Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Obor: Bezpečnostní a informační systémy

Bezpečnostní rizika projektů "Smart Cities"

Bakalářská práce

Vypracoval: Jakub Langer
Vedoucí: Ing. Hana Kopáčková, Ph.D.

2018

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub Langer**
Osobní číslo:	**E14827**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Bezpečnostní rizika projektů "Smart Cities"**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je shrnutí bezpečnostních rizik projektů "Smart Cities" na základě mezinárodní literární rešerše.

Osnova práce:
- Základní pojmy a definice
- Charakteristika bezpečnostních rizik dle typu projektu Smart City
- Problematika ochrany soukromí

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

NAM, T., PARDO, T. A. Smart city as urban innovation: Focusing on management, policy, and context. In Proceedings of the 5th international conference on theory and practice of electronic governance, 2011, pp. 185-194.
CARAGLIU, A., DEL BO, C., NIJKAMP, P. Smart cities in Europe. Journal of urban technology, 2011, 18.2: 65-82.
EDWARDS, L. Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective. CREATe Working Paper 2015/11 (December 2015)
SAUNDERS, T., BAECK, P. Rethinking Smart Cities from the Ground up. Nesta, 2015.

Vedoucí bakalářské práce: **Ing. Hana Kopáčková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2017**

Termín odevzdání bakalářské práce: **30. dubna 2018**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 1. září 2017

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách) ve znění pozdějších předpisů a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne

PODĚKOVÁNÍ:

Tímto bych rád poděkoval své vedoucí práce Ing. Haně Kopáčkové, Ph.D. za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá problematikou Smart cities a technologií IoT a Cloud z hlediska bezpečnosti. Autor uvádí několik konceptů Smart city a popisuje jejich zranitelná místa i možná protiopatření na základě mezinárodní rešerše.

KLÍČOVÁ SLOVA

inteligentní město, internet věcí, Cloud, inteligentní sítě, inteligentní vozidla, inteligentní budovy

ANNOTATION

This bachelor thesis deals with the issues of Smart cities and IoT and Cloud technologies in terms of safety. The author introduces several Smart city concepts, describing their vulnerabilities and possible countermeasures based on an international research.

KEYWORDS

Smart city, IoT, Cloud, Smart grid, UAV, BAS, Smart car

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

IoT	internet věcí
UDS	unified Diagnostic Services
SG	smart grid
MITM	man in the middle
ECU	elektronická řídicí jednotka
DoS	denial of service
GPS	globální poziční systém
WSN	wireless sensor network
RFID	radio-frequency identification
M2M	machine to machine
API	application programming interface
AES	advanced Encryption Standard
IP	internet Protocol
TCU	transmission control unit
ISP	internet service provider
LVV	letecká veřejná vystoupení
UAS	bezpilotní letadlo
LČPVP	letecké činnosti pro vlastní potřebu

ÚVOD

V současné době polovina z celkového počtu obyvatel žije ve městech. Svět je na nebývalé úrovni urbanizace. Expanze měst čelí mnoha problémům. Ačkoli města zabírají méně než dvě procenta z pevniny na zemi, obyvatelé měst spotřebovávají více než tři. Problémy vyplývající z rychlé urbanizace ukazují ztrátu základních funkcionalit: například obtíže při nakládání s odpady, nedostatek zdrojů, znečištění ovzduší, dopravní zácpy atd. Aby se zabránilo tomu, že rychlá urbanizace bude krizí, musí města fungovat inovativním způsobem. Za tímto účelem byl vytvořen koncept inteligentního města jako nový přístup k rozvoji měst. [1]

Inteligentní města jsou perspektivní, progresivní a účinně využívají zdroje zároveň přináší vysokou kvalitu života. Podporuje sociální a technologické inovace a propojení stávajících infrastruktur. Obsahuje nové energetické a dopravní koncepce, které ve velké míře nezatěžují životní prostředí. [4] Existuje mnoho definic například:

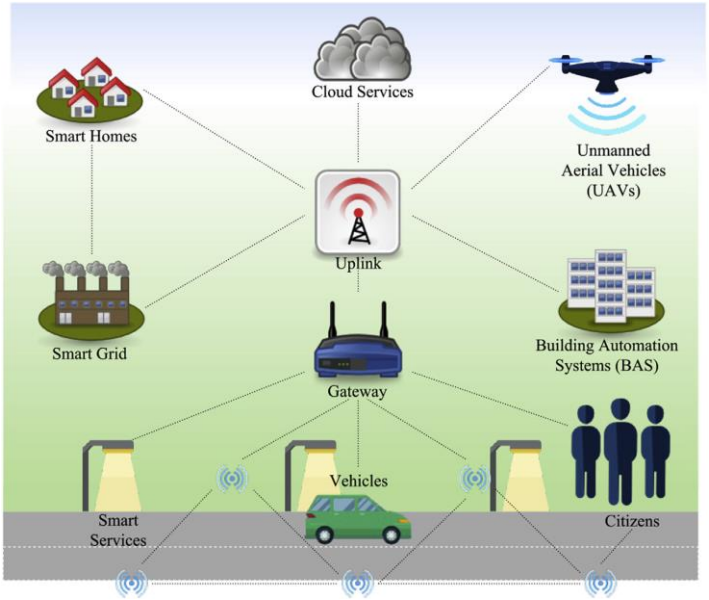
- Inteligentní město jako vysoce náročné a pokročilé město, které spojuje lidi, informace a městské prvky využívající nové technologie za účelem vytvoření udržitelného, ekologického a konkurenceschopného místa pro inovativní obchod a zvýšenou kvalitu života. [5]
- (Inteligentní) města jako území s vysokou kapacitou pro učení a inovace, která jsou postavena na kreativitě jejich obyvatel, jejich institucí vytváření znalostí a jejich digitální infrastruktury pro komunikaci a řízení znalostí. [6]
- Město, které monitoruje a integruje podmínky všech svých kritických infrastruktur včetně silnic, mostů, tunelů, kolejnic, podchodů, letišť, námořních přístavů, komunikací, vody, energie, dokonce i hlavní budovy. Lépe optimalizuje své zdroje, plánuje preventivní údržbu a sleduje bezpečnostní aspekty a maximalizuje služby svým občanům. [7]
- Inteligentní města mají vysokou produktivitu, protože mají relativně vysoký podíl vzdělaných občanů, pracovní místa náročná na znalosti, orientovaná na výstupy systémů plánování, tvůrčí činnosti a orientaci na udržitelnosti iniciativ. [8]
- Inteligentní město je městská oblast, která spojuje lidi, informace a technologie s cílem zvýšit kvalitu života. Inteligentní města jsou ty komunity, které usilují o udržitelný hospodářský rozvoj prostřednictvím investic do lidského a sociálního kapitálu a řídí přírodní zdroje prostřednictvím participačních politik. Inteligentní

město monitoruje podmínky a integruje kritické infrastruktury, jako jsou mosty, tunely, silnice, metro, letiště, námořní přístavy a budovy. Inteligentní město se rozděluje na 6 kategorií a těmi jsou: [9]

- Inteligentní ekonomika
- Inteligentní lidé
- Inteligentní správa
- Inteligentní mobilita
- Inteligentní prostředí
- Inteligentní bydlení

Pro svou rešerši jsem se rozhodl využít poslední uvedenou definici od autorů Vito Albino, Umberto Berardi a Rosa Maria Dangelico. Důvodem mého rozhodnutí je, že dle mého názoru nejvíce vystihuje situaci smart cities a je správně rozdělena do podkategorií, které jsou v takto obsáhlém tématu nezbytné.

Protože cílem mé práce je shrnout bezpečností rizika projektů inteligentního města, tak se budu zabývat čtyřmi složkami z výše uvedených 6 kategorií, které jsou nejvíce riziky ohroženy. Těmi jsou inteligentní sítě (Inteligentní prostředí), systémy automatizace budov (Inteligentní bydlení), bezpilotní prostředky (Inteligentní mobilita) a inteligentní vozidla (Inteligentní mobilita).



Obrázek 1: Inteligentní město

Zdroj [27]

1. POSTUP VYTVOŘENÍ REŠERŠE

Cílem mé práce je shrnutí bezpečnostních rizik projektů "Smart Cities" na základě mezinárodní literární rešerše. Existuje mnoho definic a rozdělení problematiky smart city. Já jsem si pro svou práci využil podsložky tří ze šesti kategorií z definice od Vito Albino, Umberto Berardi a Rosa Maria Dangelico, těmi jsou inteligentní sítě (smart grid), inteligentní budovy (BAS), inteligentní auta (smart car) a UAV (bezpilotní letadla alias drony).

Rešerši jsem prováděl v digitálních knihovnách a webech:

- Web of Science
- Scopus
- ScienceDirect
- ResearchGate
- Ieeexplore

Využil jsem vyhledávací metodu klíčových slov, kterými jsou: smart city, security in smart city, smart cities, security in smart cities, UAV, security issues in UAV, BAS, security issues in BAS, smart car, security issues in smart car, Smart grid, security issues in smart car, internet of things, Cloud. Nalezené dokumenty jsem analyzoval na z informací v nadpisu a abstraktu. Na základě těchto analýz jsem provedl užší výběr dokumentů, které jsem podrobně prostudoval a použil.

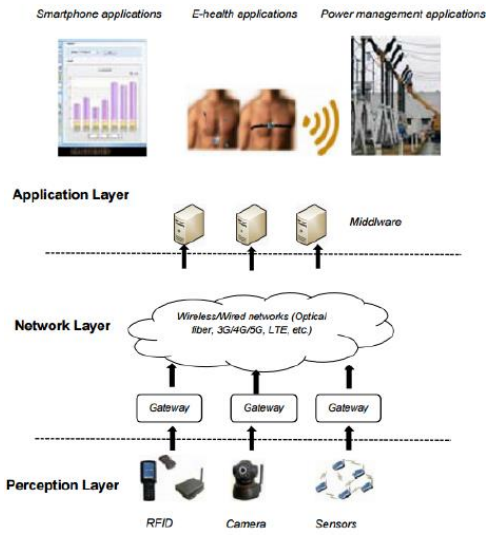
2. INTERNET VĚCÍ

Internet věcí poskytuje integraci různých senzorů a předmětů, které mohou komunikovat přímo mezi sebou, bez lidského zásahu. „věci“ v internetu věcí mohou zahrnovat fyzická zařízení, jako jsou senzorová zařízení, která monitorují a shromažďují všechny typy dat. Příchod této technologie vedl ke stálému univerzálnímu připojení lidí, objektů, senzorů, a služeb. [2] Výzkumné centrum Pew definuje IoT jako: globální, propracované, neviditelné síťové prostředí postavené prostřednictvím inteligentních senzorů, kamer, softwaru, databází a datových center [3]

Hlavním cílem je poskytnout síťovou infrastrukturu s interoperabilními komunikačními protokoly a softwarem, umožňující připojení a začlenění fyzických, nebo virtuálních senzorů, osobních počítačů (PC), inteligentních zařízení, automobilů, a předmětů, jako jsou lednice, myčka, mikrovlnná trouba, jídlo a léky do sítě. Nicméně požadavky na nasazení ve velkém měřítku se rychle zvyšují, což pak vede k významným bezpečnostním obavám. Bezpečnostní otázky, jako jsou soukromí, ověřování, řízení přístupu, systém konfigurace, uchovávání informací a management, jsou hlavními výzvami v prostředí internetu věcí. [2]

2.1. BEZPEČNOST IOT

Obecně platí, že IOT je rozdělen do tří vrstev: Vrstva vnímání (perception), Síťová vrstva a Aplikační vrstva [10], [11]. Všechny tyto tři vrstvy mají rozsáhlou škálu informací s různými technologiemi a funkcemi. Každá vrstva čelí rozdílnému typu ohrožení. [17]



Obrázek 2: Tři vrstvy architektury IoT

Zdroj [15]

Bezpečnost na perception vrstvě (vnímání)

Je to nejnižší úroveň konstrukce IoT. Tato vrstva je zdrojem přístupu k informacím během celého internetu. Problémy se zabezpečením zahrnují fyzickou bezpečnost snímacích zařízení a zabezpečení sběru informací. IoT nemůže poskytnout bezpečnostní systém ochrany a je zranitelný kvůli rozmanitosti, omezené energii, jednoduchost a slabé ochraně snímacího uzlu, která ovlivňuje zabezpečení WSN, RFID a M2M. [18]

Bezpečnost na síťové vrstvě

Cílem síťové vrstvy je přenášet informace a ty musí být přenášeny bezpečně. Bezpečnost síťové vrstvy má dva hlavní typy:

