

Zabezpečení autonomních systémů proti útokům a selháním senzorů

Marek Tyl

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Marek Tyl
Osobní číslo: A22256
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Zabezpečení autonomních systémů proti útokům a selháním senzorů
Téma práce anglicky: Securing autonomous systems against attacks and sensor failures

Zásady pro vypracování

- Vypracujte literární rešerši na téma autonomních robotů v bezpečnostních aplikacích.
- Analyzujte bezpečnostní senzory využívané v autonomních robotech.
- Identifikujte slabiny v aktuálních autonomních robotech.
- Navrhněte experiment pro ověření identifikovaných slabin.
- Vyhodnotte výsledek experimentu a navrhněte ochranné mechanismy.

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

Seznam doporučené literatury:

1. LUCKCUCK, Matt; FARRELL, Marie; DENNIS, Louise A.; DIXON, Clare a FISHER, Michael. Formal Specification and Verification of Autonomous Robotic Systems. Online. ACM Computing Surveys. 2020, roč. 52, č. 5, s. 1–41. ISSN 0360-0300. Dostupné z: <https://doi.org/10.1145/3342355>
2. GNAMBS, Timo a APPEL, Markus. Are robots becoming unpopular? Changes in attitudes towards autonomous robotic systems in Europe. Online. Computers in Human Behavior. 2019, roč. 93, s. 53–61. ISSN 07475632. Dostupné z: <https://doi.org/10.1016/j.chb.2018.11.045>
3. LI, Keyu; XU, Yangxin a MENG, Max Q.-H. An Overview of Systems and Techniques for Autonomous Robotic Ultrasound Acquisitions. Online. IEEE Transactions on Medical Robotics and Bionics. 2021, roč. 3, č. 2, s. 510–524. ISSN 2576-3202. Dostupné z: <https://doi.org/10.1109/TMRB.2021.3072190>
4. GUGAN, Gopi a HAQUE, Anwar. Path Planning for Autonomous Drones: Challenges and Future Directions. Online. Drones. 2023, roč. 7, č. 3. ISSN 2504-446X. Dostupné z: <https://doi.org/10.3390/drones7030169>
5. HUSSEIN, Mahmoud; NOUACER, Réda; CORRADI, Federico; OUHAMMOU, Yassine; VILLAR, Eugenio et al. Key technologies for safe and autonomous drones. Online. Microprocessors and Microsystems. 2021, roč. 87. ISSN 01419331. Dostupné z: <https://doi.org/10.1016/j.micpro.2021.104348>

Vedoucí bakalářské práce: **Ing. Stanislav Kovář, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**

Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Tato bakalářská práce se zabývá problematikou zabezpečení autonomních systémů, zejména jejich odolností vůči útokům a selháním senzorů. V teoretické části je proveden přehled vybraných autonomních systémů a jejich architektur, popsány jsou typy hrozeb, včetně ztráty senzorových dat, výpadků komunikace nebo záměrného rušení. Pozornost je věnována i možnostem ochrany, jako je senzorová redundance, algoritmy pro autonomní rozhodování a šifrování datových přenosů. Praktická část práce se soustředí na experimentální ověření slabiny v oblasti bezdrátové komunikace, při němž byl testován dron VISU L900 PRO SE za použití zařízení Flipper Zero k simulaci rušení řídicího signálu. Výsledky ukazují, že i komerčně dostupné drony jsou náchylné k výpadku kontroly a absence pokročilých obranných mechanismů zvyšuje riziko selhání. Na základě pozorování jsou navrženy kroky ke zvýšení provozní bezpečnosti.

Klíčová slova: autonomní systémy, bezpečnost, dron, experiment, Flipper Zero, návrh ochranných opatření, reakce systému, redundance, rušení komunikace, senzorové selhání

ABSTRACT

This thesis addresses the issue of security of autonomous systems, in particular their resilience to attacks and sensor failures. In the theoretical part, an overview of selected autonomous systems and their architectures is given, and the types of threats are described, including sensor data loss, communication failures or intentional jamming. Attention is also paid to protection options such as sensor redundancy, algorithms for autonomous decision making, and encryption of data transmissions. The practical part of the thesis focuses on experimental verification of the weakness in wireless communication, in which the VISU L900 PRO SE drone was tested using the Flipper Zero device to simulate control signal interference. The results show that even commercially available drones are susceptible to control failure and the lack of advanced defence mechanisms increases the risk of failure. Based on the observations, steps to improve operational safety are proposed.

Keywords: autonomous systems, security, drone, experiment, Flipper Zero, design of protective measures, system response, redundancy, communication interference, sensor failure

Děkuji své přítelkyni a rodině za podporu během psaní této bakalářské práce. Velké poděkování patří především vedoucímu mé bakalářské práce panu doktorovi Stanislavu Kovářovi, za odborné vedení a trpělivost, kterou mi po celou dobu věnoval.

„The real problem is not whether machines think but whether men do.“

B. F. Skinner

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	13
1 ÚVOD DO PROBLEMATIKY AUTONOMNÍCH SYSTÉMŮ.....	14
1.1 DEFINICE AUTONOMNÍCH SYSTÉMŮ.....	14
1.2 HISTORIE A VÝVOJ AUTONOMNÍCH TECHNOLOGIÍ.....	15
1.3 VÝZNAM AUTONOMNÍCH SYSTÉMŮ V MODERNÍ SPOLEČNOSTI.....	17
2 BEZPEČNOST AUTONOMNÍCH SYSTÉMŮ	19
2.1 ZÁKLADNÍ POJMY V OBLASTI BEZPEČNOSTI.....	19
2.2 SPECIFIKA ZABEZPEČENÍ AUTONOMNÍCH SYSTÉMŮ	20
2.3 VÝZNAM SENZORŮ A KOMUNIKAČNÍCH KANÁLŮ	21
3 BEZPEČNOSTNÍ HROZBY PRO AUTONOMNÍ SYSTÉMY.....	23
3.1 KYBERNETICKÉ ÚTOKY NA AUTONOMNÍ SYSTÉMY	23
3.1.1 Útoky na integritu senzorových dat	23
3.1.2 Útoky na komunikační kanály	24
3.2 SELHÁNÍ SENZORŮ	25
3.2.1 Příčiny selhání senzorů	26
3.2.2 Následky selhání senzorů.....	26
3.3 PŘÍKLADY REÁLNÝCH INCIDENTŮ	27
3.3.1 Selhání autonomních vozidel	27
3.3.2 Incidentsy v průmyslové automatizaci	27
3.3.3 Incidentsy s drony	28
4 OCHRANNÉ MECHANISMY V AUTONOMNÍCH SYSTÉMECH	29
4.1 DETEKCE ÚTOKŮ A MONITOROVÁNÍ SENZORŮ.....	29
4.1.1 Analýza dat ze senzorů.....	29
4.1.2 Strojové učení a AI.....	30
4.2 ZABEZPEČENÍ KOMUNIKAČNÍCH KANÁLŮ.....	30
4.2.1 Šifrování a autentizace dat	31
4.2.2 Bezpečné komunikační protokoly	31
4.3 ZVYŠOVÁNÍ SPOLEHLIVOSTI SENZOROVÝCH SYSTÉMŮ	32
4.3.1 Hardwarová redundance.....	32
4.3.2 Softwarové metody zajištění spolehlivosti.....	33
5 LEGISLATIVNÍ A ETICKÉ ASPEKTY ZABEZPEČENÍ AUTONOMNÍCH SYSTÉMŮ	34
5.1 MEZINÁRODNÍ STANDARDY A REGULACE.....	34
5.2 ETICKÁ DILEMATA A ZNEUŽITELNOST AUTONOMNÍCH SYSTÉMŮ	35

5.3	TECHNICKÉ ASPEKTY SLEDOVÁNÍ A VYHODNOCENÍ SELHÁNÍ AUTONOMNÍCH SYSTÉMŮ	36
II	PRAKTICKÁ ČÁST	39
6	ANALÝZA ZRANITELNOSTI AUTONOMNÍHO SYSTÉMU A EXPERIMENTÁLNÍ OVĚŘENÍ	40
6.1	METODIKA PRAKTICKÉ ČÁSTI	42
6.2	MODEL AUTONOMNÍHO SYSTÉMU	42
6.3	SWOT ANALÝZA ARCHITEKTURY SYSTÉMU	44
6.4	IDENTIFIKACE KLÍČOVÝCH SLABIN SYSTÉMU	45
6.5	TEST REAKCE NA RUŠENÍ ŘÍDICÍ KOMUNIKACE	46
7	VYHODNOCENÍ VÝSLEDKŮ EXPERIMENTU	55
7.1	ANALÝZA NAMĚŘENÝCH HODNOT A CHOVÁNÍ SYSTÉMU	56
8	NÁVRH OCHRANNÝCH OPATŘENÍ	57
	ZÁVĚR	59
	SEZNAM POUŽITÉ LITERATURY	61
	SEZNAM OBRÁZKŮ	68
	SEZNAM TABULEK	69
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	70

ÚVOD

Autonomní systémy představují jednu z nejdynamičtější se rozvíjejících oblastí současné techniky a informatiky. Jejich nasazení v reálném prostředí přináší významné výhody v oblasti efektivitu, přesnosti, snížení lidské zátěže a schopnosti operovat v podmínkách, které by pro člověka byly nebezpečné nebo nedostupné. Uplatnění nacházejí jak v civilním sektoru, například v dopravě, průmyslové výrobě či zdravotnictví, tak i v oblasti bezpečnosti a obrany. Autonomní drony, robotická vozidla nebo průzkumné roboty dnes běžně slouží k monitorování objektů, pátrání po osobách, doručování zásilek nebo i k detekci nebezpečných látek. Jejich rostoucí autonomie však zároveň přináší nové výzvy spojené s odpovědností, etickými dilematy, a především s bezpečností provozu.

Bezpečnost autonomních systémů je klíčovým faktorem ovlivňujícím jejich spolehlivost, důvěryhodnost i společenskou přijatelnost. Tyto systémy se při svém rozhodování spoléhají na komplexní sadu senzorů, datových vstupů a softwarových algoritmů. S rostoucí mírou autonomie navíc přibývá situací, kdy lidský operátor nemá možnost okamžitého zásahu. Proto je třeba, aby autonomní systémy byly navrženy tak, aby zvládly neočekávané události, dokázaly rozpoznat selhání a aktivovat adekvátní ochranné mechanismy.

Z hlediska bezpečnostního managementu je nezbytné analyzovat nejen technické aspekty provozu autonomních systémů, ale také identifikovat slabiny, které mohou vést ke kompromitaci jejich funkce. Zvláštní pozornost je třeba věnovat senzorům a komunikačním kanálům, protože právě na těchto místech dochází v praxi nejčastěji k útokům nebo poruchám. Kromě samotné technické odolnosti je přitom důležitá i schopnost systému reagovat – tedy přejít do bezpečnostního režimu, přepnout na záložní senzory nebo alespoň informovat operátora o vzniklé anomálii.

Cílem této bakalářské práce je analyzovat zranitelnosti autonomních systémů se zaměřením na útoky a selhání senzorů a komunikačních prvků, a následně navrhnout a experimentálně ověřit možné ochranné mechanismy. Práce si klade za cíl nejen identifikovat slabá místa, ale také ukázat, jak konkrétní incident může ovlivnit chování systému a jak mu lze čelit. Praktická část se zaměřuje na simulaci výpadku řídicí komunikace u dronu VISU L900 PRO SE, přičemž rušení bude realizováno pomocí zařízení Flipper Zero. Výsledky experimentu poslouží k vyhodnocení schopnosti systému čelit takovému narušení a stanou se základem pro návrh zlepšení.

Pro jazykovou a stylistickou kontrolu textu byl využit nástroj Gemini, vyvinutý společností Google. Tento nástroj napomohl k revizi gramatických chyb a zvýšení srozumitelnosti odborného textu. Všechny finální úpravy byly následně zkontrolovány autorem s ohledem na věcnou i obsahovou správnost.

I TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY AUTONOMNÍCH SYSTÉMŮ

Autonomní systémy (AS) se v posledních letech stávají nedílnou součástí mnoha technologických oblastí. Jejich schopnost samostatného rozhodování bez nutnosti lidského zásahu přináší zásadní změny v oblastech, jako je doprava, průmysl, zdravotnictví či bezpečnostní operace. Cílem této kapitoly je představit základní charakteristiky autonomních systémů, jejich historický vývoj a současné využití v praxi. Porozumění těmto aspektům je klíčové pro pochopení rizik, která s sebou jejich nasazení přináší, a také pro návrh účinných bezpečnostních opatření. [1]

1.1 Definice autonomních systémů

Autonomní systémy lze definovat jako technologie schopné samostatného vykonávání specifických úkolů bez přímého lidského zásahu. Tyto systémy využívají pokročilé algoritmy a umělou inteligenci (AI), aby dokázaly analyzovat okolní prostředí, vyhodnotit situaci a provést rozhodnutí na základě dostupných dat. [1] Typickými prvky autonomních systémů jsou:

- senzory, které poskytují vstupní data o prostředí (např. kamera, radar, LiDAR, GPS);
- procesory a řídicí jednotky, které data analyzují a generují příslušné akce;
- komunikační moduly, umožňující výměnu informací mezi jednotlivými částmi systému nebo s jinými systémy;
- výkonné části, které realizují konkrétní rozhodnutí (např. motory, manipulátory). [1]

Autonomní systémy jsou schopny adaptace na změny prostředí a flexibilní reakce na nečekané situace. Tato schopnost vychází ze zapojení metod strojového učení, díky kterým systémy zlepšují své rozhodování na základě předchozích zkušeností. Jedním z klíčových rysů autonomních systémů je jejich nezávislost, což znamená, že nemusí čekat na přímé pokyny od operátora. Tato vlastnost je klíčová pro aplikace, kde lidský zásah není možný, například v průzkumu nebezpečných oblastí, při záchranných operacích nebo v kosmických misích. [2],[4]

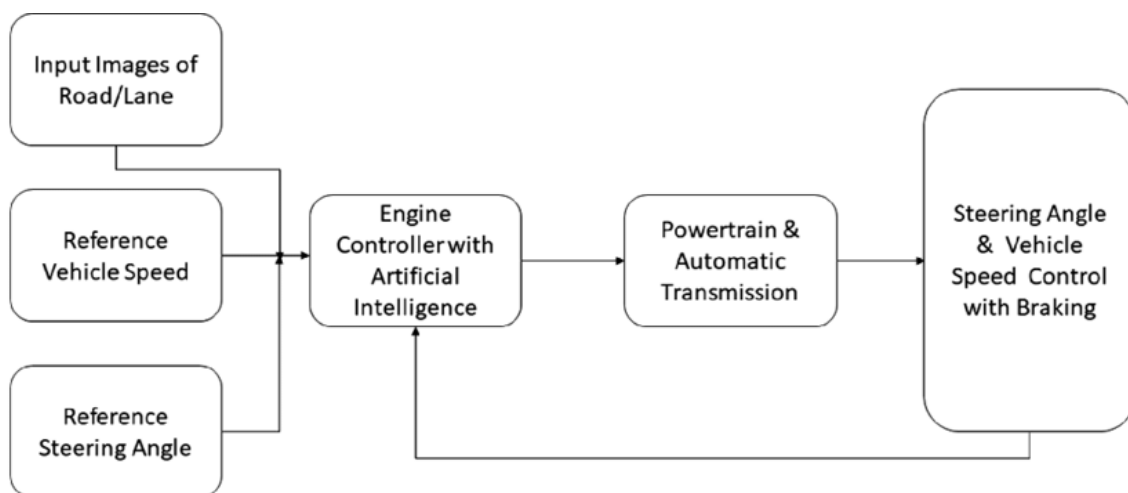
Autonomní systémy nacházejí využití v širokém spektru aplikací:

