Scientific Research Publishing

Journal of Transportation Technologies, 2024, 14, 463-499
https://www.scirp.org/journal/jtts
ISSN Online: 2160-0481
ISSN Print: 2160-0473

Reviewing the SAE Levels of Driving Automation and Research Gaps to Accelerate the Development of a Quantum-Safe CCAM Infrastructure

Fazal Raheman[1], Tejas Bhagat[1], Angel Batalla[2]

[1]Kesklinna Linnaosa, Tallinn, Estonia
[2]Last Mile Team, Madrid, Spain
Email: drfazal@bc5.eu, tejas@bc5.eu, abatalla@lastmile.team

How to cite this paper: Raheman, F., Bhagat, T. and Batalla, A. (2024) Reviewing the SAE Levels of Driving Automation and Research Gaps to Accelerate the Development of a Quantum-Safe CCAM Infrastructure. *Journal of Transportation Technologies*, **14**, 463-499.
https://doi.org/10.4236/jtts.2024.144027

Received: July 22, 2024
Accepted: August 26, 2024
Published: August 29, 2024

Abstract

Based on a review of 28 Horizon Europe-funded CCAM projects, this paper studies the current state of Connected, Cooperative, and Automated Mobility (CCAM) and identifies significant research gaps in taxonomy, cybersecurity, Artificial Intelligence (AI) and 6G research, that hinder the advancement of a future-ready CCAM infrastructure. The research emphasizes the crucial role of infrastructure in achieving autonomous mobility, shifting focus from the current vehicle-centric approach. It critiques the SAE J3016 taxonomy for its lack of emphasis on infrastructure and proposes an updated framework with an automation level dedicated to infrastructure automation. The paper highlights the existential threats posed by Quantum Computers (QC) and AI, stressing the need for quantum-safe cybersecurity measures and an ethical, controllable AI framework proposing a decentralized Collective Artificial Super Intelligence (CASI) framework. Identifying the critical need for a cooperative approach involving Road and Transport Authorities (RTAs) to achieve 100% vehicle connectivity and robust digital infrastructure, the study outlines the European Commission's Vision 2050 goals, aiming for zero fatalities, zero emissions, and sustainable mobility. The paper concludes by providing recommendations for future research directions to accelerate the development of a comprehensive, secure, and efficient CCAM ecosystem.

Keywords

CCAM, Horizon Europe, SAE J3016 taxonomy, Vision 2050, AI, Quantum Computers

1. Introduction

Mobility is one of the significant ways humanity will change in the near future [1]. 90% of 1.3 million road deaths and more than 50 million serious injuries [2] costing $1.8 Trillion annually to the global economy are caused by human errors [3]. The European Vision 2050 of **Zero Fatalities** sounded like a Utopian dream in 2011 when the European Commission published one of its first white papers on the future of mobility [4], but with self-driving collision-free autonomous vehicles (AVs) on the horizon, that dream appears a lot closer to realization than one can imagine. Free of human errors, autonomous mobility is the panacea for road accidents and deaths. Conventional wisdom would presume that autonomous vehicles will automatically lead to accident-free autonomous traffic because they eliminate human error. But will the availability of AVs indeed automatically result in autonomous traffic? The answer isn't as simple as it might appear. Autonomous vehicles are one thing, and autonomous traffic management system (ATMS) is quite another. This is essentially because our cities are far from being ready for autonomous mobility, and unfortunately not much is done to build the necessary digital infrastructure. It is the connectedness of the vehicles and the relative awareness of their peers and their navigational paths that's key to autonomous mobility. It is the shared collective intelligence of the participating vehicles that makes the traffic collision-free and autonomous. If it is the collective intelligence of the moving vehicles that makes the traffic autonomous, it must be generated, compiled, interpreted, and disseminated amongst all the participating vehicles in real-time by an autonomous traffic management system (ATMS). Such ATMS must not only provide networkability but establish robust vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or collectively V2X (vehicle-to-everything) connectivity to achieve collision-free navigation through dense, dynamic traffic of participating vehicles. Thus, the major showstopper is not the availability of fully autonomous vehicles, but the lack of 100% connectedness of the vehicles. The disconnect between all the participating vehicles and the non-existent ATMS makes completely autonomous traffic impossible. There is a need to make digital infrastructure smart enough so that AVs understand roads well enough to help them drive better than humans. The diversity of traffic regulations adds to the problem. For example, within the EU, each of the member countries has different regulations. It would be virtually impossible for manufacturers to match them all. Even a single non-participating vehicle on a busy high-speed road can ruin the smooth flow of autonomous traffic. Therefore, 100% connectedness is crucial for city or state-wide collision-free implementation of AVs, and zero accident goals cannot be achieved unless 100% V2X connectivity is achieved, and autonomous traffic infrastructure is built.

1.1. AV Research Vs Infrastructure Research

Today, level 3 automated vehicles (AVs) are in production and driving on real-world streets; and in the future, AVs are expected to play a growing role in

transport worldwide. This may be the greatest change to the way roads work since the arrival of the motor car. The adoption of autonomous mobility has the potential to increase roadway safety by minimizing the impact of human error, the principal cause of most accidents [5]. Although AVs are specifically designed to minimize the propensity to accidents, they may indeed have to face the unavoidable ones. A recent detailed review of 107 research reports on accidents involving AVs, revealed that AVs are more prone to rear-end and sideswipe collisions [6]. The review also finds that in most such collisions, the conventional human-driven vehicle was at fault for driving too fast and too close to the AV. Liu, *et al.* [7] utilized statistical analysis to identify the differences between the pre-crash scenarios of conventional vehicles and AVs and determined that the two groups differed in the number of collisions when the situation was the same. The difference between the perception-reaction time of drivers of conventional vehicles and AVs, and deficient familiarity with the dynamic driving style of AVs that embraces full compliance with traffic regulations, in addition to human driving being susceptible to human errors or behaviors, were the reasons for such accidents [8]. This leads to the conclusion that no amount of AV-centered research will lead to the "Zero Fatality" goal of Europe's Vision 2050 [9] unless 100% vehicle connectivity is achieved and the infrastructure is favorable to autonomous traffic. In conclusion, because most accidents involving AVs are rear-end and sideswipe collisions, it is obvious that the fault is not of AVs but of the conventional human-driven vehicles that can hit the AVs, irrespective of the perfection achieved by the AVs. There is a need to pay more attention to the infrastructure research that warrants a shift from current AV-centric research.

1.2. Agenda 2030 and Vision 2050 Goals

As a part of Vision 2050 "A clean planet for all" [10], the European Commission, on June 23, 2021, launched the CCAM (Connected, Cooperative, and Automated Mobility) Partnership, which aligns all stakeholders' R&I efforts to accelerate the implementation of innovative CCAM technologies and services in Europe. Since then, the commission has funded 28 projects under the Horizon Europe funding program [11]. Considering that about 50% of global road vehicle exports come from the EU [12] and considering the EU legislation around security and data protection [13], CCAM is one of the most important EU initiatives in modeling future sustainable cities. The European Union has taken a leadership position by legislating the Digital Services Act (DSA) and the world's first Artificial Intelligence Act (AIA) to regulate platforms that deploy AI [14].

Since autonomous mobility is a long-term vision (Vision 2050) to accomplish zero fatality, zero-emission, and sustainability goals, it is imperative to keep in mind the trajectory of enabling technologies and design solutions that comply with the timeline to Agenda 2030. The Vision for 2050 is what we aim to achieve for society and it calls for the necessary short-term actions, the Agenda 2030, which will then allow an Outlook to 2040.

Relevant to CCAM four domains are distinguished in EC's Agenda 2030 [15]:

1) **Highways and corridors**: Most likely the first industrialized solutions for temporarily driving without any human driver responsibility.

2) **Confined areas**: Various use cases where easier traffic circumstances promote early demonstration and limited industrialization.

3) **Urban mixed traffic**: The most important contributor to societal objectives.

4) **Rural roads**: The biggest challenge, combining high vehicle speed with full traffic complexity.

In 2050, it is expected that all vehicles will have 100% real-time connectivity on the relevant road network and all registered vehicles will have automation but at different levels:

- A vast majority of shuttles, buses, and delivery vehicles in cities will operate autonomously.
- Nearly all vehicles on highways will be able to operate without immediate driver intervention giving the occupant time for relaxation and increased productivity.
- All vehicles on all roads will have very sophisticated supporting systems installed contributing significantly to near-zero crashes as well as further reducing emissions.

ERTRAC is the European Road Transport Research Advisory Council. It is the European technology platform that brings together all CCAM stakeholders to develop a common vision for road transport research in Europe. ERTRAC aims to create and implement the needed research and innovation strategies for a sustainable and competitive European road transport system. In this context, ERTRAC is recognized and supported by the European Commission and plays an important role in meeting the EU's "*Smart and sustainable mobility strategy*".

1.3. The CCAM Enabling Technologies

In the realm of autonomous mobility, ICT plays a critical role in ensuring the smooth functioning of the infrastructure that is designed and built for CCAM. At least three technology fields will play a very important role in enabling and perhaps challenging the autonomous mobility space of the future:

i) Quantum computers will soon represent a real threat to the Internet and consequently to the CCAM infrastructure. According to the CCAM timeline (see Section 2.2 and Section 3.2), Level 5 AVs are not expected until 2030, which as illustrated in **Figure 1** is also projected as the year for the launch of the quantum computers (QC) [16] powerful enough to break current cryptography algorithms that all the Internet security protocols deploy [17]. Feared as an existential threat to humanity, the Q-Day threat is soon becoming a reality [18]. The ability of a quantum hacker to forge certificates and signatures will enable an attacker to mislead vehicles, causing massive traffic gridlock, or even manipulating vehicle movements to cause severe, possibly fatal crashes. Because QCs are already hitting a million qubit mark [19] and companies are already offering their QC services to scientists, researchers, and developers to build, test, and run quantum computing

algorithms [20], we are already hard-pressed for the time when we have to secure connected vehicles against the emerging Q-Day threat to the entire ICT infrastructure that's connected. If this threat is not addressed, the safety and security of drivers and passengers traveling in tens of millions of vehicles that use safety-critical V2X applications will be put at risk [21]. In AVs, V2X is present as a sub-category of ADAS (Advanced Driver Assistance System) [22].

Figure 1. Countdown to Q-Day (Y2Q). Credit: Cloud Security Alliance [16].

ii) Artificial Intelligence also imposes a significant challenge as it is marching towards AGI (Artificial General Intelligence). Last year the release of GPT-4 caused an uproar worldwide on speculation that the next version of GPT (GPT-5) may be AGI. Experts believe the early experiments with GPT4 already show early signs of AGI [23], and that the next version of GPT-5 may be AGI itself [24]. This led to thousands of AI experts and stakeholders signing a petition to pause further GPT-5 development for at least six months, highlighting AI's potential dangers [25]. When the respondents of an internal survey were asked about the probability of human extinction from Autonomous AI or AI misuse (**Figure 2**), a majority agreed the probability was more than 80% [26]. The existential threat and unstoppability of AI are addressed in Section 3.3.

iii) 6G (sixth generation) telecommunication technology [27] is also slated to be launched in 2030, the year of the Y2Q deadline. The ability of QC to break the classical encryption of 6G security can cause havoc across the Internet let alone disrupt the connected vehicles [28]. Section 4.4 deals with an approach to deal with this challenge.

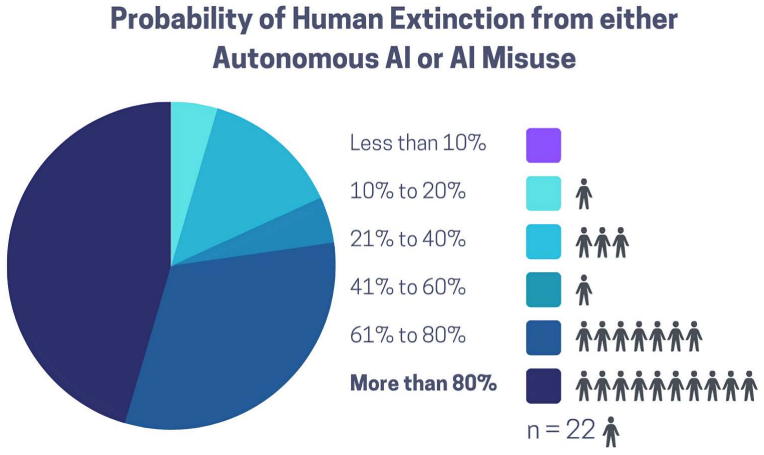

Figure 2. AI's Human Extinction Survey. Source: Conjecture [26].

1.4. Study Objectives and Structure of the Paper

Connected and autonomous mobility is a vast topic spanning across multiple disciplines. Our focus in this study is limited to identifying the gaps in European CCAM research and proposing directions to researchers and policymakers to accelerate their CCAM development initiatives.

The European Commission has so far funded 28 CCAM projects (11 IA and 17 RIA) in Horizon Europe calls since its launch in 2021. While these projects are significantly contributing to the overall CCAM knowledge base, a closer look at these projects reveals some challenges that are likely to pose obstacles to the EU's AGENDA 2030 goals and consequently adversely impact VISION 2050, but remain unaddressed. They are:

1) The current SAE Taxonomy, universally considered a gold standard, is vehicle-centric underplaying the role of mobility infrastructure in enabling CCAM and overlooks the key role of the Road and Transport Authority (RTA) of a concerned mobility jurisdiction, as a major CCAM stakeholder. Without the active cooperation of RTA, vehicles cannot become roadworthy and operate on roads.

