An Enhanced Threat Analysis and Risk Assessment for Connected and Automated Vehicles Unifying upon Security and Privacy Standards

Benyahya, Meriem

This publication URL: https://archive-ouverte.unige.ch//unige:178971

Publication DOI: 10.13097/archive-ouverte/unige:178971

AN ENHANCED THREAT ANALYSIS AND RISK ASSESSMENT FOR CONNECTED AND AUTOMATED VEHICLES UNIFYING UPON SECURTIY AND PRIVACY STANDARDS

Une évaluation innovante des menaces et des risques, dédiée aux véhicules connectés et automatisés, unifiant les normes de cybersécurité et de protection des données à caractère personnel

THESIS
submitted to the
Geneva School of Economics and Management,
University of Geneva, Switzerland,

by
Meriem BENYAHYA

Under the direction of

Prof. Dimitri KONSTANTAS, supervisor

Dr Niels Alexandre NIJDAM, co-supervisor

Dr Anastasija COLLEN, co-supervisor

in fulfillment of the requirements for the degree of

Docteur ès économie et management
mention *systèmes d'information*

Jury members:

Prof. Thomas STRAUB, Chair, University of Geneva
M. Eric SILVA, ROSAS
Dr Eduardo SOLANA, University of Geneva

Thesis no 146
Geneva, July 2024

La Faculté d’économie et de management, sur préavis du jury, a autorisé l’impression de la présente thèse, sans entendre, par-là, émettre aucune opinion sur les propositions qui s’y trouvent énoncées et qui n’engagent que la responsabilité de leur auteur.

Genève, le 3 juillet 2024

Dean
Markus MENZ

Impression d’après le manuscrit de l’auteur

Dedicated to the memory of my grandmother, and to my mother,
along with all Moroccan women who aspired to higher education.

À la mémoire de ma grand-mère, et en dédicace à ma mère ainsi
qu’à toutes les femmes marocaines, qui ont rêvé, sans pouvoir
accéder à l’enseignement supérieur.

لذكرى جدتي، ولأمي، ولجميع النساء المغربيات اللاتي طمحن بالالتحاق الى التعليم
العالي.

Acknowledgements

I express my gratitude to my supervisors Dr. Anastasija COLLEN, Dr. Niels A. NIJDAM and Prof. Dimitri KONSTANTAS who assisted me with endless guidance, trust and an exceptional working environment. I feel privileged for all the insightful recommendations they proposed from research, and technological to career planning perspectives. I extend my thanks to the jury members, Prof. Thomas STRAUB, Dr. Eduardo SOLANA and Mr. Eric SILVA for providing valuable feedback which enhanced the overall quality of the present thesis. I am very thankful also to all partners, from Horizon projects (AVENUE, SHOW, and ULTIMO), particularly to Melisa FAZLIC and Jeroen BEUKERS from Transport Publique Genevois as well as Jonathan PECLAT from LOXO, for sharing equipment and expertise which supported the related implementations within this research.

I am profoundly grateful to my husband, Ali JAAKIK, for encouraging me throughout my academic journey, undertaking family duties on my behalf, listening to my brainstorming despite being from a different field of expertise and strengthening my motivation during challenging moments. To my children, Joumana and Sharif, who have shown understanding beyond their ages, thank you for being the source of my determination. Special thanks to my grandmother, who, unfortunately, departed at the moment of this thesis' elaboration. Her perseverance, patience and simplicity virtues have been notably inspiring during my pathway. I sincerely thank my parents and my family-in law who stood by me and believed on me.

I could not have reached this academic milestone without esteemed colleagues and friends. I thank my lab-mate Teri LENARD for all the positive vibes and productive discussions which definitely supported in pushing my research works forward. I thank my great friends around the world: Lamia BERRADA, Mikiko BORGHI, Kathy CAHUENAS SANDOVAL, Daria SUPRINOVIC CRNA OBRVA, Iris GAUDRA and Isabelle KELLEDJIAN who patiently tracked my progress and publications.

Geneva, July 2024
Meriem BENYAHYA

Abstract

Protecting Connected and Automated Vehicles (CAVs) from cyber attacks and data breaches is one of the main challenges facing the deployment of driverless vehicles nowadays. The CAV embedding cutting edge sensors, advanced Electronic Control Units (ECUs), innovative artificial intelligence (AI) components, and connection to everything, has the potential to beneficially change the transport dimensions in the near future. Six levels, varying from L0 (no automation) to L5 (fully automated), were predefined by the Society of Automotive Engineering (SAE) [385]. To assure the CAV's highly autonomous navigation of SAE L4 and L5, the vehicle intelligently compiles inputs from both its internal (including cameras and sensors) and endless external connections to the Intelligence Transport System (ITS) infrastructure as well as to end-users. However, such high automation, complex in-vehicle components and ubiquitous connectivity impose the CAV to inherit cybersecurity and data privacy challenges and open up caveats for security assessments.

Both literature and industry have witnessed potential attacks that can dramatically impact the CAV's acceptance and jeopardise its passengers' safety and privacy. The recorded attacks vary from taking control over the braking and the steering systems [330], tracking passengers' locations and identities [304], to blinding the vehicle sensors and leading to a crash [462]. In light of the growing need to shield the CAV's ecosystem, Threat Analysis and Risk Assessment (TARA) is considered, by the core regulations and standards, as the efficient way to keep systems at an acceptable level of risk [114]. While numerous TARA versions are available, they are not-ready-to-use methods, do not sufficiently tackle the properties of L4 and L5 CAVs and do not consider data privacy threats at the forefront of secure CAV's implementation.

In this thesis, and within the frame of ULTIMO [89]- the Horizon Europe project, we propose and showcase an improved TARA methodology, named TARA 2.0. This endeavour involves thorough investigations aiming to identify the enhancement avenues across three research pillars: cybersecurity, data privacy and regulations & standards. For this purpose, a holistic view of existing cybersecurity and data privacy threats as well as their related regulation and standardisation requirements were put forward. Based on this knowledge, the gaps and shortcomings of the key legislation publications were spotlighted. Furthermore, we conducted a systematic study on recent TARA methodologies and simulated the most prominent standard to determine their limitations in adequately modelling CAV's threats and compiling their related risks. These efforts led to the development of TARA 2.0, which was implemented and validated through a proof of concept.

The results showed that our framework incorporates fine-grained analysis of data privacy threats as well as the CAV's automation level throughout the assessment

process. Additionally, our findings indicate a strong promise that, in the context of expert-dependent assessments, TARA 2.0 enhances objectivity by transparently addressing the experts involvement within the assessment. Moreover, while the proposed solution offers a step-by-step guide for future replications to internal or external assessors, it servers as a significant reference point for any academic researcher, policymakers, smart cities operators, data controllers and service provider aiming to integrate CAVs into their respective landscapes.

Résumé

Les Véhicules Connectés et Automatisés (CAV) sont perçus comme le nouvel horizon du transport intelligent, fiable et autonome. Néanmoins, les cyberattaques et les violations de données à caractère personnelles qui en découlent, representent un obstacle majeur à leur déploiement à grande échelle. Les CAV sont équipés de capteurs de pointe, des caméras embarquées de haute définition, des unités de commandes électroniques (ECU) avancées ainsi que des composants intelligence artificielle (AI) innovants. Ils bénéficient également d'une connectivité étendue avec des systèmes externes (infrastructure, cloud, d'autres véhicles, utilisateurs finaux..). Cependant, cette technologie avancée, qui permet une navigation indépentente des interventions humaines, représente également une source de menaces et de cyberattaques, exigeant des évaluations de sécurité très rigoureux.

Durant la dernière décénie, l'industrie automotive a été témoins de potentielles attaques, allant de la prise de contrôle des systèmes de freinage, au suivi de localisation malveillant, à l'aveuglement des capteurs du véhicule. Les conséquences de ces attaques se sont accentuées par la réduction des interventions humaines, notament sur les CAV hautement automatisés tels que les niveaux 4 et 5 définis par la SAE. Face au besoin croissant d'une protection optimale des CAVs, la méthodologie d'évaluation coordonnée des menaces et des risques (TARA) est considérée, par les réglementations et les normes dominantes, comme un moyen efficace de maintenir les systèmes à un niveau de risque tolérable. Bien que de nombreuses versions de TARA soient disponibles, elles restent ambigues et pas évidentes à exploiter ou à executer, ne traitent pas suffisamment les spécificités des CAV de niveaux L4 et L5 et ne considèrent pas les menaces relatives aux données à charactère personnelles comme priorité absolue.

A cet effet, l'adapation de la méthodologie TARA s'impose de plein droit. Par la présente thèse, et dans le cade du projet Horizon Europe ULTIMO [89], une déclinaison, nomée TARA 2.0, est proposée. Notre porposition est fondée sur des invesigations qui portent sur trois piliés : la cybersécurité, la protection des données et la normalisation. Dans cette optique, une vue exhaustive des menaces potentielles ainsi que les exigences en matière de réglementation et de normalisation ont été explorées. De plus, nous avons mené une étude systématique sur les méthodologies TARA récentes et prometteuses. Ainsi, nos investigations ont donné l'occasion de mettre le point en pratique sur leur lacunes et insuffisances afin d'extraire les mesures scuceptibles à adopter et les pistes à améliorer.

Ces efforts ont conduit au développement de TARA 2.0, qui a été mise en œuvre et validée par le biais d'une démonstration de concept. Les résultats démonstrent que notre solution fournit un traitement approfondi des menaces liées aux données des usagers et à leur vie privée. De plus, notre solution assure l'intégration d'une nouvelle métrique qui

incorpore le niveau d'automatisation dans le processus d'évaluation. Nos conclusions indiquent également que, dans le contexte des évaluations dépendant des avis des experts, TARA 2.0 améliore l'objectivité en abordant de manière transparente l'implication des experts dans le processus d'évaluation.

Cette thèse met ainsi au service des chercheurs, auditeurs, responsables de traitement et opérateur de villes intelligentes, un faisceau d'indices, de processus et de procédures pour mener à bien une étude de risque adéquate aux traitements de données envisagés, respectueuse de la nature des CAV du niveau 4 & 5 et en conformité avec la réglementation et les normes requises.

ملخص

تمثل حماية المركبات المتصلة والآلية (CAVs) من الهجمات الإلكترونية واختراق البيانات في تحدي كبير يواجه نشر المركبات ذاتية القيادة. تتميز المركبات ذاتية القيادة بتقنيات متطورة مثل أجهزة الاستشعار والوحدات الإلكترونية والذكاء الاصطناعي، مما يجعلها قادرة على تحويل مستقبل النقل. يتضمن هذا التحول مستويات مختلفة من التطور التكنولوجي والتحكم الآلي، مما يتطلب التأكد من أمان البيانات والتواصل بين المركبات والبنية التحتية لنظام النقل الذكي. هذه الأتمتة والتواصل الواسع النطاق يجلبان تحديات جديدة في مجال الأمن السيبراني وحماية البيانات، مما يستدعي النظر في تقييمات أمنية محددة.

شهدت كل من الأدبيات والقطاع الصناعي هجمات محتملة يمكن أن تؤثر بشكل كبير على قبول المركبات الآلية ذاتية القيادة وتعرض سلامة الركاب وخصوصيتهم للخطر. تتنوع الهجمات المسجلة من السيطرة على أنظمة الكبح والتوجيه، وتتبع مواقع الركاب وهوياتهم، إلى تعمية أجهزة استشعار السيارة مما يؤدي إلى وقوع حادث. يعتبر تحليل التهديدات وتقييم المخاطر (TARA)، وفقًا للوائح والمعايير الأساسية، الطريقة الفعالة للحفاظ على مستوى مقبول من المخاطر. على الرغم من توفر العديد من إصدارات TARA، إلا أنها ليست طرقًا جاهزة للاستخدام، ولا تعالج بشكل كافٍ خصائص المركبات ذات الدرجة الرابعة والخامسة ولا تأخذ في الاعتبار تهديدات خصوصية البيانات كما أنها ليست سهلت التطبيق.

في هذه الأطروحة، نقترح منهجية TARA المحسّنة تحت عنوان، TARA 2.0، لتحسين الأمن السيبراني وخصوصية البيانات والمعايير. تضمنت الجهود استكشاف تهديدات الأمن السيبراني والخصوصية البياناتية ومتطلبات التوحيد القياسي، وتحديد الثغرات في اللوائح والمعايير الرئيسية، ودراسة منهجيات TARA الحديثة. أدت هذه الجهود إلى تطوير وتنفيذ منهجية TARA 2.0، والتحقق من صحتها من خلال إثبات المفهوم.

أظهرت النتائج أن إطار عملنا يدمج تحليلًا دقيقًا لخصوصية البيانات ومستوى أتمتة التقييمات المعتمدة على الخبراء خلال عملية التقييم. كما أوضحت النتائج أن TARA 2.0 تعزز الموضوعية برفع شفافية مشاركة الخبراء في التقييم. بالإضافة إلى ذلك، يمكن أن يكون الحل المقترح دليلاً مهماً للتكرار المستقبلي للمقيمين الداخليين أو الخارجيين، مما يجعله نقطة مرجعية للباحثين الأكاديميين وصناع السياسات ومشغلي المدن الذكية ومراقبي البيانات ومقدمي الخدمات الذين يسعون إلى دمج المركبات ذاتية القيادة في عملهم.

Contents

List of Figures

List of Tables

List of Acronyms

e Specialised expertise.

k Knowledge of the item/ component.

l SAE Lx.

o Windows of opportunity.

q Equipment.

t Elapsed time.

3GPP 3rd Generation Partnership Project.

5GAA 5G Automotive Association.

A-SPICE Automotive Software Process Improvement and Capability dEtermination.

AAFL Aggregated Attack Feasibility Level.

Ac accountability.

ACEA European Automobile Manufacturers Association.

ACS Automated City Shuttle.

ACSW Workshop on Automotive Cybersecurity.

ADS Automated Driving System.

AES Advanced Encryption Standard.

AI artificial intelligence.

AI intelligence artificielle.

AKS Asymmetric Key Schemes.

ANIDS Anomaly-based Network Intrusion Detection System.

ANN Artificial Neural Network.

AP Attack Path.

APPI Act on the Protection of Personal Information.

ARCADE Aligning Research and Innovation for Connected and Automated Driving in Europe.

ASIL Automotive Safety Integrity Levels.

ATA Attack Tree Analysis.

Auto-ISAC Automotive Information Sharing and Analysis Center.

AUTOSAR Automotive Open System Architecture.

AV Automated Vehicle.

AVENUE Autonomous Vehicles to Evolve to a New Urban Experience.

BC Blockchain.

BSI British Standards Institution.

BSM Basic Safety Message.

BTS Base Transceiver Station.

C-ITS Cooperative Intelligent Transport Systems.

CAL Cybersecurity Assurance Level.

CAM Cooperative Awareness Messages.

CAN Controller Area Network.

CAV Véhicules Connectés et Automatisés.

CAV Connected and Automated Vehicle.

CCAM Connected, Automated and Autonomous Mobility.

CD committee draft.

CEM The Common Methodology for Information Security Evaluation.

CEN European Committee for Standardization.

CENELEC European Committee for Electronical Standardisation.

CIA Confidentiality, Integrity, Availability.

CJEU Court of Justice of the European Union.

CNN Convolutional Neural Network.

Com compliance.

CPPA Conditional Privacy-Preserving Authentication.

CPS cyber-physical system.

CRA Cyber Resilience Act.

CRSS CVSS Based Risk Scoring System.

CSMS Cyber Security Management System.

CSV comma-separated values.

CVE Common Vulnerabilities and Exposure.

CVSS Common Vulnerability Scoring System.

DBN Deep Belief Network Network.

DDT Dynamic Driving Task.

DENM Decentralized Environmental Notification Messages.

DES Data Encryption Standard.

DFD Data Flow Diagram.

DH Diffie-Hellman.

DIS draft international standard.

DNN Deep Neural Network.

DoS Denial of Service.

DOT Department of Transport.

DPA Data Protection Authorities.

DPIA data protection impact assessment.

DS Domain Specifity.

DSR Design Science Research.

DSRC Dedicated Short Range Communications.

DSSAD Data Storage System for Automated Driving vehicles.

E/E Electrical-Electronic.

ECC Elliptic Curves Cryptography.

ECU unités de commandes électroniques.

ECU Electronic Control Unit.

EDPB European Data Protection Board.

EEA European Economic Area.

ELK Elasticsearch, Logstash and Kibana.

ENISA European Union Agency for Cybersecurity.

ETSI European Telecommunication Standards Institute.

EU European Union.

EVITA E-safety Vehicle Intrusion proTected Applications.

FABULOS Future Automated Bus Urban Level Operation Systems.

FAIR Factor Analysis of Information Risk.

FDIS final draft international standard.

FG-AI4AD Focus Group-AI for Autonomous and Assisted Driving.

FMEA Failure Mode and Effects Analysis.

FMVEA Failure Mode, Vulnerabilities and Effects Analysis.

FOI Fake Object Insertion.

GDPR General Data Protection Regulation.

GNSS Global Navigation Satellite System.

GPS Global Positioning System.

GSIS Group Signature and Identity-based Signature.

HARA Hazard Analysis and Risk Assessment.

HEAVENS HEAling Vulnerabilities to Enhance Software Security and Safety.

HIPS Host-based Intrusion Prevention System.

IaaS Infrastructure as a Service.

ICDPPC International Conference of Data Protection and Privacy Commissioners.

ICT Information Communication Technologies.

IDEA International Data Encryption Algorithm.

IDS Intrusion Detection System.

IEC International Electronical Commission.

IoT Internet of Things.

IoV Internet of Vehicles.

IPA Information-Technology Promotion Agency.

IS Impact Score.

ISO International Organization for Standardization.

IT Information Technology.

ITS Intelligence Transport System.

ITS système de transport intelligent.

ITU International Telecommunication Union.

ITU-T International Telecommunication Union - Telecommunication Standardization Sector.

IWGDPT International Working Group for Personal Data Protection in Telecommunications.

JAMA Japan Automobile Manufacturers Association.

JASPAR Japan Automotive Software Platform and Architecture.

JRC Joint Research Centre.

JSAE Society of Automotive Engineers of Japan.

L4V L4 Evaluation Vehicle.

LBS location-based services.

LiDAR Light Detection and Ranging.

LIN Local Interconnect Network.

LINDDUN Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of data, Unawareness, and Noncompliance.

LRR Long Range Radar.

LTE Long-Term Evolution.

MaaS Mobility as a Service.

MAC Message Authentication Code.

MDL Machine and Deep Learning.

MEAN MongoDB, Express.js, AngularJS (or Angular), and Node.js.

MitM Man in the Middle.

MMW Millimetre Wave Radar.

MNO mobile network operator.

MOST Media-Oriented System Transport.

MRC Minimal Risk Condition.

MRM Minimal Risk Manoeuvre.

NA Not Applicable.

NASA National Aeronautics and Space Administration.

NHTSA National Highway Traffic Safety Administration.

nIove A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles.

NIS Network and Information Security.

NP new proposal.

NVD National Vulnerability Database.

OBD-II On-board Diagnostics System.

OBE on-board equipment.

OBU on-board unit.

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation.

ODD Operational Design Domain.

OEM automobile manufacturer.

OT Operational Technology.

OTA Over-the-Air.

PaaS Platform as a Service.

PAS Publicly Available Specification.

PASTA Process for Attack Simulation and Threat Analysis.

PbD Privacy by Design.

PbDf Privacy by Default.

PET Privacy Enhancing Technologies.

PETS Privacy Enhancing Technologies Symposium.

PIER Probability, Impact, Exposure, and Recovery.

PII Personally Identifiable Information.

PIPEDA Personal Information Protection and Electronic Documents Act.

PKC Public Key Cryptography.

PKI Public Key Infrastructure.

PoC Proof of Concept.

PPGCV Privacy-Preserving Group Communication Scheme for VANETs.

PTO Public Transport Operator.

RA Risk Assessment.

RACE Risk Analysis for Cooperative Engines.

RADAR Radio Detection and Ranging.

REM Risk Event Manager.

RMV On-Road Motor Vehicle.

RNN Recurrent Neural Network.

RQ Research Question.

RSA Rivest-Shamir-Adleman.

RSU road side unit.

RTU Root of Trust for Update.

SAAM Swiss Association for Autonomous Mobility.

SaaS Software as a Service.

SAE Society of Automotive Engineering.

SAHARA Security-Aware Hazard and Risk Analysis.

SARA Security Automotive Risk Analysis Method.

SCM Standards Coverage Map.

SDO Standard Development Organisation.

SDR Software Defined Radio.

SFOP Safety Finance Operations Privacy.

SHOW SHared automation Operating models for Worldwide adoption.

SIEM Security Information and Event Management.

SJR SCImago Journal Rank.

SKS Symmetric Key Schemes.

SPACE Shared Personalised Automated Connected vEhicles.

SPMT Start, Predict, Mitigate, and Test.

SPS Sequential Problem-Solving.

SRR Short Range Radar.

STAD Spatial and Transport Impacts of Automated Driving.

STRIDE Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service and Elevation of privilege.

SUMS Software Update Management System.

SVM Support Vector Machine.

TA Trusted authorities.

TAF Targeted Attack Feasibility.

TARA méthodologie d'évaluation coordonnée des menaces et des risques.

TARA Threat Analysis and Risk Assessment.

TEA Tiny Encryption Algorithm.

THARA Threat/Hazard Analysis and Risk Assessment.

TMT7 Microsoft Threat Modeling Tool.

TOD Target Object Insertion.

TPG transports publics genevois.

TPM Trusted Platform Module.

TPMS Tyre Pressure Monitor Systems.

TRA Transport Research Arena.

TRENG Transportation Engineering.

TVRA Threat, Vulnerability and Risk Assessment.

U unlinkability.

UK United Kingdom.

ULTIMO Advancing Sustainable User-centric Mobility with Automated Vehicles.

UNECE United Nations Economic Commission for Europe.

USA United States of America.

V2C Vehicle-to-Cloud.

V2G Vehicle-to-Grid.

V2I Vehicle-to-Infrastructure.

V2P Vehicle-to-pedestrian.

V2V Vehicle-to-Vehicle.

V2X Vehicle-to-Everything.

VANET Vehicular Ad Hoc Network.

VAST Visual, Agile, and Simple Threat.

VeRA Vehicles Risk Analysis.

VM virtual machines.

VPN Virtual Private Network.

W3C World Wide Web Consortium.

WAVE Wireless Access in Vehicular Environments.

WD working draft.

WG working group.

WG4 Data Protection Working Group 4.

WIP Work in Progress.

WP29 Article 29 Working Party.

ZKP Zero Knowledge Theory.

Part I

Introduction

Chapter 1

Overview

Contents

1.1 Context

"If it is smart, it is vulnerable."— Mikko Hyppönen

The automotive sector has evolved rapidly since the 19th century, with significant advancements in engine technology, energy efficiency and driver comfort. However, the most notable change has been the switch of road vehicles to become cyber-physical system (CPS), integrating both digital systems through Information Technology (IT) components and physical Operational Technology (OT) processes [391]. Such incorporation aimed, initially, to ensure enhanced vehicle management and entertainment, while, now, it has been extended to cooperative and automated driving capabilities. This context has enabled the Connected and Automated Vehicle (CAV) to become the ultimate component of today and future smart mobility.

CAVs, as defined by the Society of Automotive Engineering (SAE), are motor vehicles that integrate mechanical systems with a range of IT systems such as Electrical-Electronic (E/E), artificial intelligence (AI), computing systems and networks. Additionally, they incorporate numerous OT systems, including sensors, control systems and actuators, enabling the vehicle to sense its surroundings and navigate with various degrees of human involvement [389]. This definition confirms the dominant role of IT in shaping CAV's technology, offering significant opportunities for safety, environmental, and societal benefits. Particularly, CAVs aim to enhance road safety by mitigating accidents caused by human errors [48]. Additionally, they intend to reduce emissions through optimised and efficient driving [355]. Furthermore, they are promising an improved mobility for individuals who are unable to drive due to age, disability, or other factors [351].

To ensure autonomous navigation with limited human intervention, the CAV relies on its internal modern architecture, as well as the data exchanged with external entities. In the CAV landscape, driver vision capabilities are substituted by high-resolution cameras, LiDAR and RADAR. These data inputs, along with data from GPS, odometric, ultrasound sensors and various other sensors, are processed by each component's dedicated Electronic Control Unit (ECU). Subsequently, the processed data is transmitted via vehicle communication buses such as Controller Area Network (CAN) or Ethernet to reach the Automated Driving System (ADS) fusion system. The ADS then utilises this data to derive navigation planning, obstacle detection, traffic signs recognition, collision avoidance, and other driving decisions.

Besides, the CAV's extensive external connections represent another essential source of data influencing the autonomous driving behaviour. The CAV's connectivity aligns with Internet of Vehicles (IoV) and Intelligence Transport System (ITS) concepts. The CAV is a subset of IoV and a crucial element of the ITS, which encompasses a wide range of innovative mobility services [263]. The IoV, stemming from the Internet of Things (IoT), has transformed conventional vehicles into smart agents that remain constantly connected to internet, exchanging data with various external entities, thereby enabling Vehicle-to-Everything (V2X) communications [48]. These entities include roadside infrastructure (Vehicle-to-Infrastructure (V2I)), other vehicles (Vehicle-to-Vehicle (V2V)), cloud-based systems (Vehicle-to-Cloud (V2C)), power grids Vehicle-to-Grid (V2G), and even pedestrians (Vehicle-to-pedestrian (V2P)) [37]. Consequently, achieving highly automated driving relies on the efficient processing of gathered inputs from sensing components, and V2X communications.

While the advanced technologies of CAVs bring us significant advantages, they are also chilling unprecedented risks. The CAV's complex and interconnected ecosystem is intertwined with several cybersecurity and data privacy flaws that can be a real show stopper to their deployment if not properly addressed. Every IT or OT component from the CAV's ecosystem can be both an essential source to achieve the automated driving operations and an attack surface from which malicious intentions can exploit series of attacks. For instance, any intrusion to the CAV's in-vehicle bus can lead to taking control over the entire driving functionality, posing a direct threat to passengers' safety [434]. Additionally, any breach in the V2X may cause cascading effects on other ITS entities and vice versa [380]. Furthermore, by compromising one of the CAV's component, hackers can capture huge amount of Personally Identifiable Information (PII), threatening the end users privacy [76]. Consequently, evidence on CAVs' resilience, against diverse cybersecurity and data privacy vulnerabilities, is essential before their widespread deployment and full integration into daily life.

With the race towards a trade-off between maximising CAV's benefits and minimising the associated threats, Standard Development Organisations (SDOs) have been actively involved in developing strategies, guidelines and legislation to establish clear regulatory frameworks. Notable efforts include the United Nations Economic Commission for Europe (UNECE) R155 [430], which mandates the Cyber Security Management System (CSMS) certification as a prerequisite for vehicle type approval. This regulation aligns with the ISO/SAE 21434 [233] standard, providing a road-map to effective automotive cybersecurity governance. Specifically, the R155 requires an exhaustive Threat Analysis and Risk Assessment (TARA) in line with the ISO/SAE 21434 requirements. Additionally, beyond the automotive sector, several European Union (EU) regulations also apply. Network and Information Security (NIS) directives [422, 423], General Data Protection Regulation (GDPR) [424], Cyber Resilience Act (CRA) [145] and AI act [312] came to focus on assessing the risk impact and bring it to an acceptable level.

At this context, a thoroughly established TARA, that tackles the advanced CAV's particularities and evolving technologies, becomes vital for their successful deployment. TARA is an evaluation methodology which consists of identifying cybersecurity threats and appraising the risks associated to the determined threats [387]. The fulfillment of the CAV's type approval and the related requirements rely on TARA outcomes which consist of a clearly reported asset inventory, an in-depth threat identification as well as a comprehensive risk categorisation and calculation [326].

This thesis, which represents four years of investigations and experimental insights, analyses how cybersecurity and data privacy threats have evolved with the emergence of CAVs and how they can be properly assessed using TARA. It also showcases the efforts from SDOs aiming to regulate such environment based on standardised approaches. This implicates studying the limitations associated to the existing regulations and TARA methodologies to cope with the CAV's rapidly evolving technologies. Based on the identified pitfalls, the present work proposes an innovative and enhanced TARA addressing crucial shortcomings while maintaining the compliance with the key regulations and standards.

1.2 Motivation and problem definition

Safety has historically been the ultimate goal in the automotive industry, while cybersecurity obtained less attention until recent years. Since the integration of IT and OT components into modern vehicles' design, functional safety processes have become imperative, particularly with regard to software components. Initially, these processes focused on isolating those components from the driving engine. However, with the progressive incorporation of software and connected attributes through OT subsystems, the focus shifted towards the execution of Hazard Analysis and Risk Assessment (HARA) following the publication of ISO 26262 in 2011. HARA is a systematic approach which aims to identify and evaluate the likelihood and impact of accidental and hazardous harm [377]. At that stage, cybersecurity risks were often considered as part of the system failures or malfunctions. The introduction of SAE J3061 [387] in 2016 marked a significant step toward comprehensive cybersecurity management in the automotive domain. It represented the first draft of the TARA that was expanded further through the joint efforts from International Organization for Standardization (ISO) and SAE which led to establish the ISO/SAE 21434 [233] in 2021. The UNECE R155 [430] upraised the importance of cybersecurity by entering into force in July 2022. To that end, cybersecurity has emerged as a recent and pressing concern in the automotive sector just within the last decade.

While significant progress has been made with the introduction of dedicated regulations and standards, the increasing automation level adds another layer of complexity to CAV's cybersecurity governance. The SAE introduced six levels of automation which vary from L0 (no automation, the entire driving duty is on the human driver); L1 (driver assistance on either steering or speed, handled by the vehicle in a specific context); L2 (partial automation of the driving performance, but the driver is needed to react to external events); L3 (entire driving performance is automated, but human fallback is still required); L4 (entire driving and fallback are automated but in a specific context) to L5 (fully automated with unlimited conditions) [385]. Particularly, the L4 and L5 represent the highest automation stages, where vehicle can operate autonomously within a defined Operational Design Domain (ODD). Consequently, these CAVs are expected to mitigate cyber risks in real-time manner, while those at lower levels, such as L3, may still require human intervention to manage attacks. In contrast, existing regulations and recommendations treat CAV's of SAE L3 onward uniformly, without an explicit differentiation among the various levels [271]. For instance, the UNECE R155 mandates the same TARA process for the three levels (L3, L4 &L5). This fails to consider the complex risk characteristics linked to every level of automation. A risk assessed as low in an L3 CAV may escalate to high in L4, and even higher in an L5 CAV where the ADS replaces the human control in risk mitigation [321].

In addition to SAE levels related challenges, privacy is another key concern, albeit it has got minor attention in the L4 & L5 CAVs domain. For every mile driven, the CAV generates, processes and exchanges a large amount of data through its in-vehicle systems or V2X means [75]. For instance, the CAV's cameras which intend to capture environmental data, may potentially record personal facial identities simultaneously. Additionally, the CAV geographical location can be jointly processed with passengers' identities yielding to an array of location tracking threats [412]. Moreover, the CAV's high connectivity opens doors to innovative services like location-based services (LBS), which entail additional data exchanges with third parties' platforms [406]. Consequently, assessing privacy threats and their corresponding countermeasures is capital. Unfortunately, the state-of-the art, existing regulations and TARA methods overlook privacy threats and fail to accord them the same level of consideration as cybersecurity threats. Therefore, investigating data protection challenges and putting higher emphasis on privacy aspects throughout the TARA process play a crucial role in protecting personal data against various breaches and ensuring the compliance to fundamental data protection laws.

While it is essential to assess cybersecurity and data privacy threats, the quality of the assessment per se is of utmost importance. The TARA process involves extensive manual efforts to build analysis on damage scenarios, model threat scenarios, and determine the impact and feasibility of potential attacks [3]. However, the experts involvement in the process may lead to subjective results, as they are likely to have varying opinions, biases and perspectives[267]. Despite the reliance on experts knowledge, existing TARA methodologies do not provide any confidence factors to support in determining the objectivity of the assessment outcomes. Therefore, while the reliance on expert knowledge remains essential to conduct TARA, it is crucial to complement this expertise with an assessment of the experts' confidence about the results as well as transparent communication of the level of the experts involvements.

The demands for tackling the CAVs' cybersecurity and data privacy challenges are constantly expanding. Alongside the SDOs efforts, several projects have emerged to support the CAVs testing and development. Among those efforts, the Horizon Europe Research and Innovation funded projects Autonomous Vehicles to Evolve to a New Urban Experience (AVENUE) [419], A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles (nIove) [141], SHared automation Operating models for Worldwide adoption (SHOW) [401] and Advancing Sustainable User-centric Mobility with Automated Vehicles (ULTIMO) [140]. These projects served both to gear up the cybersecurity and data privacy investigations and to push the present thesis dissertation forward. The provided real-world L4 CAVs, testing environments and the concrete architecture endorsed our research work. More particularly, the exchange of knowledge with project partners and engagement with expert teams have been instrumental in supporting the verification and validation of our scientific findings.

Despite the emergent research interest in cybersecurity and privacy, significant efforts in addressing L4 & L5 CAV particularities and assessing their unique threats are still lacking. This can be attributed to several factors. First, there is a dominant focus on safety in the forefront of research efforts, with comparatively less attention given to cybersecurity and even less to privacy concerns. Second, existing regulations and recommendations remain insufficient, as they are applicable to conventional vehicles of SAE L3, where the risks are incomparable and necessitate different approaches from those of L4 onwards. Therefore, our research leverages the context of the Horizon Europe projects to conduct thorough investigations and propose TARA 2.0 as an appropriate assessment framework to L4 & L5 CAVs, permitting a fine-grained modeling of potential threats, an incorporation of the automation level and privacy features as well as a consideration of providing evidence on the experts objectivity.

1.3 Research questions

As the CAV embraces the cybersecurcity and data privacy facets and based on the SAE definitions of the automation levels, the following Research Questions (RQs) have been investigated throughout the present thesis:

- RQ1: How to efficiently mitigate cybersecurity and data privacy threats related to CAVs according to a holistic view of all eventual risks?
- RQ2: By implementing the published standards, and assuring the compliance to the existing regulations, how robust the CAVs would be from both security and data protection perspectives?
- RQ3: How the existing standards and regulations can be upgraded to cope with the CAVs technological evolution and legal requirements?
- RQ4: What factors drive the wide adoption of TARA from ISO/SAE 21434?
- RQ5: To what extent TARA methodology can be adapted to the highly automation properties of SAE L4 and L5 and the data privacy challenges?
- RQ6: How to build the most auspicious security assessment model based on TARA approaches with respect to the CAVs landscape?

1.4 Significance

In light of the significant growth of threats and their consequential impacts, as well as the limitations of existing legislation and standards, the present work aims to provide a deeper knowledge about the cybersecurity and data privacy challenges before any large deployment of the CAVs as intended within the near future [434]. It serves also as a consolidated reference point to researchers and smart cities operators evaluating the cybersecurity and data privacy concerns while incorporating CAVs as a part of the ITS. Additionally, by proposing and showcasing an enhanced TARA, we aim to provide a fine-grained road-map to tackle a thorough assessment in line with both: relevant regulations and L4 & L5 properties. Type approval experts, internal/external auditors, automobile manufacturers (OEMs) and ITS service providers could leverage the insights from the demonstrated work for any future replication. Furthermore, the proposed improvements avenues are intended to be presented within standardisation committees with the aim to take part of the Work in Progress (WIP) pertinent standards related to TARA.

1.5 Methodology

The objectives set for this thesis present a good fit for combining SPS and DSR methodologies [436]. On one hand, the SPS represents a step-by-step structured model where the problem identification, refinement and solving occur through distinct multiple stages. In a such model, each stage is built based on the gained insights from the preceding steps. The SPS consists of the following steps [110]:

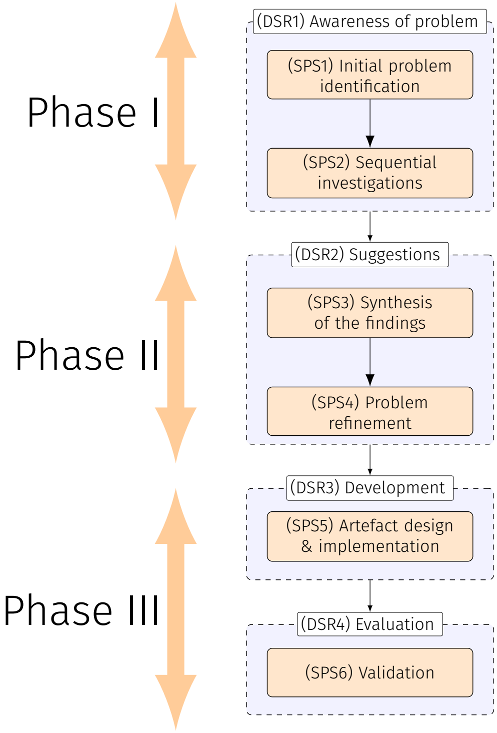

Phase I
Phase II
Phase III
(DSR1) Awareness of problem
(SPS1) Initial problem identification
(SPS2) Sequential investigations
(DSR2) Suggestions
(SPS3) Synthesis of the findings
(SPS4) Problem refinement
(DSR3) Development
(SPS5) Artefact design & implementation
(DSR4) Evaluation
(SPS6) Validation

Figure 1.1: Overall thesis methodology combining Design Science Research (DSR) and Sequential Problem-Solving (SPS).

- SPS1: Initial problem identification,
- SPS2: Sequential investigations,
- SPS3: Synthesis of the findings,
- SPS4: Problem refinement,
- SPS5: Artefact design & implementation, and
- SPS6: Validation.

On the other hand, the DSR focuses on designing, implementation and validating an artefact. The DSR methodology relies on four major steps [436]:

- DSR1: Awareness of problem,
- DSR2: Suggestions,
- DSR3: Development, and
- DSR4: Evaluation.

While the overall flow of the two methodologies may overlap, more particularly in the two last steps (SPS5/DSR3 and SPS6/DSR4), they are complementing each other in providing detailed investigations and a staged approach problem identification. In this thesis, we leveraged the experiences gathered regarding the use of both models through three major phases as detailed in Figure 1.1 and in the following subsections.

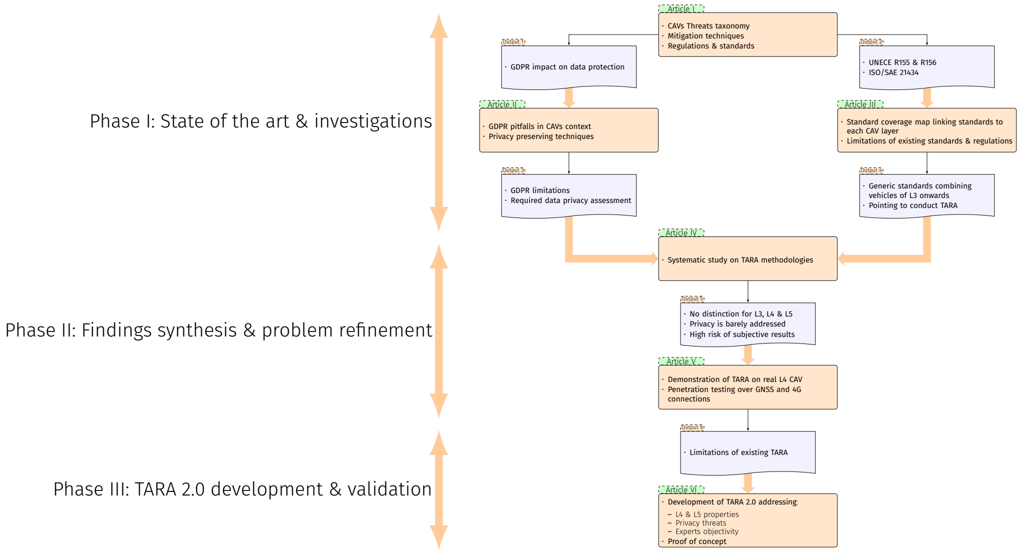

Phase I: State of the art & investigations
Phase II: Findings synthesis & problem refinement
Phase III: TARA 2.0 development & validation
Article I
· CAVs Threats taxonomy
· Mitigation techniques
· Regulations & standards
Output 1
· GDPR impact on data protection
Output 2
· UNECE R155 & R156
· ISO/SAE 21434
Article II
· GDPR pitfalls in CAVs context
· Privacy preserving techniques
Article III
· Standard coverage map linking standards to each CAV layer
· Limitations of existing standards & regulations
Output 3
· GDPR limitations
· Required data privacy assessment
Output 4
· Generic standards combining vehicles of L3 onwards
· Pointing to conduct TARA
Article IV
· Systematic study on TARA methodologies
Output 5
· No distinction for L3, L4 & L5
· Privacy is barely addressed
· High risk of subjective results
Article V
· Demonstration of TARA on real L4 CAV
· Penetration testing over GNSS and 4G connections
Output 6
· Limitations of existing TARA
Article VI
· Development of TARA 2.0 addressing:
– L4 & L5 properties
– Privacy threats
– Experts objectivity
· Proof of concept

Figure 1.2: Papers correlations.

1.5.1 Phase 1: State of the art and investigations

This phase is represented by the first two steps of the SPS methodology where a progressive approach was adopted to explore the subject and generate theories to ultimately define the core thesis problem. At the beginning, an initial identification of the problem, marking the SPS model (SP1), was conducted by working on an extensive state of the art. Therefore, the three pillars of the present research were set: cybersecurity, data privacy and standards. In this step, a rough draft of RQs were elaborated and the motivation for conducting thorough investigations was triggered. The sequential investigations (SPS2) are illustrated through the efforts on the three pillars depicted through the primary three articles from Figure 1.2. First, an in-depth overview of the different CAV's threats and the relevant technical mitigation techniques were addressed through an initial manuscript (Article I, Chapter 2, [41]). Second, the knowledge regarding personal data protection within the CAV's environment was consolidated through the identification of gaps between the legal provisions of privacy laws and security technologies implementations. To underpin such knowledge, it was fundamental to collaborate with a lawyer to build up a multidisciplinary article (Article II, Chapter 3, [44]). Third, the knowledge from the two other pillars was exploited to evaluate the existing standards and highlight their shortcomings through Article III (Chapter 4, [39, 38]). Through those research efforts, the CAV's entire system layers were identified and mapped to latest standards and regulations from both cybersecurity and data privacy perspectives. Moreover, to achieve such goals, it was imperative to join ISO and International Telecommunication Union (ITU) working groups to closely track the progress throughout the key ongoing standards related to CAVs.

1.5.2 Phase 2: Findings synthesis and problem refinement

The synthesis of the findings from each of the three articles, marking the SPS3 step, reflects relevant advancements and limitations in the CAV's environment with regards to the three predefined pillars accordingly. At that stage, it is noteworthy to mention that the AVENUE project context provided an ample opportunity for verifying our theoretical findings through the Automated City Shuttle (ACS) model as a special case of CAVs. To that end, the derived results laid to a refinement of the core thesis problem (SP4). More particularly, by acknowledging that a risk zero can never exist in such environment, the research focus was shifted from what are the cybersecurity and data privacy threats in CAVs, to how to have them properly assessed and tolerated at an acceptable level of risk while maintaining an alignment with the key standards and regulations. Such refinement was achieved through a systematic study on TARA frameworks as Article IV (Chapter 5, [40]), which supported in both finalising the thesis RQs and suggesting the requirements for an efficient solution as the main outcome of the second step of the DSR methodology.

1.5.3 Phase 3: TARA 2.0 development and validation

During this phase, we proceeded with the theoretical definition of the artefact addressing the common intentions of the DSR3 and SPS5 combined step of our methodology. To achieve this, we employed both analytics and experimental approaches. The analytics approach is represented through the extraction of the limitations of existing TARA frameworks from Article IV. The experimental approach is mirrored across the demonstration of the most prominent framework from ISO/SAE 21434 (hereinafter referred as TARA 1.0) as Article V (Chapter 6, [43]). Both articles spotlighted the pitfalls of TARA 1.0 representing the key enhancements proposed by the thesis artefact TARA 2.0.

After establishing the theoretical framework of TARA 2.0, we proceeded to implement the artefact within the ULTIMO project and through Article VI (Chapter 7, [42]). The tangible L4 CAV architecture, the existing documentation on the ADS related assets and the involvement of the experienced experts facilitated in concretising the TARA 2.0 framework into a practical context. These conditions have contributed to the validation of the proposed framework through a Proof of Concept (PoC) as a final step of our methodology (DSR 4 and SPS6). Furthermore, the conducted demonstration of TARA 1.0 served as another enabler of the research validation. The experiences from both TARA 1.0 and TARA 2.0 demonstrations supported in deriving a comparative analysis of both frameworks and their respective performances. The results asserted the notable performance of TARA 2.0 over TARA 1.0 in addressing privacy concerns, automation level and experts subjectivity while maintaining the full compliance to the key regulations and standards.

1.6 Contributions summary

The present thesis gathers articles which were peer-reviewed and published either on scientific journals or conferences. Table 1.1 depicts detailed information of all the publications while below is a brief overview of each paper:

1.6.1 Article I

Benyahya, M., Collen, A., Kechagia,S., Nijdam, N.A. (2022, September). *Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments.* Computers and Security 122, 102904.

In this article, we introduce the state-of-the art of the cybersecurity and data privacy threat vectors, mitigation strategies as well as the relevant regulations and standards applied to the CAV's landscape. More specifically, the paper focuses on the ACS as an illustration of real integration of CAVs into public transportation domain. The paper provides the foundations for a thorough understanding of the CAV's environment complexity and challenges through detailed analysis of potential in-vehicle and out-of vehicle surface attacks in addition to the key standards to comply with. Driven by the real development of the ACS within the H2020 AVENUE project in Geneva site, our work further debates the trade-off between maximising the ACS' benefits and minimising the associated security and privacy vulnerabilities through an overview of technical and legal countermeasures.

1.6.2 Article II

Benyahya, M., Collen, A., Kechagia,S., Nijdam, N.A., (2022, April). *The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis.* Applied Sciences, 12(9), p.4413.

Following up on the ACS ecosystem evaluation under the umbrella of the AVENUE project, this paper provides an interdisciplinary overview of the data privacy requirements from both the legal and security perspectives. By considering the pervasive collection and processing of personal data within the ACS environment, the paper objectives are twofold: first study the GDPR requirements as well as the stakeholder roles at the collection, storage, use, and transmission of data to and from the vehicles; and second analysis the effectiveness of the privacy-preserving techniques within the ACS environment. The paper expands further the gap between the legal definitions and the technological implementation of the relevant mitigation techniques through the GDPR pitfalls.

1.6.3 Article III

Benyahya, M., Collen, A., Nijdam, N.A., (2022, November). *Analysis on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap.* Transportation Engineering, vol 14, 12 2023.

Following up with the sequential investigations approach (Figure 1.1), the two previous papers created ample opportunity to investigate further on the CAVs's standardisation maturity. In this paper, SDOs and working groups (WGs), who have been active on normalising the cybersecurity and data privacy governance for CAVs, are identified. Additionally, the leading standards and regulations on providing a cybersecurity governance frameworks are spotlighted. The article asserts that ISO/SAE 21434 and UNECE R155 represent the most unified and dominant guidelines. Moreover, the article introduces the Standards Coverage Map (SCM) where CAV's layers are mapped to existing and WIP standards. The map depicts a granular foresight on how safety-critical components are addressed by the SDOs and how relevant they are regarding the potential threats. Applied to the AVENUE pilots, this work proposes mandatory regulations to comply with as well as a clear roadmap to consider for CAV's standardised cybersecurity governance. This article embodies an extended version of the conference proceeding manuscript[39] presented in Transport Research Arena (TRA)'22.

1.6.4 Article IV

Benyahya, M., Lenard. T, Collen, A., Nijdam, N.A., (2023, August). *A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicle* In The 18th International Conference on Availability, Reliability and Security (ARES 2023), Benevento, Italy.

Driven by Articles I, II & III's findings which point out the ISO/SAE 21434 guidelines as the core standard and UNECE R155 as the mandatory regulation to comply with, we leverage their ultimate common requirement to consider at all the vehicle's life-cycle stages to be: TARA implementation. Although several TARA methodologies have been introduced by both standardisation bodies and researchers within the automotive sector, very few approaches are designed for highly automated CAVs. Investigating into the existing TARA methodologies is an absolute necessity to construct thorough insights about what makes a methodology applicable or not to L4 and L5 CAVs. Through a systematic review following Kitchenham and Charters [272] practices, this article identifies relevant methodologies and provides their consonance and pitfalls with regard to CAV's properties. The inquiry emphases on how each TARA addresses the SAE automation level, privacy threats and their risk impact computation as well as the experts subjectivity and involvement within the entire assessment process. Article IV recognises that there is no one ideal TARA. The article embraces the fact that TARA is a broad, yet adaptive, process which spans different threat modelling mechanisms and definite risk metrics that are compiled to retrieve cybersecruity goals and claims.

1.6.5 Article V

Benyahya, M., P. Bergerat, Collen, A., Nijdam, N.A., (2023, March). *Symbiotic Analysis of Security Assessment and Penetration Tests Guiding Real L4 Automated City Shuttles* Telecom, vol.4, pp. 198-218.

Since early stages of the systematic study conducted in Article IV [40], it has been revealed that TARA from ISO/SAE 21434 (hereinafter, referred as TARA 1.0) is the most adopted methodology for the last three years where all recent developed methodologies are either seeking to comply or to slightly enhance. Therefore, this article depicts a direct demonstration of TARA 1.0 by strictly following its steps as claimed in ISO/SAE 21434 standard. Over real L4 CAV, the demonstration focuses on the vehicle wireless connections including Global Navigation Satellite System (GNSS) and 4G as the evaluated asset. The research work elevates further the TARA outcome by conducting penetration testing as a mean of verification and validation process of the assessment.

1.6.6 Article VI

Benyahya, M., Collen, A., Nijdam, N.A., (2024, April). *Driving towards resilience: Advancements in threat analysis and risk assessment for connected and automated vehicles*, IEEE Transactions on Intelligent Vehicles - Under first review.

Guided by the identified pitfalls, from Article IV and V, of existing TARA methodologies in general, and the limitations of TARA 1.0 in specific, this Article proposes the enhanced TARA 2.0. This paper's objectives are threefold: (i) propose enhancements avenues to elevate TARA 1.0 to become more privacy-centric, address L4 and L5 CAVs's properties, and provide more subjective results (ii) provide fine-grained guidelines in a step-by-step manner allowing to replicate the assessment (iii) showcase TARA 2.0 at a granular level and by reducing the multiple aggregations in TARA 1.0 that serves rather for higher level risk analysis Through a PoC and a comparative analysis between TARA 1.0 and TARA 2.0, this Article showcases the feasibility of the proposed framework.

Table 1.1: Scientific contribution.