- drony - slouží pro přepravu, průzkum nebo monitorování (např. drony pro inspekce potrubí nebo hledání osob v obtížně přístupném terénu); příkladem je DJI Matrice

300 RTK, který je vybaven termokamerou a senzory pro průmyslové inspekce a záchranné operace;

- autonomní vozidla - redukuje riziko dopravních nehod a zvyšují efektivitu přepravy; příkladem je Waymo One, plně autonomní taxislužba provozovaná bez řidiče v některých oblastech USA;
- průmysloví roboti - zajišťují vysokou produktivitu a preciznost ve výrobních procesech; příkladem je ABB IRB 6700, robot používaný v automobilovém průmyslu pro těžké montážní a svařovací operace.
- lékařské systémy - například robotické systémy pro autonomní ultrazvukové skenování nebo chirurgii; příkladem je Da Vinci Surgical System, který umožňuje přesné minimálně invazivní chirurgické zákroky řízené robotem. [5]

Přestože autonomní systémy přinášejí obrovský potenciál, jejich nasazení vyžaduje důkladné zabezpečení. Zranitelnosti spojené s neautorizovaným přístupem, fyzickým poškozením senzorů nebo selháním komunikace mohou vést k vážným problémům. Bezpečnost autonomních systémů je proto klíčovým tématem výzkumu i aplikace. [2]



Obrázek 1 - Blokové schéma autonomního vozidla

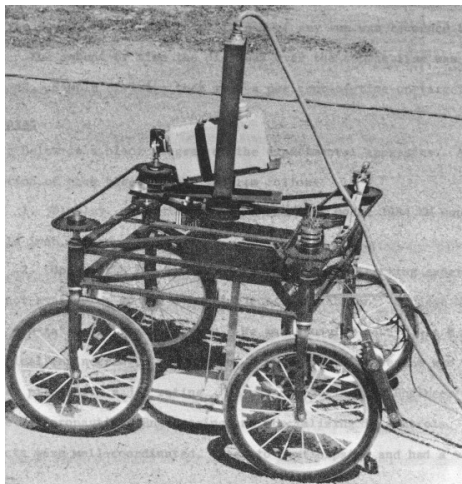
(zdroj:[47])

1.2 Historie a vývoj autonomních technologií

Historie autonomních technologií sahá až do poloviny 20. století, kdy byly poprvé formulovány základy pro stroje schopné samostatného rozhodování. První pokusy o vytvoření autonomních systémů byly ovlivněny vývojem kybernetiky, která se zabývá

studiem samoregulačních systémů. Tato disciplína položila teoretické základy pro návrh prvních autonomních strojů, jež byly původně koncipovány jako robotické systémy s jednoduchými pravidly řízení. [1]

V 60. a 70. letech 20. století se vývoj autonomních technologií zaměřil na robotiku a vojenské aplikace. Například vývoj bezpilotních letadel (UAV - Unmanned Aerial Vehicle) byl z velké části financován armádou Spojených států. Tyto rané drony byly navrženy především pro špiónážní a průzkumné mise. Paralelně s tím vznikaly první autonomní vozidla, přičemž jedním z prvních významných projektů byl vůz Stanford Cart, vyvinutý na Stanfordově univerzitě v 70. letech, který byl schopen základní autonomní navigace. [2]



Obrázek 2 - Stanford Cart: první autonomní vozidlo vyvinuté na Stanfordu

(zdroj:[11])

V 80. a 90. letech došlo k významnému posunu v oblasti senzoriky a zpracování dat, což umožnilo vývoj složitějších autonomních systémů. Zavedení LiDARu (Light Detection and Ranging) jako klíčového senzoru pro měření vzdáleností a mapování prostředí znamenalo revoluci pro autonomní vozidla a drony. Během tohoto období se také začaly objevovat první průmyslové roboty schopné autonomního rozhodování v rámci předem definovaných pravidel. [4]

Začátek 21. století přinesl prudký rozvoj výpočetní techniky a metod umělé inteligence. Systémy strojového učení (machine learning) a hlubokého učení (deep learning) umožnily autonomním technologiím zpracovávat složitější úkoly a rychleji se adaptovat na nové situace. V této době také došlo k rozmachu autonomních vozidel, zejména díky soutěžím,

jako je DARPA Grand Challenge, která významně přispěla k popularizaci a výzkumu autonomního řízení. [5]

Současné autonomní technologie se zaměřují na aplikace v běžném životě, jako je autonomní doprava, průmyslová automatizace a zdravotnictví. Klíčovými prvky moderních systémů je propojení pomocí internetu věcí (IoT), sdílení dat v reálném čase a bezpečnostní prvky, které minimalizují riziko kybernetických útoků nebo selhání systémů. Díky těmto inovacím se autonomní technologie stále více stávají běžnou součástí každodenního života. [3]

1.3 Význam autonomních systémů v moderní společnosti

Autonomní systémy, schopné samostatného vykonávání úkolů bez přímého lidského zásahu, se staly klíčovým prvkem moderní společnosti. Jejich integrace do různých odvětví přináší významné změny v efektivitě, bezpečnosti a kvalitě života.

- **Doprava a mobilita**

V oblasti dopravy autonomní vozidla slibují zvýšení bezpečnosti silničního provozu a efektivitu dopravy. Podle Ministerstva dopravy ČR mohou autonomní systémy přispět k redukci dopravních nehod způsobených lidskou chybou a optimalizaci dopravních toků. [6]

- **Průmysl a výroba**

V průmyslové sféře autonomní systémy umožňují automatizaci výrobních procesů, což vede k vyšší produktivitě a kvalitě výrobků. Podle článku na SystemOnline se průmysl postupně posouvá od tradiční automatizace k autonomním systémům, které dokážou samostatně reagovat na změny ve výrobním prostředí. [7]

- **Zdravotnictví**

V oblasti zdravotnictví autonomní systémy, jako jsou robotické chirurgické nástroje, zvyšují přesnost a efektivitu lékařských zákroků. Autonomní robotické systémy umožňují provádět složité chirurgické procedury s minimálním zásahem, což vede k rychlejšímu zotavení pacientů, jak ukazuje studie publikovaná v časopise *IEEE Transactions on Medical Robotics and Bionics* [8].

- **Logistika a doprava**

Autonomní systémy hrají klíčovou roli v logistice, kde samořiditelná vozidla a drony umožňují efektivní doručování zboží. Podle článku na Vše o průmyslu autonomní stroje a drony přispívají k optimalizaci dodavatelských řetězců a snižování nákladů na dopravu. [9]

- **Etické a právní aspekty**

S rostoucí integrací autonomních systémů do společnosti se objevují nové etické a právní výzvy. Je nezbytné vypracovat rámce pro regulaci a zajištění bezpečnosti autonomních vozidel, aby se minimalizovala rizika spojená s jejich nasazením, jak uvádí Ministerstvo dopravy ČR [6].

Integrace autonomních systémů do moderní společnosti přináší řadu výzev, ale také příležitostí pro zlepšení kvality života, efektivity a bezpečnosti v různých oblastech. Je nezbytné pokračovat ve výzkumu, vývoji a regulaci těchto technologií, aby jejich přínosy byly maximalizovány a potenciální rizika minimalizována.

2 BEZPEČNOST AUTONOMNÍCH SYSTÉMŮ

Bezpečnost AS představuje komplexní a dynamickou oblast výzkumu, která se zabývá ochranou systémů schopných autonomního rozhodování a operací před riziky selhání, kybernetickými útoky a dalšími hrozbami. Tento bod shrnuje základní pojmy spojené s bezpečností těchto systémů a zdůrazňuje hlavní výzvy, které musí být překonány pro jejich efektivní a bezpečné nasazení v reálném světě. [1], [2]

2.1 Základní pojmy v oblasti bezpečnosti

Bezpečnost je základním pojmem nejen v technických a informačních systémech, ale i v oblasti autonomních systémů. Obecně ji lze definovat jako stav, ve kterém je minimalizováno riziko ohrožení životů, majetku nebo systémových procesů. V kontextu moderních technologií bezpečnost zahrnuje ochranu před záměrnými útoky, náhodnými chybami a schopnost odolávat selhání systému. [10]

Jedním z klíčových aspektů bezpečnosti je dostupnost (availability). Ta označuje schopnost systému nebo služby zajistit nepřetržitý přístup ke zdrojům v požadované kvalitě a čase. V případě autonomních systémů, jako jsou drony nebo průmyslové roboty, je klíčové zajistit nepřerušenou funkci komunikačních a řídicích systémů. [1]

Dalším důležitým prvkem je integrita (integrity), tedy ochrana dat před neoprávněnými změnami. U autonomních systémů se to týká zejména sensorových dat, jejichž manipulace může vést k nesprávnému rozhodování systému. [2]

Důvěrnost (confidentiality) se vztahuje na ochranu citlivých informací před neautorizovaným přístupem. To zahrnuje například údaje o poloze zařízení, řídicí algoritmy nebo komunikaci mezi jednotlivými komponentami systému. V případě dronů je důvěrnost klíčová při misích, které zahrnují přenos citlivých dat. [4]

V oblasti autonomních technologií hraje zásadní roli také autonomie a rozhodování. Tyto systémy musí být schopny samostatně reagovat na změny prostředí a činit správná rozhodnutí i v podmínkách nejistoty. To vyžaduje pokročilé algoritmy pro analýzu situací a predikci možných scénářů. [5]

Neméně důležitá je odolnost vůči útokům (resilience), tedy schopnost systému zotavit se z incidentu a pokračovat ve své činnosti. Odolnost se zajišťuje kombinací technik prevence, detekce a reakce, například pomocí redundantních senzorů nebo bezpečných komunikačních protokolů. [3]

2.2 Specifika zabezpečení autonomních systémů

Autonomní systémy představují komplexní integraci softwarových algoritmů, hardwarových komponent a senzorických systémů, které společně umožňují jejich samostatné rozhodování. Tato komplexita však přináší specifické bezpečnostní výzvy. Jedním z hlavních problémů je zajištění integrity komunikace mezi jednotlivými komponentami systému. Například výpadek senzorů nebo zkreslená data mohou způsobit řetězovou reakci, která negativně ovlivní rozhodovací procesy systému. Vzhledem k tomu, že autonomní systémy často fungují v dynamických prostředích, musí být jejich zabezpečení navrženo tak, aby umožňovalo reakci v reálném čase. [1]

Autonomní systémy jsou také častým cílem kybernetických útoků, které mohou ovlivnit jejich rozhodování nebo je zcela vyřadit z provozu. Mezi nejčastější útoky patří manipulace s daty senzorů (např. tzv. data poisoning), útoky typu man-in-the-middle na komunikační kanály a zneužití softwarových zranitelností. Důležitými opatřeními proti těmto hrozbám jsou implementace šifrovacích protokolů, pravidelné aktualizace softwaru a využití monitorovacích systémů pro detekci anomálií. [2]

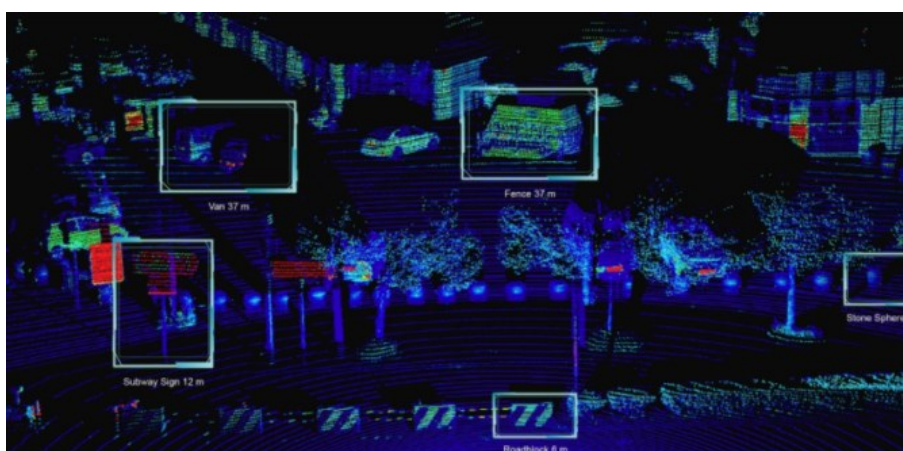
Vedle kybernetických hrozeb čelí autonomní systémy také fyzickým rizikům, jako jsou vandalismus, sabotáže nebo extrémní okolní podmínky (např. teplota, vlhkost, elektromagnetické rušení). Ochrana na fyzické úrovni zahrnuje použití odolných konstrukčních prvků, redundantních komponent a schopnosti systému autonomně se zotavit v případě poškození. Například zapojení více senzorů stejného typu pro ověření správnosti dat významně zvyšuje celkovou odolnost systému. [4]

Klíčovým aspektem bezpečnosti je i odolnost vůči selhání senzorů, které hrají zásadní roli v rozhodovacím procesu. Jakékoli zkreslení, výpadek nebo rušení senzorických dat může způsobit chybnou interpretaci prostředí. Moderní autonomní systémy proto často využívají algoritmy pro fúzi dat, které umožňují identifikovat a eliminovat chybná nebo nedůvěryhodná měření. [5]

V prostředích, kde jakékoli selhání může mít závažné důsledky je důležité uplatňovat principy redundance. Redundantní komponenty a vícevrstvé systémy umožňují autonomním jednotkám pokračovat v provozu i při výpadku některé z částí systému. Kombinace technické redundance a pokročilých rozhodovacích algoritmů výrazně zvyšuje celkovou bezpečnost a spolehlivost těchto technologií. [10]

2.3 Význam senzorů a komunikačních kanálů

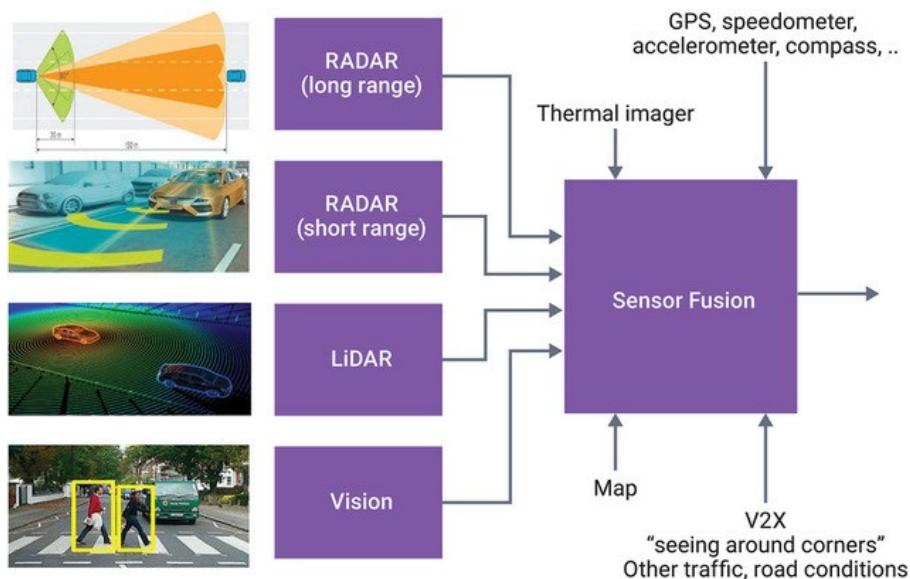
Senzory tvoří základní stavební prvek autonomních systémů, neboť umožňují vnímání okolního prostředí a poskytují data nezbytná pro rozhodování. Používají se různé typy senzorů – od kamerových systémů, lidarů a radarů až po gyroskopy nebo ultrazvukové snímače. Každý typ senzoru má své specifické vlastnosti: například lidar poskytuje detailní 3D mapu okolí, zatímco radar umožňuje detekci pohybujících se objektů na delší vzdálenosti. Úspěšná integrace těchto senzorů do autonomního systému vyžaduje přesnou kalibraci a kombinaci dat z více zdrojů. [11]



