AUTONOMNÍ VOZIDLA

Štěpán Jůda

Faculty of Mechanical Engineering, Brno University of Technology
Institute of Automation and Computer Science
Technicka 2896/2, Brno 616 69, Czech Republic
217282@vutbr.cz

Abstract: *Tato práce popisuje autonomní vozidla. Dále se zabívá stručnou historií a dále úrovněmi automatického řízení. Následně definuje největší problémy s velkou distribucí autonomních vozidel. Nadále pak mluví i o jejich výhodách a o tom čím mohou přispět v budoucnosti společně s vývojem dalších technologii.*

Keywords: *Autonomní vozidlo, Senzory, Úrovně řízení, Problémy, Počasí, Budoucnost, Kybernetika*

1 Úvod

Autonomní automobily nebo také auto bez řidiče nebo robotické auto je auto, které je schopné cestovat bez lidského zásahu. K řízení sama sebe auta využívají nejrůznější senzory, jako termografické kamery, radary, ultrazvuk, GPS, apod. Řídící systém těchto aut pak informace z těchto senzorů vyhodnotí a vytváří model okolí auta. Podle tohoto modelu pak vyhodnotí nejvhodnější cesty, reakce na dopravu a přkážky.[5] [8]
V dnešní době tato auta ještě stále nejsou schopna samostatného řízení, bez jakékoli kontroli lidského řidiče. Běžně používané autonomní automobily v dnešní době dosahují 3 úrovně automatického řízení. [3]

2 Historie samořídících automobilů

Úplně první koncept samořídících aut můžeme vystopovat do dvacátých let 20. století. Kde ovšem nešlo o samořídící auto, ale o auto dálkově ovládané, při demonstarci síly rádio komunikace. První počítačem řízené auto bylo vytvořeno na univerzitě Carnegie-Mellono v Pittsburghu v Pensylvánii. Kde bylo představeno v osumdesátých letech 20. století pod přezdívkou *Navlab 1.* Toto auto bylo schopno zatáčet a vyhýbat se překážkám. Poté v roce 1995 byly představena auta, která se sama dokázala držet v pruzích vozovky, s inteligentním rychlostním automatem, a dokázala vylepšit zorné pole řidiče. Neboli tato auta měla funkce, které dnes najdeme v běžných komerčních automobilech.
Potenciál těchto aut a automaticky naváděných systémů byl velice rychle rozpoznán. Například v USA byla v roce 1991 uvolněna částka 650 milionů dolarů na výzkum národního automatizovaného dálničního systému. Dále automobil *Navlab* ujel v roce 1995 4584 kilomentrů napříč Amerikou, kdy 4501 kilometrů bylo ujeto autonomě. Další milník přišel v roce 2012 kdy Amazon začal používat automatizované roboty. Roku 2015 pak bylo v některých státech USA povoleno testování automatizovaných vozidel na veřejných komunikacích. V roce 2017 oznámila firma *Waymo* (dříve známá jako google sefl-driving car) testování vozů bez řidiče i bez bezpečnostního řidiče. Do listopadu roku 2018 ujela tato auta 16 milionů kilometrů v automatizovaném režimu. V roce 2021 pak Honda začal pronajímat automatizované automobily na 3. úrovni automatického řízení. [2]

3 Úrovně automatického řízení

Society of Automotive Engineers, zkráceně SAE, definovala 6 úrovní automatického řízení. A další důležité pojmy v kontextu automatizace motorových vozidel a jejich provozu na pozemních komunikacích.
Úrovně autonomnosti jsou definovány následovně:

Table 1: Definice úrovní autonomního řízení [4]

Úroveň	Míra Autonomnosti
Úroveň 0	Žádná aotomatizace řízení
Úroveň 1	Asistence pro řidiče
Úroveň 2	Částečná automatizace jízdy
Úroveň 3	Podmíněná automatizace řízení
Úroveň 4	Vysoká automatizace jízdy
Úroveň 5	Plná automatizace řízení