	Article I	**Article II**	**Article III**	**Article IV**	**Article V**	**Article VI**
Title	Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments [41]	The Interface of privacy and data security in automated city shuttles: The GDPR analysis [44]	Analysis on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap [38]	A systematic review of threat analysis and risk assessment methodologies for connected and automated vehicles [40]	Symbiotic Analysis of Security Assessment and Penetration Tests Guiding Real L4 Automated City Shuttles [43]	Driving towards resilience: Advancements in threat analysis and risk assessment for connected and automated vehicles [42]
Authors	**M. Benyahya**, A. Collen, S. Kechagia, and N.A. Nijdam	**M. Benyahya**, A. Collen, S. Kechagia, and N.A. Nijdam	**M. Benyahya**, A. Collen, and N.A. Nijdam	**M. Benyahya**, T. Lenard, A. Collen, N.A. Nijdam	**M. Benyahya**, P. Bergerat, A. Collen, N.A. Nijdam	**M. Benyahya**, A. Collen, T. Lenard, N.A. Nijdam
Stages	Initial problem identification (SPS1) Sequential investigations (SPS2) Synthesis of the findings (SPS3)	Sequential investigations (SPS2) Synthesis of the findings (SPS3)	Sequential investigations (SPS2) Synthesis of the findings (SPS3)	Synthesis of the findings (SPS3) Problem refinement (SPS4) Artefact design (SPS5)	Synthesis of the findings (SPS3) Problem refinement (SPS4) Artefact design (SPS5)	Artefact design & implementation (SPS5) / (DSR3) Validation (SPS6) / (DSR4)
Methods	Literature Review Requirements Analysis Use case studies	Literature Review Expert opinions Use case studies	Literature Review; Standards WGs	Kitchenham and Charters [272] systematic review guidelines; Workshop	Threat modeling ISO/SAE 21434 appendices black-box testing Use case studies	Threat modeling Experiments Expert workshops Use case studies
Impact	IS: 7.35 h-Index: 112 SJR: 1.605	IS: 2.48 h-Index: 22 SJR: 0.336	IS: 5.40 h-Index: 13 SJR: 0.864	B category	IS: 2.1 citescore: 4.8	IS: 7.70 h-Index: 43 SJR: 1.583
Publication	*Journal* Computers and Security, Elsevier, 2022	*Journal* Applied sciences, MDPI, 2022	*Journal* Transportation Engineering, Elsevier, 2023	*Conference Proceedings* The 18th International Conference on Availability, Reliability and Security (ARES), 2023	*Journal* Telecom, MDPI, 2023	*Journal* IEEE Transactions on Intelligent Vehicles, 2024
Status	Published	Published	Published	Published	Published	Under 1st review
Contributions	Own contribution: 90% Concept: M.B., A.C Methodology: M.B. Writing: M.B., S.K., A.C., N.N. Visualisation: M.B., N.N. Supervision: A.C., N.N.	Own contribution: 75% Concept: M.B., A.C., N.N. Methodology: M.B., S.K. Writing: M.B., S.K., A.C., N.N. Visualisation: M.B., N.N. Supervision: A.C., N.N.	Own contribution: 95% Concept: M.B. Methodology: M.B., N.N. Writing: M.B., A.C., N.N. Visualisation: M.B., N.N. Supervision: A.C., N.N.	Own contribution: 95% Concept: M.B., T.L., A.C. Methodology: M.B., A.C., N.N. Analysis: M.B, A.C Writing: M.B., T.L., A.C., N.N. Visualisation: M.B., N.N. Supervision: A.C., N.N.	Own contribution: 60% Concept: M.B., P.B., A.C., N.N. Methodology: M.B., P.B. Pentesting: P.B. Analysis: M.B., P.B., A.C. Writing: M.B., P.B., A.C., N.N. Visualisation: P.B., N.N. Supervision: A.C., N.N.	Own contribution: 95% Concept: M.B. Methodology: M.B., A.C Analysis: M.B., A.C., N.N. Writing: M.B., A.C., N.N. Visualisation: M.B., A.C., N.N. Revision: A.C., T.L. N.N. Supervision: A.C., N.N.
Related project	AVENUE and SHOW	AVENUE, nIoVe and SHOW	SHOW and ULTIMO	SHOW and ULTIMO	SHOW and ULTIMO	ULTIMO

1.7 Structure

The present thesis is organised as follows:

- Part 1 – Introduction: This part lays the groundwork of the thesis including the identification of the context, scientific problem and RQ motivating the research work. It also outlines the methodology adopted as well as a brief description of the Articles consisting the body of the thesis.
- Part 2 – Cybersecurity, data privacy and standardisation investigations: This part incorporates the first phase (Section 1.5.1) of the methodology as depicted in Figures 1.1 and 1.2. It focuses on how the SPS1 and SPS2 steps are achieved via the elaboration of the first three Articles corresponding to the following chapters:
  - Chapter 2 (Article I): with its fundamental background taking the form of a state-of-the art, this chapter effectively tackles research RQ1 while providing partial insights into RQ2 & 3. It represents the first step towards identifying the thesis problem. It also encapsulates the results from the cybersecurity investigations as the first pillar of this research.
  - Chapter 3 (Article II): dedicated to data privacy investigations, this chapter complements the answer to RQ2. It provides insights into the second pillar of this research investigation through the examination of the GDPR data processing principles as well as on the privacy preserving techniques.
  - Chapter 4 (Article III): by providing in-depth analysis of the existing and ongoing efforts from the SDOs, this chapter complements the answer to RQ2 & 3. It outlines the correlation among prominent regulations and standards as well as their limitations with regard to the CAV's system layers.
- Part 3 – Threat Analysis and Risk Assessment (TARA): The chapters in this part of the thesis mirror the second phase of our methodology where the thesis problem was refined and the reasoning behind an appropriate TARA implementation was developed:
  - Chapter 5 (Article IV): through a systematic review, existing TARA methodologies were evaluated and their limitations in addressing L4 & L5 CAV's properties were spotlighted. The manuscript underscores the significance of TARA 1.0 and hence fully addressing RQ 4 and partially answering RQ 5.
  - Chapter 6 (Article V): here we showcased TARA 1.0 implementation for an experimental understanding and elicitation of the assessments methodology pitfalls. The implementation results were elevated further by conducting several attack simulations, also referred as penetration testing in the chapter.
- Part 4 – Enhanced TARA implementation: This part corresponds to the third phase of our methodology which is represented through:
  - Chapter 7 (Article V): with its complete TARA 2.0 implementation, demonstration and validation, this chapter complements the answer to RQ 5 and fully addresses RQ 6.

- Part 5 – Conclusions: This part consists of one chapter:
  - Chapter 8: plays an important role in synthesising the entire thesis findings. It highlights the overall research limitations and sets the envisioned future work before it concludes the thesis.

Disclaimer

From the structure perspective, this thesis comprises previously published papers, which are integrated as chapters. However, the included text was further harmonised to ensure consistent writing style throughout the thesis.

From the terminology perspective, “ACS” and “CAV” terminologies are used interchangeably to denote the evaluated vehicle model. Additionally, “cybersecurity” and “security” terms are used as synonyms to point to attack and threat-related security, excluding physical security concerns.

Funding statement

The present thesis has been co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

Part II

Cybersecurity, data privacy and standardisation challenges

Chapter 2

Article I: Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments

Relevance

This article introduces the foundations of the cybersecurity and data privacy challenges related to the CAV landscape. In here, we developed the initial formulation of the research methodology adapted in this thesis. The article fully tackles the thesis' RQ1 and partially answers RQ2 and RQ3 that were supplemented by Chapter 3 and Chapter 4.

Context

This article [41] was published in the Journal of Computers & security ranked as a B journal according to CORE classification[1], and whose Impact Score (IS): 7.35, h-Index: 112 and SCImago Journal Rank (SJR): 1.605 according to the Resurchify portal[2].

Own contribution

Taking on the role of the lead author of this paper, I provided the conceptualisation, visualisation, analysis and elaboration. I produced the majority of the content while co-authors assisted in reviewing the manuscript through several rounds and proposed constructive orientations. Being my first latex project, co-authors played a supportive role in formatting and designing the manuscript tables.

[1] http://portal.core.edu.au/

[2] https://www.resurchify.com/about

Contents

2.1 Abstract

The ACSs aim to shape the future public transportation and provide more efficient and accessible mobility in smart cities. With the absence of a driver, such mini-busses process the sensors' inputs and exchanged data with other vehicles and intelligent transport systems to achieve a real time assimilation of its surroundings. Consequently, the technologies supporting the driverless functionalities ushered new cybersecurity risks and data privacy breaches. Unfortunately, several studies mostly focus on individual CAV, though intrinsic underpinnings of the ACS's threat vectors remain unexplored. In the present chapter, we considerably extend that investigation by proposing a comprehensive state of the art with farsighted analysis addressing security threats and data privacy concerns from both technical and legal perspectives to thwart potential attacks. Moreover, as existing approaches have not provided yet a clear road map about ACS's security standards, the present work sheds light on recent and up to date standards and standardisation bodies dealing with cybersecurity and privacy issues in the automated driving ecosystem. This paper presents an analysis debating the trade-off between maximising the ACS benefits and minimising the associated security vulnerabilities and attacks through an overview of technical and legal mitigation strategies.

2.2 Introduction

Within the last few years, cities have been acquiring management approaches based on new technologies to enhance citizen's quality of life. Modern cities are motivated to provide new shared mobility services with higher efficiency and reliability at lowest costs. Integrating ACSs to the urban environment is one effective manner to tackle this challenge. ACSs introduce an innovative public transportation paradigm through customised offers like on-demand and door-to-door services [199]. Meyer et al. [328] demonstrated how the automated vehicles can improve the public transportation in Swiss municipalities by increasing its accessibility up to 40%. As ACSs are providing a non-stop service, they are expected to reduce drivers payroll costs to public transportation companies [296] and provide cheaper commuting for the passengers [51]. In addition, integrating such mini-buses, with extensive automated capabilities, to the public transportation promises more accessibility to elderly, children and disabled users [104, 85]. ACSs can also decrease accidents per the absence of the human factor error, improve traffic flow and road transport capacity [293]. Based on such assumptions, ACSs will not just improve the passengers' experience, but they will beneficially change the urban dimensions and push it forward to a new era.

Driverless vehicle can be a personal individual car, a taxi, a bus, a shuttle or a mini-bus, an emergency car, a truck, a train, a tram, etc. with different levels of human involvement [53]. The SAE defined a complete range of six automation levels varying from level 0, where none of the safety-critical functions are automated, to level 5, presenting a full automation of control systems [385]. In addition, the regulation 2019/2144 of the European Parliament and of the Council of 27 November 2019 defined "Fully Automated Vehicle" to be motor vehicle operating autonomously without the human supervision and intervention [421]. The present paper concentrates on ACS as fully automated mini-buses for public transportation with levels 4 and 5 from the SAE classification.

ACS represents a unique challenge not only by deploying the latest Information Communication Technologies (ICT) advancement into the public transportation sector, but also by expanding the existing city's infrastructure into smart enabled environment. This process involves several upgrades and adaptation, including the city infrastructure, the social and economic impacts, political aspects, cybersecurity challenges, implementation of relevant regulations and standardisation which should come to support the ACS deployment. In this paper, we focus on cybersecurity threats, data privacy issues and their related regulations and standards as critical challenges that can be very harmful to ACSs' integration if not well considered. The concern remains about the trade of maximising the ACS benefits and minimising associated vulnerabilities and attacks' unintended outcomes.

Collard et al. [84] have updated the cybersecurity definition based on the last years challenges related to IoT. The authors defined cybersecurity as the organisation and the protection of information technologies with the combination of the following notions: availability, confidentiality, criticality, attack impact, integrity, ownership, sensitive values, legal risk, contextualisation, risk assessment and information storage [84]. Applied to IoV paradigm, National Highway Traffic Safety Administration (NHTSA) defined cybersecurity as the protection of the vehicle components, infrastructure and communications from any harmful attacks, unauthorised access or anything that jeopardises the safety functions [350]. Given that the ACS functioning depends on many in-vehicle hardware and software systems in addition to a permanent connection to the external environment, the risk of vulnerabilities escalates.

The existing literature has witnessed multitude of successful attacks in the last decade over automated driving components. Miller and Valasek [330] presented how they remotely attacked the CAN bus of the Jeep Cherokee causing a loss of control over the braking and the steering systems. Zhang, Antunes and Aggarwal [467] described the operational and safety disruptions that may be caused by a malware if it infects the connected vehicles' ECUs. Yan, Xu and Liu [462] demonstrated how automated driving sensors in Tesla S can be blinded and led to a crash. With the increase of interest in deploying automated driving within public transportation, the motivation and the likelihood to conduct similar attacks will grow. This is why we consider of great interest to analyse, based on security-by-design mechanisms, the potential cybersecurity threat vectors and their technical and legal countermeasures in the present paper.

As the ACS moves from one place to another, it communicates permanently with other vehicles, infrastructure and external devices. While moving, the shuttle exchanges data also with its passengers. The shuttle's user may be requesting customised ACS services which requires the integration of LBS, such as Mobility as a Service (MaaS). MaaS is a mobility platform which bridges public transport to mobility services by providing, for example, door-to-door services based on the passengers information including their location [406]. Such new transport model requires an endless exchange of information, among vehicles, public transportation interfaces, users' smart devices and other third parties, which raises data privacy concerns [338].

In the scientific literature, there are several definitions of data privacy. These definitions vary depending on the sector that explores them and prove that data privacy is a notion with many facets [295]. With the growth of IoT technologies, data privacy is perceived as the protection from any unauthorised access and usage control of the collected, processed and stored individuals information [260]. Applied to the IoV context, it refers to the vehicle passengers' privacy and the vehicle location [316]. In other words, while exchanging messages with other vehicles and external devices, the ACS and the passengers' identities and locations should not be revealed (except to relevant authorities). Unlike the individual CAV, where such risk impacts a limited number of people, in the ACS the data privacy concern is applicable to a larger group of individuals, including the shuttle operators and passengers. Hence, considering the increased scope of the impact, in comparison to CAVs, data privacy in ACS must be looked at differently by incorporating adapted countermeasures and referring to existing laws, policies and standards.

In a context of exploring cybersecurity and data privacy threats, there has been much work conducted on studying attacks and countermeasures over CAVs [372, 367, 378, 113, 264, 380, 269, 413, 373]. Though, the existing work didn't cover all potential threats and mitigation solutions comprehensively. It has also discussed the threats in a generic way without addressing the specificity of ACSs. In addition, data privacy concerns were extensively analysed in the literature but either as one of the threats [392, 98, 363] or from liability perspective [369, 94, 415, 281, 441] without a thorough review or a designation of applicable protocols, preserving privacy, while exchanging personal data within the vehicular environment. Organisational solutions to prevent from personal data breaches within automated vehicles as a means of public transport are also barely over-viewed. Furthermore, regulations and standards, related to cybersecurity and data privacy, were partially discussed [395, 81, 398, 301, 304, 12, 10, 293], sometimes with a focus on a single regulation [91] or an individual standard [309, 397] or just as an open issue for future research efforts [98]. To the best of our knowledge, the existing research proposals neither provide comprehensive technological and legal guidelines for the ACS deployment nor identify the key standards for such vehicles' security certifications. A detailed description of other researchers' efforts along with a comparison between our efforts and their findings are highlighted in Section 2.3.

This trend encourages for a new breed of in-depth analysis and exhaustive statement of the state of the art, combining and focusing on three areas: cybersecurity, data privacy and related regulations and standards over ACSs. Our added value and main contributions are summarised as follow:

- A comprehensive review and a classification of attack surfaces and how they are exposed to potential threats per the heterogeneous nature of ACSs.

- A mapping between the attacks and their corresponding mitigation strategies by recommending a combination of countermeasures per attack type based on an overview of the advantages and disadvantages of each mitigation scheme.

- Advocate a set of security and privacy regulations and guidelines that the stakeholders should bear on to have a valid approach on protecting the ACSs system.

- Elevate the existing privacy preserving schemes further by discussing their strengths and weaknesses and how they are applicable to the exchanged data within the ACS ecosystem.

- Based on a thorough investigation of road vehicle, safety, vehicular cybersecurity, data privacy, public transport, ITS and IoT related standards; a selection of up to date standards is provided to point out not only the published but also the under-development ones that are promising security and privacy by design deployment for the ACS.

This article addresses the following questions:

- RQ1: What are the existing cybersecurity and data privacy risks related to ACSs? Can a specific mapping between the threat vectors and the countermeasures help in accurately shielding the ACS' environment?

- RQ2: Would individuals' privacy remain preserved while using ACSs? Would the implementation of powerful privacy preserving protocols be enough to protect personal data processed within the ACS's system?

- RQ3: What are the technical and legal strategies to mitigate or reduce the identified risks? And what are their limitations?

- RQ4: Is there an existing framework or standards addressing the security compliance relevant only to ACSs?

The remainder of this paper is structured as follows: Section 2.3 discusses the related work and a comparison of the present work with those previously published. Section 2.4 presents an overview of classified cybersecurity threats. This section identifies two layers impacting security of the ACS: the in-vehicle equipment and external communications. It also presents the existing risk mitigation plans and the regulations covering such security threats. Section 2.5 gives an overview of data protection risks, the existing technical solutions to offset such threats and the regulatory frameworks aiming to preserve privacy within the ACS ecosystem. Section 2.6 describes existing standards and those under-development supporting the shuttle resiliency, including the protection from data privacy leakage. Section 2.7 acknowledges the present research limitations and provides a discussion over the future work orientation. Finally, Section 2.8 offers concluding remarks on the state of the art.

2.3 Related work

In recent years, few papers focused their interest on ACSs as a means of public transportation. Iclodean, Cordos and Varga [199] evaluated the safety and social implications related to the technological solutions implemented within ACSs. Ainsalu et al. [9] studied ACSs' energy efficiency and their legal framework with regard to civil liability. Although, research works did not address cybersecurity and data privacy concerns over ACSs.

Table 2.1: Related work comparison

Related Work	**Year**	**Scope**		**Cybersecurity**				**Data Privacy**			**Standards**		
		ACS	CAV	In-V. attacks	Ext. attacks	Mitigation	Regulations	Risk	Mitigation	Regulations	ISO	ETSI	Others
Iclodean et al. [199]	2020	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗
Ainsalu et al. [9]	2018	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗
Petit and Shladover [372]	2015	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗
Parkinson et al. [367]	2017	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
Cui et al. [98]	2019	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
Ren et al. [378]	2020	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗
Dibaei et al. [113]	2020	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗
Khan et al. [264]	2020	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
El-Rewini et al. [380]	2020	✗	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗
Kim et al. [269]	2021	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
Suo et al. [413]	2020	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗
Lonc and Cincilla [301]	2016	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗
Costantini et al. [91]	2020	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓
Schmittner and Macher [395]	2019	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓
This work		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Motivated by the safety risk of cybersecurity attacks in the vehicular environment, multiple literature reviews discussed security threats and data privacy concerns. Petit and Shladover [372] highlighted the consequences of remote or direct access attacks over CAVs. Parkinson et al. [367] addressed the challenges and knowledge gaps facing the IoV sector from cybersecurity vulnerabilities perspective. Cui et al. [98] presented the inter-relation between CAVs safety failures and security attacks; in addition to a broad mapping of potential attacks impacting the data privacy and their eventual countermeasures. Ren et al. [378] drew in depth threats related to sensors and in-vehicle communication networks. The authors stated security guidelines including recommendations for privacy preservation. Dibaei et al. [113] investigated attacks and defences to shield the automated environment while presenting detailed technical mitigation strategies.

Recent researchers have drawn more comprehensive frameworks, such as Khan et al. [264] and El-Rewini et al. [380], discussing potential attacks and their respective mitigation strategies with a particular focus on communication challenges. Kim et al. [269] presented a new classification of attacks and defences over CAVs. Suo et al. [413] presented cybersecurity threats through a fault tree view. They also classified the existing mitigation solutions through a layered view with a focus on location-based schemes to countermeasure the location leakages while communicating with the infrastructure.

The majority of the cited works have introduced few standards at glance or as an expected effort for the future work without a profound review of the standards' implication within the driverless vehicles' environment. Very few papers [301, 91] presented ISO and European Telecommunication Standards Institute (ETSI) as unique existing standardisation bodies related to the automated driving environment. The most detailed reviews were published by Schmittner, in collaboration with other authors [397, 395, 81, 309, 398]. Though, the efforts remain limited to the automotive cybersecurity risk management tools without an exhaustive identification of all existing regulations and standards.

Per the analysis from Table 2.1, we differentiate from the aforementioned works by:

- Focusing on the ACS as a special case of CAVs ecosystem.
- Presenting an in-depth analysis on attacks and mitigation strategies.
- Presenting an interdisciplinary and comprehensive approach regarding cybersecurity and data protection by connecting the technological cyber defences with the existing regulatory and policy privacy frameworks as well as the security standards.

2.4 Cybersecurity threats

To ensure safety and security of the ACS, it is crucial to depict the system attack surfaces and build the required shields accordingly. Academic researchers have been debating the different types of attackers, attacks, and attack surfaces to identify adequate mitigation plans.

Attackers can be internal or external, malicious or rational, active or passive and intentional or unintentional as described by Cui et al. [98]. The internal active attacker deploys an attack on purpose with an authenticated profile by sending malicious packets in the network (for example) while the external passive attacker is an intruder who is eavesdropping the system. On the other hand, a rational attacker seeks personal profit while an unintentional attacks occur by coincidence or due to an equipment failure.

Based on the attacker profile and type, similar works discuss two groups of CAVs related attacks. Petit and Shladover [372] presented the “Autonomous Automated” attack surfaces, defined as all in-vehicle surfaces through which an attack can be accomplished; and “Cooperative Automated” referring to infrastructure and communication surfaces which can be targeted by an attacker. Van Wyk et al. [439] classified the attack surfaces as internal (referring to in-vehicle devices, vehicle sensors, and in-vehicle networks) and external (like communication interference with other vehicles and devices). As a result, our work was built on the categorisation of two cybersecurity layers as potential attacks entry points impacting the ACS ecosystem:

- *In-vehicle threats*: defining any in-vehicle component through which an attack can be conducted. It covers the potential vulnerabilities on the vehicle sensors, the ECUs data flows and in-vehicle communication networks as described in Figure 2.1.
- *Communication threats*: refer to the communication with, public transportation and city infrastructure (V2I), other vehicles (V2V), and any surrounded devices or services (V2X) as shown in Figure 2.2.

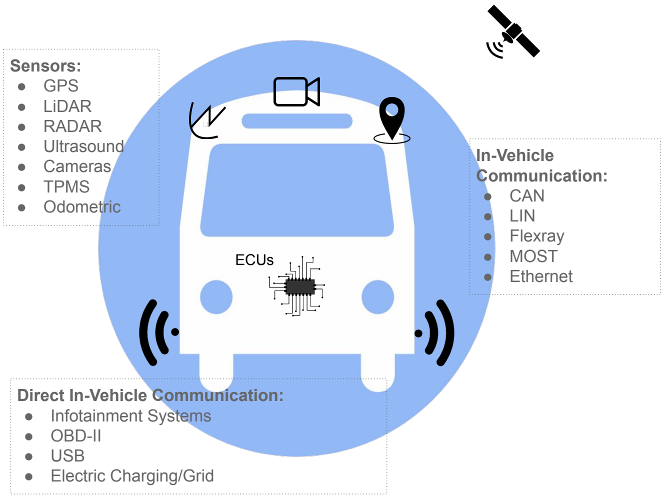


Figure 2.1: In-vehicle attack surfaces.

2.4.1 In-vehicle threats

In-vehicle sensors

With the absence of the human driving in the ACS, the passenger's safety depends completely on the vehicles' sensors and their interpretations to the collected inputs. Based on such information, the ACS builds a picture of its surroundings to drive in the correct path, detects obstacles in a real time manner and, hence, avoid collisions [449]. Sensors are expected to have numerous advantages to the automated driving [373]. However, they can be victims to potential security breaches. Considerable collections of research identified attacks targeting the in-vehicle sensor systems [462, 367, 378, 449, 392]. This subsection presents the most discussed in-vehicle sensors vulnerabilities and the most known attacks on them as summarised in Table 2.2.

Table 2.2: Sensors threats summary.

Sensor	Signal Type/Inputs	Automated Driving Function	Attacks Types	Demonstration Reference
GPS	Microwave	Navigation	Spoofing Jamming	[466] [105]
LiDAR	Laser Pulses	Behaviour prediction Collision avoidance Pedestrian detection Object recognition	Spoofing Jamming Relay Tampering	[78] [63] [373]
RADAR	Radio waves	Collision avoidance Object recognition	Spoofing Jamming	[462] [392]

Continued on next page

Table 2.2: Sensors threats summary. (Continued)

Acoustic/ Ultrasonic	Ultrasound waves	Parking Backing	Spoofing Jamming Quieting	[462] [461]
Cameras	Visible Light	Pedestrian detection Object recognition Lane detection Traffic sign detection	Blinding Fooling	[462] [373]
TPMS	Tire Measurements	System decision	Falsifying Tampering	[102]
Odometric	Data fusion	Navigation Orientation	Fooling	[426]

Global Positioning System (GPS), which is a widely used GNSS, provides positioning, navigation and time services to ACSs [123]. Accurate GPS positioning data is one of the critical inputs enabling safe self-driving, yet such technology has been potentially concerned with cyber-attacks [289]. Spoofing and jamming are the most common GPS attacks leading to disrupt sensor readings. A spoofing attack happens when an incorrect but valid GPS signals are sent to mislead the positioning [466]. In the recent simulation of Dasgupa et al. [105], a sophisticated spoofing attack was conducted by mimicking GPS signal and broadcasting falsified location coordinates. On the other hand, a jamming attack occurs when noise is transmitted on the GPS frequency preventing the GPS from distinguishing the accurate signals [367].

Light Detection and Ranging (LiDAR) is a key sensor to automated driving in any light condition. The sensor provides functionalities such as behaviour predictions, collision avoidance, pedestrian detection and object recognition [78]. LiDAR offers a 360° view and 3D perception by firing laser pulses, getting back their reflections and hence perceive a point cloud used for object detection [63]. Several researchers recorded LiDAR's vulnerability to spoofing, jamming, relay and tampering attacks leading the vehicle to assume nonexistent obstacles and to a halt. Cao et al. [63] demonstrated a successful spoofing attack by replaying laser pulses from a malicious device at the roadside and hence creating an erroneous point cloud. Petit et al. [373] conducted remotely a successful relay attack by making objects appear either closer or further than they really are. In addition, LiDARs are vulnerable to data tampering attacks that can be launched from inside the vehicle [78]. Such attacks happen when a hacker gets access to the in-vehicle network interfaces like CAN and execute by modifying/tampering the LiDAR's point cloud. Changalvala and Malik [78] identified two types of data tampering attacks: Fake Object Insertion (FOI) and Target Object Insertion (TOD). As a matter of fact, when data is tampered either by inserting fake data (FOI) or by removing existing one (TOD), decision making units will be impacted leading the vehicle to a prompt halt [462, 367].

Similar to LiDAR, but using radio waves instead of laser signals, **Radio Detection and Ranging (RADAR)** provides the object recognition and collision avoidance functions to driverless vehicles [392]. ACSs use two main radar types: Short Range

Radar (SRR) to detect objects at short - called also Millimetre Wave Radar (MMW)- and Long Range Radar (LRR) for long distances (up to 150m) [462]. Additionally, RADARs support the automated driving by detecting the speed and direction of other objects heading toward it [392]. However, by using the same frequency band, the signal can be spoofed or jammed causing the vehicle to be fooled, to presume nonexistent obstacles or to fail in detecting objects as demonstrated by Yan et al. [462].

Acoustic sensors, called also ultrasonic sensors, work similarly to LiDAR and RADAR, but using ultrasound waves (called pings) instead of light or radio signals [461]. Such sensors are mainly used for backing up or parking purposes by sending high frequency sound waves to measure echoes to determine the distance to objects [392]. Researchers have demonstrated how acoustic sensors can be victims to quieting attacks, where noise and/or echoes can be eliminated, preventing the vehicle from receiving the echoes required to measure distance to objects [462]. Acoustic sensors can be spoofed or jammed causing the vehicle to hit unperceived surroundings, as demonstrated in Tesla S by Xu et al. [461].

In addition to GPS, LiDAR, RADAR, ultrasonic, and other sensors, **cameras** are required to insure safe automated driving, though, they can be blinded or fooled too. Yan et al. [462] demonstrated how cameras can be blinded or permanently damaged with malicious optical inputs (laser and LED) using low cost resources. The authors named the demonstration “blinding attack” causing undesired vehicle breaking or deviation from planned trajectory or road navigation. When blinded, important functions to the automated driving are disrupted such as lane detection, traffic sign recognition, pedestrians or any other physical obstructions [367]. Petit et al. were also successful to blind the vehicle cameras using a simple laser pointer, disabling the vehicle from detecting the vehicle ahead [373].

Tyre Pressure Monitor Systems (TPMS) is another vulnerable small sensor which is essential in all vehicles, including non automated ones [367]. The TPMS broadcasts non-encrypted tire measurements like air pressure and temperature to the TPMS ECU [102]. Since the transmitted data is not encrypted, the sensor can be easily attacked as the message can be replaced by a false one or modified to hide important tyre information.

Odometric systems include wheel encoders and gyroscope sensors which are used for inertial-odometric navigation [372]. Such equipment aims to compute the vehicle position and movement by fusing data from the wheel readings (rotation and velocity) and the vehicle sensors (GPS, RADAR) to predict changes in position [426]. Obviously, if falsified data is computed, the vehicle orientation is impacted, leading to a wrong system decision making.

In-vehicle communication

The in-vehicle communication occurs by transmitting messages between the vehicle ECUs, the vehicle ports and the infotainment systems [380]. Such messages' transmission is enabled by the vehicle bus systems. This section highlights the threats related to the vehicle internal communication system.

The discussed attacks in Section 2.4.1 might impact implicitly or explicitly the vehicle **ECUs** which are vulnerable to direct attacks too. ECUs are the most important in-vehicle component as they are controlling the vehicles' system and subsystems by receiving and processing broadcast signals from the sensors [363]. Compared to non automated vehicles, the number of ECUs has been incremented in ACSs as they are responsible for the automated driving decisions [273]. With the increased number of ECUs, the lines of codes are expended too, enlarging the risk to code vulnerabilities [367].

ECUs communication occurs by exchanging network packets through heterogeneous in-vehicle communication protocols such as CAN, Local Interconnect Network (LIN), Media-Oriented System Transport (MOST), FlexRay and Ethernet [363, 102]. Each protocol supports different communication within the vehicular network; however, they embed multiple security concerns. Researchers showcased multiple attacks such as Denial of Service (DoS) [380], packet injection [330], sniffing / eavesdropping [113], spoofing [462], relaying, and bus-off [79] over the in-vehicle communication networks.

CAN buses are famous for their low cost, high bandwidth and flexibility; though, they were not designed with high security concerns [458]. First, the packets can be easily sniffed or falsified since they are broadcast into all nodes without containing any authentication information [78]. Second, the malicious packets can't be back-traced as the packets are not associated with a CAN ID [363]. The Keen Lab identified 14 vulnerabilities and demonstrated an attack over the BMW X5 where the vehicle was completely controlled by getting access to its CAN bus [471]. Upgrades have been rolled out by the car manufacturer; though, with the increase of wireless communications on ACSs, further attacks might be witnessed if CAN's vulnerabilities are not adequately addressed.

LIN may substitute the CAN for transmissions where high bandwidth is not required [380]. It is a cheaper communication protocol that is mainly used for the vehicle control (like seats and doors) and which communicates in a master-slave mode [125]. Hence, if the master node is compromised, false data is then sent to all the LIN slave nodes as demonstrated through a rogue attack by Ernst and Michaels [125]. Takahashi et al. demonstrated that the response collision and header collision attacks are occurring when messages are not synchronised between master and slave nodes leading to undesired vehicle controls like keeping doors open [416].

The security of CAN and LIN buses has been rigorously studied, however the other in-vehicle networks are subject to malicious intentions too. **Flexray** is designed to be the next generation of the in-vehicle communication protocol with its high reliability and data rates; though, like CAN, it lacks confidentiality and authentication implementation [378]. Flexray transmission has static and dynamic segments which are vulnerable to spoofing, eavesdropping, injection and replay attacks [380, 378, 113]. Additionally, **MOST** is mainly designed for media transfer with its high data rate that is considered 10 times faster than the Flexray and 100 times higher than the CAN [125]. The communication in the MOST is synchronised by time frames which makes it vulnerable to jamming or DoS attacks if the synchronisation is disrupted [380]. Last but not least, **Ethernet** is another promising protocol providing cost and bandwidth advantages [458]. Like in normal computer networking, Ethernet consists of hosts and switches which may add more vulnerabilities to the vehicle if attackers access to an open port on a switch. Hence, once access is gained, any further attack can take place like DoS, sniffing or falsifying impacting the confidentiality and integrity of the vehicle [380].

Additional **physical ports** can present the point of entrance of an attack over the in-vehicle network. On-board Diagnostics System (OBD-II) port is designed mainly for the vehicle monitoring and system upgrading. However, if accessed by a malicious actor, all the vehicle data can be gathered and any of the listed attacks in Table 2.3 may occur [264]. Moreover, USB ports present additional risks in modern vehicles, generally, and ACS, specifically, as attacks can inject malware and viruses into the system leading to endless attacks scenarios [317]. Furthermore, the electric charging port has been studied as an additional attack surface. Bhusal and Benidris [47] highlighted the risks of Man in the Middle (MitM), DoS, and false data or malware injection through the electric charging systems and the plugging into the grid.

Finally, the in-vehicle communication networks can be attacked through the vehicle **infotainment system** which offers user-friendly functions and an integration with smartphone applications [363]. They are systems combining information and entertainment through pairs applications where one is executed in-vehicle and the other one on an external device like a smartphone. Such systems are connected to the CAN bus which makes it an entry point to a malicious packet injection as demonstrated by Mazloom et al. [325].

2.4.2 Communication threats

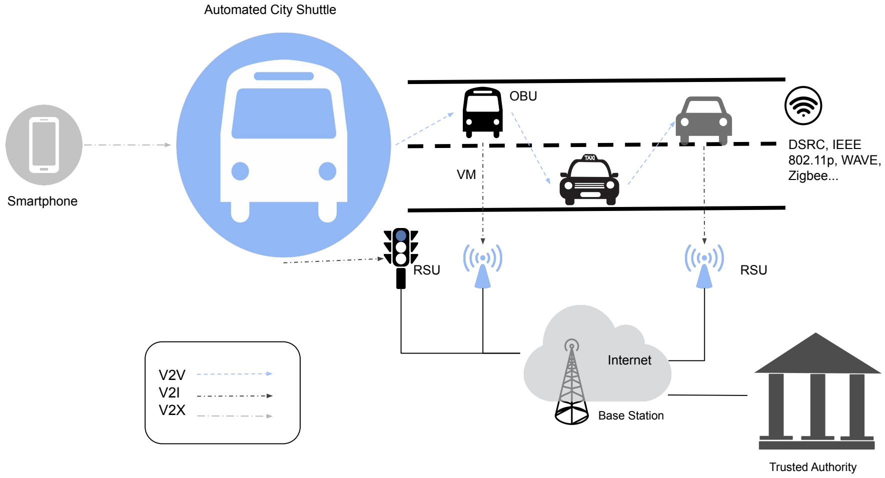


Figure 2.2: ACS communication modes.

Connectivity to external entities complements the in-vehicle components to achieve the automation of the ACS. Such connectivity is built through multiple channels: radio (AM/FM/DAB/RFID), WIFI (IEEE 802.11), Bluetooth, cellular (3/4/5G), bidirectional communication (IEEE 802.11p, Dedicated Short Range Communications (DSRC), Wireless Access in Vehicular Environments (WAVE)) and, in some cases, IoT networks (IEEE 802.15.4, Zigbee) [380, 317]. With the presence of wireless connections, Vehicular Ad Hoc Network (VANET) can be spontaneously created among connected and moving vehicles [287]. Initially, such ad-hoc networks were connecting only vehicles leading to V2V communication mode. Although, with the increase of modern concepts, infrastructure and additional devices, V2I and V2X were required to assist the VANETs for data storage and data transmission for long distances [287]. Nevertheless, being hyper-connected by nature, ACS environment has to deal with additional cybersecurity breaches highlighted as communication attack vectors in this section and in Figure 2.2.

Vehicle-to-Vehicle (V2V)

V2V provides means for ACSs to connect to other vehicles to broadcast traffic conditions and share the predictions and information within the VANET range [367]. V2V technology is mainly supported by DSRC and WiFi which raises the risk of security breaches [123]. Relying on the weaknesses of communication technologies, numerous attacks such as jamming, bogus information, sybil, impersonation and timing can be conducted [380, 46, 113]. Baqer and Krings demonstrated how the loss of messages on V2V due to jamming can make the vehicle invisible within the ad-hoc network [33]. Performed on wireless networks, bogus information attack occurs when incorrect information is transmitted pushing other vehicles to change their path while freeing the way for the attacker [380]. Gu et al. [190] demonstrated a sybil attack which happens when a vehicle declares itself as multiple ones, either to create congestion or congestion-free routes. Furthermore, a timing attack takes place when a malicious vehicle adds time delay to a received message, then forward it back to other vehicles, causing accidents due to the non-real time inputs [113].

Vehicle-to-Infrastructure (V2I)

This communication is illustrated by the data exchange between on-board unit (OBU) (also called on-board equipment (OBE)) and road side unit (RSU) [380]. Located at the ACS, OBU sends and receives messages to RSUs using virtual machines (VM) as secure cloud connections [123]. Messages sent from OBU to RSU through VM (also called beacon messages) may contain the vehicle velocity, location and pseudonyms. Such messages can include Cooperative Awareness Messages (CAM), Decentralized Environmental Notification Messages (DENM) or Basic Safety Message (BSM) where CAM and DENM are mainly used in European standards while BSM is used in United States of America (USA) [281]. However, if eavesdropped by an attacker, location information in DENM or vehicle information in CAM can be inferred leading to a mapping attack where location privacy leakage is occurring [256]. By making an RSU unable to function, Maple et al. [317] pointed out the risk of DoS attack, hardware tampering and disabling attack. Dibaei et al. added the risk of replay attacks over the communication with RSUs by repeating or delaying valid transmission data [113].

Furthermore, V2I embeds the communication between ACS and Trusted authorities (TA) systems [372] which represent an additional attack surface. Initially, the TA role is to generate short term certificates and public/private keys to verify the exchanged traffic messages [12]. In a scenario of an attack, invalid messages through fake certificates would lead the TA systems to failure to warn about a crash for example [372].

Vehicle-to-Everything (V2X)

This communication mode wraps both V2I and V2V technologies and respectively the attacks risks. V2X also compasses cloud and edge servers communication in addition to any further devices or peripherals interacting with the vehicle such as smartphones, car keys or Bluetooth devices [372]. V2C and V2P are additional vehicle communications classifications highlighted by Lozano and Sanguino [303] and considered as a part of V2X. Maple et al. [317] described further attacks like DoS, black hole and MitM that can be conducted over the vehicular network through a cloud connection and edge servers. Pan et al. [363] demonstrated a smartphone attack by connecting an Android mobile phone to the vehicular system and injecting malicious CAN data through Bluetooth connection.

2.4.3 Mitigation strategies

Table 2.3: High level summary of attacks and their corresponding mitigation techniques.

Attack	Attack surface	Mitigation	References
Spoofing	GPS, LiDAR, RADAR, Acoustic sensors, In-vehicle networks	Redundancy, Randomisation, Cryptography, BC, MDL	[289, 31, 400, 399, 45]
Jamming	GPS, LiDAR, RADAR, Acoustic sensors, In-vehicle network, V2V	Redundancy, Cryptography, Firewalling, BC	[372, 380, 371]
Relay/Replay/ MitM	LiDAR, Vehicle Ports, In-vehicle network, V2V, V2X	Redundancy, Cryptography, Firewalling, BC	[113, 371, 266]
Tampering/ Falsifying	LiDAR, TPMS, Odometric sensors, V2I	Redundancy, Cryptography	[102]
Quieting	Acoustic sensors	Redundancy, Fusion	[462, 461]
Blinding	Cameras	Redundancy	[367, 373]
DoS	In-vehicle networks, Vehicle ports, V2I	Redundancy, Cryptography, Firewalling, BC, IDS	[380, 458, 13, 371]
Sniffing	In-vehicle networks, V2X	Cryptography, BC, IDS	[358]
Malware Injection	In-vehicle networks, Vehicle ports, V2X	Cryptography, IDS	[467, 317]

Continued on next page

Table 2.3: High level summary of attacks and their corresponding mitigation techniques. (Continued)

Rogue	In-vehicle networks	Cryptography, IDS	[125]
Bus-off	In-vehicle networks	Cryptography, IDS, MDL	[257]
Eavesdropping	In-vehicle networks, V2I	Cryptography, IDS	[378, 266]
Bogus Information	V2V	Cryptography	[380]
Sybil	V2V	Cryptography	[113, 380]
Timing	V2V	Cryptography, Firewalling	[113, 46, 266]
Impersonation	V2I, V2X	Cryptography	[113, 264]
Black hole	V2X	Cryptography	[113, 264]

As ACSs' related threats have been identified in Sections 2.4.1 and 2.4.2, it is important to recognise existing defences and mitigation solutions against them. As described in Table 2.3, many researchers highlighted the advantages of redundancy and cryptography to countermeasure spoofing, sniffing, jamming, replaying, and tampering attacks [78, 102, 31, 266, 347]. Others focused on newer trends such as BC, IDS and MDL to detect abnormal behaviour and, hence, circumvent the security challenges [113, 380, 191, 358]. Besides, classical prevention techniques such as firewalling and network segmenting remain essential to restrain the occurrence of jamming, DoS or MitM attacks over in-vehicle networks [371] or cloud communications [317]. By considering the advantages and disadvantages of each mitigation technique, the present work agrees on the requirement of adapting and combining multiple defences in addition to the consideration of the human factors to shield the ACSs.

Redundancy, fusion and randomisation

Anomalous sensor readings can be improved by sensor redundancy [462]. In case of a GPS jamming, the combined data from other sensors, like LiDAR and RADAR, can cross-validate the initial measurement for the same parameter, maintain the vehicle navigation until the GPS signal is back and, therefore, discard the attack consequences [439]. Redundant cameras can also countermeasure the cameras' blinding attack. By multiplying the number of cameras and locating them in different points, the vehicle can continue operating even if one of the cameras is blinded [367]. Petit and Shladover [372] highlighted the advantages of redundancy as a mitigation solution to jamming, yet the additional equipment or processing for fusing data would certainly increase related costs and computations overhead.

Moreover, introducing randomness into RADAR, LiDAR and ultrasonic sensors would reduce the spoofing risk [378]. Shin et al. [400] assessed that by emitting signals in random instants, the attacker can no longer induce multiple fake dots.

Cryptography

In connected automated driving environment, encryption is a crucial strategy to ensure security and, thus, safety. On a vehicular network, the vehicle needs to be securely authenticated using key encryption algorithms to communicate with RSUs, OBUs and to get TA certifications [113]. Symmetric Key Schemes (SKS) and Asymmetric Key Schemes (AKS) can assure secure authentication of the vehicle within the VANET and protect from attacks such as replay, sybil and impersonation [113]. In SKS, which is also called secret-key encryption, it is assumed that the sender and receiver nodes share a single key that is used for both encryption and decryption [340]. Advanced Encryption Standard (AES), Data Encryption Standard (DES), Tiny Encryption Algorithm (TEA), International Data Encryption Algorithm (IDEA) are examples of SKS providing high security against attacks like MitM [266]. AKS also known as Public Key Cryptography (PKC) is an approach used to build secure communication between two or more nodes where the sender encrypts the message using the public key and the receiver decrypts it using his private key [347]. The AKS include Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH) and Elliptic Curves Cryptography (ECC) which have been proven to strengthen the system again attacks like timing and eavesdropping [266].

As discussed in Section 2.4.1, messages exchanged among ECUs are in general neither encrypted nor authenticated. Potential authentication techniques using Message Authentication Code (MAC) have been investigated to countermeasure attacks over the in-vehicle networks such as CAN [418] and LIN [416]. Such solutions may employ SKS and AKS to authenticate the sender ECU, initiate the message exchange and let the receiver ECU detect the attack [380]. Nguyen et al. [346] introduced quantum cryptography based on SKS to detect intrusions and secure the communication between ECUs and the CAN. Though, calculation time should be considered in order to limit the traffic overhead [418, 191].

Not limited to network attacks only, it has been showcased that cryptography reduces attacks on sensors and protects the ACS ports. Daimi and Saed [102] suggested the replacement of regular sensors (like TPMS) with more performing ones which contain processing resources for authentication and encryption functionalities. Bailey [31] demonstrated the efficiency of cryptography on limiting the GPS spoofing. El-Rewini et al. [380] added that SKS and AKS would prevent from injecting malware through OBD-II, USB and electric charging ports.

Despite their advantages, encryption algorithms may cause latency and impact the network efficiency due to their computational complexity [78, 347].

Blockchain

To reduce the implementation burden of cryptography, BC has been introduced as a promising defence which increases the authentication on the VANETs, in-vehicle communication and the accuracy of GPS positioning [113]. BC is a distributed ledger technology made of connected data blocks which verify the state of component (like ECU for example) based on a decentralised consensus [352]. In other words, as the blocks of data are protected by the consensus protocols, the distributed nature of the BC makes it difficult to conduct an attack [80]. Li et al. [289] proved how their proposed blockchain-based GPS model provides accurate positioning data even in the case of a GPS spoofing or jamming. Oham et al. [358] demonstrated the BC efficiency on monitoring the in-vehicle network and detecting attacks over it. Gupta et al. [191] discusses the advantages of integrating BC to the CAV architecture by emphasising on how it countermeasures the limitations of cryptography within the driverless system.

Intrusion Detection System and Machine and Deep Learning

IDS has been judged as the most reliable countermeasure to VANET [468] and in-vehicle communication threats [380]. It aims to detect and isolate anomalies while monitoring the network traffic. The IDS can be deployed either by detecting predefined attacks through the signature-based detection techniques; or by distinguishing a behaviour change through the anomaly-based detection method [200]. The signature-based detection identifies the attack by comparing the attack case to a database of signatures of already known attacks [200]. The anomaly-based detection can incorporate machine learning methods to train itself on normal behaviours, then anything that is different from the expected cases will be detected as an attack [113]. Wu et al. [458] and Ali Alheeti and Mc Donald-Maier [13] demonstrated the efficiency of the IDS over network attacks like DoS. Further research works extended the IDS to be collaborative and distributed within the VANET which enables knowledge sharing among vehicles while reducing storage and workload burden [468].

Multiple studies detected anomalous behaviour using MDL theories. Van Wyk et al. [439] presented a real-time anomaly detection by combining a deep learning technique (Convolutional Neural Network (CNN)) with Kalman filtering [405] which provides high accuracy for automated driving environment. The authors' generic framework was proved to detect anomalous behaviour originating internally from in-vehicle sensors, or externally from an OBU or/and an RSU. In addition, Kang and Kang [257] demonstrated the efficiency of Deep Neural Network (DNN) in monitoring and detecting attacks over the CAN bus. Further researchers [399, 45] showcased the efficiency of their models based on Bayesian Network as a deep learning theory to monitor attacks from sensors. Khanam et al. [266] assessed the advantages of additional MDL algorithms, in detecting network spoofing and DoS attacks within the IoT environment, such as Recurrent Neural Network (RNN), Artificial Neural Network (ANN), Deep Belief Network Network (DBN) and Support Vector Machine (SVM).

Software vulnerability detection

With the high risk of code intrinsic vulnerabilities on ECUs and any software embedded to the automated driving system, static and dynamic analysis, in addition to MDL methods have been mainly used for software vulnerability detection. Static analysers are used to check the program without executing it, while the dynamic techniques check the code during the program execution [113]. Pattern matching, lexical analysis, parsing, control flow analysis and data flow analysis are examples of static methods providing short analysis time but with high false positive rate [164]. On the other hand, fault injection, fuzzing and dynamic taint analysis illustrate dynamic analysis mechanisms granting higher accuracy but with a longer analysis time [270]. However, static and dynamic analysis have been considered as traditional methods by considering their drawbacks and tend to be replaced by machine deep learning methods. Russell et al. [383] and Li et al. [292] trained the MDL algorithms and demonstrated their effectiveness on software vulnerability detection. Jeon, Park and Jeong [253] used CNN to detect new and variant malware within the IoT environment.

Further solutions supporting technical mitigation techniques

An indirect, but interesting defence to V2X cyber risks, would be the 5G new communication technology. It is true that 5G may inherit some of the 4G vulnerabilities as few specifications remain unchanged from the precedent protocol; though, it provides higher bandwidth which facilitates the encryption and authentication implementations without causing network latency [80]. Dibaei et al. [113] added that the ultra-low latency and real-time response features of the 5G would enable real time warnings and attacks detection within the V2X environment. Nevertheless, Ahmad et al. [8] warned about further known and unknown threats caused by the 5G that CAVs would have to cope with as additional threats.

In addition to technical solutions, human factors can contribute to build defences within the vehicular environment. Linkov et al. [297] highlighted the fact that human behaviour during cyber attack should be taken into account when designing ACSs and when recruiting operators working on them. The authors added that cybersecurity can be improved by considering human factors such as workload, knowledge and training about cybersecurity risks. Operators who are informed about the cyber attacks risks and who had training on secure authentication and phishing would behave more securely.

Marksteiner and Ma [320] assessed that testing is very important in the security development, though, it is mainly conducted by in-house pentesters, and their results depend on the human skills and the manufacturer budget. With the trend of minimising human intervention, researchers such as Chu and Lisitsa [82], Johari et al. [254] and Casola et al. [66] introduced automated pentesting models within IoT and proved their efficiency on both code and network vulnerabilities. However, the authors approach is limited to known threats while powerful criminal cyber attacks took place usually over unknown vulnerabilities [433].

Hence, OEMs and the public transportation companies should take into consideration findings related to human factors while forming their ACSs' teams by emphasising on collaborators' cybersecurity risk knowledge and awareness.

To that end, the ACS's stakeholders should carefully deploy the accurate mitigation measures based on the embedded systems within the vehicle and the mini-buses connectivity modes supported by the VANET. Nevertheless, the countermeasures can not be limited to technical and human defences as organisational regulations can be combined to the aforementioned discussed solutions for an optimal vehicle shielding, as described in the following subsection.

2.4.4 Cybersecurity regulations

Cybersecurity should be considered while deploying every piece of hardware and software on the ACS to avoid the aforementioned threats. In addition to the technical countermeasures, governments, regulatory bodies and information systems institutions can contribute on building secure ACSs' environment. It has to be mentioned that there are not many mandatory legal frameworks incorporated in the legal systems in the field of cybersecurity, let alone in specific sectors such as transport. Though, many stakeholders including OEMs, regulatory bodies, IT and telecommunication suppliers, operators of ITS, and mobility service providers collaborate and establish new regulatory approaches, strategies and guidelines. In this section, we highlight global efforts, with a focus on Europe, in building cybersecurity legal frameworks and guidelines for the automated driving landscape as summarised in Table 2.4. The table highlights the regulations and their regulatory bodies, their locations and date of entry into force. The table also lists the regulations based on their types to be either a law (a mandatory act), guidance (a statement of advice pertaining to practice) or recommendation (a statement of practice) [362].

European Union

CAVs stakeholders have been encouraging "Regulatory Sandboxes" and "Living Labs", where new technologies are tested accordingly to the legal requirements by predicting undesired consequences and through a learning-by-doing approach [91]. C-ROADS [59] platform illustrates such labs in Europe supporting on testing and implementing the European Strategy on Cooperative Intelligent Transport Systems (C-ITS) since 2016. Furthermore, the Connected, Automated and Autonomous Mobility (CCAM) single platform was launched in 2019 by the European Commission for supporting on open road testing including activities related to connectivity, digital infrastructure, cybersecurity and access to in-vehicle data [146, 157, 156].

Based on such labs' findings, the first EU-wide law on cybersecurity, the Directive (EU) 2016/1148 [422], known as "NIS Directive", came into force. This directive defines measures for a high level of network security and information systems across the EU. The "NIS Directive" covers the vehicles' cybersecurity issues under its generic security scope for preventing and minimising the incidents and attacks impact. In December 2020, new proposals were published with an updated version called "NIS 2" [423]. Both directives call the operators of essential services and the digital services providers to take the appropriate and proportionate technical and organisational measures to manage the risks posed to the security of information systems.