2) Quantum-safe Cybersecurity is mandatory as Internet-breaking quantum computing is projected to premiere around 2030.

3) Artificial Intelligence is projected to soon reach the next level of AGI and pose an existential threat to humanity by becoming unstoppable if it goes rogue and unethical.

4) The estimated launch of a key CCAM enabler in the future—6G is also projected for the year 2030, around the same time as QC becomes available to threaten 6G security and consequently CCAM security.

Accordingly, the objective of this study is to:

i) review the literature to address these yet unmet challenges to CCAM.

ii) design solutions to fill the gaps in CCAM research.

iii) contribute new knowledge to the CCAM knowledge base.

iv) draft recommendations for future research in CCAM.

The following are the major contributions of this paper that advance the state-of-the-art in CCAM research:

i) A de novo review of the established taxonomy used in CCAM research suggests that it needs to be updated to shift the focus from current AV-focused autonomous mobility development to autonomous mobility infrastructure-focused development. This can be done by revising the current 6 levels of vehicle-centric driving automation to add a seventh level of infrastructure-centered autonomous traffic management system (ATMS) (Section 4.1).

ii) There is an urgent need to upgrade the current NIST (National Institute of Standards and Technology) and ENISA (European Union Agency for Cybersecurity) security recommendations of the "*Zero Trust*" (ZT) architecture to an autonomous "*Absolute Zero Trust*" (AZT) framework for mitigating the impending threats to the digital infrastructure from soon-to-premier quantum computers (QC) that pose an existential threat to humanity resulting from their capabilities to break the Internet encryption. Post Quantum Cryptography (PQC) is being

developed to counter the Q-Day threats. PQCs are failing and may not be suitable for CCAM deployment. An alternate cybersecurity strategy is proposed as a backup if PQCs fail (Section 4.2).

iii) Artificial Intelligence is one of the key technologies that enable CCAM. Unfortunately, experts predict that future generations of AI may have the potential to become uncontrollable and unstoppable causing an existential risk to humanity and a threat to human civilization [29]. A secure, ethical, controllable, and collaborative AI framework for CCAM is proposed (Section 4.3).

iv) The telecommunication network is another key enabler of CCAM, 6G is the next generation of telecommunication to be launched in 2030 coinciding with the QC arrival making 6G vulnerable to cyberattacks. There is a need to secure a 6G network [30]. A quantum-safe 6G networking protocol is discussed (Section 4.4).

The layout of the rest of this paper is structured as follows: Section 2 provides a detailed review of the literature. Section 3 examines the current gaps in EU-funded CCAM research and explores solutions to resolve those gaps. Section 4 lays down the study summary, limitations, and recommendations for future CCAM research, which is followed by the conclusion in Section 5.

2. Review of Literature

This review of the literature is specifically in reference to the challenges to CCAM and the research gaps particularly mentioned above. The previous decade had seen a lot of hope and hype around autonomous mobility. But mainstream self-driving remains far distant from early expectations. Self-driving has proven harder to get off the ground than expected. Level 3 AVs (Automated Vehicles) are already in production, but their utility is currently limited as the regulatory technological control of traffic by regulatory authorities remains grossly deficient. A decade of hype has ended in companies missing deadlines for deployments. Most autonomous mobility startups [31] have either shut down [32] or sold to big tech companies [33]. Even major ride-hailing companies such as Uber and Lyft have sold their self-driving vehicle program [34]. This is essentially because our cities are far from being ready for autonomous mobility, and unfortunately not much is done to build the digital infrastructure that is ready for future automation. Much of the CCAM research remains vehicle-centric. We review the literature de novo to identify the challenges that CCAM research is currently facing and explore solutions to resolve those challenges.

2.1. SAE Levels of Driving Automation

In achieving CCAM, building self-driving AVs may well seem to be the easiest part. The far more difficult task will be creating, securing, and maintaining our urban transportation infrastructures for AVs. The presumption that the availability of self-driving AVs will automatically result in autonomous traffic and achieve the "Zero Fatality" goal of Vision 2050 is flawed. AVs per se can neither achieve the "Zero Fatality" goal on their own, nor our current AV-centric research on

autonomous mobility can automatically make the traffic autonomous. There is a need to make digital infrastructure smart enough so that AVs understand roads well enough to help them drive better than humans. The diversity of traffic regulations adds to the problem.

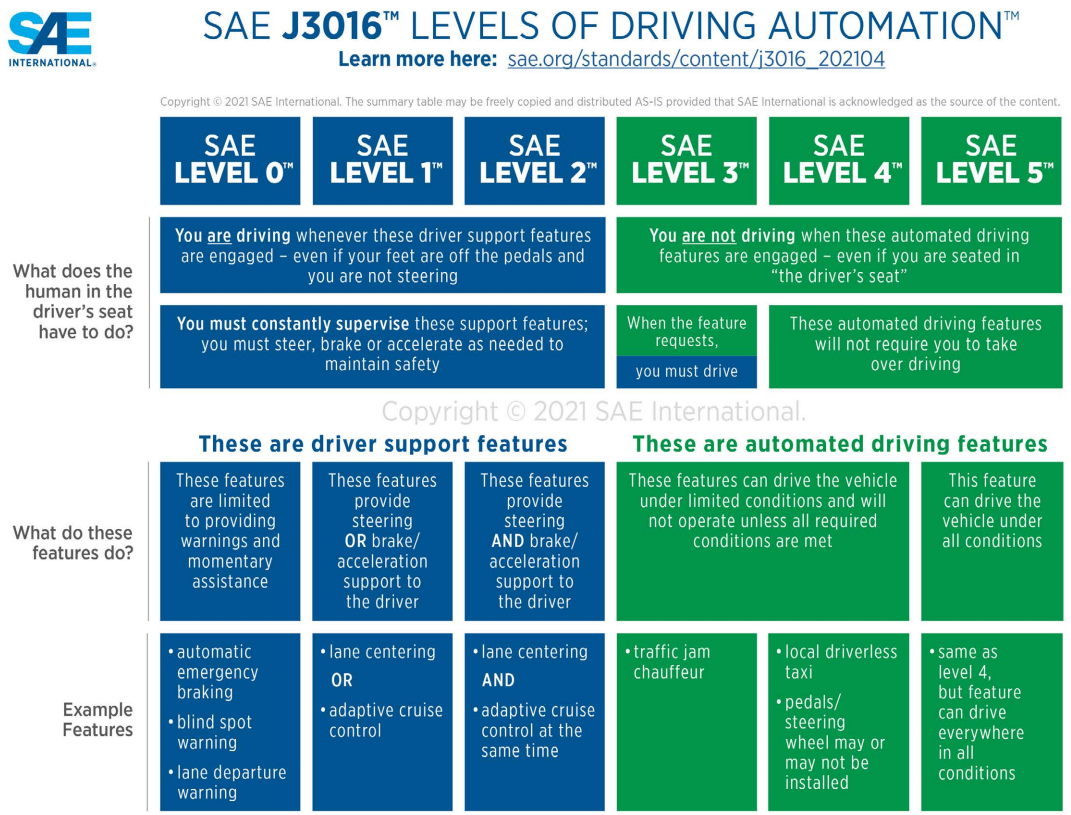

Figure 3. SAE levels of driving automation, Source: SAE [37].

One reason why CCAM research is so predominantly AV-focused and a bit easy on infrastructure development can be attributed to the SAE taxonomy on levels of driving automation (**Figure 3**). Established as a de facto gold standard for defining autonomous mobility, all 6 levels of the SAE taxonomy define autonomous mobility exclusively from the AV perspective paying little attention to the infrastructure. All of the CCAM projects, particularly, FAME [35] and INFRAMIX [36], dealing with CCAM taxonomy and CCAM infrastructure, built their concepts relying on the well-established SAE Levels of Driving Automation [37], published in 2014 by the Society of Automotive Engineers (SAE) (**Figure 3**).

2.2. Present and Future of CCAM Cybersecurity

In CCAM, the possibilities for integrating devices, infrastructure paraphernalia, and vehicles seem endless. IoT devices are deeply embedded in the automotive and smart mobility ecosystem, dramatically transforming CCAM industries with increased efficiencies and innovation. However, this rapid technological evolution presents unique challenges, particularly in ensuring the cybersecurity and data

integrity of IoT devices. The EU has been a leader in IoT compliance, enacting comprehensive legislation such as the Cybersecurity Act and GDPR compliance measures to safeguard its digital ecosystem. And, because the connectivity of these is the mainstay of CCAM, there are security risks to the networks they are connected to. As the use of open-source software in building CCAM applications becomes the norm, the risk of zero-day vulnerability increases exponentially, and the risk of cyber-attacks against connected vehicles and AVs multiplies [38]. As a result, new threats and dangers arise every day. The complexity of the growing number of safety and other features that modern vehicles integrate has caused the amount of software code to grow exponentially. CCAM development mandates a much higher reliance on software for enabling autonomous mobility leaving AVs more vulnerable to cyberattacks. Operating AV on public roads is complex on account of interactions with very unpredictable items and risks such as other vehicles, pedestrians, cyclists, potholes, or animals. As a result, AVs require orders of magnitude more complex software than aircraft [39]. For example, as illustrated in **Figure 4** an AV may have 100 million lines of code, while a Boeing 787 or a F-22 jet fighter may have only 6.5 million and 1.7 lines of code respectively [40]. Producing such CCAM software for AVs is challenging, costly, and ridden with errors, increasing the propensity of vulnerabilities system failures, and accidents [41].

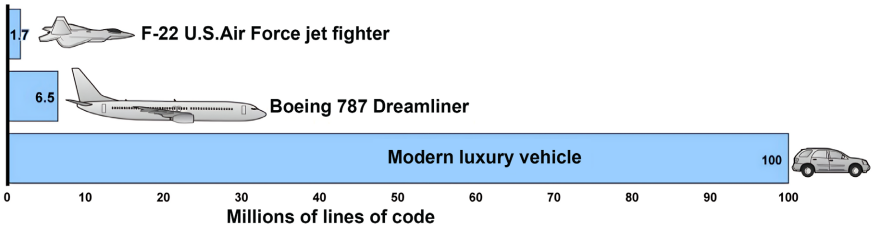

Figure 4. Aircraft and automobile code comparison. Source: GAO [40].

2.2.1. Current Cybersecurity Status

"Cybersecurity is the mother of all problems. If you do not solve it, all the other technology stuff just does not happen," [42] Cybersecurity experts unanimously agree [43] that data within a connected device can never be entirely secure because network exposure can never be risk-free. If there was a foolproof solution to cybersecurity, cybercrime would not have been predicted to skyrocket to become over $23.8 Trillion industry by 2027 [44].

a) Cyberattack Incidents:

The number and scale of cyber incidents have grown significantly over the years, threatening passenger and vehicle safety and carrying operational implications. A recent report on automotive cybersecurity report published the following facts [45]:

- In 2023, the number of high and massive-scale incidents potentially impacting millions of mobility assets increased by 2.5 times compared to 2022.
- 95% of cyber-attacks are executed remotely, and 85% of them are long-range.
- High and massive-scale attacks can potentially impact up to millions of mobility

assets (e.g. vehicles, charging stations, companion apps, backend systems).

- In 2023, deep and dark web activities related to the Automotive and Smart Mobility ecosystem have increased by 165%.
- Nearly 65% of deep and dark web cyber activities had the potential to impact thousands to millions of mobility assets.
- Attacks on telematic and application servers account for 43% of all attacks (up from 35% in 2022).
- 37% of threat actors' actions had a far-reaching impact – targeting multiple OEMs simultaneously.
- Attacks on infotainment systems have almost doubled in 2023 – accounting for 15% of all attacks (up from 8% in 2022).

In the first 6 months of 2024, Upstream reported 1300+ incidents of cyberattacks on the automotive industry[1].

Such extraordinary growth of cybercrime will get worse when the Q-day arrives. Q-Day is when quantum computers, with computing speeds millions of times faster than the fastest classical computer, will break the Internet [46].

For all the above reasons, it is imperative that the automotive sector increases its level of preparedness and reinforces its response capabilities to handle emerging cybersecurity issues connected to AI. Because the hacks could be dangerous for passengers, pedestrians, and other people on the road, AVs impose high external costs; they have higher testing and regulation standards than other technologies such as personal computers and mobile phones.

b) The AV Attack Surface:

Modern vehicles come with multiple interfaces that connect the vehicle to the external networks leaving the vehicle's safety-critical systems, such as braking and steering, vulnerable to attacks, through direct, physical access to a vehicle (via the statutorily mandated onboard diagnostics port), as well as remotely through short-range and long-range wireless channels (**Figure 5**) exploiting the vulnerabilities in the short-range and long-range wireless connections to vehicles [40] (**Figure 5**). Long-range attacks could potentially impact many vehicles and allow an attacker to access targeted vehicles from anywhere in the world. With the proliferation of the infrastructure mobility devices that attack the surface are expected to grow exponentially.

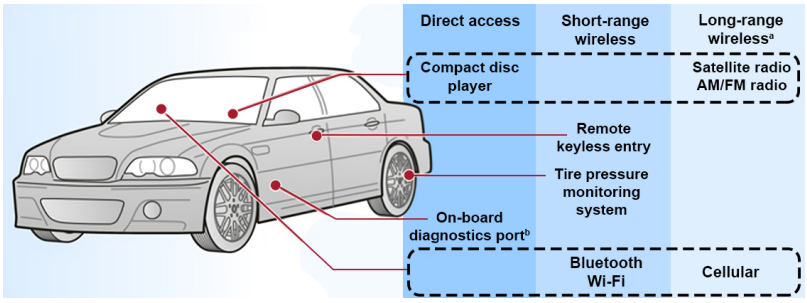

Figure 5. Hackers entry points. Source: US Government Accountability Office (GAO) [40].