- Bezpečnostní riziko samotného IOT;
- Technologie a defekty při navrhování a implementaci protokolu. [10]

V bezdrátových sítích lze uzly volně pohybovat, mohou vstoupit, nebo opustit síť kdykoliv bez předchozího ověření. To dělá bezdrátové sítě více náchylné, nebo zranitelné proti případným útokům. [17]

Bezpečnost na aplikační vrstvě

Obsahuje zejména celou řadu aplikací například průmyslový monitoring, inteligentní sítě, monitorovací služby, nebo jakýkoli jiný inteligentní systém. Hlavním problémem jsou konstrukční chyby a softwarové zranitelnosti, které mohou přilákat jakékoli útočníka. [12]

2.2. Bezpečnostní protiopatření

Xu Xiaohui [10] hovoří o opatřeních vedoucích k problematice bezpečnosti internetu věcí. Některé z nich, jako certifikace, řízení přístupu a šifrování dat jsou popsány v následujících odstavcích.[17]

- **Certifikace**

  Je bezpečný způsob, jak potvrdit pravou identitu obou stran, které komunikují mezi sebou navzájem. Z tohoto důvodu pomocí Public Key Infrastructure (PKI) je možné dosáhnout silného ověřování prostřednictvím obousměrného veřejného certifikačního klíče pro prevenci pravdivosti a důvěrnosti systému IOT. [13]

- **Kontrola přístupu**

  Je další mechanismus, který poskytuje bezpečné prostředí IOT, omezením řízení přístupu ke strojům, předmětům, nebo osobám, které se pokouší o nelegální přístup k zařízením. Certifikace a řízení přístupu jsou technologie, které pracují ve vzájemném vztahu. Pro správné řízení přístupu se musí správné provést identifikace certifikační technikou. Řízení přístupu může být implementován na oblasti, jako je: zašifrování hesel, důvěrné adresáře, nebo soubory, konfiguraci a aktualizací práv atd. [17]

- **Šifrování dat**

  Šifrování se používá, aby se zabránilo manipulaci s informací, zachová mlčenlivost a integritu informací. Když data zachycuje útočník, šifrování brání v rozluštění údajů. Existují dva způsoby šifrování: [17]

  - Hop by Hop šifrování, poskytuje šifrovaný převod textu na každém uzlu tak, aby byl bezpečnější na síťové vrstvě. [17]
  - End to End šifrování, kde pouze odesílatel a příjemce mohou šifrovat a dešifrovat zprávu. [17]

  Podle obchodních potřeb je možné zvolit různé metody šifrování. Použitím bezpečnější výměnu klíčů a klíčových systémů řízení lze zabránit útokům na IOT, například odposlech a replay útok atd. [14]

2.3. Použití v praxi

Mnoho měst experimentuje s internetem věcí, uvádím zde následující příklady: [16]

Barcelona: chytré koše

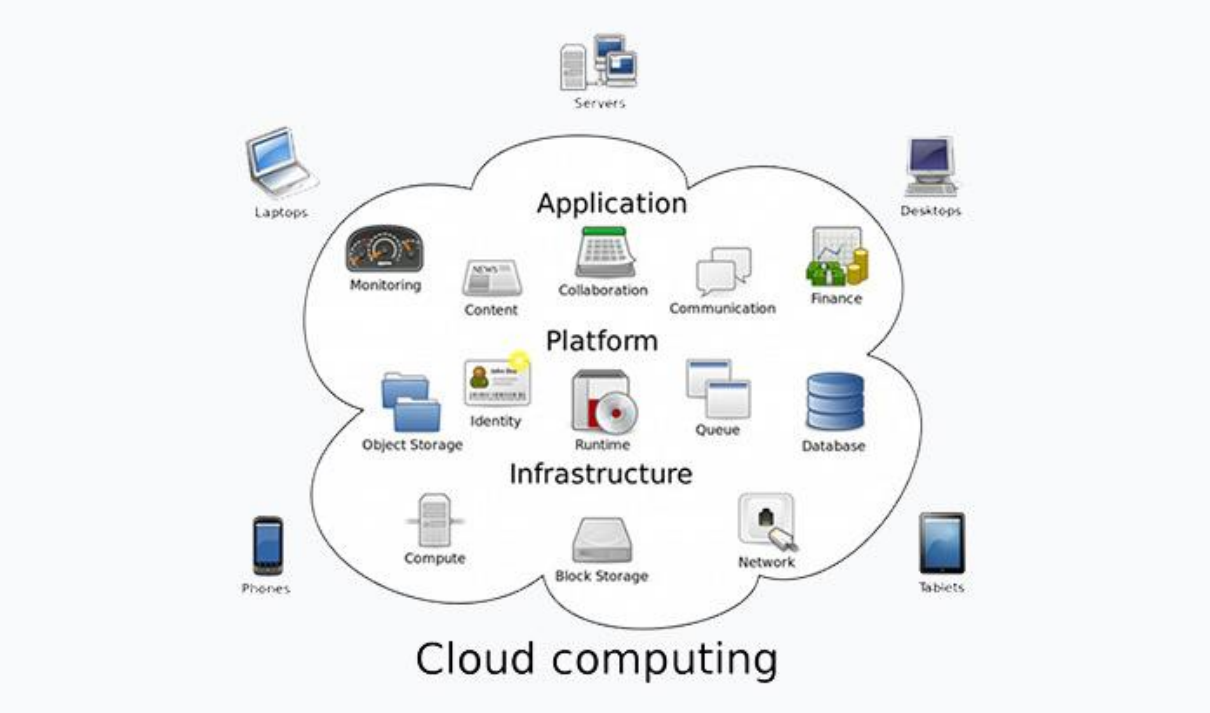
Využívá senzory na koši k optimalizaci trasy pro sběr odpadů, umožnuje tedy sběr již plných košů. Město odhaduje, že systém ušetří 10 % nákladů na likvidaci odpadu. [16]

Glasgow: inteligentní pouliční osvětlení

Šetří energii tak, že umožní osvětlení automaticky zapnout a vypnout, když lidé kolem nich chodí. [16]

3. CLOUD

Definice cloudu nemusí být úplně jasná, ale v zásadě je to termín, který se používá pro popis globální sítě serverů, z nichž každý má svoji funkci. Cloud není fyzický objekt, ale rozsáhlá síť vzájemně propojených vzdálených serverů po celém světě, které fungují jako jeden ekosystém. Tyto servery jsou navržené buď k ukládání a správě dat, spouštění aplikací, nebo doručování obsahu a služeb, jako je streamování videí, webová pošta, kancelářský software, nebo sociální média. Místo přistupování k souborům a aplikacím z místního, nebo osobního počítače se k nim přistupuje online z jakéhokoli zařízení s podporou internetu – informace tak budou dostupné kdekoli a kdykoli. [19]



Obrázek 3: Cloud computing

Zdroj [26]

3.1. Model nasazení cloudu

Model nasazení popisuje, jak jsou cloudové služby poskytovány. Rozdělují se do tří hlavních kategorii viz. Obrázek 3, a to na soukromý cloud, veřejný cloud a hybridní cloud. [25]

- **Veřejný cloud:** Veřejný cloud se definuje jako výpočetní služba nabízená externími poskytovateli veřejnosti prostřednictvím internetu tak, aby byla zajištěna maximální dostupnost služeb. [20]

- **Soukromý cloud:** V soukromém cloudu jsou škálovatelné prostředky a virtuální aplikace poskytované dodavatelem cloud spojeny dohromady a jsou k dispozici pro uživatele, kteří je používají. To se liší od veřejného cloudu, všechny zdroje a aplikace jsou řízeny samotnou organizací, podobně jako funkčnost intranetu. Využití privátního cloudu může být mnohem bezpečnější než u veřejného cloudu kvůli své specifické vnitřní expozici. [21],[25]
- **Hybridní cloud:** Hybridní cloud je soukromý cloud spojen s jedním, nebo více externími cloudovými službami, centrálně řízen a řízen jako jeden celek. [22] Poskytuje virtuální IT řešení prostřednictvím kombinace veřejných i soukromých cloudů. Hybridní Cloud poskytuje bezpečnější kontrolu dat a aplikací a má také otevřenou architekturu, která umožňuje rozhraní s jinými systémy pro správu. [25]

3.2. Distribuční modely cloudu

Distribuční model vypovídá o tom, co je v rámci cloudové služby nabízeno, tedy software, hardware, nebo kombinaci obojího. Rozděluje se do tří skupin a to IaaS, PaaS a SaaS. [25]

- **Infrastruktura jako služba (IaaS):** Infrastruktura jako služba, kde dodavatel sdílí zdroje cloudu pouze za smluvní poplatek. Tím se výrazně snižuje potřeba obrovské počáteční investice do počítačového hardwaru, jako jsou servery, síťová zařízení a výpočetní výkon, tedy poskytovatel cloudu poskytuje infrastrukturu. Představitel toho distribučního modelu je třeba Microsoft Azure. [23]
- **Platforma jako služba (PaaS):** Je sada softwaru a vývojových nástrojů hostovaných na serverech poskytovatele. Nabízí integrovanou sadu pro vývojářské prostředí, které vývojář může použít k vybudování svých aplikací. Poskytuje kompletní správu životního cyklu vývoje software. PaaS pracuje jako IaaS, ale poskytuje další úroveň funkčnost. Příkladem je Google App Engine. [22]
- **Software jako služba (SaaS):** To je také nazýváno model doručení, kdy jsou software a data licencovány jako služba. Uživatel SaaS platí za přístup k aplikaci, ale aplikaci nevlastní a má k ní přístup odkudkoli na internetu. Příkladem může být emailová služba Kerio. [25]

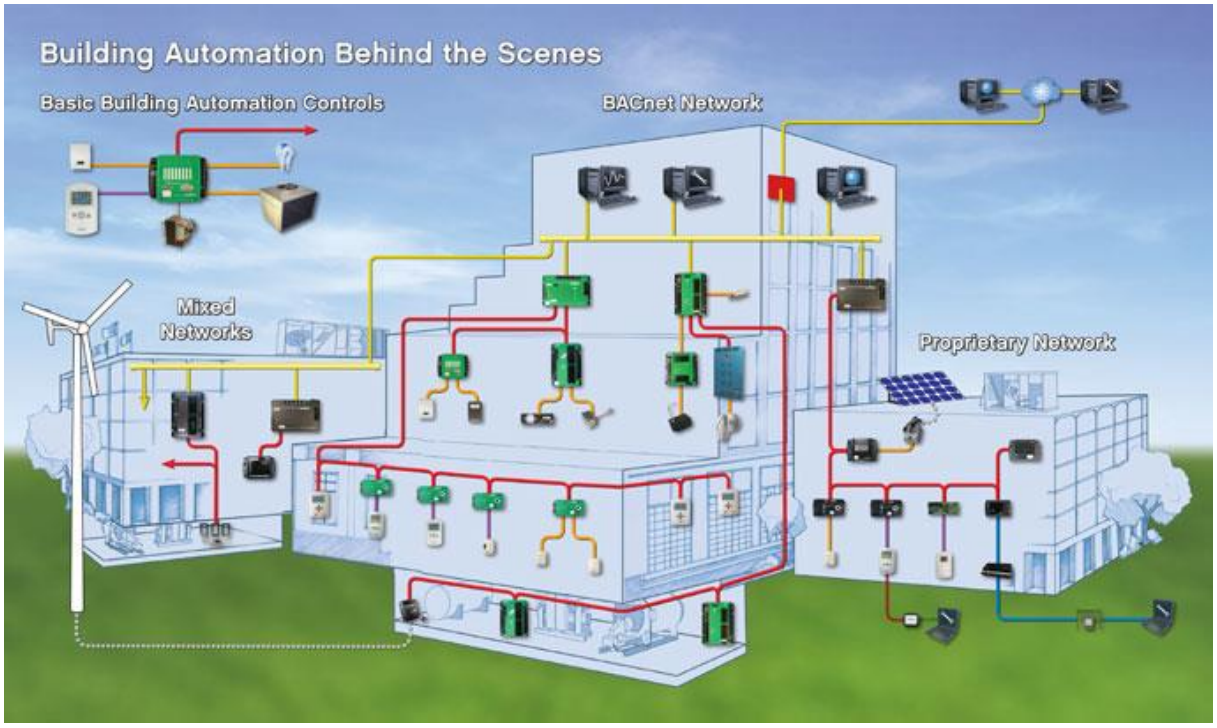
3.3. Bezpečnostní rizika cloudu

- **Zneužití:** Hackeři, nebo další zločinci využívají vhodných prostředků k neoprávněnému přístupu do cloudových služeb. Příkladem je útok hrubou silou, nebo slovníkový útok. [24]
- **Nezabezpečené API**: Uživatelé komunikují s cloudem prostřednictvím rozhraní, nebo API. Poskytovatelé musí integrovat spolehlivý bezpečnostní mechanismus do svých modelů poskytování služeb, zatímco uživatelé si musí být vědomi bezpečnostních rizik. [24]
- **Únos**: Takzvaný únos účtu, nebo služby se obvykle provádí s ukradenými pověřeními. K takovým útokům patří phishing, využívání softwarových zranitelností, nebo sociální inženýrství. Pokud je útok úspěšný útočníci mají přístup do kritické oblasti služeb cloudu jako důvěrnosti, integrity a dostupnosti služeb. [24]
- **Dostupnost:** V případě výpadku internetu, nebo samotného cloudu, například z hlediska lidské, nebo technické chyby, budou služby nedostupné.

