služba k tomu používá OPC komunikační protokol, který má za úkol sjednotit formy komunikace nezávisle na výrobci a ovládačích průmyslového zařízení. Výhodou Kepserveru je široká škála ihned dostupných plug-in modulů dedikovaných pro nejčastěji používaná průmyslová zařízení. V případě vlastních přístrojů nabízí taky Software Developlment Kit pro integraci svého vlastního proprietárního ovládače.

Databáze PostgreSQL

Systém ThingWorx a všechny instance Kepserverů využívají instance open-source databáze PostgreSQL k ukládání všech sbíraných dat.

2.3.2 Datové toky

Projekt FIOT je zaměřený hlavně na monitorování výrobních procesů pro zlepšení reakční doby a možnosti předvídání případných poruch. Z tohoto důvodu je většina datových toků jednosměrně centralizovaná do systému ThingWorx, jak můžeme vidět na Obr. 11. Nepočítá se, že komunikace směrem z ThingWorx do podřízených zařízení a služeb bude běžnou záležitostí. Kromě úprav konfigurace systémů a zařízení správci OT není důvod, proč by hlavní systém upravoval něco jiného kromě sebe samého. Veškerá interakce pak v případech poruch následně probíhá za osobní přítomnosti kompetentní osoby.

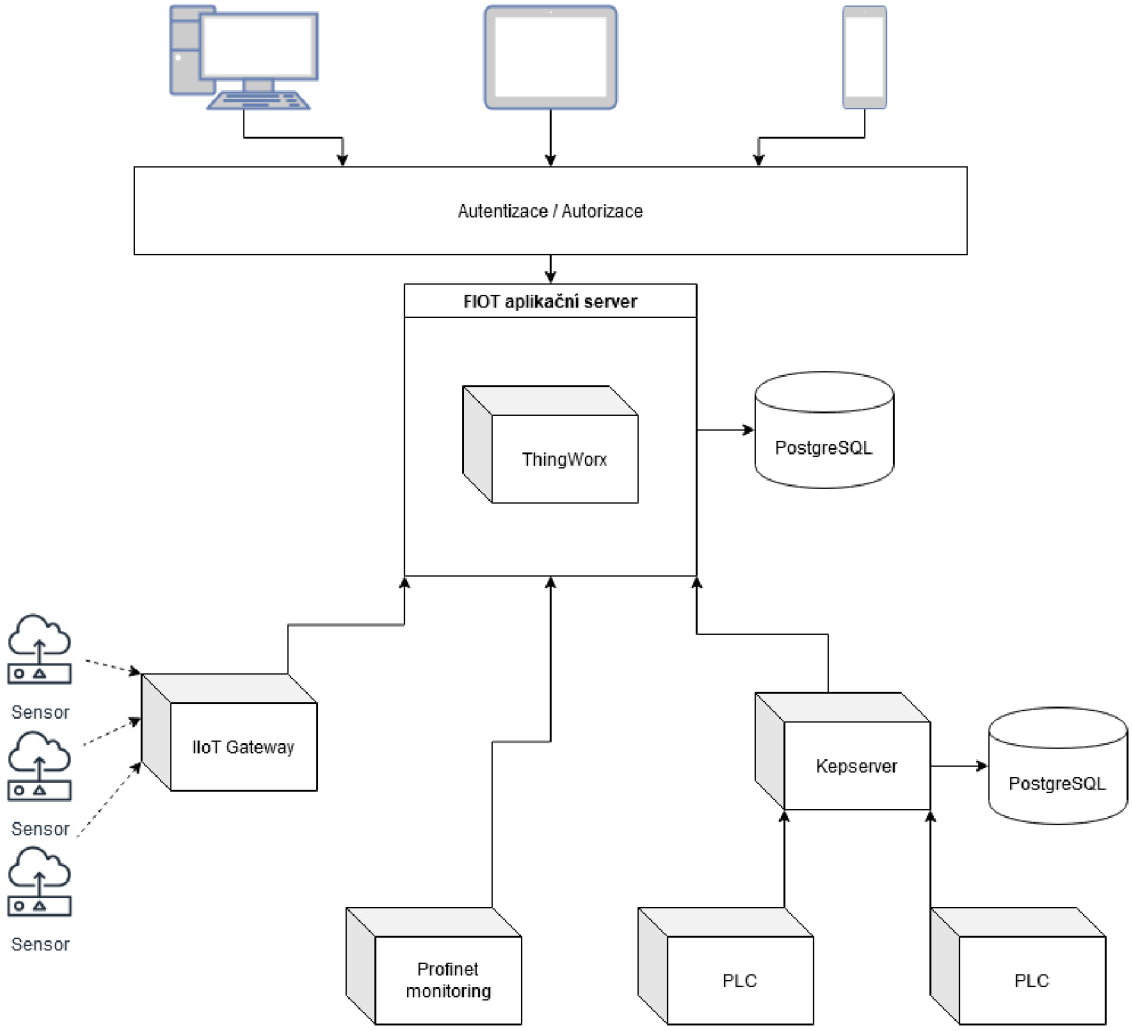
Směr bottom up

Systém je zásobován třemi hlavními druhy zdrojů dat – IIoT bránami, Kepservery a PROFINET sítěmi. Na IIoT bránu lze bezdrátově napojit až 5 čidel pomocí protokolu IQRF. PROFINET síť dokáže komunikovat napřímo s FIOT serverem, proto není potřeba

použít mezičlánek. V případě monitorování PLC zařízení, je již potřeba nejdřív data centralizovat v rámci úzkého perimetru do Kepserveru, který disponuje svou vlastní databází a následně data následně předává do hlavního centra sledování.

Směr top down

Uživatele se nyní mohou připojit k ThingWorx z řady zařízení ať už se jedná o počítač, tablet nebo mobil. Existuje odlišná sada pravidel pro těmi uživateli, kteří se připojují z interní sítě a těmi, kteří se připojují z internetu. V každém případě musí projít autentizací a autorizací skrz LDAP protokol.



Obr. 11: Schéma toku dat FIOT platformy (Zdroj: Vlastní zpracování dle (40))

2.3.3 Smluvní zajištění

S hlavním dodavatelem služeb FOXON s.r.o. je sjednána Service Level Agreement (SLA) dohoda, ve které jsou obsaženy položky zajišťující mlčenlivost dodavatele a taky jeho odpovědnost za škody způsobené příjemci služeb. Samotná SLA dohoda slouží jako podpůrný dokument pro Všeobecné Nákupní Podmínky ŠKODA AUTO a.s., kde jsou podrobněji rozebrána práva a povinnosti dodavatele a příjemce (44).

2.4 Metoda asistovaného zhodnocení

K bližšímu zhodnocení zavedených bezpečnostních opatření ve firmě jsem použil výčet doporučených bezpečnostních opatření od organizace ENISA zmíněných v teoretických východiscích. Tato doporučení vychází z doporučení národních i mezinárodních institucí, IT standardizačních organizací i samotných výrobců IT a OT.

Tato opatření obsahují celkově 110 doporučení, rozdělených do 20 tematických okruhů viz. Obr. 7. Pro případný audit bezpečnosti lze tato doporučení přeměnit do podoby otázek, za jejichž pomocí lze prozkoumat, jak je daný podnik efektivní při řízení informační bezpečnosti. Výhodou těchto doporučení je to, že jsou šité na míru výrobnímu prostředí, kde se aplikuje IIoT technologie.

K vyplnění tabulek níže jsem vycházel z celé řady interních předpisů, zejména těch pod správou segmentu odpovídajících za IT governance a bezpečnost. Mezi další zdroje informací se řadí možnosti osobních rozhovorů se zaměstnanci ŠKODA AUTO a také jsem měl k dispozici celkovou dokumentaci projektu FIOT.

2.4.1 Obecná opatření

První skupina opatření se zaměřuje hlavně na obecnou integraci bezpečnostních opatření do firemních procesů a má za cíl učinit bezpečnost více konkrétní a robustní. V případě security a privacy by design je potřeba vždy zohlednit kontext, ve kterým je IIoT použito. Tyto dva koncepty budou v různých scénářích vyžadovat jinou sadu okolností a prostředí, které je potřeba brát v úvahu.