[1]https://upstream.auto/research/automotive-cybersecurity/?id=null.

c) The Zero Trust Defense Strategy:

A report by the European Union Agency for Cybersecurity (ENISA) finds that self-driving vehicles are vulnerable to hacking because of the advanced computers they contain [47]. The ENISA report contains several recommendations, one of which is that security assessments of AI components be performed regularly throughout their lifecycle to ensure that AI models and vehicles always behave correctly when faced with unexpected situations or malicious attacks. The report also stresses that the automotive industry should embrace a *security-by-design* approach for the development and deployment of AI functionalities, where cybersecurity becomes the central element of digital design from the beginning. Zero Trust network architecture is another ENISA recommendation for any ICT development [48]. Zero Trust (ZT) was created because traditional security models operate on the outdated assumption that everything inside an organization's network should be implicitly trusted. In 2020, NIST defined it as "*a term for an evolving set of cybersecurity paradigms that move defenses from traditional static, network-based perimeters to focus on users, assets, and resources* [49]." It lays out a user-centric security vision as compared to its perimeter-focused predecessors. Rooted in the principle of "*never trust, always verify*," ZT is designed to protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing threat prevention, and simplifying granular, "least access" policies. But strictly speaking, all cybersecurity approaches in the state-of-the-art, including ZT remain policy-based [50] [51], and autonomous, unmonitored zero trust security by design that CCAM ideally requires, is virtually impossible [52].

2.2.2. Future of CCAM Cybersecurity in the Age of Quantum Computing

The non-linear exponential growth in QC has opened the possibility of threatening the PKI and hash functions in the near term [53]. Q-Day, the day when quantum computers can render all current encryption methods meaningless, is predicted to arrive sooner than one thinks [54], possibly as early as 2030 [55]. In fact, at least 6 companies have already started offering their current QC capabilities as commercial cloud services [20].

Quantum Computing (QC) is rapidly evolving as a new computing paradigm that utilizes quantum mechanics to solve complex problems faster than classical computers. As much as QC is a boon for research endeavors globally, it can also be deployed as a tool of destruction that adversaries can potentially exploit [56]. Because of its extraordinary computing speed, QC can easily decrypt today's encryption schemes to break the Internet [46]. Theoretically, all cryptographic algorithms are vulnerable to quantum attacks. QC with sufficient qubits capacity will be able to break nearly all modern public-key cryptographic systems, threatening an impending Quantum apocalypse [56] [57]. Any security risk to the Internet impacts CCAM and is also considered an existential risk to humanity [58] and needs to be mitigated with some urgency. Last year, the Cloud Security Alliance launched a countdown to Y2Q (years to quantum) that predicts just under six

years until QC can crack current encryption (**Figure 1**), while others think it might arrive earlier than that [54]. Before the QCs arrive with sufficient qubits, we must be ready with quantum-safe cryptographic algorithms, tools, techniques, & and deployment strategies to protect our ICT infrastructure. Post Quantum Cryptography (PQC) is being aggressively pursued worldwide to secure our cryptography-dependent digital infrastructure as recommended by NIST [59].

Two major NIST initiatives taken in recent years aimed at mitigating the cybersecurity crisis include:

i) *Post Quantum Cryptography* (*PQC*) *Standardization Project* [60],

ii) *Zero Trust Architecture* (*ZTA*) [48] [49].

These initiatives are also supported by the ENISA (EU cybersecurity agency) in its revised EU directive on the security of network and information systems (NIS2) [61]. The NIS2 Directive and the Cyber Resilience Act, seek to enhance IoT device security standards across the EU. A EuroQCI (European Quantum Communication Infrastructure) initiative was launched in 2019 [62]. The US Congress passed the Quantum Computing Cybersecurity Preparedness Act (H.R. 7535) in July 2022 [63], and on December 21, 2022, President Biden signed it into law [64]. The Act encourages "*federal government agencies to adopt technology that will protect against quantum computing attacks*." This marks a major milestone in the global effort to develop and deploy quantum-resilient cybersecurity. These legislations made the world move quickly against the coming QC threat since upgrading existing governmental and commercial cryptography infrastructure takes significant effort and years. This has accelerated the adoption of the *Zero Trust Architecture* in Europe and redefined the approach to cybersecurity [65]. In a recent RSA2023 event, experts suggested that PQC (Post Quantum Cryptography) will become a core part of IT infrastructure to extend *Zero Trust* to future QC [66]. If we don't do anything, the Internet as we know it now may simply cease to exist. These initiatives can significantly impact operators, distributors, and manufacturers of IoT devices, imposing fines or reporting requirements, marking a major milestone in the global effort to develop and deploy quantum-resilient cybersecurity, making the world move quickly against the coming QC threat since it takes significant effort and years to upgrade existing governmental and commercial cryptography infrastructure. However, these initiatives are facing implementation challenges.

In 2016 NIST published a report on the rising threat to encrypted Internet data by QC and the catastrophic impact that would have on the integrity of the global IT infrastructure [64]. In 2017 NIST launched an initiative to standardize PQC for real-world commercial use in securing our digital infrastructure from quantum threats [67]. However, all the currently available evidence indicates that it will be virtually impossible to defend against QC threats as the classical security primitives that vehicles support will eventually be compromised by quantum attacks because the hardware security modules of vehicles on the road cannot simply be disenrolled from the V2X system [68], At the same time, the strategy to simply

roll out new vehicles with only Post-Quantum Cryptography (PQC) support (once possible), while most vehicles on the road support only classical cryptography, is highly optimistic and likely impractical for two reasons:

Firstly, all the PQC algorithms selected for standardization by the NIST have so far failed [52].

Secondly, even if any PQC algorithm succeeds in sustaining quantum threats, it cannot be used in a plug-and-play manner with current V2X systems [68].

All of this means the cybersecurity of CCAM faces a catch-22 situation not envisaged when the CCAM goals were planned not considering the existential threat from QC and its impact on V2X communication [30].

2.3. Artificial Intelligence (AI): The Key Enabler of CCAM

The AI Act seeks to ensure a democratically legitimate, interdisciplinary, stakeholder-inclusive, and responsive approach to AI regulation, which can safeguard fundamental rights and anticipate, identify, and mitigate a broad spectrum of AI risks [69]. The existential threat to humanity from Artificial Intelligence (AI) [70] and its rapid industrialization is increasingly becoming a cause of concern because of its vulnerabilities and misuse by bad actors [58]. Experts warn of existential risk [58] and cyber warfare [71] from AI being greatly amplified by the development of QC. All types of autonomous mobility, whether surface-bound AVs, UAVs (Underwater autonomous vehicles), or airborne UAVs (unmanned aerial vehicles), in all modes of CCAM, entirely rely on the security, integrity, robustness, and ethical controllability of the AI systems deployed.

AI is not a monolithic term but a phenomenon that bears nuances that need to be seen through the lens of its evolutionary stages consisting of ANI (artificial narrow intelligence), AGI (artificial general intelligence), and ASI (artificial super intelligence) [72]. The use of the AI term in the paper implies inclusivity of its evolutionary stages.

2.4. 6G Telecommunication Network for CCAM

Along with QC and AI, production-grade 6G is also projected to be launched in the year 2030 [73] [74]. As we approach the QC era, the security threats to 6G networks from QC have become real. Harvest now and decrypt later attacks are already happening [75]. This will result in new challenges to achieving at least three of the eight 6G goals [75], as illustrated in **Figure 6** (highlighted in red-colored circles) and listed herein:

1) 1000 times lower cost compared to 5G [30],

2) Reliability Resilience, Security on account,

3) Very low latency.

Cryptography remains the mainstay of securing the Internet and the 6G networks. Post quantum cryptography (PQC) algorithms are currently under development and standardization by the NIST and other regulatory agencies. PQC deployment will make the 6G goals of very low latency and low cost almost unachievable, as most

PQC algorithms rely on keys much larger than those in classical RSA (Rivest, Shamir, and Adleman) algorithms. The large PQC keys consume more storage space and processing power, increasing the latency and costs of their implementation. Moreover, all the PQC candidates under NIST evaluation have so far failed [52], seriously jeopardizing their standardization and placing the security of 6G against the Q-Day threat in a catch-22 situation [30].

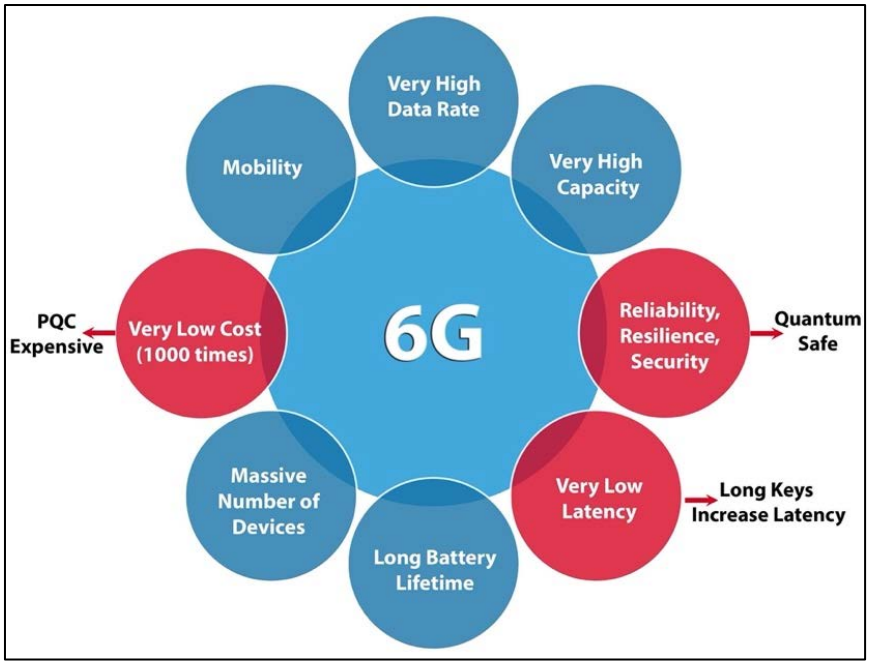

Figure 6. Impact of quantum computing on 6G networks. Source: Journal of Information Security, 15(3), 340-354.

2.5. Role of Policy and Regulatory Frameworks in Supporting CCAM

Effective policy and regulatory frameworks are essential for advancing Connected, Cooperative, and Automated Mobility (CCAM) systems. Collaboration among governments, manufacturers, and tech companies is crucial to creating a cohesive regulatory environment. Governments play a pivotal role in setting safety standards, data privacy laws, and ethical guidelines for autonomous vehicles (AVs), providing a predictable environment that encourages investment and innovation. Developing stringent safety standards covering performance, sensor reliability, cybersecurity, and emergency response is essential. Robust data protection laws are necessary to ensure secure data handling and user privacy, while transparent ethical frameworks must be established for decision-making in AV scenarios to reflect societal values.[2]

Collaboration is key to a cohesive regulatory environment. Public-private partnerships allow governments and private sector players to test technologies and

[2]https://assets.publishing.service.gov.uk/media/62ff438c8fa8f504cdec92df/cam-2025-realising-benefits-self-driving-vehicles.pdf.

refine regulations through joint AV projects. Participation in standardization bodies like ISO and SAE helps develop universal technical standards. Joint research and development initiatives accelerate technological advancements and address challenges. Continuous dialogue through forums and working groups enables stakeholders to adapt regulations to emerging issues.

Public trust is crucial for the successful deployment of AVs. Clear communication about AV benefits and risks through public awareness campaigns is vital. Demonstration projects and pilot programs help familiarize the public with AV technology, reducing skepticism. Proactively addressing concerns such as job displacement ensures the equitable distribution of AV benefits.

A well-coordinated regulatory environment that addresses safety, ethical, and societal challenges is key to the successful implementation of CCAM. Collaboration among governments, manufacturers, and tech companies, along with public-private partnerships, standardized regulations, and continuous engagement, will pave the way for the widespread adoption of autonomous mobility solutions.

2.6. Case Studies on Autonomous Vehicle Implementations

Successful examples and case studies illustrate the progress towards achieving 100% vehicle connectivity through autonomous vehicle (AV) trials. These examples highlight potential benefits such as enhanced safety, reduced emissions, and improved traffic management, all in alignment with the European Commission's Vision 2050 goals.

In Amsterdam, trials with autonomous shuttles and delivery vehicles have proven pivotal [76]. These AVs, equipped with technology for full connectivity with traffic signals and infrastructure, help optimize traffic flow and reduce congestion, contributing valuable data for sustainable urban mobility. Similarly, Barcelona has integrated AVs into its public transport system, aiming to reduce congestion and emissions while enhancing efficiency [77]. These AVs communicate with traffic lights and infrastructure, ensuring smooth traffic management and aligning with Vision 2050 objectives for sustainable urban transport. Germany has also launched several pilot projects focusing on automated driving in urban areas.[3] These projects assess the safety and efficiency of AVs in mixed-traffic environments, providing critical data to develop future regulations and standards. The trials demonstrate robust connectivity and communication capabilities essential for integrating AVs into existing traffic systems.