More specific to the road transport sector, European Union Agency for Cybersecurity (ENISA) came up with guidelines on implementing the NIS Directive. ENISA published multiple reports depicting the key challenges and requirements for smart cars and smart cities from cybersecurity perspectives [155, 154, 158, 157, 159]. Among the European Commission's efforts, the Joint Research Centre (JRC) has set up a security Public Key Infrastructure (PKI) model for a safe V2X communication [142]. ENISA and JRC published their latest report in February 2021 discussing AI specific cybersecurity challenges related to automated driving environment [156].

By taking into account ENISA's recommendations, the European Automobile Manufacturers Association (ACEA) identified key principles for cybersecurity protection against attacks on CAVs emphasising on implementing cybersecurity requirements through every stage of the vehicle development lifecycle [138]. In 2019, ACEA published a roadmap for the deployment of automated driving in the EU spurring OEMs to self-audit, testing, and deploying incident response plans [139].

United Kingdom

According to KPMG's CAV readiness index, the United Kingdom (UK) was ranked as number one in the world in 2020 for cybersecurity in terms of regulations efforts [280]. In 2015, the Department for Transport in the UK published "The Pathway to Driverless Cars" as good to have practices, on automated driving, highlighting cybersecurity risks and privacy issues [112]. In 2017, the UK government presented the eight key cybersecurity principles for CAVs pointing out the importance of organisation security management, system resiliency and risk assessment throughout the vehicle lifecycle using a defence-in-depth approach [196]. In 2018, the UK's first legislation on CAVs titled "Automated and Electric Vehicles Act 2018" came into force [186]. Considering the quick progress of the driverless ecosystem, the British government launched a second consultation on exploring the regulation of secure ACSs [425]. Furthermore, the UK government's efforts contributed to the development of the British Standards Institution (BSI)'s standards discussed later in section 2.6.6.

United States of America

In January 2020, the Department of Transport (DOT) shared a report titled "Ensuring American Leadership in Automated vehicle Technologies 4.0" [344]. From the report, the USA government highlighted their efforts with different stakeholders to ensure security and cybersecurity mechanisms through successful prevention, mitigation and investigation of security threats targeting the driverless ecosystem. The report further assessed the NHTSA mission on developing and updating cybersecurity best practices. Since 2016, the NHTSA shared a voluntary guidance to strengthen motor vehicle cybersecurity and protect the electronic systems from potential attacks, which was updated in 2020 [348, 415]. The updated guidance consists of general cybersecurity requirements like vulnerabilities reporting, incident monitoring and responses in addition to self auditing. The NHTSA guidance includes also technical cybersecurity best practices like the implementation of PKI certifications, encryption keys and secure software updates [350]. Besides, Automotive Information Sharing and Analysis Center (Auto-ISAC) is an alliance of global automakers who joined their forces to develop and upgrade a series of best practices with the evolving of CAVs ecosystem. Similarly to NHTSA, the Auto-ISAC best practices focus on cybersecurity general requirements like threat detection, monitoring and response in addition to security development lifecycle considerations [25].

Japan

In 2013, the Japanese Information-Technology Promotion Agency (IPA), published a guidance paper where the in-vehicle threats and countermeasures are mapped [274]. The publication includes also a checklist for vehicular developers on how to mitigate particular attacks like DoS. The IPA recommendations are presented through a mapping of four security levels to the automotive system lifecycle including management, planning, development, operation and disposal. Even being dated, the IPA guide is much applicable and serves as a background to the Japanese guideline, JASO TP-15002, published in 2016 by the Society of Automotive Engineers of Japan (JSAE). JASO TP-15002 recommends a security analysis process of five phases focusing on security evaluation and major security risks mitigation [262]. Further notable collaborations between JSAE and Japan Automobile Manufacturers Association (JAMA) led to the creation of the Japan Automotive Software Platform and Architecture (JASPAR) [252] and a Japanese Auto-ISAC [251] focusing on local specific cybersecurity and information sharing issues related to ECUs and in-vehicle networks [327].

Intergovernmental recommendations

In an intergovernmental context, the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) [243] from the United Nations agency, has a working group focusing on developing security recommendations related to CAVs. Since 2017, their recommendations series (X.1371 to X.1376) cover security threats definition, security guidelines for V2X, specification of secure software update procedure for ITS's devices, guidelines for intrusion and misbehaviour detection as presented in details in Table 2.4.

Furthermore, UNECE working party WP29 adopted two new regulations on uniform provisions concerning the approval of CAVs with regards to cybersecurity and software update management systems [50]. The regulations known as "UN R155" [430] and "UN R156" [431] were adopted in June 2020 and came into force from January 2021 to offer a practical and holistic approach to automotive cybersecurity. The two regulations cover the cybersecurity risk management, security by design, security incidents detection and mitigation, and secure software updates over the CAV lifecycle including development, production and post-production [410]. Among the two regulations requirements, certificate of compliance for software update management systems and CSMS has become recommended for vehicles with level three onward (according to the SAE automation classification) and for three years renewal [189, 81].

Table 2.4: Cybersecurity regulations summary.

Regulatory Body	Regulation	Type	Country	Date
European Parliament and the Council of the EU	NIS Directive 1 [422]	Law	EU	July 2016
	NIS Directive 2 [423]	Law	EU	January 2020
ENISA	Cyber security for Smart Cities [155]	Guidance	EU	December 2015
	Cyber Security and Resilience of Smart Cars [154]	Guidance	EU	December 2016
	Good Practices for Security of Smart Cars [158]	Guidance	EU	November 2019
	Cybersecurity Stocktaking in the CAM [157]	Guidance	EU	November 2020
	Guidelines for Securing the IoT [159]	Guidance	EU	November 2020
JRC	Certificate Policy for Deployment and Operation of European C-ITS [142]	Guidance	EU	December 2015

Continued on next page

Table 2.4: Cybersecurity regulations summary. (Continued)

ENISA and JRC	Cybersecurity Challenges in the Uptake of AI in Autonomous Driving [156]	Guidance	EU	February 2021
ACEA	Principles of Automobile Cybersecurity [138]	Guidance	EU	September 2017
	Roadmap for the Deployment of Automated Driving in EU [139]	Guidance	EU	December 2019
UK Government	The Pathway to Driverless Cars [112]	Guidance	UK	February 2015
	The Key Principles of Vehicle Cyber security for CAVs [196]	Guidance	UK	August 2017
	Automated and Electric Vehicles Act 2018 [186]	Law	UK	July 2018
DOT	Ensuring American Leadership in Automated vehicle Technologies 4.0 [344]	Guidance	USA	January 2020
NHTSA	Automated Driving Automated Driving Systems A vision for Safety [348, 350]	Guidance	USA	2016, 2020
Auto-ISAC	Best Practice Guide [25]	Guidance	USA	July 2016
IPA	Approaches for Vehicle Information Security [274]	Guidance	Japan	August 2013
ITU-T	X.1371: Security Threats to Connected Vehicles [244]	Rec.†	Intergov.⋆	May 2020
	X.1372: Security Guidelines for V2X [245]	Rec.†	Intergov.⋆	March 2020
	X.1373: Secure Software Update Capability for ITS Communication Devices [246]	Rec.†	Intergov.⋆	March 2017
	X.1374: Security Requirements for External Interfaces and Devices with Vehicle Access Capability [247]	Rec.†	Intergov.⋆	October 2020
	X.1375: Guidelines for an Intrusion Detection System for In-Vehicle Networks [248]	Rec.†	Intergov.⋆	October 2020
	X.1376: Security-related Misbehaviour Detection Mechanism using Big Data for Connected Vehicles [249]	Rec.†	Intergov.⋆	January 2021
UNECE	UN R155 [430], UN R156 [431]	Law	Intergov.⋆	January 2021

† Rec. = Recommendation.

⋆ Intergov.= Intergov.

2.4.5 Cybersecurity summary

To answer the RQ1, the present section provided a systematic categorisation of cybersecurity threats. Two main vectors were identified: in-vehicle, where the vehicle sensors and the in-vehicle communication attack surfaces were depicted; and external communication threats where the potential VANET's vulnerabilities are discussed. Spoofing and jamming were described as the most likely attacks to occur impacting several in-vehicle sensors. Even minor threats leading to non-accurate positioning or incorrect vision can make the vehicle perceive non-existing obstacles or hit disbelieved surroundings. Such consequences would definitely impact the safety and the acceptance of the ACS as a new public transportation mode. Regarding communication threats, either conducted directly or remotely, DoS and malware injection were assessed as the most destructive attacks that can be fatal in highly connected environments. Additionally, it is true that the more connections are built with the vehicle's external environment, the more sophisticated are the services provided by the ACS. However, more risks and attack surfaces have to be considered with the increase of the mini-buses' connections.

Several countermeasures were discussed and grouped into technical and legal mitigation strategies. From the technical perspective, redundancy, fusion and randomisation were recommended to cross-validate the data collected from the sensors and discard any malicious inputs. Moreover, the strength of cryptography was showcased against network attacks, in-vehicle or VANET communication's threats. Though, such mitigation solutions require additional equipment and involve computational overhead. As a matter of fact, we discussed more lightweighted countermeasures such as BC which reduces the implementation burden. Besides, as we believe that risk mitigation is not pertinent only until the occurrence of a cyberattack, this section also discussed monitoring and attack detection tools such as MDL.

From the legal perspective, the NIS directives represent the unique cybersecurity text laws in Europe even if they are applicable to all IT fields. More specific to CAV, the R155 from UNECE requires the implementation of the CSMS certification for all vehicles starting from SAE level three. It is true that such certification provides more control to the vehicle type approval process, although it remains generic as it is relevant to levels three, four and five of automation where safety and security risks are not comparable. Furthermore, ENISA and JRC represent good practices to follow for deploying CAVs in Europe. Similarly, the other cited institutions and regulators discussed recommendations with interesting security-by-design approaches. However, to the best of our knowledge, there is no formal published regulation dedicated to ACS which require a combination of the existing text laws and recommendations and an adaptation of technical solutions based on the vehicle nature and its connectivity maturity.

Consequently, the human presence has a crucial role on both mitigating and reacting to a cyber threat within the ACS landscape. By considering an ACS, of SAE level 4 of automation, multiple fatal situations can be avoided by a well trained operator aboard. Taking a case of a simple laser pulse attack where the vehicle can be blinded, the operator can take over and correct the vehicle navigation. Nevertheless, on an ACS of level 5 of automation, the vehicle decision making units must have the accurate mitigation strategies in place and run on a fail-safe mode to assure security and safety accordingly.

To that end, RQ3 has been partially answered through the review of technical and legal strategies mitigating cybersecurity threats. Apart from security concerns, data privacy represents another challenge to tackle within deploying ACSs. It is conspicuous that in the automated driving ecosystem, some cybersecurity attacks embed privacy leakage risks too. To complement the answer for RQ3, the following section covers data privacy concerns by identifying related risks, technical mitigation strategies and relevant personal data protection regulations.

2.5 Data privacy

With their hyper-connected nature, the ACS generates data permanently and spawns multiple challenges to their users' fundamental rights and to the protection of personal data and privacy. The shuttle's sensors, cameras, in-vehicle systems, its V2X communication and eventual embedded MaaS platforms, produce huge amounts of data, most of which is considered as personal data such as vehicle's location, video/audio surveillance and passengers' identities and positions. This practically means that personal data can be received by an unrestricted data controllers (recipients), whose intentions and technological capacity are not, and cannot be known to the data subject (users) [281]. Such situation creates concerns about the transparency, the proportionality and the necessity of data processing which requires higher level of personal data controls [20]. Moreover, being a part of the public transport system, ACSs may have more data controllers than CAVs , and hence further potential personal data leakage risks [9, 293].

The article 4 from the GDPR defines the data processing impacting personal privacy to be: data collecting, recording, organising, structuring, storing, adapting, alternating, retrieving, consulting, using, transmitting, disseminating, aligning, combining, restricting, erasing and/or destructing [424]. As a matter of fact, by processing the data, the personal information can be exposed to various threats which vary from intentional criminal breaches to economical and social purposes [260] [367].

Criminal threats are illustrated as intrusions, in-vehicle thieves' attacks, tracking attacks or vehicle behaviour's manipulation like attacks discussed on Section 2.4. On the other hand, data can be processed for social profiling, improving the commercial services through LBS/ MaaS or tailored advertising and hence generating social and economic benefits [293]. It can also help disabled people, elderly and young kids to be followed by their relatives [85]. In addition, collected data can contribute to the smartness of the city as it can reveal real time information on traffic, road condition and the CO_2 emission [260]. This non-criminal intention remains harmless and very important for the vehicle integrity; though, legal rights and data controllers have to be transparent to data subjects for any required data processing [367].

2.5.1 Technical mitigation solutions

Despite the intention, personal data recorded from ACSs has to be kept anonymous and encrypted wherever transmitted and securely stored. Cryptography and secure computation have been discussed in the literature as key technical solutions for preserving personal data and location privacy. Statistical and machine learning theories have been investigated as techniques that would preserve the data confidentiality and anonymity without ownership restrictions or usage agreements.

Cryptography for personal data protection

As discussed in section 2.4.2, privacy cannot be bypassed in VANETs as the vehicle identity and location are shared with RSUs, OBUs and TAs. Conditional Privacy-Preserving Authentication (CPPA) protocols have been introduced to make the TA as the only partner who can extract the real vehicle identity which may be hidden using signed messages or vehicle's pseudonyms [316]. Lu, Qu and Liu [304] assessed that the anonymity is assured by using PKI based authentication, identity based signature, certificateless signature or group signature as cryptography mechanisms. Based on AKS, Dibaei et al. [113] presented further privacy preserving protocols such as Group Signature and Identity-based Signature (GSIS) and Privacy-Preserving Group Communication Scheme for VANETs (PPGCV) providing robust privacy protection within the vehicular network. Though, as any authentication based schemes, computations and storage burden should be considered. Multiple researchers [193, 457, 258, 447] have introduced upgraded CPPA protocols and lightweight algorithms which guarantee privacy requirements with less computational and storage costs.

Additionally, encryption algorithms have been adapted for multimedia data to protect visual personal data. In video surveillance context, Asghar et al. [22] defined the encryption approach to be the process of translating, completely or partially, plaintext to ciphertext using SKS and AKS. Standard ciphers like AES were initially used for their level of security, though more specific video encryption and lightweight algorithms [464, 118, 334], came afterwards to adhere the multimedia requirements. Moreover, encryption theories have been combined to redaction-based techniques like scrambling to localise and encrypt recorded personal faces, however such algorithms require more storage considerations as they increase the video size [299].

Among cryptography solutions, Zero Knowledge Theory (ZKP) is a promising protocol that is based on an exchange of messages between the prover and the verifier where the prover has a secret but does not reveal information about it. However, the prover should provide more information about his secret to establish the trust with the verifier [446]. Theoretically, the protocol is powerful and efficient for cryptographic applications, but the iterations for finding required proofs remain unpractical and costly in real-world use. The ZKP theory was improved in [446] and [15] by reducing the number of iterations rounds and hence reducing its costs; though, the additional collected information by the verifier presents a risk for a future data leakage and again impacts the individual's privacy.

Location privacy protection

Lu, Qu and Liu [304] defined the location privacy risk to be the ability to link an entity's spacial information to its identity. The vehicle ID, timestamp and GPS coordinates that are transmitted within CAM and DENM messages (also referred to as beacon messages [441]), are mainly used for collision avoidance, transport services (MaaS), or customised LBS. However, if eavesdropped, beacon messages may be reused for malicious vehicle tracking, or to infer future vehicle movements based on its past locations [23]. [417] classified location protection mechanisms into two main groups and recommended their combination: anonymisation-based techniques where the identity is concealed and obfuscation-based schemes where the location is perturbed.

In anonymisation-based schemes, pseudonyms replace the vehicle real identity and are changed periodically per the vehicle speed and direction [304]. Such schemes are illustrated through Mix-zones or Silent approaches where beacon messages can't be easily eavesdropped as vehicles change their pseudonyms frequently [23]. Furthermore, Kang et al. [256] introduced pseudonym-changing synchronisation schemes to prevent from location leakage while communicating with RSUs using random identifiers.

Obfuscation-based schemes are used to make the unauthorised tracking difficult by decreasing the accuracy of location information on purpose [304]. Such schemes aim to perturb position and beacon frequency to increase the tracker confusion [23]. Lim et al. [294] demonstrated an obfuscation-based solution to confuse the tracker while the location privacy and the quality of LBS are preserved.

Statistical and machine learning protocols

Differential Privacy [120] and Randomised Response [450] techniques illustrate the promise of learning useful information about a population while the individuals privacy is conserved. By adding random noise to a set of data before learning from it, private inputs get hidden without impacting the result accuracy [345]. Additionally, the haystack privacy policy [255] is another efficient method preserving privacy using almost the same principle as Differential Privacy and Randomised Response, but with larger data owners participation. Applied to vehicular data, Zhang and Zhu [468] demonstrated a collaborative IDS on VANETs based on differential privacy while Joy and Gerla [255] showcased the haystack privacy theory over CAV's collected data. They assessed that such algorithms represent a new vision for privacy protection over vehicular training data sets.

Given the aforementioned theories, privacy can be technically assured. However, the presented techniques won't be enough if ownership rights and legislation are not well defined while using public ACSs. In the discussion that follows, the focus is on how individuals' privacy can be protected from legal perspectives, and what are the existing regulations controlling data governance to enhance privacy and confidentiality on ACSs without impacting their benefits.

2.5.2 Data privacy regulations

Personal data protection regulations govern the processing, usage, storage, and sharing of personal data. Those regulations have been identified also to give the opportunity to data subjects, as passengers in the case of ACSs, to consent or not to the use of their own personal information and to decide about the type of data and its relevant processing [183]. This section sheds light on the existing mandatory data privacy regulations (hard laws) in addition to existing soft law guidelines supporting the protection of personal information generated within the automated driving landscape as summarised in Table 2.5.

The EU Regulations and Initiatives

In the EU, the **Data Protection Working Group 4 (WG4)** of C-ITS analysed multiple options to deem lawful processing of personal data [420]. In the final report published in 2016, the WG4 assessed that the exchanged CAM and DENM (beacon messages) within the V2X environment, is personal data requiring legal and technical protection. Additionally, the WG4 highlighted the challenges on implementing the consent in practice [281].

Besides, the **Article 29 Working Party (WP29)** did further analysis on data privacy protection [20]. In 2017, the WP29 provided guidance on the processing of personal data in the context of C-ITS. Thereafter, the European Data Protection Board (EDPB), successor of WP29, published initially in January 2020 and updated in March 2021, guidelines highlighting privacy and data protection risks. The EDPB guide includes also recommendations on data protection by design and by default, in addition to a simulation of five illustrations of data processing within CAV environment [147, 149]. Moreover, the guidelines focus on consent as the legal basis for processing personal data inside the vehicle and through V2X communications [281]. The EDPB guidance incorporates both e-Privacy directive and GDPR [147]. Although the guidelines are referring to the processing of personal data in relation to the non-professional use of CAVs, it could be perceived as a valuable guide for the protection of personal data for the public ACSs as well [5].

The **e-Privacy Directive** [152] represents a mandatory standard applying to electronic communication networks and entities reading from a terminal equipment within the European Economic Area (EEA). Such terminal equipment can be identified as the ACS per the EDPB definition [147]. The e-Privacy directive sets rules of tracking technologies, and presents fragmentation of legislation with an alignment to GDPR [441].

The Regulation (EU) 2016/679 ("General Data Protection Regulation" GDPR [424]) replaced the directive 95/46/EC and contains provisions and requirements related to the processing of personal data in order to protect fundamental rights and freedoms of natural persons, the data subjects, and in particular their fundamental right to privacy and the protection of personal data. Inter alia, the GDPR identifies new data governance roles (data subjects, data controller, data processor and data protection officer) and introduces the accountability principle as the cornerstone of personal data processing.

According to the GDPR, the data should be processed lawfully and fairly under transparency and minimisation principles (art. 5 and 6) GDPR)[424]. In addition, the GDPR attributes rights to data subjects as well as obligations for the data controllers and data processors. The GDPR emphasises on data subjects rights which vary from rights to transparent information access (art. 12, 13 and 15), right to rectification (art. 16), right to erasure (art. 17), right to restriction of processing (art. 18), to right to be notified in case of data breaches occurrence (art 33 and 34). Any failure of the data controller and the data processor to comply with these principles and not to protect the rights of data subjects, may result in fines (article 83). Applied to the ACS ecosystem, the shuttle passengers and operators (if any) should be informed, with transparency, and provide their consent about all the processing applicable to their personal data in addition to being notified, under circumstances, when cyber incidents take place and their personal information may be leaked (or breached).

Moreover, the GDPR come up with technical and security commitments that should be considered by data controllers to guarantee data integrity and confidentiality. Articles 25 and 32 introduce the concepts of Privacy by Design and by Default requiring the implementation of risk management mechanisms and appropriate mitigation techniques such as encryption, pseudonymisation and data minimisation procedures from the outset [424]. The GDPR also recommends a data protection impact assessment (DPIA) as a useful practice within the design phase as detailed in articles 35 and 36 [149]. As far as the processing concerns personal data, the GDPR and the e-Privacy Directive are considered as the main regulations in the EU to protect individuals' data within any deployed technology [148].

Furthermore, based on GDPR and ePrivacy regulations, new initiatives and projects have emerged in the EU. One is **GAIA-X** [161] which has been merging to increase data transparency and user trust. GAIA-X was launched in 2019 by stakeholders from business, politics and science fields to provide proposals on data protection rules and architecture standards in many areas including mobility and smart cities [162]. **Data for Road Safety** is another initiative pushing for trustful and legal smart data exchange in the EU [106]. Data for Road Safety discusses connected vehicles of all automation levels and gathers partners from European Commission, industry, and governments to reach cooperative, trustworthy and free of charge vehicles data exchange with respect to the European regulations.

International initiatives

Not limited to the EU, some governments have either enacted laws on the protection of personal data or published guidelines that provide useful recommendations addressing privacy concerns in the automated driving environment. As CAVs had started entering the market, some countries (e.g. USA and Australia) have included automated driving concerns to their data protection regulations, while others (e.g. Japan) are still adjusting the broad laws that are not specific to driverless ecosystem, though applicable to the protection of personal data or privacy [91, 293, 415]. To illustrate, the **USA** government published dedicated acts for highly automated vehicles in a wide scope including ACSs. The S.2182 SPY Car [88] and the H.R.3388 Self Drive [87] Acts oblige OEM to develop written privacy plans prior to offering or importing CAVs. The acts highlighted that the privacy plan must be developed with respect to the collection, use, sharing and storage of personal data. Within the privacy plan, the vehicle passengers should be notified about the privacy policy unless the personal data is anonymised or encrypted. Similarly, **Australia** [24] published their dedicated regulations on protecting personal data within the automated driving environment. On the other hand, in **Japan**, Act on the Protection of Personal Information (APPI) [370] is the main data protection law but with a broad scope. The regulation came into force in May 2017 addressing the individual's information standalone or comprised with other data enabling the inference of the personal information which makes the law applicable to CAVs environment. According to articles 82 to 85 of the APPI, any violation of the act would lead to fines or imprisonment.

Intergovernmental initiatives

Additionally, at an intergovernmental level, the **UNECE** with its 56 governments as member states, made noteworthy efforts regarding the protection of personal data within CAVs environment. In 2016, the Informal Working Group on Intelligent Transport Systems and Automated Driving published guidelines proposal on cybersecurity and data protection [429]. The guidelines emphasises on data protection by default and by design. The report also assessed that data processing systems installed within an automated vehicle have to be data protection friendly. In 2019, UNECE published a framework document on CAVs where they identified the key principles of safety and security including Data Storage System for Automated Driving vehicles (DSSAD) [432]. The purpose of DSSAD is to establish legal data processing within a crash investigation context with respect of the national and regional data protection laws.

Furthermore, annual forums and international conferences contribute to setting the data privacy regulations for the driverless environment. In 2017, the **International Conference of Data Protection and Privacy Commissioners (ICDPPC)** adopted a high level resolution on CAVs where regulation bodies and OEMs were called to adopt privacy by design and privacy by default at every stage of the vehicle's devices and services development [198]. In a more detailed report, **International Working Group for Personal Data Protection in Telecommunications (IWGDPT)** adopted a working paper on CAVs discussing the type of data to be protected and recommendations to the multiple stakeholders [250]. The IWGDPT working paper also listed the privacy risks to be: lack of transparency, unlawful processing, unauthorised secondary use, excessive collection, lack of control, inadequate security, and lack of accountability.

Table 2.5: Data privacy regulations summary

Type	European	Global*
Hard Laws	e-Privacy Directive [152] GDPR [424]	S.2182 SPY Car [88] H.R.3388 Self Drive [87] Australia Policy Paper [24] APPI [370]
Soft Laws / Regulatory Bodies	WG4 [420] EDPB [147, 149] GAIA-X [173] Data for Road Safety [106]	UNECE [429, 432] ICDPPC [198] IWGDPT [250]

* *Limited to the cited countries in the present section*

2.5.3 Data privacy summary

To cover multitude nuances of RQ3 in this section, we investigated and identified the key privacy preserving theories that are commonly used in general IT contexts and applied them to the ACS scope. We identified relevant cryptography protocols to assure authentication of vehicular information, or hide visual data within the mini-buses cameras' recordings. Other powerful protocols anonymising personal identities or obfuscating vehicles' locations were discussed respectively. Such policies are very promising and highly recommended if not obliged by the discussed hard laws such as the GDPR.

Though, such mechanisms remain vulnerable to re-identification risks that can lead to easily infer or predict individuals and/or location attributes [261, 90]. In other words, machine learning techniques implementing anonymisation requirements, such as Differential Privacy, Randomised Response and haystack privacy, as cited in Section 2.5.1, allow to recognise a person from mining non-personal inputs or by combining multiple data sets. With such a gap between technical implementations and legal provisions, the strict deployment of regulations may fall short in some real world situations. Hence, the application of a legislation has to be adapted to the context and type of data which can vary within the processing and the eventual reverse engineering technologies.

To conclude, and as an answer to RQ2, it is true that the deployment of the most pointed privacy preserving theories and the existing laws and regulations certainly increases data transparency and guarantees lawful processing. However, the de-anonymisation risk is never zero and personal data can still be somehow consumed and generate benefits for data controllers and third parties.

A more appropriate approach to overcome such shortcomings is to consider any technical mitigation technique or legal text on a case-by-case basis and/or as cooperative guidelines built by data controllers, policy makers, ACS' stakeholders and standardisation bodies that should be frequently updated to cope with the ACS evolving technologies. The following section presents standards and standardisation bodies' efforts on protecting the vehicular ecosystem from cybersecurity and data privacy breaches.

2.6 Standards

As in the automotive sector, ACSs stakeholders have been collaborating with standardisation bodies to build up measures and processes addressing security and privacy challenges. According to ENISA [157] relevant standards can be classified into three groups: Automotive where mainly ISO, SAE and Automotive Open System Architecture (AUTOSAR) have identified security framework and road maps over the in-vehicle components. The second group is the cooperative communication where ETSI working groups have outlined technical specifications on ITS. Finally, the third one is the generic cybersecurity group combining ISO and International Electronical Commission (IEC) collaborations. Beyond ENISA's classification, noteworthy efforts from other standardisation bodies such as European Committee for Standardization (CEN)-European Committee for Electronical Standardisation (CENELEC), BSI, and World Wide Web Consortium (W3C) are investigated and reviewed in this section as summarised in Table 2.6.

2.6.1 International Organization for Standardization (ISO)

ISO standards can be generic and transverse but still relevant to vehicular environment. The ISO 9001 [216], covering quality management requirements, can be relevant to any organisation regardless its services or products. In collaboration with IEC, the ISO/IEC 27K standards series [203] came up to address information security and risk management controls. For more cybersecurity focused standards, there are the ISO/IEC 15408 [222], ISO/IEC 18045 [224] and ISO 20077/78 [208, 209] which present general cybersecurity processes recommendations and computer security certifications. Additionally, ISO/IEC 20243 [228] aims to reduce the risks related to malicious hardware or software. ISO standards embed also generic road vehicle safety requirements like ISO/PAS 21448 (which will be replaced by ISO/DIS 21448) [230], ISO 26262 [214] and the last ISO/CD 24089 [213] which is under-development to discuss specifications for the vehicles' software updates.

To incorporate cybersecurity considerations in the vehicle environment, the ISO/TC22 working group joined their efforts to SAE and established the ISO/SAE

21434 [233]. The ISO/SAE 21434 is a descendent of SAE J3061 which sets high level guidelines of cybersecurity approaches based on a lifecycle framework definition [397]. Based on the SAE J3061, ISO/SAE 21434 aims to achieve a common understanding of security by design over the entire supply chain in order to reduce the potential cybersecurity threats. ISO/SAE 21434 covers also risk management requirements by referring to the generic ISO 3100 [398]. Nevertheless, the standard draft has been criticised by Macher et al. [309] as being ambiguous since processes are described at a high level without prescribing specific technologies to countermeasure cybersecurity threats on the CAVs' environment. As further efforts from the ISO/TC22, ISO/SAE PAS 22736 [206] came to update the taxonomy of the six levels of automation that was initially defined in SAE J3061. To that end, other standards such as ISO/DPAS 5112 might provide more visibility on automotive cybersecurity auditing [231].

In the context of ITS, ISO founded ISO/TC 204 working groups who have been developing standards supporting the integration of CAVs and ACSs [241]. Among the ISO/TC 204 efforts, ISO/TS 21177 [238] was published to specify security and authenticity requirements for the exchanged data among OBUs, RSUs and TAs. The ISO/TS 21177 will be replaced by ISO/CD 21177 which is under-development. The ISO 22737, which was published in July 2021, came up with the system requirements for the specific ACS case operating at level 4 of autonomy and with low-speed configuration [210]. ISO/AWI 21734 [217] is a promising standard on which ISO/TC 204 is still progressing to present connectivity and safety requirements for the deployment of CAVs into public transportation through automated driving buses of all sizes. Moreover, and within the public transportation scope, the ISO 24014 [204] was published in January 2021 and which highlights security management and identification schemes for all public transportation vehicles including the automated mini-buses. The ISO/TC 204 working groups are still developing further standards related to CAVs such as ISO/AWI TR 23254 [219], which is about designing a high level referential architecture, and ISO/AWI TS 22726 [220] for the vehicles' map database specifications. Further standards are still on early stages but they are dedicated to ACSs such as ISO/PWI TR 5255 [232] discussing low-speed automated driving system architecture and ISO7856 [229] presenting the specifications for ACSs remote assistance.

2.6.2 Automotive Open System Architecture (AUTOSAR)

Automotive industry has also pushed to standardise security approaches over on-board systems through their collaboration on AUTOSAR standards. AUTOSAR series tend for securing in-vehicle communication networks and ECUs, protecting data confidentially and implementing cryptography [170] as detailed in Table 2.6. However, following AUTOSAR security specifications like AUTOSAR664 does not imply the vehicle compliance to ISO standards like ISO 26262 [29].

2.6.3 European Telecommunication Standards Institute (ETSI)

Besides, ETSI is a European standard Organisation proposing many standards related to security and privacy on the ITS [132]. ETSI TC ITS WG5 working group focuses on identifying threats and their countermeasures, specifying requirements and building standardised architecture for CAVs communications [301]. Table 2.6 describes ETSI releases ensuring privacy preserving communication, exchanged certificates with RSUs, secured message formats, and PKI implementation.

2.6.4 European Committee for Standardization-European Committee for Electronical Standardisation (CEN-CENELEC)

CEN founded CEN/TC 278 as the European ITS committee since 2013. Among its working groups, CEN/TC 278/WG16, which is fully joined with ISO TC 204 WG 18, has been focusing on V2I and V2V communications' standardisation [71]. The key published standard to cite within the context of security and data privacy is CEN ISO/TR 21186-3 [72, 237] which provides guidelines on access control, and PKI for a secure automated driving ecosystem. Moreover, CEN/TC 278/WG17 focuses on urban ITS and has been developing new sets of standardisation initiatives dealing with the integration of CAVs to the urban infrastructure [73]. The CEN/TC 278/WG17 publications represented first drafts of the ISO TC204/WG19 efforts once the two groups joined their contributions [167].

Additionally, CEN and CENELEC consolidated their collaboration by creating CEN-CENELEC as a platform for the development of European standards through a wide range of sectors including transportation and information technologies [69]. In collaboration with the European Commission, ISO, and other standardisation bodies, CEN-CENELEC created the CEN/CLC/JTC13 technical committee acting on cybersecurity and data protection field on a broad scope [68]. As published on CEN-CENELEC program for 2021 [70], CEN/CLC/JTC13 aims to develop new cybersecurity standards for the IoT sector and privacy by design and by default within the context of the GDPR.

2.6.5 DATEX-II

Furthermore, transportation data exchange in Europe is controlled by DATEX II which is the road transport standard [91]. DATEX II was launched by CEN to address traffic data sharing and transmission including transmitted data in cooperative and connected mobility [108]. Among its specifications, DATEX II 3.1 proposes a standardised message format between vehicles and RSUs which support the standardisation of V2I communication [107].

2.6.6 Publicly Available Specification (PAS)

BSI, the UK standardisation body, has developed a series of Publicly Available Specification (PAS) standards dedicated to CAVs cybersecurity related topics. PAS 1885:2018 [58] represents a high level set of guidelines discussing the fundamental principles of cybersecurity over the development and use lifecycle. Additionally, PAS 11281:2018 came afterwards with more detailed recommendations for managing security risks impacting the safety [55]. Newer BSI standards such as PAS 1880 [56] and PAS 1881 [57] should be considered as they are acknowledging the consequences of cyber attacks over the vehicle safety.

2.6.7 World Wide Web Consortium (W3C)

The W3C, specialised on developing web standards, has two working groups who published candidate standards, applicable to the vehicular environment, and which are intending to become standards according to W3C documentation classes [445]. W3C has launched the Automotive Working Group who proposed on 2018 a recommendation on the Vehicle Information Service specification [175]. The recommendation specifies how the in-vehicle system, that is responsible for exposing vehicle signals and data to on-board clients, communicates with other vehicles and devices via WebSocket. The recommendation advocates security access control mechanisms such as token and encryption using PKI. The Automotive Working Group has also published the Vehicle Information API Specification providing access restrictions to the vehicle data [288]. The second working group is the WEB of Things working group who is focusing on standards enabling integration across IoT systems including IoV. In November 2019, the group disclosed a non-normative guidance of security and privacy using threat model describing the key security stakeholders, potential attackers and attack surfaces of IoT systems in a generic view [379].

Table 2.6: Standards summary.

S.Body	Standard ID	Scope	Description	Status
ISO	ISO 9001 [216]	Generic	Quality management systems	Published
	ISO 27K [203]	Generic	Information security and risk management controls	Published
	ISO/IEC 15408 [222]	Cybersecurity	Evaluation criteria for IT security	Published
	ISO/IEC 18045 [224]	Cybersecurity	Methodology for IT security	Published
	ISO/IEC 20077 [208]	Vehicle Cybersecurity	Extended vehicle communication	Published
	ISO/IEC 20078 [209]	Vehicle Cybersecurity	Extended vehicle web services	Published
	ISO/IEC 20243 [228]	Cybersecurity	Threats related to malicious hardware or software	Published
	ISO/PAS 21448 [230]	Road vehicle safety	Safety of the intended functionality	Published
	ISO 26262 [214]	Road vehicle safety	Functional Safety	Published
	ISO/CD 24089 [213]	Vehicle software update	Vehicle software update	Under development
	ISO/SAE 21434 [233]	Vehicle Cybersecurity	Cybersecurity engineering	Published
	ISO/SAE PAS 22736 [206]	ITS	Taxonomy and definitions for automation systems	Published
	ISO/DPAS 5112 [231]	CAV's Audit	Guidelines for auditing cybersecurity engineering	Under development
	ISO/TS 21177 [238]	ITS	Security and authenticity requirements for V2X	Published
	ISO 22737 [210]	ACS	Low-speed automated driving systems for predefined routes	Published
	ISO 24014 [204]	Public Transport	Interoperable fare management system	Published
	ISO/AWI 21734 [217]	Automated driving buses	Connectivity and safety functions	Under development
	ISO/AWI TR 23254 [219]	ITS	CAVs' architecture	Under development
	ISO/AWI TS 22726 [220]	ITS	Dynamic data and map database specification for CAVs	Under development
	ISO/PWI TR 5255 [232]	ACS	Mobility integration low-speed automated driving architecture	Under development
	ISO7856 [229]	ACS	Remote support for low-speed automated driving	Under development
	ISO/TR 21186-3 [237]	C-ITS	Security guidelines on the usage of standards	Under development
AUTOSAR	AUTOSAR 402 [26]	In-vehicle Communication	Specification of crypto service manager	Published
	AUTOSAR 438 [27]	In-vehicle Communication	Specification of crypto abstraction library	Published

Continued on next page

Table 2.6: *Standards summary. (Continued)*

	AUTOSAR 654 [28]	In-vehicle Communication	Specification of secure onboard communication	Published
	AUTOSAR 664 [29]	Vehicular Software	Overview of functional safety measures	Published
ETSI	ETSI TR 102 893 [127]	ITS	Threat, vulnerability and risk analysis	Published
	ETSI TS 102 731[131]	ITS	Security services and architecture	Published
	ETSI TS 103 097 [137]	ITS	Security header and certificate formats	Published
	ETSI TS 102 940 [132]	ITS	Communications security architecture and management	Published
	ETSI TS 102 941 [134]	ITS	Trust and privacy management	Published
	ETSI TS 102 942 [135]	ITS	Access control	Published
	ETSI TS 102 943 [136]	ITS	Confidentiality services	Published
	ETSI EN 302 637-2 [126]	ITS	CAMs specifications	Published
PAS	PAS 1885:2018 [58]	Vehicle Cybersecurity	The fundamental principles of automotive cyber security	Published
	PAS 11281:2018 [55]	CAV	Impact of security on safety	Published
	PAS 1880 [56]	CAV	Guidelines for developing and assessing control systems	Published
	PAS 1881 [57]	CAV	Assuring the safety of automated vehicle trials	Published
W3C	Candidate [175]	Vehicle Cybersecurity	Vehicle information service specification	Under development
	Editor's Draft [288]	Vehicle Cybersecurity	Vehicle information access API	Under development
	WG Note [379]	IoT	Security and privacy guidelines	Under development

2.6.8 Standards summary

Through an in-depth review of the core standardisation actors, this section presented a selection of key standards that are appropriate to cybersecurity and data privacy within the driverless environment. Additionally, since the initiation of the present work, a tracking of all new standards' related publications was conducted to provide up to date analysis and findings that keep pace with the rapidly evolving technologies of the ACS landscape. Under the auspices of ISO standards, including their joint efforts to CEN-CENELEC, the ISO/TC22 and ISO/TC204 conceived a rich directory of standards for cybersecurity daunting challenges within ITS and smart cities. The recently published ISO/SAE 21434 represents the most eagerly awaited standard covering cybersecurity guidelines for road vehicles. Though, the standard scope is broad enough to wrap all vehicles with electrical and electronic systems that can match any SAE automation level. Likewise, the ISO/SAE 21434 scope covers only the in-vehicle component and not external systems through which potential attacks can occur. Hence, further standards need to be joined to the flamboyant ISO/SAE 21434 for a more comprehensive security assessment. Even in their larval state, other standards remain constructive and more specific to ACSs such as ISO/AWI21734, ISO/PWI TR5255 and ISO7856. However, they are not directly addressing the cybersecurity risks.

Besides, AUTOSAR, ETSI and PAS published alluring guidelines on implementing security by design at different layers within a connected vehicular environment; still they need to be upgraded to tackle highly automated vehicles such as ACSs. Regarding data privacy concerns, DATEX-II is standardising the exchanged messages within the vehicular context, while W3C is working on more specific privacy guidelines within IoT settings. However, both efforts remain generic without approaching specific measures on protecting personal data within the ACS that has different data controllers.

As a matter of fact, the answer to our RQ4 is foreseen to be a partial and temporal "NO", as the existing standards need some leveraging, fusion and enhancement to build a comprehensive security framework which is intended to be our future work as discussed in Section 2.7.1.

2.7 Discussion & future work

With the intrinsic super smart in-vehicle components (hardware and software), its rich input and output data, and their communication with anything and everything, the ACS might not reach complete cyber safety without being built within a standardised framework and strong policies. However, some future work is still required and limitations should be noted. The present section depicts the required efforts from security, privacy and standardisation perspectives.

2.7.1 Future work related to security certification

Reaching a complete secure vehicular system seems to be impossible according to Linkov et al. [297]. Therefore, an effective strategy would not be eliminating them but being prepared for their occurrence and knowing how to adequately react to their impact. Consequently, as a future work, we are currently working on proposing a certification model using security- and privacy-by-design approaches to establish a thorough security audit. We elevate the results of the present work further by evaluating the existing standards, which thereafter are processed (selecting the best standards, propose improvements and make them more specific towards the CAV ecosystem) to constitute the skeleton of our proposed certification model. To this end, the certification model will tie together the organisational procedures, risk and threat assessment approaches and recommendations of the most adequate patching, scanning and penetration testing methods. Thereupon, our intended certification model would present the road map for security auditing of highly automated vehicles.

2.7.2 Future work related to data privacy

With regard to the privacy by design of ACS, there is a need to have more clarity on the various technical measures implemented at the ACS such as anonymisation and pseudonymisation. Still there is much debate about the effectiveness of the anonymisation technologies and the inherent risk to de-anonymise data by using reverse engineering technologies or by combining anonymised data with other information leading to identify a person. As a future work, we are progressing on identifying the compatibility of privacy laws with security technologies focusing on the gap between the legal definitions and the technological implementation of pseudonymisation and anonymisation.

2.7.3 Work limitations

Furthermore, the number of standards from various standardisation bodies at any stage, published or under development, changes very often which requires a recurrent update of the standards findings. Moreover, multiple standards can be overlapping, like ETSI standards that are partly rivalling with CEN and ISO sets; which let the concern open to the OEM or the service provider to select the standard to which they are seeking compliance. Finally, the cost to dive deeply into some standards represents a real limitation of the present review since the research was done based on the standard description or through free institutional resources.

2.8 Conclusion

With the advancements in the domain of CAVs, authorities are looking into integrating these, as ACSs, into the traditional public transports, either to extend or to replace existing services. The introduction of the ACS brings promise of great benefits to its citizens, especially for those with special needs, making public transport more personalised. However, as with everything Internet capable, it inherits its flaws and dangers in addition to being a ‘new’ vehicle that is still in its infancy. As the use of these mini-buses are intended to no longer have a driver (legally still required in many countries), it is up to the services provided to its users to ensure a comfortable and safe journey. This endeavour involves a significant amount of digital services and a complex infrastructure for operating a fleet of automated mini-buses, which require always to be connected and communicating in real-time.

Consequently, the goal of the present work is to provide a united and collated source of references for any researcher to look into when analysing associated cybersecurity and data privacy risks of integrating ACS in his/her city on the way to the future development. We want to have a holistic approach to include three facets of the risk plan (security, data protection, standards) in a singular framework for ACS integration into smart cities' operational environment.

In each facet, extensive analysis have been provided by pointing out the gaps and shortcomings in regard to this comprehensive view. A systematic categorisation and a mapping within each of the domains provides structuring and clarity on the scope of the threat landscape and efforts by the research community, the authorities and public & private organisations. Furthermore, based on a thorough investigation of the latest technologies and regulators efforts, the paper provides a novel and up to date reference of threats, technical and legal mitigation strategies to the ACS as a specific case of the IoV domain.

For cybersecurity, we defined two layers on which cyber attacks can occur, 'in-vehicle threats' dealing with the internals of the vehicle and 'communication threats' that includes all different types of possible communication that may influence the operation of a mini-bus. The attack surfaces have been further analysed and associated mitigation techniques have been aggregated into six mitigation strategies providing in-depth technical review relevant to ACS and their commonalities with CAV, ITS and IoV landscape. As the human factors in greatly to any effective defence strategy, cybersecurity regulations are essential to any ICT infrastructure. This work looked at the main key players from different governmental authorities EU, UK, USA, Japan as well as intergovernmental working groups. In regard to the data privacy, clarity is provided through identification of the laws, guidelines and recommendations from the different regulatory bodies (key players). Three major technical mitigation solutions were analysed concerning the safe storage and transmission of data and are highlighting the importance of employing good data privacy solutions. The data privacy regulations have been summarised into the hard and soft laws, aggregating the most relevant regulations and laws from EU, international and intergovernmental initiatives, while underlining the new efforts being made towards CAVs. The last domain, summarised the main (seven) standardisation bodies and their standards regarding the cybersecurity and data privacy. It further provides insights in how these organisations operate, joined efforts and specialise in specific domains relevant to the ACS ecosystem.

This work brought together the key pieces of information on cybersecurity and data privacy relevant to the exploitation of ACSs. It can be summarised that great efforts are made in each of the domains and are expected to continue alongside the evolvement of the CAV, ITS and IoV in terms of technological progress, deployment environments (urban, suburban and rural requirements) and business-models & services (inter-transport connectivity, advertisement strategies, on-demand flexibility).

Acknowledgment

This work has been funded and supported by the European Union's Horizon 2020 Research and Innovation Programme through AVENUE project (https://h2020-avenue.eu/) under grant agreement No 769033 and SHOW project (https://show-project.eu/) under grant agreement No 875530. The authors would also like to thank Allan Berrocal, from University of Costa Rica, for his insightful recommendations and orientations.

Chapter 3

Article II: The interface of privacy and data decurity in automated city shuttles: The GDPR analysis

Relevance

As part of the data privacy examination, this article provides an in-depth analysis of the data protection requirements that should be considered by the CAV generally, and the ACS's stakeholders specifically. To complement the answer to RQ2, this article extends further the data privacy investigation presented in Chapter 2 by exploring the GDPR articles in details and examining the privacy-preserving techniques efficiency. This paper outcome represents a crucial pillar in developing a privacy-aware TARA as demonstrated in Chapter 7.

Context

This article [44] was published in the Journal of Applied Sciences whose IS: 2.48, h-Index: 22 and SJR: 0.336 according to the Resurchify portal[1].

Own contribution

My contribution to this work consists of: (i) leading fine-grained investigation on data privacy implications related to the ACS deployment (ii) providing holistic study of privacy preserving techniques (iii) evaluating concrete implementations of GDPR obligations. While the majority of the paper content was edited by me, the legal discussion and the GDPR articles mapping was provided by the second author. The content was subsequently examined by other co-authors and adapted to fit a scientific journal rather than a legal one.

[1] https://www.resurchify.com/about

Contents

3.1 Abstract

The fast evolution and prevalence of driverless technologies has facilitated the testing and deployment of Automated City Shuttles (ACSs) as a means of public transportation in smart cities. For their efficient functioning, ACSs requires a real-time data compilation and exchange of information with their internal components and external environment. However, that nexus of data exchange comes with privacy concerns and data protection challenges. In particular, the technical realisation of stringent data protection laws on data collection and processing are key issues to be tackled within the ACSs ecosystem. The present chapter provides an in-depth analysis of the GDPR requirements that should be considered by the ACSs' stakeholders during the collection, storage, use and transmission of data to and from the vehicles. First, an analysis is performed on the data processing principles, the rights of data subjects and the subsequent obligations for the data controllers where we highlight the mixed roles that can be assigned to the ACSs stakeholders. Secondly, the compatibility of privacy laws with security technologies focusing on the gap between the legal definitions and the technological implementation of privacy preserving techniques are discussed. In face of the GDPR pitfalls, our work recommends a further strengthening of the data protection law. The interdisciplinary approach will ensure that the overlapping stakeholder's roles and the blurring implementation of data privacy preserving techniques within the ACSs landscape are efficiently addressed.

3.2 Introduction

The emergence of novel technologies based on AI and IoT in the transport sector presents substantial regulatory challenges. Since the early stages of the IoV deployment through CAVs, multifaceted problems of compliance to the European personal data protection regulation have been raised [32]. To a greater extent, with the envisioned deployment of CAVs into the public transportation through the ACSs, there are novel and daunting regulatory hurdles to overcome [9].

The ACS, such as the one deployed in a pilot-site within the Avenue project [277] and depicted in Figure 3.1, compiles multiple sensors and AI units' inputs to achieve a high automation driving, as per the SAE levels 4 and 5 [385]. A highly connected ACS would use intrinsic communications and endless exchange of information through V2V, V2I, V2C, and V2P to broadcast traffic conditions and share the predictions within the vehicular network. Such a complex system makes the ACS able to navigate autonomously while using real-time and fine-grained data.

With the rise of registered information by the in-vehicle components and the vehicular external communications, data protection needs to become more significant and applicable to the different types of data generated by the ACS. The ACS's sophisticated cameras can record both eventual obstacles disrupting the autonomous driving mode and any visual personal data, including facial identities. In addition, within the vehicular network, the nodes, which can be an ACS or a RSU, exchange beacon messages combining identity, location, and temporal properties. Such messages embed timestamps, vehicular information, authorisation certificates, and location data [123, 441], which is qualified as personal data. In other words, those messages'

Figure 3.1: Example of an automated city shuttle (Geneva, Switzerland).

content is linked to identified or identifiable natural persons (hereinafter, referred as "data subjects") under Article 4 of the GDPR [424]. Sometimes personal location data, such as travel itineraries, can reveal sensitive information about data subjects' health condition, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership [32]. In these cases, stricter privacy protection rules are required to be applied.

An idiosyncratic element to consider when exploring the ACS ecosystem is the provision of customised services to the passengers through the integration of LBS such as the MaaS. MaaS is a mobility platform which bridges public transport to mobility services by providing, for example, door-to-door services based on the passengers information, including their location [406]. Hence, the more LBS services are deployed, the more personal data are transferred through external digital platforms, leading to higher risk of privacy violation. Based on such assumptions, the WP29, the predecessor of the EDPB "whose purpose is to ensure consistent application of the GDPR", assessed the necessity of transparency and proportionality controls due to high risk of personal data leakage and unlawful processing of mobility data [20].

The mere identification of the collection and further processing of personal data is of vital importance to ensure protection from privacy risks, which is attempted to be provided by regulatory frameworks such as the GDPR in the EU. Any failure to comply with the GDPR requirements could potentially result in physical, material, or non-material damage to natural persons, such as loss of control over their personal data or limitation of their rights (Recital 85) [424]. Additionally, the ACS data privacy risks entail further regulations such as the ePrivacy [152] and the NIS directives [422, 423]. Those directives urge to take the appropriate and proportionate measures for a high level of information systems' security to prevent and minimise the impact of cyber incidents and attacks. For the purpose of our work, we constrain our analysis to explore only the GDPR implications.

The present article provides the following contributions:

1. An extensive analysis on how the GDPR discusses the principles of data processing, the rights of data subjects, and roles and responsibilities of the stakeholders (data controllers, data processors, sub-processors, etc.) before, during, and after the processing of personal data collected from the ACS.

2. Categorisation of the main privacy-preserving techniques that are applicable to the ACS environment.

3. Presentation of the gaps between the legal definitions and technological implementation of privacy-preserving schemes recommended by the GDPR, which are mainly pseudonymization and anonymization techniques.

4. Investigation, through interdisciplinary efforts, into the shortcomings and pitfalls of the GDPR data processing principles in protecting personal data within the complex ACS context.

This article addresses the following research questions:

- RQ1: According to the GDPR, what are the rights of data subjects that data controllers have to take into consideration before initiating any processing of collected data from the ACS ecosystem?