4. AUTOMATIZOVANÉ SYSTÉMY BUDOV (BAS)

Budovy jsou základním rysem inteligentního města. [30] Inteligentní město nemůže existovat bez inteligentní budovy. Inteligence v budovách je dosažena použitím Building Automatic system (BAS). BAS centralizuje monitorování a řízení prostřednictvím sdíleného síťového média. Typické služby budov zahrnují vytápění, větrání a vzduchotechniku (HVAC), výtahy, řízení přístupu, uzavřený kamerový systém (CCTV), osvětlení, vodní a energetické systémy. Zařízení BAS, jako jsou snímače a senzory IoT, oznamují a zajišťují fyzickou kontrolu přes řídicí zařízení. Spojením těchto značně odlišných služeb dohromady vzniká inteligentní budova a lze vše řídit automaticky a vzdáleně přes internet. [27]

Výhodou inteligentní budovy bude snížení spotřebované energie pro osvětlení, a to např. tak, že senzory rozpoznají, zda se v místnosti vyskytují lidé, odešlou data na centrálu, a ta podle vyhodnocení dat zapne osvětlení v místnosti. Stejné to může být i s vytápěním.



Obrázek 4: Ukázka BAS

Zdroj [29]

4.1. Zabezpečení BAS

Musíme chránit naše sítě a připojené zařízení před viry, červy a hackery, kteří se je snaží kompromitovat. Nicméně, zabezpečení sítě není jen o datových sítích. Senzorové sítě čelí podobným hrozbám. Většina nových budov, nebo průmyslových zařízení, patří do

inteligentních sítí, které jsou schopné řízení a monitorování jak mechanického, tak i elektrického vybavení budovy. Ačkoli obyčejná síť poskytuje útočníkům vyšší počet možných cílů, inteligentní sítě se stále více a více stávají zajímavějším cílem [46]. Tyto typy sítí představují zajímavé prostředí nutné především pro více cílených útoků s možným velkým dopadem na základní funkce podniku, nebo společnosti. [47]

BAS jsou navrženy tak, aby plnily cíle za pomocí automatizace a sledování dostupných služeb. Bohužel, nedostatek celostního, nebo strategického přístupu znamená, že každá výše zmíněná automatická služba byla vyvinuta samostatně, s použitím samostatných protokolů, zařízení a fyzického média. [33]

BAS sítě obvykle kombinují pomocí LAN infrastruktury s některými ne průmyslovými síťovými protokoly. Tento přístup umožňuje využití stávající infrastrukturu a propojit BAS komponenty. Kromě toho síť na bázi IP umožňuje dálkové ovládání a jednodušší údržbu. Na druhé straně to zvyšuje bezpečnostní rizika. [34]

4.2. Zranitelnost protokolů

BAS obsahuje množství protokolů, některé specifické pro tuto oblast použití a jiné obecnější. Mezi specializovanými komunikačními protokoly se řadí třeba DALI, pro řízení osvětlení, nebo BACnet, který se používá pro správu klimatizačních systémů. KNX, LonWorks jsou naopak příklady obecnějších protokolů.[35]

Mnoho z těchto protokolů je již velmi zastaralých a bezpečnost nebyla jednou z návrhových priorit při jejich tvorbě. V dnešní době musí všechny použité protokoly obsahovat interoperabilní bezpečnostní opatření, jako je šifrování, nebo ověřování. [35]

V posledních letech se k těmto výše uvedeným přidala řada nových bezdrátových protokolů nové generace. Tito zahrnují ZigBee, Wifi, EnOCEAN. Bezdrátové protokoly umožňují vyšší úroveň zabezpečení, což snižuje riziko vnějších útoků, ale postrádají spolehlivost svých kabelových protějšků (z hlediska dostupnosti, latence atd.). [35] Následně se zaměřím na bezpečnost protokolů BACnet, LonWorks, KNX.

4.2.1. BACnet

BACnet je standardní komunikační protokol pro sítě automatizace a řízení budov (Building Automation and Control Networks) vyvinutý americkým sdružením ASHRAE (American Society of Heating, Refrigerating and Air-conditioning Engineers). Hlavním cílem bylo

vytvořit protokol, který by umožňoval integraci systémů různých výrobců, primárně určených pro automatizaci budov. [36]

BACnet nabízí několik služeb, které zabraňují neoprávněnému použití zachycování a modifikaci vyměňovaných dat. [38][39] Tyto mechanismy používají symetrické šifrování (DES) algoritmus a důvěryhodný klíčový server, který je odpovědný za generování a distribuci klíčů. Tyto klíče se používají k šifrování přenášených dat mezi dvěma síťovými uzly. K vytvoření bezpečného připojení ke klíčovému serveru, každý uzel musí vlastnit tajný klíč. BACnet může být obecně ohrožen následujícími hrozbami [39][40][42]:

- **BACnet spoofing:** Tento útok je podobný ARP spoofingu, nebo spoofingu IP, které se vyskytují v prostředí IT. Kompromitovaná zařízení vytvářejí falešné zprávy, které přinutí ostatní zařízení k posílání vlastních zpráv přes útočící zařízení. [37]
- **Útoky odmítnutí služby:** se provádí zaplavením sítě BACnet. Útočník pošle zprávy na neurčený seznam cílových zařízení, kterému musí odpovídat všechna zařízení a vytváří zbytečný provoz v síti a tím ji zatěžuje. [37]
- **Útok na schopnosti psaní:** Změní aktuální hodnotu vlastností objektu BACnet. Výsledek tohoto útoku závisí na objektu, kterého se to týká.[37]
- **Zakázání síťových připojení:** To lze provést pomocí několika služeb BACnet. Směrovací tabulky sítě BACnet mohou být poškozeny kompromitovaným zařízením, které sdílí chybné informace o směrování. Je také možné zakázat síťové připojení odesláním konkrétních chybných zpráv. [37]

4.2.2. LonWorks

Na rozdíl od BACnetu je LonWorks proprietární technologií, která vyžaduje specifický čip Echelon nazvaný Neuron. Díky nízké ceně a flexibilitě pro integraci komponent od jiných výrobců, využívá LonWorks miliony zařízení pro automatizaci budov.[37]

LonWorks je název technologie. Použitý protokol se nazývá LonTalk a je založen na otevřeném standardu ISO / IEC 14908. Tato technologie funguje podobně jako síť LAN, tedy i její název LON (Local Operating Network). Na fyzické úrovni může LonWorks pracovat na kabelu s krouceným párem, Ethernetem, elektrickým kabelem (PLC), optickým vláknem atd., což z něj činí vysoce univerzální technologii.[37]

LonTalk poskytuje ověření pomocí čtyř kroků, mechanismus reakce na výzvu. Odesílatel, který si přeje ověření přenosu potvrzuje ověření bit zprávy. Přijímače odpovídají náhodným

64bitovým číslem. Odesílatel vrátí vypočítanou hodnotu 64 bitů nad obsahem zprávy a náhodným číslem pomocí sdíleného klíče. Přijímač provádí stejný výpočet a srovnává výsledky. Nicméně, [41] popisuje následující bezpečnostní nedostatky:[43]

- Autentizační služby podporují pouze ověřovací identitu odesílatele. Identitu příjemce nelze zkontrolovat. [43]
- Protokol ověřování je citlivý na (DoS). [45], útočník odešle spoustu zpráv se sadou ověření bitů. Pro každou zprávu přijímač bude generovat náhodné číslo a vypočítat potřebné „hash value“. A to je časově náročné.
- Kryptografický algoritmus není otevřeně dostupný. Délka klíče je omezena na 48 bitů. Proto je všeobecně považován za slabou bezpečnostní ochranu. [43]
- Každý uzel může používat pouze jeden ověřovací klíč. To znamená, že všechny entity, které chtějí komunikovat, musí navzájem sdílet stejný ověřovací klíč. [43]
- Protokol LonTalk neposkytuje mechanismus distribuce tajného klíče bezpečným způsobem. Klíčová distribuce musí být tedy provedena v bezpečném prostředí, aby nedošlo k zachycení. [43]

4.2.3. KNX

KNX je otevřený a rozšířený protokol BAS technologie. Používá vrstvenou strukturu a podporuje kabelové komunikace přes kroucenou dvojlinku a elektrický kabel (PL), jakož i bezdrátové komunikace rádiovým přenosem. Kromě toho podporuje komunikaci s hostiteli IP založené zvláštním typem routeru (KNXnet / IP). [44]

KNX byl vtvořen ze tří předních norem European Installation Bus (EIB), European Home Systems Protocol (EHS) a BatiBUS. Jedná se o otevřený a na platformě nezávislý standard. Rovněž podporuje různé druhy fyzických médií, což umožňuje jeho použití v různých prostředích.[44]

Tento protokol nenabízí mechanismy pro zajištění důvěrnosti a integrity dat. Ani nepodporuje specializované služby ověřování. Poskytuje pouze základní schéma řízení přístupu na základě prostého textu hesla [43]. Vzhledem k tomu je ochrana přístupu velmi primitivní, neposkytuje potřebné mechanismy pro zajištění bezpečného prostředí. Kromě toho trpí obecnými bezpečnostními nedostatky [43]:

- Klíče jsou přenášeny ve formě prostého textu
- Mechanismus ochrany přístupu nelze použít ke zpracování datové komunikace, a proto nelze zabránit neoprávněnému použití.
- Paralelní připojení nejsou podporována: Pokud uzel naváže spojení s konkrétním zařízením, všechny ostatní požadavky na připojení jsou ignorovány. Útočník toto může použít pro omezení a provést DoS útok.
- Injekce zpráv: zfalšovat zdroj přenášené adresy může být velmi snadné, útočník může jednoduše použít škodlivou zprávu. [43]

4.3. Souhrn

Bezpečnostní mechanismy společností LonWorks a KNX nejsou dostatečné pro splnění požadavků na integraci BAS bezpečnostních subsystémů. Nemohou být efektivní při ochraně před hrozbami. Bezpečnostní architektura BACnetu je pokročilejší. Použitý kryptografický algoritmus je však zastaralý a měl by být nahrazen moderním (např. Pokročilý Šifrovací standard (AES)). Navíc protokol musí být vylepšen, aby se předešlo jistým bezpečnostním nedostatkům. Tabulka 1 uvádí přehled bezpečnostních architektur.[43]

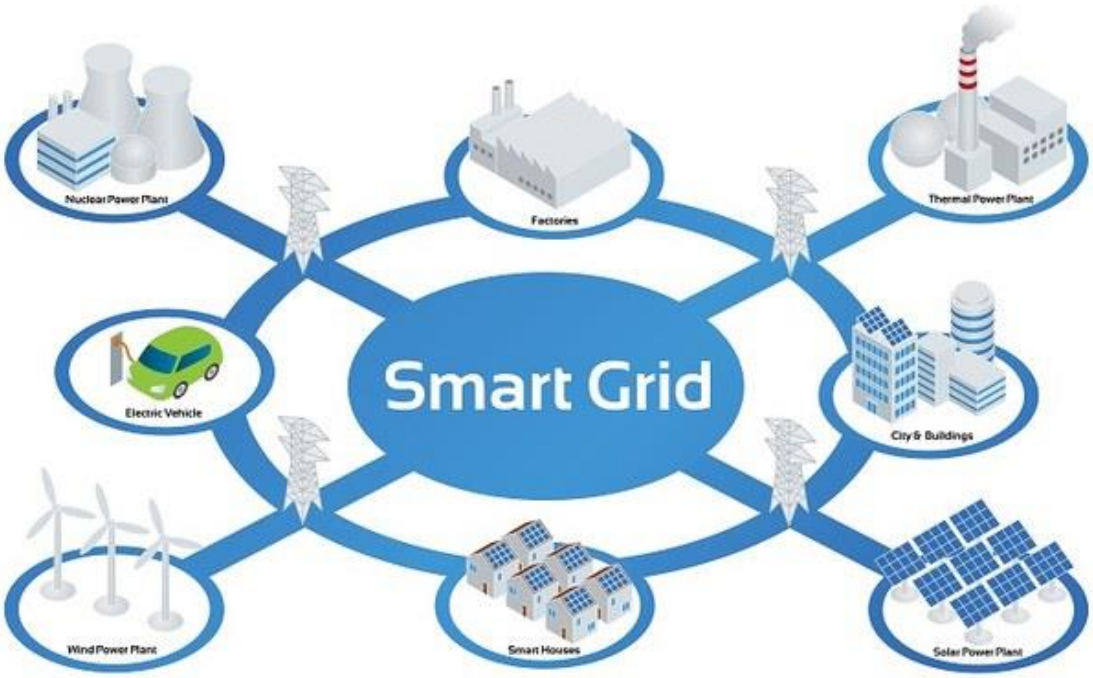
	LONworks	BACnet	KHX
Autentizace	64 bit MAC (48 bit key)	DES	32 bit password
Integrita	65 bit MAC (48 bit key)	DES	-
Důvěrnost	-	DES	-