Obrázek 3 - Detekce objektů pomocí lidarů

(zdroj:[49])

Fúze dat ze senzorů je klíčovou technikou pro zvýšení přesnosti a spolehlivosti. Tento přístup spočívá v kombinaci informací z různých senzorů, čímž se eliminuje zkreslení nebo výpadky jednotlivých zdrojů. Redundance, tedy záměrné použití více senzorů pro sledování jednoho jevu, je dalším nástrojem pro zvýšení odolnosti systému. Například autonomní vozidla standardně kombinují lidar, kameru a radar, aby získala komplexní obraz o okolí i za zhoršených podmínkách. [12]



Obrázek 4 - Schéma výkonné fúze senzorů s vestavěným rozpočtem

(zdroj:[50])

Stejně důležité jako senzory jsou i komunikační kanály, které umožňují výměnu informací mezi komponentami systému i s okolní infrastrukturou. Tyto kanály musí být navrženy s ohledem na rychlost, nízkou latenci a odolnost vůči výpadkům či útokům. V autonomních dronech zajišťují komunikační kanály přenos telemetrie, příkazů a videozáznamů, přičemž jejich selhání může vést k okamžitému ohrožení bezpečnosti. [13]

Vzhledem k rostoucímu výskytu kybernetických hrozeb je nezbytné přenos dat chránit. To zahrnuje šifrování komunikace, detekci anomálií v síťovém provozu a ochranu proti rušení, například GPS signálu. V budoucnu by mohla významně přispět kvantová kryptografie. V současnosti se běžně používají bezpečné protokoly jako TLS a redundantní komunikační moduly pro minimalizaci výpadků. [14]

Správně integrované senzory a zabezpečené komunikační kanály jsou nezbytné pro autonomní rozhodování. Například v dopravě umožňují autonomním vozidlům předvídat pohyb ostatních účastníků provozu, zatímco komunikace mezi vozidly (V2V) a infrastrukturou (V2I) zajišťuje koordinaci a prevenci kolizí. Tímto způsobem přispívají k vyšší bezpečnosti i efektivitě provozu autonomních systémů. [15]

3 BEZPEČNOSTNÍ HROZBY PRO AUTONOMNÍ SYSTÉMY

S rostoucím nasazením autonomních systémů v kritických oblastech, jako jsou doprava, průmysl nebo zdravotnictví, roste i jejich atraktivita jako cílů kybernetických útoků. Tyto útoky mohou narušit rozhodovací procesy, poškodit infrastrukturu nebo ohrozit bezpečnost uživatelů i okolí. Efektivní zabezpečení autonomních systémů proto vyžaduje detailní pochopení možných vektorů útoku a mechanismů obrany vůči nim. [1]

Jednou z hlavních výzev je fakt, že autonomní systémy jsou často silně propojené s jinými zařízeními prostřednictvím internetu nebo lokálních sítí. Toto propojení vytváří potenciální vektory útoku, které mohou útočníci zneužít k narušení systémů, manipulaci dat nebo získání neoprávněného přístupu. Kromě kybernetických útoků jsou autonomní systémy ohroženy i fyzickými útoky, selháním hardware nebo software a různými provozními anomáliemi. [1]

V následujících podkapitolách jsou detailně popsány hlavní typy bezpečnostních hrozeb, kterým autonomní systémy čelí, včetně kybernetických útoků, selhání senzorů a incidentů v reálném prostředí. Tyto hrozby představují významnou výzvu pro návrh a implementaci ochranných mechanismů, které by zajistily bezpečný provoz autonomních technologií v dynamických a často nepředvídatelných podmínkách.

3.1 Kybernetické útoky na autonomní systémy

Kybernetické útoky na AS jsou jednou z nejzávažnějších výzev v oblasti jejich bezpečnosti. Tyto útoky mohou narušit funkčnost systému, způsobit selhání jeho komponent nebo kompromitovat citlivá data. Rozdělujeme je podle cíle útoku na senzory, komunikační kanály a řídicí algoritmy. [1], [3]

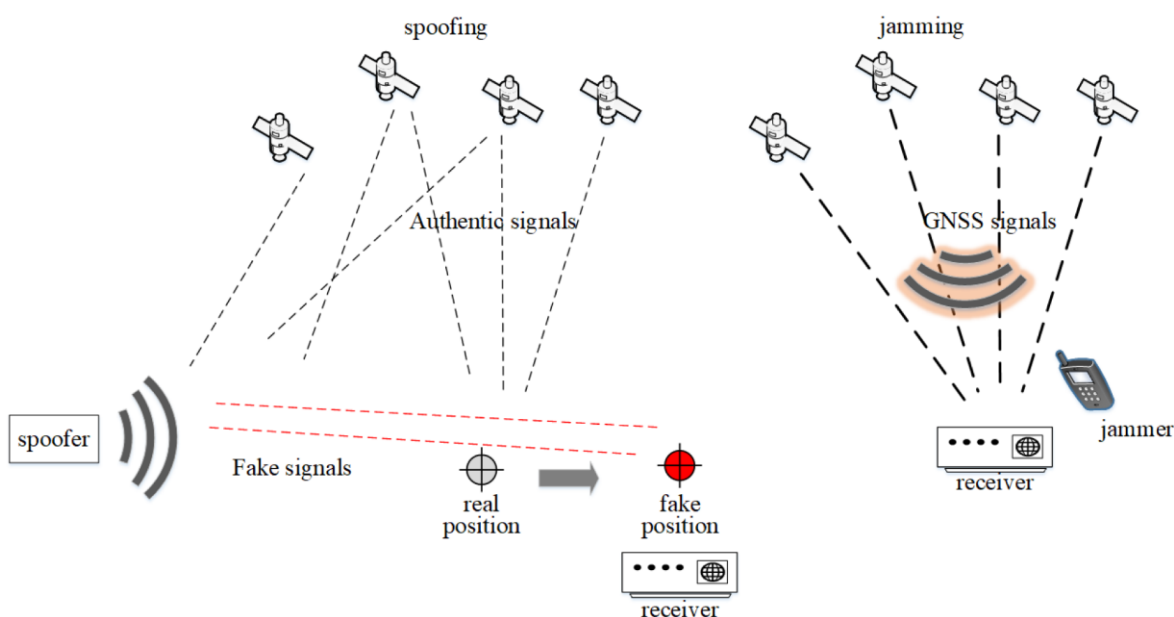
3.1.1 Útoky na integritu senzorových dat

Manipulace s daty

Senzory hrají klíčovou roli při získávání informací z okolí autonomního systému. Útoky zaměřené na změnu dat ze senzorů, jako je například GPS spoofing, mohou způsobit, že systém získá falešné informace o své poloze. To může vést k chybnému rozhodování, což je obzvláště rizikové u autonomních vozidel nebo dronů. Dalším příkladem jsou útoky na kamerové systémy, které mohou zmanipulovat obrazová data a ovlivnit procesy jako je rozpoznávání objektů. [16]

Jamming signálů senzorů

Útoky typu jamming, tedy rušení signálů senzorů, mohou způsobit ztrátu klíčových dat potřebných pro provoz autonomního systému. Typickým cílem těchto útoků je GPS nebo LIDAR, jejichž rušení může vést k dezorientaci systému nebo k výpadkům v navigaci. Efektivní obrana proti jammingu zahrnuje redundanci senzorů a použití pokročilých filtrovacích algoritmů. [17]



Obrázek 5 - rozdíl mezi spoofing a jamming

(zdroj:[51])

Útoky na fyzickou integritu senzorů

Útočníci mohou fyzicky narušit senzory, například jejich oslepením laserem nebo zničením pomocí nárazu. Tyto útoky jsou obzvláště nebezpečné v prostředí, kde autonomní systémy operují bez přímého lidského dohledu. Prevence zahrnuje implementaci ochranných obalů a využití více redundantních senzorů. [18]

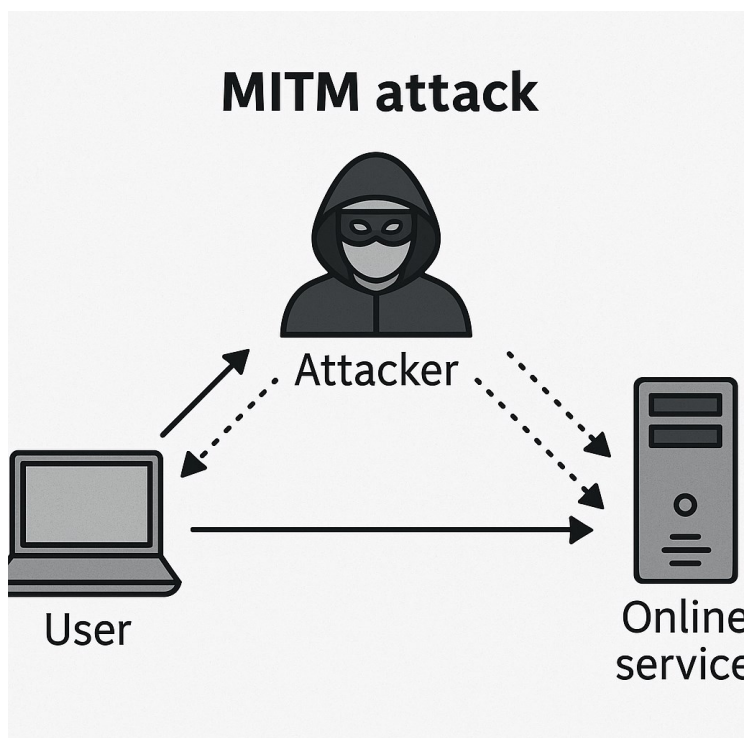
3.1.2 Útoky na komunikační kanály

Denial of Service (DoS) a Distributed Denial of Service (DDoS)

Útoky typu DoS a DDoS cílí na zahlcení komunikačních kanálů autonomního systému, což vede k nedostupnosti služeb nebo zpožděním v přenosu dat. Například autonomní vozidlo se může stát obětí DDoS útoku, který přeruší komunikaci mezi vozidlem a cloudovou infrastrukturou. To může způsobit selhání navigace nebo brzdových systémů. [1]

Man-in-the-Middle (MITM) útoky

MITM útoky umožňují útočníkům odposlouchávat a manipulovat datové přenosy mezi komponentami autonomního systému. Například komunikace mezi senzory a centrálním procesorem může být zachycena a změněna tak, že autonomní systém začne vykonávat neoprávněné příkazy. Obrana zahrnuje šifrování a autentizaci všech přenosů. [1]



Obrázek 6 -schéma MITM

(zdroj: vlastní)

Exploity a softwarové zranitelnosti

Komunikační protokoly používané v autonomních systémech mohou obsahovat zranitelnosti, které útočníci zneužijí k neoprávněnému přístupu. Exploity tohoto typu se často zaměřují na slabiny v softwarových knihovnách nebo nedostatečně zabezpečené přenosové protokoly, což může vést ke kompletnímu převzetí kontroly nad systémem. [1]

3.2 Selhání senzorů

Senzory jsou klíčovým prvkem autonomních systémů, protože zajišťují vnímání okolního prostředí, detekci překážek, navigaci a další kritické funkce. Jakékoliv selhání těchto senzorů může vést k zásadním problémům, včetně výpadku systému, nesprávného rozhodování nebo

dokonce ohrožení bezpečnosti lidí a majetku. Tento bod se zabývá hlavními příčinami selhání senzorů a jejich následky.

3.2.1 Příčiny selhání senzorů

Hardwarové poruchy

Selhání senzorů může být způsobeno fyzickým poškozením hardwaru, jako jsou nárazy, vibrace, extrémní teploty nebo vlhkost. Například u autonomních vozidel mohou kolize poškodit LIDAR nebo radarové systémy, což vede ke ztrátě schopnosti detekovat překážky. Tyto problémy jsou časté v náročných provozních podmínkách a vyžadují robustní konstrukci senzorů. [2]

Softwarové chyby

Chyby v algoritmech, které zpracovávají senzorová data, mohou způsobit nesprávnou interpretaci vstupů. Například špatně kalibrované senzory mohou poskytovat zkreslené hodnoty, což negativně ovlivňuje rozhodování autonomního systému. Softwarové chyby mohou být důsledkem nedostatečného testování nebo komplikací při integraci nových funkcí. [1]

Rušení a útoky

Senzory mohou být cílem vnějších útoků nebo rušení. Například jamming signálu GPS může způsobit ztrátu lokalizačních dat, což má za následek dezorientaci autonomního systému. Podobně mohou být kamerové systémy oslepeny silným světlem nebo laserem, což znehodnocuje jejich schopnost rozpoznávat objekty. [1]

3.2.2 Následky selhání senzorů

Ztráta navigace a orientace

Jedním z hlavních důsledků selhání senzorů je ztráta schopnosti autonomního systému navigovat v prostoru. Například při výpadku GPS nebo LIDAR systému nemůže vozidlo přesně určit svou polohu a směr, což může vést k nehodám nebo ztrátě kontroly. [4]

Zhoršení rozhodovacích procesů

Chybějící nebo zkreslená data ze senzorů mohou způsobit, že autonomní systém učiní nesprávná rozhodnutí. Například nesprávné rozpoznání překážky může vést k nebezpečnému manévru. Systém musí být navržen tak, aby minimalizoval riziko takových chyb prostřednictvím redundance senzorů a pokročilých algoritmů detekce chyb. [5]

Riziko bezpečnostních incidentů

Selhání senzorů může vést k ohrožení bezpečnosti okolí. Například dron se selháním gyroskopem může ztratit stabilitu a spadnout, což může způsobit materiální škody nebo zranění. Proto je klíčové implementovat mechanismy pro detekci selhání a automatické přepnutí na záložní systémy. [2]

3.3 Příklady reálných incidentů

V průběhu let bylo zaznamenáno několik významných incidentů spojených s autonomními systémy, které odhalily jejich zranitelnost vůči selhání senzorů, kybernetickým útokům a jiným bezpečnostním hrozbám. Tyto příklady poskytují cenné poznatky o tom, jaké důsledky může mít nedostatečná bezpečnost, a podtrhují potřebu efektivních ochranných mechanismů.