Despite these advancements, several challenges remain. Sensor reliability is a major issue, as current technologies can be affected by adverse weather conditions. Ethical concerns in decision-making algorithms, particularly in life-and-death situations, require transparent development and societal input. Additionally, public acceptance of AV technology is critical. Overcoming skepticism involves rigorous testing, transparent reporting, and public engagement to build trust and understanding.

[3]https://www.eict.de/en/projects.

3. Gaps in CCAM Research

After identifying the gaps in CCAM research it is pertinent to design solutions or at least propose directions that CCAM researchers can take to fill these gaps.

3.1. CCAM Taxonomy

AVs represent a significant departure from conventional road transport. Much of the CCAM research focuses on the capabilities of an AV in terms of the technology onboard but a vehicle's surroundings play an equally important part. Infrastructure is a crucial part of the operating environment of any AV that determines where and how it can operate. The infrastructure comprises physical infrastructures, such as roads, traffic signs, and signals, as well as the invisible digital infrastructure. Creating special-purpose physical infrastructure solely for the use of AVs is impossible because of the prohibitory costs and time constraints. At present, there is limited incentive to invest in physical upgrades to the road network because there is limited evidence on what makes a road "good" for AVs, as technology is still evolving. Moreover, there are no standards available for designing or refitting roads for the benefit of AVs. Hence, creating vehicles capable of working on the existing physical road network is a better strategy [78]. But there is a better case for developing the "invisible infrastructures" of digital connectivity, data, and institutional capacity on which AVs will rely, such as V2X connectivity, availability and reliability of high-definition maps, the availability of live data on road infrastructure, including all traffic regulations and establish data standards, architectures for applicable digital infrastructures for improving AV's ODD (Operational Design Domain) modeling.

3.1.1. The Invisible Infrastructure

It is the invisible infrastructure support to the connectedness of the vehicles and the relative awareness of their peers and their navigational paths that's key to CCAM. It is the shared collective intelligence of the participating vehicles that makes the traffic collision-free and autonomous. If it is the collective intelligence of the moving vehicles that makes the traffic autonomous, it must be generated, compiled, interpreted, and disseminated amongst all the participating vehicles in real-time by an autonomous traffic management system (ATMS). Such ATMS must not only provide networkability but establish robust vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or collectively V2X (vehicle-to-everything) connectivity to achieve collision-free navigation through dense, dynamic traffic of participating vehicles. The future of AVs will depend on how well that interaction can be managed. Thus, the major showstopper is not the availability of AV, but the lack of supporting digital infrastructure. The disconnect between the participating vehicles and the non-existent ATMS makes any level of autonomous traffic impossible.

3.1.2. SAE J 3016 Taxonomy Criticism

Although CCAM is a multidisciplinary research field, it is mostly dominated by

AV stakeholders, keeping the research AV-centered. Even the SAE taxonomy for "*levels of driving automation*" is AV-centered, without all levels being classified from the perspective of a vehicle. The vehicle-centricity of SAE J3016 is understandable coming from a professional society of automotive engineers that's dominated by automotive industry stakeholders and does not include adequate representation from the traffic regulators, mobility infrastructure builders, and intelligent transportation managers. Consequently, autonomous mobility has seen the total absence of Road and Transport Authorities (RTAs) as stakeholders when their role is so crucial that no vehicle can be on the road without their approval in the first place. The term closest to an RTA in SAE and FAME projects is "road operator," which is too narrow to incorporate the essential functions of licensing and regulating the mobility of vehicles in any jurisdiction[4]. No vehicle in any jurisdiction can become roadworthy unless approved by RTA.

The impact of any scientific statement is not solely determined by its intrinsic merit or efforts but largely by the collective response and interactions of a broader community, which includes both supporters and dissenters [79]. We noticed this inadequacy while scanning through the EU-funded CCAM projects to find the gaps in CCAM research and design a future-ready, quantum-safe, AI-powered CCAM infrastructure that revolved around the RTA as a principal stakeholder. We are not the only ones to point out the fallacy. There are other researchers who believe that the "SAE levels have served their purpose, but they now look inadequate to the task of informing future discussions," and should turn outward toward environments [80]. Hopkins & Schwanen show how SAE taxonomy contributes to a narrow conceptualization of automated futures not allowing for more nuanced spatial and temporal understandings of future systems [81]. They further conclude that they would have drawn similar conclusions if BASt (Germany) and NHTSA (US) standards had become the de facto global standard. Some other authors opine that 'SAE J3016 implies an "all or nothing" approach for the human operation of the driving task' [82], and SAE taxonomy "does not fully consider the infrastructure support required for each level," and propose a supplementation to the SAE taxonomy [83] [84].

However, ignoring the onboarding of RTA as the key CCAM stakeholder, and

[4]"Infrastructure" is more than the physical road. The digital and data components that support automation are just as important, and the legal and institutional frameworks governing and managing their use are also critical. Surprisingly the SAE International taxonomy does not define the most important mobility stakeholder, viz. government authorities who license motor vehicles for their roadworthiness. No AV can be on the road without regulatory approval from the respective government. The term "road operator" in SAE (https://www.sae.org/standards/content/j3216_202107/) or SAE-inspired FAME project taxonomy (https://taxonomy.connectedautomateddriving.eu/road-operator/) neither incorporates all the nuances that CCAM implementation entails, nor a fair representation of the regulatory authority that authorizes the vehicles to operate on the roads. At best it may represent an agency that builds the roadside infrastructure, such as road facilities, signages, markings, and service stations, or software vendors for the operation, control, and maintenance of communication networks. In many jurisdictions, a motor vehicle registry that licenses the vehicles for roadworthiness operates separately from a public works department that builds, supports and maintains the roadway infrastructure and the law enforcement department that enforces law and order.

with the much inconspicuous dissent, SAE's 6 levels of automation have become a cornerstone and de facto gold standard of CCAM research. The vehicle-centric development of CCAM on its own will not take us to the zero-fatality goals without involving the road and transport infrastructure and its controlling stakeholder—the road traffic authorities (TRAs). It is therefore imperative to introduce another level of automation that enables the development of an autonomous traffic management system (ATMS).

3.1.3. Time to Update CCAM Taxonomy to Include the Infrastructure Automation

A review of the criticism of the SAE J3016 Taxonomy for levels of driving automation makes it clear that all the criticism arises from the SAE classification being too AV-centric with inadequate representation of the role of infrastructure in the autonomous mobility taxonomy [80]-[84]. As elaborated later in this discussion, this deficiency is also perceived by the Commission-funded INFRAMIX project that proposed a five-sublevel supplement to the SAE taxonomy to address the deficiency of infrastructure underrepresentation.

Given the pace of developments in AI, 6G, and quantum computing (QC), the enabling technologies most relevant for the CCAM extravehicular infrastructure, onboarding RTAs for boosting the infrastructure-focused development of CCAM is long overdue. Better late than never, this report is an attempt to fill the gap. As SAE levels have become the gold standard for autonomous mobility taxonomy, simply staying closer to that standard contextually and visually makes more sense than the complex approaches suggested by other authors [81]-[84]. Not disturbing the existing SAE levels, and adding another level of infrastructure automation that incorporates autonomous traffic as the seventh level should serve the purpose. As illustrated in **Figure 7**, the new proposed "*Levels of Automated Mobility for CCAM*," adds level 7 to the CCAM development roadmap by inducting autonomous traffic management infrastructure. This new taxonomy splits CCAM development into Autonomous Vehicle Research and Autonomous Traffic Research and draws up a roadmap to Vision 2050 based on the ERTRAC CCAM Roadmap, which provides the position of an independent European Technology Platform, aiming at drawing an overall long-term picture together with the next steps for realistic use cases (**Figure 8**).

INFRAMIX, an EC-funded project reinforces the fact that SAE taxonomy is indeed vehicle-centric and ignores infrastructure development. It defines Levels of Infrastructure Support for Automated Driving (ISAD) as a general way of classifying available roadway infrastructure features that could affect the ODD constraints of CAD (connected autonomous driving) systems [85]. These levels aim to classify and harmonize the capabilities of a road infrastructure to support AVs. The rationale for proposing this classification scheme is to find a mechanism to augment the limitations of environmental perception of AV onboard sensors with the numerous traffic and environmental sensors already present in the road infrastructure. In anticipation of this, information shortage on the vehicle side can be

compensated by information provided by the road infrastructure. Moreover, as these levels can be assigned to parts of the road network, they can give automated vehicles and their operators guidance on what the INFRAMIX project calls "readiness" of the road network for CAD system deployment. National projects such as AUTOMOTO have further elaborated on the attributes of ISAD infrastructure support levels [86]. **Figure 9** illustrates a roadmap with the proposed levels of automated mobility integrated with ISAD infrastructure classification developed by the INFRAMIX project.

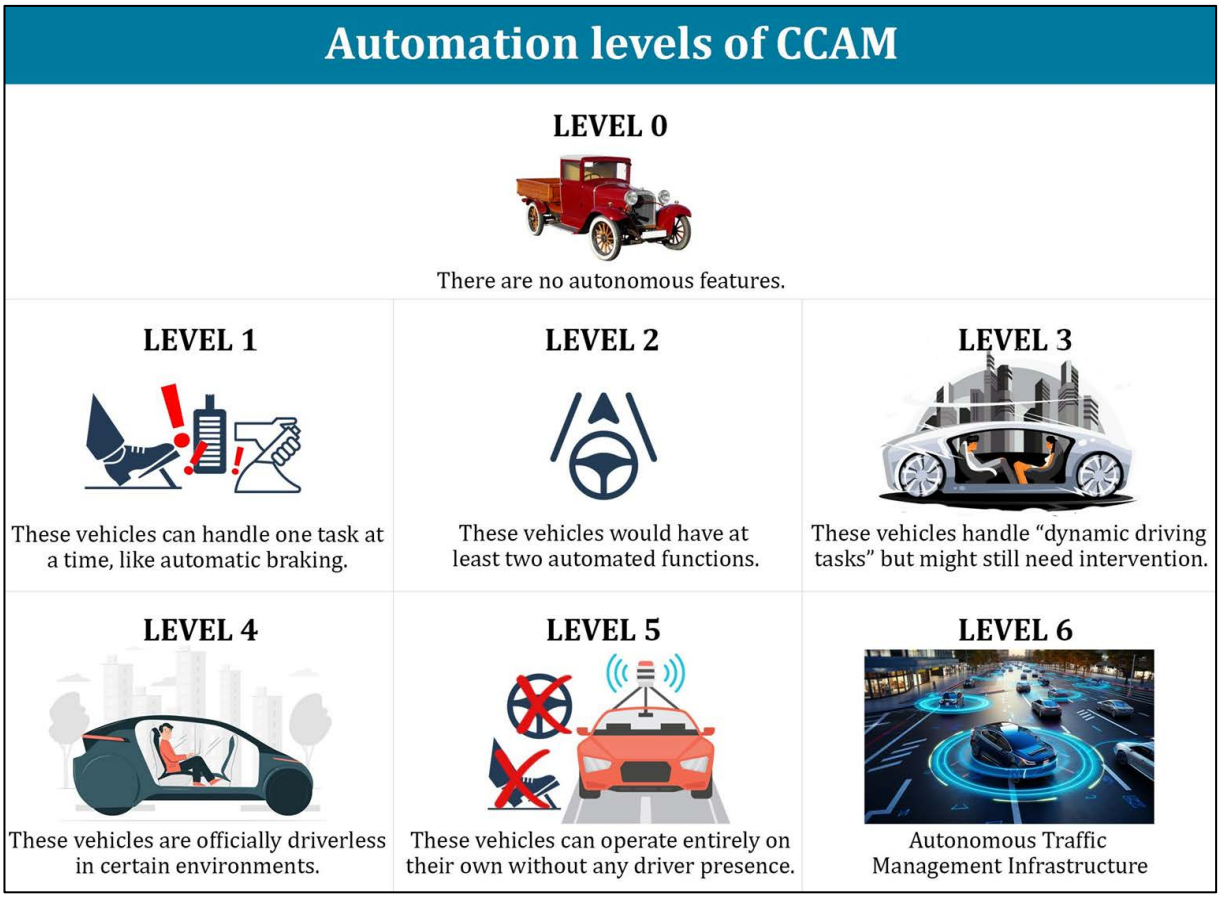

Figure 7. Levels of automated mobility for CCAM.

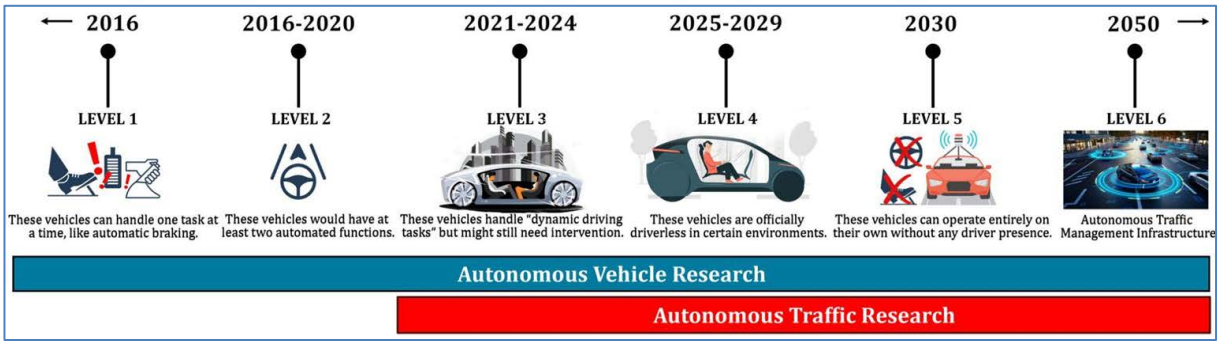

Figure 8. Timeline to vision 2050 with new levels of automated mobility for CCAM.