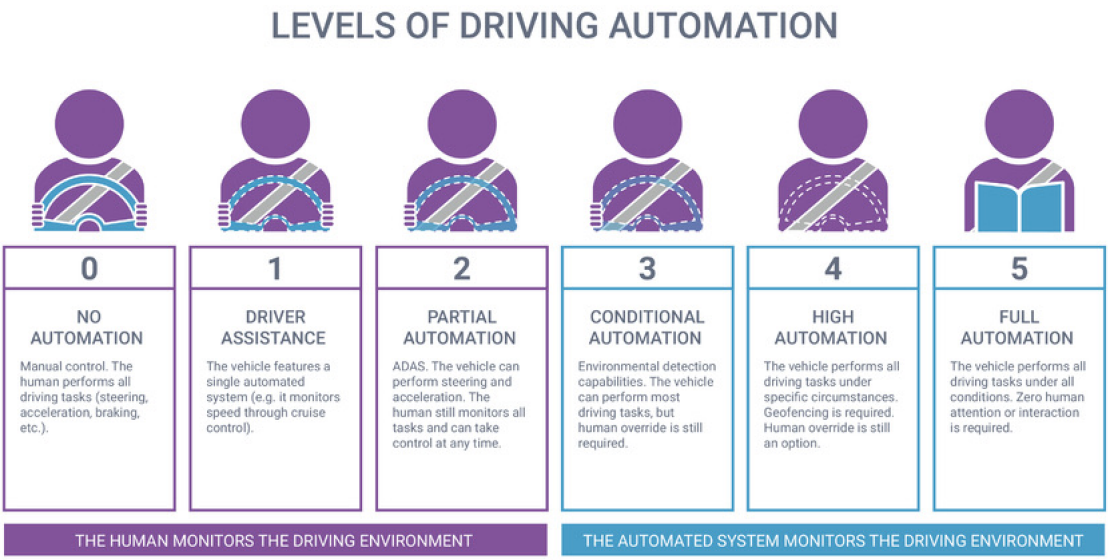

Figure 1: Úrovně autonomnosti řízení [1]

Dále také definují tři hlavní aktéry v řízení a to: (Lidského) Uživatele, systém automatizace řízení a další systémy, komponenty vozidla (nebo vozidlo obecně). Samotné úrovně automatizace řízení jsou pak definovány s odkazem na roli, kterou má každý z těchto tří aktérů v úloze dynamického řízení. "Role" odkazuje na očekávanou roli primárního aktéra, ne nutně na jeho skutečný víkon. Například řidič, který při zapojení adaptivního systému tempomatu úrovně 1 nesleduje vozovku, je stále v roli řidiče.

4 Potenciální problémy autonomních vozidel

Jak jsem již zmiňoval autonomní dopravní prostředky mají obrovský potenciál. Ovšem tato technologie stále není dokonalá a je stále omezována řadou problémů, které je nutné vyřešit před úplným zavedením. Mezi tyto problémy může patřit například:
Čas potřebný k uvedení autonomních vozidel, kdy bude část vozidel na komunikaci stále neautonomní. Obavy o bezpečnost, jak cestujících tak potenciálních obětí. Kybernetické útoky na autonomní vozidla. Etické problémy, kdy je software nucen rozhodnout v případě nevyhnutelné havárie. Potenciál velké nezaměstnanosti, kvůli irelevatnosti řidičské profese. Přístup k obrovské databázi dat ze senzorů autonomních vozidel. Interpretace verbální a neverbální komunikace všech účastníků provozu softwarem. Problémy omezené viditelnosti senzorů a podobně.

4.1 Etické problémy

Etické problémy autonomních vozidel jsou nejlépe demonstrovatelné v situaci, kdy systém nemůže předjít nehodě a musí si vybrat kdo bude obětí nehody. Tento problém je především známí jako *Tramvajové dilema*. Což je serie otázek, kdy je nehoda nevyhnutelná a aktér má možnost rozhodnou, kdo bude obětí nehody. Tento problém se může zdát být nerelevatní, jelikož jak ukazuje studie tak asi 94 procent nehod je zaviněno lidským faktorem.

Tudíž by se mohlo zdát, že autonomní vozidla tyto chyby neudělají. Ovšem můžou nastat situace kdy je nehoda opravdu nevyhnutelná. Dalším problémem je, jak lze vůbec eiku do sofwaru naprogramovat ?[6]