3.3.1 Selhání autonomních vozidel

Případ Uber – smrtelná nehoda autonomního vozidla

V roce 2018 došlo k tragické nehodě autonomního vozidla společnosti Uber v Arizoně, kdy systém nezaznamenal chodce přecházejícího silnici. Vyšetřování ukázalo, že senzory vozidla detekovaly chodce, avšak software vyhodnotil situaci jako falešný poplach. Tato nehoda zdůraznila nutnost spolehlivějších algoritmů pro rozpoznávání objektů a přísnějšího testování autonomních technologií. [19]

Tesla Autopilot – nehody způsobené nevhodným použitím systému

V několika případech uživatelé vozidel Tesla zneužili funkci Autopilot, což vedlo k nehodám. Například v roce 2021 došlo ke smrtelné kolizi, kdy řidič nechal systém řídit vozidlo bez dohledu. Systém nezareagoval na překážku, což vyústilo v srážku. Tyto incidenty ukazují na omezení současných technologií a nutnost jasnější komunikace o jejich schopnostech. [20]

3.3.2 Incidenty v průmyslové automatizaci

Selhání robotického ramene v továrně

V roce 2015 došlo k nehodě v německé automobilce, kdy robotické rameno během montážního procesu zasáhlo pracovníka, což mělo smrtelné následky. Šetření odhalilo

selhání bezpečnostních senzorů, které měly detekovat přítomnost člověka. Tento případ poukazuje na důležitost integrace redundantních bezpečnostních mechanismů. [21]

Kybernetické útoky na průmyslové systémy

Příklad útoku na autonomní průmyslové systémy představuje incident WannaCry z roku 2017, kdy ransomware zasáhl zařízení využívající Windows. Výsledkem byla odstávka některých výrobních linek, což mělo za následek vysoké finanční ztráty. Tato událost ukázala zranitelnost autonomních systémů vůči kybernetickým hrozbám. [22]

3.3.3 Incidenty s drony

Pád dronu při závodě

V roce 2020 během závodu dronů selhal navigační systém jednoho z dronů kvůli ztrátě signálu GPS. Dron narazil do bariéry, což vyvolalo diskuse o nutnosti záložních navigačních systémů pro autonomní zařízení. [4]

Incidenty na letištích způsobené drony

Například na londýnském letišti Gatwick v roce 2018 způsobil opakovaný výskyt dronů v blízkosti ranvejí masivní narušení provozu, což vedlo k rušení letů. Tento incident ukázal na potřebu lepší regulace a detekčních systémů proti neoprávněným dronům. [2]

4 OCHRANNÉ MECHANISMY V AUTONOMNÍCH SYSTÉMECH

Ochranné mechanismy v autonomních systémech jsou klíčovým prvkem pro zabezpečení provozu těchto zařízení a zajištění jejich bezpečnosti v reálném světě. Zatímco autonomní systémy jsou navrženy tak, aby fungovaly s co největší mírou samostatnosti, stále existuje riziko selhání nebo vnějších útoků. Bezpečnostní mechanismy se zaměřují na ochranu proti kybernetickým útokům, selháním senzorů, chybám v algoritmech rozhodování a jiným nebezpečím, která by mohla ovlivnit správnou funkci autonomního systému.

4.1 Detekce útoků a monitorování senzorů

Detekce útoků a monitorování senzorů jsou základními metodami pro ochranu autonomních systémů. Sensory jsou v autonomních systémech odpovědné za detekci okolního prostředí a poskytování dat pro rozhodovací algoritmy. Pokud dojde k útoku na senzory nebo k jejich selhání, může to mít vážné důsledky pro bezpečnost a provozní efektivitu systému. K tomu, aby bylo možné takové incidenty detekovat a reagovat na ně včas, je nezbytné implementovat metody detekce útoků a monitorování výkonu senzorů. To zahrnuje analýzu dat generovaných senzory a používání pokročilých metod pro detekci anomálií.

4.1.1 Analýza dat ze senzorů

Analýza dat ze senzorů je nezbytná pro identifikaci a eliminaci chybných nebo manipulovaných měření, které mohou ovlivnit rozhodovací procesy autonomních systémů. Sensory, jako jsou kamery, LiDAR, radary nebo GPS, mohou být náchylné k různým typům poruch, včetně ztráty signálu, rušení nebo útoků, které se zaměřují na zkreslení senzorických vstupů.

Pro zajištění spolehlivosti a přesnosti měření se běžně využívá redundantních senzorů. Redundance spočívá v použití více senzorů stejného typu, což umožňuje porovnávat výsledky měření a detekovat odchylky. Tento přístup je obzvláště důležitý v kritických aplikacích, jako jsou autonomní vozidla, drony nebo roboty používané v nebezpečných prostředích. Pokud jeden senzor vykazuje chybu nebo neobvyklé chování, systém může přepnout na jiný senzor a stále zajistit správnou detekci.

Redundantní senzory tak přispívají k vyšší přesnosti a spolehlivosti autonomního systému, což pomáhá minimalizovat riziko poruchy nebo manipulace s daty. Systémy s redundancí senzorů jsou zvláště efektivní v prostředích, kde je kladeno vysoké nároky

na bezpečnost, například v autonomních vozidlech, robotických systémech nebo při monitorování kritických infrastruktur. [2]

4.1.2 Strojové učení a AI

Strojové učení a AI hrají klíčovou roli při detekci anomálií v datech generovaných senzory. Pomocí algoritmů strojového učení je možné analyzovat velké množství dat z různých senzorů v reálném čase a identifikovat neobvyklé vzory, které mohou naznačovat útoky nebo selhání systému. Anomální detekce je metoda, která se používá k identifikaci odchylek v datech, které by mohly být způsobeny chybami nebo vnějšími vlivy, jako je kybernetický útok.

Metody strojového učení, jako jsou rozhodovací stromy, neuronové sítě nebo shlukovací algoritmy typu k-means, se používají k analýze rozsáhlých datových souborů ze senzorů a k identifikaci vzorců chování systému. Tyto metody umožňují detekci odchylek od běžného provozu, které mohou signalizovat útok, poruchu senzoru nebo jinou anomálii. V případě zjištění nesrovnalostí mohou systémy automaticky spustit varování nebo zahájit korektivní opatření, například přepnutí na záložní senzory či přechod do bezpečného režimu. Tento přístup je klíčový nejen pro detekci útoků, ale také pro zajištění kvality senzorických dat a eliminaci falešných poplachů, což je zásadní pro spolehlivý a bezpečný provoz autonomních systémů.

Díky kombinaci strojového učení a AI je možné autonomní systémy nejen chránit před externími útoky, ale také neustále zlepšovat jejich schopnost detekovat nové typy hrozeb na základě historických dat a zkušeností. Tato adaptivní schopnost je důležitá pro dlouhodobou bezpečnost autonomních systémů, zejména v dynamických a neznámých prostředích. [5]

4.2 Zabezpečení komunikačních kanálů

V AS hrají komunikační kanály klíčovou roli při přenosu dat mezi jednotlivými komponentami systému – například mezi senzory, řídicí jednotkou, akčními členy nebo cloudovým zázemím. Tyto kanály zahrnují jak fyzická spojení (např. kabelové sběrnice, bezdrátové sítě Wi-Fi, LTE nebo 5G), tak i softwarové protokoly (např. MQTT, ROS 2 nebo DDS), které zajišťují strukturovanou a spolehlivou výměnu dat. Jejich zabezpečení je nezbytné pro ochranu před útoky, které by mohly narušit provoz systému, odcizit citlivé

informace nebo zmanipulovat přenášená data. Mezi hlavní techniky zabezpečení patří šifrování, autentizace a implementace bezpečných komunikačních protokolů. [1]

4.2.1 Šifrování a autentizace dat

Základní ochranou proti odposlechu nebo manipulaci s daty během přenosu je šifrování. Při šifrování dochází k přeměně čitelné zprávy (tzv. otevřeného textu) na nečitelný formát (tzv. šifrovaný text) pomocí kryptografického algoritmu a klíče. Tento proces zajistí, že zachycená data nejsou srozumitelná pro neoprávněné osoby. Na straně příjemce se data pomocí správného klíče opět dešifrují zpět do původní podoby.

V prostředí autonomních systémů se často používá AES (Advanced Encryption Standard), symetrický šifrovací algoritmus, kde odesílatel i příjemce používají stejný tajný klíč. AES je považován za velmi bezpečný a zároveň dostatečně rychlý i pro aplikace v reálném čase. [5]

Autentizace doplňuje šifrování tím, že ověřuje identitu účastníků komunikace. Typickými metodami autentizace jsou digitální certifikáty, asymetrické kryptografie (např. RSA) nebo elektronické podpisy, které potvrzují, že data pochází ze spolehlivého zdroje a nebyla po cestě změněna. [23], [24], [25] Správná kombinace šifrování a autentizace významně zvyšuje důvěryhodnost a bezpečnost komunikačních kanálů a chrání autonomní systém před útoky typu man-in-the-middle nebo podvržením dat.

4.2.2 Bezpečné komunikační protokoly

Bezpečné komunikační protokoly jsou klíčové pro ochranu dat při jejich přenosu. MQTT je lehký protokol, často využívaný v prostředích s omezenými zdroji, jako jsou autonomní drony nebo IoT zařízení. Pro zvýšení bezpečnosti MQTT lze použít šifrování pomocí TLS a autentizaci pomocí uživatelských jmen a hesel nebo certifikátů. [26]

Dalším významným protokolem je ROS 2, který je široce používán v robotických aplikacích. ROS 2 obsahuje vestavěné bezpečnostní prvky, jako je šifrování komunikace a autentizace prostřednictvím DDS Security. Tento přístup umožňuje bezpečný přenos dat mezi roboty a dalšími zařízeními i v nepřátelských prostředích. [27]

Bezpečné komunikační protokoly nejenže chrání data před odposlechem a manipulací, ale také zajišťují dostupnost a integritu přenášených informací. Tím přispívají k celkové spolehlivosti autonomních systémů, zejména v kritických aplikacích, jako jsou autonomní vozidla nebo průmysloví roboti. [28], [29]

4.3 Zvyšování spolehlivosti senzorových systémů

Spolehlivost senzorových dat je zásadním předpokladem pro bezpečný provoz autonomních systémů. Sensory poskytují informace, na jejichž základě dochází k rozhodování, řízení i reakci systému na okolní podmínky. Jakékoli zkreslení, porucha nebo výpadek senzoru může vést k chybnému vyhodnocení situace a potenciálně i k havárii. [30]

Jedním z hlavních nástrojů pro zvýšení spolehlivosti je hardwarová redundance, tedy použití více senzorů stejného typu nebo různých technologií pro měření téhož jevu. Například autonomní drony mohou být vybaveny dvěma nebo třemi GPS moduly, barometry nebo IMU jednotkami. Data z těchto senzorů jsou porovnávána pomocí tzv. voting mechanismů, kde systém vyhodnotí většinou shodu hodnot jako správnou. [31], [32]

Další úroveň spolehlivosti přináší fúze senzorových dat (sensor fusion) – tedy kombinace informací z různých typů senzorů, jako jsou LIDAR, kamera, radar nebo ultrazvuk. Tato kombinace umožňuje vytvořit konzistentní a přesný obraz o prostředí, i když některý senzor selže nebo poskytuje nepřesné údaje. Fúze dat také zvyšuje odolnost systému vůči vnějším vlivům, jako je mlha, tma nebo rušení. [33], [34]

Kromě hardwarových opatření se využívají i softwarové techniky, které zajišťují detekci anomálií v datech a předcházejí poruchám. Pomocí algoritmů strojového učení lze modelovat běžné chování senzorů a odhalit odchylky, které signalizují potenciální selhání. Například prediktivní modely na základě historických dat mohou upozornit na zhoršující se výkon senzoru ještě před jeho úplným výpadkem. [35]

Zvýšení spolehlivosti senzorových systémů je tedy komplexní úkol, který zahrnuje jak fyzické zálohování hardwaru, tak inteligentní softwarovou analýzu. V kombinaci tyto přístupy významně zvyšují odolnost autonomního systému vůči poruchám a útokům a přispívají k jeho celkové bezpečnosti.

4.3.1 Hardwarová redundance

Hardwarová redundance spočívá v instalaci více senzorů stejného typu na jeden systém, což umožňuje ověřování správnosti dat pomocí jejich vzájemného porovnání. Například autonomní drony mohou mít dva až tři barometry nebo GPS moduly, aby eliminovaly chyby způsobené poruchou jednoho z těchto senzorů. Takový přístup je často využíván v letectví a automobilovém průmyslu, kde je spolehlivost klíčová. [31]

Vícenásobné senzory mohou být konfigurovány v různých modech, například v tzv. *voting* režimu, kdy systém vyhodnocuje většinový výsledek sensorových dat, aby rozhodl o správné hodnotě. Tento přístup minimalizuje riziko chybných dat, a tím zajišťuje stabilitu systému i v případě selhání jednoho nebo více senzorů. [5], [32]

4.3.2 Softwarové metody zajištění spolehlivosti

Kromě hardwarové redundance hrají v autonomních systémech důležitou roli také softwarové přístupy, které zvyšují spolehlivost sensorických dat a schopnost systému odhalit chyby včas. Tyto metody zahrnují zejména prediktivní diagnostiku, detekci anomálií, statistickou analýzu dat a algoritmickou fúzi sensorových vstupů.

Pomocí algoritmů strojového učení lze vytvářet modely běžného chování senzorů. Pokud systém zaznamená odchylky od očekávaných hodnot, může upozornit na potenciální poruchu nebo spustit korektivní reakci. Například prediktivní modely trénované na historických datech mohou předpovědět blížící se selhání senzoru a zajistit přepnutí na záložní vstupy ještě před výpadkem. [33]

Další důležitou technikou je fúze dat na softwarové úrovni, kdy systém kombinuje informace z různých senzorů a analyzuje jejich konzistenci. Pokud se například údaje z kamery a LIDARu významně liší, systém může vyhodnotit, který vstup je pravděpodobně chybný, a ignorovat ho. Tím se minimalizuje riziko rozhodování na základě chybných nebo zmanipulovaných dat. [34], [35]

Softwarové metody zajištění spolehlivosti tak umožňují včasnou detekci nestandardního chování, adaptaci systému v reálném čase a zvýšení celkové robustnosti rozhodovacích procesů. Jsou proto klíčovou součástí obranné strategie autonomních systémů, zejména v prostředích s vysokými nároky na bezpečnost a provozní kontinuitu.

5 LEGISLATIVNÍ A ETICKÉ ASPEKTY ZABEZPEČENÍ AUTONOMNÍCH SYSTÉMŮ

Zabezpečení autonomních systémů není pouze technickým problémem, ale také záležitostí legislativy, regulací a etických zásad. Globální standardizace a regulace jsou nezbytné pro zajištění bezpečnosti, kompatibility a důvěry veřejnosti. Tento bod se zaměřuje na klíčové mezinárodní standardy a regulace, které ovlivňují kybernetickou bezpečnost a ochranu autonomních systémů.

5.1 Mezinárodní standardy a regulace

Bezpečný vývoj a provoz autonomních systémů vyžaduje nejen technická opatření, ale také existenci mezinárodních standardů a právního rámce, které nastavují pravidla pro zabezpečení, interoperabilitu a ochranu uživatelů. Standardy a regulace poskytují jednotné principy, které vývojářům i provozovatelům umožňují navrhovat systémy s odpovídající úrovní bezpečnosti, důvěryhodnosti a odpovědnosti.

Jedním z nejvýznamnějších standardů v oblasti kybernetické bezpečnosti je ISO/IEC 27001, který definuje požadavky na systém řízení bezpečnosti informací (ISMS). Tento standard je aplikovatelný i na autonomní systémy, které zpracovávají velké množství dat ze senzorů, komunikace a uživatelských vstupů. Implementace ISO/IEC 27001 umožňuje systematicky identifikovat a řídit rizika spojená s kybernetickými hrozbami a zabezpečit integritu a důvěrnost dat. [36], [37]

V oblasti autonomních vozidel a dronů existují specializované předpisy, které upravují jejich provoz a technické požadavky. V USA je klíčovým orgánem Federal Aviation Administration (FAA), která stanovuje pravidla například prostřednictvím Part 107, určující podmínky pro provoz malých bezpilotních letounů. V Evropské unii tuto oblast reguluje European Union Aviation Safety Agency (EASA), která vytvořila rámec pro provoz dronů založený na hodnocení rizik, certifikaci a technických požadavcích. [38], [39]

Důležitou součástí regulačního rámce je také ochrana osobních údajů. V evropském prostoru hraje klíčovou roli Obecné nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation), které vstoupilo v platnost v roce 2018. Jde o právní rámec Evropské unie, jehož cílem je chránit práva jednotlivců na soukromí a kontrolu nad tím, jak jsou jejich osobní údaje sbírány, zpracovávány a uchovávány.

Autonomní systémy – například vozidla, drony nebo zdravotnické roboty – často pracují s daty, která lze považovat za osobní. Může jít o lokalizační informace, vizuální záznamy, biometrické údaje nebo chování uživatele. GDPR má tedy přímý vliv na to, jak tyto systémy musí být navrženy a provozovány, aby neporušovaly práva subjektů údajů.