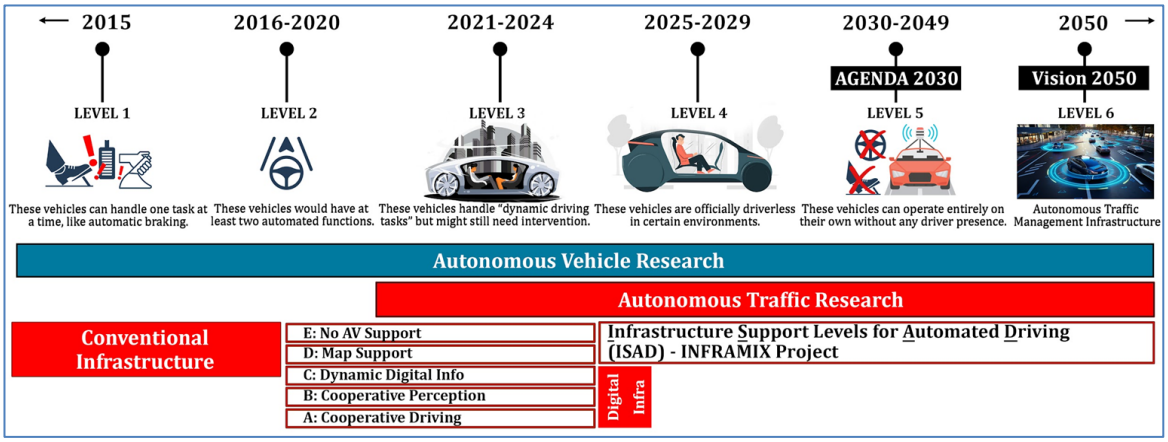

Figure 9. Vision 2050 timeline with levels of automated mobility integrated with ISAD infrastructure taxonomy [x].

3.2. CCAM Cybersecurity: Mitigating the Q-Day Challenge

Life without computers is unimaginable, and so is a computing device without third-party permissions or inherent vulnerabilities [30] [42] [52] [56] [58] [74] [87]-[89]. These permissions make computers usable but introduce vulnerabilities that make them a soft target for cybercriminals. Legacy computing devices or for that matter CCAM devices cannot be built without third-party permissions, which, on the one hand, makes the device usable with accessibility to a diverse range of applications, but on the other hand, allows bad actors to exploit those permissions creating vulnerabilities. Hence, all computers are inherently vulnerable, and the attack surface is the necessary evil that we must live with. ZVC is an award-winning cybersecurity paradigm [89] that challenges the status quo to design future computers that can revolutionize conventional cryptography-dependent cybersecurity. It is encryption agnostic and therefore inherently resistant to QC.

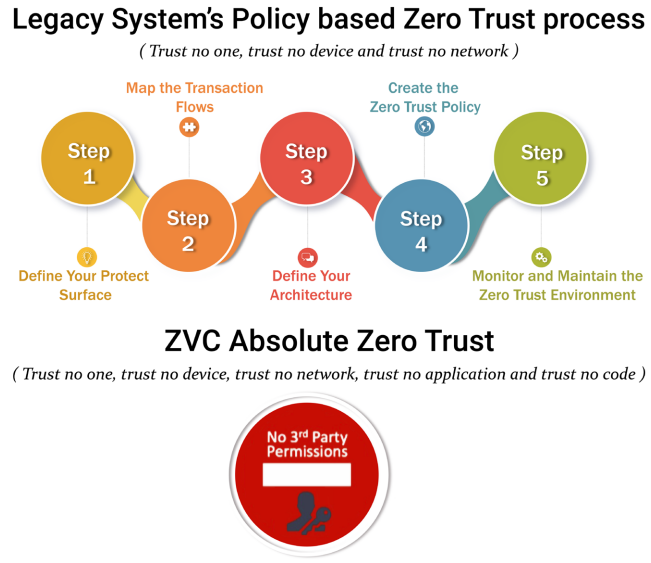

Figure 10. 5-step legacy zt process vs autonomous AZT. Source: Journal of Computer & Communications 12(3): 252-282.

3.2.1. Zero Trust Is Not Absolute or Autonomous

As discussed in Section 2.2.1c all regulators (NIST and ENISA) recommend Zero Trust Architecture for securing any digital infrastructure. In legacy computing environments, trust itself is a vulnerability and should be eliminated, like all vulnerabilities [90]. Hype surrounds any new concept or phenomenon, as is the case with "ZTA" (Zero Trust Architecture). Michael, *et al*. claim that the concept of ZTA is currently a moving target, and developing and sustaining ZTA is essentially impossible [50]. Some experts consider Zero Trust as a misnomer [91]. When a good majority of cybersecurity experts believe ZTA itself is impossible or illusive [92], the legitimacy of research reports claiming ZTA by design is, at best, questionable. Moreover, implementing the legacy zero-trust strategy is a multi-step process that entails defining the protection surface, mapping the transaction flows, defining the relevant architecture, creating the zero-trust policy, and monitoring and maintaining the zero-trust environment (**Figure 10**). Integrating all these steps into ZTA by design at the build-time is impossible as these conditions change during the runtime according to the prevailing circumstances and require continuous monitoring by a dedicated team. Therefore, "Absolute Zero Trust" (AZT) by design was impossible in the prior art because its complex policy implementation could not run autonomously 24/7 without human intervention [51] [52].

3.2.2. The Autonomous Absolute Zero Trust (AZT) Architecture

A recent report extends the concept of ZT beyond "*trust no one*, *trust no device and trust no network*," to "*trust no application and trust no code*" (**Figure 10**). The legacy ZT implementation remains a policy-based strategy or model and not a product, while AZT is a product that delivers autonomous security by design coded into the program at build time without the need to define or continuously monitor policies. **Figure 11** illustrates an AZT framework powered by ZVC, AI, and blockchain. We recently described a Quantum-safe Ledger Technology (QLT), a blockchain framework that is resilient to Q-Day threats [93]. As we will see in the next section AI is decentralized with QLT blockchain. As third-party permissions are banned, only authorized users can enter the AZT network through the V2X gateway. The AZT network is owned and operated by RTA to run the ATMS (autonomous traffic management system). Since the V2X router is the gateway to the AZT network and a single point of entry to the AZT network, all handshakes with peers for access to the network components including the participating vehicles' CAN bus should be authenticated at the V2X gateway device. It is therefore imperative that both the V2X components of the CCAM infrastructure, the RSU (roadside unit) and the OBU (onboard unit), are controlled and operated by the RTA. Although OBU V2X comes built into the AV, the RTA can mandate a plug-and-play V2X device at the time of AV registration. Compliance with this mandate ensures that the onboard security of AV is not compromised through CAN bus hacks (**Figure 11**).

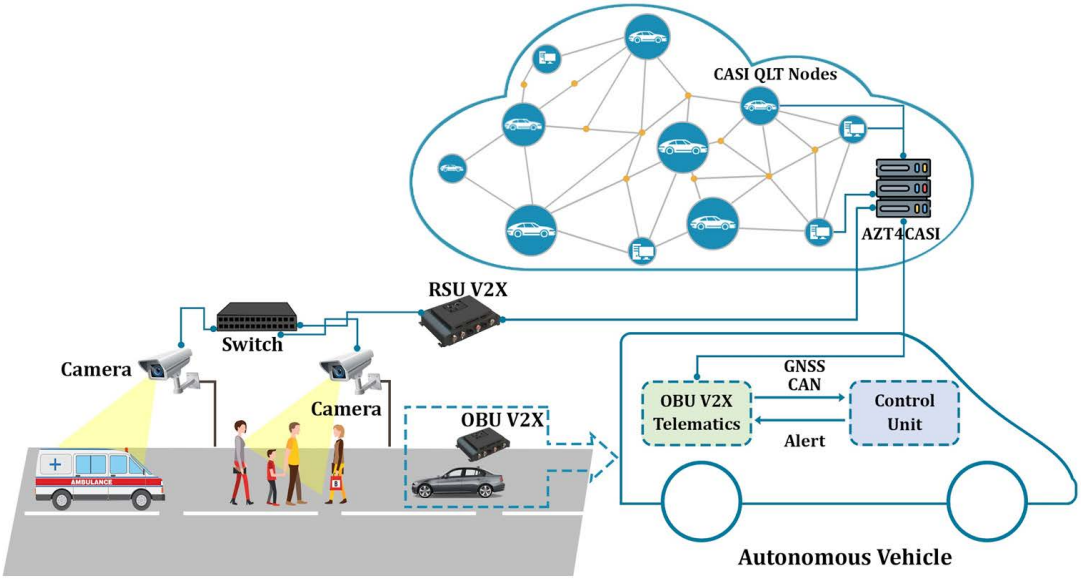

Figure 11. The absolute zero trust (AZT) architecture for CCAM powered with ZVC, AI, and wechain.

3.3. CCAM Intelligence: Taming the AI with Collective Artificial Super Intelligence (CASI)

AI is a key enabler of CCAM. As discussed in Sections 2(iii) and 3.3, AI runs the risk of existential risk to humans if it goes into rogue hands and becomes unstoppable. This is essentially routed in two inherent mandatory and uncircumventable rules of computing that render computers vulnerable. A recent report tested the following hypothesis [94].

"*Safe, secure, ethical, and controllable AGI/QC is possible by conquering the two unassailable rules of computability with Collective Artificial Super Intelligence* (*CASI*)."

These rules are:

i) Third-party permissions, which we discussed in the preceding section.

ii) Whether a specific Turing machine should halt or run infinitely is undecidable. Termed "*the Halting Problem*" [95], this phenomenon renders AI/AGI unstoppable and uncontainable if it goes rogue [96].

These rules are paradoxical and sort of necessary evils that cannot be circumvented in prior art (**Figure 12**).

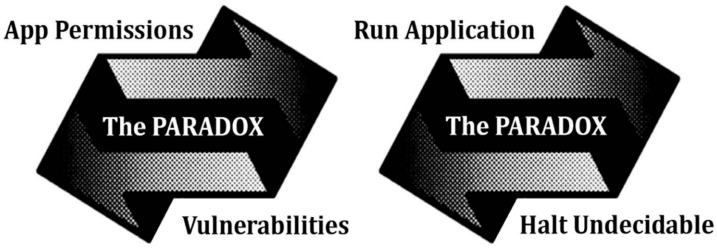

Figure 12. The permissions paradox and the halting problem paradox. Source credit: Intelligent Information Management, 16(3), 121-146 [94].

3.3.1. Solving the Halting Problem with Blockchain

Alfonseca *et al.* argue that total containment of superintelligence is principally impossible due to the fundamental limits inherent to the theory of computing itself [98]. However, we discovered that blockchain's smart contract can solve the halting problem in any of the two unconventional ways [94].

i) Smart Contract Fee Restriction: Smart contracts offer transparent, tamperproof, and cost-effective alternatives to traditional contracts. Miners/validators of blockchain transactions spend resources to validate and record each transaction on the blockchain, which costs are recovered as transaction fees. A miner/validator will terminate the script if it runs out of funds. Thus, blockchain can indirectly address the halting problem by introducing the concept of gas (transaction fee) restriction. Any unethical decision by smart contract transaction can be stopped by fee restriction by diving all ML actions into two types:

- routine, no-fee ML actions pre-approved by the DAO (decentralized autonomous organization) that governs the blockchain;
- All new suspect ML actions require fee-based smart contract authentication, wherein the DAO controls such fee remittance.

ii) Non-Turing Complete Smart Contract: Conventional smart contracts are coded in a Turing complete programming language. Recent evidence suggests that smart contracts can also be efficiently coded using a non-Turing complete language [97]. Vyper is a non-Turing complete programming language that does not face the halting problem, and smart contracts coded in Vyper are more efficient in terms of performance speed, storage, and eliminating certain classes of bugs [98]. This means a CASI smart contract coded in a non-Turing language can automatically stop anytime the ML detects an unethical anti-human action [94].

3.3.2. Decentralized Machine Learning for a Democratic and Ethical AI

The decentralized cyber secure AZT framework of CASI provisions a Federated Machine Learning (FML) architecture to distribute ML/DL across layers of devices (**Figure 13**). Such a decentralized training model deploys the QLT blockchain framework [93] and overcomes the shortcomings of the conventional centralized learning, which is prone to single point failure and has serious privacy and security issues, besides being slower and resource intensive compared to a system distributed across several nodes. Thus, the AZT infrastructure federates ML models across all the layers of the AZT cloud continuum infrastructure laying a foundation for a complete computing continuum that's capable of federating infrastructures, programming applications, and services, composing dynamic workflows and most importantly democratizing the decision options (**Figure 13**). Because of its network architecture that redistributes resources across all the layers, AZT powered CASI ecosystem is resilient, energy-efficient and capable of efficiently reacting in real-time to unpredictable data sizes, availability, locations, and data transmission rates. This will also provide application developers with greater control over network, computing, and data infrastructures and services,

and the end-user will benefit from seamless access to continuous service environments.