Tabulka 1: Bezpečností mechanizmy v BAS

Zdroj [43]

5. INTELIGENTNÍ SÍTĚ

Existuje mnoho definic Inteligentní energetické sítě, dále jen Smart Grid. Krátká definice zní: „Smart Grid je elektrická síť, která může inteligentně začlenit působení všech uživatelů připojených činitelů, jako jsou generátory, spotřebiče a elektronické rozvody, aby se efektivně zajistila udržitelná, ekonomická a bezpečná dodávka elektřiny “[48]. National Institute of normy a technologie (NIST) definuje Smart Grid takto: „Modernizována síť, která umožňuje obousměrné toky energie a využívá obousměrné komunikační a řídící schopnosti, které povedou k řadě nových funkcí a aplikací “[49]. Podle US Department of Energy zní definice takto: „Smart Grid je technologie, která zahrnuje pokročilé technologie snímání, řídicí systémy a integrované komunikace do existující elektrické sítě“ [50].

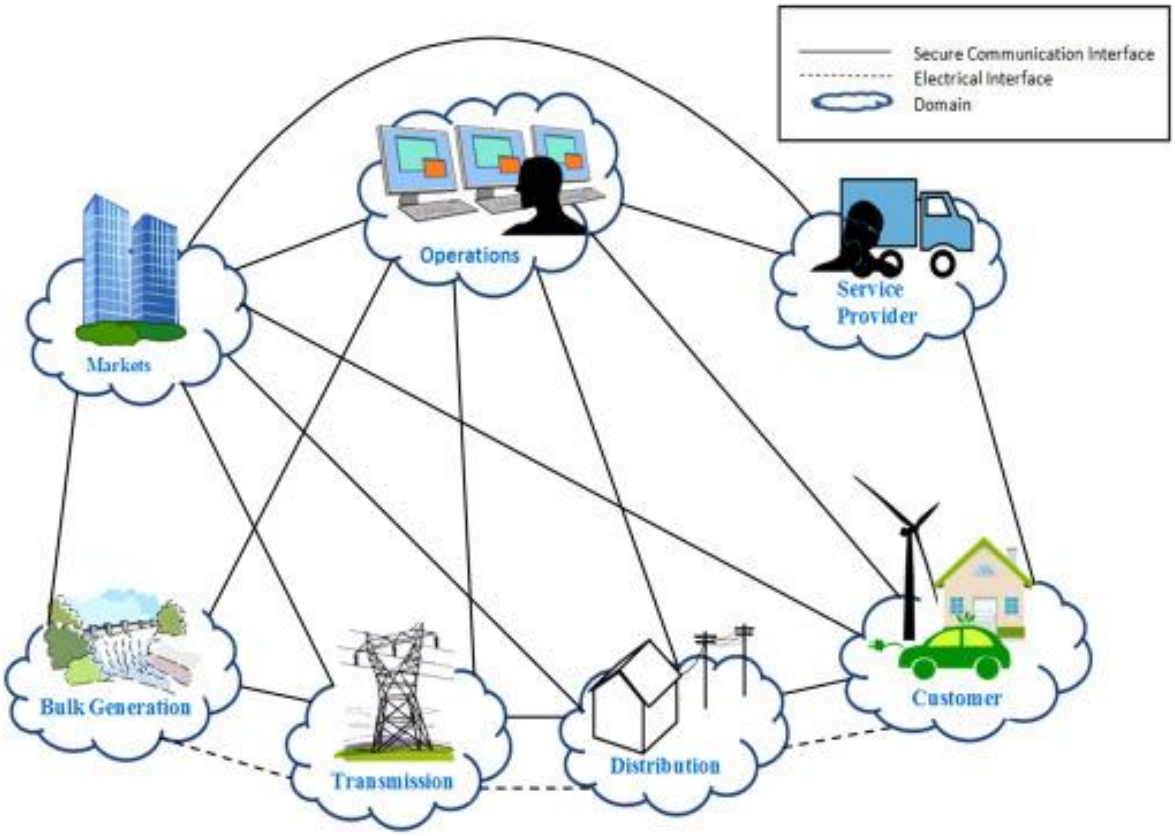


Obrázek 5: Diagram smart grid

Zdroj [56]

Smart grid je považován za největší instanci v síti internetu věcí [51]. Prostupuje celým řetězcem rozvodné sítě od výroby energie v elektrárnách pro spotřebitele, tedy rodinné domy, budovy, továrny, veřejné osvětlení, elektrické automobily, inteligentní spotřebiče atd., včetně přenosových a distribučních energetických sítí, ty budou schopny obousměrné komunikace, sledovaní a kontroly elektrické sítě kdekoli a s vysokou přesností. Například, inteligentní domy budou vybaveny inteligentními měřiči a inteligentními spotřebiči, zatímco generátory

elektrické energie a elektrické přenosové a distribuční sítě budou vybaveny různými čidly. Cílem SG je udržet real-time bilance mezi výrobou a spotřebou energie monitorováním a kontrolou napájecího řetězce, a to díky obrovskému množství obousměrné komunikace inteligentních objektů (inteligentní měřiče, inteligentní zařízení, senzory, atd). [52]



Obrázek 6: Jak funguje smart grid

Zdroj [57]

5.1.Bezpečnost a hrozby pro SG

Bezpečnostní řešení vyvinutá pro tradiční IT sítě nejsou účinná v rastru sítí [53] a to z důvodu velkých rozdílů mezi nimi. Jejich bezpečnostní cíle jsou odlišné v tom smyslu, že bezpečnost v IT sítích si klade za cíl prosadit tři zásady zabezpečení (důvěrnost, integritu a dostupnost).

Zatímco bezpečnost v automatizačních sítích (grid) si klade za cíl zajistit bezpečnost osob, zařízení, ochrany elektrického vedení a operačního systému. Bezpečnostní architektura počítačových sítí je jiná než Grid sítě, protože je bezpečnosti v oblasti IT sítí dosaženo tím, že poskytuje větší ochranu ve středu sítě (kde sídlí data) a ochrana automatizačních sítí se provádí v síťovém centru. Jejich základní topologie je také jiná. IT sítě používají dobře definovanou sadu operačních systémů (OSS) a protokolů a automatizační sítě používají

vícenásobné korektnosti OS a protokoly specifické pro dodavatele. Hlavní rozdíl je v tom, že v případě poruchy, nebo upgradu je v oblasti IT sítí možné zařízení restartovat, zatímco v případě automatizačních sítí to není přijatelné, protože služby musí být k dispozici po celou dobu. [54] SG může být vystaveno následujícím hrozbám:

- **Malware**: Útočník může vyvinout malware a rozšířit jej, a tak infikovat inteligentní měřicí přístroje, či firemních servery. Malware může být použit jako libovolná funkce v zařízení, nebo systému. [54]
- **Replay útok**: Útočník posílá pakety k injekci nepravdivých informací v síti, jako jsou například nesprávné údaje k propočtům nesprávných cen za elektřinu, nebo vyvolání falešné mimořádné události apod. Falešné informace mohou mít obrovský finanční dopad na trzích s elektřinou. [54]
- **Dostupnost sítě**: Vzhledem k tomu, že SG využívá protokol IP a TCP / IP, je možnost prostřednictvím DoS útoků využít zranitelnosti související s TCP / IP. DoS útoky zdrží, blokují nebo poškodí přenos informací tak, aby zdroje SG nebyly k dispozici. [54]
- **Odposlouchávání a analýza provozu**: Protivník získává citlivé informace o monitorování síťového provozu. Příklady sledovaných informací zahrnují budoucí cenové informace, řídící strukturu sítě a spotřebu energie. [54]

5.2. Návrhy řešení možných hrozeb

- Ochrana proti škodlivému softwaru by měla být zahrnuta v systému. Vestavěné systémy musí spouštět software, který je dodáván výrobcem. Výrobce je povinen vložit do svých výrobků bezpečné úložiště, které obsahuje řešení pro validaci softwaru. Pomocí klíče systém ověří veškerý nově stažený software před spuštěním. Systémy pro všeobecné použití jsou určeny na podporu softwaru třetích stran. Pro tento systém je nutné využít často aktualizovaný antivirový software spolu se základní bezpečnostní prevencí.[54]
- Zařízení musí znát zdroje a cíle se kterými komunikují. Toho je dosaženo vzájemnou autentizací pomocí Transport Layer Security (TLS), nebo Internet Protocol Security (IPSec).

- Zařízení by měla podporovat virtuální privátní sítě (VPN) a architekturu pro bezpečnou komunikaci.[54]
- Zařízení musí využívat infrastruktury veřejných klíčů (PKI) k zajištění komunikace [55]. Nicméně existují některá omezení týkající se šifrování a správy klíčů. [58] Současná zařízení nemají dostatek výpočetního výkonu a paměti na provádění pokročilého šifrování autentizačních metod. V inteligentní distribuční síti se komunikace přenáší přes kanály, které mají různá připojení a různé šířky pásma. Certifikační autority musí být dostupné po celou dobu.[54]
- Je nezbytné vytvořit robustní autentizační protokol při komunikaci v inteligentní síti. Protokol musí pracovat v reálném čase a dodržovat co nejnižší výpočetní výkon bez ztráty robustnosti bezpečnostního algoritmu, nízkou komunikační režii a odolnost vůči útokům, zejména DoS útoků.[54]

5.3. Souhrn

Smart grid velmi těží z vize, internetu věcí, kde inteligentní objekty, či zařízení jsou rozmístěny podél energetické dráhy, od výroby elektrické energie ke koncovému zákazníkovi. Čelí stejným bezpečnostním problémům jako IoT. V případě poškození tohoto konceptu dochází ke kritickému stavu, který může vést k přerušení dodávek elektrické energie do klíčových oblastí. Vize Smart grid razantně zlepší stávající správu elektrické sítě. Ale bezpečnost není na adekvátní úrovni. Jelikož Smart grid ovládá a kontroluje důležitý zdroj pro inteligentní město, stává se lákavým cílem pro útočníky.

6. INTELIGENTNÍ VOZIDLA

Jsou to auta opatřená celou řadou senzorů a elektronickými řídicími jednotkami (ECU) a ta vyhodnocují data získaná ze senzorů. Je připojeno do sítě, aby mohlo komunikovat s jinými inteligentními vozidly a inteligentním městem. V praxi to tedy znamená, že počítač automobilu v reálném čase vyhodnocuje stovky parametrů, od stupně únavy řidiče až po upozornění na nefunkčnost semaforů. Pokud se před vozidlem objeví nečekaný předmět, senzory pošlou data na danou ECU, ta situaci v milisekundách vyhodnotí a vozidlo zastaví. [67] Inteligentní auta můžeme rozdělit na dva typy, a to na autonomní a tzv. připojená.