Konkrétní dopady zahrnují například povinnost minimalizace dat, tedy že autonomní systém smí shromažďovat pouze ta data, která jsou nezbytně nutná pro provoz. Dále je vyžadována transparentnost, tedy jasné informování uživatele o tom, jaká data jsou sbírána a za jakým účelem. Provozovatelé systémů musí také počítat s možností odvolání souhlasu nebo žádosti o výmaz dat, a zajistit odpovídající technická a organizační opatření – jako je šifrování, řízení přístupových práv nebo pseudonymizace. [40]

Z praktického hlediska je proto nutné, aby autonomní systémy byly vyvíjeny v souladu s principem privacy by design, tedy aby ochrana soukromí byla integrována přímo do návrhu systému. Nedodržení pravidel GDPR může mít pro provozovatele závažné důsledky v podobě vysokých pokut a poškození důvěryhodnosti.

Standardy a regulace tedy neplní pouze formální roli, ale mají zásadní dopad na návrh, testování i provoz autonomních systémů. Umožňují zajištění bezpečnosti, ochranu uživatelů a zároveň posilují důvěru veřejnosti v nasazení těchto technologií v reálném prostředí.

5.2 Etická dilemata a zneužitelnost autonomních systémů

Autonomní systémy přinášejí nejen technologický pokrok, ale také řadu etických otázek souvisejících s jejich možným zneužitím. Například drony mohou být použity k monitorování osob bez jejich vědomí, což představuje narušení soukromí a vyvolává obavy o ztrátu kontroly nad osobními daty. [6] Veřejnost často vnímá tyto technologie s nedůvěrou, přičemž výzkum ukazuje, že se postoj k autonomním robotickým systémům v Evropě postupně zhoršuje. [2]

Existují doložené případy zneužití dronů pro pašování drog a zboží přes hranice, například v USA a Mexiku, kde byly autonomní bezpilotní prostředky zachyceny při přepravě nelegálních látek do věznic nebo přes státní hranice [52]. Zprávy byly zaznamenány také v Evropě – například ve Spojeném království, kde byly drony využívány k nelegálnímu monitorování stavebních pozemků nebo ke sledování konkurence [53]. V konfliktních oblastech, jako je Ukrajina nebo Blízký východ, bylo zaznamenáno nasazení autonomních nebo poloautonomních systémů pro účely cílených útoků. Tyto případy

vyvolávají závažné otázky týkající se odpovědnosti za rozhodnutí o útoku, etiky nasazení a souladu s mezinárodním humanitárním právem, zejména pokud stroje rozhodují bez lidského zásahu. [41] Autonomní zbraňové systémy (LAWS – Lethal Autonomous Weapon Systems) jsou předmětem intenzivních debat. Hlavní obavou je, že rozhodování o životě a smrti může být přeneseno na algoritmy bez možnosti lidské korekce. Takový vývoj by mohl být v rozporu s principy mezinárodního práva a lidské důstojnosti. [42], [43] Zároveň ale autonomní systémy nacházejí i eticky přípustné a přínosné využití. Například doručovací drony přispívají ke zlepšení dostupnosti zdravotní péče v odlehlých oblastech a průzkumné drony se uplatňují při monitorování infrastruktury nebo záchranných operacích. [5], [9] Tyto aplikace mají významný humanitární i ekonomický potenciál. Navzdory těmto pozitivním příkladům však etická úskalí přetrvávají. Je nutné nastavit mezinárodně platná pravidla, která zamezí zneužití těchto technologií, zajistí transparentnost rozhodovacích procesů a definují jasnou odpovědnost za jejich chování a následky.

5.3 Technické aspekty sledování a vyhodnocení selhání autonomních systémů

Jedním z největších právních a etických problémů při používání autonomních systémů je otázka odpovědnosti za škody způsobené jejich selháním. Pokud autonomní systém způsobí dopravní nehodu, poškodí majetek nebo zraní člověka, není jednoznačné, kdo nese odpovědnost – zda výrobce zařízení, vývojář softwaru, provozovatel, nebo samotný uživatel. V tradičních systémech je odpovědnost obvykle jasně definována, avšak v případě autonomních technologií je situace komplikovanější kvůli jejich samostatnému rozhodování.

Evropská unie přijala v roce 2024 Nařízení o umělé inteligenci (AI Act), jehož cílem je vytvořit jednotný právní rámec pro vývoj, nasazení a používání systémů umělé inteligence na území EU. Toto nařízení klasifikuje AI systémy podle míry rizika – od nepřijatelných až po minimální – a zavádí specifické povinnosti pro poskytovatele a uživatele vysoce rizikových systémů, mezi které mohou spadat i autonomní prostředky.

Ačkoliv AI Act výslovně neupravuje odpovědnost za škodu způsobenou autonomním systémem, stanovuje technické a organizační požadavky, jejichž nedodržení může vést k právním důsledkům. Právní odpovědnost tedy zůstává zakotvena v obecných principech práva, ale porušení požadavků stanovených AI Actem může být bráno jako indikátor nedbalosti při posuzování odpovědnosti. [44]

Jedním z technických problémů při používání autonomních systémů je tzv. „black box efekt“, který označuje situaci, kdy není možné jednoduše vysvětlit, proč systém přijal určité rozhodnutí. Tento jev se vyskytuje zejména u komplexních modelů strojového učení, jako jsou hluboké neuronové sítě, které zpracovávají data prostřednictvím milionů parametrů a jejich rozhodování není lidsky čitelné. Nedostatečná transparentnost takových modelů představuje problém při zpětné analýze chyb a při určování odpovědnosti v případě selhání.

Aby se minimalizovala rizika a zvýšila důvěryhodnost autonomních systémů, je nezbytné při jejich vývoji a nasazení využívat systematické testovací strategie. Tyto přístupy ověřují, zda systém vykonává své funkce spolehlivě i ve složitých nebo neočekávaných situacích. Black-box testování se zaměřuje na ověření výstupů systému na základě různých vstupů, aniž by měl tester přístup k interní logice nebo zdrojovému kódu. Je vhodné zejména pro testování chování systému jako celku z pohledu koncového uživatele.

Naopak white-box testování analyzuje vnitřní strukturu systému, včetně logických větví, cyklů, rozhodovacích podmínek nebo hodnot proměnných. Umožňuje testovat pokrytí kódu a identifikovat slabiny v samotné implementaci. Tento přístup je často využíván při vývoji bezpečnostních funkcí, kde je důležité znát přesný způsob fungování algoritmů.

Grey-box testování kombinuje oba výše uvedené přístupy – tester má částečný přístup k architektuře systému (například znalost komunikačních protokolů nebo datových struktur), ale stále testuje externím způsobem. Tento typ testování je vhodný pro systémy, kde je známé API nebo specifikace, ale nikoli celý vnitřní kód.

Kromě těchto klasických metod se v oblasti autonomních systémů začíná uplatňovat také tzv. fuzz testing (fuzzování). Jedná se o metodu, při které je systém vystavován velkému množství náhodně generovaných vstupních dat, často včetně nevalidních nebo extrémních hodnot, s cílem vyvolat nečekané chování nebo chyby. Fuzz testing se osvědčil například při testování řídicích protokolů dronů, kde simulované datové poruchy odhalily nedostatečné ošetření výjimek nebo selhání komunikace.

Tyto metody jsou součástí doporučených rámců, jak je například ISTQB (International Software Testing Qualifications Board), který poskytuje standardizované přístupy k testování systémů různých kritičností. V kontextu autonomních platforem je důležité testovat jak v laboratorních simulacích, tak v reálných podmínkách, aby se ověřila odolnost vůči proměnlivému prostředí a interakcím s okolím.[45], [47]

Typickým příkladem nejasné odpovědnosti je případ smrtelné nehody autonomního vozidla Uber v Arizoně v roce 2018. Vozidlo detekovalo chodce, avšak software jeho přítomnost nesprávně vyhodnotil jako falešný poplach. Systém včas nezareagoval a došlo k fatálnímu střetu. Vyšetřování odhalilo selhání jak senzorických algoritmů, tak nedostatečného lidského dohledu ze strany operátora. Následná diskuse ukázala, že nebylo jasné, kdo má nést právní odpovědnost – zda vývojáři softwaru, Uber jako provozovatel, nebo lidský operátor. Tento případ zdůraznil potřebu právního rámce a technické transparentnosti, který umožní v budoucnu podobné situace jednoznačně řešit. [46]

Pro zajištění vyšší transparentnosti autonomních systémů se využívají principy tzv. „vysvětlitelné umělé inteligence“ (explainable AI, XAI). Tyto přístupy umožňují zpětně analyzovat, jaké faktory vedly systém ke konkrétnímu rozhodnutí, a tím zvyšují důvěryhodnost a bezpečnost provozu. XAI je obzvláště důležitá v prostředí, kde systémy pracují s neurčitostí a komplexními daty, a její využití je klíčové při auditech a zpětném vyhodnocení selhání systémů. [47]

II PRAKTICKÁ ČÁST

6 ANALÝZA ZRANITELNOSTI AUTONOMNÍHO SYSTÉMU A EXPERIMENTÁLNÍ OVĚŘENÍ

Autonomní systémy se při svém provozu spoléhají na správnou funkci senzorických prvků, stabilitu komunikačních kanálů a spolehlivost rozhodovacích algoritmů. Jakékoli selhání v těchto oblastech může výrazně ohrozit jejich činnost a v důsledku i bezpečnost okolí. Kritickým bodem je zejména řízení v reálném čase prostřednictvím bezdrátového přenosu, jehož výpadek může způsobit ztrátu kontroly nad zařízením. Cílem této kapitoly je analyzovat zranitelnosti konkrétního autonomního systému, bezpilotního prostředku VISU L900 PRO SE, a následně ověřit experimentálně jeho reakci na cílené rušení řídicí komunikace.

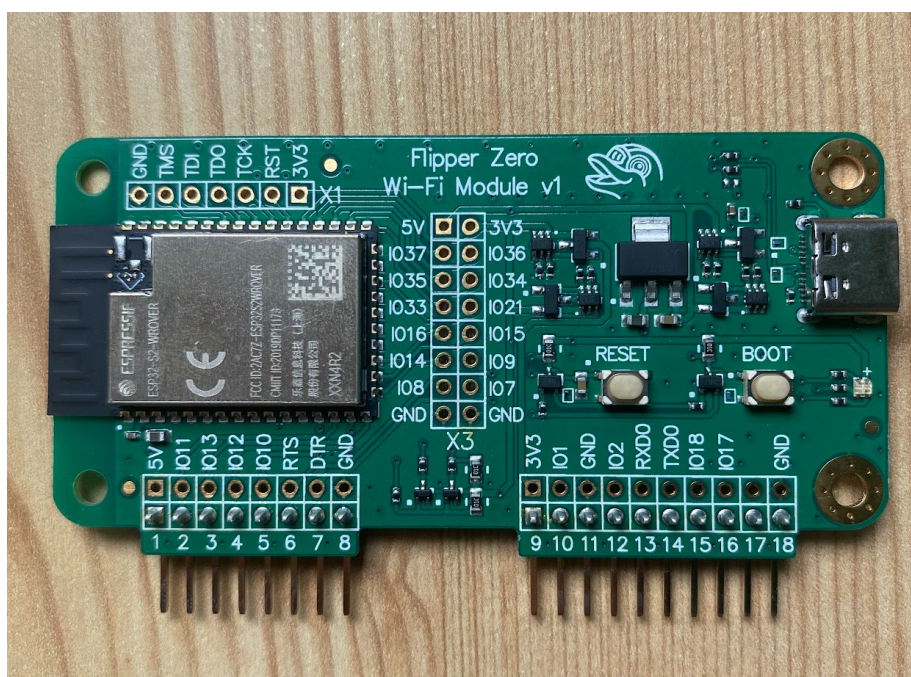
Zvolený dron představuje typické komerčně dostupné UAV zařízení nižší třídy. Je vybaven základními funkcemi pro autonomní stabilizaci letu, mezi které patří inerciální měřicí jednotka (IMU– Inertial Measurement Unit), satelitní navigace (GNSS – Global Navigation Satellite System) a funkce automatického návratu do výchozího bodu (RTH – Return to Home). Řízení probíhá prostřednictvím fyzického ovladače, který komunikuje s dronem v pásmu 2405–2475 MHz, přičemž podle oficiální zkušební zprávy je aktivním vysílačem právě ovladač. Pro přenos obrazu a telemetrie mezi dronem a mobilní aplikací je využíváno samostatné připojení v pásmu 5 GHz, což však nebylo předmětem tohoto testu. [54]

Z hlediska bezpečnosti je právě řídicí spojení mezi ovladačem a dronem v pásmu 2.4 GHz identifikováno jako nejzranitelnější. Tento komunikační kanál je bezlicenční, hojně využívaný a náchylný k interferenci. Vzhledem k tomu, že systém neobsahuje žádné mechanismy pro detekci rušení nebo pro adaptivní přesměrování komunikace, může jeho přerušení způsobit neočekávanou reakci systému. Pokud navíc nedojde k aktivaci bezpečnostní funkce, může být systém zcela neovladatelný.

Pro experimentální ověření této zranitelnosti byl použit nástroj Flipper Zero s alternativním firmwarem Unleashed, který obsahuje pokročilou aplikaci WiFi Marauder pro aktivní skenování a simulaci narušení bezdrátové sítě. Za účelem rušení byl Flipper rozšířen o modul ESP32-S2 WROVER, který umožňuje samostatné vysílání v pásmu 2412–2462 MHz a poskytuje stabilitu rušivého signálu. Podle certifikace FCC RSHD200218007-00A je tento modul schopen provozu ve všech běžných Wi-Fi kanálech a odpovídá normě FCC Part 15.247. [55]



Obrázek 8 - Flipper zero s aplikací wifi marauder

(zdroj: vlastní)

Obrázek 7 – modul ESP32-S2 WROVER

(zdroj: vlastní)

Test probíhal v otevřeném prostoru za přirozených podmínek. Rušení bylo směřováno výhradně na spojení mezi ovladačem a dronem, přičemž signál z Flipperu a ESP32 nepřesahoval rozsah povolený pro pokusy ve volném pásmu. Bylo sledováno, jakým

způsobem dron reaguje na výpadek spojení. Zda aktivuje RTH, zůstane na místě, nebo zcela ztratí stabilitu. Výsledky tohoto testování budou podrobně analyzovány v následujících částech práce.

6.1 Metodika praktické části

Tento experiment vychází z předpokladu, že narušení řídicího signálu, ať už úmyslné nebo náhodné, může vést k selhání systému, ztrátě kontroly nad zařízením nebo k ohrožení bezpečnosti okolí. Testovaný scénář představuje běžně se vyskytující slabinu v komunikační architektuře autonomních systémů, zejména těch, které využívají bezlicenční pásmo 2.4 GHz bez dodatečných zabezpečovacích mechanismů. [2] Praktická část práce se zaměřuje na testování této slabiny pomocí zvoleného autonomního prostředku, dronu VISU L900 PRO SE, který byl vyhodnocen jako vhodný model pro simulaci ztráty spojení v řízeném prostředí.

Metodika spočívá v postupném provedení několika scénářů narušení, při kterých bude sledováno chování systému během a po ztrátě komunikace. Konkrétně bude zaznamenáváno, zda systém aktivuje některý z bezpečnostních režimů, zda zůstane stabilní, a zda je možné spojení obnovit po ukončení rušení. Data budou získávána analýzou videozáznamu a cíleným pozorováním chování dronu v průběhu experimentu, přičemž sledovány budou zejména jevy jako kolísání výšky, opožděné reakce na řídicí povely a případný přechod do bezpečnostních režimů. Audiovizuální záznam bude pořizován pomocí statické kamery s fixním zorným polem, která bude umístěna v úrovni letové dráhy dronu, což umožní opakované vyhodnocení jednotlivých situací a přesné vizuální zachycení reakce systému na vnější rušení.