4.2 Vliv špatného počasí na autonomní vozidla

Dalším z problémů autonomních vozidel je vliv nepříznivého počasí na senzory. Například v mlze, dešti sněhu a podobně, jsou lidské smysly ovlivněny a řidiči jsou více závislí na autonomní asistenci vozidla. Problémem je, že i senzory těchto autonomních systémů jsou taky negativně ovlivněny. Tudíž může docházet ke špatnému vyhodnocení informací, které jsou kvůli vnějším vlivům na senzory nepřesné a může docházet k nehodám.
Všechna autonomní vozidla využívají různé senzory ke snímání svého okolí, aby na základě těchto informací mohli vyhodnotit situaci a zachovat se co nejlépe. Nyní zde popíši vlivy nepřízně počasí na různé senzory autonomních vozidel.
Lidar je senzor, který používá laser k měření vzdálenosti a polohy oběktů. Senzor vyšle laseroví pulz, který se při setkání s překážkou odrazí a vrátí zpět do senzoru. Senzor pak vyhodnotí vzdálenost oběktu na základě času, jak dlouho trvalo paprsku se vrátit. Za deštivých podmínek vytváří vodní kapky, které jsou v těsné blízkosti senzoru mají velkou šanci zmást senzor, který vyhodnotí překážku v těsné blízkosti vozidla, což by mohlo vést k nehodám.
Kamery ve vozidle mají za úkol shromažďovat pomocné visuální informace pro řidiče. Například pomáhat detekovat chodníky, silniční značky, potencionální nebezpečí nebo překážky. Tyto systémy fungují perfektně za ideálních podmínek, jako je slunečné počasí. Ovšem nepříznivé počasí by nemělo jejich funkci ovlivnit jelikož řidiči, kteří jsou ne stížené situaci způsobené počasím, se na ně budou více spoléhat. Za deštivého počasí dochází ke snížení intenzity obrazu, který kamery vidí, tento obraz bude mít rozostřené okraje. Husté sněžení a kroupy můžou zvýšit intenzitu obrazu a tím zakrýt okraje objektu na obraze, tudíž systém nemusí objekt vůbec rozpoznat. Dalším problémem může být poškození kamer vlivem vlhkosti nebo mrazu a ledu.
GPS nám určuje přesnou reálnou polohu vozidla, což je základem každého navigačního systému. Počasí prakticky neovlivňuje přesnost systému GPS, ovšem může může ho ovlivnit nepřímo. Například pokud je senzor GPS umístěn na čelním skle, stěrače přejíždějící přes sklo mohou ovlivnit příjmanou informaci.
Radar má jeden z nejlpších výkonů jako senzor při nepříznivém počasí. Především radar využívající milimetrové vlny namísto mikro vln. Na takovýto radar má největší vliv tříštění vodních kapek za deštně nebo sněhových vloček.

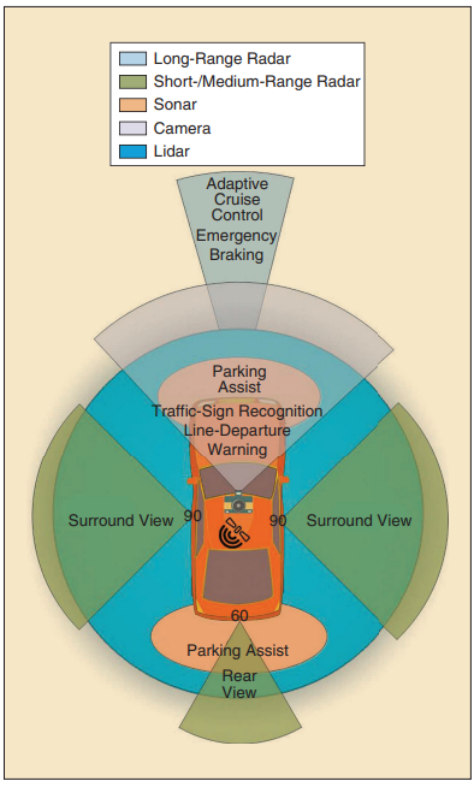

Figure 2: Různé senzory na autonomním vozidle [11]

4.3 Kybernetické útoky na autonomní vozidla

Autonomní vozidla se v blízké budoucnosti pravděpodobně dostávat více a více mezi společnost. Tudíž bude pravděpodobnější, že se některá z vozidel stanou obětí kybernetického útoku. V roce 2015 byla vytvořena tabulka, která popisuje většinu možných kybernetických útoků na autonomní vozidla. Dále popisu jak jim předejít a co přesně takové útoky můžou způsobit, od pouhého rozptýlení řidiče až po havárii. Dále ukazuje jak snadné či náročné je jednotlivé útoky detekovat jak systémem tak řidičem. Z tabulky vyplívá že při kombinaci systému a pozornosti řidiče jde většina útoků detekovat snadno.