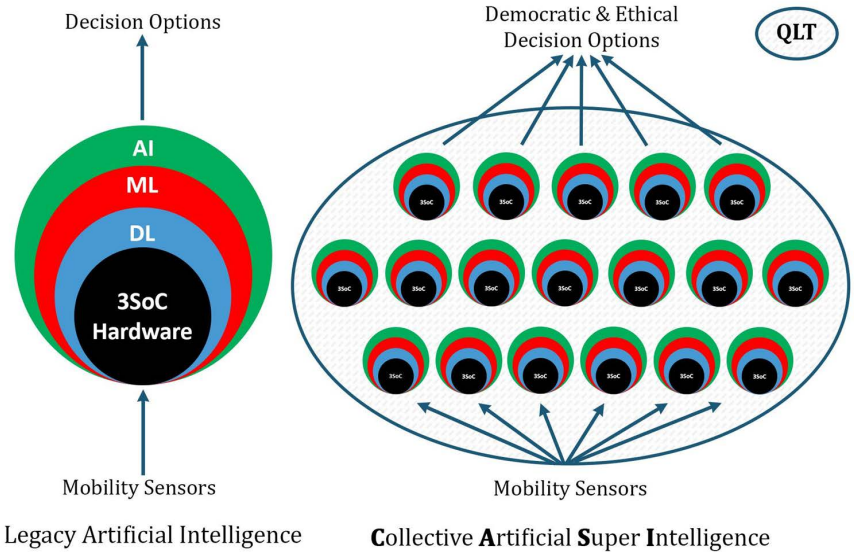

Figure 13. Machine learning & deep learning: Legacy AI vs Collective Artificial Super Intelligence (CASI).

3.4. Security of Future 6G C-V2X Networks with AZT

While the debate on the choice of technology for V2X between DSRC (Dedicated Short-Range Communication) and cellular network (C-V2X) goes on in Europe, Aziz *et al.* [99] recently demonstrated that future use cases of autonomous driving will require both technologies to be used in coordination. For connecting drivers, pedestrians, and road infrastructure C-V2X is crucial. State-of-the-art multi-wireless standard devices employ individual modules for different technologies. When a vehicle is equipped with DSRC technology, the location, heading, and speed are broadcast 10 times per second. Although a still to premier, 6G technology is expected to provide a data collection speed of up to 1,000GB per second (100 times faster than 5G), with a capacity to service 10 million devices per square kilometer (compared to 1 million devices with 5G) [100]. Although DSRC can efficiently enable short-distance communications, DSRC alone cannot support the entire CCAM digital infrastructure. C-V2X with 6G will become indispensable in the future.

Cryptography remains the mainstay of securing the Internet and the 6G networks. As discussed in previous sections, PQC (Post quantum cryptography) algorithms are currently being developed and standardized by the NIST (National Institute of Standards and Technology) and other regulatory agencies. PQC deployment will make the 6G goals of very low latency and low cost almost unachievable, as most PQC algorithms rely on keys much larger size than those in classical RSA algorithms that are deployed today. Because of its file size, the PQC keys consume more storage space and processing power, increasing the latency

and costs of their implementation resulting in compromising the desired latency and pricing goals of 6G networks. Moreover, all the PQC candidates under NIST evaluation have so far failed [52], seriously jeopardizing their standardization and placing the security of 6G against the Q-Day threat in a catch-22 situation [30].

Research on 6G networks currently faces a catch-22 situation [30], perhaps not envisaged when the 6G targeted parameter goals were planned [101] [102]. However, as we approach the QC era, the security threats to 6G networks from QC have become real [103], resulting in new challenges in achieving at least three of the eight 6G goals, as illustrated in **Figure 6** in Section 3.4:

- 1000 times lower cost compared to 5G [30] [102],
- Reliability Resilience, Security on account,
- Very low latency.

PQC is the only defense currently explored by researchers and regulatory authorities to secure the Internet from the Q-Day threat. There is no plan B in case PQCs fail, and the current evidence indeed suggests exactly that [30]. Although computer security heavily relies on cryptography, recent evidence indicates it can transcend beyond encryption by deploying ZVC (Zero Vulnerability Computing) technology [93]. A series of recent reports disclose a novel ZVC-based way to deal with the impending Q-Day threat [30] [42] [52] [56] [87] [88] [93] [94]. Such AZT (Absolute Zero Trust) is encryption agnostic and, therefore inherently quantum resistant (**Figure 14**). It is also light, energy-efficient, fast, and low-cost as it does not rely on the resource-intensive PQC. While conventional Zero Trust, per se, is policy-based and not autonomous, Absolute Zero Trust (AZT) security architecture is a seamless and self-governing framework that runs continuously and autonomously without the need for monitoring the network and delivers autonomous quantum-safe security to 6G networks, guaranteeing their latency and price reduction goals [30].

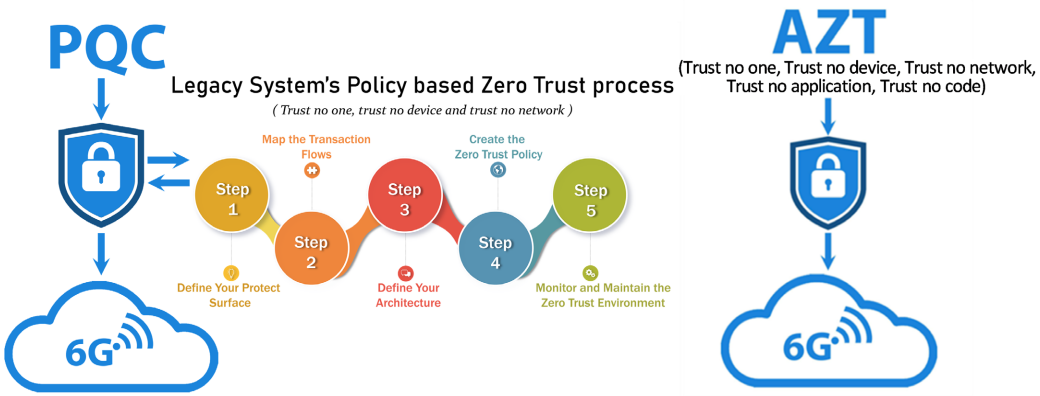

Figure 14. Policy based Legacy Zero Trust (ZT) vs Autonomous Absolute Zero Trust (AZT). Source: Journal of Information Security, 15(3), 340-354.

4. Summary, Limitations of the Study, and Recommendations

We summarize the study outcome with a visual infographic representation of the

CCAM landscape, point out the limitations, and list the detailed recommendations with the objective and outcome of each recommendation.

4.1. Bird's Eye View of the CCAM Development Landscape

We try to summarize the overall CCAM development scene with a bird's eye view of the autonomous mobility landscape with the help of a CCAM development wheel (Figure 15). The CCAM wheel has V2X as its hub connecting four pillars of autonomous mobility that constitute the rim:

1) Avs.
2) Mobility Infrastructure.
3) Quantum-Safe Cybersecurity.
4) ATMS.

V2X Gateway is the hub of the wheel that connects to the rim via the following spokes:

1) AZT for security of AVs.
2) Cellular (6G) + DSRC for network connectivity.
3) CASI/FML for ATMS.
4) AZT for cybersecurity.

Because most CCAM research is AV-centered, it predominantly remains focused around the first two spokes of the CCAM development wheel, while the latter two (ATMS & Cybersecurity) remain under-rated and underfunded.

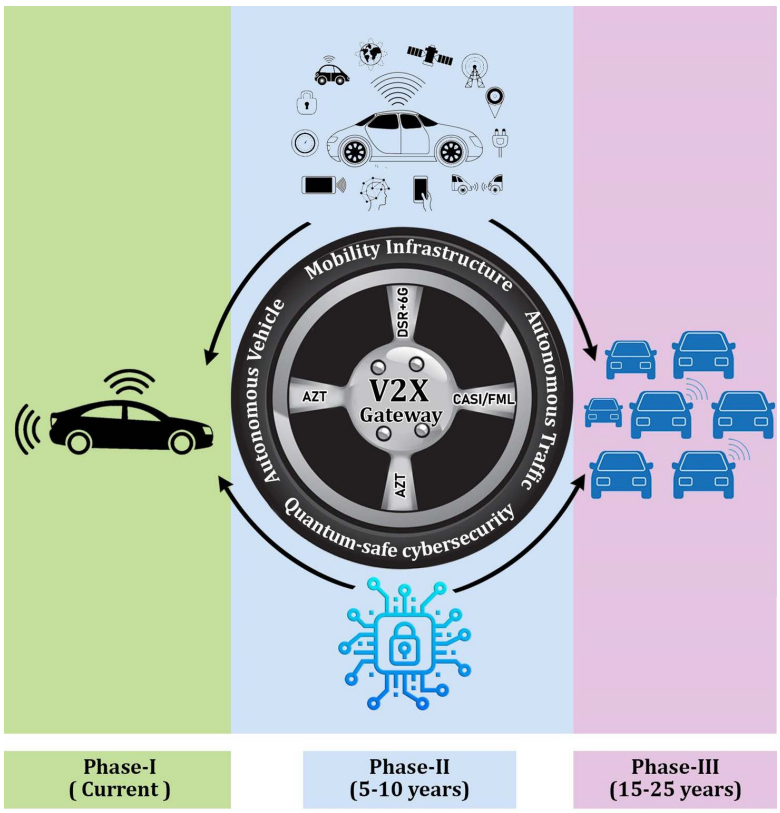

Figure 15. Bird's eye view of the CCAM development wheel.

This proposal focuses on building a robust V2X gateway as the hub that first provides universal connectivity to all vehicles irrespective of whether they are AVs or not, and subsequently operates as a future substrate that supports all the components of the CCAM to be plugged in, as and when they reach maturity to roll the wheel of autonomous mobility. The V2X gateway, if owned and operated by the RTA (road transport authorities) as a plug-n-play accessory to modern vehicles, has substantial present-day utility in making today's road and transport operations more efficient, and can also serve as a hub for facilitating the transition to the autonomous mobility of the future.

4.2. Limitations of the Study

Autonomous mobility is a vast space facing many challenges that are beyond the scope of this article. Since the study specifically focuses on the gaps in the current CCAM initiatives funded by the European Commission the findings are limited to the research gaps identified and predicted for future development and providing a little more clarity to the CCAM roadmap. Predicting the future and drawing roadmaps can never be an exact science. Nevertheless, prediction is central to the process of science and fundamental to scientific methods [104]. Scientists test their ideas and theories by comparing theoretical predictions to actual observations in the real world or their laboratories. Predictions are also important for policymakers. Autonomous mobility has faced some difficulties that have faltered some of the early predictions. For example, Agrawal *et al.* [105] reviewed timeline predictions made by public and private sector stakeholders and concluded that none of the AV-predicted timelines have been met so far and that public stakeholder predictions were more conservative than the private stakeholders.

We believe the EU's Vision Zero cannot be realized within the defined timeline unless the identified gaps are addressed with priority. The principal objective of this research was not to make any predictions about the future of CCAM. It is to make our perspective available to a broader community of CCAM researchers for testing and building on the concepts that we put forth, as we pursue our own journey through CCAM. This report is no more than hypothesis-supporting research intended to build a new direction that researchers worldwide can pursue with experiments and field trials to test and prove or disprove the novelty enshrined in this study. Until such studies are conducted, great care should be taken to extrapolate the findings of this report to real-world settings.

4.3. Recommendations for Future CCAM Research

1) Enhance Infrastructure Focus in CCAM Development

Objective: Strengthen infrastructure's role in autonomous mobility preferably by engaging RTA.

Actions:

✓ Implement advanced digital infrastructure (high-definition maps, V2X gateway).

- ✓ Assess and upgrade current infrastructure.
- ✓ Conduct pilot projects with V2X connectivity.

Outcome: Improved V2X connectivity for safer, more efficient traffic management.

2) Implement Quantum-Safe Cybersecurity Measures

Objective: Protect CCAM systems from quantum computing threats.

Actions:

- ✓ Integrate post-quantum cryptography (PQC) or an alternate Q-Day security approach.
- ✓ Develop an autonomous Zero Trust quantum-safe cybersecurity framework.
- ✓ Collaborate with cybersecurity experts.

Outcome: Resilient CCAM infrastructure against quantum threats.

3) Establish an Ethical, Democratic, and Controllable AI Framework

Objective: Ensure safe and ethical AI in CCAM.

Actions:

- ✓ Develop guidelines for transparency, accountability, and fairness.
- ✓ Implement decentralized collective AI systems (exploring blockchain).
- ✓ Foster collaboration among AI stakeholders.

Outcome: Trustworthy AI systems enhancing CCAM safety and efficiency.

4) Facilitate the Integration of quantum-safe 6G Telecommunication Technology

Objective: Leverage 6G for enhanced CCAM performance and security.

Actions:

- ✓ Conduct research and pilot projects for 6G applications.
- ✓ Develop quantum-safe 6G security protocols.
- ✓ Collaborate with telecom providers.

Outcome: Improved CCAM networking capabilities with secure 6G networks.

5) Update and Expand SAE CCAM Taxonomy

Objective: Create a comprehensive infrastructure-focused CCAM taxonomy.

Actions:

- ✓ Revise SAE J3016 to include infrastructure automation.
- ✓ Develop a framework for vehicle-infrastructure interaction.
- ✓ Use visual aids to illustrate the updated taxonomy.

Outcome: Holistic taxonomy supporting both AVs and infrastructure development.

6) Foster Collaboration with Road and Transport Authorities (RTAs)

Objective: Engage RTAs as key CCAM stakeholders and V2X operators.