Výsledky testů budou sloužit jako základ pro vyhodnocení provozní odolnosti systému a následně pro návrh možných technických opatření, která by v reálných aplikacích mohla zlepšit bezpečnost autonomních platforem vystavených obdobným hrozbám.

6.2 Model autonomního systému

Pro účely experimentální části byl zvolen komerčně dostupný dron VISU L900 PRO SE, který představuje typického zástupce autonomních systémů nižší třídy určených pro běžné civilní využití. Přestože se nejedná o profesionální zařízení, jeho architektura je dostatečně komplexní k tomu, aby bylo možné analyzovat reakce na narušení komunikace a otestovat základní bezpečnostní mechanismy při selhání spojení.

Dron je vybaven základní sadou senzorických a autonomních prvků:

- inerciální měřicí jednotka (IMU) slouží ke stabilizaci během letu a poskytuje informace o náklonu a zrychlení;
- GNSS modul (kombinace GPS a GLONASS) zajišťuje navigaci, plánování trasy a přesné udržení pozice;
- barometrický senzor a šestiosý gyroskop přispívá k udržení výšky v režimu „hover“;
- funkce automatického návratu (RTH) se aktivuje v případě ztráty spojení nebo při dosažení kritické úrovně baterie;



Obrázek 9 – Dron VISU L900 PRO SE

(zdroj: vlastní)

Řízení dronu probíhá prostřednictvím fyzického ovladače, který komunikuje v pásmu 2.4 GHz (2405–2475 MHz) pomocí modulace GFSK. Podle certifikační zprávy je aktivním vysílačem právě ovladač, zatímco dron signál pouze přijímá. Tato architektura je typická pro spotřebitelské UAV systémy a zároveň představuje potenciální slabinu, neboť signál je možné narušit nebo zcela přerušit externím vlivem. [54]



Obrázek 10 - Ovladač dronu

(zdroj: vlastní)

Pro přenos videa z kamery a telemetrických dat do mobilní aplikace je využívána samostatná Wi-Fi síť v pásmu 5 GHz, která je však z hlediska řízení letu nezávislá na komunikační lince mezi ovladačem a dronem. Výpadek videa tak neznamena automaticky ztrátu řízení, zatímco přerušení signálu v pásmu 2.4 GHz může způsobit aktivaci nouzového režimu.

Z pohledu bezpečnosti je testovaný model zranitelný zejména v oblasti řídicí komunikace, neboť nepodporuje pokročilé formy šifrování ani adaptivní přepínání kanálů. Jakýkoli výpadek nebo rušení spojení může vést k nežádoucímu chování, a systém se tak musí spoléhat pouze na jednoduché nouzové funkce, které nemusí být vždy dostačující v reálných podmínkách. Důvodem, výběru právě tohoto modelu je tedy jeho srovnatelná struktura se skutečnými provozními systémy, dostupnost pro praktické testy a schopnost ukázat základní reakce systému na výpadek nebo narušení komunikačního spojení. V následujících částech bude tento model podroben řízenému testování, jehož cílem je odhalit limity současného řešení a navrhnout možnosti zlepšení.

6.3 SWOT analýza architektury systému

Pro systematické vyhodnocení silných a slabých stránek testovaného autonomního systému byla zvolena analytická metoda SWOT (Strengths, Weaknesses, Opportunities, Threats).

Tato metoda umožňuje identifikovat vnitřní i vnější faktory, které ovlivňují bezpečnost a spolehlivost provozu autonomního zařízení.

Tabulka 1 - SWOT analýza

Silné stránky (Strengths)	Slabé stránky (Weaknesses)
Přítomnost režimu RTH pro zajištění bezpečnosti při výpadku signálu	Absence šifrování a autentizace komunikace (zranitelnost vůči spoofingu a jammingu)
Stabilizace letu pomocí IMU a GNSS	Žádná redundantní sensorika ani alternativní navigační systém (např. vizuální odometrie)
Možnost připojení k mobilní aplikaci pro zobrazení polohy a videa	Zpožděná aktivace režimu RTH, která může způsobit dočasnou ztrátu stability
Automatický návrat při ztrátě spojení	Není k dispozici záznam událostí (logování), což znemožňuje zpětnou analýzu selhání
	Komunikace probíhá v neregulovaném pásmu 2.4 GHz bez odolnosti vůči rušení
Příležitosti (Opportunities)	Hrozby (Threats)
Možnost doplnění o bezpečnostní software/firmware (např. šifrování, autorizace příkazů)	Zneužití signálu pro převzetí kontroly nebo záměrné narušení (např. Flipper Zero, WiFi rušiče)
Implementace redundantních senzorů nebo přechod na RTK GNSS	Ztráta signálu ve frekvenčně rušeném prostředí (města, závody, vojenské oblasti)
Využití externích logovacích modulů a telemetrie pro záznam činnosti	Právní a etické důsledky při selhání zařízení (např. poškození majetku, ohrožení osob)
Integrace s bezpečnostními standardy UAV v rámci evropské legislativy (EASA, ISO 21384)	Rychle se vyvíjející prostředí kybernetických hrozeb, na které není hobby zařízení navrženo

(zdroj: vlastní)

6.4 Identifikace klíčových slabin systému

Na základě analýzy architektury testovaného systému a předešlých poznatků lze identifikovat několik zásadních zranitelných míst, která mohou mít vliv na provozní bezpečnost dronu VISU L900 PRO SE. Nejvýznamnější z nich se nacházejí v oblasti bezdrátové komunikace a absence pokročilých mechanismů pro detekci a zvládání anomálií.

Nejkritičtější zranitelností je závislost systému na jediném komunikačním kanálu v pásmu 2.4 GHz, který zajišťuje přenos řídicích dat mezi fyzickým ovladačem a dronem.

V tomto směru není systém vybaven žádnou formou ochrany proti rušení, detekci jammingu ani šifrováním přenosu. Podle zdrojů je vysílačem samotný ovladač, zatímco dron signál pouze přijímá. To znamená, že narušení signálu z ovladače, například cíleným rušením, vede k okamžité ztrátě kontroly, aniž by systém disponoval možností přepnutí na alternativní komunikační kanál nebo samostatné rozhodovací logiky. [54]

Další slabinou je omezená autonomní schopnost systému po ztrátě spojení. Dron sice obsahuje funkci RTH, která se má aktivovat v případě výpadku komunikace, nicméně její aktivace je časově zpožděná a závisí na tom, zda je k dispozici aktuální pozice ze satelitního systému GNSS. V případě souběhu rušení a výpadku GNSS signálu může dron setrvat ve vzduchu bez reakce, nebo vykonat chybný manévr.

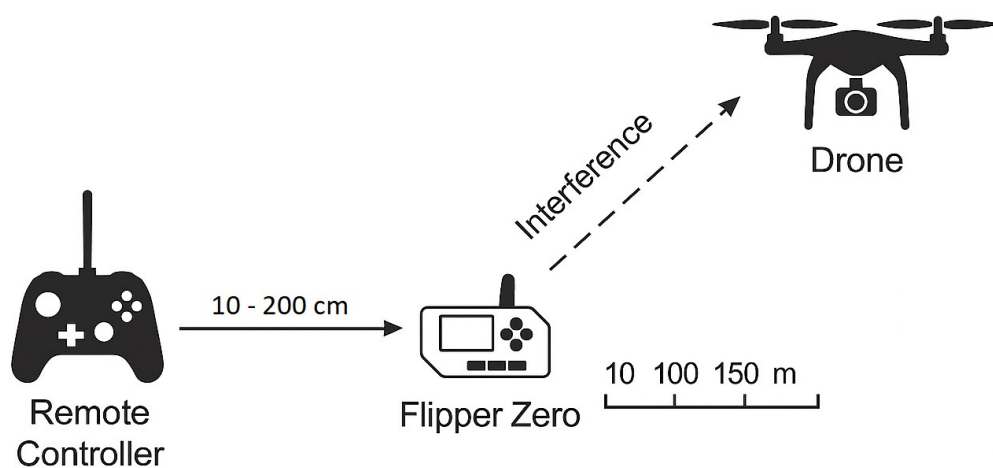
Z hlediska senzoriky je třeba zmínit také chybějící senzorovou redundanci. Systém se spoléhá pouze na základní kombinaci GNSS, IMU a barometru, bez vzájemného ověřování nebo pokročilé fúze dat. V případě selhání některého senzoru není systém schopen spolehlivě detekovat nekonzistenci nebo provést korekční reakci. Například výpadek barometrického senzoru by mohl ovlivnit schopnost dronu udržet výšku, bez jakéhokoli upozornění nebo záložního řešení. Z hlediska kybernetické bezpečnosti je systém zcela otevřený – nepoužívá šifrování, autentizaci ani ochranu proti falešným příkazům. To znamená, že potenciální útočník může nejen rušit spojení, ale teoreticky také napodobit signál ovladače a převzít řízení, což však v této práci není předmětem testování.

Z výše uvedeného je zřejmé, že nejkritičtějším bodem testovaného systému je vysoká závislost na kvalitě bezdrátového spojení a absence aktivních mechanismů pro detekci a zvládání bezpečnostních incidentů. Proto se praktická část této práce zaměřuje právě na testování reakce systému při výpadku řídicí komunikace, neboť tento scénář představuje reálnou a závažnou hrozbu v běžném provozu.

6.5 Test reakce na rušení řídicí komunikace

Cílem této části práce je prakticky ověřit, jak autonomní systém v podobě dronu VISU L900 PRO SE reaguje na ztrátu řídicí komunikace v důsledku cíleného rušení. Experiment je zaměřen výhradně na spojení mezi fyzickým ovladačem a dronem, které probíhá v pásmu 2.4 GHz. Rušení je realizováno pomocí zařízení Flipper Zero s firmwarem Unleashed a aplikací WiFi Marauder, doplněné o ESP32-S2 WROVER, který umožňuje aktivní vysílání rušivého signálu.

Testování probíhalo na otevřeném nezastavěném prostranství. Dron byl během každého pokusu umístěn do tří různých vzdáleností od výchozího bodu – konkrétně 50 m, 100 m a 150 m. Rušička (Flipper Zero) byla umístěna ve vzdálenostech 10, 50, 100, 150 a 200 cm od fyzického ovladače. Pro každý pokus byla navíc variována doba aktivního rušení: 10, 20, 30, 40 a 50 sekund. Tím bylo možné otestovat nejen prostorové, ale i časové limity reakce systému na přerušení řídicího signálu.



Obrázek 11 - Schéma experimentálního testování reakce dronu na rušení řídicí komunikace

(zdroj: vlastní)



Obrázek 13 - Startovací pozice dronu

(zdroj: vlastní)



Obrázek 12 - Vzdálenost Flipperu od ovladače

(zdroj: vlastní)

V každém jednotlivém testu bylo zaznamenáno:

- zda dron ztratil spojení s ovladačem a spustil režim návratu (RTH),
- délka aplikovaného rušení v sekundách,

- čas od zahájení rušení do momentu, kdy dron zahájil návrat,
- případné nežádoucí reakce systému nebo ztráta stability.

Každý scénář byl realizován třikrát za stejných podmínek s cílem eliminovat náhodné výkyvy a ověřit opakovatelnost výsledků. Rušení bylo vždy aktivováno na pevně stanovenou dobu (10 až 50 sekund) a byl sledován čas do zahájení návratu, přesnost přistání a případná ztráta stability. Chování systému bylo dokumentováno audiovizuálním záznamem a doplněno ručními zápisy pro každé jednotlivé měření. Výsledky jednotlivých pokusů byly porovnány a následně zprůměrovány.

V rámci validace byly vyloučeny pokusy, u kterých došlo k neočekávanému zásahu vnějších faktorů (např. silný vítr, výpadek GNSS signálu mimo vlastní rušení). Experiment tak probíhal v kontrolovaném prostředí s cílem zajistit reprodukovatelnost a věrohodnost zjištěných výsledků. Výsledky testů jsou uvedeny v následujících tabulkách, které jsou rozděleny podle vzdálenosti Flipper Zero od ovladače a doby rušení. V každé tabulce jsou uvedeny všechny kombinace vzdálenosti dronu, délky rušení, reakce systému a doby odezvy.

Vyhodnocení času do zahájení návratu (RTH) probíhalo pomocí audiovizuálního záznamu z pozemní kamery. Čas byl měřen od okamžiku aktivace rušení (stisknutí tlačítka „start“ ve WiFi Marauder) do prvního viditelného projevu reakce dronu – obvykle šlo o rotaci ve směru návratu. Časový údaj byl odečítán ze záznamu s přesností na desetiny sekundy. U každého testu byl čas měřen dvěma osobami a v případě odchylky vyšší než 0,5 s byl test opakován.

Přesnost návratu byla stanovena jako přímá vzdálenost mezi reálným místem přistání a původním vzletovým bodem (zachyceným předem pomocí GNSS a vizuálního referenčního bodu na zemi). Vzdálenost byla měřena svinovacím metrem s přesností $\pm 0,05$ m. Při více testech ve stejném scénáři byla uvedena průměrná hodnota. Odchylky jednotlivých přistání se pohybovaly obvykle do 0,5 metru, což odpovídá očekávané přesnosti GPS systému v běžném prostředí.

Tabulka 2 - Flipper Zero ve vzdálenosti 10 cm

Doba rušení (s)	Vzdálenost dronu (m)	Dokončil návrat (ANO/NE)	Čas do zahájení návratu (s)	Přesnost návratu (m)	Ztráta stability (ANO/NE)
10	50	ANO	3,1	0,3	NE
10	100	ANO	3,1	0,3	NE
10	150	ANO	3,0	0,1	ANO
20	50	ANO	2,8	0,1	NE
20	100	ANO	1,9	0,2	NE
20	150	ANO	2,8	0,7	NE
30	50	ANO	2,5	0,6	ANO
30	100	ANO	2,1	0,1	NE
30	150	ANO	2,9	0,3	ANO
40	50	ANO	3,0	0,6	NE
40	100	ANO	2,3	0,4	NE
40	150	ANO	3,3	0,4	NE
50	50	ANO	2,6	0,2	NE
50	100	ANO	3,3	0,5	NE
50	150	ANO	3,2	0,5	ANO

(zdroj: vlastní)

Tabulka 3 - Flipper Zero ve vzdálenosti 50 cm

Doba rušení (s)	Vzdálenost dronu (m)	Dokončil návrat (ANO/NE)	Čas do zahájení návratu (s)	Přesnost návratu (m)	Ztráta stability (ANO/NE)
10	50	ANO	2,2	0,2	NE
10	100	ANO	2,6	0,1	ANO
10	150	ANO	2,7	0,4	NE
20	50	ANO	2,7	0,1	NE
20	100	ANO	2,1	0,6	NE
20	150	ANO	3,1	0,8	NE
30	50	ANO	2,5	0,4	NE
30	100	ANO	3,3	0,6	NE
30	150	ANO	2,3	0,5	NE
40	50	ANO	2,4	0,5	NE
40	100	ANO	3,1	0,1	NE
40	150	ANO	2,5	0,7	ANO
50	50	ANO	2,1	0,2	NE
50	100	ANO	2,5	0,5	NE
50	150	ANO	3,1	0,3	NE

(zdroj: vlastní)

Tabulka 4 -Flipper Zero ve vzdálenosti 100 cm

Doba rušení (s)	Vzdálenost dronu (m)	Dokončil návrat (ANO/NE)	Čas do zahájení návratu (s)	Přesnost návratu (m)	Ztráta stability (ANO/NE)
10	50	ANO	2,5	0,1	NE
10	100	ANO	2,2	0,2	NE
10	150	ANO	3,1	0,1	ANO
20	50	ANO	2,2	0,5	NE
20	100	ANO	2,5	0,1	ANO
20	150	ANO	3,4	0,4	NE
30	50	ANO	2,3	0,7	NE
30	100	ANO	2,5	0,8	NE
30	150	ANO	3,2	0,7	ANO
40	50	ANO	2,4	0,7	NE
40	100	ANO	2,6	0,1	NE
40	150	ANO	2,1	0,1	NE
50	50	ANO	3,0	0,6	NE
50	100	ANO	2,4	0,7	NE
50	150	ANO	3,3	0,2	NE