- RQ2: What is the attribution of role for each stakeholder involved in the ACS landscape? What are their respective responsibilities based on the GDPR?

- RQ3: What are the relevant privacy-preserving techniques to protect personal data within the ACS environment and how do each guarantee personal information protection in line with the GDPR? Would the techniques recommended by the GDPR be enough for an optimal protection?

The remainder of this paper is structured as follows: Section 3.3 discusses the related work and makes a comparison of the present work with already published efforts. Section 3.4 delivers a thorough review of the most crucial GDPR regulatory effects while applied to the automated driving ecosystem. Section 3.5 overviews the gaps between technological and regulatory disciplines in terms of implementation of mitigation techniques to data privacy risks related to the ACS deployment. Section 3.6 offers concluding remarks and future work orientation about lawful processing of personal data within the ACS environment.

3.3 Related work

With the pervasive technologies leading to driverless vehicles and their associated privacy challenges, the GDPR has been serving as the European prominent legal reference. As well as beyond the EU, the GDPR has paved the way for a global impact regarding data protection [91]. To illustrate, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) was influenced by the GDPR to strengthen consumer rights through aligned and similar obligations [359]. Additionally, the Australian national transport authority acknowledged the GDPR while regulating the ITS and automated vehicles' data processing [24]. To that end, the GDPR has been perceived as the international legislation for data governance with strict obligations to data controllers, data subjects, and engineers for consent and privacy-enhancing technology implementations [176]. Therefore, our work demonstrates efforts on deep investigation into the GDPR and its relation to the automated vehicles. To this end, we present three main avenues, namely, GDPR requirements, recognition of privacy challenges, and privacy-preserving methods.

3.3.1 GDPR in driverless landscape

Several works exist in the domain of data protection, aiming to provide analysis on the GDPR's proposed measures under the scope of the generic vehicular environment. For instance, Taeihagh and Lim [415, 293] provided a brief overview of the GDPR with a focus on consent and penalties conditions. Similarly, Pattinson, Chen and Basu [369] discussed, as a GDPR requirement, the role of the data subjects' consent while operating on level 3 and 4 CAVs. Additionally, Vallet [437] presented the GDPR's applicability within a CAV environment but with a focus on drivers and vehicles owners' rights. Moreover, Krontiris et al. [281] analysed the data protection challenges within the CAV environment by categorising the types of collected data, data subjects, and data controllers profiles. The authors also highlighted the implications of the GDPR on AI by matching relevant articles to technologies used for data processing. Further multidisciplinary works presented interesting overviews on how the GDPR can be considered within the development life cycle to avoid data privacy breaches [441, 91]. The genuine interest for such publications is the protection of the data subject rights. Yet, an explicit and holistic review of all the CAV's stakeholders rights and obligations is still lacking.

Shifting from legal requirements on consent, data subjects, and data controller, Bastos, El-Mousa and Giubilo [34] synthesised the principles of data processing and the DPIA concerns. However, the paper scope remains broad to all IoT devices. Despite the fact that ACS can be considered as a complex IoT device too, it has specific parameters to be taken into account while performing such analysis. Conversely, Ainsalu et al. [9] provided a more specific review to ACS discussing the legal framework of testing and deploying such vehicles in Europe, though the authors referred broadly to the GDPR as the integral law that controls the required processing within the ACS without an in-depth analysis on the GDPR implications or limitations.

3.3.2 Data privacy challenges within vehicular environment

Extensive efforts in identifying data privacy challenges within the CAV's ecosystem were provided in multiple research works. Collingwood [85] and Glancy [183] warned about the privacy implications of using automated vehicles as a means of public transportation. They identified three fields of concerns, which are "autonomy privacy interests, information privacy interests, and surveillance privacy interests", where the individuals acquire the total liberty and control to make independent choices about themselves, their lives, and their data. They argue that by collecting and processing data from CAVs, the passengers will lose control over their private information as the data controllers may infer the individuals' past, present, and future locations and behavior. However, these papers do not refer to or analyse the compliance to any specific law or regulation.

3.3.3 Data privacy-preserving methods

Motivated by the potential of privacy-preserving schemes, as recommended by the GDPR, multiple literature reviews outlined clarification about the implementation of pseudonymization and anonymization. Karnouskos and Kerschbaum [260] studied the feasibility of insuring the integrity of automated vehicles while preserving the individuals' privacy. Two particular concepts are brought forth by the GDPR, namely, Privacy by Design (PbD) and Privacy by Default (PbDf). Although these concepts are not necessarily new [195], as part of the GDPR their impact can be significant. PbD starts with the implementation of security measures from the outset of data processing and extends to the implementation of technical and organisational measures during the whole lifecycle of the data involved, whereas PbDf calls for personal data, which is necessary and proportionate for each specific purpose of the processing to be accomplished. This relates to the amount of personal data collected, the extent of the processing, the retention period, and who has access to it. The authors focused on the deployment of PbD principles and technical mitigation techniques based on encryption and anonymization in the scope of CAVs. Similarly, Mulder and Vellinga [336] highlighted the difference between pseudonymization and anonymization as the key privacy-preserving techniques required by the GDPR and applied to vehicular environment. In a broader scope, Ribeiro and Nakamura [381] compared pseudonymization and anonymization techniques and how they can protect personal data within IoT systems. Unfortunately, most of these works neither provided a comprehensive categorisation of the applied pseudonymization and anonymization techniques to the ACS environment, nor flagged the re-identification risks related to such techniques.

The most detailed analysis attempting to raise re-identification risks were proposed in [54, 290, 300]. Brasher [54] discussed the limitation of anonymization and encouraged its conjunction with pseudonymization to reduce the re-identification risks. Li et al. discussed the inference and de-anonymization risks within the driverless environment [290]. Löbner et al. [300] evaluated the re-identification risks and impact within the vehicular context through a real test bed scenario, though the efforts remain limited to some of the privacy-preserving techniques without reviewing them thoroughly.

Not limited to researchers, EU institutions initiatives assessed the re-identification risks in multiple publications. The opinion 05/2014 of the WP29 [20] represents one of the first guides approaching the effectiveness of anonymization techniques. ENISA provided deeper analysis on pseudonymization and anonymization implementation, differences and limitations [124, 153]. Nevertheless, such publications' scope remain very wide, yet applicable to driverless environment.

Following this presentation on the related research and the analysis from Table 3.1, we differentiate from the other efforts by:

- Presenting an interdisciplinary approach regarding data protection requirements in the ACS ecosystem by assessing and addressing simultaneously both regulatory and technical challenges.

- Providing an in-depth analysis of the GDPR provisions and limitations that are relevant to the ACS.

- Having a closer examination on how the legal requirements are compatible with the technologies deployed in the ACS.

- Analysing the inconsistencies between the legal definitions on pseudonymization and anonymization in the GDPR and their technical implementation through a comprehensive categorisation of the most relevant applicable techniques into the ACS landscape.

- Developing a significant reference point for academic research on ACS, public transportation operators, OEMs, policymakers, and service providers, acquiring or looking forward to deploying ACSs within their systems.

Table 3.1: Related work comparison

Table 3.1:

Related Work	Year	Scope				PC[a]	GDPR Implications					PP[d]			GDPR Pitfalls
		ACS	CAV	IoT	IT		Principles	DS Rights[b]	DC Obligations[c]	Roles	DPIA	Pseudonymization	Anonymization	Risks	
ENISA [153]	2022	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓
Mulder and Vellinga [336]	2021	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Löbner et al. [300]	2021	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
ENISA [124]	2021	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗
Pattinson, Chen and Basu [369]	2020	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
Krontiris et al. [281]	2020	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
Costantini et al. [91]	2020	✗	✓	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
Vallet [437]	2019	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗
Ribeiro and Nakamura [381]	2019	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗
Li et al. [290]	2019	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗
Taeihagh and Lim [415, 294]	2018	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Veitas and Delaere [441]	2018	✗	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
Bastos, El-Mousa and Giubilo [34]	2018	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗
Ainsalu et al. [9]	2018	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Karnouskos and Kerschbaum [260]	2018	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗
Brasher [54]	2018	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓
Collingwood [85]	2017	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗
WP29 [21]	2014	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗
Glancy [183]	2012	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗
This work		✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

[a] Privacy Challenges
[b] Data Subjects
[c] Data Controllers
[d] Privacy Preserving

3.4 GDPR implications

While the level of privacy protection for ACSs has been effective with a number of technical solutions offered by pseudonymization and anonymization techniques, further discussed in Section 3.5, it is noteworthy that the respective legal framework as set forth in GDPR faces new regulatory challenges [336]. In the present section, we overview how the data protection regulation covers the principles of data processing and the rights of data subjects. This section sheds the light on the difficulties regarding the application of the data processing principles within the ACS ecosystem, and the risks to data subjects' rights during the data processing operations. In addition, we identify all the stakeholders who manage personal data, their interaction, their exact roles in the ACSs ecosystem based on the GDPR terminology, and their compliance requirements. Furthermore, by analysing whether it is justifiable to incorporate DPIA in relation to the purposes of personal data collected, generated, and stored by ACS, and its value [20, 122, 24].

3.4.1 Data processing principles

Any processing of personal data should occur in the light of the legal principles as set in the body of the GDPR subsequently illustrated in Figure 3.2. According to Article 83 Section 4 [424] of GDPR, any failure of the entities involved in the processing to comply with the data processing principles may result in administrative fines and other sanctions. Certainly, the adherence to these principles by the controllers seems to be a fundamental requirement for the assessment of their compliance to the GDPR. To that end, data should be processed with respect to the following principles [424]:

1. Lawfulness, transparency, and fairness: where data collection practices are conducted based on a thorough understanding of the GDPR law and without hiding the type of collected data and the reason for its processing from the data subjects (Article 5, Section 1.a and 6).

2. Purpose limitation: where the processing is approached based on the specified, explicit, and legitimate purposes with no further processing in a manner that is incompatible with those agreed on purposes (Article 5 Section 1.d).

3. Storage limitation: calling for data storage no longer than it is necessary for the purpose for which the personal data is processed (Article 5 Section 1.e).

4. Accuracy: where controllers should take necessary measures to process only correct data (Article 5 Section 1.b).

5. Data minimization: aiming to limit the amount of processed data to the lowest level and requiring data destruction once the purpose of the processing is completed (Article 5 Section 1.e).

6. Security: requiring data controllers to employ the appropriate technical and organizational measures designed to effectively implement integrity and confidentiality through PbD and PbDf principles (Article 25 Sections 1 & 2).

7. Accountability: requiring data controllers to put in place appropriate privacy-preserving measures that are able to demonstrate compliance to the regulation at any stage (Article 5 Section 2).

To support continuous automated navigation of ACS, data are used permanently. This perpetual data usage poses multiple challenges to the aforementioned principles. First of all, collecting large datasets of personal data to train the AI models jeopardizes the data minimization principle [281]. Secondly, further collection, use, transmission, or storage of personal data may exceed the purpose limitation principle from the beginning of these data processing operations. Additionally, innovative autonomous and connected technologies applied in the ACS complicate the implementation and monitoring of the proper security measures in line with as the data protection by PbD and PbDf principles. Finally, while being part of the public transport system, the ACS have multiple stakeholders involved in data processing. These stakeholders act as data controllers or data processors or their roles change. For this reason, they have to provide personal data guarantees and mitigate potential privacy-related risks [9, 293] based on the accountability principle.

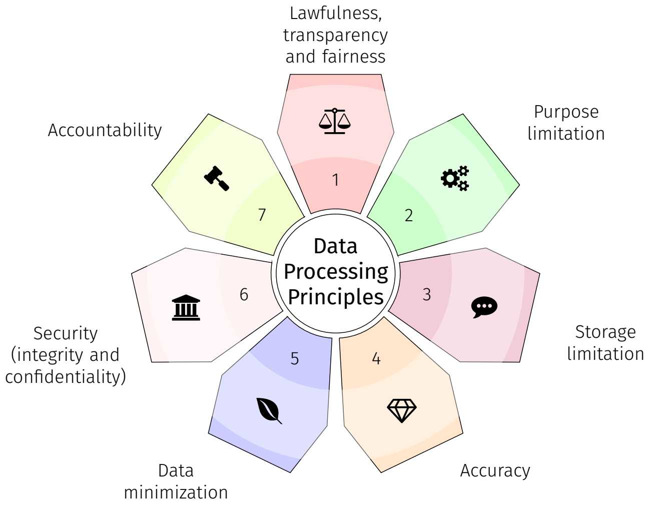

Lawfulness, transparency and fairness
1
Purpose limitation
2
Storage limitation
3
Accuracy
4
Data minimization
5
Security (integrity and confidentiality)
6
Accountability
7
Data Processing Principles

Figure 3.2: Data processing principles summary.

The subsequent sections are the result of our research to find the answers to the target research questions. Section 3.4.2 sets the basis for understanding the scope of RQ1 and provides the relevant findings. Then, Section 3.4.3 outlines our analysis in the form of a comprehensive study focused on the ACS's environment to address the RQ2.

3.4.2 Data subjects rights

To ensure transparency and fairness of data processing, the GDPR grants the data subjects specific control rights [437]. It should be mentioned that, at every stage of data processing, data subjects remain the owners of their personal data as verified by the right of access to personal data by virtue of Article 15 of the GDPR. By providing individuals access rights, the GDPR imposes a number of obligations to the entities that collect and process data, as well as allows the Data Protection Authoritiess (DPAs) to ask for demonstrations of accountability or impose fines if data subjects' rights are not secured. Data controllers provide specific practices and technologies to the data subjects to control and exercise their rights during the entire data processing. For instance, the information about the exercise of rights is available in the privacy policy at the controller's website. Controllers can facilitate, specifically, the access, the deletion, the transfer, or the removal of personal data by providing modification settings [149].

One of the most crucial rights is the *right to be informed* (Articles 12–14). Prior to the processing of personal data by the controllers, the data subjects shall be informed, in a transparent way, of the identity of the data controller, the purpose of processing, the data recipients, the data retention period, and the data subjects' rights. In relation to the right to be informed, it is noted that data subjects should be informed in clear and plain language about any data breaches where their personal information is leaked and this leakage is likely to result in a high risk to their rights and freedoms as per Article 34 of the GDPR. For exercise of the right to be informed when the collection and use of data is intended for the vehicular automated decision-making and profiling purposes, the data subjects should receive "meaningful information about the logic involved" as well as the significance and the envisaged consequences of such processing for the data subject as per Article 13 Section 2.f [424]. The WP29 in its revised guidelines [18] clarified that the complexity of the technologies should not justify the lack of information. In the light of this clarification, the OEMs, other equipment manufacturers, and service providers, qualifying as data controllers, should explain clearly to the ACS' data subjects the automated processing methods and their objectives.

Other rights include the *right to rectification* (Article 16). This right allows the data subjects to correct their personal data when it is inaccurate. *The right to erasure* (or right to be forgotten) allows the individuals to ask for their personal data to be deleted (Article 17). For instance, if an ACS operator (i.e., data subject) has consented to test the efficiency of a newly deployed system, he or she can withdraw such consent at any time and require the controller to erase all the information that was processed for the validation of this system. However, in following our example, if the OEM (i.e., data controller) demonstrates that he or she collects and processes personal data to detect shortages in the ACS with a view to improve safety of the vehicles and, subsequently, the safety of the public (overriding legitimate interests), the right to be forgotten may not be invoked pursuant to Article 17 Section 1.c of the GDPR. Further, the *right to restriction of processing* gives the data subjects the power to limit the processing of their personal data with several rules and exceptions (Article 18) [424]. Article 20 of the GDPR foresees the *right to portability*, permitting the data subjects to receive a copy of their personal data in a structured, commonly used, and machine-readable format and to transmit those data to another controller without impediment from the initial controller. An illustrative example of the exercise of data portability takes place when ACS passengers may require an ACS technical service provider to give all the information collected during a specific period and share it with a third party, such as an insurance company, in case of a car accident. As per Article 21, the data subjects also have the *right to object* to any processing of their personal data that they do not consent to. This latter right could require special attention and enforcement due to the large amounts of data collected and analyzed from the ACS. Meaning, continuous data from sensors, onboard processing, and big-data increase the complexity and impose additional requirements. Furthermore, the necessity for safe operating implies the capture of potential (inadvertently) subject data, where an objection would compromise its safe operation. From the above analysis, it is clear that the exercise of these rights is a vital part of the privacy interests of the data subjects, offering many possibilities to perform them and demanding the necessary guarantees from the controllers. The existence of several controllers in the ACS ecosystem means that common controllers should specify whose responsibility is the protection of the rights as per Article 26 Section 1 of the GDPR.

3.4.3 Data controllers' and data processors' compliance

The data controllers play a crucial role in the course of processing as they decide its purposes and means. A data controller can be a natural or legal person, a public authority, an agency, or other bodies. The core responsibilities of the data controllers involve [424]:

- The implementation of the data processing principles (Articles 5–11).
- To inform data subjects as elaborated in Section 3.4.1 and secure their rights (Articles 12–23).
- The implementation of security measures such as the deployment of privacy-preserving techniques discussed in Section 3.5 (Articles 5, 25, and 32).
- The arrangements with the joint controller (if any) (Article 26).
- The engagement of processors (Article 28).
- The notification of personal data breach to the relevant data protection authority (Article 33).
- The communication of personal data breach to the data subjects (Article 34).
- The realization of DPIA (Article 35).
- The designation of the Data Protection Officer (Article 37).
- The transfer of data to third countries (Chapter V, Articles 44–50).
- The communication with the DPAs (Articles 31, 36, and 37).
- The compliance with specific processing situations (Articles 85–91).
- Retain all the necessary documentation and records (as listed throughout GDPR articles).

The existence of two or more data controllers makes the involved parties "joint controllers" by virtue of Article 26 of the GDPR. Based on this article, two entities meet the requirements of joint controllers when they "jointly" determine the purposes and means of processing. If the criterion of joint decision is missing, then the stakeholders are not "joint" but sole data controllers. The EDPB with its recent guidelines on data controllers and data processors shed light on the ambiguity regarding the respective roles of joint controllers. Under Article 26, the joint controllers need to clearly define their respective compliance obligations, especially with regard to the exercising of data subjects' rights and the provision of information under Articles 13 and 14 of the GDPR. With regards to the legal relationship among the joint data controllers, the GDPR does not require a specific legal binding act. Nevertheless, for reasons of legal certainty, the EDPB recommends a contract or other legal act under EU law to identify the specific obligations that (joint) controllers have. In general, the principles of transparency and accountability of the data controller are applicable to all the joint controllers. Therefore, the responsibilities enlisted above extend to them. This practically means that joint controllers are responsible for demonstrating compliance to the GDPR based on their specific obligations as described in the contract or any other legal act, and noncompliance may result in administrative fines under Article 83 [122].

The Court of Justice of the European Union (CJEU) has adopted a broad definition regarding the notion of joint controllers and the allocation of their responsibilities. In a 2019 decision, in the Facebook Fan Pages case, the Court held that the administrators of Facebook fan pages are joint controllers together with Facebook. Although they had access only to anonymized statistical data and not to any personal data by creating the fan webpage, the administrators allowed to Facebook to collect data and made it joint controller. This judgment also stated that "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data" [99]. Further, in another notable case, the Facebook Fashion ID case [100] it was held that the "existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case". With these two decisions, the CJEU has validated a broad scope of joint controllers and has taken a clear position on the level of involvement in the data processing, the extent of responsibilities of joint controllers at every processing stage, and the degree of their liability.

The analysis of the joint controllership is relevant to the ACS because many service providers may qualify as joint controllers, as Figure 3.3 shows. The Public Transport Operators (PTOs), the OEMs, and cloud service providers may determine the means and data processing purposes of data collection and usage by the ACS. In actuality, in the light of the Facebook ID case, it was held that the notion of joint controllership exists even if the data are not personal. This statement extends the possibilities of joint controllership to other actors who process even anonymized data in the ACS. As far as the obligations and responsibilities, a clear arrangement among the data controllers should arrange the compliance to the regulation and the data subject's rights. It should be noted that the decision about joint controllership may reveal that the very same of the above stakeholders may act as joint controllers in the event of commonly determining the means and purposes of processing. In other cases, though, this interaction concerns a party that processes personal information on behalf of another while both parties may have been involved in joint operations that precede or are subsequent in the overall chain of processing [150].

When the data processing is carried out on behalf of the data controller, the entity performing the processing acts as a data processor. Under Article 4, a data processor can be a natural or legal person, public authority, agency, or other body. Article 28(1) of the GDPR necessitates that only processors providing sufficient guarantees to implement appropriate technical and organizational measures should be engaged by a controller.

Although the definitions of the data controllers and data processors are clear by law, there is perplexity around the identification of the data controllers and the data processors in the ACS ecosystem [335]. This perplexity can be justified due to the fact that the roles of data controllers and data processors change rapidly. This may also mean that when a processor acts in a way that infringes the contract or another legal act or makes decisions in an autonomous way about the purpose and the the means of a specific processing

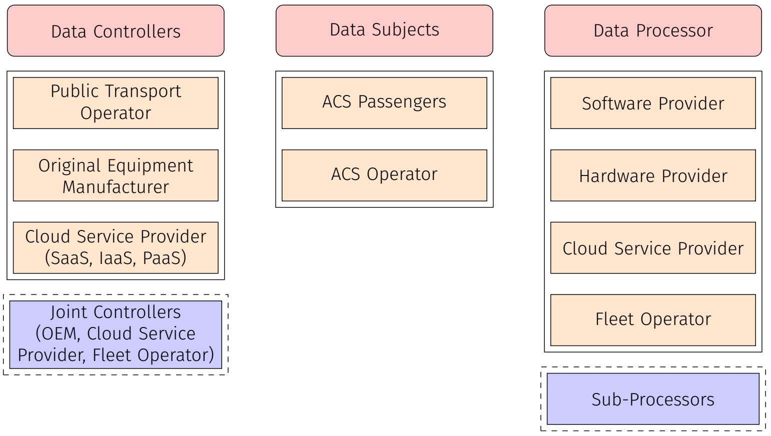

Data Controllers
Public Transport Operator
Original Equipment Manufacturer
Cloud Service Provider (SaaS, IaaS, PaaS)
Joint Controllers (OEM, Cloud Service Provider, Fleet Operator)
Data Subjects
ACS Passengers
ACS Operator
Data Processor
Software Provider
Hardware Provider
Cloud Service Provider
Fleet Operator
Sub-Processors

Figure 3.3: ACS's stakeholders classification per the GDPR terminology.

operation, it may qualify as a controller (or a joint controller). When a processor acts as a delegate of the data controller with a mandate to perform specific tasks following specific instructions, this entity remains a processor as long as the duties do not deviate from these responsibilities. It is noted that data processors can engage in the data processing of other entities. The latter entities qualify as sub-processors. Pursuant to Article 29 Section 2, the data controller should provide a prior specific or general written authorization.

The GDPR has a detailed description of the legal relationship among controllers and processors. The basis is a contract or other legal act under Union or Member State law that is binding. This legal document sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. Article 28 Section 3 of the GDPR enlists the specific processing duties that this legal act describes [424]. Inter alia, data processors should take all security measures required under Article 32, such as a data pseudonymization and encryption that will be reviewed in the section hereafter. Furthermore, they should assist controllers in fulfilling their obligations to respond to requests for exercising the data subject's rights. Finally, data processors should assist controllers' compliance with the obligations pursuant to Articles 32 to 36.

More specifically, as shown in Figure 3.3, in the essence of data processing in the ACSs we have the data subjects. The OEMs can be regarded as data controllers since they determine the means and purposes of processing. A fleet operator can be seen as joint data controller, under the conditions of joint controllership mentioned above, as they process data on behalf of the controllers [336]. Further examples of data processors include the distributors who perform legitimate remote monitoring, auto repair shops, navigation software providers and navigation apps developers, telematic service providers, or mobile network operators (MNOs) [281]. Per the required V2C communication within the ACS environment, the cloud service providers have a duplicated role to be considered, which can be a data processor or a data controller. This differentiation of the cloud service providers' roles derives from the fact that depending on the specific "service" they offer, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and/or Infrastructure as a Service (IaaS), different roles and respective responsibilities are assigned.

3.4.4 Data protection impact assessment

Pursuant to Article 35 of the GDPR, the data controllers are required to undertake a DPIA prior to data processing, especially when this processing is likely to result in a high risk to the rights and freedoms of natural persons. In particular, the GDPR enlists a non-exhaustive list of risk factors to be taken into consideration, and once assessed, a DPIA must be performed:

- A systematic and extensive evaluation of automated processing, including profiling and similar activities that have legal effects or affect the data subjects.
- Processing on a large scale of special categories of sensitive data such as racial or ethnic origin, political opinion, and of personal data relating to criminal convictions and offenses.
- A systematic monitoring of a publicly accessible area on a large scale.

Data processing at a large scale seems more relevant to the processing of personal data by and within the ACSs. Recital 91 provides information about what large scale means. It is the processing by making reference to the number of data subjects concerned, the volume of data processed, and the duration and the geographical extent of the data processing activity. It is understood that under these circumstances a DPIA is mandatory.

Nonetheless, even in cases where a DPIA is not legally mandated, data controllers should consider evaluating the data processing. Such practice would allow them to make a thorough assessment of the envisaged processing operations and to mitigate the risks as detailed in Article 35 [424]. In general, even in the cases where a DPIA is not required, it would be useful to carry out one as early as possible in the design process [149] under Articles 35(1) and 35(10) in combination with recitals 90 and 93 and with prior consultation of the DPAs under Article 36 of the GDPR. The DPIA should be publicly available and "continuously reviewed and regularly reassessed" [19].

Finally, conducting a DPIA is a tool of controllers' accountability. As such, it is part of the data controller's responsibilities to which they must show compliance, and, as mentioned, inability to be compliant to Articles 35 and 36 holds them accountable. However, due to the rapidly evolving nature of the autonomous technologies, the time for the realization of a DPIA, and the requirement of periodical assessment, a DPIA, in practice, might not fulfill its purpose and this challenges the controller's accountability.

3.5 The interface of privacy and data security in ACSs

Our next challenge that we would like to tackle uncovers how legal requirements, as derived from the GDPR, meet and coexist with technical solutions for preserving privacy within the ACSs ecosystem. More specifically, we seek for an answer to the RQ3 to advance the ACS specific knowledge on the appropriateness of the existing technological solutions for the data privacy preservation. As stated in Section 3.4, PbD and PbDf require the implementation of several technological measures, such as pseudonymization and anonymization. Multiple scientific research reviews and law provisions [153, 124, 336] discussed those techniques to meet the integrity and confidentiality in addition to data minimization as part of the GDPR data processing principles (Figure 3.2). Besides, such techniques embed further reverse engineering risks leading to re-identification of personal information as assessed by the opinion 05/2014 of the WP29 [20]. The present section elevates the discrepancy of the required mitigation solutions by evaluating legal recommendations and technical approaches.

3.5.1 Privacy-preserving techniques overview

The GDPR introduces pseudonymization and anonymization as prominent countermeasures to protect personal data since they lower the risk of linking personal data to their related data subjects. In legal terms, such schemes are forethought differently and independently, while, technically, they offer incommensurable levels of privacy-preserving.

We observed an ongoing debate regarding the effectiveness of privacy-preserving approaches and the inherent risk to re-identify data by using specific reverse engineering technologies or by combining anonymized data with other information [368, 6]. The opinion 05/2014 flagged three main risks related to non-robust privacy-preserving methods [21]:

- "Singling out": when the data subject's data are isolated to identify the natural person attributes or track their localization.
- "Linkability": when correlation of multiple records, at least two, of the same individual leads to the identification of the person.
- "Inference": when a data subject's data are deducted from a dataset or through additional information leading to their identification [290].

By extending the opinion 05/2014 risks, we present a clear categorization and highlight the limitations of the most relevant pseudonymization and anonymization schemes for the ACS environment.

Pseudonymization

The pseudonymization technique is introduced in Article 4 (5) of the GDPR [424] as a privacy-preserving measure and a safeguard that supports data processors and controllers to meet the data protection obligations. Pseudonymization does not remove all identifying information from the personal data but merely reduces the linkability by hiding the identity of the data subjects from third parties [21, 153, 124]. Technically, by using pseudonymization, the data subjects identifiers are substituted by a code, hiding the sensitive data, which can be re-identified using a key [444].

Encryption illustrates perfectly the pseudonymization technique as it uses secret keys that can reversely be decrypted and hence make personal data readable. Within the automated driving context, multiple researchers [316, 113] introduced several privacy-preserving encryption schemes such as CPPA and GSIS where only predefined and trusted authorities are legitimated to decrypt the keys within the vehicular communication system. To that end, encryption increases the confidentiality and lowers the risk of misusing personal data. However, such protection depends on the strength of the algorithm that can be built either using public/private keys or hash functions which guarantee different levels of security [381].

Tokenization is another pseudonymization scheme that can be considered within the vehicular environment. It is the process of replacing sensitive characters by other random non-sensitive values that cannot be mathematically computed from the data source length [361]. Although, when applied to location data, even if the identities are replaced by pseudonyms, individuals can still be singled out and tracked, as demonstrated by De Montjoye et al. [109].

ZKP is a promising cryptographic protocol that is based on an exchange of messages between a prover and a verifier where the prover has a secret but does not reveal information about the secret, per se. However, the prover should provide more information about their secret to establish the trust with the verifier [446]. Gabay, Akkaya and Cebe [172] demonstrated how ZKP can be used for electric vehicle authentication within the V2X communication. ENISA [153, 124] presented the ZKP as a pseudonymization technique implementing authentication and which increases confidentiality and data minimization required by the GDPR, although, the additional collected information by the verifier presents a risk for a future data leakage and again impacts the individual's privacy.

Consequently, not all pseudonymization techniques are suitable to any sensitive data type within the ACS environment. In addition, data controllers and data processors have to keep track of such techniques to make the processing part of the GDPR scope. Furthermore, the combination of pseudonymization with further anonymization-based schemes is much recommended and would definitely strengthen the privacy within the ACS ecosystem [6, 153, 21].

Anonymization

The anonymization technique is where both identifiers and keys are removed and the link between individuals and their locations is concealed for identity perturbation purposes [417]. It is considered as a solution to permanently remove personal data leading to identification of a natural person [424]. Recital 26 excludes anonymous information from the GDPR scope as it is assumed to be a long-lasting and irreversible solution. Similarly, the ePrivacy Directive [152] emphasizes erasing or anonymizing traffic and location data within the vehicular communications (Article 6 (1) and Article 9 (1)).Despite the best efforts on removing identifiers or even the keys, privacy can still be compromised [444].

There is a wide spectrum of anonymization techniques that can be applied to protect vehicular data, but their definitions are noticeably overlapping and commonly mistaken [361]. Data randomization (also called noising) and data generalization are the core anonymization families according to opinion 05/2014 of the WP29 [21]. Researchers discussed multiple *randomization* approaches that vary from noise addition, differential privacy, and swapping, to masking.

Noise addition occurs when an appropriate and proportionate noise is added to randomly modify the sensitive data [300]. Applied to location data, noise addition would result in falsifying, for example, the exact differential GPS coordinates with an additional 10 km. Although, with some knowledge about the other dataset's attributes, an attacker can filter out the noise or link it to another database to regenerate the missing information [21]. Differential privacy is a different approach of noise addition that can be applied to larger datasets with the promise of learning useful information about a population while the individual's privacy is conserved. By adding random noise to a set of data before learning from it, private inputs are hidden without impacting the result accuracy [119]. However, simple efforts would lead to inferring or predicting individuals and/or location attributes [192]. Swapping, also called permutation, is a randomization technique that leads to falsifying a data entry by shuffling personal information within a dataset. Although, if a dataset has redundant attributes, the permutation will not be efficient and will lead to potential failure of the intended anonymization goals [21].

Data masking is frequently considered as a further randomization technique that refers to the process of hiding true values to make the sensitive information inconceivable, such as by replacing characters with asterisks [361]. Nevertheless, data masking remains a generic term that refers to the process of hiding true values [153], which at the end can refer to pseudonymization or anonymization [414]. The key measure to classify data masking as either an anonymization or a pseudonymization scheme is the eventual reversibility property. According to the GDPR (Recitals 28 and 29, Article 4 (5)) [424], a reverted process is considered as a pseudonymization technique which, unlike anonymization, makes it subject to different legal provisions and additional technical and organization efforts from data controllers. Therefore, in our view, we consider data masking to be a parent node for pseudonymization and anonymization, as depicted in Figure 3.4. This reflects how easily misunderstandings about the anonymization techniques can lead to unintentional unlawful processing [6].

Generalization is when the attribute's value is substituted with a broad but semantically logical value [339]. Applied to personal data within the automated driving system, generalization can replace the specific location data with a broad city or country name. Such techniques are implemented by generalizing or diluting the identifiers in a way that replaces the week instead of the day and the country instead of a city location [21]. The main limitation of the generalization theories is that it cannot be applied to all types of data such as names or data entry identifiers, yet they remain efficient for location data. Meanwhile, even with the most refined generalization technique, the risk of inference depends on the adversary's knowledge and the selected anonymization parameters [448]. The key generalization techniques, pointed out by the WP29 [21] and ENISA [153], and which can be applied to the ACS personal data, are:

- k-anonymity/aggregation: hides a data subject in the crowd (called also equivalent class) by grouping their attributes with k-1 other individuals. The scheme provides a convenient protection from being singled out, though the inference risk remains important [381].

- l-diversity: handles the k-anonymity limitation by ensuring that in every crowd there are l-different values. Such difference reduces the inference risk but does not completely eliminate it [390].

- t-closeness: is a refinement of the l-diversity theory that aims to set a t-threshold by computing the resemblance of a sensitive value distribution within the equivalent class in comparison to the attribute distribution in the whole dataset [361].

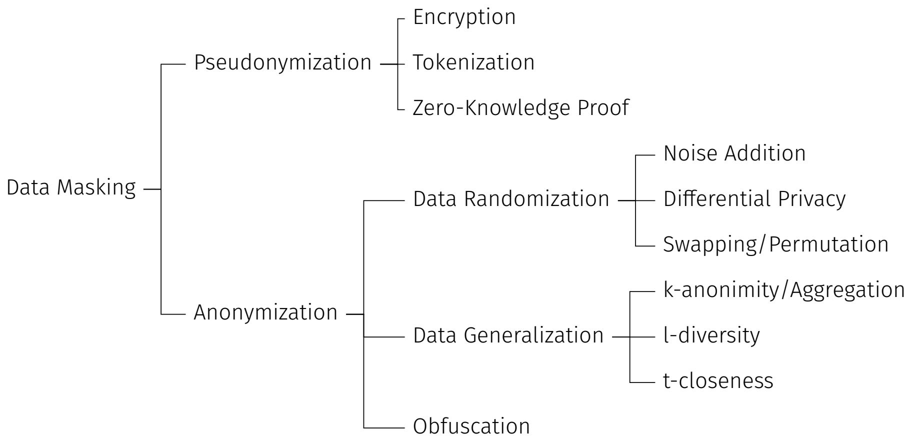


Figure 3.4: Classification of privacy-preserving techniques.

More specific to location data, *obfuscation* techniques are meant to purposely return incorrect location information to make the unauthorized tracking difficult [261]. Although the obfuscation approach is considered as a multifaceted scheme that does not have a straightforward definition in the literature, multiple researchers interpret obfuscation as a type of data masking or noise addition [361, 304, 300], while others [417, 294] define it as a segregated principle from anonymization and pseudonymization. As depicted in Figure 3.4, the obfuscation has been classified as an anonymization scheme for its theoretical irreversibly. Despite the definition, the obfuscation techniques come with the promise to definitively break the linkability between the individuals' data and their location in combination with time, though it is true that obfuscation techniques offer geo-indistinguishability and protect location data. However, such mechanisms remain as vulnerable to re-identification attacks as other anonymization theories, as per Kawamoto and Murakami's attack simulation [261, 337].

To that end, there is no "one-size-fits-all" [300], and privacy-preserving is a process of combining accurate schemes depending on the nature of personal data, the acceptable level of re-identification with regard to data protection obligations, and the intended data usability.

3.5.2 Privacy-preserving pitfalls

The aforementioned discussion highlights the discrepancy between regulator's efforts and scientific works. From the legal perspective, we summarize below our key findings:

- Pseudonymization is indicated as an appropriate "technical and organizational measure" for data protection (Article 25 (1)) [424] without proposing the mixed use of pseudonymization and anonymization schemes to make the privacy-preserving level even higher.

- The GDPR considers the pseudonymization to be a reversible process and anonymization to be permanent without highlighting the de-anonymization risk over the time.

- The opinion 05/2014 WP29 introduced the main risks and mitigation solutions against the re-identification risk of anonymization; though the recommendations do not cope with the rapid evolving technologies as more risks and countermeasures are worthy to be extended by the WP29, which is currently represented by EDPB.

- There is no precision from legal provisions about which anonymization technique should be applied to each context, even if the likelihood of re-identifying personal information might vary from one technique to another [444, 21].

Nonetheless, from the technical perspective:

- The re-identification likelihood can never be zero.

- Anonymization is not everlasting, as it can be reverted in the future. Instead of a one-time operation, it should be assessed continuously.

- The choice of privacy-preserving scheme depends on the nature of the attribute of the private data itself. To illustrate, techniques applied to anonymize a data subject's name or data entry identifier might not be suitable for location data.

- There is a common misunderstanding, as pointed out in Section 3.5.1, in defining data masking as a subcategory of anonymization techniques. However, this technique is broad enough to embed both pseudonymization and anonymization, which would apply to different data protection obligations.

- Some researchers wrongly discussed encryption as an anonymization scheme, though it should be considered as a powerful pseudonymization technique.

- There is no unique solution that fits all processing, but the privacy-preserving technique should be selected on a case-by-case basis and depending on technologies involved within the ACS.

To that end, the implementation of the GDPR principles may fall short even without the compliance violation. Pseudonymization and anonymization help to comply with the data protection obligations. However, they just assist in reducing the risks and not to completely preserve privacy within the automated vehicle ecosystem. Hence, the GDPR-ordained implementation requires further guidance from DPAs and the EDPB to keep pace with the rapidly evolving technologies embedded within the ACS environment.

3.6 Conclusions and future work

Many ACS manufacturers envisage the deployment of ACS for public transport in the coming years. According to The Global Market Insights report [375], its value will rise from 1 billion USD in 2021 to 4 Billion USD in 2028. Addressing the privacy concerns is crucial and a major challenge for the adoption of the ACS. The GDPR EU law provides an unprecedented level of data protection. Nevertheless, the collection and further processing of personal data raise crucial privacy concerns. We have identified the challenges for the principles of purpose limitation and data minimisation resulted from the immense amount of data processed by the ACS. These principles, encapsulated within the concepts of PbD and PbDf, aim to mitigate any risks to the fundamental rights and freedoms of data subjects by the implementation of appropriate technical and organisational measures. These risks are also associated with the multiple data controllers and data processors, and their roles in the lifecycle of data processing as stakeholders of ACS ecosystems. The multiplicity of stakeholders who are involved in collection, transfer and storage of data, complicates the transparency of processing, the adoption of the appropriate and sufficient security measures and, finally, their compliance on the basis of the accountability principle.

With regard to the responsibility of the data processors and sub-processors, new regulatory efforts have been initiated at European level [74] with a view to reinforce the responsibilities throughout the supply chain. Similar efforts could be initiated for the management of the automated and connected vehicles supply chain. It should be highlighted that the efforts to address the regulatory complexity of the innovative ecosystems should be approached in an interdisciplinary way by examining all the existing regulatory aspects in the domain of AI, privacy, human rights, together with the involving technologies and per sector. For instance, in 2021 the draft of the AI act was circulated by the EU [160], destined to impact the critical infrastructures, the transport sector being one of them.

In this work we raise the complexity of the stakeholders duties and how they may accumulate multiple roles and obligations. Our recommendation to the stakeholders, who act as controllers and processors, is to encompass all those factors to protect fundamental rights and prevent potential data breaches within the ACS environment. We advise to push for deploying specific use cases with constant security control, monitoring and assessment overtime. Additionally, the present paper discussed the discrepancy between the privacy preserving techniques and the way the same techniques are advocated by the GDPR. As the existing data protection laws leave much uncertainty about the effectiveness of pseudonymization and anonymization as major countermeasures, the present work recommends a combination of legal provisions, more fine grained definitions and a description of specific technologies preventing from re-identifying personal data within the automated driving ecosystem. Additionally, we endorse continuous control and aggregated countermeasures to exchange data and knowledge leading towards lawful processing, secure interoperability and safe integration of ACS to the new mobility concepts. As a matter of fact, the present findings can be considered as the foundation for a potential upgrade of the European personal data protection regulations to provide more granular insights on the ACS's stakeholders roles and reconsider the de-anonymization risks for an optimal data privacy protection within the IoV environment.

As an ongoing effort, and under the umbrella of the AVENUE project, a data privacy assessment will be implemented to rate, audit and quantify the technical and organisation mitigation techniques in place with regard to the GDPR requirements. Then, by elevating the findings from the present work, we intend to provide a risk management plan to the potential privacy threats through a real testbed on a predefined testing site, and over a vehicle of SAE automation level four.

As a future work regarding the security and, more specifically, the implementation of PbD within the ACS landscape, there is a need to have more clarity as there is no consensus nor directive on the exact definition or methodology of what this implementation should look like. As an example, collecting data from non users (data subjects that are not using the ACS) [281] should be looked at as a future work, as the ACSs' cameras can collect images of the outside environment of the vehicle, personal video surveillance concerns should be raised to protect not only the users but also non users of the ACS. Moreover, another open issue requiring further research is the insurance regimes in case of hacked ACSs or personal data breach. The classic vehicular insurance model is more likely to evolve with the wide spread integration of ACSs. The new transition from driver controlled public transportation vehicles to ACSs operating without human interaction will obviously impact the insurance fees and policies and their implication to the public transport sector.

Acknowledgment

This work has been funded and supported by the European Union's Horizon 2020 Research and Innovation Programme through AVENUE project (https://h2020-avenue.eu/) under grant agreement No 769033, nIoVe project (https://www.niove.eu/) under grant agreement No 833742 and SHOW project (https://show-project.eu/) under grant agreement No 875530.

Chapter 4

Article III: Analysis on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap

Relevance

As part of the investigations towards answering RQ2 and RQ3, this article complements the findings from the article presented in Chapter 2. In here, we examined the CAV's standards and regulations, from the cybersecurity and data privacy perspectives, in two ways: (i) from a critical point of view of the standards' guidelines and regulations requirements as well as their applicability to address and overcome the CAV's threats (ii) from a visual representation mapping the corresponding standards and regulations to each CAV's layer depicted in the format of an SCM

Context

This article was presented at the TRA conference in November 2022 and discussed through a poster (Section 8.5). The conference proceeding article was further edited and published as an extended version in the Transportation Engineering journal whose IS: 5.40, h-Index: 13 and SJR: 0.864 according to the Resurchify portal[1].

Own contribution

Being the lead author, the majority of the content was provided by me while co-authors supported with their reviews and orientations. I elaborated the manuscript's analysis, discussions and findings and got assisted by co-authors in the figures and tables' visualisation.

[1] https://www.resurchify.com/about

Contents

4.1 Abstract

Protecting CAVs from cyber attacks and data breaches is a major challenge facing the deployment of driverless vehicles. The CAV is a complex interconnected system consisting of sensors, AI processors and external units to assure the automated driving without human interaction. Such complexity increases the attack surfaces and makes the CAV highly vulnerable to cyber assaults. It also entangles security audits and certifications procedures. Our work lays out a novel approach towards CAV's certification focused on cybersecurity and data privacy aspects. Stipulated by the analysis on existing standards' limitations, we propose a Standards Coverage Map (SCM) outlining the CAV's entire ecosystem and linking organisational and technical aspects to the latest standards and regulations from the cyber perspective.

4.2 Introduction

The CAV embedding cutting edge sensors, advanced ECUs, trailblazing AI components, and connection to everything, has the potential to beneficially change the transport dimensions in the future. Six levels, varying from L0 (no automation) to L5 (fully automated), were predefined by the SAE through the SAE J3016 and the ISO/SAE 22736 standards as depicted in Table 4.1. Every level is differentiated by the reference to the automation of the Dynamic Driving Task (DDT), reflecting the human as well as the ADS engagement, and the ODD describing the driving conditions and delimitation[389].

To assure the CAV's highly autonomous navigation of SAE L4 and L5, the vehicle intelligently compiles inputs from both its internal (including cameras, GPS, RADAR, LiDAR, TPMS, odometric, and ultrasound sensors) and endless external connections to the infrastructure (V2I), to other vehicles (V2V), to cloud (V2C), to grid (V2G) and to everything (V2X) [41], as depicted in Figure 4.1. Such connectivity is built through multiple channels like DSRC and cellular (LTE/5G) leading to the spontaneous creation of VANETs [287]. However, such high automation and ubiquitous connectivity imposes the CAV to inherit cybersecurity and data privacy challenges and opens up caveats for audit and certification concerns.

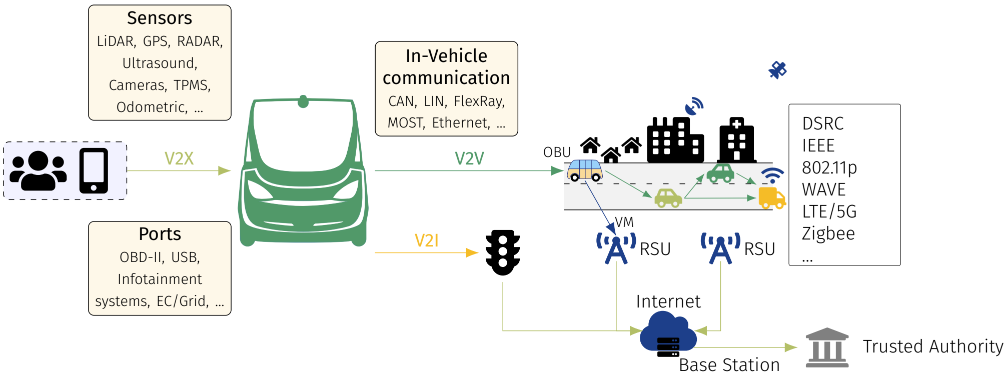

Sensors
LiDAR, GPS, RADAR, Ultrasound, Cameras, TPMS, Odometric, ...
In-Vehicle communication
CAN, LIN, FlexRay, MOST, Ethernet, ...
V2X
V2V
OBU
VM
DSRC
IEEE 802.11p
WAVE
LTE/5G
Zigbee
...
Ports
OBD-II, USB, Infotainment systems, EC/Grid, ...
V2I
RSU
RSU
Internet
Base Station
Trusted Authority

Figure 4.1: CAV's environment and attack surfaces.

Physical audits have been the unique method for safety certification of conventional vehicles [174]. Though, with the emerging technologies like CAVs, the physical testing is not feasible and adapted procedures are needed [319]. Additionally, safety is not the unique concern as the CAVs' stakeholders are highly aware of the new cybersecurity risks. Several researchers reported multiple attacks over CAVs varying from getting control over decision making units [330], imperiling the vehicle's sensors [462] to location tracking revealing the passengers and vehicle identities [23]. Safety and cybersecurity are closely related as demonstrated by cybersecurity researchers [43], where a simple spoofing or a jamming attack can blind the vehicle from existent obstacles [314]. Nevertheless, while the safety requirements are standardised, the processes and methods for vehicular cybersecurity are generic. This is underlined by standardisation and regulatory bodies who consider the automotive cybersecurity state of the art as immature [396].

Table 4.1: SAE automation levels by SAE J3016 and ISO/SAE 22736 [389, 206, 180].

Properties	L0	L1	L2	L3	L4	L5
Driving automation	No	Driver assistance	Partial	Conditional	High	Full
ODD	N/A	Domain specific	Domain specific	Domain specific	Domain specific	Unlimited
DDT fallback	Driver	Driver	Driver	Fallback ready-user	ADS or fallback ready-user	ADS
Connectivity	Not required	Not required	Not required	Recommended	Recommended	Extended V2X

Cybersecurity and data privacy audit assesses the entire information security management to provide evidence on how the system is protected from threats and data leakages. Such process is conducted through verification plans within real world scenarios. Those plans can also be called certifications if the evaluation is conducted upon a single or multiple standards by external authorised organisations [231]. To that end, certifications' processes tie together organisational and technical procedures, including the audit, to assure that the assessed risks have been controlled.

Under the auspices of SDOs, efforts were made to shield the CAV's environment. The ISO and SAE claim to provide a complete cybersecurity management for the driverless landscape [398]. The UNECE published acts to unify the automotive standards by requiring the CSMS and Software Update Management System (SUMS) certifications for the SAE L3 onward. The GDPR is the fundamental privacy data law in Europe. The ETSI, ITU, 5G Automotive Association (5GAA) and AUTOSAR institutions provide advice for securing vehicular communication [271].

Despite the notable publications by the SDOs, the evolving attack feasibility and the SAE's levels introduce a new dimension of complexity, which blurs the certification process and creates uncertainty. The existing and WIP standards are applicable commonly to vehicles of SAE L3 where the risks are incomparable and have to be tackled differently from those of L4 and L5. Depending on the SAE level, the driver or the ADS has to take over or relinquish the DDT in case of a fallback led by a system failure or a cyber attack [180]. In the instance of a blinding attack targeting the perception sensors of an L3 or an L4, a fallback ready-user (remote or in-vehicle driver) can drive the vehicle into a stable and safe condition (also called Minimal Risk Condition (MRC)[389]). Projecting an equivalent scenario over an L5 CAV, the ADS per se must achieve the MRC independently from any type of human intervention. As reflected in Table 4.1, several features support distinguishing the properties of each SAE level including the ODD limitation, how the MRC can be conducted, and the connectivity multiplicity. However, by combining the three highest SAE levels, the SDOs consider cyber threats and their related risks to be governed equally despite their properties' dissimilarity.

Furthermore, the multiple regulations are overlapping and end up by pointing to the CSMS and SUMS certifications or to high level standards which are broad enough to not to cope with the particularities of the CAV's cyber and privacy risks [309]. Thus, an SCM would guide cybersecurity and data privacy assessment and monitoring on the CAVs landscape. Our work identifies the promising standards and links them to sub-components which need to be audited. Our added value and main contributions are summarised as follows:

- Investigation into the gaps and faults of existing standards, regulations and certification schemes, which aim to fulfil the vehicular cybersecurity and data protection expectations within CAVs' of SAE L4 and L5.

- Development of an SCM combining technical and organisational requirements where attack surfaces are mapped to standards and regulations to serve as the foundation of a future cybersecurity and data privacy certification model.

These aimed contributions create ample opportunity to gear up the following RQs. First, we analyse *what are the limitations of the CAVs' cybersecurity and data privacy related standards and regulations, by building a structural representation of the standards suitability* in Section 4.4 (RQ1). Secondly, we evaluate *weather a combination of existing standards and regulations offer the foundation to build a future cybersecurity and data protection certification framework* (RQ2).

The paper is structured as follows: Section 4.3 makes a comparison of the present work with recent efforts. Section 4.4 delivers a review of crucial standards and regulations. Section 4.5 outlines the CAVs' SCM and its development methodology. Finally, Section 4.6 offers future work orientation while Section 4.7 summarises our findings and provides concluding remarks.

4.3 Related work

A plethora of studies on building safety certification models for CAVs' environment exists, while the reviews on cybersecurity and data privacy certification models remain barely evoked. Furthermore, we observe a scarcity of multi-standards frameworks defining how to thoroughly certify the CAV's system-wide layers. There is also a remarkable lack on reviews pointing out data privacy certification as it is believed that the GDPR compliance is all what is required for assuring an optimal data protection. We highlight researchers' efforts aiming to construct holistic cybersecurity and data privacy assessments of the CAV's environment based on existing and emerging standards and regulations.