6.1. Autonomní vozidlo

Autonomní vozidla, také známá jako robotické automobily, jsou motorová vozidla, která pracují bez lidského řidiče (pouze úrovně 4) snižují náklady na dopravu a zlepšují pohodlí a bezpečnost. [69]

mohou využít palubního čidla, kamery, GPS a telekomunikačních sítí za účelem získání informací pro vyhodnocení úsudku ohledně bezpečnosti v kritické situaci a jednat odpovídajícím způsobem. Autonomní vozidla se posuzují podle následujících úrovní [73]

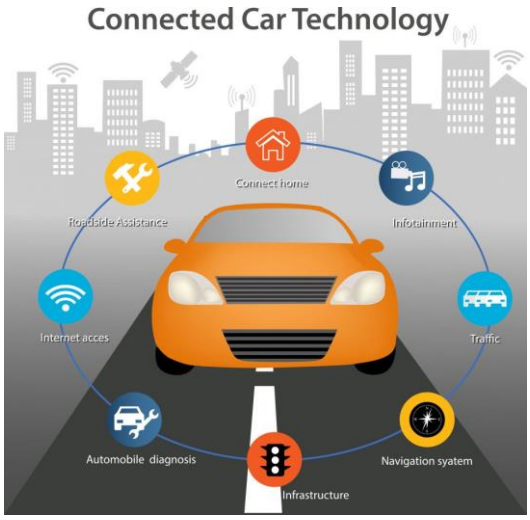
- **Úroveň 0**: Řidič má úplnou a výhradní kontrolu nad primárními ovládacími prvky vozidla (brzdy, řízení atd.). Ve všech okolnostech je plně zodpovědný za sledování vozovky a provoz všech ovládacích prvků vozidla. Vozidla, která mají určité podpůrné systémy, ale nemají kontrolní pravomoci nad řízením, stále spadají do úrovně 0. Příklady zahrnují systémy poskytující automatizované sekundární ovládací prvky, jako jsou stěrače, světlomety, směrová světla atd.[73]
- **Úroveň 1**: Automatizace na této úrovni zahrnuje jednu, nebo více specifických řídících funkcí. V případě více automatizovaných funkcí fungují nezávisle na sobě. Řidič má celkovou kontrolu a je plně zodpovědný za bezpečný provoz. Může rozhodnout podstoupit omezenou moc nad primárním systémem (např. adaptivní tempomat). Mezi příklady specifických funkcí automatizačních systémů patří: tempomat, automatické brzdění a udržování jízdního pruhu.[73]
- **Úroveň 2**: Tato úroveň zahrnuje automatizaci alespoň dvou primárních řídicích funkcí určených pro práci v souladu ulehčit řidiči ovládání těchto funkcí. Vozidla na této úrovni automatizace mohou využívat sdílenou autoritu, když řidič podstoupí aktivní primární kontrolu v určitých omezených jízdních situacích. Řidič je stále

odpovědný za sledování vozovky a bezpečný provoz a očekává se, že bude k dispozici pro kontrolu za všech okolností a na krátkou dobu. Systém se může vzdát kontroly bez předchozího ohlášení a řidič musí být připraven bezpečně ovládat vozidlo. [73]

- **Úroveň 3**: Vozidla na této úrovni automatizace umožňují řidiči postoupit plnou kontrolu nad všemi funkcemi z hlediska bezpečnosti za určitého provozu, či okolních podmínek a v těchto podmínkách spoléhat na vozidlo při sledování změn, které vyžadují přechod zpět na ovládání řidičem. Řidič má být k dispozici pro občasnou kontrolu, ale s dostatečně vyhovujícím časovým intervalem. Vozidlo je určeno k zajištění bezpečného provozu při automatizovaném režimu jízdy. Příkladem může být automatické, nebo samostatné řídicí vozidlo, které je schopno určit, kdy systém již není schopen podporovat automatizaci. [73]
- **Úroveň 4**: Vozidlo je určeno k provádění veškerých řídicích funkcí. Takový návrh předpokládá, že řidič poskytne cílový, nebo navigační vstup, ale neočekává se, že bude k dispozici pro kontrolu kdykoliv během jízdy. To zahrnuje obsazená a neobsazená vozidla. Podle návrhu bezpečného provozu spočívá výhradně na automatizovaném systému vozidla.[73]

6.2. Připojené vozidlo

Připojené automobily jsou ty, které mají přístup k internetu a řady senzorů, které jsou schopny odesílat a přijímat signály, analyzovat fyzické prostředí kolem nich a komunikovat s ostatními vozidly, nebo subjekty.[69]

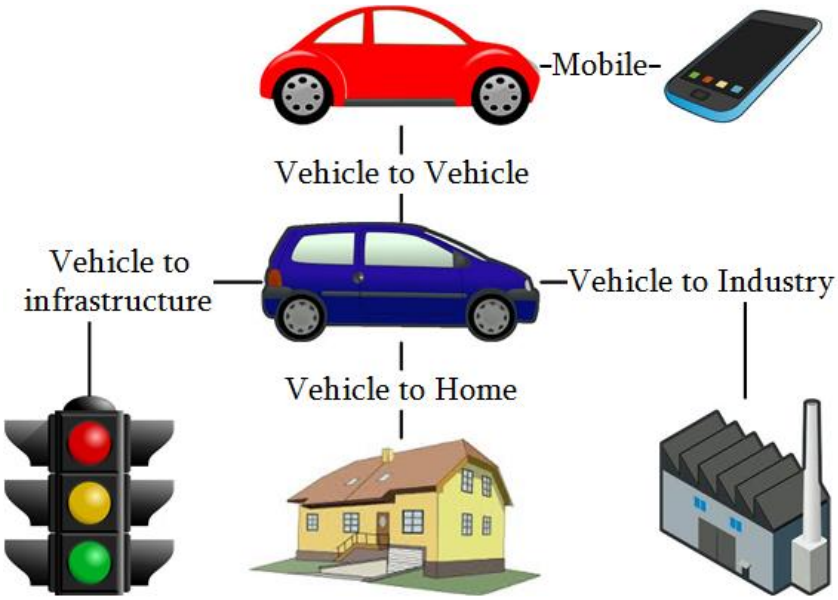


Obrázek 7: Připojené auto

Zdroj [71]

Typy komunikace

- V2V (Vehicle to Vehicle): Tato forma připojené komunikace je výměna informací mezi dvěma vozy, sdílení informací o rychlosti a poloze, varování před překážkami na vozovce, nebo před jinými riziky. Cílem je snížit nehodovost.[70]
- V2I (Vehicle to Infrastructure): Tento termín se vztahuje k bezdrátové komunikaci mezi vozidly a součástmi infrastruktury.[70]
- V2C (Vehicle to Cloud) Cloud nahrazuje lokální úložiště dat úložištěm, které je přístupné přes internet.[70]
- V2X (Vehicle to Everything) Označuje výměnu informací mezi vozidly, jinými dopravními prostředky, infrastrukturou, nebo řídícím centrem a různými internetovými aplikacemi. [70]



Obrázek 8: Připojené koncepce automobilů

Zdroj [70]

ECU

V automobilovém průmyslu je elektronická řídicí jednotka (ECU) vestavěné elektronické zařízení, v podstatě digitální počítač, který čte signály pocházející ze snímačů umístěných v různých částech a v různých komponentách automobilu a v závislosti na těchto informacích řídí automatické operace.[64]

Funkčnost se pohybuje od malých úkonů, jako je otevírání okna a odemykání dveří k pokročilejším funkcím, jako jsou automatické brzdové systémy a systémy varování před kolizí. Jednotky ECU jsou proto velmi přijatelné cíle pro budoucí útoky. Pro zajištění specifické funkčnosti každá ECU pracuje s vlastním nezávislým firmwarem. Nadcházející trend pro výrobce automobilů je provést vzdálenou aktualizaci diagnostiky a aktualizace firmwaru bezdrátovým přenosem [65], což umožňuje identifikovat problémy s hardwarem a odstraňovat chyby softwaru s minimálním dopadem na pohodlí zákazníka. [66],[68]

6.3. Automobilová síť

V současné době se používá široká škála komunikačních systémů vozidel. Možnosti použití sahají od elektronického řízení motoru, několik jízdních asistentů a bezpečnostních mechanismů až po širokou škálu zábavných aplikací. Tabulka č. 1 uvádí 5 komunikačních skupin rozdělených podle základních technických vlastností a aplikačních oblastí.[59]

Skupina	**Subbus**	**Spuštění události**	**Časová událost**	**Multimedia**	**Bezdrát**
Reprezentanti	LIN, K-LINE	CAN, VAN, PLC	FlexRay, TTP, TTCAN	MOST, D2B, GigaStrar	Bluetooth, GSM, WLAN

Tabulka 2: Seskupení vybraných automobilových systémů sběrnic

Zdroj [59]

Následně více popíšu vybrané protokoly LIN, CAN, FlexRay a MOST.

- **CAN:** Je síť s lineárním sběrnicovým typem. V takové síti jsou všechny uzly připojeny k jedné komunikační sběrnici. Výhodou tohoto typu sítě je, že je snadné připojení nového uzlu k síti a nízké náklady na kabeláž. Tím je CAN hojně používána v automobilech, neboť je odolný proti elektromagnetickému rušení. Hlavní nevýhodou je, že má jediný bod selhání. Selhání sběrnice vede k tomu, že část sítě se stává nedostupnou. Norma CAN však určuje pouze fyzickou a datovou vazbu na vrstvy modelu OSI. Zásady vytváření sítí, jako je například adresování a kontrola chyb, tedy nejsou v rámci standardu CAN implementované.[59]
- **MOST:** Je vyšší komunikační síť určená pro multimediální účely. Namísto lineární topologie MOST-bus používá kruh. Vzhledem k tomu, že sběrnice MOST je určena speciálně pro multimédia, zahrnuje všech 7 vrstev modelu OSI.[59]

- **FlexRay:** V důsledku další digitalizace uvnitř automobilů vznikla potřeba vysoké šířky pásma s nízkou latencí. Tato nová síť musí být rychlejší než běžně používaná síť CAN a flexibilnější z hlediska topologie. To vedlo k vytvoření nové sítě. Díky přenosové rychlosti 10 Mbit/s se používá nejnovější inovace např. adaptivní tempomat (ACC) a asistent jízdního řádu.[59]
- **LIN:** Místní propojovací síť slouží jako jednoduchá, nákladově efektivní sběrná síť, která se používá na nesložité úkoly. Často se využívá jako podsíť sítě CAN.[59]
- **Bluetooth:** Je bezdrátové propojení. Znamená výraznou bezpečnostní nevýhodu oproti kabelové komunikaci v tom, že všechny informace jsou vysílány přes otevřené a viditelné spojení. I když jsou přenosy Bluetooth tkv. jednoduché, existují různé proveditelné útoky. [61][62][63]

6.4. Bezpečnost

Důsledky útoků mohou být v rozmezí od menších komfortních nedostatků až k riziku nehody. Proto je úroveň zabezpečení vyžadována v každém daném sběrnicovém systému. Jak je uvedeno v tabulce 3, zatímco útoky na LIN, nebo multimediální sítě, mohou mít za následek selhání elektrického ovládání oken, nebo navigační software. Úspěšné útoky na sítě CAN mohou způsobit nefunkčnost některých důležitých jízdních asistentů, což by vedlo k ohrožení bezpečné jízdy. [59]

	LIN	**CAN**	**FlexRey**	**MOST**	**Bluetooth**
Vystavení riziku	Malé	Velké	Akutní	Malé	Pestré
Možné škody	Zmírnění funkčnosti	Snížení jízdní bezpečnosti	Nebezpečí vzniku nehody	Krádež dat, Nedostatek komfortu	Neoprávněný přístup k datům

Tabulka 3: Rizika protokolů

Zdroj [59]

Fyzikální hrozby

Přinášejí několik scénářů: manipulaci s ECU, nebo TCUs (obnovit klíče nebo k fyzickému ladění rozhraní); použití zařízení elektromagnetického vyzařování nebo spotřebu energie k

úniku informací (boční kanál); ke změně chování zařízení a nakonec získání přístupu k chráněným datům. Fyzické hrozby vyplývají z dobře identifikovaného útoku prostřednictvím fyzické manipulace zařízení. Mohou vést k různým typům rizik. [60]

Výpadek sítě

Výpadek sítě (například od ISP) může mít za následek odmítnutí služby pro citlivé operace, jako OTA, opravy kritických chyb a zranitelností. To platí i pro interní selhání sítě. Obecněji, jakýkoli návrh, který příliš spoléhá na připojení, vystavuje vozidlo potenciálním problémům v případě výpadků. Vozidla musí být navržena tak, aby mohla používat degradovaný režim provozu v případě výpadku. [60]

Poškození / ztráta

- **Ztráta informací v cloudu:** Citlivá data mohou být ztracena v důsledku útoku, nebo nehody, pokud jsou uloženy poskytovateli cloudu třetích stran. [60]
- **Škody způsobené třetí stranou:** Citlivá data mohou být ztracena, nebo ohrožena kvůli fyzickým poškozením v případě dopravní nehody či krádeže. [60]
- **Únik informací:** Soukromá, nebo citlivá data (například informace o platbách, řidičské návyky atd.) mohou být zneužity, když je vůz prodán jinému uživateli. [60]