(zdroj: vlastní)

Tabulka 5 - Flipper Zero ve vzdálenosti 150 cm

Doba rušení (s)	Vzdálenost dronu (m)	Dokončil návrat (ANO/NE)	Čas do zahájení návratu (s)	Přesnost návratu (m)	Ztráta stability (ANO/NE)
10	50	ANO	2,9	0,6	NE
10	100	ANO	3,0	0,0	NE
10	150	ANO	3,2	0,1	NE
20	50	ANO	2,3	0,0	ANO
20	100	ANO	2,78	0,7	NE
20	150	ANO	2,3	0,2	NE
30	50	ANO	3,2	0,4	NE
30	100	ANO	2,9	0,6	NE
30	150	ANO	2,1	0,9	ANO
40	50	ANO	1,9	0,4	NE
40	100	ANO	2,3	0,6	NE
40	150	ANO	3,2	0,6	NE
50	50	ANO	2,8	0,6	NE
50	100	ANO	2,4	0,3	NE
50	150	ANO	3,0	0,4	ANO

(zdroj: vlastní)

Tabulka 6 - Flipper Zero ve vzdálenosti 200 cm

Doba rušení (s)	Vzdálenost dronu (m)	Dokončil návrat (ANO/NE)	Čas do zahájení návratu (s)	Přesnost návratu (m)	Ztráta stability (ANO/NE)
10	50	ANO	3,2	0,9	NE
10	100	ANO	2,3	0,8	NE
10	150	ANO	2,9	0,1	NE
20	50	ANO	2,2	0,9	ANO
20	100	ANO	2,5	0,3	NE
20	150	ANO	3,4	0,0	NE
30	50	ANO	3,3	0,9	NE
30	100	ANO	3,4	0,8	NE
30	150	ANO	3,0	0,2	ANO
40	50	ANO	3,1	0,5	NE
40	100	ANO	2,9	0,0	NE
40	150	ANO	2,3	0,7	NE
50	50	ANO	2,5	0,2	NE
50	100	ANO	2,5	0,8	ANO
50	150	ANO	2,6	0,3	NE

(zdroj: vlastní)

7 VYHODNOCENÍ VÝSLEDKŮ EXPERIMENTU

Experimentální část práce byla zaměřena na ověření reakce autonomního systému VISU L900 PRO SE na výpadek řídicí komunikace způsobený rušením v pásmu 2.4 GHz. Testy probíhaly na otevřeném prostranství, kde byly kombinovány různé vzdálenosti dronu od ovladače (50, 100 a 150 metrů), vzdálenosti rušiče (Flipper Zero s připojeným ESP32-S2 WROVER) od ovladače (10 až 200 centimetrů) a různé délky rušení (10 až 50 sekund). V každém scénáři bylo sledováno, zda dojde ke ztrátě komunikace, jak rychle systém reaguje, zda aktivuje RTH a jak přesně se dokáže vrátit k výchozímu bodu.

Výsledky ukázaly, že ve všech případech byl návrat úspěšně dokončen. Autonomní systém detekoval ztrátu spojení a spolehlivě aktivoval režim RTH bez nutnosti zásahu operátora. Důležitým zjištěním je, že čas do zahájení návratu byl velmi krátký – ve všech scénářích se pohyboval v rozmezí 1,9 až 3,4 sekundy, což svědčí o rychlé detekci výpadku signálu a okamžité reakci systému. Tento výsledek je pozitivní i vzhledem k tomu, že testovaný systém nevyužívá pokročilé komunikační protokoly ani šifrování.

Co se týče přesnosti návratu, systém vykazoval velmi stabilní chování. Dron se ve všech případech vrátil v rozmezí jednoho až tří metrů od výchozího bodu, což odpovídá standardní odchylce GNSS navigace v daných podmínkách. Přistání proběhlo vždy kontrolovaně a v dostatečné vzdálenosti od operátora. Navzdory celkové spolehlivosti však byla v několika testech pozorována krátkodobá ztráta stability. Ta se projevila poklesem výšky o přibližně jeden metr bezprostředně po ztrátě signálu, ještě před zahájením návratu. Tento jev nenarušil let samotný, ani nedošlo k pádu či ztrátě kontroly, nicméně poukazuje na přechodný stav systému, ve kterém nemusí být výšková stabilita okamžitě zajištěna.

Celkově lze experimentální část hodnotit jako úspěšnou. Testy prokázaly, že systém v kontrolovaných podmínkách dokáže na ztrátu komunikace reagovat spolehlivě, rychle a bez kritických výpadků. Výsledky zároveň poukázaly na dílčí slabinu v oblasti stabilizační logiky, která by mohla být v náročnějším prostředí zdrojem potenciálního rizika. Tento poznatek tvoří základ pro návrh technických a systémových opatření, které budou rozvedeny v následující kapitole.

7.1 Analýza naměřených hodnot a chování systému

V rámci experimentálního testování byly systematicky sledovány čtyři hlavní parametry – čas do zahájení návratu, úspěšnost dokončení návratu, přesnost přistání a přítomnost ztráty stability. Data byla získána napříč několika testovacími scénáři, které kombinovaly různé vzdálenosti dronu (50, 100 a 150 metrů) a různé vzdálenosti rušiče (10 až 200 cm) od ovladače, při délce rušení 10 až 50 sekund.

Nejdůležitějším zjištěním je skutečnost, že ve všech scénářích byl návrat úspěšně dokončen, bez výjimky. To svědčí o správné funkci bezpečnostního režimu RTH a jeho schopnosti aktivovat se i za podmínek trvajících rušení. Systém se tak jeví jako robustní z hlediska základní reakce na ztrátu spojení. Čas do zahájení návratu byl velmi konzistentní. Ve všech 15 měřených případech se pohyboval v rozmezí 1,9 až 3,4 sekund. Průměrná hodnota se ustálila kolem 2,7 sekund. Tato rychlost reakce potvrzuje schopnost systému okamžitě detekovat přerušení signálu bez výrazného zpoždění. Nebyla pozorována přímá závislost mezi délkou rušení a dobou aktivace RTH – chování bylo konzistentní napříč všemi testy. Přesnost návratu se pohybovala od 0 do 0,9 metrů, což odpovídá očekávané odchylce způsobené přesností GNSS lokalizace.

Ztráta stability byla zaznamenána v 14 ze 75 případů. Vyhodnocení ztráty stability probíhalo formou přímého pozorování operátorem z hlavního ovládacího stanoviště. Pokles výšky o přibližně 1 metr byl zaznamenán u části testů, a to bezprostředně po ztrátě signálu a před aktivací režimu návratu (RTH). Tento jev se neobjevil u všech měření, ale jeho výskyt byl zaznamenán opakovaně v několika scénářích. K vyloučení vlivu povětrnostních podmínek byly všechny testy prováděny za stabilního počasí bez větru nebo při velmi slabém vánku (do 1 m/s, ověřeno pomocí aplikace Windy). Na základě těchto skutečností byl pokles vyhodnocen jako pravděpodobná autonomní reakce systému na výpadek komunikace, nikoli jako důsledek náhodného environmentálního vlivu.

Z dat vyplývá, že čas do zahájení RTH byl nezávislý na délce rušení a že systém zůstal provozně stabilní, i když došlo ke krátkodobé výškové odchylce. Tyto výsledky potvrzují, že testovaný systém je dostatečně robustní pro základní krizové scénáře. Zároveň však poukazují na prostor ke zlepšení v oblasti stabilizační logiky a signalizace stavu systému operátorovi.

8 NÁVRH OCHRANNÝCH OPATŘENÍ

Na základě výsledků experimentálního testování bylo potvrzeno, že autonomní systém VISU L900 PRO SE dokáže při výpadku řídicí komunikace spolehlivě aktivovat bezpečnostní RTH a úspěšně dokončit přistání. Nicméně v některých případech byla zaznamenána krátkodobá ztráta výškové stability, konkrétně pokles výšky o přibližně jeden metr bezprostředně po ztrátě signálu. Tato reakce naznačuje, že systém sice zvládá krizovou situaci z hlediska celkového řízení, ale nedisponuje okamžitou stabilizační odezvou na dynamické rušení. Dále byl identifikován nedostatek v podobě absence šifrování, autentizace a zpětné vazby o stavu spojení.

Ačkoli standardní bezdrátové protokoly, jako je Wi-Fi, již obsahují některé bezpečnostní prvky (například šifrování WPA2), v prostředí autonomních systémů tyto mechanismy často nepostačují. Tyto protokoly byly primárně navrženy pro běžnou spotřebitelskou komunikaci, nikoli pro kritické řízení v reálném čase, které klade vysoké nároky na dostupnost, spolehlivost a integritu dat. V minulosti byly odhaleny zranitelnosti jako například KRACK (Key Reinstallation Attack), která ukázala, že i relativně pokročilé bezpečnostní standardy mohou být snadno zneužitelné, pokud nejsou správně implementovány nebo pravidelně aktualizovány. [60] Na základě těchto zjištění lze navrhnout následující soubor technických opatření ke zvýšení odolnosti systému vůči útokům i náhodným výpadkům komunikace.

Prvním doporučením je implementace zabezpečené komunikace mezi ovladačem a dronem. Testovaný systém využívá nešifrované přenosy v pásmu 2.4 GHz, které jsou zranitelné vůči útokům typu jamming, spoofing či hijacking. Z hlediska kybernetické bezpečnosti by mělo dojít k nasazení symetrické kryptografie, například AES-128 nebo AES-256, v kombinaci s autentizačními mechanismy typu HMAC (Hash-based Message Authentication Code). Klíčová výměna může být realizována buď staticky před vzletem, nebo dynamicky s využitím asymetrického protokolu. Takové řešení by výrazně snížilo riziko neoprávněného vstupu do řídicího kanálu. [56]

Dalším navrženým opatřením je integrace systému pro detekci rušení a anomálií v přenosu. Systém by měl být schopen v reálném čase monitorovat signálové parametry jako je síla signálu (RSSI – Received Signal Strength Indicator), poměr signálu k šumu (SNR – Signal-to-Noise Ratio) nebo četnost ztracených paketů. V případě odchylky od normálního chování může systém aktivovat varování, přepnout do bezpečnostního režimu, případně

přejít na záložní kanál. Detekce může být provedena jak heuristicky, tak na základě prediktivních modelů využívajících strojové učení. [57]

Pro prevenci rizik spojených s neřízeným pohybem v prostoru je doporučena implementace geofencingu, tedy softwarově definovaných hranic provozu. Při překročení předem definované oblasti, nebo v případě ztráty spojení mimo povolenou zónu, může systém provést nouzové přistání, přejít do režimu loiter nebo se vrátit do výchozího bodu. Režim loiter označuje stav, kdy se dron začne automaticky pohybovat v kruhové trajektorii kolem poslední známé pozice (nebo zadaného bodu) ve stanovené výšce a rychlosti, a vyčkává na další pokyny nebo obnovení spojení. Tato metoda omezuje provoz zařízení pouze na bezpečně definovanou oblast a snižuje pravděpodobnost škod. [58][58]

Neméně důležitým prvkem je záznam provozních dat. Dron by měl kontinuálně logovat klíčové parametry letu jako je poloha, výška, stav spojení, přijaté příkazy a systémové reakce. Tato data, ukládaná do kruhového bufferu, umožňují zpětnou analýzu incidentů, optimalizaci parametrů řízení a forenzní vyšetření v případě selhání. Datový formát může být založen na otevřených standardech jako je MAVLink, nebo na binárním proprietárním protokolu s exportní funkcí po přistání. [59]

Zavedení výše uvedených opatření výrazně zvyšuje provozní bezpečnost a systémovou odolnost autonomních zařízení. Ačkoliv se v testovaných scénářích jednalo o relativně jednoduchý komerční UAV, principy těchto návrhů jsou přenositelné i na komplexnější autonomní platformy určené pro profesionální nasazení v oblastech s vysokými požadavky na bezpečnost a spolehlivost provozu.

ZÁVĚR

Tato bakalářská práce se zabývala problematikou bezpečnosti autonomních systémů se zaměřením na jejich odolnost vůči výpadkům řídicích komunikačních kanálů a potenciálním bezpečnostním hrozbám, které z takových výpadků vyplývají. Teoretická část práce poskytla úvod do architektury autonomních systémů, analyzovala základní komponenty jako senzory, komunikační moduly a rozhodovací algoritmy a poukázala na klíčová rizika spojená s útoky na integritu, dostupnost a funkčnost těchto systémů. Zvláštní důraz byl kladen na detekci rušení, metody redundance a mezinárodní standardy kybernetické a provozní bezpečnosti.

V praktické části byl jako modelový autonomní systém zvolen komerčně dostupný bezpilotní prostředek VISU L900 PRO SE. Pomocí nástroje Flipper Zero s alternativním firmwarem Unleashed a připojeným modulem ESP32-S2 byl v řízených podmínkách simulován výpadek komunikace způsobený rušením v pásmu 2.4 GHz. Experiment probíhal ve třech vzdálenostech dronu (50, 100 a 150 m) a při pěti vzdálenostech rušiče od ovladače, přičemž byl sledován čas aktivace bezpečnostního režimu návratu (RTH), přesnost návratu, reakce systému a výskyt ztráty stability.

Výsledky testů prokázaly vysokou míru robustnosti základních funkcí systému – návrat byl ve všech případech úspěšně dokončen a čas do zahájení návratu se pohyboval v úzkém rozmezí 1,9 až 3,4 sekundy. Z hlediska přesnosti návratu byla odchylka většinou v intervalu 1–3 metrů, což odpovídá možností standardní GNSS navigace. Zároveň však bylo v 14 z 75 případů pozorováno krátkodobé narušení letové stability v podobě poklesu výšky po ztrátě spojení. Tento jev, i když nepředstavoval bezprostřední riziko, poukazuje na určitá omezení reakční logiky systému.

Na základě získaných poznatků byla navržena technická opatření ke zvýšení bezpečnosti autonomních systémů. Mezi klíčová doporučení patří zavedení šifrování a autentizace komunikace, detekce rušení pomocí síťových metrik nebo strojového učení, geofencingu a kontinuální logování provozních dat. Tato opatření jsou realizovatelná i v prostředí komerčních UAV a mohou výrazně zvýšit jejich odolnost vůči provozním i cíleným hrozbám.