Actions:

- ✓ Establish communication channels between RTAs, policymakers, and technology providers.
- ✓ Develop joint initiatives and pilot projects with RTAs, wherein RTAs own and operate the V2X Gateway.
- ✓ Provide training for RTAs on CCAM systems.

Outcome: Enhanced collaboration for effective CCAM infrastructure implementation.

7) Conduct Targeted Pilot Projects

Objective: Test and validate CCAM solutions in controlled environments.

Actions:

✓ Select confined areas and highway locations for initial pilot projects.
✓ Implement and monitor advanced infrastructure and AI systems.
✓ Gather data and feedback for refinement.

Outcome: Validated CCAM solutions ready for broader and more complex implementations.

8) Advocate for Harmonized Policy and Regulatory Frameworks

Objective: Supportive regulatory environment for CCAM.

Actions:

✓ Develop standardized regulations for CCAM technologies.
✓ Address regulatory challenges and propose solutions.
✓ Promote international collaboration for harmonized policies.

Outcome: Consistent regulatory framework encouraging CCAM innovation and deployment.

5. Conclusions

In conclusion, this paper has highlighted critical gaps in current CCAM research and emphasized the necessity of integrating a robust infrastructure focus alongside vehicle-centric advancements. The proposed expansion of the SAE taxonomy to include infrastructure automation is crucial for realizing the full potential of autonomous mobility. By addressing the quantum computing threat, reinforcing AI ethics and control, and preparing for the integration of 6G networks, this research outlines a comprehensive approach to developing a quantum-safe CCAM ecosystem.

The review of EU-funded CCAM projects underscores the importance of a cooperative strategy involving Road and Transport Authorities (RTAs) to achieve the European Commission's Vision 2050 goals of zero fatalities, zero emissions, and sustainable mobility. As we move towards these ambitious goals, it is imperative to prioritize the development of digital infrastructures that move towards 100% vehicle connectivity and real-time data sharing. Future research should focus on refining these proposed frameworks, implementing quantum-safe cybersecurity measures, and continuously monitoring the evolution of AI to prevent existential threats. By fostering collaboration among stakeholders and leveraging cutting-edge technologies, we can accelerate the progress toward a safer, more efficient, and sustainable transportation future. The findings and recommendations presented in this paper aim to guide researchers, policymakers, and industry stakeholders in their efforts to advance CCAM development, ensuring that the technological innovations are secure, ethical, and aligned with long-term mobility goals.

Acknowledgment

The authors are grateful to Sadiya Khan for her assistance in preparing this manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Edvardsson Björnberg, K. (2022) Vision Zero and Other Road Safety Targets. In: Edvardsson Björnberg, K., Belin, M.Å., Hansson, S.O. and Tingvall, C., Eds., *The Vision Zero Handbook*, Springer, 1-27. https://doi.org/10.1007/978-3-030-23176-7_1-1

[2] WHO (2023) Road Traffic Injuries. WHO Newsroom. https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[3] Chen, S., Kuhn, M., Prettner, K. and Bloom, D.E. (2019) The Global Macroeconomic Burden of Road Injuries: Estimates and Projections for 166 Countries. *The Lancet Planetary Health*, **3**, e390-e398. https://doi.org/10.1016/s2542-5196(19)30170-6

[4] European Commission (2011) Roadmap to a Single European Transport Area—Toward a Competitive and Resource-Efficient Transport System. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0144

[5] Novat, N., Kidando, E., Kutela, B. and Kitali, A.E. (2023) A Comparative Study of Collision Types between Automated and Conventional Vehicles Using Bayesian Probabilistic Inferences. *Journal of Safety Research*, **84**, 251-260. https://doi.org/10.1016/j.jsr.2022.11.001

[6] Almaskati, D., Kermanshachi, S. and Pamidimukkala, A. (2024) Investigating the Impacts of Autonomous Vehicles on Crash Severity and Traffic Safety. *Frontiers in Built Environment*, **10**, Article 1383144. https://doi.org/10.3389/fbuil.2024.1383144

[7] Liu, Q., Wang, X., Wu, X., Glaser, Y. and He, L. (2021) Crash Comparison of Autonomous and Conventional Vehicles Using Pre-Crash Scenario Typology. *Accident Analysis & Prevention*, **159**, Article ID: 106281. https://doi.org/10.1016/j.aap.2021.106281

[8] Petrović, Đ., Mijailović, R. and Pešić, D. (2020) Traffic Accidents with Autonomous Vehicles: Type of Collisions, Manoeuvres and Errors of Conventional Vehicles' Drivers. *Transportation Research Procedia*, **45**, 161-168. https://doi.org/10.1016/j.trpro.2020.03.003

[9] Vaillant, L., Eyssartier, C., Douet, M., Dewailly, B., Cavagnet-to, N., *et al.* (2022) Initial Target Vision for Multimodal Traffic Management Ecosystem: ORCHESTRA Project Deliverable: D2.1—Version 1.1. D2.1—V1.1, European Commission—DG Research. https://hal.science/hal-04029880/file/D2.1%20Initial%20target%20vision%20-%20H2020%20ORCHESTRA.pdf

[10] Wachsmuth, J., *et al.* (2022). The European Commission's 2050 Vision "A Clean Planet for All"—Implications for Sector Strategies and Climate Governance. Ressortforschungsplan of the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection. https://www.umweltbundesamt.de/sites/default/files/medien/479/publikationen/cc_17-2022_the_european_commissions_2050_vision.pdf

[11] Garrote, P.A. (2020) Towards Cooperative, Connected, and Autonomous Mobility: Contributions of Horizon Europe Projects Managed by CINEA. https://www.ccam.eu/wp-content/uploads/2023/05/HE-CCAM-2023_brochure-web-FIN.pdf

[12] Yoshizawa, T., Singelée, D., Muehlberg, J.T., Delbruel, S., Taherkordi, A., Hughes, D., *et al.* (2023) A Survey of Security and Privacy Issues in V2X Communication Systems. *ACM Computing Surveys*, **55**, 1-36. https://doi.org/10.1145/3558052

[13] Benyahya, M., Kechagia, S., Collen, A. and Nijdam, N.A. (2022) The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis. *Applied Sciences*, **12**, Article 4413. https://doi.org/10.3390/app12094413

[14] Garrod, D. (2024) Final Approval of Ground-Breaking EU AI Act. https://www.akingump.com/en/insights/alerts/final-approval-of-ground-breaking-eu-ai-act

[15] Gaitanidou, E., Bekiaris, E. and Loukea, M. (2022) Automation User Acceptance Creation Path Roadmap. https://www.drive2thefuture.eu/wp-content/uploads/2023/01/D8.6-Automation-User-Acceptance-creation-path-roadmap.pdf

[16] Huttner, B. and Kalsi, M. (2022) Countdown to Y2Q: Working Group, Quantum-Safe Security. Cloud Security Alliance. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

[17] Maheshwari, A., *et al.* (2023) Is Quantum Computing a Cybersecurity Threat? In: Rawat, R., *et al.*, Eds., *Quantum Computing in Cybersecurity*, Wiley, 353-368. https://doi.org/10.1002/9781394167401.ch21

[18] Majot, A. and Yampolskiy, R. (2015) Global Catastrophic Risk and Security Implications of Quantum Computers. *Futures*, **72**, 17-26. https://doi.org/10.1016/j.futures.2015.02.006

[19] Kim, J., Min, D., Cho, J., Jeong, H., Byun, I., Choi, J., *et al.* (2024). A Fault-Tolerant Million Qubit-Scale Distributed Quantum Computer. *Proceedings of the* 29*th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, *Volume* 2, La Jolla, 27 April-1 May 2024, 1-19. https://doi.org/10.1145/3620665.3640388

[20] Scott III, F. (2021) A Buyer's Guide to Quantum as a Service: Qubits for Hire. https://www.zdnet.com/article/a-buyers-guide-to-quantum-as-a-service-qubits-for-hire/

[21] Xu, D., Yu, K., Liu, L., Chen, G., Kumar, N., Guizani, M., *et al.* (2024) Post-quantum Authentication against Cyber-Physical Attacks in V2X-Based Autonomous Vehicle Platoon. *IEEE Transactions on Intelligent Transportation Systems*, **25**, 5034-5044. https://doi.org/10.1109/tits.2023.3339787

[22] Wippelhauser, A., Edelmayer, A. and Bokor, L. (2023) A Declarative Application Framework for Evaluating Advanced V2x-Based ADAS Solutions. *Applied Sciences*, **13**, Article 1392. https://doi.org/10.3390/app13031392

[23] Bubeck, S., *et al.* (2023) Sparks of Artificial General Intelligence: Early Experiments with GPT-4. arXiv: 2303.12712.

[24] Blake, A. (2023) GPT-5 Could Change the World in One Incredible Way. Digital Trends. https://www.digitaltrends.com/computing/gpt-5-artificial-general-intelligence/

[25] Clarke, L. (2023) Call for AI Pause Highlights Potential Dangers. *Science*, **380**, 120-121. https://doi.org/10.1126/science.adi2240

[26] Sala, M. (2023) Conjecture Internal Survey: AGI Timelines and Probability of Human Extinction from Advanced AI. LESSWRONG. https://www.lesswrong.com/posts/kygEPBDrGGoM8rz9a/conjecture-internal-survey-agi-timelines-and-probability-of

[27] Liu, G., Huang, Y., Li, N., Dong, J., Jin, J., Wang, Q., *et al.* (2020) Vision, Requirements and Network Architecture of 6G Mobile Network Beyond 2030. *China Communications*, **17**, 92-104. https://doi.org/10.23919/jcc.2020.09.008

[28] Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Röning, J., *et al.* (2020). 6G White Paper: Research Challenges for Trust, Security and Privacy. arXiv: 2004.11665.

[29] Growiec, J. (2024) Existential Risk from Transformative AI: An Economic Perspective. *Technological and Economic Development of Economy*, 1-27. https://doi.org/10.3846/tede.2024.21525

[30] Raheman, F. (2024) Formulating and Supporting a Hypothesis to Address a Catch-22 Situation in 6G Communication Networks. *Journal of Information Security*, **15**, 340-354. https://doi.org/10.4236/jis.2024.153020

[31] Bellan, R. (2022) Local Motors, the Startup behind the Olli Autonomous Shuttle, Has Shut Down. TechCrunch. https://techcrunch.com/2022/01/13/local-motors-the-startup-that-created-the-olli-autonomous-shuttle-has-shutdown/

[32] Azevado, M.A. (2020) Self-Driving Truck Startup Starsky Robotics Shuts Down after Series B Falls through. Crunchbase. https://news.crunchbase.com/venture/self-driving-truck-startup-starsky-robotics-shuts-down-after-series-b-falls-through/

[33] Korosec, K. (2019) Apple Acquires Self-Driving Startup Drive AI on the Brink of Closure. TechCrunch. https://techcrunch.com/2019/06/25/self-driving-startup-drive-ai-is-closing-down/

[34] McCarty Carino, M. (2021) Lyft, Uber Back away from Autonomous Cars. https://www.marketplace.org/2021/05/04/lyft-uber-back-away-from-autonomous-cars/

[35] European Commission (2020) Framework for Coordination Automated Mobility in Europe. https://cordis.europa.eu/project/id/101069898

[36] European Commission (2017) Road Infrastructure Ready for Mixed vehicle flows. https://cordis.europa.eu/project/id/723016

[37] SAE (2018) Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. https://www.sae.org/standards/content/j3016_201806/

[38] Malik, S. and Sun, W. (2020). Analysis and Simulation of Cyber Attacks against Connected and Autonomous Vehicles. 2020 *International Conference on Connected and Autonomous Driving* (*MetroCAD*), Detroit, 27-28 February 2020, 62-70. https://doi.org/10.1109/metrocad48866.2020.00018

[39] USGA Office (2016) Vehicle Cybersecurity: DOT and Industry Have Ef-forts under Way, but DOT Needs to Define Its Role in Responding to a Real-World Attack. GAO-16-350. https://www.gao.gov/products/GAO-16-350

[40] Litman, T. (2020) Autonomous Vehicle Implementation Prediction: Implications for Transport Planning. Victoria Transport Planning Institute. https://nationalcenterformobilitymanagement.org/wp-content/uploads/2020/03/avip.pdf

[41] Wise, D. (016) Vehicle Cybersecurity: DOT and Industry Have Efforts under Way but DOT Needs to Define Its Role in Responding to a Real-World Attack. https://www.gao.gov/products/GAO-16-350

[42] Raheman, F. (2024) Harvesting, Tokenizing, and Sharing the Influence of Planetary Abundance to Mitigate the Global Debt Catastrophe. *Theoretical Economics Letters*, **14**, 125-163. https://doi.org/10.4236/tel.2024.141008

[43] Weber, S., Kaufman, D., Thomas, D. and Cohn, A. (2019) Cybersecurity Futures 2025 Insights and Findings. Center for Long-Term Cybersecurity, University of Berkley.

[44] Fleck, A. (2022) Cybercrime Expected to Skyrocket in Coming Years. Statista. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[45] Kavipriya (2024) Upstream Release 2024 Automotive Cybersecurity Report. Telematics Wire. https://www.telematicswire.net/upstream-releases-2024-automotive-cybersecurity-report/

[46] Grimes, R.A. (2019) Cryptography Apocalypsee: Preparing for the Day When Quantum Computing Breaks Today's Crypto. Wiley. https://doi.org/10.1002/9781119618232

[47] Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A., and Sanchez, I. (2021) Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving, EUR 30568 EN. Publications Office of the European Union, Luxembourg.