Odposlech

- **Replay zpráv**

  Pokud nejsou vnitřní sítě dostatečně chráněny proti replay, potenciální útočníci mají snadný přístup k širokému spektru nebezpečných příkazů. [60]

- **Odmítnutí akcí**

  Odpovědnost řidiče je možná zapojena do nehod, nebo pojištění. Existuje motivace k ohrožení údajů souvisejících s používáním automobilu, jako jsou jízdní zvyklosti, nebo lokalizace. Jedná se pouze o rozšíření stávajících podvodných režimů například na tachometru. [60]

- **Škodlivý software**

  Integrace mobilních ekosystémů může způsobit riziko zavedení potenciálního škodlivého softwaru přímo uživatelem. Škodlivý software může poskytnout první

krok pro útočníky ve vícestupňovém útoku. Je třeba poznamenat, že tyto vazby na mobilní platformy a PC ekosystémy znamenají, že útočníci mohou recyklovat známé útoky z prostředí (Linux, Android, Windows), aby ovlivnili funkčnost inteligentních vozů. [72]

7. BEZPILOTNÍ VZDUŠNÉ DOPRAVNÍ PROSTŘEDKY (UAV)

Jedná se rozsáhlá civilní, obchodní a bezpilotní letecká vozidla (UAV) alias drony. S rozvojem mikroprocesorů a výrobou techniky jsou malé bezdrátové drony přístupné pro každého za cca 6000 Kč. Tyto drony mají také řadu funkcí a typicky obsahují palubní kameru. Dalšími součástmi mohou být senzory, jako výškoměr a rychloměr. [27] UAV mají širokou škálu aplikací a modelů. Jsou rozděleny do tří kategorií, kterými jsou bezpečnostní kontrola, vědecký výzkum a komerční aplikace. Aby se dosáhlo dobře navržené aplikace UAV, musí existovat přesné informace o podpoře, která je nezbytná pro úspěšně fungující systém. Je dobře známo, že UAV mají využití v mnoha odvětvích od zemědělství až po dopravu ropy a zemního plynu. Architektura typického UAV se skládá z hlavních částí, které tvoří řídicí systém, monitorovací systém, systém pro zpracování dat a systém přistání. Vnitřní systém poskytuje široké spektrum funkcí od navigace k poskytování přenosu dat k zemi. Trh s UAV stále roste a UAV jsou zapojeny do nových činností a řeší nové problémy [75].

Obrázek 9: Ukázka UAV

Zdroj [84]

7.1. Bezpečnostní obavy

Všechny drony by měly být řádně zajištěny, aby nebyly náchylné k hackům. Je zapotřebí něco udělat pro boj s riziky a výzvami, které drony vytvářejí. Bezpečnost a soukromí jednotlivců je zásadní a musí být zajištěna. S vylepšenými a snadno dostupnými nástroji, které mohou hackeři získat, jsou i méně kvalifikovaní hackeři schopni provádět útoky,

kterých by dříve nebyli schopni. Drony mohou být napadeny buď zachycením, modifikací vložením datového toku do telemetrického spojení přes sériový port, nebo je možné, že útočník podvrhne spojení a tím dosáhne úplné kontroly nad rozhraním. Mezi některé významné obavy patří. [74]

- **Soukromí:** Pro drony je běžné, že mají možnost vidět a zachytit data ve formě obrázků a videa. Ochrana osobních údajů vyvolává obavy. Uživatelé takových dronů, vybavených kamerami, mohou bez souhlasu jednoduše zachytit záběry (livestream, nebo záznam) jednotlivce, nebo místa. Přestože je tato technologie prospěšná, je pro útočníky prostředkem ke sledování jejich potenciálních cílů. [74]
- **Přístup k datům:** Obrazy shromážděné dronem budou pravděpodobně přenášeny zpět uživateli, nebo do cloudu. Použité připojení není vždy bezpečné. Díky tomu je přístup k datům poměrně jednoduchý. Útočník tedy může zachytit a ukrást data. [74]
- **Drony se zbraněmi:** Drony lze použít pro bojové účely. Tím se stávají bezpečnostním problémem a nebezpečím pro obyvatelstvo. [74]
- **Vzdálené únosy:** Problémům, kterým drony čelí, jsou stejné jako u jiných technologií, které využívají bezdrátovou komunikaci. Drony jsou zpravidla řízeny připojením k dálkově ovládanému zařízení (smartphone, tablet, nebo speciální zařízení) přes Wi-Fi, nebo Bluetooth a toto spojení není většinou bezpečnostně zajištěno. Je-li připojení Wi-Fi otevřeno, tedy nezabezpečené, může se k němu kdokoli připojit a napadnout tak dron. Je velmi důležité, aby tyto technologie měly přísná bezpečnostní opatření. [74] Pokud je dron pod vlivem útočníka, není nic, co by mohl uživatel udělat, aby získal kontrolu zpět. Nejenže to může vést ke krádeži dronu, ale větší obavou je potenciální riziko pro veřejnou bezpečnost. [74]
- **Nezabezpečené protokoly:** Implementované protokoly nejsou tak bezpečné, jak by měly být a umožňují útočníkům instalovat škodlivý software do systémů. Systémy jsou často také zranitelné, když zařízení nefunguje, protože je stále připojeno k internetu pro nahrávání zachycených dat, nebo aktualizačního softwaru. Pokud není připojení řádně zajištěno, je to příležitost k zavedení škodlivého kódu. [74]

7.2. Využití dronů v Inteligentním městě

Drony disponují širokou škálu využití, v následující podkapitole popíši několik těchto využití pro inteligentní město.

Dodávaní balíčků

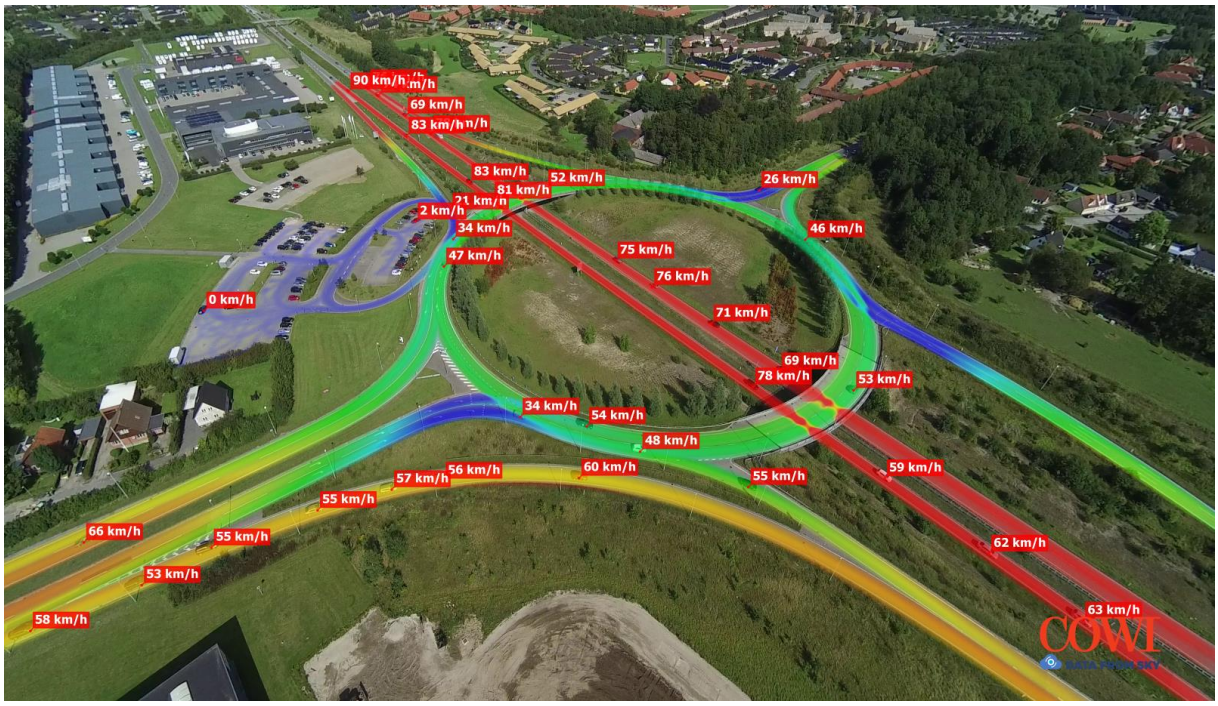
Vylepšení služeb je důležitou součástí inteligentního města. Drony mohou značně přispět k dodávání balíčku, mnoho významných prodejců a logistických společností vyvíjejí úsilí o začlenění dronů do svých systémů. V roce 2016 společnost DHL úspěšně uskutečnila více než 100 dodávek s dronem Parcelcopter 3.0 v Bavorských Alpách. [78] Amazon vytvořil obrovskou soutěž o legalizaci svého doručovacího projektu s názvem "Prime Air", jak je ukázáno na obr. 3. [79]

Obrázek 10: Amazon Prime Air Drone

Zdroj [77]

Monitoring provozu

Monitorování přes dron představuje novou perspektivu, která by mohla pomoci v optimalizaci systémů silničního provozu překonáním omezení tradičních metod sledování z důvodu jejich mobility a schopnost pokrýt velkou plochu. Také kvůli rostoucímu objemu provozu ve městech vyžaduje nejmodernější inteligentní zařízení ke sledování provozu pomocí přesných informací o dopravních tocích a dopravních nehodách s cílem omezit přetížení provozu. [80] Příkladem může být COWI, což je dánská inženýrská společnost, patří mezi první, která používá technologii dronů pro sledování a analýzu dopravního provozu. [81]



Obrázek 11: COWI monitoring dopravy

Zdroj [32]

Hasičské a záchranné operace

Drony mohou provést záchranné operace bezpečněji, rychleji a efektivněji než tradiční operace s posádkou. Protože mohou létat samostatně a přistupovat k obtížně dostupným oblastem a provádět shromažďování dat, které je pro lidi nemožné. [82] Příkladem je: "Knight Hawk" specializovaný protipožární dron vybavený tepelnými senzory a navigačním systémem.

7.3. Bezpečnostní hrozby

V současné době mají civilní drony různou úroveň bezpečnosti, a to hlavně v závislosti na jejich ceně. [31] Například studie v běžně používaném civilním dronu Parrot AR Drone 2

však ukázala nedostatečné zabezpečení. Dron používá nezabezpečené připojení WiFi mezi inteligentním zařízením, jako je smartphone, či jiný ovladač a řídicím systémem na bázi Linuxu, který řídí let. Palubní systém běží s privilegovaným uživatelským účtem (root) a s otevřenými službami Telnet a FTP pro interakci. Kybernetické hrozby, kterým dron čelí, jsou tedy na vysoké úrovni. [27]

Civilní drony nepoužívají kryptografické techniky k zabezpečení komunikace mezi řídicími systémy a samotným dronem. Metody používané ke komunikaci s jednotlivými řadiči lze snadno prolomit, a to je příležitost i pro méně schopné hackery. Jako takové mohou být civilní drony náchylné na vzdálené únosy, ztrátu připojení, zachycení videa, a dokonce převzetí celkové kontroly nad dronem. [31] V ideálním případě je tedy nutné používat šifrovanou komunikaci, a tu levnější modely nenabízejí. [27]

Tabulka 4 poskytuje přehled o různých typech hrozeb, kterým dron čelí.

Ohrožení	**Dopad**
Chyba systému, nevysvětlitelné vypnutí	Dron letí mimo kurs, případně do uzavřeného pásma, které představuje hrozbu pro bezpečnost letecké společnosti, městské bezpečnosti atd.
Útok MITM	Dron může být unesen a použit pro různé účely
Slabé zabezpečení (šifrování, autentizace, jedinečný klíč pro všechna zařízení)	Dron může být unesen a použit pro různé účely
Zfalšování GPS geolokace	Dron bude cestovat do falešného bodu a potenciálně způsobí poškození
DOS proti spojení C2	Dron je paralyzovaný a nedá se kontrolovat přes příkazy
DOS proti spojení s Cloudem	"Připojený dron" ztratí přístup k databázi
Zatížení senzorů dronu	Systém zpracovává chybná data
Únik dat z důvodu chyby softwaru, nebo konfigurace	Zneužití dat útočníkem
Nezabezpečené protokoly	Instalace škodlivého softwaru, odposlech

Tabulka 4: Souhrn hrozen a jejich dopadů pro UAV

Zdroj [83]

7.4. Legislativa

V ČR dohlíží na provoz UAV úřad pro civilní letectví. Dronů se hlavně týká l letecký předpis „Pravidla létání L2“ A „Doplněk X – bezpilotní systémy“ tento předpis byl vydaný 4.12. 2014. Protože je tato legislativa velmi rozsáhlá, vyberu pouze výčet některých pravidel.