Through multiple publications and in collaboration with other authors, Schmittner has been tracking the progress of the ISO/SAE 21434 development and implemented an automotive cybersecurity risk management solution compliant to that standard. Schmittner and Macher [395] provided an initial overview of the first automotive initiatives on elaborating CAV's safety and cybersecurity standards. They presented a preview of the ISO/SAE 21434 structure that was still a WIP at that time in addition to all the other under development standards by SAE, ITU and UNECE. Subsequently, Schoitsch and Schmittner [398] provided an updated review on the ongoing SDOs efforts with a focus on ISO and UNECE. In a risk management-based approach, Schmittner, Schrammel and Konig [396] discussed an asset based automotive cybersecurity risk management approach stemming from ISO/SAE 21434. Furthermore, Vogt et al. [443] presented the interaction between safety and security through the ISO 26262 and ISO/SAE 21434 respectively. To that end, those approaches outlined succinct risk assessment methodologies without reflecting other SDOs's standards.

Similarly, Marksteiner et al. [321] proposed a standardised testing process of automotive cybersecurity based on ISO/SAE 21434 and the latest regulations R155 (CSMS) and R156 (SUMS) from the UNECE. In another work, Marksteiner and Bronfman [319] highlighted the limitations of the standard for not specifying the testing procedure. To that end, the authors designed a black box security testing as a compliment to that standard. Their analysis showcased improvement avenues that are applicable to any type of vehicle where ADS or V2X are implemented without directly considering the full automation property.

Mateo Sanguino, Lozano Domínguez and Carvalho Baptista [323] provided a literature review on cybersecurity certifications and audits based standards. The authors identified the steps toward cybersecurity certification in addition to a listing of audit techniques and certifying bodies. As with the rapid development of automotive standards, ISO/SAE 21434 and ISO/PAS 5112 were not reported by the time of the research work elaboration. Kim and Shrestha [271] pointed out the standardisation and regulation challenges with regard to the complex CAV environment. The authors classified the legal and standardisation requirements impacting the CAV into three groups: automotive industry, DSRC wireless based and 5G V2X communication regulations. Per each group, the authors identified the relevant regulations and standardisation bodies initiatives. However, the review combines both safety and cybersecurity and is focused mostly on V2X standards. Sui and Muehl [411] adopted a similar approach by providing a high level overview of the mainstream standards related to V2X. Khalid Khan, Shiwakoti and Stasinopoulos [263] delineated a conceptual cybersecurity assessment model anticipating, in a cause-effect manner, the possible system behaviour upon the deployed CAV's cybersecurity mechanisms. The authors developed a model that was distinct from any standard or regulatory obligation as their analysis showcased that existent policies do not keep pace with the rapidly evolving cybersecurity risks.

Per the analysis from the existing studies, we differentiate from the aforementioned works by: (i) Focusing on CAV's cybersecurity and data privacy regulations and standardisation and not safety or physical security certification (ii) Providing an up to date review on the ongoing efforts from the SDOs on the automotive cybersecurity and data privacy standardisation and regulation (iii) Mapping the identified standards to procedural and technical layers of the CAV's ecosystem through the SCM

4.4 Key standards and regulations efforts

4.4.1 Active SDOs in vehicular cybersecurity and data privacy landscape

With the CAVs emergence, the development of multiple standards and regulations have been witnessed by numerous working groups from the global SDOs. The SAE was the first standardisation body to issue a vehicular cybersecurity standard through the SAE J3016 [389]. From ISO, the ISO/TC22, ISO/TC204 and ISO/IEC JT1 are the key active committees on vehicular cybersecurity, ITS concerns and privacy assessments accordingly. As described in details in 4.7, the first committee focuses on standardising the CAVs' safety and cybersecurity risk management systems mainly through the ISO/SAE 21434 (where they joined their efforts with the SAE) and ISO/PAS 5112. The second committee provides the basic taxonomy of terms related to automated driving systems and associated security guidelines of the V2X communication through standards such as ISO/TS 21177 and ISO/TR 21286-3. Furthermore, the ISO/IEC JT1 aims to standardise security and privacy evaluations processes and procedures through the ISO/IEC PWI 5888 and ISO/IEC 29134.

UNECE has a devoted task force working towards global vehicular cybersecurity regulations. Through the new regulations R155 and R156, the UNECE WP29 made the CSMS and SUMS certification mandatory in Europe for all new vehicles' types starting from June 2022 and for all vehicles starting from 2024 [319]. Still from the United Nation board, the ITU working groups developed series of security recommendations related to connected vehicles, on the one hand, X.1371 to X.1376 [244, 249] which outline security threats definition, security guidelines for V2X, specification of secure software update procedure for ITS's devices and guidelines for intrusion and misbehaviour detection. On the other hand, the ITU has a dedicated Focus Group-AI for Autonomous and Assisted Driving (FG-AI4AD) that is more focused on ethical and legal matters with regard to the vehicle SAE level. Moreover, the ETSI proposed several standards related to security, privacy and establishment of standardised architecture for connected vehicles. However, these guidelines are not specifying or targeting a specific CAVs' automation level.

The working group 7 from the 5GAA is another global organisation who published multiple technical guidelines aiming to unify security and privacy requirements for the cooperative V2X [1, 2]. In collaborations with ETSI, ISO and SAE, the 5GAA is promoting standards supporting 5G connectivity and its implementation within the V2X communication [271]. Before that, the 3rd Generation Partnership Project (3GPP) provided the first V2X foundations, but they were limited to the Long-Term Evolution (LTE) connectivity [442]. Furthermore, the automotive industry has also pushed to standardise security approaches over on-board systems through their collaboration on AUTOSAR standards. AUTOSAR recommendation series tend to secure in-vehicle communication networks and ECUs, protect data confidentially and implement cryptography. From the data protection perspective, the GDPR remains the main law to comply with for data protection in any context including the vehicular environment. Nonetheless, the law provides the basic obligations to consider by the CAVs stakeholder without guaranteeing an optimal protection from data privacy risks.

4.4.2 Key regulations and standards for cybersecurity and data privacy assessments

In this section, a review of the crucial regulations and standards is provided. Their gaps and limitations are also highlighted. We constrain our analysis to explore only the standards and regulations that have been promoted and cross-referred by the key SDOs. Additionally, as presented in Section 4.3, they have been the main focus of multiple researchers as they are perceived to assure a flawless protection from cyber threats and data privacy violation. Figure 4.2 wraps those standards and regulations in a pyramid structure presentation view, where each slab represents a more narrowed and granular recommendations from the automotive cybersecurity assessment perspective. The pyramid base consists of generic, yet compulsory regulations. The second slab is represented by ISO/SAE 21434, the generic cybersecurity risk management framework that is pointed out by the UNECE R155 and UNECE R156. The third slab epitomises the ISO/SAE 8475 which complements the outcome from the previous layer. The fourth level checks the conformity of those outcomes through ISO/SAE PWI 8477. Finally, the pyramid summit is represented by ISO/PAS 5112 which encapsulates all previous outputs yielding to the CAVs' procedural audit.

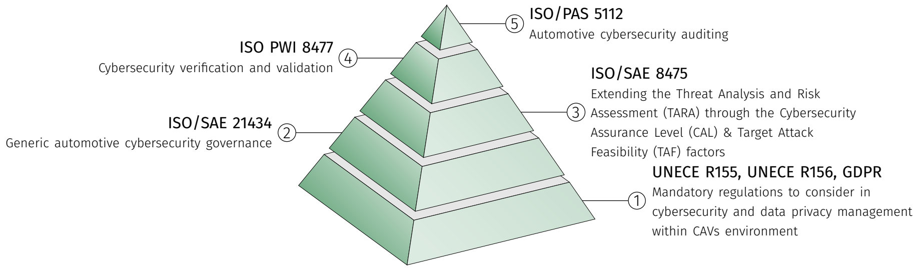

ISO/PAS 5112
Automotive cybersecurity auditing
5
ISO PWI 8477
Cybersecurity verification and validation
4
ISO/SAE 8475
Extending the Threat Analysis and Risk Assessment (TARA) through the Cybersecurity Assurance Level (CAL) & Target Attack Feasibility (TAF) factors
3
ISO/SAE 21434
Generic automotive cybersecurity governance
2
UNECE R155, UNECE R156, GDPR
Mandatory regulations to consider in cybersecurity and data privacy management within CAVs environment
1

Figure 4.2: Key regulations and standards co-relation.

UNECE R155 [430] is the prominent regulation making the CSMS certification mandatory at the vehicle type approval stage. The CSMS certification aims to provide a trustworthy proof of efficient threat governance, including risk monitoring, assessment and mitigation. While the UNECE R155 regulation requires the manufacturer to have a cybersecurity management system in place counter-measuring the predefined risks annexed to the regulation; the risk of unknown attacks, also annotated hereinafter as residual risks, occurrence remain high with the CAV ecosystem [263]. Additionally, the regulation is limited to vehicles of SAE L3 onward. In other words, the UNECE R155 considers vehicles of L3, L4 and L5 to be proportionately qualified to respond to limited cyber threats, which backfires the CSMS efficiency.

UNECE R156 [431] comes along with UNECE R155 to ensure that the manufacturer put in place appropriate safety and security processes for conducting software updates. The regulation mandates an assessment that has to be carried out, exclusively, by approval authorities, who issue a SUMS certification upon the software update processes' conformity at type approval stage. According to the regulation, the SUMS has to be renewed every three years or after major software updates occurring even before the end of the three years cycle. Albeit the recently published ISO 24089 has brought out several requirements related to software update processes, technical specifications per se are still lacking as the SUMS is limited to assessing the self-documented measures developed by the manufacturer.

GDPR [424] is perceived as the most advanced European personal data protection framework with a global impact [271]. The GDPR sets strict obligations related to personal data processing, rights for concerned individuals, technical requirements to employ privacy preserving mitigation strategies, and DPIA deployment for any new technologies with privacy risks. However, within the CAV's complex environment, the application of the GDPR data processing principles remain convoluted, as the CAV's stakeholder can accumulate multiple roles making them data processors and data controllers at the same time [44]. Another limitation of the GDPR is that it excludes anonymisation as a privacy preserving technique from the legislation scope considering that it is a permanent solution. Though, with minor reverse engineering efforts, the personal data can be de-anonymised with no compliance violation to the GDPR [153]. Based on the GDPR requirements, further analysis on data privacy protection was evoked by the EDPB [147, 149]. Although the EDPB's guidelines are referring to the processing of personal data in relation to CAVs and highly recommends the DPIA execution, they inherit the GDPR's pitfalls. To that end, a successful implementation of DPIA, and even full compliance to the GDPR, does not rhyme with an absolute personal data protection for CAVs, confirming the need for a combined execution of further standards from the upper levels as depicted in Figure 4.2.

ISO/SAE 21434 [233] came up with high level definitions and guidelines to implement cybersecurity management principles throughout the entire life-cycle, including concept, development and post-development phases for all road vehicles. In a light-weighted approach, the standard elicited the road map on how to conduct TARA, the appropriate cybersecurity assessment for the vehicular vulnerabilities [40], which is intended to be extended in ISO/SAE 8475. Similar to TARA presentation, the standard introduced fundamental definitions for other cybersecurity actions and processes like cybersecurity verification and validation in addition to auditing that are elevated further in ISO/SAE PWI 8477 and ISO/PAS 5112 respectively. Though, the standard scope is broad enough to cover all vehicles with electrical and electronic systems that can match any SAE level. Additionally, the ISO/SAE 21434 did not evoke specific technologies to counter cybersecurity risks. Furthermore, while it is true that it offers agility on applying security concepts at different stages of the vehicle life-cycle, no detailed guidance is provided on how to implement them and using which tools.

ISO/SAE 8475 [234] evokes the Cybersecurity Assurance Level (CAL) and Targeted Attack Feasibility (TAF) factors to complement the TARA process introduced by the ISO/SAE 21434. In parallel to TARA steps, the CAL is initiated and reviewed throughout the process to reflect the assurance level and confidence on the asset protection. Conversely, the TAF represents an additional metric to the assessment reflecting the intended level of attack feasibility. Both the CAL and TAF can be used for continuous monitoring, which means even after the TARA accomplishment. Additionally, they can be updated whenever an operational change occur to the system.

ISO/SAE PWI 8477 [236] is foreseen as a complement to the ISO/SAE 21434, ISO/SAE 8475 and UNECE R155 where the TARA outcomes are verified and the residual risks are validated. On the one hand, the verification process relies on confirming the appropriateness of the risk treatment conducted within the TARA. It iteratively justifies the conformity of the implemented risk mitigation with regard the cybersecurity requirements until no further refinement is necessary. On the other hand, the validation process aims to confirm, with tolerable level of confidence, that the residual risk is acceptable. The cybersecurity validation can be executed through fuzzy or penetration testing with the intention to test the system's robustness. To that end, the ISO/SAE PWI 8477 standard can provide valuable technical inputs to conduct procedural audit as defined in ISO/PAS 5112 standard.

ISO/PAS 5112 [231] is a result of combining the outcomes and requirements from preceding levels as shown in Figure 4.1. Consequently, the brand new standard provides an extension of the ISO/SAE 21434 through a mapping of the audit objectives and evidences managing the conformity to the CSMS and SUMS certifications program. The standard aims to be applicable to conduct internal or external audits as well as to train auditors competences. Albeit the ISO/PAS 5112 orients toward a successful audit program focusing on organisational cybersecurity processes, it does not provide technical requirements on achieving cybersecurity or data privacy assessments.

As an answer for RQ1, the following limitations demonstrate shortcomings of the key existing standards and regulations:

- The current approaches remain generic to different automation levels, while the highly automated vehicles of SAE L4 and L5 should be tackled properly with reference to their features including ODD, DDT fallback and connectivity as reported in Table 4.1.

- The standards do not consider granular evaluation per CAV's layer and sub components.

- Standards that are providing coarse verification techniques, as per ISO/SAE 8475 and ISO/SAE PWI 8477, are still WIP which make them more tailored to major changes and with the risk to influence the audit quality that can be perceived by the ISO/SAE 5112.

- The data protection within CAV's environment requires more efforts to strengthen the existing regulation and to provide more insights on conducting continuous privacy assessments.

4.5 CAV’s ecosystem standards coverage map

The present section discusses the established methodology on constructing the SCM, delineates its layers and outlines the confronted challenges on building such mapping.

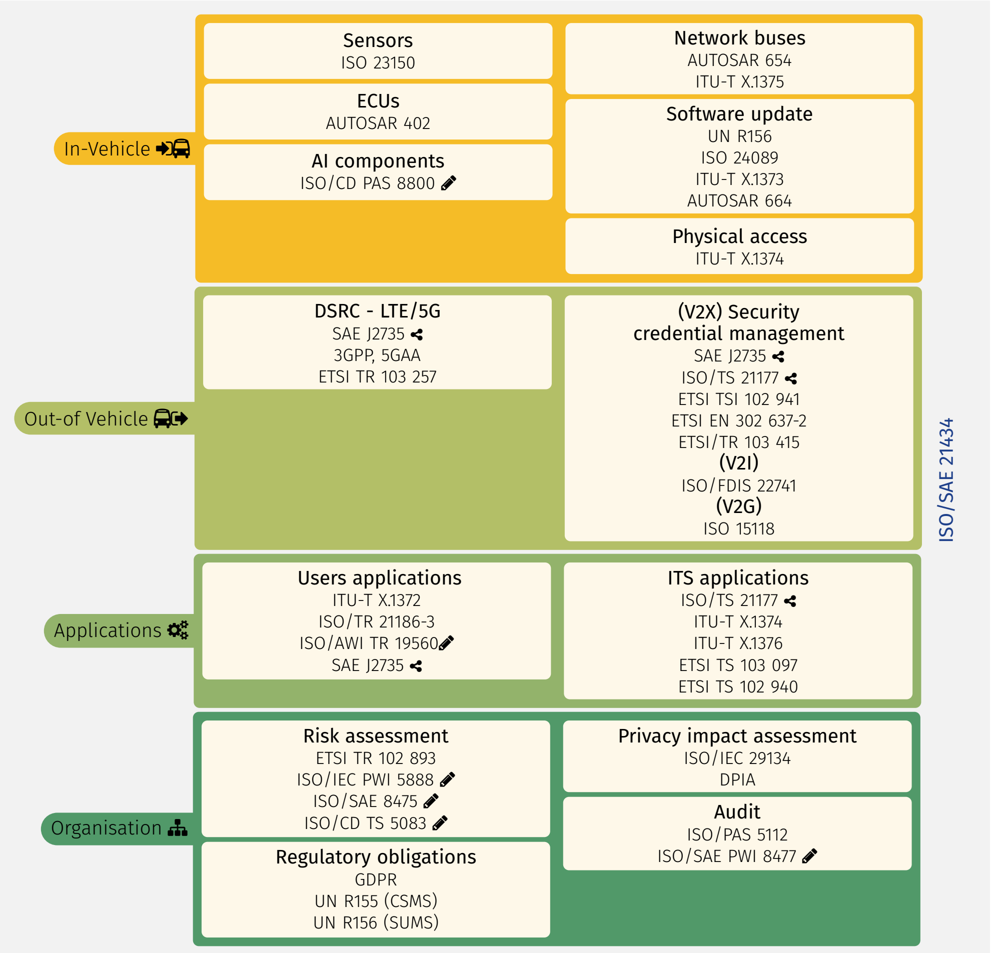
4.5.1 Methodology

A suitable approach to build a robust cybersecurity and data privacy certification framework starts from a foresight analysis of the CAV’s potential threats, an in-depth assimilation of the existing regulatory and standardisation bodies efforts; and a visual representation that simplifies the knotted CAV’s ecosystem. We initiated our process with building a taxonomy of potential threats and mapped them to their related attack surfaces and mitigation schemes through our previous works [41, 44]. This approach enabled a granular capturing of all the components requiring a cybersecurity and data privacy assessments which supported to construct our SCM. We opted for a representation reflecting the empirical attack surfaces, the intertwined standardised processes and the main facets of cybersecurity audits. Furthermore, guided by the review of the most recent standards from Section 4.4, we elevate our SCM further by matching the identified attack surfaces to the existing or WIP standards as drawn in 4.7. As a result, Figure 4.3 depicts our SCM which combines the technical and organisational audit avenues applied to the CAV’s ecosystem. The map is classified into four layers: in-vehicle, out-of vehicle, applications and organisation, where every layer groups the respective technical standards. As a parent node of the four layers, ISO/SAE 21434 is set as the core, yet the broad standard. The combination of both generic and technical standards on the SCM is foreseen to overcome the broadening of the ISO/SAE 21434 leading to a more thorough assessment.

4.5.2 The SCM layers

The in-vehicle layer incorporates the attack surfaces at the vehicle level which we classify into six sub-layers. First, ‘sensors’ category defines the guidance on standardising the interfaces between the different sensors and the fusion unit leading to the automation navigation decisions. Second, ‘network buses’ category where standards propose guidelines on detecting intrusions and authentication measures within the in-vehicle communication networks. Third, the ‘ECUs’ standard aims to prevent from non-authorised access to the vehicular software modules. Fourth, ‘software update’ outlines the directives on how to conduct secure software update during the vehicle life-cycle. Fifth, ‘AI components’ standard provides guidance on secure usage of AI-based functions involved on the automation decision making. Finally, the ‘physical access’ specifies countermeasures against threats from plugged external devices.

The out-of vehicle layer relies on two main categories wrapping standards related to CAV’s internet channels and V2X communications. To secure the CAV’s internet access using ‘DSRC, LTE and 5G’, considerable standards provided a set of secure channel models and through several use cases. Besides, the multiple V2X communications have been standardised by ISO, ETSI and SAE. The ‘security credential management’ standards, which sets V2X certificates security and privacy



In-Vehicle

Sensors
ISO 23150

ECUs
AUTOSAR 402

AI components
ISO/CD PAS 8800 ✎

Network buses
AUTOSAR 654
ITU-T X.1375

Software update
UN R156
ISO 24089
ITU-T X.1373
AUTOSAR 664

Physical access
ITU-T X.1374

Out-of Vehicle

DSRC - LTE/5G
SAE J2735 <
3GPP, 5GAA
ETSI TR 103 257

(V2X) Security
credential management
SAE J2735 <
ISO/TS 21177 <
ETSI TSI 102 941
ETSI EN 302 637-2
ETSI/TR 103 415
(V2I)
ISO/FDIS 22741
(V2G)
ISO 15118

Applications

Users applications
ITU-T X.1372
ISO/TR 21186-3
ISO/AWI TR 19560✎
SAE J2735 <

ITS applications
ISO/TS 21177 <
ITU-T X.1374
ITU-T X.1376
ETSI TS 103 097
ETSI TS 102 940

Organisation

Risk assessment
ETSI TR 102 893
ISO/IEC PWI 5888 ✎
ISO/SAE 8475 ✎
ISO/CD TS 5083 ✎

Regulatory obligations
GDPR
UN R155 (CSMS)
UN R156 (SUMS)

Privacy impact assessment
ISO/IEC 29134
DPIA

Audit
ISO/PAS 5112
ISO/SAE PWI 8477 ✎

ISO/SAE 21434

✎ = Work in progress

< = Present in multiple layers

Figure 4.3: CAV's ecosystem SCM.

requirements, define the precise structure, format, and authentication schemes supporting the CAV's communication to peer instances. It is noteworthy to mention that other V2X communications such as 'V2I' and 'V2G' have been supported by dedicated standards while others as per the V2C is still considered under the umbrella of broad standards like SAE J2735.

The application layer consists of two sub-layers reflecting two types of applications: users and ITS. The CAV's deployment is associated to the means of several services provided to the end user and to the smart city. The 'users applications' standards focus on data access and cryptography best practices to consider while building interfaces to the CAV's hardware or software. Likewise, the 'ITS applications' standards recommend mechanisms to determine permitted actions among the peer ITS applications to achieve security properties such as authorization, integrity and confidentially. Though, it is worthy to be highlighted that standards such as SAE J2735 and ISO/TS 21177 have larger scope covering the V2X communication in general and, hence, other sub-components from the second layer too.

The organisation layer incorporates four procedural sub-layers. The 'risk assessment' reflects evaluation procedures on quantifying cybersecurity threats likelihood and impact. The 'privacy impact assessment' warps standardised processes and reports on privacy impact assessments. The 'regulatory obligations' sets the mandatory laws that the CAV's environment has to comply with which are summarised into the GDPR, UNECE R155 and R156. Finally, the 'audit' group wraps the cybersecurity verification, validation and auditing processes that are encapsulated on ISO PAS 8477 and ISO/PAS 5112.

4.5.3 Challenges

To build our SCM and synthesised standards in 4.7, several challenges were confronted where few assumptions were made. First, the identified standards' scope, even for the most technical ones, aggregate multiple attack surfaces which justifies their appearance in multiple sub-layers as shown in Figure 4.3. Second, duplicated efforts were observed to protect components such as software update, V2X communication and ITS applications while other vectors remain uncovered or limited. Additionally, the SAE level definition lacks granular descriptions within multiple guidelines. Very few standards like ISO/PAS 5112 and ISO/CD TS 5083 specify the automation level to be L3 onward, while the others either target connected vehicles without automation description or invoke the presence of ADS (which provides partial automation at L2 and full automation starting from L3 [278]). To that end, standards targeting only connected vehicles are classified in 4.7 to be of SAE L1 onward, while standards covering vehicles with implemented ADS are foreseen to be an L2 onward. On the same note, a Not Applicable (NA) attribute was assigned to standards where knowledge on the connectivity maturity or ADS availability was lacking, as well as when the standards' scope is not limited to CAVs.

4.6 Discussion & future work

The SCM presented in this paper is currently an ongoing research. To address RQ2, the SCM has been developed to reflect an efficient approach on tackling the overall cybersecurity and data privacy CAV's assessment and as a step toward building a certification framework considering risks related to L4 and L5 CAVs. It is envisioned to conduct several iterations of the SCM to cope with the rapidly evolving CAV's technologies and to keep pace with the regulation and standardisation efforts. As a work in progress, we intend to build a certification framework for CAV's ecosystem that represents the road-map to audit the whole system layers. Based on sets of procedures and processes and a clear workflow, the framework aims to identify, in a step by step manner, the path to a compliant environment. The archetype would introduce a harmonised ratings reflecting the evolving attacks feasibility, priority and impact per SAE automation level. It aims to measure and quantify risks upon an established catalogue of scenarios related to cybersecurity critical situations and personal data leakage. Then, a testing environment with predefined architecture and configuration will be chosen to deploy the required assessment on a pass-fail criteria mode. In other words, the verification of our certification framework is foreseen to be tested in real world cases, specifically within the scope of SHOW [401] and ULTIMO [140] projects where vehicles of SAE L4 and L5 are deployed.

4.7 Conclusion

It is true that there is no standard to identify what constitutes or motivates a cyber assault, though the CAVs' standards need to be specific and improved to effectively protect from malicious attacks harming the CAVs' users security, privacy and, hence, safety. The attacks will not remain frozen in time, hence, standards, regulations and adequate risk management models have to continuously evolve to ensure an optimal protection. Our research goal was threefold: present an up to date review of the SDOs efforts, highlight the key standards and regulations with a review of their current limitations and provide the technical and procedural audit avenues through the SCM. Per our findings, topic on how to ensure the CAV cybersecurity and data privacy certification is still not comprehensively addressed. The existing approaches remain theoretical, broad and not holistic to cover all the sophisticated sub-components of the complex CAVs' environment. Bearing that in mind, we proposed the SCM which wraps potential attack surfaces, the most recent SDOs efforts, and both generic and specific guidelines into a graphical view.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 875530 through SHOW project, Horizon Europe research and innovation programme under grant agreement No 101077587 through ULTIMO project and from the Swiss State Secretariat for Education, Research and Innovation (SERI). We would also like to thank Teri Lenard for the valuable insights on the manuscript and proofreading.

Appendix A: Standards summary

Table 4.2: CAV's cybersecurity and privacy standards baseline.

Organisation	Standard ID	Year	Scope	SAE[1]	Description
ISO/TC22	ISO/SAE 21434 [233]	2021	CAV	●●●●●●	Cybersecurity engineering
	ISO/PAS 5112 [231]	2022	CAV	○○○●●●	Guidelines for auditing cybersecurity engineering
	ISO 23150 [212]	2021	CAV	○○●●●●	Data communication between sensors and data fusion unit for automated driving functions
	ISO 15118 [207]	2019	CAV	○●●●●●	Vehicle to grid communication interface
	ISO/CD PAS 8800 [218]	WIP	CAV	○○○●●●	Safety and artificial intelligence
	ISO 24089 [213]	2023	CAV	○●●●●●	Software update engineering
	ISO/SAE 8475 [234]	WIP	CAV	○●●●●●	Cybersecurity Assurance Levels and Target Attack Feasibility
	ISO/SAE PWI 8477 [236]	WIP	CAV	○●●●●●	Cybersecurity verification and validation
	ISO/CD TS 5083 [221]	WIP	CAV	○○○●●○	Safety for automated driving systems- Design, verification and validation
ISO/TC204	ISO/SAE PAS 22736 [206]	2021	CAV	●●●●●●	Taxonomy and definitions for terms related to driving automation systems for RMV
	ISO/AWI TR 19560 [205]	WIP	CAV	○○○●●○	Information interface framework between ADS and user
	ISO/TS 21177 [238]	2019	ITS	○●●●●●	ITS station security services for secure session setup and authentication between trusted devices
	ISO/TR 21186-3 [237]	2021	ITS	○●●●●●	Guidelines on the usage of standards - Part 3: Security
	ISO/FDIS 22741 [211]	2022	ITS	NA	Roadside modules AP-DATEX (application profile data exchange) data interface
ISO/IEC JT1	ISO/IEC 29134 [226]	2017	IT	NA	Guidelines for privacy impact assessment
	ISO/IEC PWI 5888 [227]	WIP	CAV	○○○●●●	Cybersecurity and privacy protection - Security requirements and evaluation activities for CAVs
UNECE WP29	R155 [430]	2021	CAV	○○○●●●	Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system
	R156 [431]	2021	CAV	●●●●●●	Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system
ITU	X.1371 [244]	2020	ITS	○●●●●●	Security threats to connected vehicles
	X.1372 [245]	2020	ITS	○●●●●●	Security guidelines for V2X
	X.1373 [246]	2017	ITS	○●●●●●	Secure software update capability for ITS communication devices
	X.1374 [247]	2020	ITS	○●●●●●	Security requirements for external interfaces and devices with vehicle access capability
	X.1375 [248]	2020	ITS	○●●●●●	Guidelines for an intrusion detection system for in-vehicle networks
	X.1376 [249]	2021	ITS	○●●●●●	Security-related misbehaviour detection mechanism using big data for connected vehicles
	FG-AI4AD-2 [242]	2021	ITS	○○○●●●	Automated driving safety data protocol-Ethical and legal considerations of continual monitoring
ETSI	ETSI TR 102 893 [127]	2017	ITS	○●●●●●	Threat, vulnerability and risk analysis
	ETSI TS 102 731 [131]	2010	ITS	○●●●●●	Security Services and Architecture
	ETSI TS 102 940 [132]	2019	ITS	○●●●●●	ITS communications security architecture and security management

Continued on next page

Table 4.2: CAV's cybersecurity and privacy standards baseline. (Continued)

	ETSI TS 102 941 [134]	2021	ITS	○●●●●●	Trust and Privacy Management
	ETSI TS 103 097 [137]	2020	ITS	○●●●●●	Security header and certificate formats
	ETSI TS 103 415 [129]	2018	ITS	○●●●●●	Pre-standardisation study on pseudonym change management
	ETSI TS 103 257-1 [128]	2019	ITS	○●●●●●	Channel Models for the 5,9 GHz frequency band
	ETSI EN 302 637-2 [126]	2014	ITS	○●●●●●	Specification of cooperative awareness basic service
SAE	J2735 [386]	2020	V2X	○●●●●●	V2X communications message set dictionary
	J3216 [388]	2021	CAV	●●●●●●	Taxonomy and definitions for terms related to cooperative driving automation for RMVs
	J3016 [389]	2016	CAV	○○●●●●	Taxonomy and definitions for terms related to driving automation systems for RMV
AUTOSAR	402 [26]	2014	In-Vehicle	●●●●●●	Specification of crypto service manager
	654 [28]	2017	In-Vehicle	●●●●●●	Specification of secure onboard communication
	664 [29]	2016	In-Vehicle	●●●●●●	Overview of functional safety measures

[1] The ● refers to the indicated SAE level(s)

Part III

Threat Analysis and Risk Assessment

Chapter 5

Article IV: A systematic review of threat analysis and risk assessment methodologies for connected and automated vehicles

Relevance

This article is a fundamental work to investigate RQ4 and RQ5. Following the regulations and standards provisions, extracted from Chapter 4, in considering TARA as a pillar of the automotive cybersecurity governance, we believe that fine-grained insights about existing TARA methodologies is required. In here, the suitability of such methodologies to the CAV's environment is examined. Through a systematic study, the manuscript establishes the path towards an in-depth understanding of existing TARA limitations in addressing L4 and L5 CAVs' properties as well as their incorporation to privacy concerns. At the time this article was elaborated and presented, requirements to propose our innovative TARA 2.0 were defined and initiated afterwards through the manuscript in Chapter 7.

Context

This article was presented at the 18th International Conference on Availability, Reliability and Security (ARES 2023), which was hold between August 29th and September 1st, 2023 in Benevento, Italy. The conference is ranked as a B category according to CORE2023 [1] and the Resurchify portal[2].

Own contribution

Being the lead author, my contribution to this work consists of conducting the entire investigations, examination and evaluation of existing TARA methodologies. The majority of the paper content was elaborated by me which was further reviewed by other co-authors.

[1] http://portal.core.edu.au/conf-ranks/

[2] https://www.resurchify.com/about

Contents

5.1 Abstract

With the prevalence of high cyber risks within the CAV's environment, the core regulation bodies mandated applying TARA methodologies. Conducting auspicious TARA is essential to ensure acceptable level of risk by analysing potential threats and determining corresponding mitigation strategies. Albeit plethora of standardised TARA versions are available, they are not-ready-to-use methods or they do not encapsulate heterogeneous CAVs properties. By considering the TARA emerging trends and the CAVs' SAE automation levels, the present work provides a systematic study of salient TARA methodologies in the last ten years. The methodology we applied starts with a systematic review identifying TARA approaches that are relevant to the automotive domain at a large scope. After that, the methods' applicability to CAVs is evaluated based on their threat analysis avenues and risk metrics. We elevate our appraisal further with a focus on how the automation level is considered, how the privacy impact is assessed by each TARA method, and how subjective the experts were while assessing scores to the risk metrics. Our investigation spotlights how different methods are intertwined and joint to meet the compliance with key standards such as ISO/SAE 21434. We believe that the present study's findings identify knowledge gaps and help to shape the next generation of TARA methods to keep pace with rapidly evolving automotive technologies and support the readiness of CAV of SAE levels four and five.

5.2 Introduction

The SAE defines six levels of automation. They vary from L0 (no automation, the entire driving duty is on the human driver); L1 (driver assistance on either steering or speed, handled by the vehicle in a specific context); L2 (partial automation of the driving performance, but the driver is needed to react to external events); L3 (entire driving performance is automated, but human fallback is still required); L4 (entire driving and fallback are automated but in a specific context) to L5 (fully automated with unlimited conditions) [385]. CAVs of L4 and L5 are anticipated as the new paradigm aimed at shaping the future transportation model where a driver is no longer needed.

To assure the autonomous driving functionalities, CAVs embed multiple cutting edge sensors such as LiDARs, cameras, AI processing units, advanced ECUs in addition to numerous V2X connections [41]. Those components turn the autonomous driving from dream into reality, but expose CAVs to fatal consequences if such safety critical systems are not sufficiently prepared for all traffic scenarios, including a cyber attack.

The CAV's technologies come with cybersecurity and data privacy threats, dramatically impacting the vehicle acceptance and jeopardising its passengers' safety and privacy [44]. To illustrate, Miller and Valasek [330] presented the remote take over of the braking and the steering systems of a Jeep Cherokee. Yan, Xu and Liu [462] demonstrated Tesla S sensors' blinding leading to a crash. Asuquo et al. [23] showcased a location privacy threat revealing the vehicle and passenger identities for tracking and feeding social profiling.

As there are always risks in the CAV's ecosystem, TARA is considered by the new UNECE R155 regulation [430] and the ISO/SAE 21434 [233] standard as the efficient way to keep systems at an acceptable level of risk. TARA is a valuation methodology whose essence consists of identifying cybersecurity threats and appraising the risks associated to the determined threats [387]. Therefore, as the ADSs are safety critical units, TARA is envisioned as the relevant automotive cybersecurity management tool to support the secure development of the highly automated vehicles [114].

Nevertheless, the existing TARA methodologies lack granularity and are no-ready-to-use methods [443]. Moreover, there is still a lack of in-depth descriptions on the appropriateness of TARA framework regarding CAV's specific assets and properties. Furthermore, TARA metrics vary from one methodology to another where, for example, the controllability factor, reflecting either the driver or the ADS reactivity within a threat scenario, remains optional. On the same note, the vehicle software and hardware fluctuate with the SAE automation level [49]. Consequently, L4 and L5 CAVs are supposed to mitigate cyber risks individually and on real time manner, while an L3 vehicle attack is likely to be controlled by human interventions. Inspired by such challenges, our research builds a systematic literature review, comparing the key TARA methodologies in the highly automated CAV's field, by evaluating how the SAE automation level is considered, how privacy impact is assessed and how the risk is computed.

The present article provides the following contributions:

- An extensive analysis of existing TARA methods applicable to CAVs' landscape, selected based on the methodology's essence, scope and domain.
- An investigation into the connections between generic TARA and CAVs' oriented methodologies.
- An evaluation of how the ISO/SAE 21434 [233] triggered a paradigm shift within the TARA development.

In the course of the present chapter, Section 5.3 provides background definitions while Section 5.4 describes our methodology. Section 5.5 presents a granular classification of the existing TARA methodologies. Then Section 5.6 discusses our findings and leverages the major research gaps with regard to the existing TARA methods leading to outline our future work. After the analysis on the key TARA methodologies, the related work is presented afterwards in Section 5.7. Finally, the concluding remarks are presented in Section 5.8.

5.3 Background

To facilitate the technical discussion on different TARA methodologies, we first align the terms used throughout the manuscript. Thereafter, the key standards embedded in TARA are highlighted.

5.3.1 Definitions

Risk Assessment (RA) and TARA encapsulate common concepts that lead to overlapping definitions or misinterpreted terms. RA is: 'the process of planning, preparing, performing and reporting a risk analysis, and evaluating the results against risk acceptance criteria' [377]. TARA consists of assessing potential cyber threats, rating the associated risks, and recommending appropriate mitigations [387]. A main difference between the two definitions is the term 'threats'. While RA focuses on risks in general, TARA involves threats identification and their link to risks. A common pitfall is to address RA under the TARA name and vice versa. Hence, we delimit the present systematic study to frameworks where the essence of the methodology is aligned with the TARA definition.

Furthermore, there is a large misunderstanding on safety and security requirements within the TARA scope. A starting step in the TARA process is the asset identification. In safety engineering, an asset is defined as anything of value that can be protected from significant accidental harm prompting remedial action [96]. In security engineering, an asset represents valuable properties that needs to be protected from malicious harm, such as data privacy and software integrity [377]. On one hand, safety methods derived from HARA evaluate the likelihood and impact of accidental and hazardous harm. On the other hand, the security methods derived from TARA are focused on intended harm conducted by attackers. As the safety and security concepts can be overlapping, we therefore constrain our research to TARA with a focus on security issues, yet with safety implications.

5.3.2 Key standards

Within the last decade, efforts have been made to provide standardised TARA guidelines related to the CAV's ecosystem. SAE J3061 [387] evoked a complete cybersecurity management for the driverless landscape representing a first draft of the TARA. The final standardised TARA draft came along with the joint efforts from ISO and SAE through the ISO/SAE 21434 [233]. Further ISO standards remain inspiring for the elaboration of other TARA methods. ISO 26262 [214] brought the basic principles of safety recommendations into the automotive environment and recommends the Automotive Safety Integrity Levels (ASIL) [177] determination approach for system's failure quantification and ranking. ISO 31000 [215] orients towards risk management foundations and efficiency. Additional standards are required within the assessment process to rate the impact and assign attack feasibility values within the TARA process as per ISO/IEC 15408 [222] and ISO/IEC 18045 [224] that were constructed on the top of The Common Methodology for Information Security Evaluation (CEM) V3.1 [86]. More focused on C-ITS scope, ETSI released multiple standards on identifying threats and their countermeasures including dedicated guidelines on TARA deployment through the ETSI TS 102 165 [130].

5.4 Methodology

Based on Kitchenham and Charters [272] guidelines known for their rigour review instructions, the present section describes the adopted methodology for our systematic review. As the first and most important step, research questions are elaborated to drive the entire research process. Then, research questions are addressed through primary and secondary studies where a set of relevant sources are selected and fully investigated to meet the inclusion and exclusion criteria. Followed by the data extraction step, the

Table 5.1: Search string.

(threat **OR** risk) **AND** (assessment **OR** analysis **OR** evaluation **OR** test) **AND** (connected **OR** automated **OR** autonomous) **AND** (vehicle **OR** automotive)

Table 5.2: Paper selection results.

Source	**Primary selection**	**Secondary selection**		**Final inclusion/exclusion**
	Search string	Title/ abstract	Content screening	Full text analysis
ACM digital library	641	54	15	4
IEEExplore	540	28	17	7
MDPI	136	10	2	0
Science Direct	966	42	10	1
Springer	824	41	14	5
Wiley Online Library	438	11	6	1
SDOs portals (ISO, SAE, ETSI, UNECE, ENISA)	384	29	15	5
Total	**3929**	**215**	**79**	**23**

findings are filtered and ready to be synthesised and compared to meet the research purpose.

5.4.1 Research questions

The deployment of highly automated vehicles cannot occur apart but in a symbiotic way with the development of robust threat and risk assessment methodologies. The present work aims to assess how the existing TARA methodologies are coping with the CAVs' evolving technologies and how such topic is addressed by current research. This factor motivates our systematic review which is driven by the following research questions:

- RQ1: What are the existing TARA methods that can be applied to the highly automated and connected vehicles?
- RQ2: What are the limitations of TARA methods, including the trending methodology defined by ISO/SAE 21434 [233], to address the properties of CAVs of SAE L4 and L5?

5.4.2 Primary studies selection

The primary research was conducted by using the advanced search feature in publication platforms such as ACM digital library and IEEExplore, as spotlighted in Table 5.2. Not limited to academic and scientific search engines, the SDOs' databases were also used to complement our findings with standardised methods. The search string drawn in Table 5.1 consists of boolean operators as per OR and AND to fetch relevant publications. The query was adjusted depending on the source database for a comprehensive search. Within the advanced search interfaces, only publications from January 2014 to April 2023 were filtered.

5.4.3 Secondary studies selection

The secondary studies overviewed the primary findings through two steps. First, only peer-reviewed publications as well as journals and conference proceedings were selected. Such selection was further elevated by studying the manuscripts' titles and abstracts. Second, 215 selected publications were screened for context relevance where 79 papers were finally chosen.

5.4.4 Final inclusion and exclusion

With the aim of drawing a systematic review on TARA methods specific to CAVs, the 79 manuscripts were fully read and assessment methods were thoroughly evaluated. To that end, only methodologies that are aligned with TARA essence and scope were considered. The inclusion criteria relies on selecting methods wrapping up both threat modelling and RA. Following such procedure, generic RA methodologies, which are lacking the threat analysis, were excluded from our analysis, as well as methods that are not focused on the automotive or CAVs' domain. Additionally, HARA methods that are assessing system failures or hazardous events without tackling the cyber threats properties are beyond the scope of our selection. Further guided by the key standards, we excerpt standardised methods and those aiming the compliance to crucial ISO, SAE or ETSI standards. Based on such inclusion and exclusion criteria, 23 manuscripts out of 79 were selected to be deeply evaluated in Table 5.2.

5.4.5 Data extraction and comparison factors

The data extraction step was conducted using data collection forms that were elaborated, edited and adjusted by the present work's authors. The results were cross-checked afterwards and compared among involved researchers where disagreements were resolved by consensus or arbitration. To that end, the investigation into TARA methods was guided by evaluating the following factors per selected model: (i) clear definition of the method acronym; (ii) year/s of release (depending if there was one or multiple versions per model) (iii) type of the method (to be quantitative QT and/or qualitative QL) (iv) category of the method as standardised by ISO 27001 [225] (asset-based or scenario-based indicating whether the methodology is guided by a targeted asset or a risk scenario accordingly) (v) level or group of levels with regard to the SAE automation level [385] (vi) privacy impact reflecting how the privacy weight was approached by the method (vii) metrics considered for risk determination as entitled by the method's authors (viii) rating methodology or scaling reference that the experts used to assign values and scores for the metrics involved in the assessment (ix) standards for which the method aims compliance (x) related TARA methods constituting the bases of the identified methodology Table 5.3 reflects how the aforementioned factors were analysed, while the following section provides a detailed discussion per TARA method.

5.5 Threat and risk assessment methods

Given the intertwined concepts between traditional TARA methods and recent releases, we believe that the exploration of TARA applicable to the CAV's landscape occurs interdependently with an investigation into fundamental TARA methodologies. It is noteworthy to mention that classical, yet salient, threat modelling or risk scoring methods constitute the bases for the emerging TARA methodologies.

5.5.1 Fundamental methods

The present discussion spotlights popular methods that were not identified in the primary studies selection phase of our systematic review as they are not relevant to the predefined research time period. Though, such methods remain pertinent to leverage granular insights for TARA properties as well as their applicability into the highly connected and automated driving ecosystem.

Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service and Elevation of privilege (STRIDE) [329] is a threat modelling technique provided by Microsoft, identifying six types of security threats, categorised per the attacker intentions and known vulnerabilities. The method is based on graphical classification without imposing any risk metrics computation. STRIDE was designed for the IT industry, but since it was recommended by the SAE J3061 [387], it started to be part of multiple automotive TARAs.

Another compelling threat modelling method is the Attack Tree Analysis (ATA) [377]. Based on a tree structure, the ATA sets the attack target as a parent node while children nodes depict the events triggering the attack. On one hand, the top-down analysis showcases the attack paths. On the other hand, the bottom-up interpretation spotlights the attack surfaces and the potential vulnerabilities. The ATA is foreseen to be a powerful tool for the threat scenario identification step, though, it needs to be combined with other risk scoring methods for risk determination.

Similar to ATA, being a scenario-based and a graphical representative tool, FAIR is a riveting method but for risk analysis instead of threat modelling. FAIR [169] is a quantitative method providing a taxonomy of risks to systems of different scales. FAIR's tree graphical view breaks down every risk into discrete factors, computing a value per factor and summing the overall risk through a range representation instead of a single number score. FAIR combines the loss event frequency, determining the susceptibility of a threat event to become a loss event, and the loss magnitude, assessing the impact from an event.

Common Vulnerability Scoring System (CVSS) [377] is an industry free and open standard providing quantitative measurements and qualitative ranking. Based on a CVSS calculator, the vulnerability severity is determined for decision-making process. The score is computed based on the attack ease and impact. The attack ease evaluates how close an attacker is from the asset or how the authentication can be passed to reach the asset while the impact factor reflects the threat severity and eventual consequences.

One of the pioneering comprehensive methods combining both threat modelling and RA is the Failure Mode and Effects Analysis (FMEA) [443]. It is an industry wide accepted process which evaluates the modes, causes and effects of a failure based on the IEC 60812 standard [443]. The methodology was initially developed for safety analysis,

Table 5.3: Threat Analysis and Risk Assessment methods.

Table 5.3:

Method	Description	Year	QL/QT†	Type	SAE Lx	Privacy	Metrics	Rating practice	Aimed compliance	Based on
FMVEA [394]	Failure Mode Vulnerabilities and Effects Analysis	2014	QL	Asset	N/A	✗	Severity Probability of occurrence	Experts knowledge	ISO 26262 IEC 60812	FMEA, ATA
RACE [52]	Risk Analysis for Cooperative Engines	2015	QL	Asset	≤ L2	✓	Severity Attack probability Controllability	ISO/IEC 15408 ISO/IEC 18045	ETSI TS 102 165	EVITA, TVRA
SAHARA [31(	Security-Aware Hazard and Risk Analysis	2015	QL	Asset	≤ L2	✗	User profile User knowledge Safety impact	ASIL	ISO 26262	HARA, STRIDE
HEAVENS [2(285]	HEAling Vulnerabilities to Enhance Software Security and Safety	2016	QL	Asset	≤ L3	✓	Threat level Impact level	ASIL CEM V3.1 Experts knowledge	ISO 26262 ISO/SAE 21434	EVITA, STRIDE
Dominic et al. [116]	Risk Assessment for Cooperative Automated Driving	2016	QL	Scenario	≥L1	✓	Impact Motivation Attack feasibility	NHTSA [60] ISO/IEC 15408 Experts knowledge	N/A	HEAVENS
TVRA [133, 130]	Threat, Vulnerability, Risk Analysis	2017	QL	Scenario	Not specified	✗	Occurrence likelihood Impact value	ISO/IEC 15408	ETSI TS 102 165 ISO/IEC 15408	EVITA
SARA [331]	Security Automotive Risk Analysis Method	2018	QL QT	Asset	L3 L4	✓*	Attacker profile Vehicle controllability	ISO/IEC 15408 ISO/IEC 18045	SAE J3061 ISO 26262	ATA
SPMT [409]	Start, Predict, Mitigate, and Test	2018	QL QT	Asset	Not specified	✓	Occurrence likelihood	Experts knowledge	SAE J3061	HEAVENS, STRIDE, ATA
TARA+ [49]	Controllability-aware TARA for L3 Automated Driving Systems	2019	QL	Asset	L3	✓	Impact Attack feasibility Controllability	ISO/IEC 18045 Experts knowledge	SAE J3061 ISO 26262	TARA 1.0, HEAVENS
VeRA [97]	Vehicles Risk Analysis	2020	QL QT	Asset	L3 L4	✓	Attack probability Severity Human control	Experts knowledge	SAE J3061	EVITA
Khatun, Glass and Jung [268]	Scenario-Based Threat Analysis and Risk Assessment	2021	QL	Asset	≥ L3	✓	Attack probability Severity	ASIL	SAE J3061	STRIDE, EVITA, HEAVENS
TARA 1.0 [23: 387]	Threat Analysis and Risk Assessment	2021	QL	Asset	Not specified	✓	Impact Attack feasibility	ISO/IEC 18045 Experts knowledge	ISO/SAE 21434 SAE J3061	OCTAVE, EVITA, TVRA, HEAVENS
ThreatGet [39	Asset Driven Automotive Cybersecurity Analysis	2021	QL	Asset	Not specified	✓	Threat level Impact level	ISO/IEC 18045 Experts knowledge	ISO/SAE 21434	SAHARA, TARA 1.0, STRIDE
Dobaj et al. [115, 114]	Security-driven automotive development lifecycle	2021	QL QT	Scenario	≥ L3	✓	Threat level Impact level	FAIR ISO/IEC 18045 Experts knowledge	ISO/SAE 21434	TARA 1.0
Vogt et al. [443]	Comprehensive Risk Management in Intelligent Transport Systems	2021	QL QT	Scenario	Not specified	✓	Severity Failure probability	FAIR Monte Carlo simulation Experts knowledge	ISO 26262 ISO/SAE 21434	FMEA, FAIR
Wang et al. [451]	A Systematic Risk Assessment Framework of Automotive Cybersecurity	2021	QT	Asset	Not specified	✓	Impact Attack feasibility	BSI 100–4 [163] ISO/IEC 18045	ISO/SAE 21434	HEAVENS
ThreatSurf [4	Threat Surface assessment in automotive cybersecurity engineering	2022	QL	Asset	L3	✓	Threat level	ISO/IEC 18045 Experts knowledge	ISO/SAE 21434	TARA 1.0
PIER [366]	Probability, Impact, Exposure, and Recovery	2022	QT	Scenario	≤ L3	✓	Occurrence likelihood Impact Exposure likelihood Recovery	Experts knowledge	ISO/SAE 21434	TARA 1.0
Zhou et al. [469]	Data Security Risk Assessment Method for Connected and Automated Vehicles	2022	QT	Asset	≥ L3	✓*	Data value Feasibility Impact	National regulations (GB/T 20984-2007) [408]	ISO/SAE 21434	EVITA, HEAVENS, TARA 1.0

† QL = Qualitative, QT = Quantitative
* Higher weight on privacy

but it was extended to cover cyber-physical security. The threat analysis in FMEA is provided by determining how the security attributes fail while the risk is assessed by combining severity and probability properties.

A more comprehensive method was initiated in 1999 through Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [11] and its variants: OCTAVE-S, OCTAVE Allegro, OCTAVE Forte. OCTAVE was released to evaluate cyber risks from the management, organisational and technical perspectives. The methodology encapsulates assets, threats and vulnerability assessments where risks to be mitigated are prioritised. Being customisable, easily self-directed and with high interoperability [284], OCTAVE represents the foundation of the TARA from the ISO/SAE 21434.

E-safety Vehicle Intrusion proTected Applications (EVITA) is another pillar of the TARA from the ISO/SAE 21434. Over a decade ago, the EVITA project was the pioneer to present asset-based TARA methodology for the automotive environment. It evaluates risks based on severity and attack probability where the threats are rated and prioritised with the consideration of the driver controllability [382]. Though, EVITA remains limited to CAVs of SAE L0, L1 and L2 requiring the driver presence and intervention.