SEZNAM POUŽITÉ LITERATURY

- [1] LUCKCUCK, Matt; FARRELL, Marie; DENNIS, Louise A.; DIXON, Clare a FISHER, Michael. Formal Specification and Verification of Autonomous Robotic Systems. *ACM Computing Surveys*, 2020, roč. 52, č. 5, s. 1-41. ISSN 0360-0300. Dostupné z: <https://Dostupné z.org/10.1145/3342355>.
- [2] HUSSEIN, Mahmoud; NOUACER, Réda; CORRADI, Federico; OUHAMMOU, Yassine; VILLAR, Eugenio et al. Key technologies for safe and autonomous drones. *Microprocessors and Microsystems*, 2021, roč. 87. ISSN 01419331. Dostupné z: <https://Dostupné z.org/10.1016/j.micpro.2021.104348>.
- [3] GNAMBS, Timo a APPEL, Markus. Are robots becoming unpopular? Changes in attitudes towards autonomous robotic systems in Europe. *Computers in Human Behavior*, 2019, roč. 93, s. 53-61. ISSN 07475632. Dostupné z: <https://Dostupné z.org/10.1016/j.chb.2018.11.045>.
- [4] GUGAN, Gopi a HAQUE, Anwar. Path Planning for Autonomous Drones: Challenges and Future Directions. *Drones*, 2023, roč. 7, č. 3. ISSN 2504-446X. Dostupné z: <https://Dostupné z.org/10.3390/drones7030169>.
- [5] LI, Keyu; XU, Yangxin a MENG, Max Q.-H. An Overview of Systems and Techniques for Autonomous Robotic Ultrasound Acquisitions. *IEEE Transactions on Medical Robotics and Bionics*, 2021, roč. 3, č. 2, s. 510-524. ISSN 2576-3202. Dostupné z: <https://Dostupné z.org/10.1109/TMRB.2021.3072190>.
- [6] Ministerstvo dopravy ČR. Minimum pro státní správu: Etická komise pro autonomní mobilitu [online]. Praha: Ministerstvo dopravy ČR, 2023. Dostupné z: https://md.gov.cz/getattachment/Uzitecne-odkazy/Autonomni-mobilita/Eticka-komise-Link/Minimum_pro_statni_spravu_EK.pdf.aspx
- [7] ROESE Matthias. Cesta průmyslu od automatizace k autonomii. Dostupné z: <https://www.systemonline.cz/rizeni-vyroby/cesta-prumyslu-od-automatizace-k-autonomii.htm>
- [8] IEEE Transactions on Medical Robotics and Bionics. Autonomní robotické systémy v chirurgii [online]. IEEE, 2022. Dostupné z: https://ak.aos.sk/images/repozitar/vr/vr_2_2022/vr_2_2022_4_ZRZ.pdf

- [9] Vše o průmyslu. Technologické trendy budoucnosti: digitální dvojčata, autonomní stroje a umělá inteligence [online]. Praha: Trade Media International, 2023. Dostupné z: <https://www.vseoprumsly.cz/inspirace/trendy/technologicke-trendy-budoucnosti-digitalni-dvojcata-autonomni-stroje-a-umela-inteligence.html>
- [10] ČSN ISO/IEC 27000:2019. Informační technologie Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník. Česká technická norma, 2019.
- [11] SICILIANO, Bruno; KHATIB, Oussama. Springer Handbook of Robotics. Cham: Springer, 2016. ISBN 978-3319325507.
- [12] THRUN, Sebastian; BURGARD, Wolfram; FOX, Dieter. Probabilistic Robotics. Cambridge, MA: MIT Press, 2005. ISBN 978-0262201629.
- [13] STENGEL, Robert F. Flight Dynamics. Princeton: Princeton University Press, 2022. ISBN 978-0691220255.
- [14] KUMAR, Rakesh; RATHORE, Virender Singh. Secure and Robust Communication in Autonomous Systems. IEEE Transactions on Systems, Man, and Cybernetics. 2020, ISSN 2168-2216.
- [15] GANDHI, T.; TRIVEDI, Mohan M. Computer Vision and Machine Learning for Enhancing Autonomous Driving Systems. IEEE Transactions on Intelligent Transportation Systems. 2007, roč. 8, č. 4, s. 742–753. ISSN 1524-9050.
- [16] TIPPENHAUER, Nils Ole et al. On the requirements for successful GPS spoofing attacks. In: Proceedings of the ACM Conference on Computer and Communications Security. Chicago, IL, 2011, s. 75–86. ISBN 978-1-4503-0948-6. Dostupné z: 10.1145/2046707.2046719.
- [17] HUMPHREYS, Todd E. Statement on the vulnerability of civil unmanned aerial vehicles to GPS spoofing. Testimony before the Subcommittee on Oversight, Investigations, and Management, House Homeland Security Committee, 2012.
- [18] KOLIAS, Christos et al. DDoS in the IoT: Mirai and other botnets. Computer. 2017, roč. 50, č. 7, s. 80–84. ISSN 0018-9162. Dostupné z: 10.1109/MC.2017.201.
- [19] GOODALL, Noah J. Machine Ethics and Automated Vehicles. In: Road Vehicle Automation 6. Cham: Springer, 2019, s. 109–119. ISBN 978-3-030-22948-6. Dostupné z: 10.1007/978-3-030-22948-6_7.

- [20] FAVARÒ, F. M. et al. Examining accident reports involving autonomous vehicles in California. *Accident Analysis & Prevention*. 2018, roč. 123, s. 274–282. Dostupné z: 10.1016/j.aap.2018.03.021.
- [21] Associated Press in Berlin. Robot kills worker at Volkswagen plant in Germany. *The Verge* [online]. 2015. [cit. 2025-05-27]. Dostupné z: <https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany>.
- [22] GREENBERG, Andy. The WannaCry ransomware attack. *WIRED* [online]. 2017. [cit. 2025-05-27]. Dostupné z: <https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/>.
- [23] STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. Boston: Pearson, 2016. ISBN 978-0134444284.
- [24] SCHNEIER, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: Wiley, 2015. ISBN 978-1119096726.
- [25] BONNEAU, Joseph et al. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: *2012 IEEE Symposium on Security and Privacy*. San Francisco, CA, 2012, s. 1–16. Dostupné z: 10.1109/SP.2012.44.
- [26] LOCKE, David; RICHARDSON, Curtis. MQTT Version 5.0. OASIS Standard [online]. 2020. [cit. 2025-05-27]. Dostupné z: <https://mqtt.org>.
- [27] MORIARTY, Ken. *Network Security with OpenSSL: Cryptography for Secure Communications*. Sebastopol, CA: O'Reilly Media, 2020. ISBN 978-0596002701.
- [28] MUCCHI, L. et al. Enhancing communication security in IoT using lightweight cryptographic approaches. *Sensors*. 2018, roč. 18, č. 11, s. 3836. Dostupné z: 10.3390/s18113836.
- [29] ROS 2 Documentation. Security in ROS 2 [online]. 2023. [cit. 2025-05-27]. Dostupné z: <https://docs.ros.org>.
- [30] ISERMANN, Rolf. *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Berlin: Springer, 2006. ISBN 978-3540303688.

- [31] CHEN, J.; PATTON, R. J. Robust Model-Based Fault Diagnosis for Dynamic Systems. Boston: Springer, 1999. ISBN 978-0792384622.
- [32] MORRISON, Mark; SCHWARTZ, David. Fault-tolerant sensor systems in autonomous vehicles. *Automotive Sensors Journal*. 2019, roč. 22, č. 4, s. 345–359. Dostupné z: 10.1016/j.autsen.2019.04.010.
- [33] KHALEGHI, Bahram et al. Multisensor data fusion: A review of the state-of-the-art. *Information Fusion*. 2013, roč. 14, č. 1, s. 28–44. Dostupné z: 10.1016/j.inffus.2011.08.001.
- [34] KORTENKAMP, David; SIMMONS, Reid. Sensor Fusion in Robotics: Principles and Practice. New York: Springer, 2008. ISBN 978-1441964587.
- [35] MURPHY, Robin. Using sensor fusion for fault-tolerant control in robotics. *Robotics and Automation Magazine*. 2019, roč. 26, č. 3, s. 56–63. Dostupné z: 10.1109/MRA.2019.2926887.
- [36] International Organization for Standardization. ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO, 2013.
- [37] CALDER, Alan. ISO/IEC 27001:2013—A Pocket Guide. Ely: IT Governance Publishing, 2020. ISBN 978-1787782182.
- [38] FEDERAL AVIATION ADMINISTRATION. Summary of Small Unmanned Aircraft Rule (Part 107) [online]. Washington, D.C.: FAA, 2016. [cit. 2025-01-04]. Dostupné z: <https://www.faa.gov/>.
- [39] EUROPEAN UNION AVIATION SAFETY AGENCY. European Union Aviation Safety Agency: Drones - Regulatory Framework [online]. Cologne: EASA, 2020. [cit. 2025-01-04]. Dostupné z: <https://www.easa.europa.eu/>.
- [40] VOIGT, Paul; VON DEM BUSSCHE, Axel. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer, 2017. ISBN 978-3319579597.
- [41] SHARKEY, Noel. Saying “no!” to lethal autonomous targeting. *Journal of Military Ethics*. 2010, roč. 9, č. 4, s. 369–383. Dostupné z: 10.1080/15027570.2010.536403.

- [42] SPARROW, Robert. Killer robots. *Journal of Applied Philosophy*. 2007, roč. 24, č. 1, s. 62–77. Dostupné z: 10.1111/j.1468-5930.2007.00346.x.
- [43] WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*. 2021, roč. 41, s. 105567. Dostupné z: 10.1016/j.clsr.2020.105567.
- [44] EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689, 12 July 2024. [Online]. [Cit. 2025-05-27]. Dostupné z: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [45] ISTQB. Standard Glossary of Terms used in Software Testing. Online. Version 4.0. International Software Testing Qualifications Board, 2021. [Cit. 2025-05-27]. Dostupné z: <https://glossary.istqb.org>
- [46] PAGALLO, Ugo. *The Laws of Robots: Crimes, Contracts, and Torts*. Cham: Springer Science & Business Media, 2013. ISBN 978-9400765641.
- [47] GILPIN, Leilani H.; BAHRAMI, Mohammad; ZHANG, Ayesha et al. Explaining Explanations: An Overview of Interpretability of Machine Learning. Online. IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA), 2018. s. 80–89. ISBN 978-1-5386-5090-5. Dostupné z: <https://doi.org/10.1109/DSAA.2018.00018>
- [48] TILLY, Reuben. 1960 – “Stanford Cart” – (American). CyberneticZoo.com [online]. 7. února 2010 [cit. 2025-05-21]. Dostupné z: <https://cyberneticzoo.com/cyberneticanimals/1960-stanford-cart-american/>
- [49] HAMILTON, Danny Shapiro. *What Is a LiDAR Sensor?*. NVIDIA Blog [online]. 14. října 2021 [cit. 2025-05-21]. Dostupné z: <https://blogs.nvidia.com/blog/lidar-sensor-nvidia-drive/>
- [50] SULLIVAN, Kevin. A DSP For Implementing High-Performance Sensor Fusion On An Embedded Budget [online]. SemiEngineering, 2021 [cit. 2025-05-21].

- Dostupné z: <https://semiengineering.com/a-dsp-for-implementing-high-performance-sensor-fusion-on-an-embedded-budget/>
- [51] RADOŠ, Katarina, BRKIĆ, Marta a BEGUŠIĆ, Dinko. Recent Advances on Jamming and Spoofing Detection in GNSS [online]. *Sensors*, 2024, roč. 24, č. 13, s. 4210. ISSN 1424-8220. Dostupné z: <https://www.mdpi.com/1424-8220/24/13/4210>
- [52] MOORE, Ben; BISH, Alex. [Drones could bring in more 'risky' items to prison. BBC [online]. 2024-11-26. [cit. 2025-05-27]. Dostupné z: <https://www.bbc.com/news/articles/cr4lk0g96zpo> The Guardian. Drones used for corporate espionage spark privacy fears. The Guardian [online]. 2018 [cit. 2025-05-21]. Dostupné z: <https://www.theguardian.com/technology/2018/feb/12/drones-used-corporate-espionage-privacy-concerns>
- [53] GATES, Megan. A Rising Threat: Using Drones to Conduct Corporate Espionage. Online. Security Management, 2025 [cit. 2025-05-21]. Dostupné z: <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/march/drone-corporate-espionage/>
- [54] Shenzhen CTB Testing Technology Co., Ltd. FCC test report No. CTB230320001RF – *REMOTE CONTROL QUADCOPTER (Model L900 PRO)*. Shenzhen, 2023. 28 s. Dostupné ve formátu PDF.
- [55] Bay Area Compliance Laboratories Corp. *Test Report – ESP32-WROOM-32E: FCC Part 15.247*. RSHD200218007-00A. Kunshan, 2020. 84 s.
- [56] PEAR, Channing. *Encryption vs. Authentication in Drone Data*. Anvil Labs [online]. 2025-01-31. [cit. 2025-05-28]. Dostupné z: <https://anvil.so/post/encryption-vs-authentication-in-drone-data>
- [57] CIBECCHINI, Sergio; CHITI, Francesco; PIERUCCI, Laura. A Lightweight AI-Based Approach for Drone Jamming Detection. *Future Internet* [online]. 2025, roč. 17, č. 1, s. 14. [cit. 2025-05-28]. Dostupné z: <https://www.mdpi.com/1999-5903/17/1/14>. DOI: 10.3390/fi17010014.
- [58] SKYBRARY Aviation Safety. *Geofencing Basics*. SKYbrary [online]. 2021. [cit. 2025-05-28]. Dostupné z: <https://skybrary.aero/articles/geofencing-basics>
- [59] STAFF WRITER. *Flight Data Recorder (FDR) and Black Box Systems for UAVs*. Unmanned Systems Technology [online]. Poslední aktualizace 2025-01-02.

[cit. 2025-05-28]. Dostupné z:
<https://www.unmannedsystemstechnology.com/expo/uav-flight-data-recorder-black-box>

- [60] VANHOEF, Mathy a PIESENS, Frank. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Online. 2017. Dostupné z: <https://www.krackattacks.com>

SEZNAM OBRÁZKŮ

Obrázek 1 - Blokové schéma autonomního vozidla	15
Obrázek 2 - Stanford Cart: první autonomní vozidlo vyvíjené na Stanfordu	16
Obrázek 3 - Detekce objektů pomocí lidarů	21
Obrázek 4 - Schéma výkonné fúze senzorů s vestavěným rozpočtem	22
Obrázek 5 - rozdíl mezi spoofing a jamming.....	24
Obrázek 6 -schéma MITM.....	25
Obrázek 7 – modul ESP32-S2 WROVER	41
Obrázek 8 - Flipper zero s aplikací wifi marauder.....	41
Obrázek 9 – Dron VISU L900 PRO SE.....	43
Obrázek 10 - Ovladač dronu	44
Obrázek 11 - Schéma experimentálního testování reakce dronu na rušení řídicí komunikace	47
Obrázek 13 - Vzdálenost Flipperu od ovladače	48
Obrázek 12 - Startovací pozice dronu.....	48

SEZNAM TABULEK

Tabulka 1 - SWOT analýza	45
Tabulka 2 - Flipper Zero ve vzdálenosti 10 cm	50
Tabulka 3 - Flipper Zero ve vzdálenosti 50 cm	51
Tabulka 4 - Flipper Zero ve vzdálenosti 100 cm	52
Tabulka 5 - Flipper Zero ve vzdálenosti 150 cm	53
Tabulka 6 - Flipper Zero ve vzdálenosti 200 cm	54

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI – Artificial Intelligence

AS – Autonomní systém

AES – Advanced Encryption Standard

DDS – Data Distribution Service

DDoS – Distributed Denial of Service

DoS – Denial of Service

EASA – European Union Aviation Safety Agency

ESP32 – Mikrokontrolér s integrovanou Wi-Fi a Bluetooth (od Espressif Systems)

FAA – Federal Aviation Administration

FCC – Federal Communications Commission

GNSS – Global Navigation Satellite System

GPS – Global Positioning System

GDPR – General Data Protection Regulation

HMAC – Hash-based Message Authentication Code

IMU – Inertial Measurement Unit

IoT – Internet of Things

LAWS – Lethal Autonomous Weapon Systems

LIDAR – Light Detection and Ranging

MITM – Man-in-the-Middle

MQTT – Message Queuing Telemetry Transport

RTH – Return to Home

RSSI – Received Signal Strength Indicator

ROS/ROS 2 – Robot Operating System

SNR – Signal-to-Noise Ratio

TLS – Transport Layer Security

UAV – Unmanned Aerial Vehicle

Wi-Fi – Wireless Fidelity

XAI – Explainable Artificial Intelligence