Pravidla létání L2

- Minimální výšky: S výjimkou, kdy je to nezbytné pro vzlet nebo přistání, nebo s výjimkou, kdy tak povolil příslušný úřad, letadlo nesmí letět nad hustě zastavěnými místy (města, vesnice, a jiná obydlená místa), nebo nad shromážděním osob na volném prostranství, pokud není ve výšce, která by v případě vzniklé nouze umožnila přistání bez ohrožení osob nebo majetku na povrchu země. [85]

Doplněk X – bezpilotní systémy

- 3.1 - Let bezpilotního letadla smí být prováděn jen takovým způsobem, aby nedošlo k ohrožení bezpečnosti létání ve vzdušném prostoru, osob a majetku na zemi a životního prostředí. [85]
- 8. - S výjimkou, kdy tak povolí ÚCL na základě předchozího souhlasu příslušného správního orgánu či oprávněné osoby, se let bezpilotního letadla nesmí provádět v ochranných pásmech stanovených příslušnými právními předpisy podél nadzemních dopravních staveb, tras nadzemních inženýrských sítí, tras nadzemních telekomunikačních sítí, uvnitř zvláště chráněných území, v okolí vodních zdrojů a objektů důležitých pro obranu státu. Nad těmito ochrannými pásmy smí být let prováděn pouze způsobem vylučujícím jejich narušení za běžných i mimořádných okolností.[85]
- 4. - S výjimkou, kdy ÚCL povolí jinak, musí být bezpilotní letadlo provozováno v přímém dohledu pilota, tj. takovým způsobem a do takové vzdálenosti, aby: [85]
    a) pilot během pojíždění a letu mohl udržovat trvalý vizuální kontakt s bezpilotním letadlem i bez vizuálních pomůcek jiných než brýle a kontaktní čočky na lékařský předpis [85]
    b) pilot, nebo kromě pilota i poučená osoba, mohl sledovat a vyhodnocovat dohlednost, překážky a okolní letový provoz [85]

ř.	maximální vzletová hmotnost	≤ 0,91 kg		> 0,91 kg a < 7 kg		7 – 25 kg		> 25 kg		bezpilotní letadlo provozované mimo dohled pilota
-	účel použití ---------- požadavek	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	
1	evidence letadla	ne	ano	ne	ano	ne	ano	ano	ano	ano
2	evidence pilota	ne	ano	ne	ano	ne	ano	ano	ano	ano
3	praktický a teoretický test pilota	ne	ano	ne	ano	ne	ano	ano	ano	ano
4	povolení k létání	ne	ano	ne	ano	ne	ano	ano	ano	ano
5	povolení k provádění LP a LČPVP	nelze	ano	nelze	ano	nelze	ano	nelze	ano	nelze
6	označení UA: ID štítek / ID štítek + pozn. značka	ne / ne	ano / ano	ano / ne	ano / ano	ano / ne	ano / ano	ano / ne	ano / ano	ano / ano
7	min. ve vzdálenosti (m): vzlet, přistání / osoby, stavby / osídlený prostor	bezpečná	bezpečná	bezpečná	bezpečná	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150
8	pojištění: běžný provoz / LVV (mil. Kč)	ne / 0,25	dle nař. č. 785/2004[1]	ne / 1	dle nař. č. 785/2004[1]	ne / 3 od 20 kg dle nař. č. 785/2004 [1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]
9	dozor	ne	ne	ne	ne	ne	ne	ano	ano	ne
10	„failsafe“ systém	ne	ano	ano	ano	ano	ano	ano	ano	ano
11	provozní příručka UAS	ne	ano	ne	ano	ne	ano	ne	ano	ne
12	hlášení událostí	ne	ano	ne	ano	ne	ano	ano	ano	ano

Tabulka 5: Podmínky užívání dronů v ČR

Zdroj [85]

7.5. Souhrn

Drony mají obrovské využití pro budoucí inteligentní města. Ale stejně jako u dalších konceptů se při návrhu a výrobě nehledělo na zabezpečení, ale především na efektivitu. Zejména u levných modelů zabezpečení chybí, a i u ostatní modely pořád čelí stejným hrozbám jako bezdrátové sítě. Protiopatření zajistí použití silného šifrování a aktuální software ani to však není 100 % ochrana. Legislativa zpřísňuje používání dronů a pro budoucí provoz a jejich plné využití je třeba úprav.

8. ZÁVĚR

Cílem této práce bylo shrnutí bezpečnostních rizik projektů "Smart Cities" na základě mezinárodní literární rešerše. Dospěl jsem k závěru, že při návrhu a tvorbě zkoumaných konceptů hlavně komunikačních protokolů byl kladen důraz na použitelnost a efektivitu, čímž byla bezpečnost upozaděna. UAV, BAS, inteligentní vozidla a inteligentní sítě jsou vystaveny stejným hrozbám jako tradiční datové sítě tedy útokům DOS, Replay, MITM. Používáním bezdrátové komunikace riziko ještě vzroste. Komunikační protokoly nepoužívají žádné, nebo jen slabé šifrování to je vystavuje riziku odposlechu, manipulace a zneužití dat, které přenáší.

V své práci dále uvádím, jak některým těmto bezpečnostním rizikům čelit. Za použití kontroly přístupu, certifikátů a silného šifrování. Do budoucna je potřeba tyto postupy aplikovat a upravit legislativu UAV, aby mohl být plně využit potenciál dronů pro inteligentní město.

Největší riziko hrozí u inteligentních vozidel, kde proniknutí do vnitřního systému může vést k odcizení vozidla, nebo způsobit vážnou autonehodu s dopadem na zdraví řidiče. U SG je největším rizikem výpadek celé elektrické rozvodné sítě. V BAS není dopad tak kritický, jedná se především o ztrátu komfortu, třeba kompromitováním chytrých termostatů, za největší riziko považuji výpadek elektrické energie v celé budově. UAV nese bezpečnostní riziko hlavně v otázce soukromí to se snaží řešit zmíněná legislativa, avšak je třeba dalších úprav.

9. ZDROJE

[1] NAM, T., PARDO, T. A. Smart city as urban innovation: Focusing on management, policy, and context. In Procceeding of the 5th international conference on theory and practice of elektronic governance, 2011, pp. 185-194.

[2] ALABA, Fadele Ayotunde, Mazliza OTHMAN, Ibrahim Abaker Targio HASHEM a Faiz ALOTAIBI. Internet of Things security: A survey. In: Journal of Network and Computer Applications [online]. 2017, 88, s. 10-28 [cit. 2018-05-23]. DOI: 10.1016/j.jnca.2017.04.002. ISSN 10848045. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1084804517301455

[3] EDWARDS, L. Privacy, Seurity and Data Protection in Smart Cities: a Critical EU Law Perspective. CREATe Working Paper 2015/11 (December 2015)

[4] Smart city: What is a smart city? [online]. In: . 14.7.2015 [cit. 2018-05-23]. Dostupné z: https://www.wien.gv.at/stadtentwicklung/studien/pdf/b008403j.pdf

[5] T. Bakıcı, E. Almirall, and J. Wareham, "A Smart City Initiative: The Case of Barcelona," Journal of the Knowledge Economy 2: 1 (2012) 1–14.

[6] N. Komninos, "Intelligent Cities: Variable Geometries of Spatial Intelligence," Intelligent Buildings International 3: 3 (2011) 172–188.

[7] R.E. Hall, "The Vision of a Smart City." Proc. of the 2nd International Life Extension TechnologyWorkshop, Paris, France, 2000.

[8] K. Kourtit, and P. Nijkamp, "Smart Cities in the Innovation Age," Innovation: The European Journal of Social Science Research 25: 2 (2012) 93–95.

[9] ALBINO, Vito, Umberto BERARDI a Rosa Maria DANGELICO. Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology* [online]. 2015, **22**(1), 3-21 [cit. 2018-06-20]. DOI: 10.1080/10630732.2014.942092. ISSN 1063-0732. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/10630732.2014.942092

[10] Xu Xiaohui „" Study on Security Problems and Key Technologies of The Internet of Things", 2013 International Conference on Computational and Information Sciences

[11] Yan L, Zhang Y, Yang L T. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, 2008.

[12] N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things, Scientific American 291 (4) (2004) 76–81

[13] Abdemalek Amine, Otmane Ait Mohamed, Boualem Benatellah "Network Security Technologies: Design and Applications

[14] Rolf H. Weber "Internet of Things – New security and privacy challenges" computer law & security review 26(2010) 23 – 30

[15] TANDJAOUI, Djamel, Mohammed RIYADH ABDMEZIEM a Imed ROMDHANI. Architecting the Internet of Things: State of the Art [online]. In: . 2015 [cit. 2018-05-23]. Dostupné z: https://www.researchgate.net/publication/274718805_Architecting_the_Internet_of_Things_State_of_the_Art

[16] SAUNDERS, T., BAECK, P. Rethinking Smart Cities from the Ground up. Nesta, 2015

[17] A., Mayuri a Sudhir T. Internet of Things: Architecture, Security Issues and Countermeasures. In: International Journal of Computer Applications [online]. 2015, 125(14), s. 1-4 [cit. 2018-05-23]. DOI: 10.5120/ijca2015906251. ISSN 09758887. Dostupné z: http://www.ijcaonline.org/research/volume125/number14/bhabad-2015-ijca-906251.pdf

[18] SHIDENG, MA a Huang HAI. The Perceptual Environment Security Mechanism Research for Internet of Things [online]. In: . [cit. 2018-05-23]. Dostupné z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiRvP-6pZzbAhUEyaQKHXAxDwcQFjAAegQIARAv&url=http%3A%2F%2Fdownload.atlantis-press.com%2Fphp%2Fdownload_paper.php%3Fid%3D18594&usg=AOvVaw07L0dtf6k-NR1_hHzHqWCH

[19] Co je cloud?. Microsoft Azure [online]. [cit. 2018-05-23]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-the-cloud/

[20] Co je veřejný cloud?. Microsoft Azure [online]. [cit. 2018-05-23]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-a-public-cloud/

[21] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[22] Global Netoptex Incorporated. “Demystifying the cloud. Important opportunities, crucial choices.” pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[23] J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” Infoworld, Available: <http://www.infoworld.com/d/security-central/gartner-sevencloudcomputingsecurity-risks-853?page=0,1> [Mar. 13, 2009].

[24] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].

[25] KUYORO, S. O., F. IBIKUNLE a O. AWODELE. Cloud Computing Security Issues and Challenges [online]. 2011, December 2011 [cit. 2018-05-23]. Dostupné z: https://www.researchgate.net/publication/285011991_Cloud_Computing_Security_Issues_and_Challenges

[26] Oracle launches new cloud services. Em360tech [online]. 2016, 19th September 2016 [cit. 2018-05-23]. Dostupné z: https://www.em360tech.com/tech-news/oracle-launches-new-cloud-services-says-amazons-dominance-is-over/

[27] BAIG, Zubair A., Patryk SZEWCZYK, Craig VALLI, et al. Future challenges for smart cities: Cyber-security and digital forensics. In: Digital Investigation [online]. 2017, 22, s. 3-13 [cit. 2018-05-20]. DOI: 10.1016/j.diin.2017.06.015. ISSN 17422876. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1742287617300579

[28] Khatoun, R., Zeadally, S., 2016. Smart cities: concepts, architectures, research opportunities. Commun. ACM 59 (8), 46-57.