Less popular threat modelling methodologies, yet interesting to consider when constructing TARA for CAVs, are Process for Attack Simulation and Threat Analysis (PASTA) [428], Visual, Agile, and Simple Threat (VAST) [271], and Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of data, Unawareness, and Noncompliance (LINDDUN) [306]. Such methods can be selected based on the scale and complexity of the system. For the purpose of the present research, our analysis is constrained to only those methods that were evoked in constructing dedicated automotive TARA methodologies discussed Table 5.3.

5.5.2 TARA methods applied to CAVs

Table 5.3 overviews TARA methods that were designed for automotive systems generally and CAVs specifically. Based on the inclusion/exclusion criteria (Section 5.4.4), we selected methods varying from those derived from research projects, standardised methods, to the most recent improved methodologies.

Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) [394] represents an improved version of the FMEA method. As elicited in Section 5.5.1, FMEA is a powerful quality control methodology used to assess the entire product lifecycle; though, it is not efficient to handle multiple failures at a time and over complex systems. To overcome such limitations, FMVEA [394] was developed in a combination to STRIDE to serve the C-ITS domain.

Risk Analysis for Cooperative Engines (RACE) [52] is an extension of the EVITA methodology which assesses risks using the same metrics but with a consideration of the C-ITS's architecture [41]. Though, as it was perceived for highly connected environments, the severity metric in RACE is computed at a coarse level. RACE is advertised as an improvement of EVITA through its compliance to ETSI TS 102 165 [133].

Security-Aware Hazard and Risk Analysis (SAHARA) [310] is one of the original methodologies combining hazard analysis methods such as HARA and threat modelling tools as per STRIDE. SAHARA aims to harmonise safety and security methods by assessing security threats over safety-critical systems at the vehicle conceptual phase. The method was evaluated over a battery management system of a hybrid vehicle where additional threats were identified with regard to a simple HARA deployment.

HEAling Vulnerabilities to Enhance Software Security and Safety (HEAVENS) [201] adopted the EVITA methodology, yet with an alignment to the ISO 26262 [214] and SAE J3061 [387] requirements. As an outcome of the HEAVENS methodology, the security level of an asset is derived by combining the 'threat level' and 'impact level' being the key metrics of the approach. It combines the threat likelihood which is computed by considering the attacker expertise, the knowledge about the target, the window of opportunity and the equipment required to conduct an attack, and estimation on the expected loss per stakeholder from the Safety Finance Operations Privacy (SFOP) perspectives. To meet the ISO/SAE 21434 [233] compliance, an improved version entitled HEAVENS 2.0 [285] was recently delineated. Both HEAVENS versions intend to cope with the evolving risks within the automotive industry including CAVs, though, the SAE automation level was not imposed within the assessment. In Table 5.3 we consider both methods to be adapted to vehicles of SAE L3 rearward as the methodologies were validated through the vehicle speed limiter use cases, requiring the driver presence.

Dominic et al. [116] were the first authors who dug beneath the surface of SAE automation levels and their impact on conducting TARA within the CAVs landscape. By extending the STRIDE method and developing a CAV's reference architecture, the researchers proposed an agile TARA that can be adjusted to every OEM's design and to each automation level. Unlike the other TARA methods of that era, Dominic et al. [116] advertised the customisation of the threat model and matrix within every different system as well as the values, weights and parameters of the risk assessment. While demonstrating the methodology over driverless valet parking as an SAE L4 component, the authors depicted the TARA outcome through a threat matrix plot with visual priorities ranking.

The Threat, Vulnerability and Risk Assessment (TVRA) method was standardised by ETSI in 2011 [133] and upgraded by 2017 [130]. With a focus on vehicular telecommunication threats, the method relies on the occurrence likelihood and the impact value to assess the risk. The TVRA generates quantified risks of an asset and maps them to security mitigation techniques with the aim to bring the risks to an acceptable level [92]. Nevertheless, as the TVRA method is more adapted to V2X threats, it misses in-vehicle components perils. Also, it does not consider the safety and privacy within its risk computation approach [331].

Security Automotive Risk Analysis Method (SARA) [331] is one of the first asset-based methods targeting the assessment of risks related to the automation features and one of the unique methods focusing on the privacy weight. The methodology claims further metrics impacting the risk computation including the attacker profile and the self-controllability of the ADS reflecting the method adaptability to SAE L3 & L4. The SARA feasibility was showcased by privacy and safety scenarios on vehicle tracking and comfortable emergency brake failure.

The Start, Predict, Mitigate, and Test (SPMT) [409] came up with security enhancements over the entire vehicle lifecycle. It is a methodology wrapping up several security models including HEAVENS, ATA and STRIDE. The SPMT process is foreseen as a virtuous cycle based on prediction, security testing, mitigation and reassessment over any asset in each phase of the automotive development. Although, the methodology targets CAV's assets, the SAE automation level weight is not specified in assessment. Another limitation of the method is that it does not consider multiple metrics in computing the risk, mostly focused on the probability of occurrence.

Based on earlier drafts of TARA from the SAE J3061 [387], TARA+ [49] was built with an additional metric assessing both the driver and ADS controllability over vehicles of SAE L3. The TARA+ model is a proof of concept demonstrated by threat scenarios over the surface attacks: ADS on-board units, LiDAR and vision sensors.

Vehicles Risk Analysis (VeRA) [97] is a method inspired from the SAE J3061 but in a simplified way. The methodology captures the risk through a compilation of the attack probability, severity and the human control. Unlike other methods, the human control property in VeRA considers the SAE automation level. Nevertheless, it attributes a constant risk value for SAE L3, L4 and L5 as they are merged together in the risk classification matrix. VeRA's performance was assessed to be quicker and less complex than EVITA.

In a combined perspective of safety and security analysis, Khatun, Glass and Jung [268] designed a TARA methodology, which takes a list of hazardous events as a further input to build a scenario-based threat analysis. The method relies on the main TARA steps recommended by the SAE J3061 to assess the Over-the-Air (OTA) software update system of CAVs of SAE L3 onward. The OTA system was selected by the authors as a complex safety critical asset, yet required within automated vehicles. The proposed method followed STRIDE for damage scenario definition while it was built upon HEAVENS and EVITA methodologies to identify the attack potential and severity level.

TARA method in ISO/SAE 21434 (hereinafter, referred as TARA 1.0) was initially introduced within the SAE J3061 standard [387] which was developed based on OCTAVE, EVITA, TVRA and HEAVENS. The new ISO/SAE 21434 [233] evoked a different, yet detailed, workflow. Depicted in Figure 5.1, the blue section draws the boundaries of the TARA scope as outlined by the ISO standard. TARA 1.0 brought out a detailed description of the asset identification which can be represented through a data flow diagram supporting on enumerating the assets. Based on the cybersecurity properties, the threat scenarios are identified and the attack paths are analysed. The ISO/SAE 21434 standard suggested STRIDE or ATA as potential tools to accomplish these two steps accordingly. Similar to HEAVENS, the risk in TARA 1.0 compiles the impact rating using the same factors. The attack feasibility can be driven through three methods varying from 'attack potential-based' where feasibility rates are retrieved from the ISO/IEC18045, 'CVSS-based' using FIRST scoring system [166] to the qualitative 'attack vector-based'. From the risk value, a decision should be derived which represents the main outcome of the TARA 1.0 process. Such key output feeds the cybersecurity goals and claims afterwards to update the general vehicular cybersecurity governance. Despite the process clarity and agility of the TARA 1.0, the method remains generic and does not elicit any specific treatment per SAE automation level.

ThreatGet [396] represents a concrete implementation of TARA 1.0 method through a tool-supported approach. Not limited to the compliance with ISO/SAE

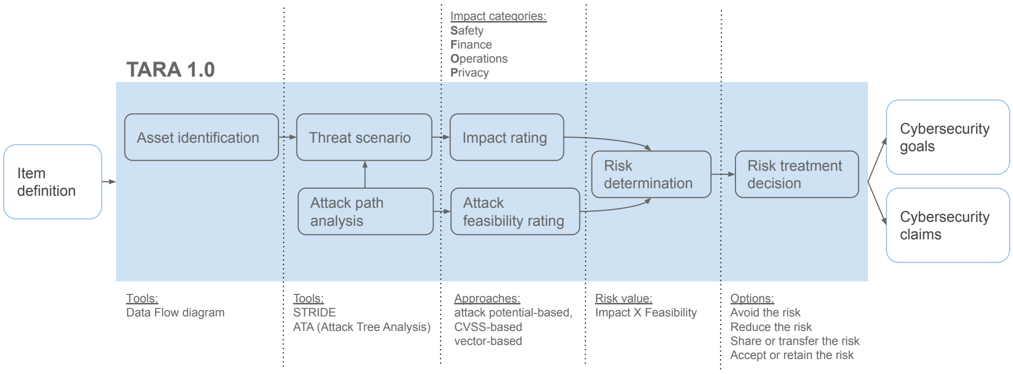


Figure 5.1: TARA 1.0 as defined by ISO/SAE 21434.

21434 [233] only, ThreatGet wraps other TARA methodologies such as SAHARA for the asset identification and HEAVENS for the risk computation. ThreatGet extended the combined TARA methodologies with automated determination of threat scenarios and attack paths. Though, the SAE automation level was not imposed by the tool parameters.

Dobaj et al. [114] proposed additional steps to the TARA 1.0 process, especially at the threat scenario modelling phase. The model maps the additional steps to the relevant vehicle lifecycle phases. To illustrate, it distinguishes between TARA actions to be taken during the concept phase and those that are applicable at design or implementation phases. Additionally, the method targets highly automated vehicles of SAE L3 onward. Nevertheless, it assesses L3, L4 & L5 equally.

Inspired from the core standards for safety, security and risk management, Vogt et al. [443] introduced a comprehensive TARA method for C-ITS including CAVs. The method combines qualitative and quantitative threat modelling and risk scoring tools such as FMEA and FAIR to offer flexibility for any C-ITS's asset assessment. For uncertain values, a Monte Carlo simulation was used to generate ranges instead of a fixed score supporting the impact and attack feasibility rates' computation. Although, the authors proposed a model wrapping the advantages of other TARA methodologies,the SAE automation level was not pushed within the assessment.

Wang et al. [451] shifts the focus from procedural adjustments to quantitative suggestions with the aim to improve the risk matrix and hence elevate the assessment's objectivity. The authors proposed different rating schemes supporting the risk calculation that can be adapted through the vehicle development lifecycle. Though, the methodology shares several commonalities with the TARA 1.0 without any explicit citation to the ISO/SAE 21434. Additionally, the vehicle's SAE automation level was not considered within the method's analysis scope.

Similar to ThreatGet, ThreatSurf [465] introduced an automated assessment of the vehicle attack surface per TARA 1.0 and hence compliant to ISO/SAE 21434. The methodology also aims to align with the UNECE R155 [430] as it is evaluated through the regulation's threat categories. ThreatSurf demonstrated an in-depth assessment of threats in modern vehicles of SAE L3. Nevertheless, the process excludes the impact rating and risk determination steps from the automation process, as it is manufacturer specific.

Probability, Impact, Exposure, and Recovery (PIER) [366] is a recent TARA methodology dedicated for CAVs of SAE L3 onward. The method focuses on assessing how the assets are exposed to risk from internal and external connections and how resilient they are on real-time base. PIER is considered as another improved version of the TARA 1.0 by embedding the recovery and rapid resilience over mission-critical components within the CAV. The method was theoretically validated through a vehicular software update and collision avoidance scenarios and a concrete implementation of the attack scenarios over a real CAV remains absent.

A more privacy focused methodology was drawn by Zhou et al. [469]. The authors merged together the data security risk assessment recommended by national regulations to TARA 1.0 steps. Furthermore, the risk computation imposes data security factors such as data value (reflecting the data sensitivity) as well as the feasibility and impact metrics involved on the TARA 1.0 risk computation. While considering the data privacy risks in the CAV's environment and the data lifecycle, the researchers demonstrated their methodology on the Telematics box data as the assessment's asset. However, the methods remains limited to national regulations requiring major adaptation for different markets.

5.6 Discussions and future work

In the following, we summarise our key findings, demonstrating the discrepancy between the existing TARA methods and CAVs readiness:

Despite being called by different terms, the main two TARA steps are threat modelling and risk analysis. While few TARA methods, such as TARA 1.0, have clear boundaries, others may include further steps like item definition and mitigation. To that end, we urge for the need on more unified and standardised terminologies and scope.

OCTAVE, EVITA and HEAVENS are ubiquitous TARA methods which literally geared up today's models. They even represent the foundations for TARA 1.0 which can be foreseen as the most pervasive method. By analysing the aims of the TARA developed within the last three years, we assert that they all either comply to ISO/SAE 21434 [233] or suggest an improvement to TARA 1.0.

Although, there is a continuous improvement to build the most auspicious TARA methodology with regard to the driver and the ADS controllability, there is no explicit distinction in addressing highly CAVs of SAE L4 and L5. There are limited efforts in distinguishing the assessment of SAE L3, L4 and L5 respectively as the majority of the reviewed TARA methodologies consider their risks to be equal. Fortunately, a potential method was initiated by Dominic et al. [116] but the methodology did not emerge with current cyber threats and today's technologies advances. Taking into account the evolving cyber risks with the increase of every automation level, there is a scarcity on TARA methods dedicated to SAE L4 and L5. A risk that can be low on SAE L3 may be defined as high in L4 and even higher in an L5 CAV where a driver control is substituted by the ADS self-risk mitigation.

By considering the high privacy risks within the CAV's ecosystem [44], several TARA methods assigned a privacy weight while measuring the risk. Except the methodologies demonstrated by SARA [331] and Zhou et al. [469], which emphasised on privacy, all other TARA methodologies assigned a weight to the privacy which remains equal to the other SFOP categories as safety, finance and operations.

A common point about the metrics used in all the methods is that they are based on feasibility and impact, while very few TARA methods consider the controllability metric. The terminology varies from attack ease, occurrence to exposure likelihood to quantify the feasibility of a threat to occur. Similarly, there are multiple terms to represent the severity impact. While the majority of the methods are focused on these two metrics, others such as RACE, SARA, VeRA and TARA+ added the controllability metric to assess either the driver or ADS control in case of an attack. We believe that the controllability metric should be imposed differently while assessing CAVs of SAE L4 and L5.

Regarding the rating values, Table 5.3 demonstrates that ISO/IEC 15408, ISO/IEC 18045 and experts knowledge represent the main sources to assign scores. In other words, Appendix I from the ISO/SAE 21434 guided several TARA methods where such sources are recommended. Nevertheless, both ISO/IEC 15408 and ISO/IEC 18045 were elaborated for IT systems without considering the CAV's features which are wrapping both IT and automotive aspects. Furthermore, as long as the experts subjectivity is involved, we consider that a confidentiality factor should be imposed. On the same note, when the estimation depends on experts evaluation, it is prone to over-confident or under-confident results. Consequently, we believe that risks computation can be biased if there is no further metric reflecting the experts confidence.

The presented TARA methods commonly provide threat modelling, risk ratings, determinations and treatments; though the scales remain not specific to cope with today's CAVs challenges including the vehicle connection maturity and SAE automation level. As a future work, it is required to build an improved TARA that will be adapted to the SAE L4 and L5 particularities. The new method aims to consider the vehicle automation level and the evolving privacy impact while computing the risk. Moreover, the process intends to add further metrics such as the experts confidence and the residual risk estimation (risk related to unknown threats) while assessing CAVs's of L4 and L5. Furthermore, the methodology should add further layers of the assessment by including the CAL concept to reflect the ideal level of assurance and protection for the asset. Such parameters were briefly introduced in the ISO/SAE 21434 [233] and will be the focus of the underdeveloped ISO/SAE AWI 8475 [234].

5.7 Related work

While a plethora of research works provided reviews on safety assessments, limited comparative studies on CAV's TARA exist. At a general security engineering scope, Kumar, Joshi and Raturi [282] studied six TARA methods including CVSS, ATA and OCTAVE. The research work asserted the need of making the methodology specific to its domain as the TARA results depend on the experts knowledge and proficiency. More focused on the automotive domain, Luo et al. [306] provided a comparative study with a taxonomy on TARA methodologies. The authors classified the methods into formula-based (representing the asset-based methods) and model based (grouping scenario-based methods). Albeit a granular presentation of TARA models was presented, the research lacks comparative discussions among the identified methods with regard to the vehicle automation and connectivity properties. In another survey, Luo et al. [305] overviewed TARA as a powerful risk-based testing tool. The authors evoked nine fundamental methods where only the application scope and the threat model of every methodology were evaluated. Similarly, Benyahya et al. [43] studied TARA methodologies and selected TARA 1.0 to be demonstrated over an L4 vehicle. The authors elevated further the assessment results by conducting penetration tests over risky damage scenarios. While the authors demonstrated the advantages and limitations of TARA over a highly automated vehicle, the research work lacks a granular comparative study.

Kawanishi et al. [262] studied threat analysis methods by comparing the performance of their risk scoring approaches through a CAV use case. Though, the study was limited to three techniques and only to the national JASO TP15002 standard requirements. In a more detailed review, Monteuuis et al. [331] provided a critical review of ten TARA methods including EVITA, TVRA and HEAVENS. The authors compared them through multiple criteria such as the vehicle type (connected or automated), the attack type (mono or multi threat) and the driver's controllability. To that end, the comparative study remains at a high scale without determining the corresponding SAE automation level.

The ENISA [284, 92] evaluated RA frameworks by categorising them into asset or scenario based, qualitative or quantitative, and based on their risk calculation methodology. Though, the ENISA's reports sought the interoperability evaluation of risk management frameworks in general without addressing neither TARA models nor the CAV's domain. For more standards related studies, Cui and Sabaliauskaite [96] evaluated TARA and HARA common phases by investigating into the ISO 26262 [214], SAE J3016 [385] and SAE J3061 [387]. Similarly, Macher et al. [308] provided a review comparing the TARA methods from SAE J3016, EVITA, HEAVENS, TVRA, OCTAVE and FMVEA. Nevertheless, as with the rapid evolving CAV's standards, both studies [96, 308] remain outdated and limited to generic automotive methodolgies without covering the new trending standards such as ISO/SAE 21434 [233].

Our contribution is different from the aforementioned works as it not only identifies the key TARA methods, but also spotlights their consonance and limitations with regard to the highly CAV's readiness. Moreover, our systematic review brings an innovative comparison using specific CAV's properties including: (i) SAE automation level and high connectivity implications; (ii) privacy impact; (iii) experts subjectivity; and (iv) standardisation evolution and compliance.

5.8 Conclusions

We seldom have enough data to build a set of accurate analysis and assumptions as input to any TARA model. Though, high certainty is much required within the CAV's environment and hence a thorough knowledge about TARA methodologies is crucial in identifying adequate cybersecurity threat modelling for highly automated driving. Our research goal was threefold: conduct a systematic review of the existing TARA methods, analyse them in relation to the ISO/SAE 21434 requirements, and build intensive understanding about how CAVs' properties are considered by the existing methodologies. The outcome shows that the automation level and privacy impacts are barely the main focus of TARA methods. On the same note, more emphasis is needed to appropriately address the specifications CAVs of SAE L4 and L5. We further rationalise a set of recommendations and needs that are driving our insights in providing an improved TARA methodology as a future work.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 875530 through SHOW project, Horizon Europe Research and Innovation programme under grant agreement No 101077587 through ULTIMO project, and from the Swiss State Secretariat for Education, Research and Innovation (SERI). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

Chapter 6

Article V: Symbiotic analysis of security assessment and penetration tests guiding real L4 automated city shuttles

Relevance

This article contributes to the validation of the theoretical findings from Chapter 5 through a real implementation of TARA 1.0. Such implementation was extended further by verifying four attack paths from TARA results through penetration testings. This article represents a fundamental training in executing a TARA and can be foreseen as a pre-requisite to Chapter 7. Consequently, it contributes to explore RQ4 and RQ5.

Context

This article [43] was published in the Telecom journal whose IS: 2.1, and citescore is 4.8.

Own contribution

My contribution to this work consists of supervising both TARA implementation, and execution of the penetration tests execution. Additionally, I took the lead on the paper conceptualization, elaboration and formal analysis of the paper.

Contents

6.1 Abstract

The CAV's deployment is a proof of the wide evolution of autonomous driving technologies enabling vehicles to gradually dispose of their drivers. Within the scope of smart cities, such innovation has given rise to a new type of CAV: the ACS. Foreseen as the new paradigm aiming to shape the public transport model, the ACS elicits a plurality of new applications, such as the on-demand service in which a driverless shuttle offers the desired ride without human intervention. However, such a model raises cybersecurity concerns through the numerous attack surfaces and vehicle hyperconnection. This phenomenon was highlighted in several studies on CAVs, but very few research works tackled the specific case of ACSs, whose challenges and risks far exceed those of personal vehicles. The present work offers a comprehensive investigation of cybersecurity attacks, demonstrates a performed risk assessment based on the ISO/SAE 21434 standard, and showcases a penetration test over a real ACS of automation level four (L4) according to the SAE's ranking. Based on our experiments, we leverage fundamental cybersecurity recommendations with a focus on the ACS's physical security.

6.2 Introduction

CAVs are motorised vehicles with embedded technologies aiming to assist and handle the driving functionality on behalf of drivers. In recent decades, the CAV industry has been increasing annually by 16% at a global scale [188]. Such a market aims to generate $300 to $400 billion by 2035 [111] with a market share of 20–35% of new vehicles by 2030 [402] and even up to 50% by 2050 [298]. Along with the ambitious forecasts and the related economic growth, the SAE defined six levels of automation, ranging from no automation at L0 to full automation of driving at L5, in which each level gradually assists the driving performance [385]. CAVs of L4 denote a level of automation capable of conducting all driving functions under certain conditions, while L5 vehicles can fully perform automated driving under any condition. Such automation is accomplished through sensors, ECUs and AI units [41]. Not limited to internal components, CAVs rely also on numerous communications with external entities to accomplish autonomous driving functions, namely V2V, V2I, and V2X [266]. In the present paper, we focus our research on exploring the ACS as a sub-class of CAV, suitable for coping with today's public transportation needs [9].

ACSs are foreseen as the next generation of smart mobility for public transportation, offering on-demand services tailored for citizens. Putting into perspective the simplicity of ordering a shuttle service while preserving the high quality of transportation, ACSs are also shown to be safer [349], to reduce traffic congestion, and to decrease pollution in comparison to conventional vehicles [117]. More specifically, ACSs are well suited for the transportation of the elderly and people with disabilities or reduced mobility [384]. Therefore, the wide deployment of ACSs could be a paradigm shift in achieving a cheap, reliable, always available, and accessible new way of transport for smart cities. Driven by these advantages, several cities throughout the world have already started testing ACSs in their fleets in multiple pilot projects [199]. However, such technologies introduce multiple security concerns threatening the passengers' safety and security as demonstrated by several researchers. To illustrate, Bec et al. [35] reported attacks on the Chevrolet Camaro; Miller and Valasek [330] implemented a remote takeover of the braking and steering systems of a Jeep Cherokee; and Yan, Xu and Liu [462] demonstrated a blinding attack over the Tesla S sensors leading the vehicle to crash.

For an in-depth understanding of the ACS threats, we had the opportunity, under the umbrella of the AVENUE project [419], to investigate, analyse and conduct penetration testing over the L4 vehicle depicted in Figure 6.1. Our study relies on the TARA methodology provided by the standard ISO/SAE 21434 "Road vehicles—Cybersecurity engineering" [233]. The methodology supports with building threat scenarios, rating the attacks' impact, and determining the risk related to the ACS's assets. We then elevate the TARA's findings further by performing penetration tests (hereinafter, referred to as pentests) over the vehicle's GNSS and 4G connections. From the obtained results, we provide our recommendations to mitigate the risks and the identified weaknesses.

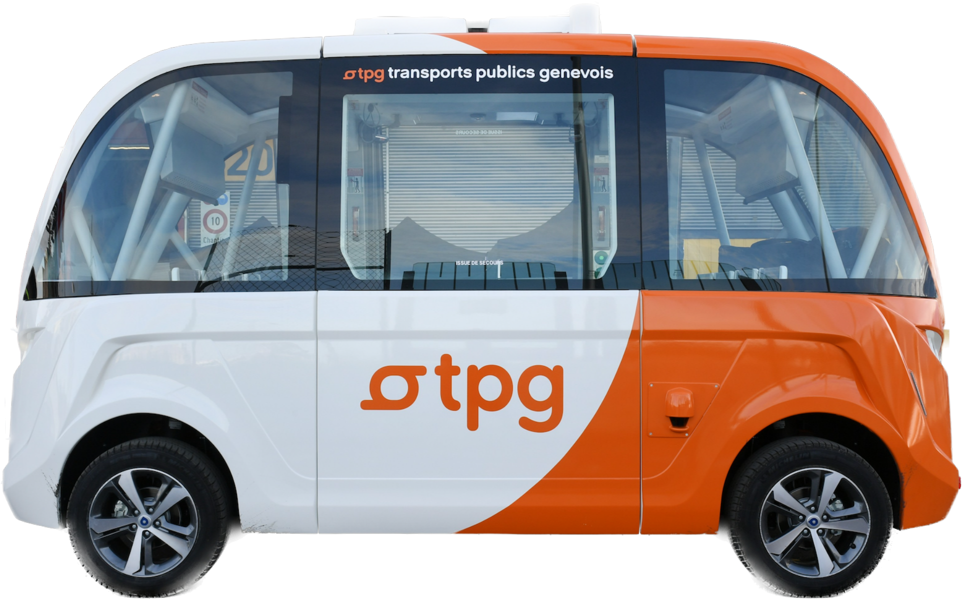


Figure 6.1: Example of the ACS investigated in the present work.

This paper aims to answer the following research questions:

- RQ1: Is the TARA methodology suitable for identifying L4 specific threats?
- RQ2: Would the execution of penetration tests confirm the resilience of the mitigations applied to the high-risk scenarios defined by the TARA?

The remainder of this paper is structured as follows: Section 6.3 discusses related works and identifies knowledge gaps in the domain. Section 6.4 provides background information on the materials used to perform the TARA approach on the L4 vehicle and describes the implementation methodology of the pentests. Section 6.5 discusses the obtained results, while Section 6.6 debates the research questions and outlines our recommendations. Finally, Section 6.7 offers concluding remarks on our findings.

6.3 Related work

With the pervasive technologies leading to ACS deployment in smart cities and their associated cybersecurity challenges, the ISO/SAE 21434 [233] is considered the prominent standard for automotive cybersecurity governance. This standard, as well as the mandatory UNECE R155 regulation [430], introduced the TARA and security testing as an efficient way to keep systems at an acceptable level of risk. Therefore, we highlight in the present research three main avenues, namely the cybersecurity challenges within the ACS ecosystem, security assessments based on the TARA from ISO/SAE 21434, and automotive pentests.

6.3.1 Cyber threats in the ACS landscape

While there are extensive efforts to identify the cybersecurity challenges within the CAV ecosystem, the research domain tackling ACSs specifically is only just emerging. Fysarakis et al. [171] spotlighted their concerns about the concept of ACSs and proposed a threat model as well as generic mitigation solutions for CAVs at a general scope. More focused on ACSs, Marin-Plaza et al. [318] offered a comprehensive analysis of the ACSs deployment, signalled about the cybersecurity risks, and discussed their social implications within modern cities. However, the review was conducted from the social science perspective without a thorough cybersecurity analysis. An in-depth research study was conducted by Benyahya et al. [41] in which a holistic state of the art of the ACSs cybersecurity and data privacy threats were provided. The authors also presented a review of relevant mitigation strategies and regulations to consider within the ACSs environment. Nonetheless, concrete and non-theoretical cyber attack implementations on ACSs are still lacking.

6.3.2 Assessments based on the TARA from ISO/SAE 21434

Although several research works have provided reviews on risk assessment approaches, a limited number of researchers has showcased methods compliant with ISO/SAE 21434 on highly automated vehicles. Islam et al. [201] conducted a threat modelling and risk assessment on the vehicle speed limiter (the unit that supports a driver to not exceed a set speed limit).
Wang et al. [452] performed a risk assessment on the vehicle T-Box (which is responsible for the automotive remote-control functions, such as contactless door opening). Both publications presented systematic risk assessment frameworks; however, the proposed models do not align with recent standards. More compliant approaches to the trending ISO/SAE 21434 were proposed by Lautenbach, Almgren and Olovsson [285] and Vogt et al. [443]; however, they are limited to conventional vehicles without targeting either CAVs or ACSs assets.

6.3.3 Automotive pentests

Motivated by testing how robust vehicles are from cyber attacks, several researchers simulated attacks on isolated CAVs' components while very few asserted pentests over real vehicles. Cao et al. [64] mimicked physical removal attacks on a LiDAR sensor aiming to deceive the obstacle-detecting system [64]. Petit et al. [373] conducted jamming and spoofing attacks on isolated LiDARs and cameras under lab conditions [373]. As real pentests, Andersson [16] performed a grey-box pentest (in which the pentester has partial knowledge of the target vulnerabilities) on the in-vehicle infotainment system of a conventional Volvo car. Similarly, Moukahal, Zulkernine and Soukup [333] conducted grey-box tests, only virtually, on the vehicular software system using OpenPilot, an automated driving simulator [360]. Fowler et al. [168] conducted a black-box test (in which the pentesters have no idea about the target vulnerabilities) on a CAN testbed. Unfortunately, most of these works had neither a real highly automated vehicle of SAE L4 or L5 nor combined multiple pentests over several attacks surfaces.

To that end, our contribution differs from the aforementioned by:

- Exploring the cybersecurity concerns of the ACS as a barely studied CAV model;
- Conducting the TARA method, which is compliant to ISO/SAE 21434 standard;
- Yielding real pentests over a highly automated vehicle of SAE L4.

6.4 Material & methods

This section describes the methodological approach followed, which is also depicted in Figure 6.2.

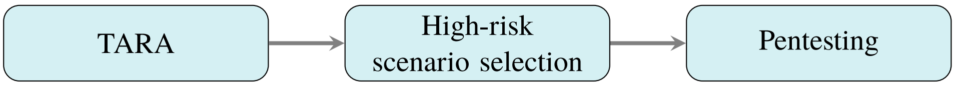


Figure 6.2: Methodology.

6.4.1 L4 evaluation vehicle

To demonstrate the TARA methodology, we analysed an ACS of automation L4, annotated throughout this paper as *L4 Evaluation Vehicle (L4V)*. The selected vehicle was used for testing highly automated driving and on-demand services for public transport on a pilot site in Geneva (Switzerland). The vehicle has a capacity of 15 passengers and drives at an average speed of 18 km/h within a predefined region of 38 hectares. Thanks to its several sensors, which include cameras, GPS, RADAR, LiDAR, and odometers, the vehicle is capable of autonomously building a picture of its surroundings, recognising obstacles, and bypassing them [470]. However, due to legal obligations, a safety operator remains required to intervene if needed, which makes it an L4 instead of an L5 vehicle.

6.4.2 Threat analysis and risk assessment

We have performed the TARA of the *L4V* using the framework provided by the standard ISO/SAE 21434. The TARA permits high-level technology agnostic risk analysis with a focus on the vehicle itself, instead of surrounding components, such as V2I/V2X or any of the backend infrastructures used by the system. The TARA includes six successive steps, depicted in Figure 6.3, in which each step relies on the findings of the preceding step. In the following sections, we describe each step that we followed and present a condensed version of our findings.

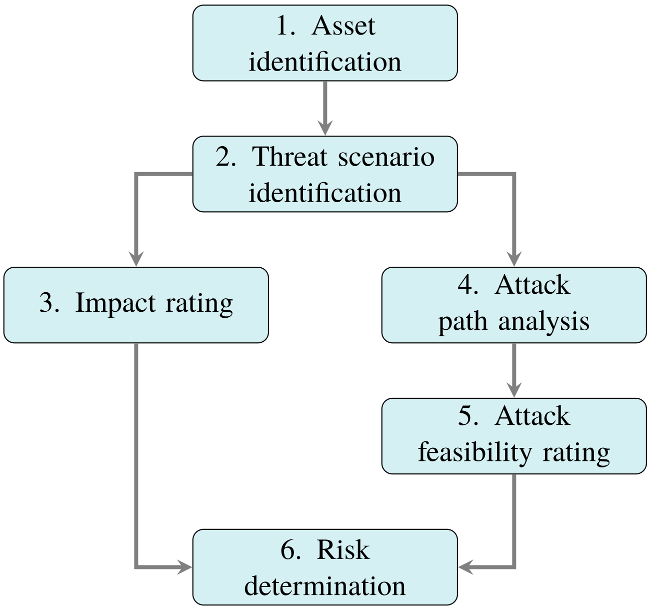


Figure 6.3: TARA steps provided by ISO/SAE 21434.

Asset identification

As the name suggests, this step is dedicated to the identification of valuable assets, which must be protected from potential damage. *L4V* was identified as having seven key assets: a 3G/4G antenna, a GNSS antenna, a 3D LiDAR, an odometer, cameras, and an on-board computer. These assets are considered to be the main entry points for an attacker and constitute every component the vehicle uses to drive autonomously. As such, any alteration to any of those components can lead to safety issues and consecutive damages. The completeness of this first step is essential as it forms the basis for determining the potential threats to the system and evaluating the likelihood and impact of those threats. It should be noted that most of these components, on the vehicle, are directly exposed to the outside environment and thus are prone to physical attacks.

Threat scenario identification

Each of the assets identified in the previous step needs to be further analysed for possible damage scenarios, leading to compromise of the cybersecurity triad Confidentiality, Integrity, Availability (CIA). Using the STRIDE threat modelling framework [329], we found 27 scenarios in total. A sample outline of the threat scenarios is shown in Table 6.1.

Table 6.1: Sample threat scenarios for 3G/4G antenna.

Asset ID	Damage Scenario ID	Description
A.1	D.1	Erroneous data are received and provoke full stop of the vehicle
	D.2	The data cannot be received and provoke full stop of the vehicle
	D.3	An external attacker modifies transmitted data or an update
	D.4	An external attacker captures the data transmitted between vehicle and the backend
	D.5	An external attacker modifies the data transmitted between vehicle and the backend
	D.6	An external attacker stops the communication between vehicle and the backend

Impact rating

The next step implies the value estimation of a potential damage scenario, performed through qualitative conversion tables provided by the TARA. It permits the assignment of a label to each scenario ranging between "Negligible" and "Severe" based on the scenario's impact on Safety (**S**), Financial (**F**), Operational (**O**), and users' Privacy (**P**). These criteria are then aggregated to obtain the "Impact Level" (**IL**), also ranging between "Negligible" and "Severe". To that end, such rankings allow us to prioritise both the economical and human repercussions to consider in order to adequately mitigate the risks based on the severity of the scenarios. An example of such a rating is provided in Table 6.2 in which severe and a major damage scenarios are depicted.

Table 6.2: Impact rating example for damage scenarios applicable to 3G/4G antenna.

Damage scenario ID	Impact category S	F	O	P	Impact level	Justification
D3	Severe	Severe	Severe	Severe	Severe	If the vehicle's software stack is modified, all data can become accessible with a risk of compromising secure driving functions such as braking, maximum speed limit, and respect of signal panels. Serious financial consequences are forecasted, as well as the loss of end-users' trust.
D.5	Severe	Severe	Severe	Negligible	Major	Active modification of ongoing communications can cause an unexpected behaviour of the vehicle or generate erroneous data for the operator.

Attack path analysis

The fourth step is designated for the synthesis of the possible implementation of damage scenarios. The resulting attack paths are a sequence of actions needed to execute an attack, as illustrated in Figure 6.4. To establish valid attack paths, one can use previous analysis from known vulnerabilities, such as the Common Vulnerabilities and Exposure (CVE) databases [343], vulnerability classifications, or taxonomies as per Sommer, Dürrwang and Kriesten [407]'s attack categorisation. The analysis can be built on a parent–child representation afterwards to meet the ISO/SAE 21434 recommendations. An example of the attack path analysis result for D.3 is demonstrated in Table 6.3 in which every path leading to the parent node from Figure 6.4 demonstrates an attack path.

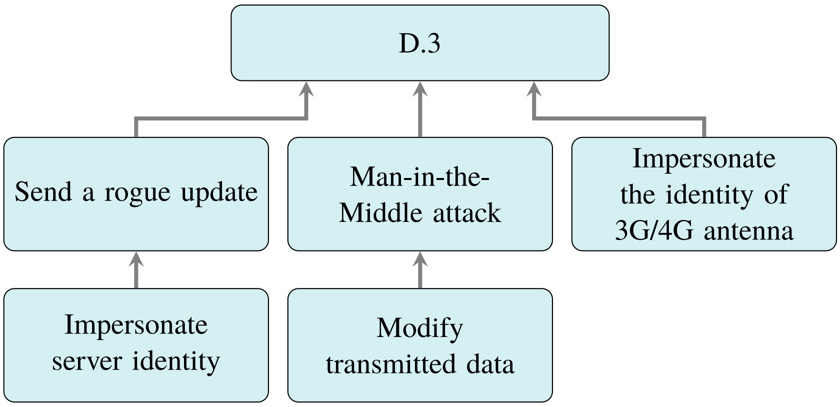


Figure 6.4: Attack tree showing three attack paths, each from lowest child to root.

Table 6.3: Sample attack path scenarios for damage scenario where attacker modifies transmitted data.

Damage Scenario ID	Attack Path Scenario ID	Attack Path Description
D3	AP.3	An attacker can impersonate the server identity to send a rogue update, thereby compromising the integrity of the legitimate data.
	AP.4	An attacker can execute a Man-in-the-Middle attack to modify transmitted data, compromising, as a result, the integrity of the legitimate data.
	AP.5	An attacker can impersonate the identity of a 3G/4G antenna and send falsified data, compromising, as a result, the integrity of the legitimate data.

Attack feasibility rating

The fifth step of the framework conducts a rating of an attack path's feasibility. This rating is based on the following criteria, listed below, in which each criterion is split into different possible ranges. Those ranges are then converted into a quantitative value and summed up to obtain the Aggregated Attack Feasibility Level (AAFL), as shown in Table 6.4. This rating represents the overall feasibility of the attack based on each of the criteria that composes it:

- Elapsed time: how much time the attack execution requires (1 week/1 month/6 months/3 years/more than 3 years);
- Expertise: skill and experience required to execute the attack, as well as how many people are needed (Layman/Proficient/Expert/Multiple experts);
- Equipment: availability of the tools needed to perform the attack (Standard/Specialised/Bespoke/Multiple Bespoke);
- Knowledge of the item or component: how much information is needed to perform the attack (Public information/Restricted information/Confidential information/Strictly confidential information);
- Window of opportunity: ease of access and time limitation (Unlimited/Easy/Moderate/Difficult).

Table 6.4: AAFL rating criteria.

Attack Feasibility	Sum
High	0–13
Medium	14–19
Low	20–24
Very low	≥25

An illustration of the previously outlined attack paths and their feasibility ratings is provided in Table 6.5.

Table 6.5: Sample of attack feasibility rating for damage scenario in which attacker modifies transmitted data.

Attack Path Scenario ID	Time	Expertise	Knowledge	Window Opportunity	Equipment	Value	Attack Feasibility
AP.3	1	6	7	4	0	18	Medium
AP.4	0	3	3	1	4	11	High
AP.5	0	3	3	1	4	11	High

Risk determination

The final step of the TARA implies the determination of the associated risk value for each damage scenario by using a risk matrix (Table 6.6). The sample output is depicted in Table 6.7.

Table 6.6: Risk matrix scale used to obtain the final risk determination.

Impact/Attack feasibility	Very low	Low	Medium	High
Severe	1	3	4	5
Major	1	2	3	4
Moderate	1	2	2	3
Negligible	1	1	1	1

Table 6.7: Final risk determination related to D.3.

Damage Scenario ID	Attack Path Scenario ID	AAFL	Impact Level	Risk Value
D.3	AP.3	Medium	Severe	4
D.3	AP.4	High	Severe	5
D.3	AP.5	High	Severe	5

6.4.3 Pentesting

The performed risk analysis is permitted to identify multiple scenarios implying high attack feasibility levels and high impact, as demonstrated in Table 6.8. Four pentest scenarios were chosen, namely AP.6, AP.11, AP.13, and AP.14, for pentest execution based on several criteria. First, the low cost and accessibility of the necessary hardware were given the highest priority as the vehicles are operating in public spaces. Second, the attacker can easily stay out of sight and has no need to physically interact with the vehicle. Finally, these scenarios can be carried out by 'script kiddies' since the software tools and documentation needed are easily accessible on the internet via open-source programs. This is why our focus was given to these wireless attack scenarios.

The pentest period was allocated outside the operating hours of the vehicles, without them being in motion, and took place at a restricted site from the public transport operator. The different attacks were carried out in a black-box environment, which is the real environment in which an external attacker could operate. The test equipment was therefore deliberately limited so as not to require hardware that was too heavy and/or too expensive. We also assume that the attacker has limited time and access to the vehicle and that no logging or system configuration information is available. The only information used to carry out the attacks is the information freely available on the internet and on the manufacturer's website.

Equipment and tools

Software Defined Radio (SDR) technologies have become mainstream. These consist of radio communication systems in which components that have been traditionally implemented in hardware (e.g., mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented using software on a computer. This allows for more flexibility in the design of the radio system and the ability to easily change its functionality. SDRs are used in a variety of applications, including wireless communication, navigation, and radio astronomy. In recent years, many new SDRs have been produced, the most well-known being HackRf, Ubertooth, or BladeRF, which we used (see Figure 6.5). The model we chose (BladeRFx40) cost us CHF 520 (≈USD 565) with two quad band antennas and was able to perform all of the attacks that we implemented. To use this equipment efficiently, we also used multiple tools, listed hereafter:

- BladeRF-cli [353] : tool required to program the BladeRF.
- GNU radio [184] : widely used open-source SDR software.
- GPS Test [185] : GNSS app for phone and tablet.
- Gps-sdr-sim [182] : generates custom GPS data streams.
- Gqrx [95] : radio waves visualization tool.
- RfCat [376] : Python library for easier programming of the BladeRF.
- Ubuntu [62] : main operating system.
- YateBTS [463] : allows the creation of one's own GSM base station.
- Wireshark [456] : open-source packet analyser.

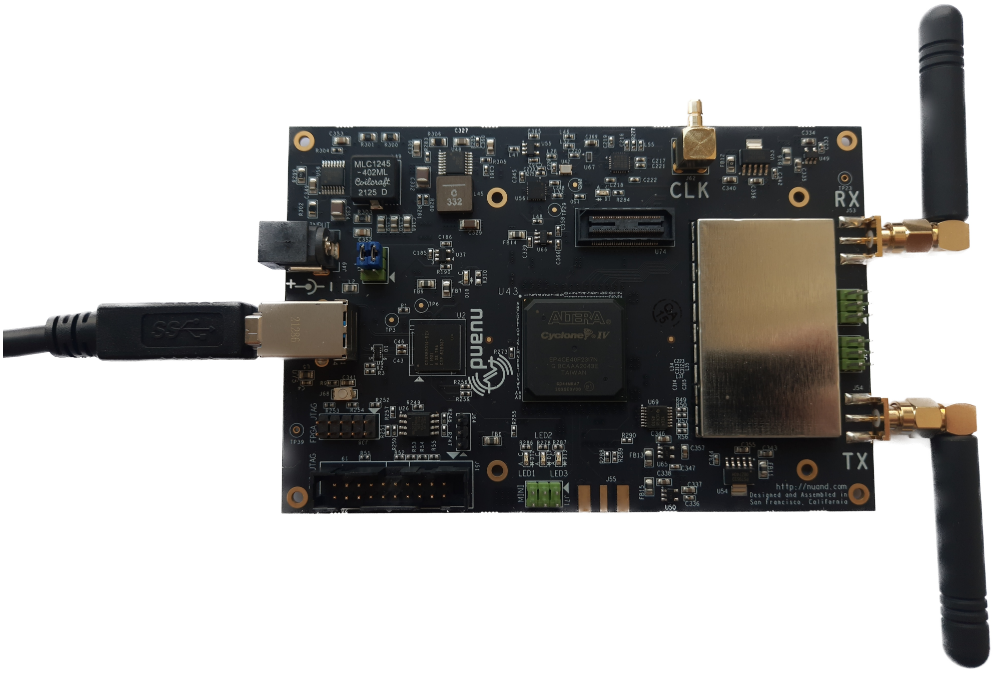


Figure 6.5: SDR BladeRFx 40 used for our experiments.

To test whether the attacks were functioning, we also used an Android phone and an Apple tablet as references. In the next sections, we show how we used those tools to perform four attacks on the *L4V*, including GNSS spoofing, GNSS jamming, rogue Base Transceiver Station (BTS), and downgrade attacks.

GNSS spoofing

GPS, which are a widely used GNSS, provide positioning, navigation, and time services to ACSs [123]. Accurate GPS positioning data are one of the critical inputs enabling safe self-driving, yet such technology has been potentially concerned with cyber attacks such as spoofing and jamming [289]. In general, spoofing is a falsified successful identification. In the case of GPS/GNSS spoofing, a radio wave transceiver is used to broadcast false signals to a GPS/GNSS receiver, which will then determine a false position. Indeed, there is no authentication method for a GNSS signal, and it can be created without much difficulty since it contains only three types of information:

- A measurement signal for position, speed, and timing.
- The ephemeris, which contains the precise positioning information of a single satellite and which has a maximum lifetime of 4 hours. Each satellite broadcasts only its own ephemeris. It is sufficient for the receiver to know the position of four satellites to propose a position [315].
- The almanack, which contains less precise information from all the satellites as well as predictions of atmospheric conditions that could change the travel time or direction of the signal. Each satellite broadcasts the almanack for all satellites. It allows the receiver to obtain data on the position of all satellites by reading only one almanack [259].

Using the published ephemeris data available on the National Aeronautics and Space Administration (NASA) website [342], it is possible to create new fictitious positions by modifying them to match the data that would actually be received if the receiver is at the simulated position. Because of its proximity to the receiver, the generated signal will be preferred to legitimate GNSS signals and will therefore modify the position announced by the receiver. This process can be used in a recreational fashion to cheat in some games that award points/bonuses based on GPS position or distance travelled, but it can also be used by attackers to disrupt the trajectory of an automated system, such as drones or CAVs. Such attacks have already been observed in Switzerland on private and commercial aircraft as well as on drones [286].

To execute a controlled GNSS spoofing attack, GNSS signals based on three positions (actual vehicle position, vehicle position offset by 4 metres and Geneva water jet) and two configurations (cold start vehicle, i.e., from a switched-off vehicle without a GNSS connection and vehicle already connected to GNSS) were transmitted using gps-sdr-sim and BladeRFx40. To accomplish this, the ephemeris was first downloaded from the NASA servers before being decompressed and used as a data source for gps-sdr-sim (see Figure 6.6). The data thus created is exported in a bitstream and then read by the BladeRF-cli program thanks to the code shown in Figure 6.7. This one sets the frequency with which the information is transmitted (1575.42 MHz) and broadcasts the data provided by gps-sdr-sim (simulation.bin). Once the program was launched, its correct operation was tested using an Android phone and an iPad to check that the spoofing was functional. For each of the tests, the two mobile devices were consistently able to lock onto the simulated position in less than 30 s, with a claimed accuracy of ±4 m.

```
wget --no-check-certificate "ftps://gdc.cddis.eosdis.nasa.gov/
gnss/data/daily/$(date -u +%Y)/brdc/brdc$(date -u +%j0.%g)n.gz"
gzip -d brdc$(date -u +%j0.%g)n.gz
mv brdc$(date -u +%j0.%g)n ephemeris
./gps-sdr-sim -e ephemeris -l [longitude,latitude,altitude] -d
[simulation_length] -o simulation.bin
```

Figure 6.6: Script used to obtain ephemerises and create the gps-sdr-sim bitstream.

```
set frequency tx 1575.42M
set samplerate 2.6M
set bandwidth 2.5M
set gain tx 32
tx config file=simulation.bin format=bin
tx start
tx wait
```

Figure 6.7: Script used to spoof the GNSS positioning.

GNSS jamming

A radio jamming attack aims to completely cut off radio communications between two points by sending powerful radio waves (noise) on the same frequencies as those used by the targeted system [123]. Thus, a jammer could target Wi-Fi, telephone communications, or RADAR, depending on the chosen frequency. Similar to GNSS spoofing attacks, jamming attacks have become more common with the advent of smaller, inexpensive solutions that can be easily set up and hidden in a bag or mounted on a wall. It should be noted that jammers are prohibited in Switzerland and more generally in Europe, from their use to their mere possession [356]. These strict measures are intended to prevent any blockage of radio waves, which are used by emergency services and aviation, among others. However, SDR devices are not subject to such restrictions, since their use as jammers is not their primary function. Thus, despite the law of 1st of January 2018 banning the import of conventional jammers, these SDR devices can be easily obtained. A BladeRF-type device cost CHF 500 (≈USD 545.2) at the time of writing, compared to several thousand francs for a conventional jammer.

The jamming attack was performed using RfCat (see Figure 6.8) in order to create noise on the desired radio frequency. This tool was used as it allows easy scripting to customise the operations of SDR platforms, whether for recording, replaying, or creating signals, as is the case here. As we already know which frequency to jam, this one is simply stored in a constant (JAMMING_FREQUENCY_IN_HZ), making this script a point jammer. If needed, it would also be possible to add in an incremental loop in order to make it a sweep jammer. Running the script resulted in a successful loss of position on both the Android phone (in "GPS only" mode) and the iPad.

```
from rflib import *

JAMMING_FREQUENCY_IN_HZ = 1575420000
_rfCat = RfCat()
_rfCat.setMdmModulation(0x30)
_rfCat.setMdmSyncMode(0)
_rfCat.setMdMRate(4800)
_rfCat.setFreq(JAMMING_FREQUENCY_IN_HZ)
_rfCat.setMaxPower()
_rfCat.makePktFLEN(0)
_rfCat.setModeTX()
```

Figure 6.8: RFlib is used to jam a predefined frequency, here 1575.42 MHz.

Rogue BTS

A rogue BTS is another method of spoofing, aiming to impersonate a telephone antenna to read the data passing through it. Victims send data through this antenna thinking it is legitimate, and the attacker can then decrypt it in offline mode and obtain compromising information while continuing to transmit the information to the legitimate network [14]. This type of attack is simple to implement, although it requires certain information about the victim's system, in particular their mobile provider, which can usually be determined from the phone number code and therefore requires knowledge of the victim's telephone number. This information is necessary because each operator transmits on different frequencies, which must be known when the attack is set up. Once again, the arrival of SDR technologies has made the implementation of such attacks much easier. With today's technology, it is possible to create a fully portable Rogue BTS with a raspberry Pi (or any other microcomputer) and external batteries, making the system lightweight and able to fit into a backpack. Because of this ease of implementation, several attacks have already been executed, notably at DEFCON 2016, where several fake antennas were spotted [93].

The Rogue BTS attack was once again carried out with BladeRF, this time using YateBTS, which is a "Software-defined Mobile Network". This tool allows for the creation of a personally owned mobile phone antenna and thus acts as the perceived operator. Once set up, it is possible to create and manage a mobile communication network and to freely communicate with any node of the network without any fees. YateBTS is highly customised which allows the impersonation of other operators. In this case, the local operator's 3G network information was inserted in order to spoof one of their antennas. The data on the frequencies and positioning of the antennas was found using Cellmapper [67], and the use of 3G was decided by watching the screen of the ACS, which used a 3G connection rather than 4G. We chose the local operator's network after reading a document from the Federal Roads Office indicating problems when using a similar vehicle due to the failure of the local operator's antenna [357]. The mobile operator was then crosschecked and confirmed by our contacts from the public transport operator. Once the dummy antenna was in place, we performed a packet analysis using Wireshark.