Tab. 1: Obecná opatření (Zdroj: Zpracováno dle (6))

	Poznámka	Hodnocení
Security by design		
Je IoT bezpečnost řízená jako PDCA model?	Posouzeno z vlastního sledování.	Ano
Řeší se IoT bezpečnost na úrovni koncových stanic nebo jako celku?		Jako celek
Jsou všechna IoT zařízení vybavena funkcemi pro svou identifikaci a autentizaci?	Historická zařízení ne.	Částečně
Jsou bezpečnostní experti zapojeni do návrhového procesu nově integrovaných technologií?	SLA musí být schválena IT bezpečnostním oddělením a nové technologie musí odpovídat internímu technickému standardu.	Ano
Je u každé dokumentace vyhrazená kapitola řešící bezpečnost informací a systému?		Ano
Privacy by design		
Je zavedená GDPR směrnice?		Ano
Je u každého zařízení stanoveno, se kterými daty pracuje a proč už při přípravě jeho integrace?		Ano
Je stanoveno, kde jsou data fyzicky umístěna a mezi kterými stranami budou přenášena se zavedením need-to-know restrikcí?		Ano
Jsou prováděny analýzy dopadu soukromí u každého IIoT zařízení?	V daném momentě IIoT zpravidla nezpracovávají data, která mohou narušit soukromí.	Částečně
Jsou osobní informace oddělovány od ostatních informací a jsou dostatečně šifrována?	V případě FIOTu se nezpracovávají osobní informace.	Ano
Správa aktiv		
Používají se nástroje pro správu aktiv, které dokážou dynamicky odhalovat, identifikovat a označovat aktiva specifických pro organizaci?	Tvorba záznamů se vytváří ručně. Zavádí se systémy, které to budou automatizované.	Částečně
Má firma konsistentní a aktuální inventuru aktiv?		Ano

V oblastech, kde se doposud používají legacy systémy, používá se hlavně pasivní monitorování? Při nutnosti aktivního monitorování, provádí se nejdříve testovací fáze?	Společnost má metodický pokyn pro testování SW změn, ethernet síť je monitorována, PROFINET síť je odizolována a nejde dynamicky kontrolovat.	Částečně
Je inventurní systém jednotný pro celé digitalizované prostředí napříč továrnami?		Ano
Je pro správu aktiv, infrastruktury a bezpečnostních opatření vyčleněná dedikovaná síť?		Ano
Zavádí se nové zařízení pouze v souladu se zavedeným, odsouhlaseným a komunikovaným procesem řízení změny?		Ano
Jsou omezené přístupové porty (USB aj.) ve všech případech kromě těch, kde je to obchodně důležité?	Technický standard, který to požaduje.	Ano
Správa rizik a hrozeb		
Projevily se při zavádění Průmyslu 4.0 změny řízení bezpečnosti zvážením nových parametrů, hrozeb a scénářů napadení?	Snaha klást více důraz bezpečnost a odpovědné osoby se upozorňují na možné zranitelnosti.	Ano
Je prováděna analýza rizik alespoň jednou ročně? Je analýza rizik napojená na jiné procesy jako jsou řízení změny, řešení incidentů a řízení zranitelností?		Ano
Provádí se průběžně průzkum nových zranitelností v kooperaci s prověřenými partnery jako jsou ISAC a CERT.	Koncern má svůj vlastní CERT a je nasazen skener zranitelností monitorující nové zranitelnosti.	Ano
Sledují se průběžně vybrané hrozby a vyhodnocuje se jejich dopad na systémy za pomocí hodnocení rizik?		Ano
V procesu řízení rizik kombinují se postupy top-down a bottom-up?	Jsou zavedené dva systémy pro sledování rizik.	Kombinovaně

Jelikož se jedná o mezinárodní firmu, která spadá do mnohem většího celku skládajícího se z dalších automobilních výrobců, má firma zavedené desítky směrnic, norem, pokynů a dokumentace, které mají za cíl sjednotit celý koncern ve výkonu všech produkčních procesů. Do toho spadá i řízení celkové bezpečnosti a informačních aktiv společnosti. Z tabulky výše lze vidět, že organizace zatím nemá přizpůsobené interní procesy pro práci s IoT, neboť se jedná o relativně nový koncept. Z dotazování vím, že společnost nyní pracuje na nápravě těch oblastí řízení IT aktiv, které nejsou zcela optimální.

2.4.2 Organizační praktiky

Organizační složka celého podniku taky hraje významnou roli při snaze zavést efektivní systém řízení informační bezpečnosti. Kritéria ochrany dat prochází celým dodavatelským řetězcem, a proto je potřeba adekvátně stanovovat smluvní podmínky s dodavateli i zákazníky, aby i ti byli odpovědní za bezpečnostní dopady svých služeb a informací.

Tab. 2: Organizační praktiky (Zdroj: Zpracováno dle (6))

	Poznámka	Hodnocení
Životní cyklus koncových zařízení		
Je bezpečnost hlídána po celou dobu životnosti zařízení?		Ano
Hlídají se všechny aspekty napříč hodnotovým řetězcem? Hlídá se SW a HW v průběhu průchodem řetězcem pro zamezení neautorizovaných změn?		Ano
Jsou během vyhlášení zakázky předem stanovené bezpečnostní požadavky na nová zařízení?	IT bezpečnostní oddělení je zapojené do celého procesu sjednání zakázky + jsou je zavedený interní technický standard.	Ano
Jsou před nasazením zařízení do ostrého provozu prováděny penetrační testování? (Factory Accaptance Testnig and Site Acceptance Testing)	Společnost má metodický pokyn pro integraci SW.	Ano
Předává se bezpečnostní dokumentace a její podklady během předávací fáze dokončeného projektu?	Při převzetí SW od třetí strany se provádí kontrola.	Ano
Zvládání incidentů		
Jsou definované a rozčleněné kybernetické incidenty do skupin podle společného attack vectoru?	V přípravě.	Zatím ne
Má firma dedikovaný SOC?		Ano
Je jasně zavedený postup identifikace a řešení incidentu? Jak často dochází k jeho revizi v závislosti na lessons-learned a času?		Ano, ročně
Zkoumají se všechny bezpečnostní anomálie? Je zaměstnancům komunikováno, aby hlásili jakákoliv domnívané bezpečnostní zranitelnosti?	Plánuje se zavedení systému, který by to kontroloval.	Částečně. Je zavedený skener, který nevidí všude

Správa zranitelností		
Je zaveden systém řízení zranitelností? Skládá se z automatických i manuálních nástrojů?	Nařízeno dle interní dokumentace.	Ano
V případě řešení zranitelností postupuje se od nejvíce kritických aktiv a systémů?		Ano
Je zavedená těsná spolupráce mezi IT a OT oddělením? Dochází někdy k tomu, že člen IT zavede bezpečnostní opatření bez vědomí OT?	Snaha o efektivní komunikaci. Nezavádí se bez vědomí.	Ano
Je zaveden jasný proces zveřejňování zranitelnosti? Je vyhlášen bug bounty program?	Zatím je zveřejňováno plošně, ale nadchází úprava komunikace zranitelností. Bug bounty není.	Ano
Provádí se průběžně penetrační testování IIoT zařízení v kontrolovaném prostředí? Jak často k tomu dochází?	Probíhá skenování zranitelností pomocí dedikovaného systému.	Ano, měsíčně
Školení a bezpečnostní povědomí		
Je zaveden holistický přístup pro školení zaměstnanců na všech úrovních ohledně povědomí o IT bezpečnosti?		Ano
Je pro nové zaměstnance zajištěno povinné školení o IT bezpečnosti?		Ano
Jsou bezpečnostní školeni prováděná pravidelně? Aktualizuje se jejich náplň v závislosti na aktuálních hrozbách a minulých incidentech?		Ano
Jsou uživatele IIoT školeni ohledně zavedených bezpečnostních opatření a o tom, kde a jak jsou použity?	Školení je obecné na všechna IT/OT zařízení.	Částečně
Je firma zapojena do pravidelných diskusí napříč celým hodnotovým řetězcem a také organizací zabývající se Průmyslem 4.0 (Plattform Industrie 4.0, IIC, Cloud Security Alliance atd.)		Ano
Vztahy s třetími stranami		
Jsou omezené přístupy pro externí partnery do výrobní sítě pomocí kličkování RJ45, časovače, MFA a je přidělován pouze on-demand?		Ano

Jsou partnerům poskytované přímé přístupy k výrobním či řídícím systémům? Pokud ne, jsou vyhrazené kanály dostatečně segregované?	Přístup musí být inicializován ze strany ŠA – pak mají kontrolovaný přímý přístup.	Ne
Je od partnerů vyžadována informace o míře bezpečnosti poskytovaných služeb? Jsou stanovená minimální bezpečnostní požadavky pro nové partnery?	Před každou spoluprací je potřeba splnit interní technický standard.	Ano
Jsou s partnery sjednávané SLA a NDA ještě před tím, než se spustí kooperace?	Je to nařízeno všeobecnými nákupními podmínkami.	Ano

Společnost má úzce spolupracuje se svými dodavateli a má jasně stanovené postupy, jak s nimi komunikovat a co od nich požadovat. Jediné dva nedostatky jsou opět spjaté s přestavením nových principů z konceptu Průmysl 4.0.

2.4.3 Technické postupy

Zatím co předchozí dvě skupiny dotazů se týkají zejména podnikového řízení a obecných praktik, je potřeba zajistit i technická opatření k minimalizaci možných zranitelností. Následující okruhy otázek zkoumají, jak jsou zabezpečené jednotlivé horizontální sektory kritické informační infrastruktury. Pro každý sektor lze pak podle potřeb zkoumat i související vertikální časti v závislosti na architektuře specializovaných IIoT komponent.