[48] Smoljić, M. (2024) European Union Directives, National Regulations, and Zero Trust Network Architecture. 2024 47*th MIPRO ICT and Electronics Convention* (*MIPRO*), Opatija, 20-24 May 2024, 1496-1501. https://doi.org/10.1109/mipro60963.2024.10569809

[49] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

[50] Michael, J.B., Dinolt, G.C., Cohen, F.B. and Wijesekera, D. (2022) Can You Trust Zero Trust? *Computer*, **55**, 103-105. https://doi.org/10.1109/mc.2022.3178813

[51] Horne, D. and Nair, S. (2021) Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.S. and Tinetti, F.G., Eds., *Advances in Security, Networks, and Internet of Things*, Springer, 512-525.

[52] Raheman, F. (2024) From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. *Journal of Computer and Communications*, **12**, 252-282. https://doi.org/10.4236/jcc.2024.123016

[53] Fernandez-Carames, T.M. and Fraga-Lamas, P. (2020) Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, **8**, 21091-21116. https://doi.org/10.1109/access.2020.2968985

[54] Ford, P. (2023) The Quantum Cybersecurity Threat May Arrive Sooner than You Think. *Computer*, **56**, 134-136. https://doi.org/10.1109/mc.2022.3227657

[55] Křelina, M. (2022) Quantum Technology in Future Warfare: What Is on the Horzon? Future Warfare and Technology: Issues and Strategies. *Global Policy Journal*, **1**, Article 107.

[56] Raheman, F. (2022) The Future of Cybersecurity in the Age of Quantum Computers.

Future Internet, **14**, Article 335. https://doi.org/10.3390/fi14110335

[57] Sharma, S. and Harjani, M. (2022) Rethinking the 'Quantum Apocalypse'. RSIS Commentaries.

[58] Schiffer, B.F. (2022) Quantum Computers as an Amplifier for Existential Risk. arXiv: 2205.02761

[59] Szymanski, T.H. (2022) The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IOT). *IEEE Access*, **10**, 45893-45930. https://doi.org/10.1109/access.2022.3169137

[60] Chen, Lily, *et al.* (2016). Report on Post-Quantum Cryptography. Vol. 12. US Department of Commerce, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

[61] Nyári, N. (2021) The Impact of Quantum Computing on IT Security. B*iztonságtudományi Szemle*, **3**, 25-37.

[62] Ribezzo, D., Zahidy, M., Vagniluca, I., Biagi, N., Francesconi, S., Occhipinti, T., *et al.* (2022) Deploying an Inter-european Quantum Network. *Advanced Quantum Technologies*, **6**, Article ID: 2200061. https://doi.org/10.1002/qute.202200061

[63] Lin, H. (2023) The Mother of All Data Breaches: Quantum Computing Holds New Promises and Dangers. Such Devices Could Overturn Our Whole Cybersecurity Regime, Revealing Not Just Mountains of Data but Secrets from Years Past. *Hoover Digest*, **1**, 79-83.

[64] Sanzeri, S. (2023) What the Quantum Computing Cybersecurity Preparedness Act Means for National Security. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/

[65] Olufon, T. (2023) Zero Trust Comes into the Mainstream in Europe. Forrester. https://www.forrester.com/report/zero-trust-comes-into-the-mainstream-in-europe/RES178958

[66] Columbus, L. (2023) How Post Quantum Cryptography Will Help Fulfil the Vision of Zero Trust. Venture Beat. https://venturebeat.com/security/how-post-quantum-cryptography-will-help-fulfill-the-vision-of-zero-trust/

[67] Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q. and Smith-Tone, D. (2019) Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. US Department of Commerce, National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303

[68] Bindel, N., Twardokus, G., McCarthy, S., & Rahbari, H. (2023) Drive (Quantum) Safe!—Towards PQ Authentication for V2V Communications. https://core.ac.uk/download/pdf/579859961.pdf

[69] Cantero Gamito, M. and Marsden, C.T. (2024) Artificial Intelligence Co-Regulation? the Role of Standards in the EU AI Act. *International Journal of Law and Information Technology*, **32**, eaae011. https://doi.org/10.1093/ijlit/eaae011

[70] Peters, M.A., Jackson, L., Papastephanou, M., Jandrić, P., Lazaroiu, G., Evers, C.W., *et al.* (2023) AI and the Future of Humanity: ChatGPT-4, Philosophy and Education—Critical Responses. *Educational Philosophy and Theory*, **56**, 828-862. https://doi.org/10.1080/00131857.2023.2213437

[71] Kline, K., Salvo, M. and Johnson, D. (2019) How Artificial Intelligence and Quantum Computing Are Evolving Cyber Warfare. Cyber Intelligence Initiative, The Institute

of World Politics.

[72] Kuusi, O. and Heinonen, S. (2022) Scenarios from Artificial Narrow Intelligence to Artificial General Intelligence—Reviewing the Results of the International Work/Technology 2050 Study. *World Futures Review*, **14**, 65-79. https://doi.org/10.1177/19467567221101637

[73] Aslam, A.M., Chaudhary, R., Bhardwaj, A., Budhiraja, I., Kumar, N. and Zeadally, S. (2023) Metaverse for 6G and Beyond: The Next Revolution and Deployment Challenges. *IEEE Internet of Things Magazine*, **6**, 32-39. https://doi.org/10.1109/iotm.001.2200248

[74] Tariq, F., Khandaker, M.R.A., Wong, K., Imran, M.A., Bennis, M. and Debbah, M. (2020) A Speculative Study on 6g. *IEEE Wireless Communications*, **27**, 118-125. https://doi.org/10.1109/mwc.001.1900488

[75] McGowran, L. (2022) Quantum Apocalypse: Experts Warn of 'Harvest Now, Decrypt Later' Hacks. Silicon Republic. https://www.siliconrepublic.com/enterprise/quantum-apocalypse-store-now-decrypt-later-encryption

[76] Benson, T., Duarte, F. and Ratti, C. (2022) From Amsterdam to New Amsterdam to Amsterdam: How Urban Mobility Shapes Cities. In: Chokhachian, A., Hensel, M.U. and Perini, K., Eds., *Informed Urban Environments*, Springer, 109-124. https://doi.org/10.1007/978-3-031-03803-7_7

[77] Pazos-Otón, M. (2024) The End of the Car City in Spain. In: Lois-González, R.C. and Rio Fernandes, J.A., Eds., *Urban Change in the Iberian Peninsula*, Springer, 275-290. https://doi.org/10.1007/978-3-031-59679-7_18

[78] Dries, M., Russ, M., Pilli-Sihvola, E. and Joaquin-Acosta, A. (2023) Preparing Infrastructure for Automated Vehicles. https://www.itf-oecd.org/sites/default/files/docs/preparing-infrastructure-automated-vehicles.pdf

[79] Latour, B. (1987) Science in Action: How to Follow Scientists and Engineers through Society. Harvard University Press.

[80] Stayton, E. and Stilgoe, J. (2020) It's Time to Rethink Levels of Automation for Self-Driving Vehicles [Opinion]. *IEEE Technology and Society Magazine*, **39**, 13-19. https://doi.org/10.1109/mts.2020.3012315

[81] Hopkins, D. and Schwanen, T. (2021) Talking about Automated Vehicles: What Do Levels of Automation Do? *Technology in Society*, **64**, Article ID: 101488. https://doi.org/10.1016/j.techsoc.2020.101488

[82] Steckhan, L., Spiessl, W., Quetschlich, N. and Bengler, K. (2022) Beyond SAE J3016: New Design Spaces for Human-Centered Driving Automation. In: Krömker, H., Eds., *HCI in Mobility, Transport, and Automotive Systems*, Springer, 416-434. https://doi.org/10.1007/978-3-031-04987-3_28

[83] Chen, S., Zong, S., Chen, T., Huang, Z., Chen, Y. and Labi, S. (2023) A Taxonomy for Autonomous Vehicles Considering Ambient Road Infrastructure. *Sustainability*, **15**, Article 11258. https://doi.org/10.3390/su151411258

[84] Inagaki, T. and Sheridan, T.B. (2018) A Critique of the SAE Conditional Driving Automation Definition, and Analyses of Options for Improvement. *Cognition, Technology & Work*, **21**, 569-578. https://doi.org/10.1007/s10111-018-0471-5

[85] Inframix (2022) Infrastructure Categorization—Inframix EU Project. https://www.inframix.eu/infrastructure-categorization/

[86] Khastgir, S., Vreeswijk, J., Shladover, S., Kulmala, R., Alkim, T., Wijbenga, A., *et al.*

(2023) Distributed ODD Awareness for Connected and Automated Driving. *Transportation Research Procedia*, **72**, 3118-3125. https://doi.org/10.1016/j.trpro.2023.11.874

[87] Raheman, F., Bhagat, T., Vermeulen, B. and Van Daele, P. (2022) Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet*, **14**, Article 238. https://doi.org/10.3390/fi14080238

[88] Raheman, F. (2024) Defining Quantum Advantage for Building a Sustainable MVP to Deliver Quantum Computing Services. *Open Journal of Applied Sciences*, **14**, 1530-1549. https://doi.org/10.4236/ojapps.2024.146102

[89] European Commission, Horizon Europe (2023) Zero Vulnerability Computing (ZVC): A New Paradigm. Seal of Excellence. https://zvchub.com/#seal

[90] Campbell, M. (2020) Beyond Zero Trust: Trust Is a Vulnerability. *Computer*, **53**, 110-113. https://doi.org/10.1109/mc.2020.3011081

[91] Georgsen, R.E. and Køien, G.M. (2022) Serious Games with SysML: Gamifying Threat Modelling in a Small Business Setting. *INCOSE International Symposium*, **32**, 119-132. https://doi.org/10.1002/iis2.12902

[92] Whitmore, T. (2022) The Elusive Promise of (and Maddening Obstacles to Implementing) a Cloud Zero Trust Architecture. Frost & Sullivan. https://www.frost.com/frost-perspectives/elusive-promise-and-obstacles-to-cloud-zero-trust-architecture/

[93] Raheman, F. (2024) Futureproofing Blockchain & Cryptocurrencies against Growing Vulnerabilities & Q-Day Threat with Quantum-Safe Ledger Technology (QLT). *Journal of Computer and Communications*, **12**, 59-77. https://doi.org/10.4236/jcc.2024.127005

[94] Raheman, F. (2024) Tackling the Existential Threats from Quantum Computers and AI. *Intelligent Information Management*, **16**, 121-146. https://doi.org/10.4236/iim.2024.163008

[95] Strachey, C. (1965) An Impossible Program. *The Computer Journal*, **7**, 313-313. https://doi.org/10.1093/comjnl/7.4.313

[96] Alfonseca, M., Cebrian, M., Fernandez Anta, A., Coviello, L., Abeliuk, A. and Rahwan, I. (2021) Superintelligence Cannot Be Contained: Lessons from Computability Theory. *Journal of Artificial Intelligence Research*, **70**, 65-76. https://doi.org/10.1613/jair.1.12202

[97] Jansen, M., Hdhili, F., Gouiaa, R. and Qasem, Z. (2019) Do Smart Contract Languages Need to Be Turing Complete? In: Prieto, J., Das, A., Ferretti, S., Pinto, A. and Corchado, J., Eds., *Blockchain and Applications*, Springer, 19-26. https://doi.org/10.1007/978-3-030-23813-1_3

[98] Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R., *et al.* (2021) A Comprehensive Survey on Smart Contract Construction and Execution: Paradigms, Tools, and Systems. *Patterns*, **2**, Article ID: 100179. https://doi.org/10.1016/j.patter.2020.100179

[99] Aziz, D., Bohm, C. and Hurley, F. (2021) Enabling 5G and DSRC V2X in Autonomous Driving Vehicles. Analog Devices Inc. https://resource.itbusinesstoday.com/whitepapers/18937-Analog-Devices-4.pdf

[100] Tim Fisher (2024) 6G: What It Is? & When to Expect It? https://www.lifewire.com/6g-wireless-4685524

[101] Bertin, E., Crespi, N. and Magedanz, T. (2021) Shaping Future 6G Networks: Needs, Impacts, and Technologies. John Wiley & Sons.

[102] Zhang, S., Xiang, C. and Xu, S. (2020) 6G: Connecting Everything by 1000 Times

Price Reduction. *IEEE Open Journal of Vehicular Technology*, **1**, 107-115. https://doi.org/10.1109/ojvt.2020.2980003

[103] Ulitzsch, V.Q., Park, S., Marzougui, S. and Seifert, J. (2022). A Post-Quantum Secure Subscription Concealed Identifier for 6g. *Proceedings of the* 15*th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, San Antonio, 16-19 May 2022, 157-168. https://doi.org/10.1145/3507657.3528540

[104] Sarewitz, D. and Pielke, R. (1999) Prediction in Science and Policy. *Technology in Society*, **21**, 121-133. https://doi.org/10.1016/s0160-791x(99)00002-0

[105] Agrawal, S., Schuster, A.M., Britt, N., Mack, E.A., Tidwell, M.L. and Cotten, S.R. (2023) Building on the Past to Help Prepare the Workforce for the Future with Automated Vehicles: A Systematic Review of Automated Passenger Vehicle Deployment Timelines. *Technology in Society*, **72**, Article ID: 102186. https://doi.org/10.1016/j.techsoc.2022.102186