Downgrade attack

To increase the security of communications, 3G/4G networks encrypt communications. Although it is possible to decrypt them with brute force attacks, the time required for decryption is often too long for the attacks to be considered cost-effective. However, when network coverage is not good enough to guarantee 3G or 4G communications, many devices default to 2G or EDGE connections to continue providing their communication services. Although useful for the user, this fallback solution has security limitations as it uses the vulnerable A5/1 data encryption protocol [14]. Indeed, there are now many tools that can decrypt A5/1 encrypted data quickly and easily [181]. To achieve this goal of relying on 2G technologies, the simplest method is to degrade 3G and 4G connections by jamming their frequencies. This can again be completed with an SDR device and will, if the device allows it, force a switch to the less secure technology.

As explained, connectivity downgrade attacks rely on jamming the newest protocols (3/4/5G). Therefore, we followed the same method and code that we used for the GNSS jamming (see Section 6.4.3) by replacing the frequency to jam with the correct one.

Table 6.8: Risk determination

Asset	Damage Scenario	Attack Path	*An attacker could…*	†C	I	A	AAFL	IL	RV	Risk Treatment
A.1	D.1	AP.1	retransmit past data using an SDR transmitter so that the vehicle receives erroneous data	✗	✓	✓	High	Moderate	3	Integrity controls
A.1	D.2	AP.2	use an SDR transmitter or a more conventional jammer to prevent the vehicle from connecting to the network antennas	✗	✗	✓	High	Moderate	3	Offline automated mode
A.1	D.3	AP.3	impersonate the backend server in order to send a rogue update to the vehicle	✗	✓	✗	Medium	Severe	4	Integrity controls Authentication Cryptography
A.1	D.3	AP.4	perform a Man-In-The-Middle attack between the vehicle and the backend server to modify the data sent by the server	✓	✓	✗	High	Severe	5	Integrity controls Authentication Cryptography
A.1	D.3	AP.5	impersonate a 3G/4G antenna and send data to the vehicle	✗	✓	✗	High	Severe	5	Integrity controls Authentication Cryptography
A.1	D.4	AP.6	perform a Man-In-The-Middle attack between the vehicle and the backend server to listen to the data sent by the server	✓	✓	✗	High	Moderate	3	Cryptography Authentication
A.1	D.4	AP.7	perform an auxiliary channel attack by ”listening” to the electromagnetic emanations of the on-board computer	✓	✗	✗	Low	Moderate	2	Side channel attacks mitigations
A.1	D.5	AP.8	impersonate the backend server in order to transmit arbitrary data	✗	✓	✓	High	Major	4	Cryptography Authentication
A.1	D.5	AP.9	perform a Man-In-The-Middle attack between the vehicle and the backend server to modify the data in transit	✓	✓	✗	High	Major	4	Cryptography Authentication
A.1	D.5	AP.10	impersonate a 3G/4G antenna and send data to the vehicle	✗	✓	✓	Medium	Major	3	Cryptography Authentication
A.1	D.6	AP.11	use an SDR transmitter or a more conventional jammer to prevent the vehicle from connecting to the network antennas	✗	✗	✓	High	Moderate	3	Offline automated mode

Continued on next page

Table 6.8: Risk determination (Continued)

Asset	Damage Scenario	Attack Path	*An attacker could…*	[†]C	I	A	AAFL	IL	RV	Risk Treatment
A.2	D.7	AP.12	use an SDR transmitter to replay previously received signals in place of the actual signals	✗	✓	✗	High	Moderate	3	Data timestamping
A.2	D.8	AP.13	use an SDR transmitter to play custom signals instead of real GNSS signals	✗	✓	✗	High	Moderate	3	Military GPS technologies
A.2	D.9	AP.14	use an SDR transmitter or a more conventional jammer to prevent the vehicle from connecting to the GNSS	✗	✗	✓	High	Negligible	1	Offline automated mode
A.3	D.10	AP.15	throw an object or hit the camera to damage it	✗	✗	✓	High	Moderate	3	Camera shielding
A.3	D.11	AP.16	throw a sticky object or other obscuring material (e.g. paint) at the camera	✗	✗	✓	High	Moderate	3	Camera shielding Hydrophobic material
A.3	D.12	AP.17	use an acoustic device to disrupt the vehicle's in-built image processing software	✗	✓	✗	Low	Moderate	2	Phonic isolation
A.4	D.13	AP.17	disrupt a gyroscope with sound, causing the vehicle to change speed due to false information about climbing or descending	✗	✓	✗	Low	Negligible	1	Phonic isolation
A.5	D.14	AP.18	use lasers to disrupt the operation of the LiDARs and cause the vehicle to stop	✗	✗	✓	High	Moderate	3	Faster LiDAR tick rate Photochromic lens
A.5	D.15	AP.19	throw a sticky object or other obscuring material (e.g. paint) at a LiDAR	✗	✗	✓	High	Moderate	3	LiDAR shielding Hydrophobic material
A.5	D.16	AP.20	throw an object or hit a LiDAR to damage it	✗	✗	✓	High	Moderate	3	LiDAR shielding
A.6	D.17	AP.21	use an acoustic device to distort the vehicle's speed measurement, which could cause it to speed up or slow down	✗	✓	✗	Low	Moderate	2	Phonic isolation
A.7	D.18	AP.22	perform an auxiliary channel attack by "listening" to the electromagnetic emanations emitted by the on-board computer	✓	✗	✗	Low	Moderate	2	Random CPU noise

Continued on next page

Table 6.8: Risk determination (Continued)

	Damage	Attack								
Asset	**Scenario**	**Path**	***An attacker could…***	**†C**	**I**	**A**	**AAFL**	**IL**	**RV**	**Risk Treatment**
A.7	D.18	AP.23	use direct access to the on-board computer to read the computer's memory continuously	✓	✗	✗	High	Moderate	3	Group policies Computer tray shielding
A.7	D.19	AP.24	use the keyboard provided in the vehicle to exit the navya program and install other programs	✓	✓	✓	High	Severe	5	Remove keyboard Computer tray shielding USB port security
A.7	D.19	AP.25	disconnect the hard drive from the on-board computer and plug in another one	✗	✓	✗	High	Severe	5	Alarm system Computer tray shielding
A.7	D.19	AP.26	use a live USB to bypass boot passwords and modify disk contents	✗	✓	✗	High	Severe	5	Bitlocker Secure boot BIOS/CMOS password USB port security
A.7	D.20	AP.27	use a live USB to bypass boot passwords and modify disk contents	✓	✗	✓	High	Moderate	3	Bitlocker Secure boot BIOS/CMOS password USB port security
A.7	D.20	AP.28	use the keyboard provided in the vehicle to exit the navya program and observe the contents of the disk	✓	✗	✓	High	Moderate	3	Service account Group Policies Computer tray shielding
A.7	D.20	AP.29	disconnect the hard drive from the onboard computer and read it on his own device	✓	✗	✓	High	Moderate	3	Bitlocker Computer tray shielding
A.7	D.21	AP.30	use the keyboard provided in the vehicle to turn off the on-board computer	✗	✗	✓	High	Major	4	Computer tray shielding
A.7	D.21	AP.31	physically damage the on-board computer	✗	✗	✓	High	Major	4	Computer tray shielding
A.7	D.21	AP.32	use the I/O button to turn off the on-board computer	✗	✗	✓	High	Major	4	Computer tray shielding
A.7	D.21	AP.33	disconnect the on-board computer	✗	✗	✓	High	Major	4	Computer tray shielding

Continued on next page

Table 6.8: Risk determination (Continued)

Asset	Damage Scenario	Attack Path	***An attacker could…***	†C	I	A	AAFL	IL	RV	Risk Treatment
A.7	D.21	AP.34	could install malware on the on-board computer	✗	✗	✓	High	Major	4	Computer tray shielding USB port security

[†] Confidentiality, Integrity, Availability (CIA); Aggregated Attack Feasibility Level (AAFL); Impact Level (IL); Risk Value (RV)

6.5 Results

6.5.1 The TARA showcasing

As demonstrated in Table 6.8, the TARA framework assessed different risks threatening the ACS security that we classify into three main groups: (i) high risks of values 4 and 5 (ii) medium risks of values 2 and 3 (iii) low risks of value 1 The first group concerns mainly communication with the backend servers, enabling real-time data transfer and OTA updates, and the on-board computer, on which all vehicle subsystems depend. Those attacks do not represent the vast majority of the state-of-the-art use cases, which usually imply an internal communication medium, such as CAN or LIN, or attacks on sensors and, hence, obtained lower values of two and three, which are significant yet unexpected. Finally, further specific attacks obtained the lowest rating value of one, as they involve tools that are difficult to put in place or have low impact.

High-risk scenarios

The scenarios obtaining the highest scores concern attacks on the means of communication as well as attacks involving physical access to the on-board computer. The former remains relatively simple to deal with as mitigation methods, such as data encryption, can be enough and are likely to be implemented by the OEM. Consequently, it is impossible to determine whether data in transit are authenticated and whether integrity checks are carried out. However, as the encryption, authentication, and integrity checks are software-based without requiring any hardware substitution, such a setup can be implemented promptly by a team dedicated to system hardening. On the contrary, attacks involving physical access to the on-board computer require different mitigation strategies that require further hardware changes.

As many of the current CAVs are prototypes, physical security for access to the digital systems is not a high priority at the moment. This can be attributed to the experimental nature and rapid development requirements of the vehicle, which include relatively easy access to the on-board computer. However, we have to mark this as a major security risk, and it may remain a high risk if no proper anti-tempering solutions are employed. The L4V is supplied with a keyboard that can allow the user to escape the OEM's program and access the host operating system. On the same note, several active USB ports are present on the machine attracting malicious intentions to plug a rogue device into the vehicle to damage the system or steal information. Theoretically, access to such ports allows the total destruction of the on-board computer via a "USB Killer", which is able to physically destroy a computer by several 240V discharges sent into the USB port. Nowadays, such attacks can even be performed remotely and without the computer being turned on, thanks to the USB Killer V.4 [435].

Medium-risk scenarios

Scenarios with a score of two and three are attacks that have a much lower immediate impact if carried out, although they are not without consequences. These attacks fall into two categories: attacks that cause the vehicle to stop and lead to damages and eavesdropping.

In the current framework of operations, involving a restricted route at low speed (18 km/h) with few or no other vehicles on the road, such attacks do not induce major risks for the users' safety, yet a sudden stop can cause minor disturbances. However, in a more dense traffic context, such attacks can impact both user and pedestrian lives. As with the high-risk scenarios, the mitigation strategies should encapsulate physical and software upgrades, including the implementation of cryptographic protocols for data security, as well as reinforcements to the vehicle's sensors.

Attacks that eavesdrop on data between the vehicle and the OEM's servers would not have an immediate impact on ongoing operations but would allow an attacker to obtain information about the operation of the vehicle for future privacy attacks. By decrypting the communications' keys, or if they were simply not encrypted, more knowledge about the data can be sucked up leading to new attack scenarios, such as vehicle tracking. Similarly, cryptographic protocols remain the key mitigation technique to consider.

Low-risk scenarios

Scenarios that have been given a minimum score of one do not necessarily require immediate intervention, yet they should not be underestimated. The impact of low-risk scenarios is asserted to be moderate because of their difficulty in implementation with the means currently available to attackers. However, with the emerging technologies that the attackers can afford, such risks can evolve in the near future and considerably facilitate the feasibility of the attacks in question.

To that end, several mitigation methods are proposed for the three scored groups as shown in Table 6.8. The suggested treatments are mainly related to the implementation of software measures, such as data encryption and hardening solutions for vehicle software components, in addition to efficient shielding of the core automated driving units, such as the on-board computer and sensors. The implementation of a fully automated mode without a wireless connection is also recommended as it decreases the jamming risk, though, it limits the chances for cooperative automated driving, which is an essential aim of smart cities. As concerns remain about the trade of maximising the readiness of self-driving operations and minimising associated cyber risks, it is crucial to set up testing tools carrying out continuous or frequent risk assessments as per pentests. The next session showcases the results of the conducted GNSS spoofing and jamming in addition to the Rogue BTS and Downgrade attacks corresponding to AP.6, AP.11, AP.13, and AP.14, respectively.

6.5.2 Penetration outcome

Jamming the radio signals was the prime motivation of our pentests. One of the goals of our research was to evaluate the vehicle reaction upon a jammed signal. This was successfully demonstrated through the GNSS jamming attack. The Rogue BTS and the Downgrade attacks showcased the fairly efficient mitigation solutions in place. Moreover, the attempted black-box GNSS spoofing did not disrupt the vehicle operations pushing for further grey- or white-box bids. Another piece of evidence of the vehicle's great resistance is that no sensitive data (such as usernames or passwords) were leaked due to the pentests, which indicated the presence of a minimum of security on the vehicle. Consequently, the pentest we provide here only tests some of the vehicle's on-board systems and is constrained to a black-box environment. More extensive testing should be explored before deploying fleets of these ACSs on the road. Such matters are discussed in the following section, as well as a detailed overview of the outcome of each conducted scenario.

GNSS spoofing

Whether the vehicle is in an active GNSS connection or not, the spoofing attack did not reflect a noticeable change in vehicle behaviour or metrics. In a disconnected state, the GNSS signal information remained the same according to the on-board monitor. Such a status is displayed through an orange symbol indicating that the vehicle is not receiving valid GNSS data. The main reasoning for such results is the dismissed access to the system logs and the limitation on the testing equipment or system knowledge. A lack of power in BladeRFx40, a safety device set up by the vehicle, or the angle of arrival of the signals to the GNSS antenna can be examples of such reasoning. On the same note, as the GNSS antenna is located on the roof of the vehicle, it is possible that the radio waves emitted by BladeRF were not received. Without access to the on-board computer logs or indications of the exact position of the vehicle, it is difficult to state the exact reason for the shuttle's inability to connect to our signals. These results were identical for all three positions and both vehicle configurations, totalling six tests.

GNSS jamming

The jamming attacks produced results fulfilling our expectations yet without great surprises. As the vehicle requires radio communication systems, it is conspicuous that blocking such signals implies that the vehicle will be disrupted or forced to a halt. This point implies a fundamental modification of the vehicle program through the implementation of a fully automated offline mode. In fact, jamming attacks are frighteningly easy to set up despite the legal constraints on their use. Therefore, in the current configuration, any owner of an SDR platform is capable of completely blocking the operations of the vehicle as it is set to stop immediately when the signal is lost. A remote control system can be considered to support the circumvention of such situations; however, the use of radio waves alone would not solve the problem since it would again be possible to jam this particular connection and thus prevent remote troubleshooting. Therefore, a fully automated offline mode allowing the vehicle to move to the side of the road or to an area suitable for dropping off its passengers should be considered. This system, therefore, leaves the door open for various improvements with other radio communication information.

Rogue BTS

The packets captured by Wireshark during the implementation of the Rogue BTS confirmed the encrypted network connection. Cross-checked with the public transport operator team, it was asserted that a Virtual Private Network (VPN) connection is built between the OEM's backend servers and the vehicle. Hence, the data in transit is encrypted from end to end and can therefore be considered secure. However, it is still possible to break the encryption keys in offline mode using existing tools such as

Hashcat. Such a practice is usually too time-consuming to be cost-effective [14]. Additionally, if the encryption keys are changed regularly (respecting perfect forward secrecy), breaking one of them will not allow the decryption of all communications but only those of the specific session of the key. Thus, Rogue BTS attacks can be considered ineffective against this vehicle.

Downgrade attack

Despite successfully jamming of the mobile network, we can see that the vehicle did not have a fallback function on a 2G (GSM) network as it simply indicated that no mobile connection was available. It is therefore not possible to exploit downgrade attacks on connectivity in that case.

6.6 Discussion & future work

Our research goal was twofold: provide recommendations upon the findings from the TARA and the pentests and study the identified research questions to set up comprehensive insight on the correlation between the cyber risks impacts and the vehicle automation level. Our work aims to support in reinforcing security requirements for a future concrete deployment of the ACS going beyond pilot site testing.

6.6.1 Recommendations

Based on the results from the TARA and the pentests, we believe that human intervention, and hence the vehicle automation level, have a direct impact on the assessed risks. Some attacks, particularly GNSS spoofing, are only applicable if there is no driver who can immediately take control of the vehicle if it goes off the road. In other words, a moderate risk in a vehicle of L4 can be considered severe in an L5 vehicle unless robust and flawless mitigation strategies are implemented.

To strengthen the entire cybersecurity governance for L4V and support the ACS L5 readiness, the following crucial, yet non-exhaustive, recommendations are delineated:

- **Physical strengthening**: where LiDARs, cameras, USB ports, and the on-board computer are unreachable and protected from any unwarranted access.

- **Fully automated offline and resilient mode**: providing high protection against jamming attacks and unjustified halt or vehicle stops at a complete connectivity loss.

- **Confidentiality and integrity of communications:** where PKI and digital signatures can be used to secure authentications in addition to HTTPS and IPSec tunnel mode (such as VPN) establishment.

- **Hardening of the on-board computer:** which relies on (i) protecting the BIOS through Root of Trust for Update (RTU) and Trusted Platform Module (TPM) usage during the firmware update [83] (ii) shielding the disk protection through Bitlocker [14] (iii) adopting operating system best practices, such as the installation of a Host-based Intrusion Prevention System (HIPS) and applying restrictive policies on the listing of files and their modification

- **Standardised security procedures and certifications:** varying from conducting CSMS [430] and SUMS [431] certifications mandated by the UNECE to comply with ISO/SAE 21434 [233] and ISO/PAS 5112 [231].

- **Security monitoring:** where continuous and frequent assessments are conducted and risks are monitored using the integration of a Security Information and Event Management (SIEM), for example.

6.6.2 Research questions analysis

To answer RQ1, the present work provided a systematic categorisation and analysis of cybersecurity risks by applying the TARA to the ACS domain. Three main groups were identified: high (risk values of four and five), medium (risk values of two and three) and low (risk value of one). Although the TARA is suitable for threat modelling and analysing risks, it remains limited in assigning an objective risk value with regard to the automation level. In fact, the weight of the automation level depends on the experts' opinion and their expertise. Furthermore, being an asset-based methodology, the automation features are impossible to evaluate as a single asset from the TARA.

Limited by several real-life pilot restrictions, the pentests that we managed to execute confirm the ease of the necessary setup for an attacker to execute high-risk scenarios. In particular, the affordability of the equipment required as well as the short timespan in which an attacker can perform an attack, have been demonstrated. As far as 3/4/5G jamming is concerned, the most cost-effective solution in terms of time is sweep jamming on the frequencies of the most widely used operators, which means that it is not necessary to find out which operator is used by the manufacturer. However, the black-box penetration tests and vehicle resilience that we observed did not provide any additional insights into whether the vehicle was affected by the intended malicious activities. Therefore, we cannot confirm if the mitigations applied to the vehicle were sufficient; hence, black-box penetration testing is not suitable. To answer RQ2, we believe that the openness of the OEM's ACS ecosystem towards elevating the restriction on internal data access (e.g. logs) is required to both execute physical attacks and cross-check the effectiveness of the conducted wireless pentests.

6.6.3 Limitations & future work

Following up on the discussion about unwarranted on-board access, it is noteworthy to highlight that diving deeply into the vehicle logs represents a real limitation to verifying the evident effects of our pentests. The restrictions also made the entire pentest more complex as it was limited to being pushed in a black-box manner. Therefore, our future efforts are focused on conducting grey and white pentests. More specifically, it is envisioned to target further assets varying from automated driving decision-making units, V2X components, on-demand service applications, and the fleet management system.

Additionally, considering the continuous upgrades impacting the vehicle operating systems, supplementary tests are foreseen to accomplish future comparative analysis with the present findings. On the same note, for a more granular and uniform analysis, it is planned to complement the attack tree paths with an additional detailed level linking CVEs to each damage scenario. Such a future work would provide consonant comparisons and an evolution of the identified vulnerabilities based on the universal CVE databases [343].

Another shortcoming to highlight in the present research is the impact of the rapidly evolving technologies on the pertinence of our findings. Being a pilot vehicle under regular emerging changes, the L4V has been subject to several modifications and upgrades. Consequently, our findings reflect the risk analysis and pentests results on the assessed vehicle configuration at the time of the elaboration of our experiments. As a future work, we intend to build an automated TARA framework supporting with continuous assessment of the L4V risks with a possible comparison of current risk values to the historical records. Such a solution aims to help keep risks at an acceptable level while coping with the technological progression.

To that end, the present work can be considered a valuable path and a starting point advertising the implementation of frequent risk assessments and the importance of penetration testing on approaching the full deployment of L4 and L5.

6.7 Conclusions

The objective of this work is to provide the first example of a cybersecurity analysis on an L4 ACS. Based on the TARA framework, threat modelling and risk analysis of the ACS were outlined on the selected vehicle assets. We elevated further the risk analysis findings by conducting four pentest scenarios focused on GNSS and 4G connections. Based on the implementation results, we proposed several mitigation solutions and technical recommendations to be implemented in future iterations. The outcome showed that the automation level is still a missing attribute throughout the TARA process, yet it has a direct impact while selecting accurate mitigation strategies with consideration of human intervention. We further identified a set of limitations that trigger motivation for future efforts.

Acknowledgment

This work has received funding from the European Union's Horizon 2020 Research and Innovation Programme (grant agreement no. 875530, SHOW project) and the Swiss State Secretariat for Education, Research and Innovation (SERI) co-funded by the European Union (grant agreement no. 101077587, ULTIMO project). The views and opinions expressed herein are, however, those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

The authors would like to thank the transports publics genevois (TPG) for their collaboration, more specifically Melisa Fazlic and Jeroen Beukers, without whom it would not have been possible to carry out this project.

Part IV

Enhanced TARA implementation

Chapter 7

Article VI: Driving towards resilience: Advancements in threat analysis and risk assessment for connected and automated vehicles

Relevance

This article fully explores RQ4, RQ5 and RQ6 of the present thesis. It effectively defines avenues for improving TARA 1.0, as proposed by ISO/SAE 21434, to properly address the properties of L4 and L5 CAV. The article defines the methodology followed to both identify and implement the required enhancements through the innovative TARA 2.0. Additionally, the article incorporates a PoC to showcase the new framework applicability. The PoC consists of demonstrating TARA 2.0, in a simplified way, over a reference architecture. The validity of the proposed framework is approached through a comparative analyses. To sum up, the article aims to deeply study the limitations of TARA 1.0, propose TARA 2.0 as a solution, demonstrate its process for future replications and showcase its performance over TARA 1.0.

Context

This article [42] is under a first review in the IEEE Transactions on Intelligent Vehicles Journal whose IS: 7.70, h-Index:43 and SJR: 1.583 according to the Resurchify portal[1].

Own contribution

Being the lead author of this article, my contribution consists of the enhancements identification, framework conceptualisation, the assessment conduction and workshops leading. While the co-authors contributed with their opinion in both threat modeling and risk analysis to increase the assessment results confidence, the majority of the paper content was provided by me. The co-authors had also the crucial role of reviewing that content and improve the figures clarity.

[1] https://www.resurchify.com/about

Contents

7.1 Abstract

CAVs are foreseen as the new shift paradigm towards smart, safe and autonomous transportation. Though, ambivalent cybersecurity and privacy concerns are contributing to the immaturity of CAVs of SAE level four (L4) and five (L5) where full automation is intended. For an appropriate risk governance, the UNECE R155 regulation and ISO/SAE 21434 standard mandate TARA implementation as a key methodology to identify, evaluate, mitigate and monitor the cyber risks. Unfortunately, existing TARA methodologies are limited to L3 CAVs, are not focused on privacy risks and rely on experts' knowledge which may impact the risk assessment subjectivity. Under the umbrella of the project ULTIMO[2], tackling the issues facing CAVs deployment, the present work proposes an improved TARA framework, referred to as TARA 2.0. This framework puts forward CAVs' properties, potential cybersecurity and privacy threats as well as a fine-grained analysis of the experts objectivity throughout the assessment process. Our approach is demonstrated through a step-by-step implementation showcasing its feasibility and compliance to ISO/SAE 21434. Our findings indicate strong promise in offering a customised TARA framework for L4 and L5 CAVs, prioritising privacy concerns and enhancing transparency regarding expert involvement throughout the process.

7.2 Introduction

For the last decade, the automotive sector has witnessed a major switch from mechanical to cyber-physical systems where IT components have become dominant. Recent technological enablers such as AI, advanced environmental sensors, ECUs, as well as V2X communications support in steering the automotive domain further to achieve highly automated driving where human interventions are reduced to a bare minimum. The SAE proposed six levels of automation, L4 and L5 representing the most advanced stages where vehicles can drive autonomously within limited or unlimited ODD [38]. Prominent illustrations of such CAVs, are already taking place in today's roads. Baidu, Cruise, Pony, Waymo and Zeekr showcase how those vehicles are progressing beyond the experimental phase [37, 194].

The CAV is a subset of the broader IoV, which itself stems from the IoT. This evolution has transformed conventional vehicles into smart agents that remain continuously connected. Stipulated by the advancement of the IoT, CAVs promise safer traffic with less human-related driving errors, smarter mobility services for individuals who are unable to drive (physical constraints), less polluting means of transportation, and lower road-ways congestion [351]. Alongside the safety, social and ecological advantages of CAVs, cybersecurity and data privacy concerns pose significant obstacles to their successful and large scale deployment [434]. By incorporating safety-critical systems, software and hardware components as well as endless data exchanges, CAVs bring out a litany of attack vectors [41].

A compromised component from the CAV's environment implies inappropriate driving operations, sensitive data infringements and even fatal accidents jeopardising

[2] The ULTIMO project (https://doi.org/10.3030/101077587) is co-funded by the European Union and the Swiss State Secretariat for Education, Research and Innovation (SERI) under the Horizon program.

the passengers safety and privacy. CAV's potential attacks vary from manipulating perception systems leading to blinding the vehicle vision, falsifying navigation data causing a go off course, infiltrating communication channels leading to malicious messages injections to code alteration impacting the vehicle motion control capabilities [179, 412]. Moreover, any malicious access to the CAV, where numerous of directly or indirectly identifiable data are exchanged, is a subject to a potential data breach [364]. Consequently, the sniffed or maliciously processed data that can likely embed PII such as name and phone number, taken routes as well as departure and arrival addresses can be the source of an array of privacy attacks including identity theft, location tracking and profiling [30, 75].

The interplay between the CAV's evolving technologies, their benefits and the related threats guided the core regulatory and standardisation bodies to harmonise the cybersecurity governance. The UNECE R155 and R156 [430, 431] mandate TARA, referring to ISO/SAE 21434 [233], as an automotive cybersecurity governance tool for detecting, evaluating, mitigating and monitoring potential threats throughout the vehicle life-cycle from design to end of life stages. As of now, security actors from industry, academia and standardisation, proposed numerous TARA methodologies such as EVITA [382, 143], HEAVENS [201], TVRA [130], SARA [331], VeRA [97] and PIER [366]. However, none of them sufficiently tackle the specific properties of L4 and L5 CAVs and the related challenges. First, existing methodologies do not consider data privacy threats at the forefront of secure CAV's implementation [30]. Second, those methodologies lack an explicit distinction in addressing CAVs of SAE L3, L4 and L5 as the proposed assessment process remain identical for the three levels [40]. Third, while the TARA process depends heavily on experts evaluation, existing methodologies do not advertise any confidence factor supporting in determining the objectivity of the assessment outcomes [3]. Fourth, existing methods lack detailed demonstrations to facilitate the entire TARA process replication. To that end, we conclude that it is an absolute necessity to resolve the shortcomings in the current TARA framework for supporting the L4 and L5 CAVs in withstanding the continuously evolving cybersecurity and data privacy threats. This work aims to reply the following RQs:

RQ 1 *Is it feasible to extend TARA methodology for L4 and L5 CAVs while improving the focus on privacy threats?*

RQ 2 *How the assessed risks from TARA can depict scrupulously the CAV's SAE automation level?*

RQ 3 *To what extend the TARA process can be automated to reduce its reliance on experts opinion?*

Our contributions are the following:

1. Formulating the improvement avenues to the mandated TARA from ISO/SAE 21434 (hereby denoted as TARA 1.0).

2. Proposing TARA 2.0 as an improved framework addressing privacy, automation level and experts subjectivity concerns.

3. Demonstrating TARA 2.0 through a PoC using a step-by-step approach to showcase the applicability of the framework.

The remainder of this paper is organised as follows: Section 7.3 sets the foundations of our discussion. Section 7.4 proposes TARA 2.0 by outlining the methodology for the construction of each step of the assessment. Section 7.5 demonstrates the use of TARA 2.0 through an assessment of the ADS processing unit of an L4 CAV. Section 7.6 delves deeper into the asserted insights, limitations and the foreseen future work. Section 7.7 captures the related work on various efforts towards improving TARA frameworks. Finally, Section 7.8 deduces the paper through concluding remarks.

7.3 Key concepts and definitions

The present section establishes the foundations for the technical discussions throughout the manuscript. It offers fundamental insights into the CAV landscape, highlights the importance of TARA regarding the key regulations and standards, and introduces the classical TARA 1.0 workflow.

7.3.1 CAVs ecosystem

Over the last decade, cybersecurity and data privacy have become of significant interest in the CAV's domain. Several factors have converged to generate such interest. First, to perceive its surroundings, the CAV relies on the measurements generated by embedded cutting edges sensors, varying from LiDAR, RADAR, to cameras, which represent a substitution of the human vision capabilities [3]. While these sensors promise efficient and safe navigation, they are susceptible to tampering or data manipulation [41]. Second, the number of lines of source code in the ECUs exceeding 300 million lines in L3 CAVs and 500 million lines in L4 and L5 [4] represent a great opportunity for malicious actions [311]. In practical terms, this means that essential driving functionalities, such as steering or braking, can be controlled by software that may inherit code vulnerabilities if adequate security defences are not in place. Third, CAVs rely on multiple connections taking the form of cellular (4/5/6G) or short range communications like Wi-Fi or DSRC [48]. On one hand, such connectivity enables the CAV to exchange data with smart infrastructure (V2I) or other vehicles (V2V), facilitates the OEM interventions for on-the-air updates or diagnosis, allows remote monitoring and teleoperating [341] and offers innovative services to end-users [453]. In the CAV's ecosystem, end-users extend beyond vehicle owners or passengers to include any customer getting benefit from the CAV's mobility services [455] such as on-demand services [65], first- and last mile transport [165] and logistics services [275]. On the other hand, either of these communications paths could be exploited by an attacker to sniff PII data or inject malicious inputs [76].

CAV's technologies are not set in stone. Throughout the CAV's life-cycle, from design to decommissioning, technologies supporting the ADS functioning will continue to evolve alongside with the offered mobility services [453]. Consequently, such evolution may potentially introduce new vulnerabilities expanding the opportunities to threat actors for malicious assaults.

Table 7.1: SAE automation levels by SAE J3016 [38].

Properties	**L0**	**L1**	**L2**	**L3**	**L4**	**L5**
Driving automation	No	Driver assistance	Partial	Conditional	High	Full
ODD	N/A	Domain specific	Domain specific	Domain specific	Domain specific	Unlimited
DDT fallback	Driver	Driver	Driver	Fallback ready-operator	ADS or fallback ready-operator	ADS
Connectivity	Not required	Not required	Not required	Recommended	Recommended	Extended V2X

Furthermore, the SAE automation levels introduce an additional level of complexity. Each level from Table 7.1 is differentiated by its reference to the automation of the DDT, encompassing both human and the ADS engagement, along with the ODD, which describes the driving conditions and limitations [389]. In case of a cyber assault, and depending on the SAE level, the driver, operator or the ADS has to take over or relinquish the DDT [180]. In the instance of an attack targeting L4 perception sensors, a prepared fallback operator, whether remote or in-vehicle operator, can guide the vehicle into a stable and safe state, referred to as the MRC in standardised terminology [389]. Projecting an equivalent scenario over an L5 CAV, the ADS per se must achieve the MRC independently of any type of human intervention. As showcased in Table 7.1, several features support distinguishing the properties of each SAE level including the ODD limitation, how the MRC can be conducted, as well as the amount of V2X connections. Therefore, cybersecurity and data privacy considerations, including threats modelling and risk governance have to address such differences respectively.

7.3.2 Standards & regulations

With the prevalence of the aforementioned risks, the core standardisation bodies, as per ISO and SAE, elicited norms reflecting risk management applications into the automotive domain. The most dominant standard to comply with is ISO/SAE 21434 [235] since it has been proposed as a key reference in the mandated regulations R155 and R156 by the UNECE WP29. Both regulations are requiring the CSMS [430] and the SUMS [431] certificates respectively. The CSMS comes with the obligations of integrating cybersecurity governance to the OEM’s organisation and over the entire value chain [326]. Similarly, the SUMS aims to demonstrate that any vehicular software update is not extorting further cyber risks or impacting the overall cybersecurity governance [431]. Both certificates have been set as pre-requisites of the vehicle type approval with a three years renewal cycle by the presentation of an assessment evidence [430]. In this context, ISO/SAE 21434 aligns with UNECE regulations in two perspectives. First, it offers guidelines for organisational audits. Second, it sets the path for obtaining type approval evidence by executing a TARA [453].

As depicted in Figure 7.1, further standards are evoked to complement the

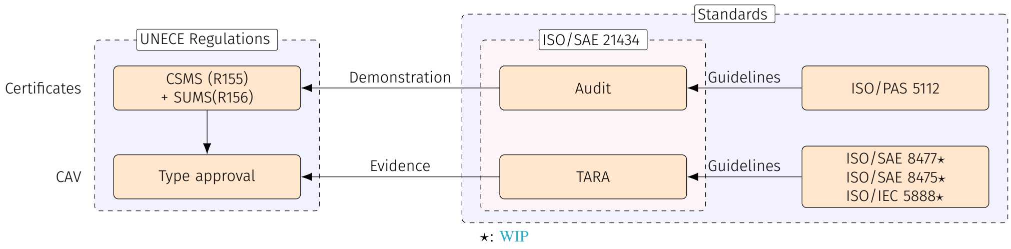


Figure 7.1: UNECE regulations vs ISO standards [453].

ISO/SAE 21434 in achieving the required conformity for the UNECE certificates. On one hand, the published ISO/PAS 5112 [231] supports in auditing organisational cybersecurity processes. On the other hand, various initiatives aim to indicate the level of rigour and support in evaluating the reliability of the TARA outcomes. Among such efforts, the ISO/SAE 8477 [236] intends to provide guidelines on verifying and validating the cybersecurity goals. The ISO/SAE 8475 [234] will introduce new metrics (CAL and TAF) reflecting the assurance level of the executed TARA. The ISO/IEC 5888 [227] posits further cybersecurity and data privacy evaluation requirements for connected vehicles in particular. While these standards show promise and convey a potential need for enhancing TARA 1.0, they are still at early developing stages and their content cannot be exploited yet [322]. Thereupon, these facts motivate the present work in proposing enhancing avenues to TARA 1.0.

7.3.3 TARA 1.0

TARA 1.0 is a risk-based automotive testing approach which aims to identify threats, evaluate their impact and feasibility, and combine them to derive and prioritise the system risks [305]. In the literature as well as in standards, TARA is used as an acronym for multiple terms including a systematic testing approach, a method, a methodology or even a framework given its comprehensive nature in incorporating multiple methodologies [393]. In this paper, methodology and framework terms are used interchangeably while referring to TARA. Further clarification about TARA is essential, emphasising its distinction from HARA [214]. Albeit they both incorporate standardised RA principles, the former, from ISO/SAE 21434, addresses intended harm conducted by malicious attackers, whereas the latter, from ISO 26262, assesses accidental and hazardous harm [377]. Given the potential overlap of safety and security concepts in the CAV's domain, our research specifically focuses on TARA 1.0, centring on cybersecurity and data privacy concerns, yet with safety implications.

For a deeper understanding of the different steps of TARA 1.0, Figure 7.2 provides visual representation outlining the systematic procedures and flow evoked by ISO/SAE 21434. The main input to the TARA is the *item definition* step as it provides the context and the required understanding of the evaluated environment. TARA consists of two major phases which are *Threat modeling* and *Risk assessment* whose steps are: (i) asset identification; (ii) threat scenario identification; (iii) attack path analysis; (iv) impact rating; (v) attack feasibility rating; (vi) risk determination; and (vii) risk treatment decision. Finally, the *cybersecurity goals* and *cybersecurity claims* are considered as post-TARA steps as they support in refining the overall strategic cybersecurity

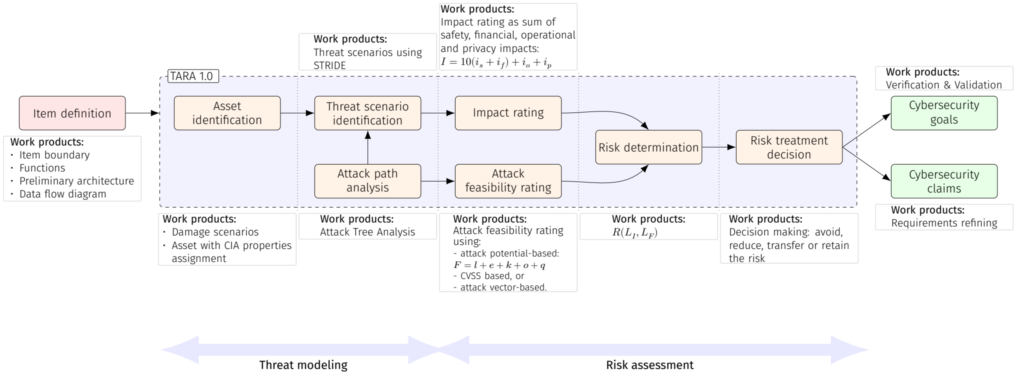


Figure 7.2: TARA 1.0 as defined by ISO/SAE 21434.

objectives.

Item definition

A clearly identified system architecture and functionalities facilitate the experts analysis throughout the assessment's process. The item definition consists of determining the item boundary, representing the extent of analysis for the asset under evaluation, and its related functionalities separately from the environment [233]. For an in-depth understanding of the item connections and different data exchanges with the other components, a generic architecture as well as a Data Flow Diagram (DFD) should be sketched to support assimilating the assessed environment.

Asset identification

This step aims to list the assets, representing valuable components or services for stakeholders as well as attractive targets for attackers [233], within the predefined item boundary (which is one of the outcomes from the prior step). Then damage scenarios are elicited for each identified asset showcasing the consequences in case each asset is compromised. Consequently, assets and damage scenarios are associated using the CIA model (embedding authorisation and authentication as subclasses of confidentiality) from ISO/IEC 27000 [203].

Threat scenario identification

Threat scenarios represent the key outcome of the threat modeling stage where every threat type is rigorously investigated with regard to the DFD's elements [438]. The threat scenario identification is accomplished by naming the action required to accomplish each damage scenario determined within the asset identification step. Albeit the ISO/SAE 21434 proclaims the efficiency of STRIDE as a taxonomy mnemonic-based technique, whose titles are mirroring threat classes, the standard remains open to similar tools, relevant misuse-case approaches [17] or any combination of both [233].

Attack path analysis

Attack Paths (APs) are elicited to indicate the sequence of events that an attacker can undertake to exploit threats identified from the previous step. The ISO/SAE 21434 propounded three approaches: (i) top-down where APs are deduced at the conceptual phase, from historical knowledge of vulnerabilities related to an item, and graphically represented through attack trees or attack graphs; (ii) bottom-up where APs are constructed from a pre-generated vulnerability analysis of an implemented item at a post-development stage; and (iii) a combination of both where supplementary analysis on vulnerabilities is jointed to the APs to actualise the threat scenario.

Impact rating

Table 7.2: Impact rating for each parameter safety(i_s), financial(i_f), operational(i_o) and privacy(i_p).

Impact	Negligible	Moderate	Major	Severe
Value	0	1	10	100

As defined in the standard, the impact rating represents an estimation of magnitude of damage conveying the severity associated to a damage scenario [233]. The standard computes the impact of each damage scenario, based on the sum of four parameters: safety(i_s), financial(i_f), operational(i_o) and privacy(i_p) whose values are assigned using a numerical scale (0, 1, 10, 100), depending on the severity (Negligible, Moderate, Major, Severe) [214], as set in Table 7.2, constructed according to ISO 26262 and ISO/SAE 21434. To determine the severity, the ISO/SAE 21434 came with a dedicated annex indicating the assignment criteria for each impact category. For instance, in the safety impact category, the severity is classified as “Negligible” if the damage would result in no injuries, whereas it is set to “Severe” if the damage would lead to fatal injuries. The impact rating in ISO/SAE 21434 as well as in most common TARA methodologies [201, 285, 143] is approached with an alignment to the ISO 26262 [214] Equation 7.1, where

$$I = 10(i_s + i_f) + i_o + i_p \tag{7.1}$$

each parameter is associated to an assigned weight that is set to 10 for safety and financial impacts and to 1 for operational and privacy impacts. According to the standard, this is justified with the criticality of safety and financial impacts over the other impacts. The derived I is mapped to determine the overall impact, per damage scenario, through the impact level L_I according to Table 7.3.

Attack feasibility rating

Every AP derived from the attack path analysis step incorporates information about the attacker, the attack surface and the attack method. To assess the attack feasibility, such information is leveraged as quantifiable parameters representing the attack likelihood.

Table 7.3: Impact rating

Impact sum (I)	**Impact level**(L_I)
0	🟢 0 - none
1-19	🟡 1 - Negligible
20-99	🟠 2 - Moderate
100-999	🔴 3 - Major
≥ 1000	⚫ 4 - Severe

The ISO/SAE 21434 advertised three attack feasibility approaches: (i) attack potential-based (as broken down in Section 7.4.5), (ii) CVSS based, and (iii) attack vector-based.

Despite the chosen method, an attack feasibility level (L_F) is derived. For instance, Table 7.4 illustrates how the aggregation is conducted following the attack potential-based method where an attack feasibility sum (F) is computed and mapped afterwards to L_F. Such aggregation is further demonstrated while proposing TARA 2.0 in the following sections.

Table 7.4: Attack feasibility rating

Attack feasibility sum (F)	**Feasibility level** (L_F)
≥10	🟢 0 - very low
7-9	🟡 1 - low
4-6	🟠 2 - medium
2-3	🔴 3 - high
0-1	⚫ 4 - critical

Risk determination

The risk value and level determination proposed by ISO/SAE 21434 combines the impact level (L_I), derived from the impact rating, and the feasibility level (L_F), derived from the feasibility rating, as follows:

$$R(L_I, L_F) \tag{7.2}$$

The levels and values are retrieved from Tables 7.3 and 7.4 respectively to construct the risk matrix. The ISO/SAE 21434 allows organisations the flexibility to define their own risk equation, which combines both impact and feasibility levels or values according to their specific needs. The standard advocates symmetric or asymmetric risk matrices [291] without mandating a specific risk matrix type. Table 7.5 depicts an example of an almost symmetric risk matrix that is compliant to ISO/SAE 21434 [285].

Risk treatment decision

After the APs identification, the risk compilation and threats prioritisation, a risk treatment decision needs to be taken to determine if the risk can be: (i) reduced (through the implementation of further security or privacy controls), (ii) accepted (by

Table 7.5: A sample 2D risk matrix

		L_I			
		Negligible	Moderate	Major	Severe
L_F	Low	1	1	2	3
	Medium	1	2	3	4
	High	2	3	4	5
	Critical	2	4	5	5

managing the risk without additional measures), (iii) shared (when the risk is delegated to a third party like insurance, and (iv) avoided (by stopping the risk from its source like when the entire activity is omitted). Despite the decision that can be taken, it is crucial that all the CAV stakeholders, including OEM and mobility service providers, get involved in the treatment decision process as associated technological, operational or financial costs may apply. Additionally, the risk should remain monitored and considered within any TARA reiteration or vulnerability management throughout the CAV life-cycle [233].

Cybersecurity goals and claims

Cybersecurity goals and claims rely on the outcome of the entire TARA process. While the risk treatment decision relies on selecting and implementing mitigation solutions for the risks identified from the TARA, cybersecurity goals and claims steps consist of verifying and validating proper treatment of the threat scenarios and APs.

7.4 TARA 2.0

The present section sets the groundwork for TARA 2.0 by outlining the methodology used throughout the assessment process. The section discusses also the motivation and the reasoning behind each enhancement proposed on the top of TARA 1.0.

7.4.1 Methodology

The aim of the present work is to provide a holistic threat modeling which incorporates the intertwined cybersecurity and privacy threats as well as a granular and objective risk assessment leading to appropriate risk prioritisation for L4 & L5 CAVs. Our methodology was built based on the analytics and experimental findings upon TARA 1.0 limitations. First, originating from systematic review of Benyahya et al. [40] on TARA frameworks applicable to CAV's environments, we established TARA 1.0 as the most prominent approach to assess CAVs vulnerabilities. However, an appropriate adaptation to tackle the SAE L4 and L5 CAVs' specifications including privacy threats and automation level implications is required. The same review asserted that TARA 1.0 outcomes rely on experts' opinion, prone to the assessment's subjectivity. To overcome such pitfalls, every step from TARA 1.0 has been evaluated and experimented as a baseline assessment [43]. The results showcased that:

1. At the asset identification and the threat scenario identification steps, mainly cybersecurity threat classes are modeled while privacy threat classes are barely assessed.
2. The privacy impact is underestimated as it has lower weights compared to safety and financial impacts as depicted in Equation 7.1.
3. The automation level does not take part at any step of the risk assessment process.
4. 6 out of 7 TARA 1.0 steps depend on experts opinion (as notated by symbol ⋆ in Figure 7.3). Consequently, transparent communication about the level of the experts involvement at various steps, is required to measure the assessment's results subjectivity.

To that end, we claim that if we provide a comprehensive assessment of privacy threats at the threat modeling phase; propose an agile weight to the privacy impact depending on the nature of the data; consider the automation level as one of the RA metrics; and quantify the experts' objectivity then the overall assessment will be improved to address L4 & L5 specifications.

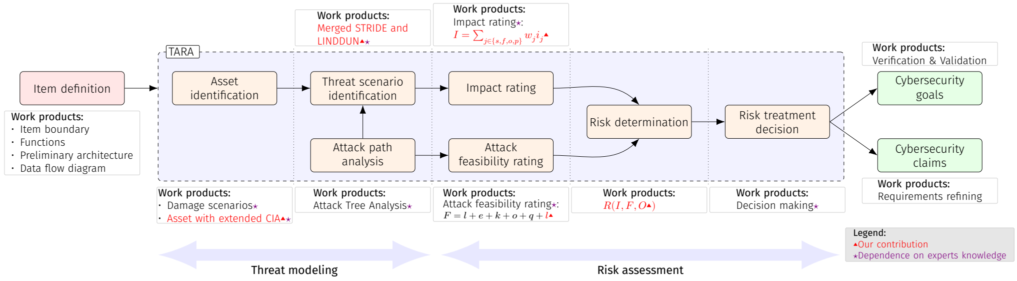


Figure 7.3: TARA 2.0 improvement avenues.

Our contribution, highlighted in red and marked with ▲ within Figure 7.3, consists of integrating improvements to several steps of TARA 1.0. At the asset identification step (7.4.2), privacy and security goals are consolidated, to extend the CIA model, for an in-depth identification of damage scenarios. At the threat scenario identification (7.4.3), the threat modeling is more extensive by considering eleven threat classes as an outcome of fusing STRIDE and LINDDUN techniques instead of limiting the analysis just to STRIDE classes. Both security and privacy threat modeling analysis were supported by the findings from previous research works [41, 44]. The impact rating is improved by expanding the privacy impact assessment through the integration of a weight representing data sensitivity and Privacy Enhancing Technologiess (PETs) solutions in place (7.4.4). The attack feasibility rating step is enhanced by incorporating the SAE automation level (7.4.5). The inclusion of the experts' objectivity index elevates further the risk determination milestone to consider any subjective influences that experts may have on the risk assessment process(7.4.6).

It is noteworthy to mention that the provided improvements are applicable only to some of the core steps of the TARA process while the input and output steps of the TARA, represented through the item definition, cybersecurity goals and claims respectively, are not in the scope of our enhancements proposal.

7.4.2 Asset identification

Guided by the privacy risks within the CAV ecosystem and the GDPR data processing principles [424], we extend further the CIA model by incorporating three privacy protection goals which are unlinkability (U), accountability (Ac) and compliance (Com). The selection of these additional goals resulted from an analysis of the privacy goals listed within ISO/IEC 27000 [203] and the privacy and data protection by design principles from ENISA [103, 153]. Unlinkability is compromised when privacy-related data can lead to identify the data owner. Accountability is a privacy goal, that is intertwined with transparency and non-repudiation concepts, where the originated entities of a claimed action or event can be proven [30]. Compliance indicates the appropriate integration of relevant privacy policies such as the GDPR. To that end, joining privacy goals to the CIA model is perceived as building blocks towards constructing both security and privacy threat modeling in the following steps of the TARA as showcased in Section 7.5.3.

7.4.3 Threat scenario identification

A holistic threat modeling for health data context was successfully demonstrated by Treacy, Loane and McCaffery [427]. We apply the same principles in TARA 2.0 by combining STRIDE [329], for its automated functionality in instantiating security threats, and LINDDUN, for its pertinence to privacy threats [76, 460], as detailed in Appendix 7.8. Table 7.6 depicts in detail full list of advantages and disadvantages of each method, which served as a decision criteria. The consolidation of both approaches led to a categorisation of eleven threat classes where repudiation/ non-repudiation and information disclosure/ disclosure of information classes are merged respectively.

Table 7.6: STRIDE vs LINDDUN

STRIDE	**LINDDUN**
(+) can be implemented using automated tools.	(-) requires manual treatment.
(+) is dedicated to modelling security threats.	(+) is dedicated to modeling data privacy threats.
(+) focuses on software and network based security with IoT extension.	(+) is applicable to all software systems.
(-) relies on an error free DFD and architecture.	(-) relies on experts knowledge and predefined assumptions.

Then, every threat scenario is mapped to one or several threat classes. Every intersection between a threat class, which can be one of the categories of STRIDE or LINDDUN classes, and the threat scenario is further developed and sketched through the attack path analysis. It is important to highlight that the attack path analysis step is not concerned with the proposed improvements in TARA 2.0 which justifies the transition of the discussion to the impact rating step directly.

7.4.4 Impact rating

Shifting from threat modeling to risk assessment phase, this subsection introduces how the impact rating is computed within TARA 2.0, as one of the core outcomes leading to the risk determination step (Section 7.4.6). The ISO/SAE 21434 proposes an impact rating per damage scenario. Therefore, as soon as damage scenarios are defined, the impact can be computed. In contrary to the standard, the present work puts forth an impact rating per AP, which occurs after accomplishing both the threat scenario identification and attack path analysis steps. By conducting granular analysis which considers the specifics associated to each AP, such as data types, a fine-grained risk determination can be also performed afterwards per AP. This approach differs from TARA 1.0 where risk determination is based on damage scenarios. The detailed examination allows also for targeted mitigation strategies to be determined for each individual AP instead of being derived per damage scenario. Considering the one-to-many relationship between damage scenarios, threat scenarios and APs in Figure 7.4, eliciting decisions per damage scenarios mirror a more generalised assessment while an assessment per AP provides more granularity. Additionally, assessing the risk for individual APs allows fewer aggregations at both impact rating and attack feasibility rating phases. Therefore, we believe that each defined AP from the previous step has a potential impact which is joined in the upcoming step to the feasibility rating for the risk compilation.