Tab. 3: Technické postupy (Zdroj: Zpracováno dle (6))

Řízení důvěry a integrity dat	**Poznámka**	**Hodnocení**
Je před instalaci SW kontrolována integrita a důvěryhodnost kódu?	Zaleží od provozu a zařízení.	Částečně
Je prováděna autentizace všech IIoT zařízení v rámci OT sítě?	Prokazuje se certifikátem nebo MAC adresou.	Částečně
Definují se bezpečné komunikační kanály mezi IIoT zařízeními? Je s tím obeznámen majitel aktiva?	Záleží na konkrétní technologii. OT protokoly částečně ne, v IT zpravidla ano.	Záleží od místa použití
Jsou definované whitelisty aplikací, které lze spouštět na ICS? Je tento seznam pravidelně obnovován?		Ano
Jsou všechny data patřičně šifrována? Jsou zavedené procesy a mechanizmy pro úschovu šifrovacích klíčů?	Jsou zaváděny certifikáty. Kromě PROFINETu.	Ano

Provádí se monitoring dat, které jsou "v klidu" a těch, které jsou na cestě za účelem identifikace nežádané modifikace?	V IT je zajištěné CIA a v OT je snaha o zavedení sondy anomálií.	Ano
Podnikatelská kontinuita a zotavení		
Je vypracován Business Continuity Plán a Disaster Recovery Plán? Jsou pravidelně kontrolovány a obnovovány?	Jednou ročně.	Ano
Jsou stanovené kritické podnikatelské a technické procesy a to, jaký mají vliv na podnikatelskou kontinuitu?		Ano
Je sepsán jasný postup toho, jak se vrátit k normálnímu stavu výroby? Je u jednotlivých kroků stanoveny role a odpovědnosti klíčových osob?		Ano
Je zaveden nouzový plán pro případ větších i menších bezpečnostních incidentů?		Ano
Jsou zohledněné třetí strany v BCP a DRP?	Probíhá oboustranné informování. Je v plánu specifičtější přístup.	Ano
Jsou stanovené důležité parametry pro chod firmy jako je potřebný čas na zotavení, potřebný bod zotavení, maximální délka odstávky a minimálné požadavek pro kontinuitu podnikání?		Ano
Machine-to-Machine bezpečnost		
Jsou dlouhodobé klíče uchovávané v HSM, které je připojené do M2M gatewaye pomocí fyzických a/nebo logických prostředků?	Jsou používané certifikáty.	Částečně
Jsou používané důvěryhodné kryptografické algoritmy pro zajištění CIA?	Stanoveno v interní dokumentaci.	Ano
Používají se komunikační protokoly, které dokážou rozeznat neautorizované opakovaní poslední zprávy?		Ne
Jsou zavedené whitelisty, které ověřují znaky vstupu před jejich zpracováním?		Ano
Ochrana dat		
Je pro data v jakémkoliv stavu zajištěná adekvátní ochrana buď za pomoci IAM, šifrování a tunelování?		Ano

Jsou OT data roztříděna do kategorií podle jejich kritičnosti a analýzy rizik?		Ano
Řídí se sdílení dat třetím stranám principem need-to-know?		Ano
Jsou pro přísně tajná data zavedené mechanizmy pro řízení šifrování a klíčů pouze pro zvolené jedince?		Ano
Jsou všechna přímá i nepřímá osobní data zpracována firemními systémy anonymizována?	Po zavedení GDPR.	Ano
Aktualizace Software/Firmware		
Je prováděna kontrola integrity SW/FW před tím, než se použije pro aktualizaci?	Jsou kontrolovány checksumy při automatické aktualizaci.	Vždy ne
Prověřuje se v případě automatických aktualizací, zda je to akceptovatelné z hlediska rizik a zda je zdroj aktualizací spolehlivý?		Ano
Instalují se záplaty IIoT zařízení pouze v případě, že neexistuje žádné negativní následky? Jsou tyto skutečnosti kontrolovány předem v kontrolovaném prostředí?		Ano
V případě, že aktualizace provádí třetí strana, je stanoven požadavek, že dotyčná strana dokáže doložit soulad s požadavky výše? Je po nich požadováno hlášení o všech aktivitách souvisejících s aktualizacemi?		Ano
Jsou legacy systémy, které nelze aktualizovat, zavedená patřičná kompenzační opatření jako je segmentace sítě, přemístěni systému a real-time monitoring?	Je snaha o segmentaci, zavádění whitelistů a hardening.	Ano
Správa přístupů		
Je segregován vzdálený přístup? Je pro něj vymezená jiná sada pravidel, včetně omezení současných připojení a plná sledovatelnost?		Ano
Je pro IIoT zavedená minimální míra autentizace včetně omezení přístupů mezi segmentovanými sítěmi?	Mají vlastní síť, komunikovat můžou, pokud je to schválené střediskem a musí se prokazovat certifikátem.	Ano

Je u všech IIoT používané MFA?	Některé IIoT tuto funkci nemají.	Částečně
Jsou při integraci zařízení změněny výchozí přístupové údaje? Jsou nová hesla přiměřeně komplikovaná pro daný případ užití?		Ano, tam kde to jde.
Je použit princip nejmenších přístupových práv pro nové uživatele? Jsou role dostatečně segregované?		Ano
Používají se sdílené účty pro přístup k IIoT zařízením a systémům?	Z legacy hlediska možná ano.	Jsou pravidla pro skupiny AD.
Jsou zavedené mechanizmy pro zablokování účtu v případě dosažení maximálního počtu chybných pokusů o přihlášení?		Ano
Je zaveden Privilage Access Management pro správu přístupových práv?		Ano
Jsou zavedená patřičná opatření pro fyzický přístup k budovám/místnostem/skříňkám? Je zaveden proces, který ihned odstraní přístupová práva pro končící zaměstnance?		Ano
Sítě, protokoly a šifrování		
Je šifrována IIoT komunikace tam, kde jeto možné a neovlivňuje to dostupnost a výkon?		Ano
Jsou průmyslové sítě segmentovány podle Purdue Modelu? Probíhá komunikace mezi administrativními a výrobními činnostmi skrze DMZ?		Ano
Je pro OT zavedená dostatečná mikrosegmentace s need-to-know principem?	V mezinárodních firmách je to na fyzické vrstvě složité.	Částečně
Jsou bezpečnostní sítě odděleny od administrativní a ovládací sítě?		Ano
Používají IIoT pouze trhem prověřené protokoly, které nemají známé zranitelnosti?		Ano
Při zavedení nových zařízení, kontroluje se kompatibilita podporovaných protokolů na úrovni zařízení či gatewaye?		Ano
Je stanoven limit na počet provozovaných protokolů?	Je snaha minimalizovat počet standardů a protokolů.	Ano

Je zavedená bezpečné prostředí pro výměnu a správu klíčů?		Ano
Je zajištěno efektivní použití kryptografie pro zajištění CIA dat?		Ano
Monitoring a audit		
Je zavedené pasivní monitorování pro IT a OT pro stanovení výchozí hodnoty síťového provozu?	Chystá se plošné zavedení.	Částečně
Sbírají se bezpečnostní logy (změny, chyby, výkon) k tomu, aby bylo možné sledovat a analyzovat události pomocí SIEM systému?		Ano
Jsou přístupová práva a konfigurace aktiv pravidelně kontrolována?	Všude, kde je to řízeno LDAPem.	Ano
Tam, kde je to možné, monitoruje se dostupnost IIoT zařízení v realtime?	FIOT se snaží o jeho zavedení.	Ne
Správa konfigurací		
Jsou zavedené výchozí bezpečnostní nastavení pro každý typ aktiva? Např. požadovaný SW, protokoly, porty a whitelisty aplikací)		Ano
Jsou používané pomocné nástroje pro řízení konfigurace? Tyto nástroje by měly umět obnovení aktiva do stavu před provedenou změnou.	Problém je OT síť a legacy systémy, v těchto případech jsou prováděny pravidelné zálohy.	Částečně
Jsou všechny změny konfigurace dokumentovány v souladu s pravidly řízení změn?	Viz otázka výše	Částečně
Je vyvinutý postup pro analýzu dopadu? Před implementací změny systému, je prováděna analýza pro stanovení kritičnosti zvažované změny?	Je zavedený proces, při kterém je informován i business owner.	Ano
Jsou u IIoT zakazované nepoužívané funkce, protokoly, porty a testovací módy?	Je provedený hardening.	Ano
Je zavedený obsáhlý plán zálohování s pravidelnými cykly a podmínkami pro tvorbu záloh a jejich testování?		Ano

Z technologického hlediska lze vidět legacy technologie a systémy, které byly zavedeny v průběhu celé své 125leté historie. Hlavní slabinou jsou industriální komunikační protokoly, které doposud počítali s plnou izolací od okolního světa, a tudíž nesledovali stejná bezpečnostní opatření, která se zaváděla v IT. Průmysl 4.0 začíná propojovat OT