Target	Means	Feasibility of the attack	Physical access	Ease of detection by driver	Ease of detection by system	Probability of success	Direct consequence(s)	Hazard created	Mitigation technique
Infrastructure sign	change sign (fake, irrelevant)	low	n/a	high	low	low-medium	false reaction	traffic disturbance	harden infrastructure sign change; map database of sign in-vehicle; driver reporting
	alter (change speed), make it unreadable	high	n/a	high	low	low-medium	false/no reaction	traffic disturbance	harden infrastructure sign change; map database; driver reporting
	remove (e.g. stop sign)	high	n/a	high	low	low-medium	no reaction	traffic disturbance	harden infrastructure sign change; map database; driver reporting
Machine vision	blind (only source of information)	high	no	medium	high	high	degraded mode	driver disturbance	multiple cameras with different angle
	blind (other source of information available)	high	no	medium	high	high	turn off the camera	none	n/a
	fake picture/emergency brake light (only source of information)	low	no	medium	low	medium	false reaction	driver disturbance	other source of data
	fake picture/emergency brake light (other source of information available)	low	no	medium	low	medium	false reaction	driver disturbance	n/a
GPS	spoofing	high	no	low	medium	high	wrong positioning	traffic disturbance or crash hazard	authentication
	jamming	high	no	low	medium to high	high	no accurate positioning information available	need to stop vehicle unless other location info sources available	Anti-Jam GPS techniques, high-quality IMU
In-vehicle devices	inject malware	medium	yes for USB, no for others	low	medium	medium	depends on malware's capability	depends on malware's capability	Separation infotainment/safety buses; Intrusion Detection System/Anti-virus/Firewall
	head unit attack	medium	yes	high*	medium	medium	display unexpected information	driver disturbance	Protection of display of safety status information
Acoustic sensor	interference (electromagnetic, loud sound, inaudible)	medium	no	low to medium	low	low	turn off the sensor	n/a	filter; spectrum analysis
	fake crash sound	high	no	low to medium	low	low	false reaction	traffic disturbance	other source of data (e.g. radar)
	fake ultrasonic reflection	medium	no	low	low	low	false positive or false negative obstacle detection	traffic disturbance or low-speed crash	other source of data (e.g. lidar)
Radar	chaff	medium	no	medium	high	medium	degraded mode	traffic disturbance	filter; other source of data
	smart material (non reflective surface, invisible object)	low	no	medium	low	medium	no detection of surroundings	collision	other source of data
	jamming (saturation with noise)	high	no	low	high	medium	turn off radar/degraded mode	traffic disturbance	filter; other source of data
	ghost vehicle (signal repeater)	high	no	medium*	medium	medium	false detection	traffic disturbance	filter; other source of data
Lidar	jamming	high	no	low	high	medium	turn off lidar/degraded mode	loss of situation awareness by vehicle	filter; other source of data
	smart material (absorbent, reflective)	high	no	medium*	medium	medium	false detection (e.g. fake delineation)	traffic disturbance	filter; other source of data
Road	modify delineation	low	n/a	medium	low	low	false detection	traffic disturbance	driver reporting
	hack smart lane LEDs	low	n/a	low	low	low	false detection	traffic disturbance	
in-vehicle sensors	eavesdropping (tire pressure, bluetooth)	high	no	low	low	medium	privacy leak	none	in-vehicle security
	eavesdropping CAN bus	high	yes	medium	low	medium	reverse engineering	none	in-vehicle security
	inject CAN messages	medium	yes	medium	high	medium	false message from internal sensors	driver/traffic disturbance	in-vehicle security
Odometric sensors	magnetic attack	high	yes	low	low	medium	wrong position/navigation	traffic disturbance	other source of data
	thermal attack of gyroscope	medium	yes	low	low	low	wrong position/navigation	traffic disturbance	casing; other source of data
Electronic device(s)	EMP	low	no	low	high	medium	temporary to permanent damage to electronic components	disabling vehicle automation	EMP protection
Maps	Map poisoning	low	no	low	medium	medium	wrong maneuver	traffic disturbance, accident	authentication of maps server

Figure 3: Možnosti kybernetického útoku na autonomní vozidla [7]