[29] BAS-Behind-the-Scenes2. In: *Myatrservice.com* [online]. [cit. 2018-06-21]. Dostupné z: http://myatrservice.com/home/wp-content/uploads/BAS-Behind-the-Scenes2.jpg

[30] Lilis, G., Conus, G., Asadi, N., Kayal, M., 2015. Integrating building automation technologies with smart cities: an assessment study of past, current and future interroperable technologies. In: International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), pp. 1-6

[31] Peacock, M., 2014. Detection and Control of Small Civilian Uavs. Thesis. http://ro.ecu.edu.au/theses_hons/120

[32] COWI presents DataFromSky on Transportforum in Sweden. Datafromsky [online]. January 8th, 2018 [cit. 2018-05-23]. Dostupné z: http://datafromsky.com/news/cowi-presents-datafromsky-on-transportforum-in-sweden/

[33] PEACOCK, Matthew a Michael N. Johnstone N. JOHNSTONE. An analysis of security issues in building automation systems [online]. 2014, , 100-104 [cit. 2018-04-16]. DOI: 10.4225/75/57b691dfd9386. Dostupné z: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1173&context=ism

[34] Flow-Based Security Issue Detection in Building Automation and Control Networks. Information and Communication Technologies [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, 2012, , 64-75 [cit. 2018-04-16]. Lecture Notes in Computer Science. DOI: 10.1007/978-3-642-32808-4_7. ISBN 978-3-642-32807-7. Dostupné z: http://link.springer.com/10.1007/978-3-642-32808-4_7

[35] INCIBE. BMS: Intelligent buildings – are they secure? [online]. 01/26/2016, 2016 [cit. 2018-04-16]. Dostupné z: https://www.certsi.es/en/blog/bms-intelligent-buildings-secure

[36] Komunikace protokolem BACnet. Promotic.eu [online]. [cit. 2018-04-16]. Dostupné z: https://www.promotic.eu/cz/pmdoc/Subsystems/Comm/Protocol/BACnet.htm

[37] INCIBE. Security in Protocols for Building Automation [online]. 04/20/2017, 2017 [cit. 2018-04-16]. Dostupné z: https://www.certsi.es/en/blog/security-protocols-building-automation

[38] BACnet – A Data Communication Protocol for Building Automation and Control Networks", ANSI/ASHRAE 135, 2004

[39] C. Schwaiger and A. Treytl, "Smart Card Based Security for Fieldbus Systems", in Proc. IEEE Conference on Emerging Technologies and Factory Automation (WFCS), volume 1, 2003, pp. 398–406.

[40] D. G. Holmberg, "BACnet Wide Area Network Security Threat Assessment", Technical report, National Institute of Standards and Technology, 2003.

[41] McDaniel, P., McLaughlin, S., 2009. Security and privacy challenges in the smart grid. IEEE Secur. Priv. 7 (3), 75-77

[42] J. Zachary, R. Brooks, and D. Thompson, “Secure Integration of Building Networks into the Global Internet”, Technical report, National Institute of Standards and Technology, 2002.

[43] GRANZER, W., W. KASTNER, G. NEUGSCHWANDTNER a F. PRAUS. Security in networked building automation systems. 2006 IEEE International Workshop on Factory Communication Systems [online]. IEEE, 2006, 2006, , 283-292 [cit. 2018-04-16]. DOI: 10.1109/WFCS.2006.1704168. ISBN 1-4244-0379-0. Dostupné z: http://ieeexplore.ieee.org/document/1704168/

[44] GLANZER, Harald, Lukas KRAMMER a Wolfgang KASTNER. Increasing security and availability in KNX networks [online]. 2016, , 241-252 [cit. 2018-04-16]. Dostupné z: https://subs.emis.de/LNI/Proceedings/Proceedings256/241.pdf

[45] A. D. Wood and J. A. Stankovic, “Denial of Service in Sensor Networks”, IEEE Computer, vol. 35, no. 10, pp. 54–62, 2002.

[46] ERIC J, Byres. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems [online]. 2004, , 1-6 [cit. 2018-04-17]. Dostupné z: https://www.researchgate.net/publication/237240867_The_Myths_and_Facts_behind_Cyber_Security_Risks_for_Industrial_Control_Systems

[47] Security Predictions 2012 & 2013 - The EmergingSecurity Threat [online]. [cit. 2018-04-17]. Dostupné z: https://www.sans.edu/cyber-research/security-laboratory/article/security-predict2011

[48] European Technology Platform Smart Grid, 'Strategic research agenda for Europe‘s electricity networks for the future', European Commission, Directorate General for Research, Directorate Energy, 2007.

[49] Smart Grid: A Beginner's Guide. Available online: http://www.nist.gov/smartgrid/beginnersguide.cfm

[50] Saifur Rahman, ‘Smart Grid and its Role in Reducing Peak Demand and Improving Electricity Delivery’. Page- 19

[51] R. Langer. “Stuxnet: Dissecting a Cyberwarfare Weapon”, IEEE Security&Privacy, Vol.9, N. 3, 20111

[52] BEKARA, Chakib. Security Issues and Challenges for the IoT-based Smart Grid. Procedia Computer Science [online]. 2014, 34, 532-537 [cit. 2018-05-16]. DOI:

10.1016/j.procs.2014.07.064. ISSN 18770509. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1877050914009193

[53] Wei D, Lu Y, Jafari M, et al. An integrated security system of protecting smart grid against cyber attacks. In: Proc. of the IEEE PES Conference on Innovative Smart Grid Technologies, 2010:1-7.

[54] ALOUL, Fadi, A. R. AL-ALI, Rami AL-DALKY, Mamoun AL-MARDINI a Wassim EL-HAJJ. International Journal of Smart Grid and Clean Energy: Smart Grid Security: Threats, Vulnerabilities and Solutions [online]. 2012 [cit. 2018-05-16]. Dostupné z: http://www.ijsgce.com/uploadfile/2012/1011/20121011121836539.pdf

[55] Metke AR and Ekl RL. Security technology for smart grid networks. IEEE Transactions on Smart Grid, 2010; 1(1):99-107.

[56] BHISEY, Rohit. Growing Implementation of Smart Meter Technologies to Improve Smart Grid Capability [online]. June 6, 2017 [cit. 2018-05-23]. Dostupné z: http://www.editiontruth.com/wp-content/uploads/2017/06/Smart-Grid-696x464.jpg

[57] TUBALLA, Maria Lorena a Michael Lochinvar ABUNDO. A review of the development of Smart Grid technologies. In: Renewable and Sustainable Energy Reviews [online]. 2016, 59, s. 710-725 [cit. 2018-05-23]. DOI: 10.1016/j.rser.2016.01.011. ISSN 13640321. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1364032116000393

[58] Iyer S. Cyber Security for Smart Grid, Cryptography, and Privacy. International Journal of Digital Multimedia Broadcasting, 2011; doi:10.1155/2011/372020.

[59] WOLF, Marko, Andre WEIMERSKIRCH a Christof PAAR. Security in automotive bus systems. 2004. Dostupné také z: http://www.weika.eu/papers/WolfEtAl_SecureBus.pdf

[60] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Cyber Security and Resilience of smart cars: Good practices and recommendations [online]. DECEMBER 2016. 2016 [cit. 2018-05-28]. ISBN 978-92-9204-184-7. doi: 10.2824/87614. Dostupné z: https://publications.europa.eu/en/publication-detail/-/publication/13d4bf8d-e9de-11e6-ad7c-01aa75ed71a1/language-en

[61] stake Security Consulting Inc. Webpage, 2003. www.atstake.com/events_news/press_mentions/press_mentions_2003.html

[62] Bundesamt für Sicherheit in der Informationstechnik. Bluetooth – Gefährdungen und Sicherheitsmaÿnahmen. In www.bsi.de/literat/doc/bluetooth/bluetooth.pdf, 2003.

[63] M. Jakobsson, S. Wetzel. Security Weaknesses in Bluetooth. In Lecture Notes in Computer Science, Vol. 220, 2001, pp. 176+.

[64] GUPTA, Ankul. Electronic Control Unit(ECU) [online]. 2015 [cit. 2018-05-12]. Dostupné z: https://www.slideshare.net/AnkulGupta2/electronic-control-unitecu

[65] Radovan Miucic and Syed Masud Mahmud. Wireless Multicasting for Remote Software Upload in Vehicles with Realistic Vehicle Movement. Technical report, Electrical and Computer Engineering Department, Wayne State University, Detroit, MI 48202, USA, 2005.

[66] Moshe Shavit, Andy Gryc, and Radovan Miucic. Firmware Update over the Air (FOTA) for Automotive Industry. In Asia Pacific Automotive Engineering Conference, Hollywood, CA, USA, August 2007.

[67] Inteligentní auto. Chip.cz [online]. 09.10.2011 [cit. 2018-05-25]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/vydani/r-2011/chip-09-11/iq-auto/

[68] LARSON, U.E., P.H. PHUNG a D.K. NILSSON. Vehicle ECU classification based on safety-security characteristics. IET Road Transport Information and Control Conference and the ITS United Kingdom Members' Conference (RTIC 2008) [online]. Institution of Engineering and Technology, 2008, 2008 [cit. 2018-05-12]. DOI: 10.1049/ic.2008.0810. ISBN 978-0-86341-920-1. Dostupné z: http://digital-library.theiet.org/content/conferences/10.1049/ic.2008.0810

[69] H. BAKER, Edward, David CRUSIUS, Marco FISCHER, et al. Opportunities, risk, and turmoil on the road to autonomous vehicles [online]. 2016, 2016 [cit. 2018-05-12]. Dostupné z: https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjpt6DgtoDbAhWhCpoKHcPxAGMQFggtMAA&url=https%3A%2F%2Fwww.mckinsey.de%2Ffiles%2Fmck_connected_car_report.pdf&usg=AOvVaw2rqdYQnle1UyQPHd5wyW5M

[70] BECSI, Tamas, Szilard ARADI a Peter GASPAR. Security issues and vulnerabilities in connected car systems. 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS) [online]. IEEE, 2015, 2015, , 477-482 [cit.

2018-05-12]. DOI: 10.1109/MTITS.2015.7223297. ISBN 978-9-6331-3140-4. Dostupné z: http://ieeexplore.ieee.org/document/7223297/

[71] https://www.powerelectronicsnews.com/technology/the-complex-demands-of-powering-tomorrows-connected-car

[72] BUTTYAN. Hacking cars in the style of Stuxnet [online]. October 28, 2015 [cit. 2018-05-14]. Dostupné z: https://blog.crysys.hu/2015/10/hacking-cars-in-the-style-of-stuxnet/

[73] NHTSA. Concerning Automated Vehicles [online]. 29.5.2013 [cit. 2018-05-14]. Dostupné z: https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf

[74] RICKY, M. a L. MONIQUE MAGALHAES. Drones - Another threat to security [online]. In: . 10.4.2016 [cit. 2018-04-26]. Dostupné z: http://techgenix.com/drones-another-threat-security/

[75] V. Kharchenko and D. Prusov, "Analysis of Unmanned Aircraft Systems Applications in the Civil Field," Taylor and Francis Group, 2012.

[76] Peacock, M., 2014. Detection and Control of Small Civilian Uavs. Thesis. http://ro.ecu.edu.au/theses_hons/120

[77] "AmazonPrimeAir,"[Online].Available:https://www.amazon.com/Amazon-PrimeAir/b?node=803772001 1.

[78] Eric Adams, "DHL's Tilt-Rotor "Parcelcopter" is both awesome and actuallyuseful,"Wired,[Online].Available: https://www.wired.com/2016/05/dhls-new-drone-can-ship-packages-around-alps,accessed May. 19, 2016.

[79] Andrew V. Pestano, "Amazon could start delivering packages by parachute,"UPI,[Online].Available:https://www.upi.com/Top_News/US/ 2017/02/17/Amazon-could-start-deliveringpackages-by parachute/5 141, accessed Feb. 17, 2017

[80] K. Kanistras G. Martins M. Rutherford and K. Valavanis "A survey of unmanned aerial vehicles (uavs) for traffic monitoring, "in Unmanned Aircraft Systems (ICUAS), International Conference on May 2013, pp. 221-234.

[81] R.L. Hansen, "Traffic Monitoring using UAV Technology," The American Surveyor,[Online].Available:http://www.amerisurv.com/content/view/15189/, accessed May 21, 2016.

[82] Lia Reich, “How drones are being used in Disaster Management?” Geo awesomeness, [Online].Available: http://geoawesomeness.com/dronesfly-rescue/, accessed Jan. 26, 2016.

[83] RUSSELL, Brian, Mohamad AMIN HASBINI a Martin TOM-PETERSEN. Establishing a Safe and Secure Municipal Drone Program [online]. In: . February 2017, s. - [cit. 2018-05-23]. DOI: 10.13140/RG.2.2.20879.48800. Dostupné z: https://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf

[84] Parrot AR.Drone 2.0. In: Pcmag.com [online]. SEP 27, 2013 [cit. 2018-05-31]. Dostupné z: https://assets.pcmag.com/media/images/335903-parrot-ar-drone-2-0.jpg?width=1000&height=833

[85] ÚŘAD PRO CIVILNÍ LETECTVÍ. *LETECKÝ PŘEDPIS PRAVIDLA LÉTÁNÍ L 2* [online]. [cit. 2018-06-21]. Dostupné z: https://lis.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/print/L-2_cely.pdf