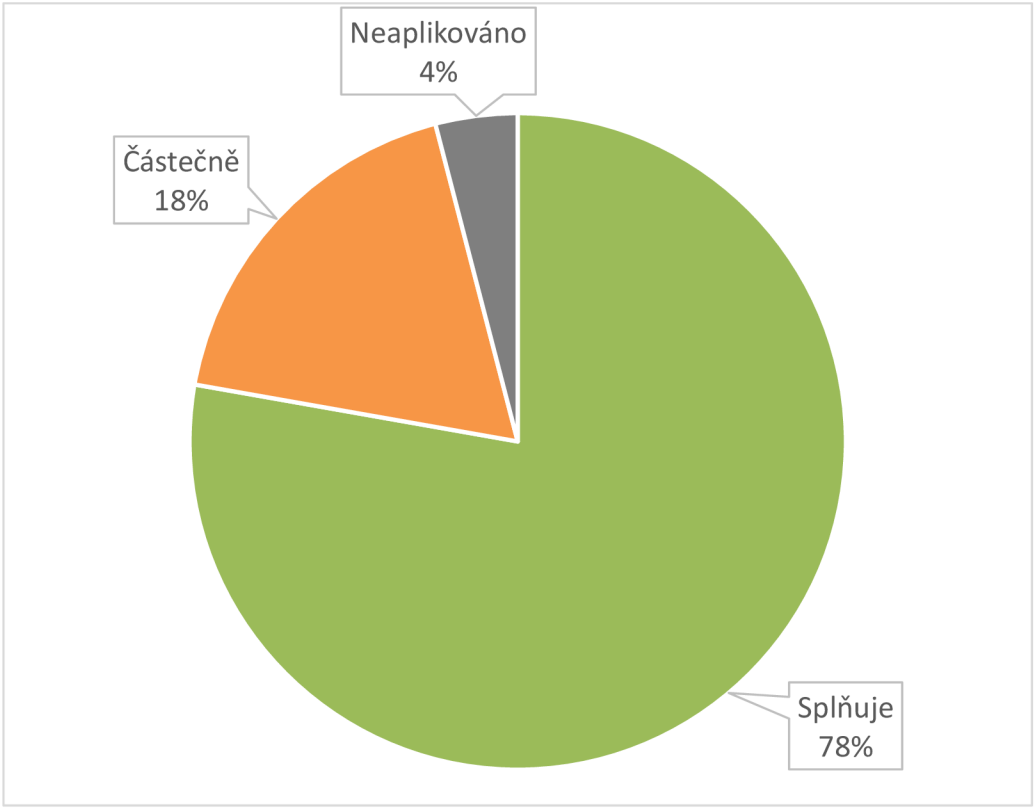
a IT vrstvy, což přináší povinnost implementovat dlouhodobé IT praktiky i do OT komunikace.

3 VLASTNÍ ZHODNOCENÍ A HYPOTÉZY

V této kapitole, zhodnotím analýzu současného stavu společnosti a toho, jak postupuje při implementaci nových technologií. Pomocí zhodnocení sepíšu možná rizika a hrozby, které vznikají při propojování IT a OT vrstev. Následuje namodelování možných následků na výrobní procesy v případě naplnění jednoho z možných rizik.

3.1 Závěry z asistovaného zhodnocení

V Graf 1 je znázorněný výsledek hodnocení dotazníku z předešlé kapitoly. Můžeme vidět, že firma má zavedenou stěžejní většinu (78 %) doporučených bezpečnostních opatření. Část doporučení (18 %) jsou zavedeny pouze z v necelém měřítku. Pouhá 4 % opatření nejsou dodržená. Z toho vyplývá, že společnost aktivně pracuje na ochraně svých informačních i IT aktiv.



Graf 1: Statistika asistovaného zhodnocení (Zdroj: Vlastní zpracování)

Za hlavní příčiny zjištěných nedostatků lze považovat:

- Protokol PROFINET zatím nedohnal nastalé změny na trhu a v technologiích. Téměř všechny průmyslové a výrobní technologie využívají tento protokol pro řízení montážní techniky a robotů. Dá se to považovat za slabinu celého podnikatelského odvětví, a nejen specifické firmy. V případě téhle firmy, jsou aplikované preventivní opatření naprostým odizolováním všech případů použití PROFINETu, kde to není obchodně opodstatněné či nutné. Níže rozeberu charakteristiky tohoto protokolu a výhledy do budoucna.
- Firma tíží technologický dluh, který je způsoben stářím podniku. To se projevuje hlavně u tzv. legacy systémů, které zatím nebyly modernizovány. U nich je obtížné aplikovat stejné metodiky a funkce, jak i u moderních řešení. Zrovna pomocí projektu FIOT má být jeden takový systém nahrazen. Ostatně, během sbíraní informací jsem zjistil, že takových případů je ve firmě ihned několik, což poukazuje na to, že vedení společnosti aktivně pracuje na nápravách.
- IIoT je nová technologie, která vyžaduje upravení dosavadních praktik a zavedení nových postupů, které změní vnímání dosud pevných hranic mezi IT a OT. Firma zatím nemá jasně dané postupy při zacházení s IIoT. Potíž často tkví také ve faktu, že pro personál, který byl zvyklý na dosavadní sadu technologií, je těžké adaptovat se k novým zařízením.

Příručka od ENISA má vypsáno ke každému doporučení i výčet možných scénářů, které mohou nastat v případě, že dané bezpečnostní opatření není použito. Pomocí nich a získaných odpovědí lze sestavit žebříček scénářů podle počtu jejich výskytu odvozených z odpovědí v otazníku. Pro zohlednění typu odpovědí Částečně/Neaplikováno použiji kombinaci kvalitativní a kvantitativní statistiky, kdy dopady plynoucí z odpovědi Neaplikováno mají dvojnásobnou váhu oproti odpovědi Částečně.

Tab. 4: Statistika výskytu možných scénářů (Zdroj: Vlastní zpracování)

Typ scénáře	*Hodnota*
Nežádaná činnost / Zneužití	21
Odposlech / Zachycení dat / Převzetí kontroly	21
Fyzický útok	14
Selhání / Poruchy	12

Neúmyslné škody	11
Právní postih	5
Výpadky	5
Kalamita	4

Každý druh scénáře pojednává několik druhů souvisejících hrozeb. Pokud se ovšem zaměříme pouze na FIOT projekt, některé scénáře nebudou mít kritické dopady navzdory tomu, že v tabulce výše mají vysoké hodnocení. Proto se musí rozlišovat míra pravděpodobnosti výskytu a míru možného dopadu. Například scénář typu Kalamita obsahuje skupiny hrozeb přírodní katastrofy (zemětřesení, povodně aj.) a vlivy na stroj působením prostředí (prach, výbuch, koroze aj.). Tyto scénáře jsou uniformní pro všechna technická aktiva firmy.

Následující scénář s nepravděpodobným dopadem je Právní postih, a to jednak z toho důvodu, že daná firma je výrobcem poslední instance, který skládá části jiných dodavatelů do hotového produktu a ten prodává koncovému zákazníkovi. Dalším důvodem je taky fakt, že FIOT nezpracovává osobní informace, nýbrž pouze stavové hodnoty strojů a výroby.

3.2 Stav protokolu PROFINET

PROFINET je průmyslovým ethernetovým otevřeným standardem sdružení PROFIBUS International (PI) a jeden z nejpoužívanějších standardů v automatizačních sítích.

Profinet je založen na průmyslovém Ethernetu, TCP/IP. Mezi jeho vlastnostmi vyniká ethernet v reálném čase, kde zařízení, která komunikují prostřednictvím sběrnice, spolupracují při zpracování požadavků v rámci dané sběrnice.

Základní konektivita, jako je ethernetový kabel je rovnocenná s úrovněmi 1 a 2 modelu OSI. Díky tomu nabízí tento protokol zlepšenou škálovatelnost v infrastruktuře. Použití ethernet sítě umožňuje snadněji propojovat a spravovat vzdálená zařízení například pomocí VPN.

V rámci tohoto standardu se nachází několik PROFINET protokolů, z nichž každý má svůj specifický účel. Mimo to lze PROFINET komunikaci rozdělit do tří služeb – standardní TCP/IP, Real Time a Isochronní Real Time.

Doposud se tento standard nezabýval implementací stejných bezpečnostních funkcí jak i IT komunikační protokoly. V takových případech se spoléhalo na izolaci PROFINET sítí od ostatních systémů pomocí IT technologií (45).

3.2.1 Plánovaný vývoj standardu

Vývoj trhu si vyžádal, aby výrobci průmyslových technologií se začali zabývat tématy, kterými doposud nemuseli. V roce 2019 organizace PI vydala whitepaper, který předkládá první možné řešení zavedení bezpečnostních prvků do rodiny protokolů PROFINET (46).

Je nutné si uvědomit, že tento standard dokáže pracovat v Real Time režimu a že kryptografické operace vyžadují jistou úroveň výpočetního výkonu proto, aby prodleva z ověření CIA byla co nejmenší. V průmyslovém nasazení je kladen největší důraz na dostupnost, která hraje největší roli při výrobních operacích.

V nových návrzích organizace řeší význam jednotlivých aspektů bezpečnosti informací. Souběžně s tím řeší i prostředí, ve kterých je standard používán. Po zvážení všech okolností organizace si stanovila tři bezpečnostní třídy k tomu, aby rozlišila případy, kde je nově přidaná bezpečnost postradatelná a tam, kde je naopak klíčová.