5 Výhody autonomních vozidel

Nyní bych chtěl poukázat na některé z výhod, které mají autonomnív vozidla. Například asistenci při parkování, kdy se řidič nemusí obávat poškození jiných vozidel při parkování. Systém si pomocí senzorů vyhledá místo, kde auto může zaparkovat a sám zaparkuje bez asistence řidiče. Dále pak asistenční systém pro udržení jízdního pruhu, kdy systém pomocí kamer sleduje hranice pruhu a snaží se je nepřekročit. Adaptivní tempomat, kdy

si řidič může nastavit rychlost, kterou chce jet a systém si sám hlídá tuto rychlost a upravuje ji v závisloti na rychlosti vozidla před námi. GPS navigační systém, který řidiči pomáhá najít nejvhodnější, nejbezpečnější cestu do jeho cíle. Tyto systémy jsou přítomné ve většině moderních vozidel dnešní doby.
Další výhody, které by mohli budoucí autonomní vozidla mít jsou například. Systém monitorování zdravotního stavu ve vozidle. Tato schopnost vozidla by mohla pomoct především starším osobám nebo osobám se zdravotními problémy, kdy by vozidlo v případě potíží vyhodnotilo život ohrožující situaci a vyhledalo pomoc. Další nemalou výhodou v budoucnu může být kompletní kontrola řízení autonomním vozidlem. Kdy nejen odpadne startost se řízením, také bude možné předejít velkému množství nehod, zvláště, když je jich 90 procent způsobeno lidským zaviněním. [9]

6 Budoucnost autonomních vozidel

V budoucnu bude díky autonomním vozidlům a umělé inteligenci mít chytrá města. Kde všechna vozidla budou propojena a komunikovat spolu díky 5G síti. Takto propojená vozidla nebudou moci komunikovat jen mezi sebou, ale i s dynamickým dopravním značením. Například při nehodě nebo poruše bude moci být inhned nastaveno rychlostní omezení, která autonomní vozidla budou dodržovat. Dále bude možná implementace autonomní veřejné dobravy. Díky všem těmto vylepšením budou lidé schopni ušetřit spoustu, času a paliva na běžném pohybu po městě. Jelikož i díky vzájemné komunikaci budou vozidla schopna vyhledávat vhodnější a rychlejší trasy.
K těmnto chytrým městům lidsvtu ještě chybí kus cesty, jelikož je nutné dosáhnout 5. úrovně autonomnosti vozidel, také sítě, která by zvládla neustále zatížení všech těchto autonomních vozů a také vyší úrovně umělé inteligence, která by takovéto města dokázala řídit. [10]

7 Závěr

V této seminární práci jsem chtěl popsat co to jsou autonomní vozidla a jejich úrovně. Dále jsem popsal historii samořídících automobilů a úrovně automatického řízení, které jsou pro tyto vozi definovány. Dále jsem se zaměřil na problémy, které můžou vzniknout s budoucím rozšiřováním autonomních automobilů. Na závěr jsem pak popsal i výhody autonomních automobilů a také kam se pravděpodobně bude jejich technologie ubírat.

References

[1] The 6 levels of vehicle autonomy explained. https://www.synopsys.com/automotive/autonomous-driving-levels.html.

[2] On the road. https://web.archive.org/web/20180323062918/https://waymo.com/ontheroad/, Mar 2018.

[3] Honda to begin sales of legend with new honda sensing elite. https://global.honda/newsroom/news/2021/4210304eng-legend.html, Mar 2021.

[4] Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. https://www.sae.org/standards/content/j3016_202104/, Apr 2021.

[5] Junyan Hu, Parijat Bhowmick, Inmo Jang, Farshad Arvin, and Alexander Lanzon. A decentralized cluster formation containment framework for multirobot systems. *IEEE Transactions on Robotics*, 37(6):1936–1955, 2021.

[6] Stamatis Karnouskos. Self-driving car acceptance and the role of ethics. *IEEE Transactions on Engineering Management*, 67(2):252–265, 2020.

[7] Jonathan Petit and Steven E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, 2015.

[8] Songtao Xie, Junyan Hu, Zhengtao Ding, and Farshad Arvin. Cooperative adaptive cruise control for connected autonomous vehicles using spring damping energy model. *IEEE Transactions on Vehicular Technology*, pages 1–14, 2022.

[9] Coughlin J.F. Yang J. In-vehicle technology for self-driving cars: Advantages and challenges for aging drivers. *International Journal of Automotive Technology*, 15(2):333–340, 2014.

[10] Ibrar Yaqoob, Latif U. Khan, S. M. Ahsan Kazmi, Muhammad Imran, Nadra Guizani, and Choong Seon Hong. Autonomous driving cars in smart cities: Recent advances, requirements, and challenges. *IEEE Network*, 34(1):174–181, 2020.

[11] Shizhe Zang, Ming Ding, David Smith, Paul Tyler, Thierry Rakotoarivelo, and Mohamed Ali Kaafar. The impact of adverse weather conditions on autonomous vehicles: How rain, snow, fog, and hail affect the performance of a self-driving car. *IEEE Vehicular Technology Magazine*, 14(2):103–111, 2019.