- 1. třída – Robustnost: Tato třída pouze mění dostupné možnosti dosavadních funkcí a možnosti nastavovat konfigurační příkazy jako „pouze ke čtení“. U této třídy zatím není pevně dáno, že se opravdu zavede.
- 2. třída – Integrita + Autentičnost: Kromě změn představených v první třídě, přidává tato třída i kryptografické operace zajišťující integritu a autentičnost dat.
- 3. třída – Důvěryhodnost: Poslední třída obsahuje změny prvních dvou a k tomu zajišťuje důvěryhodnost komunikace (46, s. 19).

Nové změny jsou navrženy tak, aby systémy všech tříd jsou dokážou vzájemně spolupracovat v rámci jedné sítě. Je to dané hlavně kvůli tomu, že u třídy dvě a výš nebude ve všech případech možné provést aktualizaci na SW úrovni. V průmyslu jsou zařízení navržená k tomu, aby vydrželi co nejdéle, a proto se počítá s tím, že nová zařízení

podporující vylepšené zabezpečení budou zaváděná v případech výměny odsloužených zařízení nebo rozšiřování stávající instalace (46, s. 20).

ŠKODA AUTO by proto měla začít sledovat vývoj plánovaných vylepšení standardu PROFINET, tak jak se ukázalo, že právě on narušuje téměř bezvadná opatření řízení bezpečnosti informací firmy.

3.3 Klasifikace možných rizik

Pro případ analýzy dopadů rizik se pro účely této práce zaměříme pouze na zkoumaný projekt FIOT, jehož cílem je monitorovat stav výroby a podávat informace všem potřebným osobám. V případě poruch či neoptimálních hodnot, systém podá oznámení údržbářům a ti pak po zvážení hlášených informací usoudí, jak nejlépe dále jednat. Zatím je většina rozhodovacích procesů v rukou zaměstnanců. V rámci tohoto projektu jsou obsaženy pouze IIoT senzory bez přidružených ovládačů, které se řídí snímanými hodnotami.

V klasifikaci rizik posuzuji jejich vlastnosti, jako je dopad, snadnost odhalení, možnost kaskádového efektu, ovlivněná aktiva, čas na zotavení a možné slabiny. U každé vlastnosti stanovím její závažnost – vysoká, střední či nízká, a toho, zda je pro podnik kritická. Všechna rizika jsou odvozená ze zjištěných slabin v dotazníku a jejich skutečná proveditelnost je pouze hypotetická, neboť pro potřeby této práce nebylo možné prozkoumat konkrétní bezpečnostní nastavení příslušných sítí.

3.3.1 Napadení na senzory

V tomto scénáři útočník napadne senzory a změní jejich konfiguraci k tomu, aby buď vykazovali pozměněné hodnoty, nebo změní limity přijatelných hodnot. Tím se vytváří jedná možná situace, kdy senzory chybně ukazují, že stav výroby je pod optimální hranici nebo že hrozí porucha. V obou případech je potřeba provést preventivní údržbu. Pokud senzory budou vykazovat lehce upravené hodnoty (v řádech jednotek procent) oproti běžným hodnotám, může to znamenat z dlouhodobého hlediska markantní nárůst provozních nákladů.

Druhým extrémem je situace, kdy senzory ukazují přijatelné hodnoty u zařízení, jejichž stav se blíží k výskytu poruchy či výpadku. V takovém případě je personál odpovědný za údržbu zaskočený, protože systém ukazoval běžné provozní hodnoty a nevyskytly se žádné signály, které by poukazovali na blížící se výpadek funkčnosti stroje.

Pro takové napadení je klíčové rozšíření se na co nejvíce zapojených senzorů, protože výstup jediného senzoru je snadno vykompenzován zbylými senzory, které stále vykazují reálné hodnoty.

- Dopad: střední – aby takový útok byl úspěšný musí být dlouhodobě neodhalený. Pokud je útok úspěšný, pak je odhalen až v momentě, kdy je možné porovnat provoz během doby od jeho zavedení s jinou odpovídající dobou provozu, kdy systémy fungovali správně.
- Snadnost odhalení: nízká až střední – jelikož se jedná o čistě monitorovací službu a výstupy senzorů jsou vyhodnocované ručně, je zde šance, že škody útoku zůstanou neodhaleny krátkou až středně dlouhou dobu. Poměrové statistiky mohou ukázat, že četnost poruch se meziměsíčně změnil.
- Kaskádový efekt: malý – napadení senzorů samo o sobě spoléhá na distribuci útoku do co možná největšího počtu koncových zařízení této sítě.
- Ovlivněná aktiva:
    - Senzory
    - Agregační střediska
    - Gatewaye
    - Rozhodovací procesy
    - Centrální vyhodnocovací systém
- Čas na zotavení: nízký až střední – doba na zotavení se odvíjí od napadeného místa a počtu ovlivněných senzorů. Jednotlivé senzory se pak musí prozkoumat a při odhalení nesouvislostí i opravit.

Jelikož se nejedná o službu, které se aktivně podílí na řízení výrobních procesů, nepovažuje se ani jedná z vlastnost jako kritická. Je potřeba dodat, že současné bezdrátové senzory nemají výpočetní kapacitu proto, aby používali stejné autentizační postupy, jako jiné výpočetní jednotky ve výrobě. Proto je jejich bezpečnost jen tak dobrá,

jak je fyzický přístup k nim a kvalita používaného bezdrátového komunikačního protokolu. Z hlediska klasifikace tohoto scénáře lze mluvit o zneužití, poruchách, odstávkách a převzetí kontroly.

Představení IIoT jen zjednodušil opakované výskyty útoků jako byl červ Stuxnet. Jeho cílem bylo napadení PLC zařízení značky Siemens v Iránském závodě pro obohacování uranu. Mezi největší výzvy bylo zavedení červu do sítě, která byla zcela odizolována od okolního světa. Provedené infikování se pak podařilo za pomocí chytře provedeného sociálního inženýrství. Úkolem červa bylo v pravidelných intervalech měnit rychlost otáček centrifug, které byly od základu navržené pro pevně dané parametry fungování a díky nečekaným změnám docházelo k častějším poruchám (47).

3.3.2 Průmyslová špionáž

V případě proaktivní údržby výrobních strojů se předpokládá, že do daného systému proudí data ze všech dotyčných zařízení, která se opotřebovávají. To znamená, že v takovém systému je z hlediska použité techniky detailně zmapovaný celý výrobní proces. Novodobé IIoT systémy také umožňují mít namodelované digitální dvojče výrobní linky k tomu, aby na obrazovkách zařízení bylo možné zobrazit virtuální reprezentaci toho, kde přesně dochází k problémům.

V tomto scénáři se pro útočníka jedná o velmi cenný zdroj dat, který zle použit pro další aktivity. Tento scénář je hodně blízký předešlému příkladu a může se považovat jako jeho logické rozšíření.

- Dopad: velký, kritický – následky takového útoku jsou zmíněné v přechozích odstavcích.
- Snadnost odhalení: střední – taková kompromitace administrativního systému lze odhalit správně zavedeným sledováním sítě a logováním všech její aktivit.
- Kaskádový efekt: velký – když útočník má k dispozici téměř mapu výrobních linek, usnadní se mu postup v následujících útocích
- Ovlivněná aktiva:
    - Síťové prvky
    - Monitorovací systém

    - Databáze
    - Citlivé informace
- Čas na zotavení: nízký – smyslem špionáže je pravidelně získávat data a nijak jinak s nimi nemanipulovat. Jestli správci bezpečnosti IT odstraní únikový bod(y) informací a zdroj útoku, vyřeší se tím i daná hrozba.

V dnešní době je průmyslová špionáž velice častým důvodem kybernetických útoků. Tajné informace mezinárodních společností jsou velmi cenné na černých trzích a také pro nepoctivé konkurenty ve stejném odvětví. Tento scénář lze kategorizovat čistě jako odposlech, zachycení dat a právní postih.

3.3.3 Pivot na OT zařízení

Doposud byly OT sítě zcela odděleny od IT sítí. Z High level reference modelu v Obr. 5 víme, že IoT vrstva slouží jako mezičlánek mezi těmito dvěma sítěmi. Jak už bylo uvedeno v sekci pro PROFINET, OT technologie nejsou připravené k tomu, aby byly napřímo propojené s internetem. IoT nyní představuje mnohem větší útočnou plochu pro napadení OT sítí. V tomto případě může útočník využít slabin IIoT systémů a zařízení k tomu, aby se laterálně přesunul na OT zařízení, jelikož některé OT protokoly nejsou navržené pro dodržování CIA. Poté může útočník převzít kontrolu nad výrobními stroji a napáchat značnou škodu nejen v digitálním prostranství.

- Dopad: velký, kritický – zásah do OT sítě znamená přístup k robotům, které mohou při nesprávném zacházení napáchat fyzickou škodu sobě a svému okolí.
- Snadnost odhalení: velká – útok se odhalí už v momentě, kdy se ramena na montážní lince začnou chovat chaoticky a provádět neočekávané činnosti.
- Kaskádový efekt: malý – stejně jak i u senzorů v prvním scénáři, tak i zde se jedná o zařízení, na které se útočník dostane právě kaskádovým efektem.
- Ovlivněná aktiva:
    - Síťové prvky
    - IIoT systémy a/nebo zařízení
    - Robotická ramena a montážní stroje
    - PLC

- Čas na zotavení: vysoký – v případě fyzických poruch na několika strojích by zabralo dlouhou dobu na obnovení výroby, protože poškozené části se musí nejdříve vyměnit a znovu nakonfigurovat k tomu, aby se zabránilo opakované poruše zapříčiněnou zkorumpovaným zdrojovým kódem.

Tento případ je považován jako nejhorší ze všech možných. Zároveň je nejméně pravděpodobný z důvodu množství kroků, které musí útočník úspěšně učinit k tomu, aby se dostal do momentu, kdy může alespoň částečně ovládat stroje. Nicméně to neznamená, že by se tento scénář měl podceňovat. Navzdory neustálému propojování IT s OT vrstvou, musí systémoví administrátoři usilovat o co možná nejmenší styčné plochy mezi těmito dvěma technologiemi.

3.4 Ukázkový případ

Pro názornou ukázku dopadu provedu kalkulaci změn finančních nákladů, pokud se naplní první scénář. V přídě Iránského závodu a červa Stuxnetu se jednalo o plánované roční nahrazování 10 % z 8700 centrifug z důvodu opotřebení. Až po inspekci Mezinárodní agentury pro atomovou energii se zjistilo, že reálné nahrazování centrifug liší o 200 až 1200 kusů oproti plánu. Důvodem tohoto rozdílu byl vliv červa, který v pevných časových intervalech zmenšoval a zvětšoval za hranice limitů otáčky centrifug vedoucích k rychlejšímu opotřebení (47).

Pro ukázkový příklad použijeme podobný princip s menší variaci k tomu, aby podobný útok byl proveditelný i během neustálého monitorování a sledovací logiky, která hlásí extrémní výkyvy.

Pro ukázku použiji montážní oddělení, kde je nyní v provozu 30 zdrojů. Jednotlivé zdroje je potřeba při poruše opravit či vyměnit. Pro potřeby této práce nesmím zveřejnit přesné peněžní částky vynaložené za materiál a jednotlivých pracovních činností. Ostatně v tomto případě nejsou důležité konkrétní rozdíly, ale výsledné procentuální změny nákladů.

Předpokládejme, že výměna/oprava zdroje stojí 1000€ a měsíčně se porouchá v průměru šest zdrojů. Pokud se výstupní hodnoty změní podle předem dané logiky, jednalo by se

v tomto případě o nepravidelné měnění snímaných hodnot. Dá se předpokládat, že změna ovlivněných zdrojů se bude chovat podle Gaussova rozdělení se střední hodnotou 15 a směrodatnou odchylkou 10. V Tab. 5 je možné vidět to, jak po dobu jednoho roku upravené hodnoty mohou změnit celkové náklady za údržbu. V tomto namodelovaném případě vyšla změna 27 % nárůstu nákladů. Do toho se nepočítá ušlý zisk z toho, že stroj připojený ke zdroji, je během jeho opravy nečinný, a tudíž se pozastavila výroba.

Tohle je jen ukázka dopadu jednoho oddělení, pokud by podobná situace nastala všude, kde je zapojený FIOT systém, pak bude rozdíl v nákladech mnohem vyšší.

Tab. 5: Kalkulace možného dopadu napadení senzorů (Zdroj: Vlastní zpracování)

	Leden	*Únor*	*Březen*	*Duben*	*Květen*	*Červen*	*Červenec*
Počet oprav zdrojů	5	6	4	7	8	3	5
Celkové náklady	5 000 €	6 000 €	4 000 €	7 000 €	8 000 €	3 000 €	5 000 €
Koeficient změny	12 %	14 %	42 %	19 %	15 %	60 %	10 %
Počet výměn po napadení senzorů	6	7	6	9	10	5	6
Celkové náklady po napadení	6 000 €	7 000 €	6 000 €	9 000 €	10 000 €	5 000 €	6 000 €
Absolutní rozdíl nákladů	1 000 €	1 000 €	2 000 €	2 000 €	2 000 €	2 000 €	1 000 €
Relativní rozdíl nákladů	20 %	17 %	50 %	29 %	25 %	67 %	20 %

Srpen	*Září*	*Říjen*	*Listopad*	*Prosinec*	***Celkem***
5	6	7	1	9	**66**
5 000 €	6 000 €	7 000 €	1 000 €	9 000 €	**66 000 €**
17 %	10 %	23 %	17 %	18 %	**-**
6	7	9	2	11	**84**
6 000 €	7 000 €	9 000 €	2 000 €	11 000 €	**84 000 €**
1 000 €	1 000 €	2 000 €	1 000 €	2 000 €	**18 000 €**
20 %	17 %	29 %	100 %	22 %	**27 %**

ZÁVĚR

Motivací pro vypracování této diplomové práce bylo zjištění, že nové technologie označované jako „internet věcí“ jsou často podceňované z hlediska bezpečnosti. Od roku 2009 kdy se stal jeden z prvních závažnějších útoků na IoT síť se jejich četnost s každým rokem zvětšovala. Zatímco spotřebitelská IoT zařízení otevírají cesty k loupežím digitálních dat osobního charakteru, v průmyslu hrozí fyzická poškození a značné finanční postihy.

Hlavním cílem této diplomové práce bylo poukázat na možné dopady bezpečnosti nových IIoT na proaktivní správu firemních aktiv k tomu, aby ve zvolené firmě měli konkrétnější podklady pro argumentaci, proč je bezpečnost internetu věcí velmi důležité téma. K tomu jsem vycházel z informací o projektu, jehož cílem je zavést aktivní monitoring výrobních linek. Se stejnou bází dat lze zavést i prediktivní údržbu strojů, jelikož některé nadcházející poruchy jsou zřetelné z průběžně degradujícím měřeným hodnotám. V rámci tohoto projektu firma zavádí IIoT technologie, pro sledování dosud neměřených hodnot. Jako zdroje informací jsem použil dokumentaci tohoto projektu a také rozhovory s ostatními zaměstnanci, kteří odpovídají za plnění jeho úkolů.

K lepšímu pochopení zabezpečení prostředí, do kterého je FIOT integrován jsem použil příručku od ENISA, která popisuje doporučené praktiky pro zabezpečení IIoT technologií. Tyto doporučení jsem pak přeměnil do podoby dotazníku pro metodu asistovaného zhodnocení. Během sbírání informací pro dotazník jsem narazil na dvě témata, která firmě narušují téměř výborný stav řízení informační bezpečnosti.

Díky asistovanému zhodnocení jsem mohl zhodnotit náchylnost společnosti na možné kategorie hrozeb. Z toho jsem vytvořil tři hypotetické scénáře útoků a toho, jaký by měli dopad na firemní aktiva a jejich údržbu.

Ve finále jsem vzal jeden scénář a propočítal ukázkový model toho, jak by dlouhodobé ovlivnění výstupů senzorů se promítne na výsledných ročních nákladech společnosti za údržbu.

CITOVANÁ LITERATURA

(1) SCHMITZ, Constanze a Fabian WANKE. Industrie 4.0. *Automa* [online]. 2019, **25**(2-3), 67-69 [cit. 2020-05-05]. ISSN 1210-0592. Dostupné z: https://www.pablikado.cz/dokument/T3UJ1zHoDtEq0diO

(2) KAGERMANN, Henning, Wolf-Dieter LUKAS a Wolfgang WAHLSTER. Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution. *VDI nachrichten*. 2011, **2011**(1311), 2.

(3) BARTODZIEJ, Christoph Jan. *The Concept Industry 4.0*. Wiesbaden: Springer Fachmedien Wiesbaden, 2017. DOI: 10.1007/978-3-658-16502-4. ISBN 978-3-658-16501-7.

(4) *Good Practices for Security of Internet of Things: in the context of Smart Manufacturing* [online]. Brussels: European Union Agency For Network and Information Security, 2018 [cit. 2020-05-06]. Dostupné z: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

(5) HOFMANN, Erik a Marco RÜSCH. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry* [online]. Elsevier B.V, 2017, **89**, 23-34 [cit. 2020-05-04]. DOI: 10.1016/j.compind.2017.04.002. ISSN 0166-3615. Dostupné z: https://doi.org/10.1016/j.compind.2017.04.002

(6) *Good practices for security of Internet of things in the context of smart manufacturing* [online]. Luxembourg: European Union Agency for Network and Information Security, 2018 [cit. 2020-05-29]. DOI: 10.2824/851384. ISBN 9789292042615. Dostupné z: http://publications.europa.eu/publication/manifestation_identifier/PUB_TP0418940ENN

(7) Industry 4.0: Definition, Design Principles, Challenges, and the Future of Employment. *Cleverism* [online]. Mountain View: CLEVERISM, 2020 [cit. 2020-05-05]. Dostupné z: https://www.cleverism.com/industry-4-0/

(8) BARROS, Alistair a Daniel OBERLE. *Handbook of Service Description: USDL and Its Methods*. 2012. Boston, MA: Springer US, 2012. DOI: 10.1007/978-1-4614-1864-1. ISBN 9781461418634.

(9) LYDON, Bill. RAMI 4.0: Reference Architectural Model for Industrie 4.0. *InTech* [online]. Durham: International Society of Automation, 2019, **66**(2), 30-33 [cit. 2020-05-04]. ISSN 0192303X. Dostupné z: http://search.proquest.com/docview/2209840151/

(10) SCHWEICHHART, Karsten. *Reference Architectural Model Industrie 4.0 (RAMI 4.0): An Introduction* [prezentace]. Plattform Industrie 4.0, 2016. Dostupné z: https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf

(11) *Baseline Security Recommendations for IoT: in the context of Critical Information Infrastructures* [online]. Athens, Greece: European Union Agency For Network and Information Security, 2017 [cit. 2020-05-06]. Dostupné z: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

(12) FAGAN, Michael, William FISHER, Naomi LEFKOVITZ, Katerina N. MEGAS, Ellen NADEAU a Ben PICCARRETA. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [online]. Gaithersburg, 2019 [cit. 2020-05-06]. NISTIR 8228. Dostupné z: https://doi.org/10.6028/NIST.IR.8228. Sbírka doporučení. National Institute of Standards and Technology.

(13) *Internet of Things (IoT) Ecosystem Study* [online]. Piscataway, 2015 [cit. 2020-05-07]. Dostupné z: https://standards.ieee.org/content/dam/ieee-

standards/standards/web/documents/other/iot_ecosystem_exec_summary.pdf. Executive Summary. Institute of Electrical and Electronics Engineers.

(14) *Unipi* [online]. Brno: UniPi.technology, 2020 [cit. 2020-05-07]. Dostupné z: https://www.unipi.technology/cs/

(15) CHOMYŠYN, Maxim. *Výběr a návrh implementace informačního systému za účelem zlepšení toku informací ve zvolené společnosti* [online]. Brno, 2018 [cit. 2020-05-29]. Dostupné z: https://primo.lib.vutbr.cz/permalink/f/1roshr/420BUT_DSpace11012/83477. Bakalářská práce. Vysoké učení technické v Brně. Fakulta podnikatelská.

(16) ROWLEY, Jennifer. The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science* [online]. 2007, **2007**(33), 163-180 [cit. 2018-05-06]. DOI: 10.1177/0165551506070706. Dostupné z: https://doi.org/10.1177/0165551506070706

(17) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(18) GOGELA, Robert. *Standardy a definice pojmů bezpečnosti informací* [online]. CyberSecurity.CZ [cit. 10.05.2020]. Dostupné z: https://www.cybersecurity.cz/data/gogela.pdf

(19) Vyhláška č. 82/2018 Sb o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitos-tech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. Praha, 2018, ročník 2018, částka 43, číslo 82. ISSN 1211-1244.

(20) ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Pátá edice. Ženeva: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

(21) Breaking Down IoT Standards and Protocols. *IoT For All* [online]. Washington, DC: LEVEREGE, 2020 [cit. 2020-05-08]. Dostupné z: https://www.iotforall.com/glossary-iot-standards-and-protocols/

(22) IoT Standards and Protocols. *Postscapes* [online]. Seattle: Postscapes, 2020 [cit. 2020-05-08]. Dostupné z: https://www.postscapes.com/internet-of-things-protocols/

(23) Protokol MQTT: komunikační standard pro IoT. *Root.cz* [online]. Praha: Internet Info, s.r.o., 2020 [cit. 2020-05-08]. Dostupné z: https://www.root.cz/clanky/protokol-mqtt-komunikacni-standard-pro-iot/

(24) CYNTHIA, J., H. PARVEEN SULTANA, M. SAROJA a J. SENTHIL. Security Protocols for IoT. *Ubiquitous Computing and Computing Security of IoT* [online]. Cham: Springer, 2019, s. 1-28 [cit. 2020-05-09]. ISBN 978-3-030-01566-4. Dostupné z: https://doi.org/10.1007/978-3-030-01566-4

(25) Zákon č. 181/2014 Sb.: ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014. ISSN 1211-1244.

(26) ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Druhé vydání. Ženeva: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(27) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Druhé vydání. Ženeva: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(28) 125 let ŠKODA AUTO. *ŠKODA Storyboard* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2020 [cit. 2020-04-22]. Dostupné z: https://www.skoda-storyboard.com/cs/serialy/125-let-skoda-auto/

(29) 10 Oldest Car Companies In The World: Most of these automotive companies are over a hundred years old, and their legacies continue even to this day and age. *HotCars* [online]. Quebec, Kanada: Valnet, 2020 [cit. 2020-04-22]. Dostupné z: https://www.hotcars.com/10-oldest-car-companies-in-the-world/

(30) Škodovka svým exportem napomáhá držet zahraniční obchod v přebytku. *Kurzy.cz* [online]. Praha: AliaWeb, spol. s r.o., 2020 [cit. 2020-04-22]. Dostupné z: https://www.kurzy.cz/zpravy/481011-skodovka-svym-exportem-napomaha-drzet-zahranicni-obchod-v-prebytku/

(31) ČÍSLO MĚSÍCE: 5: Pátý rok po sobě dodala loni ŠKODA AUTO zákazníkům přes jeden million vozů. Pětka je proto prvním číslem v novém seriálu ŠKODA Storyboard Číslo měsíce. *ŠKODA Storyboard* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2022 [cit. 2020-04-22]. Dostupné z: https://www.skoda-storyboard.com/cs/modely/cislo-mesice-5/

(32) Výpis z obchodního rejstříku: ŠKODA AUTO a.s., B 332 vedená u Městského soudu v Praze. *Veřejný rejstřík a Sbírka listin - Ministerstvo spravedlnosti České republiky* [online]. Praha: Ministerstvo spravedlnosti České republiky, 2015 [cit. 2020-04-14]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=47718&typ=PLATNY

(33) Historie | ŠKODA AUTO a.s.: NAŠE DĚDICTVÍ. *ŠKODA AUTO a.s.* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2020 [cit. 2020-04-14]. Dostupné z: https://www.skoda-auto.cz/o-nas/historie

(34) Kde všude je ŠKODA AUTO doma: ŠKODA AUTO je firma s globální působností. I když jejím domovem je stále Česká republika, vozy s okřídleným šípem ve znaku opouštějí výrobní linky i v jiných zemích a dokonce na jiných kontinentech. *ŠKODA Storyboard* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2020 [cit. 2020-04-22]. Dostupné z: https://www.skoda-storyboard.com/cs/modely/kde-vsude-je-skoda-auto-doma/

(35) ŠKODA AUTO vyrobila dvanáctimiliontou převodovku současné generace. *ŠKODA Storyboard* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2020 [cit. 2020-04-22]. Dostupné z: https://www.skoda-storyboard.com/cs/tiskove-zpravy-archiv/skoda-auto-vyrobila-dvanactimiliontou-prevodovku-soucasne-generace/

(36) *Úvodní školení ŠKODA AUTO*. Mladá Boleslav, 2020.. Prezentace před nástupem na stáž.

(37) ŠKODA Výroční zpráva 2015. *ŠKODA Storyboard* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2020 [cit. 2020-04-23]. Dostupné z: https://cdn.skoda-storyboard.com/2016/05/skoda-annual-report-2015-1.pdf

(38) ŠKODA Výroční zpráva 2018. *ŠKODA Storyboard* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2020 [cit. 2020-04-23]. Dostupné z: https://cdn.skoda-storyboard.com/2019/03/SKODA_2018_CZE.pdf

(39) *Nahlédněte s námi do Průmyslu 4.0* [interní web]. Mladá Boleslav: ŠKODA AUTO, 2017 [cit. 2020-05-21].

(40) HOMOLKA, David a Tomáš COUFAL. *Systémová specifikace: FIOT Platform*. Mladá Boleslav, 2019.

(41) *Systémová specifikace: Lisovna Condition Monitoring - PXL1*. Mladá Boleslav, 2019.

(42) *Systémová specifikace: FIOT PSW Condition Monitoring*. Mladá Boleslav, 2019.

(43) *Systémová specifikace: montáž M1 Condition Monitoring*. Mladá Boleslav, 2020.

(44) ŠKODA AUTO A.S. *Všeobecné nákupní podmínky ŠKODA AUTO a.s.* CZE 01/19. Mladá Boleslav: oddělení BA, 2019, **2019**. Dostupné z: https://www.vwgroupsupply.com/one-kbp-pub/media/shared_media/documents_1/einkaufsbedingungen/_koda_auto_a_s_/e

inkaufsbedingungen__koda_auto_a_s____allgemeine_beschaffung/Veobecn_nkupn_podmnky_KODA_AUTO_as.pdf

(45) Features and security in PROFINET. *INCIBE* [online]. León: INCIBE, 2020 [cit. 2020-05-29]. Dostupné z: https://www.incibe-cert.es/en/blog/features-and-security-profinet

(46) *Security Extensions for PROFINET: Security Extensions for PROFINETPI White Paper for PROFINET* [online]. 1.05. Karlsruhe: PROFIBUS Nutzerorganisation e. V. (PNO), 2019. Dostupné také z: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=87331&token=813b3b162034298abe7b5660d6cdf22260f7a73b

(47) Příchod hackerů: příběh Stuxnetu. *Root.cz* [online]. Praha: Internet Info, s.r.o., 2020 [cit. 2020-05-30]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

(48) Historie loga | ŠKODA AUTO a.s.: Od názvu značky Laurin & Klement k dnešní ŠKODA. In: *ŠKODA AUTO a.s.* [online]. Mladá Boleslav: ŠKODA AUTO a.s., 2016 [cit. 2020-04-14]. Dostupné z: https://www.skoda-auto.cz/o-nas/historie-loga

(49) PELINO, Michele a Paul MILLER. *The Forrester Wave™: Industrial IoT Software Platforms, Q4 2019: The 14 Providers That Matter Most And How They Stack Up*. Cambridge, USA, 2019.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

IoT	Internet of Things
IIoT	Industrial Internet of Things
CPS	Cyber Physical Systems
IoS	Internet of Services
RAMI 4.0	Reference Architecture Model Industrie 4.0
PLC	Programmable Logic Controller
PAC	Programmable Automation Controller
M2M	machine-to-machine
IT	Informační technologie
OT	Operační technologie
NIST	National Institute of Standards and Technology
ENISA	Evropská agentura pro bezpečnost sítí a informací
ISO	Mezinárodní organizace pro standardizaci
ISMS	Systém řízení informační bezpečnosti
PDCA	Plan, Do, Check, Act
ICS	Industrial Control System

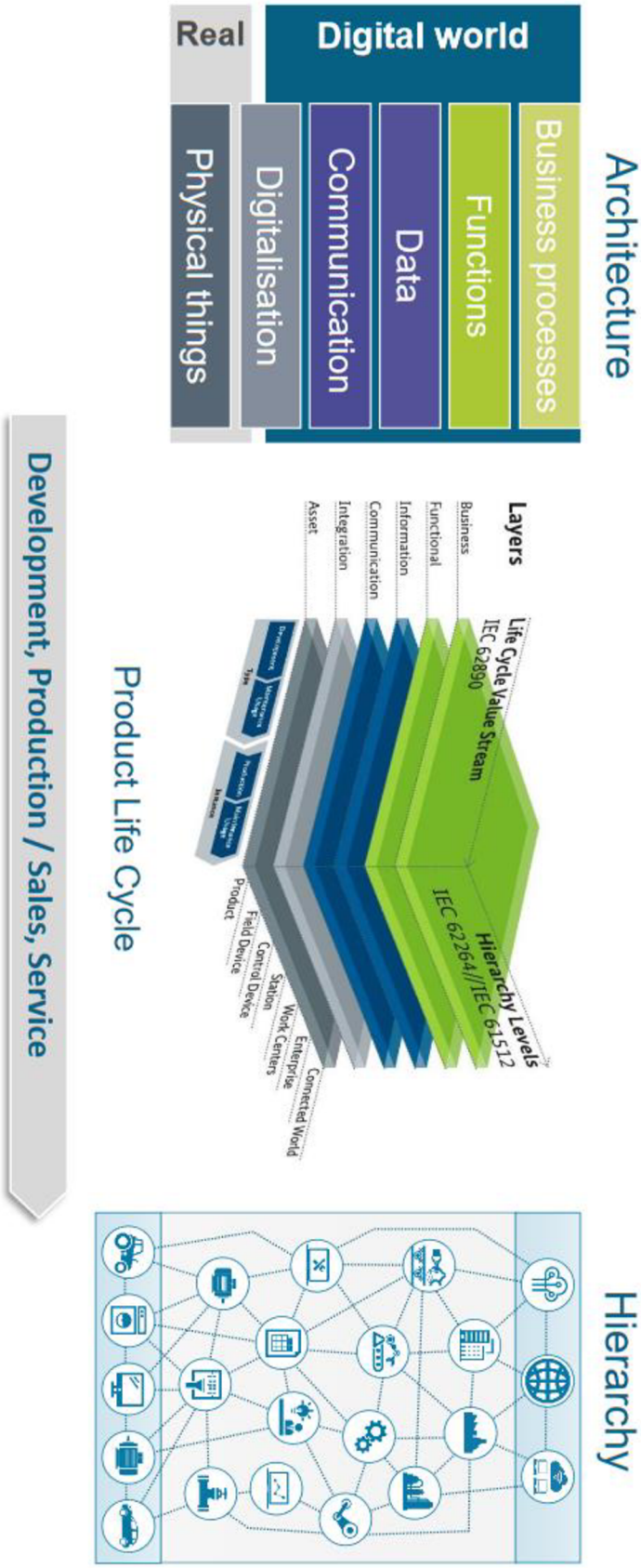
SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ

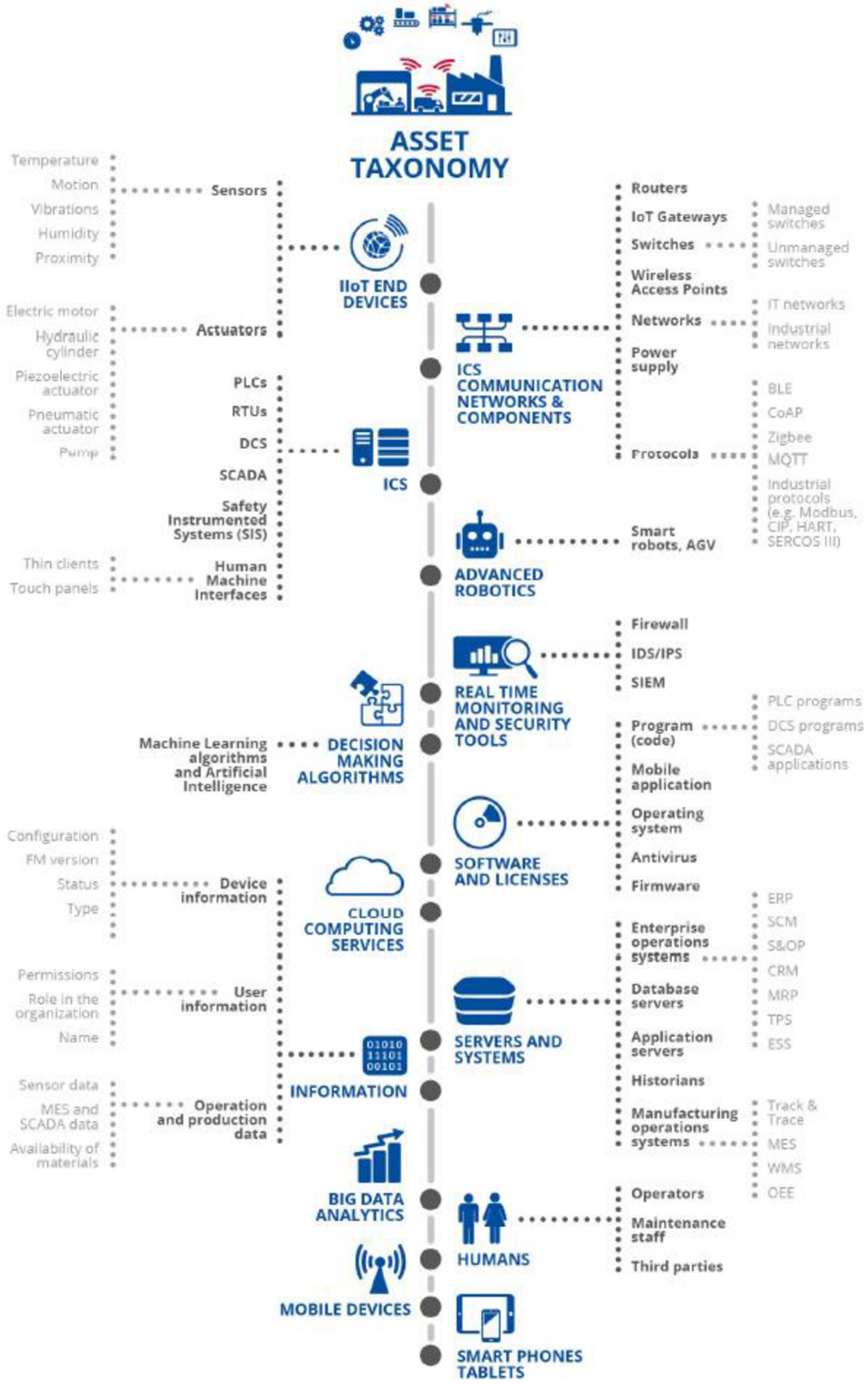
SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha 1: Rozšířené RAMI 4.0 (Převzato z 7, s. 41)



Příloha 2: ENISA taxonomie aktiv (Převzato z 12, s.21)



Příloha 3: ENISA taxonomie hrozeb (Převzato z 12, s. 27)