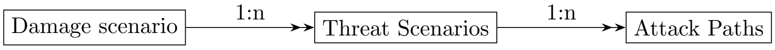


Figure 7.4: Relationship between damage scenario, threat scenarios, and APs.

Considering that TARA 1.0 follows the ISO 26262 impact rating where the privacy impact is underestimated as introduced in Section 7.3.3, we suggest to put a stronger emphasis on the privacy due to the rich data exchanges within the CAV's ecosystem. Consequently, TARA 2.0 advocates a weighted impact rating, as in [116] and in Equation 7.3, where every impact category is joined to a specific weight which is assigned depending on each context. While in Equation 7.1 safety weight w_s and w_f are fixed to ten and w_o and w_p are set to one, we propose for each impact weight to remain agile, and getting any value from the range [0, 10] (Equation 7.3).

$$I = \sum_{j \in \{s,f,o,p\}} w_j i_j \tag{7.3}$$

While focusing on the i_p and w_p, we extend the ISO/IEC 29100 [240], which elicited the privacy rating for privacy damage as referred in the ISO/SAE 21434 appendix, to bring forth a granular privacy impact assessment addressing three factors: data sensitivity, linkability to PII and the PET solutions implemented in place. As defined in Table 7.7, we established data sensitivity levels to be: highly sensitive, medium and not sensitive just as the ISO/IEC 29100 [240] classification. Similarly, the linkability to PII is scaled as easy or difficult to link. The PET factor, determining the presence of methods such as anonymisation and pseudonymisation [44, 283], is classified into: none, partial or strong implementation. The i_p and w_p are generated afterwards depending on the combination, of the three privacy factors, which are appropriate to the assessed context. The derived i_p and w_p are aggregated to the other impacts i_s, i_f and i_o with their relevant weights (w_s, w_f and w_o) which are assigned based on gathered consensus from stakeholder and panel of experts [197]. To that end, Equation 7.3 determines the overall impact (I) from which the impact level is derived, if required, according to Table 7.3.

Table 7.7: TARA 2.0 privacy impact scoring

Level	**Privacy factors**			**Privacy impact (i_p)**	**Weight (w_p)**
	Sensitivity	Linkability to PII	PET		
Severe	Highly sensitive	Easy to link	None	100	10
	Highly sensitive	Easy to link	Partial	100	9
	Highly sensitive	Easy to link	Strong	100	8
Major	Highly sensitive	Difficult to link	None	10	9
	Medium	Easy to link	None	10	8
	Highly sensitive	Difficult to link	Partial	10	7
	Medium	Easy to link	Partial	10	6
	Highly sensitive	Difficult to link	Strong	10	5
	Medium	Easy to link	Strong	10	5
Moderate	Medium	Difficult to link	None	1	5
	Not sensitive	Easy to link	None	1	4
	Medium	Difficult to link	Partial	1	3
	Not sensitive	Easy to link	Partial	1	2
	Medium	Difficult to link	Strong	1	2
	Not sensitive	Easy to link	Strong	1	1
Negligible	Not sensitive	Difficult to link	None	0	1
	Not sensitive	Difficult to link	Partial	0	1
	Not sensitive	Difficult to link	Strong	0	0

7.4.5 Attack feasibility rating

For the purpose of our study, we adopt the attack potential-based approach since it is a standardised one from ISO/IEC 18045 [224] and it considers the capabilities and intentions of potential attackers while the two approaches, CVSS based and attack vector-based, remain limited to software and network vulnerabilities.

The attack potential-based approach captures factors leading to a successful attack [233] which are: (i) Elapsed time (t) indicating the exploited time to run an attack in months or years; (ii) Specialised expertise (e) determining the attacker capabilities and if the attack is conducted by an individual or a group of attackers. It is categorised into layman, proficient, expert and multiple experts; (iii) Knowledge of the item/ component (k) evaluating the amount of information that an attacker has about the assessed item or component and which can be defined as: public, restricted, confidential or strictly confidential; (iv) Windows of opportunity (o) defining the target accessibility type and duration which can be unlimited, easy, moderate or difficult according to the ISO/SAE 21434 categorisation [233] ; and (v) Equipment (q) indicating the tool properties supporting the attack execution and which can be standard, specialised, bespoke (representing an equipment that is not readily available to the public for being very expensive or restricted to the market) [233] or multiple bespoke.

We extend further these factors by including the CAV automation level (SAE Lx (l)) as an additional constituent impacting the attack feasibility rating as depicted in

Table 7.8: TARA 2.0 feasibility rating

Elapsed time (t)	**Specialised expertise (e)**	**Knowledge of the item/ component (k)**	**Windows of opportunity (o)**	**Equipment (q)**	**SAE Lx (l)**	**Assigned value**
$\leq$ 1 month	Layman	Public	Unlimited	Standard	L5	0
$\leq$ 6 months	Proficient	Restricted	Easy	Specialised	L4 ⋆	1
$\leq$ 3 years	Expert	Confidential	Moderate	Bespoke	L4 ⋆⋆	2
$\geq$ 3 years	Multiple	Strictly confidential	Difficult	Multiple bespoke	L3	3

⋆: Remote operator; ⋆⋆: In-vehicle operator

Table 7.8. The l in this context considers the human factor, which can be either an in-vehicle driver or a remote operator, in reducing the associated risk. With this notion, the attack feasibility encompasses the transition between human and machine, exploring how this transition is likely to influence a successful attack.

Each factor in Table 7.8 has four possibilities which are associated to numerical values varying from zero to three. The smaller the value, the more likely the attack is to occur. The proposed attack feasibility rating is aligned to the ISO/IEC 18045 and ISO/SAE 21434, but uses a light-weighted numerical scaling (from 0 to 3) as in [285] unlike the larger scale (from 0 to 19) proposed in the standard [224]. For every perceived AP, the attack feasibility (F) is computed by summing up the scaled values for every parameter as in Equation 7.4:

$$F = t + e + k + o + q + l \tag{7.4}$$

Where: t = elapsed time
e = specialized expertise
k = knowledge of item
o = windows of opportunity
q = equipment
l = automation level

Thereupon, Table 7.4 value's is scaled to the inclusion of the automation level metric to allow a correct elicitation of the five feasibility levels from the new attack feasibility sum F. An interpolation is used for a linear transformation to reflect the change of F's composition. Table 7.9 depicts how the relationship between F and L_F is preserved through the new scaling which differs from Table 7.4 on the boundaries of medium, low and very low L_F. While the Table proposes the new mapping, it is noteworthy to mention that for the purpose of this research, TARA 2.0 exploits mainly F without compiling the L_F for the risk determination and visualisation discussed in the following subsection. Such decision is adopted as the F provides the needed granular value to construct the 3-D plot (Section7.5.8). Consequently, Table 7.9 is incorporated to the present work just to support any further replication aiming a classical risk matrix with the use of L_F.

7.4.6 Risk determination

In addition to the impact sum I and the attack feasibility sum F, TARA 2.0 extends further the risk determination by incorporating a third metric O, referred to as the experts'

Table 7.9: The scaled attack feasibility rating upon the inclusion of the SAE Lx metric

Attack feasibility sum (F)	**Feasibility level** (L_F)
≥12	🟢 0 - very low
8-10	🟡 1 - low
4-7	🟠 2 - medium
2-3	🔴 3 - high
0-1	⚫ 4 - critical

objectivity index:

$$R(I,F,O) \tag{7.5}$$

The experts' objectivity index (O) takes into account the experts' subjectivity while making assumptions throughout the TARA process. Following the experts' knowledge elicitation principle [354], commonly used in the statistics domain, along with the ISO/IEC 17065 requirements on impartiality [223], the O index compiles four factors AP: (i) c: certainty (representing the experts' confidence); (ii) r: peer review (determining if the analysis is conducted by one experts' group or several groups); (iii) t: measurable tools (indicating the usage of measurable metrics or automation tools); and (iv) p: impartiality (demonstrating if experts may provide any unfair or biased inputs due to their affiliations). A rate from the [0,1] interval is assigned by the experts to each factor where values close to 1 represent higher confidence and hence objective opinion while values close to 0 illustrate low confidence and hence subjective opinion. A mean value, representing the objectivity index O, of the four factors is computed as follows:

$$\bar{O} = \frac{\sum(c,r,t,p)}{n} \tag{7.6}$$

Where: c = certainty

r = peer review

t = measurable tools

p = impartiality

n = total number of factors over which the mean is computed.

The risk matrix combines the three values (I, F, O), using a three-dimensional plot where the x-axis represents the experts' objectivity index (O), the y-axis depicts the attack feasibility sum (F) and finally, the z-axis draws the impact sum (I) as demonstrated in Figure 7.8. Such visualisation simplifies the process of risk prioritisation where the tallest dots with the smallest y values and the highest x values indicate most potential APs or threats to mitigate first.

Similar to the attack path analysis step, no additional enhancements have been introduced at the risk treatment decision step, justifying its omission in this section. Though, it is noteworthy to spotlight that TARA 2.0 adheres to the same requirements as TARA 1.0 for the risk treatment decision step.

7.5 Proof of concept (PoC)

This section demonstrates TARA 2.0's usage through illustrative example of its applicability over the ADS as a PoC. Following the proposed methodology, our demonstration considers the real context of the ULTIMO[3] project [89] where L4 CAVs are designated for people and goods transportation as an integral solution for public transport systems. To that extent, our PoC consists of executing TARA 2.0 at the design stage, over a reference architecture envisioned to fulfil the ULTIMO project objectives.

7.5.1 Materials and tools

There exist several commercial tools that can be considered to conduct an automotive TARA implementation like Upstream [434], C2A [61], Cymotive [101] and VectorCast [440]. Though, such solutions remain constrained to some steps of the TARA process without covering the entire workflow. They are also more oriented to safety testing and software vulnerability than thorough cybersecurity and data privacy assessments. To accomplish our PoC, we rely on a selection of specific tools providing the ability to conduct an assessment from the outset and to showcase the proposed enhancements over a classical TARA. The following list depicts a breakdown of the used tools:

- Google sheet and MS Excel scripts: used as an inventory tool (for damage and threat scenarios elicitation) as well as for risk calculation and prioritisation.
- Microsoft Threat Modeling Tool (TMT7): used to build DFDs and derive STRIDE threat scenarios.
- LINDDUN documentation [460, 459, 403]: used to elaborate LINDDUN threat scenarios and their related ATA.

The remainder of this section describes the outcome of every TARA 2.0 step.

7.5.2 Item definition

As depicted in Figure 7.3, the item definition step is the starting point of any TARA process. According to the ISO/SAE 21434 recommendations, the following work products are determined at that step:

1. Item boundary: the ADS processing unit.
2. Functions: the ADS is intended to derive efficient autonomous motion decision by merging and cross-checking data from all sensors. A sample inputs for the ADS processing unit can be the captured image from the camera's ECU, the collision avoidance decision from the RADAR, the obstacle detection from LiDAR and all other data flows from different other ECUs. The output of the ADS is the decision on vehicle motion wrapping up localisation status, object detection and path planning. Furthermore, the ADS decides on when doors can

[3] The ULTIMO project (https://doi.org/10.3030/101077587) is co-funded by the European Union and the Swiss State Secretariat for Education, Research and Innovation (SERI) under the Horizon program.

be opened or closed, and also when to let the manual or remote driving to take over.

3. **Preliminary architecture**: Figure 7.5 depicts a generic architecture considered for the L4 CAV. The architecture wraps up the different buses (CAN or Ethernet) as well as ECUs to which the ADS processing unit is connected. The architecture shows also the different external connections including internet (4G/WiFi) and GNSS/GPS. The figure highlights the crucial connection to the manual control unit which is triggered once the human intervention (in-vehicle or remote) is required.

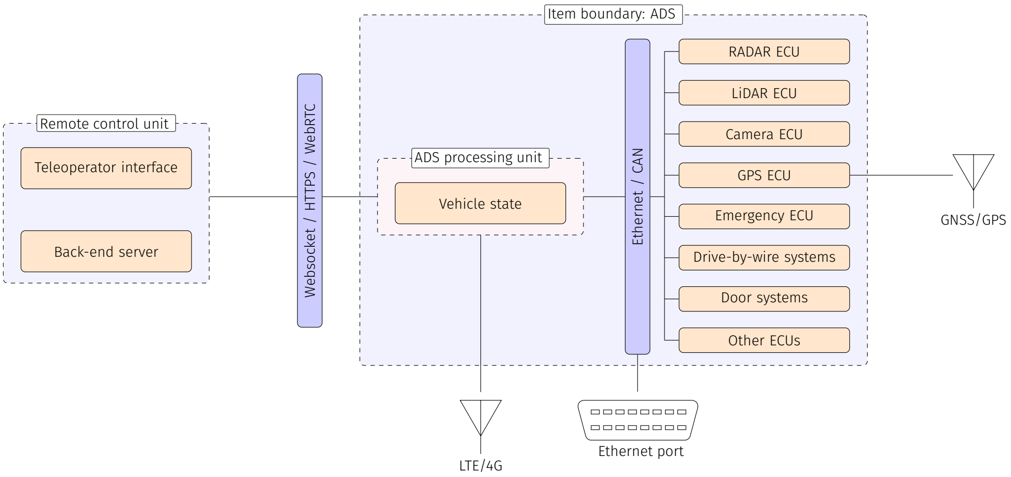


Figure 7.5: Preliminary SAE L4 architecture considered for TARA 2.0.

4. **Data Flow Diagram**: Figure 7.6 describes the different data flows exchanged with the ADS processing unit. Each data flow is represented with a one way arrow while processes are depicted on a circle design. Devices and data stores are drawn using two parallel horizontal lines. The interactors that can be either a passenger, developer, maintenance user, service customer or a third party user are depicted in a rectangular shape. The trust boundary, where trust flows occur without the use of encrypted connections to the ADS, are drawn using red dotted rectangle. Further, interfaces such as vehicle user interface and internet are represented using a dotted line boundary. The DFD was elaborated using TMT7 tool and with an alignment to the software standards symbols [329]. The sketched DFD is built using the automotive template [324]. The drawn DFD is commonly the main input to start both STRIDE and LINDDUN analysis in the upcoming steps.

7.5.3 Asset identification

The required work product for the asset identification consists of the identification of assets, their association to cybersecurity properties and their mapping to damage scenarios. Based on the system architecture and the assets derived from the DFD diagram, Table 7.10 lists a sample from the 14 valuable assets within the ADS boundary which can be a safety-critical function (like A.1) or a data set (A.14). For

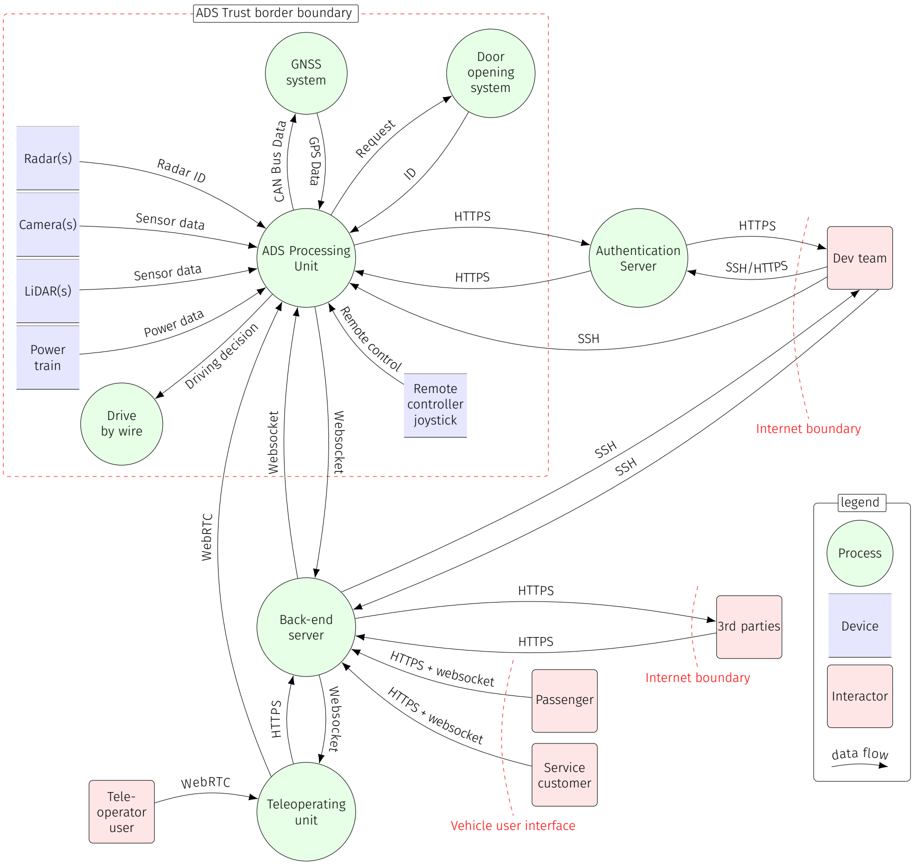


Figure 7.6: ADS data flow diagram.

every asset, damage scenarios are defined, where multiple damage scenarios can be related to a single asset. For instance, damage scenarios: D.1, D.2, D.3 relate all to A.1. As introduced in Section 7.4.2, the table leverages the CIA model further by mapping the assets to additional privacy goals: unlinkability (U), accountability (Ac) and compliance (Com). To illustrate, compromising the GNSS processing (A.1) does not only impact the CAV's integrity and availability but it affects the unlinkability privacy goal if the vehicle location data can be linked to end-users' sensitive data leading to a privacy-related damage scenario (D.3).

Table 7.10: TARA 2.0 asset identification

Asset #	**Asset description**	**Cybersecurity properties**						**Damage #**	**Damage Scenario**
		C	I	A	*U*	*Ac*	*Com*		
A.1	GNSS capturing and processing		x	x	x	x		D.1 D.2 D.3	Compromising GNSS signal Lost of GNSS signal Unauthorised location tracking
A.2	Image capturing and processing	x	x		x		x	D.4 D.5 D.6	Blinded vision Presume non-existent obstacles Unauthorised facial image capturing
A.3	Object recognition		x	x			x	D.7 D.8 D.9	Fail in detecting objects Non recognition of traffic signs Contradictory inputs from sensors where one is detecting an obstacle and the others are assessing a clear path
...	...			...				...	...
A.14	Passenger data	x		x	x	x	x	D.25 D.26 D.27	Disclosure of personal data without the user's consent PII de-anonymisation Malicious data manipulation

7.5.4 Threat scenario identification

For a holistic threat modeling, we run an automated interaction-based STRIDE using TMT7 and combine its findings to the element-centric analysis from LINDDUN.

On the one hand, 550 threats were reported from the TMT7 which are defined using an ID, a description and a categorisation through the STRIDE threat classes. For our analysis, the report is exported to a comma-separated values (CSV) file where the threats' list is filtered to remove redundant entries and is grouped per asset to match the predefined damage scenarios. The filtering criteria consists of omitting threats which: (i) are duplicated for the two ways (in/out) of data flows between the same components; and (ii) can be adequately mitigated through existing security controls. The threats synthesising and grouping led to 40 threats scenarios as sampled in Table 7.12.

On the other hand, as in LINDDUN threats must be determined by the type of DFD elements, every retained threat, from the 40 threat scenarios, is then extended with an explicit linking to the DFD elements to define the privacy threat class related to it . Following [459], we constructed a template (Table 7.11) suggesting which threat class, from LINDDUN categories, is relevant to each DFD element based on data types descriptions provided with the system architecture. Hence, every threat scenario is mapped to both security and privacy threat classes at the end of that process.

Table 7.11: Mapping LINDDUN threats to DFD elements

DFD element	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Data flow	x	x	x	x	x		x
Process			x	x			x
Entity	x	x				x	

In a nutshell, Table 7.12 illustrates the mapping between damage scenarios and the eleven threat classes, as a combination of the STRIDE and LINDDUN results. Every x in the table implies that the corresponding threat scenario is susceptible to the selected threat classes. Additionally, each x represents an interaction that needs to be elevated in the form of an ATA. The interactions annotated with ⓧ are selected to be showcased in the following subsection. For instance, a spoofing scenario was chosen as a well documented cybersecurity threat [265] and a linkability scenario is selected for being a prominent privacy threat in the CAV landscape [76].

Table 7.12: TARA 2.0's threat scenario identification illustration using STRIDE and LINDDUN.

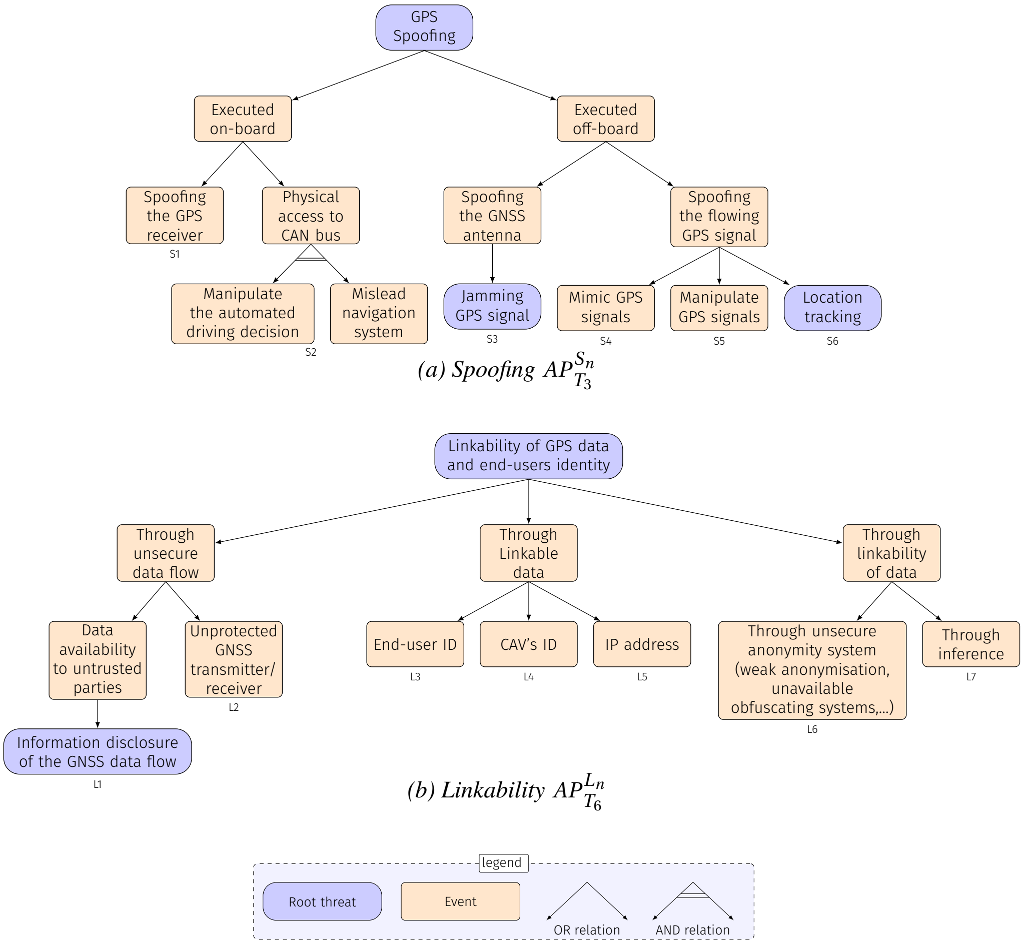
				Threat classes										
Damage #	**Threat #**	**Threat scenario**	**DFD element**	S	T	R	I	D	E	L	I'	D'	U	N
						N†	*D*††							
D.1	T.1	Compromise the GNSS in order to deliver malicious updates	Data flow			x	x		x	x	x	x		x
	T.2	Flood GNSS with invalid data	Data flow			x	x	x		x	x	x		x
	T.3	Spoof GPS signals and deliver malicious GPS data or to manipulate the vehicle	Data flow	ⓧ		x	x			x	x	x		x
D.2	T.4	Take the GNSS offline	Process			x		x			x	x		x
	T.5	Jam the GPS signal being received by the vehicle causing a DoS on the GPS antenna	Data flow			x	x	x		x	x	x		x
D.3	T.6	An attacker relating the CAV location to the end-user identity to conduct an unauthorised location tracking	Entity				x			ⓧ	x		x	
...								flow						
D.27	T.40	Malicious data manipulation through tampering data in transit sent to the ADS	Data flow		x	x	x			x	x			x

†: merged **R**epudiation and **N**on repudiation
††: merged **I**nformation disclosure and **D**isclosure of information
X: an interaction showing a mapped threat scenario to a threat class.
Ⓧ: a demonstrated interaction in Figure 7.7 and Table 7.13.

7.5.5 Attack path analysis

For the purpose of the present work, the top-down approach is selected through ATA (Section 7.3.3). To maintain simplicity, attack trees are adopted over attack graphs as the former are easier to understand and depict simple event flows showcasing the different ways an attacker can follow to achieve the attack, while the latter is more resource-intensive and involves the interconnected relationship between vulnerabilities which is more appropriate for highly complex systems [276].

ATA helps in identifying the significance of a threat to the system. By considering the eleven threat classes, every threat class per threat scenario should generate several attack paths leading to the threat execution. Such attack tree elicitation is conducted based on knowledge of the system architecture from the item definition step, the list of threats in the UNECE R155 annex [430], known CVEs [343] relevant to CAVs and attacks taxonomies [407, 412]. For simplicity purposes, we scrutinise a spoofing interaction demonstrating a security threat (T.3) and a linkability interaction illustrating a privacy threat (T.6) as depicted in Figure 7.7a and 7.7b respectively. Consequently, every path from the parent to the child node indicates a valid attack path where AND relation yields to one AP (as exemplified by our unique AND case in $AP_{T_3}^{S_2}$) while the OR relation produces distinct APs. For instance, the spoofing tree generates six attack paths starting from $AP_{T_3}^{S_1}$ to $AP_{T_3}^{S_6}$ and the linkability tree demonstrates seven attack paths from $AP_{T_6}^{L_1}$ to $AP_{T_6}^{L_7}$. The upper script on AP designates the threat class combined to the AP number within the evaluated threat scenario while the lower script designates the threat scenario ID. To illustrate, the S_1 in $AP_{T_3}^{S_1}$ refers to the first AP of spoofing as a threat class related to the third threat scenario T_3.


GPS Spoofing
Executed on-board
Executed off-board
Spoofing the GPS receiver
S1
Physical access to CAN bus
Spoofing the GNSS antenna
Spoofing the flowing GPS signal
Manipulate the automated driving decision
Mislead navigation system
S2
Jamming GPS signal
S3
Mimic GPS signals
S4
Manipulate GPS signals
S5
Location tracking
S6
Linkability of GPS data and end-users identity
Through unsecure data flow
Through Linkable data
Through linkability of data
Data availability to untrusted parties
Unprotected GNSS transmitter/ receiver
L2
End-user ID
L3
CAV's ID
L4
IP address
L5
Through unsecure anonymity system (weak anonymisation, unavailable obfuscating systems,...)
L6
Through inference
L7
Information disclosure of the GNSS data flow
L1
legend
Root threat
Event
OR relation
AND relation

(a) Spoofing $AP_{T_3}^{S_n}$

(b) Linkability $AP_{T_6}^{L_n}$

Figure 7.7: Spoofing and linkability attack trees

7.5.6 Impact rating

Table 7.13 illustrates how the impact value is calculated for the two selected APs: $AP_{T_3}^{S_2}$ and $AP_{T_6}^{L_3}$ using Equation 7.3. First, the value is defined for safety(i_s), financial(i_f) and operational(i_o) factors using the rates proposed in Table 7.2 mirroring the experts assessment (Negligible, Moderate, Major or Severe). Second, the weights are distributed by the experts respectively with regard to the impact factor importance to the AP. For instance, the operational weight (w_o) is at its highest value (10) for $AP_{T_3}^{S_2}$ in case an attacker is spoofing the GNSS data directly from the CAN bus compromising the ADS integrity and its well functioning. However, w_o has a lower weight of 1 in $AP_{T_6}^{L_3}$ as the compromise of the unlikability property does not immediately impact the vehicle route. Regarding the privacy, both impact (i_p) and weight (w_p) are retrieved using Table 7.7 based on the assessed combination of privacy factors. By summing up all the impacts, the I leads to the impact level (L_I) identification according to Table 7.3.

While Table 7.13 depicts the impact rating for both selected APs, we discuss here the impact rating performance for $AP_{T_6}^{L_3}$ in comparison to TARA 1.0. TARA 2.0 leads to an amber Moderate impact of level 3 for $AP_{T_6}^{L_3}$. However, by following TARA 1.0 impact calculation in Equation 7.1, the I would be equal to 10=10x(0+0)+0+10 (assuming a Negligible i_s, i_f and i_o with a Major i_p) resulting into a yellow Negligible L_I of level 1 (according to Table 7.3) discriminating the privacy importance in such attack path. To that end, our example illustrates how an appropriate privacy impact and weight can change the entire impact rating outcome.

7.5.7 Attack feasibility rating

Following the attack potential-based approach [235], and with the purpose to address the SAE automation level within the assessment, TARA 2.0 proposes a simplified attack feasibility rating which wraps up the SAE Lx (l) as an additional metric with an alignment to Table 7.8. By applying equation 7.4 to every defined AP, every metric from the equation is enumerated based on the background knowledge of the CAV environment as depicted in Table 7.13 for the two selected APs.

Our findings demonstrate that the success of an attack depends not only on the attacker knowledge, expertise and equipment but also on the presence and reactivity of a supervising operator (who can be in or out the vehicle). Such information is conveyed through the o and l values which are correlated especially for attacks that can be executed on-board. Such human intervention has a direct impact on L_F which can turn into high instead of medium if the same attack is conducted over an L5 rather than an L4 CAV for the case of $AP_{T_3}^{S_2}$.

7.5.8 Risk determination

TARA 2.0 risk determination relies on three parameters: the impact sum (I), the attack feasibility sum (F) and the experts objectivity index (O).

The compilation of O is demonstrated for the two selected APs in Table 7.13 where the experts' subjectivity is assessed through the four predefined metrics: certainty (c), peer review (r), measurable tools (t) and impartiality (p). Different c and t values were compiled impacting the O scores of the two APs. Such variation is caused by the usage

Table 7.13: TARA 2.0 analyses on two illustrated attack paths

Damage scenario	D.1 Compromising GNSS signal.	D.3 Unauthorised location tracking.
Threat scenario	T.3 Spoof GPS signals and deliver malicious GPS data or to manipulate the vehicle.	T.6 An attacker relating the CAV location to the en-user identity to conduct a unauthorised location tracking.
Attack path	$AP^{S_2}_{T_3}$ Physically connecting to the vehicle to access the CAN bus to manipulate the automated driving function and mislead the navigation system compromising the CAV integrity and availability.	$AP^{L_3}_{T_6}$ Linking GPS data and end-users identity through linkable end-user ID.
Impact	$w_s = 10$, $i_s = 10$ (Major) $w_f = 5$, $i_f = 10$ (Major) $w_o = 10$, $i_o = 10$(Major) $w_p = 9$, $i_p = 10$ (highly sensitive/difficult to link/none) $I = \sum_{j \in \{s,f,o,p\}} w_j i_j = 340$ $L_I =$ 🔴 3 - Major	$w_s = 5$, $i_s = 0$ (Negligible) $w_f = 1$, $i_f = 0$ (Negligible) $w_o = 1$, $i_o = 0$ (Negligible) $w_p = 9$, $i_p = 10$ (highly sensitive/difficult to link/none) $I = \sum_{j \in \{s,f,o,p\}} w_j i_j = 90$ $L_I =$ 🟠 2 - Moderate
Attack feasibility	$t = 0$ (≤1 month) $e = 1$ (proficient) $k = 0$ (public) $o = 2$ (moderate) $q = 0$ (standard) $l = 2$ (L4**) $F = t + e + k + o + q + l = 5$ $L_F =$ 🟠 2 - medium	$t = 1$ (≤6 months) $e = 2$ (expert) $k = 1$ (restricted) $o = 2$ (moderate) $q = 0$ (standard) $l = 2$ (L4**) $F = t + e + k + o + q + l = 8$ $L_F =$ 🟡 1 - low
Objectivity index O	Certainty $(c) = 1$ Peer review$(r) = 1$ Measurable tools$(t) = 0.75$ Impartiality $(p) = 0.5$ Mean $\bar{O} = \frac{\sum(c,r,t,p)}{n} = \frac{1+1+0.75+0.5}{4} = 0.81$	Certainty (c)= 0.5 Peer review$(r) = 1$ Measurable tools$(t) = 0.25$ Impartiality $(p) = 0.5$ Mean $\bar{O} = \frac{\sum(c,r,t,p)}{n} = \frac{0.5+1+0.25+0.5}{4} = 0.56$
Risk treatment	Encrypt the CAN bus flow. Implement authentication with certificates among all ECUs. Consider GPS corrector from NTRIP service providers [365].	Mask end-users' ID using differential privacy. Encrypt GPS data using zero-knowledge proofs.

of the automated tool STRIDE for the $AP^{S_2}_{T_3}$ while $AP^{L_3}_{T_6}$ was elicited manually using LINDDUN. Similarly, higher certainty value is assigned to GPS spoofing than linkability threat as the former attack is well reported and simulated within the cybersecurity community [430, 265, 43]. The r and p values are identical for both APs where r value is assessed to be 1 as multiple experts participated in the analysis while p got a score of 0.5 as the involved experts consisted of OEMs, whose expertise may impact the provided opinion.

As discussed in Section 7.4.6, and by acknowledging the limitation of 2-D matrices [291] for providing aggregated risks and not clearly asserting the priorities, the risk is determined in TARA 2.0 using a three dimensional plot as drawn in Figure 7.8. The graph compiles the rates for all APs derived from T.3 and T.6.

Furthermore, it reveals, with high confidence, that $AP^{S_3}_{T_3}$ (for its node's height) and $AP^{S_2}_{T_3}$ (for its F proximity to 0) are the most critical attacks requiring mitigation efforts.

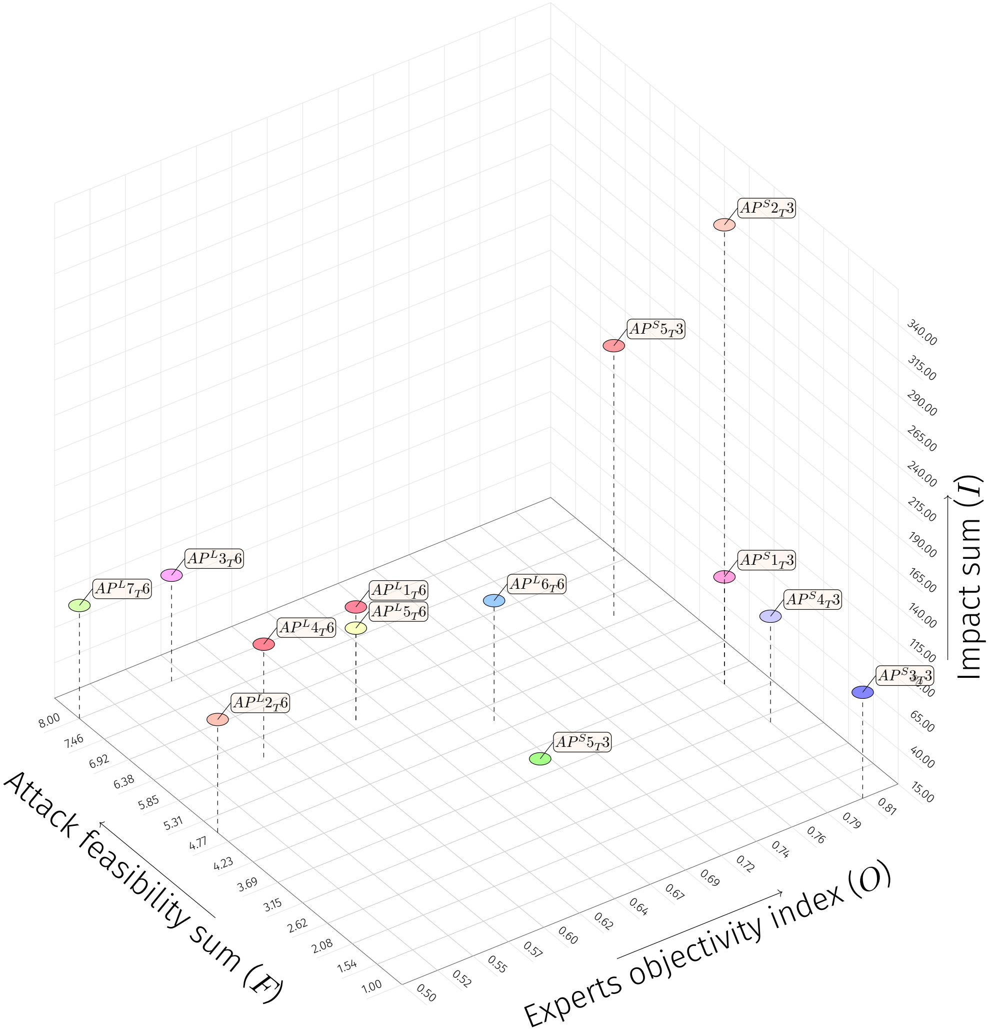


Figure 7.8: 3D risk visualisation from TARA 2.0.

7.5.9 Risk treatment decision

Based on LINDDUN supporting documentation mapping privacy threats to PET, and according to the UNECE appendix on cybersecurity best practices, we advocate robust encryption and redundancy for the GPS data flows while anonymisation solutions are recommended for data flows incorporating end-users IDs.

7.6 Discussions and future work

This section provides a comprehensive summary of our findings. We present a dedicated analysis for each RQ, compare TARA 1.0 and TARA 2.0, and acknowledge the limitations of our research. Additionally, we offer insights into future research efforts and directions.

7.6.1 Research questions analysis

RQ1- Is it feasible to extend TARA methodology for L4 and L5 CAVs while improving the focus on privacy threats?

Capturing privacy threats in parallel to cybersecurity issues was the prime motivation of the present research which prompted the formulation of RQ1. The thorough assessment of privacy threats was successfully demonstrated from three perspectives: (i) the extension of the CIA model to encapsulate further privacy goals as per unlinkability, accountability and compliance; (ii) the combination of STRIDE and LINDDUN threat modeling; and (iii) the adjustment of the privacy impact rate calculation to consider PII processing as well as the implemented PETs on the system. This approach grants the possibility to model privacy threats equally to cybersecurity ones and acknowledge their coexistence within CAVs ecosystem.

RQ2- How the assessed risks from TARA can depict scrupulously the CAV's SAE automation level?

As an answer to RQ2, our work integrates the SAE automation level and considers the human presence in controlling the risk. By integrating the SAE level as an additional metric for the attack feasibility rating, we refine the risk assessment to be specific to automated driving components rather than being generic to all automotive assets. Such assessment allows decision makers to set appropriate mitigation with regard to the SAE level and develop cost analysis comparing the cost for shifting from an in-vehicle to a remote operator and from an L4 to L5 operations.

RQ3- To what extend the TARA process can be automated to reduce its reliance on experts opinion?

Automating the entire TARA workflow is bound to the dependence on the experts opinion involvement which addresses the raised RQ3. Our work evaluates the TARA steps where experts knowledge is required as well as the existing tool-assisted solutions and the standardised measurements. Our findings concluded that a full automated TARA is still lagging behind with the consideration of the required experts involvement in the process. To cope with that fact, TARA 2.0 proposes the experts objectivity index as an additional factor within the risk analysis which determines the experts subjectivity and confidence about the assessment. Such solution enables an efficient risk prioritisation which would orient the auditor to tackle risks with higher confidence or replicate the assessment of some other APs with lower confidence.

7.6.2 TARA 1.0 and TARA 2.0 comparison

The traditional TARA 1.0 outlined in ISO/SAE 21434 represents a foundation framework for evaluating cybersecurity risks in automotive systems. However, recognising its limitations, an enhanced TARA was developed in this study. TARA 2.0

performance over TARA 1.0 is depicted in Table 7.14 and can be summarised as follows:

- **Privacy modeling:** TARA 2.0 models threats by considering privacy and security goals. It also evaluates threats over eleven threat classes while TARA 1.0 is focused on five threat classes from STRIDE. Furthermore, the privacy impact is underestimated in TARA 1.0 as it puts higher weight on safety and financial impacts than privacy and operations. Unlike TARA 1.0, TARA 2.0 evokes a weighted impact formula (Equation 7.3) associating a weight to every impact depending on the assessed environment.
- **SAE level:** TARA 1.0 discards the human controllability factor throughout the assessment and it is broad enough to assess any automotive asset while TARA 2.0 is specific to L4 and L5 CAVs.
- **Risk compilation:** On one hand, TARA 1.0 combines the impact level and attack feasibility levels to provide a risk value using a 2-D matrix. On the other hand, TARA 2.0 compiles the impact sum, the attack feasibility sum and the experts objectivity index to display the risk through a 3-D visualisation facilitating the risk prioritisation process.
- **Metrics aggregations:** TARA 2.0 provides a granular assessment per AP for both the impact and the attack feasibility ratings. Contrarily, TARA 1.0 computes the impact rating at the damage scenario level. Albeit, the attack feasibility is assessed by AP, it is aggregated afterwards using upper bound analysis based on the maximum ratings to assign a value per damage scenario.
- **Mitigations:** As long as TARA 1.0 assesses a risk value by damage scenario, a risk treatment is then derived by damage scenario. Conversely, TARA 2.0 recommends mitigation strategies for each AP offering a more fine-grained countermeasures.

Table 7.14: TARA 1.0 vs TARA 2.0

	TARA 1.0	**TARA 2.0**
Scope	cybersecurity	cybersecurity & data privacy
Domain	automotive	automotive with distinctions for L4 & L5 CAVs
Ratings	aggregated by damage scenario	assessed by AP
Risk analysis	2-D matrix	3-D matrix
Dependence on experts	yes	yes, but with the inclusion objectivity index O

To that end, TARA 2.0 not only aligns with the core principles of ISO/SAE 21434 but also ensures a more comprehensive and granular evaluation of cybersecurity and privacy risks specific to L4 and L5 CAVs. However, it is essential to acknowledge that both frameworks remain dependent on knowledge from OEMs, cybersecurity and privacy experts. Human insights remain crucial in any TARA where collaborative efforts are required to properly: (i) define the level of abstraction at the asset identification stage;

(ii) map damage scenarios to threat scenarios and then to threat classes; (iii) set attack trees and attack paths; (iv) rate impact factors, values and weights as well as feasibility metrics; and (v) analyse risk priorities with recommendations proposal. Such limitation require further exploration in future work as delineated in the following subsection.

7.6.3 Further limitations and future work

Along with the proposed experts objectivity index, further efforts are envisioned to reduce the dependence on experts opinion. Future work seeks to increase the number of automated sub-processes within the TARA 2.0. Similar to TMT7, a tool-assisted LINDDUN would reduce the experts involvement at the threat modeling phase. Consequently, it is planned to consider automated privacy threat modeling as initiated by other researchers [403, 404]. Additionally, the integration of automated attack trees generations like ThreatGet [121] would support in increasing the assessment objectivity.

Other technological limitations were also identified in our study. By running STRIDE analysis using the automotive template [324], we have realised that the threat modeling from TMT7 inherits vehicular threats and does not fully incorporate autonomous driving features. Such insights prompted us to customise the template stencils. Additionally, after the STRIDE report generation, further reasoning about each threat was still required to clean up the threats pool to avoid threats redundancy. Therefore, it is intended to develop a dedicated autonomous driving template for TMT7 and integrate optimisation functions for synthesised reporting.

Besides, integrating several improvement avenues in TARA 2.0, represents a step towards granular assessment. However, with the rapid evolving technologies, regulations and threat vectors in CAV's domain, the proposed scale needs to be reviewed and updated accordingly for further granularity. As a future work, updated threat taxonomies are intended to take part as additional inputs to the TARA 2.0 workflow. From the privacy perspective, comprehensive data inventories incorporating details about the types of exchanged data, their usage, and associated sensitivity levels would also serve as a foundational inputs to TARA 2.0.

The proposed TARA 2.0 is specifically designed to address CAVs' challenges. However, it is noteworthy to mention that TARA can be applied to a wide range of cyber-physical systems [396]. As a future work, it is aimed to generalise TARA 2.0 to fit different environments. This generalisation can be conducted through the generalisation of the SAE Lx, which was proposed at the attack feasibility rating stage, to become a Domain Specifity (DS) parameter, which can then be customised based on the assessed domain. For instance, in agricultural systems, the DS parameter can be a crop-related factor, while in healthcare systems, it may represent a medical parameter. This approach would allow for a flexible application of TARA 2.0 across several cyber-physical domains.

7.7 Related work

The focus of our work is in the creation of a privacy-centric framework that tackles L4 and L5 CAV's properties, building upon the foundation of TARA 1.0. This development implies a deep understanding of existing assessment methodologies, their sub-steps and potential areas for enhancement. Therefore, our focus encompasses five interrelated research fields gathering privacy assessments, the inclusion of SAE level, the involvement of experts knowledge, the path towards enhanced frameworks and the quality of the process demonstration.

Table 7.15: Related work comparison

Related work	**Year**	**Description**	**ISO/SAE 21434 compliance**	**Enhancing avenues**					**Demonstration**
				Privacy	SAE Lx	Objectivity	Safety	Others	
Dominic et al. [116]	2016	Risk assessment for cooperative automated driving	✗	✗	✓	✗	✗	✓	●●○
Khastgir et al. [267]	2017	HARA with increased reliability	✗	✗	✓	✓	✗	✗	○○○
Monteuuis et al. [331]	2018	SARA	✗	✓	✓	✗	✗	✗	●●○
Bolovinou et al. [49]	2019	TARA+	✓	✗	✓	✗	✗	✗	●○○
He, Meng and Qu [194]	2020	Towards a severity assessment method for CAVs	✗	✗	✓	✗	✗	✗	●○○
Wen et al. [454]	2021	A flexible risk assessment approach	✗	✗	✗	✓	✓	✗	●●○
Agrawal et al. [7]	2021	THARA	✓	✗	✗	✗	✓	✗	○○○
Vogt et al. [443]	2021	A comprehensive risk management approach in ITS	✓	✗	✗	✗	✓	✗	○○○
Dobaj et al. [114]	2021	Towards a security-driven automotive development lifecycle	✓	✗	✗	✗	✗	✓	●○○
Schmittner, Schrammel and Konig [396]	2021	Automotive cybersecurity analysis with ThreatGet	✓	✗	✗	✗	✗	✓	●●○
Plappert et al. [374]	2021	Attack surface assessment in the automotive domain	✓	✗	✗	✗	✗	✗	●●○
Lautenbach, Almgren and Olovsson [285]	2021	HEAVENS 2.0	✓	✗	✗	✗	✗	✗	●●●
Bella, Biondi and Tudisco [36]	2022	A double assessment of privacy risks	✗	✓	✗	✗	✗	✗	●○○
Chah et al. [76]	2022	Privacy threat analysis for CAVs	✗	✓	✗	✗	✗	✗	●○○
Ebrahimi et al. [121]	2022	Attack-tree threat models in connected vehicles	✓	✗	✗	✗	✗	✓	●○○
Zelle et al. [465]	2022	ThreatSurf	✓	✗	✗	✗	✗	✓	●●○
Azam et al. [30]	2023	Data privacy threat modelling for autonomous systems	✓	✓	✗	✗	✗	✗	●○○
Ghosh et al. [178]	2023	Threat analysis for autonomous vehicles perception system	✓	✗	✗	✗	✗	✓	●●○
Abuabed, Alsadeh and Taweel [4]	2023	STRIDE for assessing the vulnerabilities of modern vehicles	✓	✗	✗	✗	✗	✗	●●●
Loskin [302]	2023	TARA+AD	✓	✗	✗	✗	✗	✗	●●○
This work	**2024**	**TARA 2.0**	✓	✓	✓	✓	✗	✗	●●●

7.7.1 Privacy assessment

With the significant volume of data exchanged within the CAV's environment, privacy assessments have recently begun to attract increasing research attention. Bella, Biondi and Tudisco [36] built a dedicated risk assessment framework on data privacy. The proposed model aimed to assess how drivers' sensitive data is protected within eleven modern cars models. The impact is computed based on a data categorisation, varying from driver's behavior, phone, voice to messages, that was mapped to a list of privacy-related assets. Such assets were ranked from one to five according to data sensitiveness, joined to a weight depending on data categorisation and aggregated afterwards by car model. The attack feasibility was elaborated based on vulnerability and data breaches real occurrence, from research and media, per car brand. Albeit the authors provided comparative analysis among modern car brands from the data privacy perspective, the framework does not fully address all the TARA steps.

Similarly, Chah et al. [76] provided a CAV's assessment that is centered on privacy. The authors built the DFD based on data types reflecting the nature of personal and sensitive data. Besides, the authors relied on LINDDUN to derive threat scenarios. On the same note, Azam et al. [30] proposed a threat modeling simulation for CAV's V2I and V2V communications using STRIDE and LINDDUN distinctively. After evaluating the two methods with regard to the CAV's landscape, the authors asserted that each method per se does not assure a holistic modeling of privacy threats. While both research works offer thorough privacy investigations, they are constrained to threat modeling and qualitative analysis without encompassing risk assessment steps.

Closely aligned with our efforts, Monteuuis et al. [331] introduced a systematic TARA framework for L3 CAVs entitled SARA. The authors provided an improved threat model and a refined attack feasibility rating. The proposed threat model extended the STRIDE by adding linkability and confusion as further threat categories. Albeit the linkability attribute depicts a privacy threat class, the confusion category represents a redundant class to tampering which is already embedded in STRIDE. Furthermore, the framework employs non-unified terminology for the TARA steps, as it was constructed based on earlier versions of TARA 1.0 from the SAE J3061 [387].

7.7.2 Security assessments and the SAE automation level

Following the discussion on TARA methodologies preceding the final ISO/SAE 21434, some researchers showcased the correlation between the SAE automation level and the cyber assaults severity. Dominic et al. [116] and He, Meng and Qu [194] are among the pioneering researchers raising such concerns. Nevertheless, the authors discussed the significance of the SAE levels in a cause-and-effect manner, lacking quantified measurements. Besides, Bolovinou et al. [49] proposed TARA+ as an improved TARA framework that was intended for highly automated vehicles of SAE L3 onward. The methodology suggested an enhancement of the preliminary TARA 1.0 version by considering a driver controllability factor within the impact rating step. While the viability of the proposed approach is sound, its main limitation is that TARA+ is applicable to CAVs under a driver intervention which discards L4 and L5 CAVs settings.

7.7.3 Experts subjectivity

Assessing the experts subjectivity has been an ebb and flow at the general scope of risk assessment domain. To assess experts related factors affecting the risk score, Wen et al. [454] proposed a flexible risk assessment, based on FMEA, which embeds subjective and objective weights. Such weights are assigned by experts themselves to indicate hesitant information within the risk assessment process. From the statistics domain, O'Hagan [354] developed the expert knowledge elicitation principle where experts opinion is expressed in the form of probability distributions. The principle relies on quantifying experts uncertainty, their independence as well as their multiplicity. In a closer work to the CAV's domain, Khastgir et al. [267] demonstrated the experts' experience and cultural influences over HARA results through a conducted workshop. The study consisted of two groups of international safety experts independently performing the HARA over a low speed L4 CAV model, where the severity, exposure and controllability metrics for two hazardous events were compared. The authors results are pushed towards improving the validity of the risk analysis by automating the process and lowering experts involvement. While the experts objectivity has been extensively addressed in several critical infrastructures domains like energy and aeronautics [279, 307, 77], there is a lack of literature tackling its application to CAVs as well as its consideration within TARA.

7.7.4 Further enhanced TARA frameworks

Being highly aware of the TARA limitations within the CAV's landscape [187], multiple researchers oriented their efforts towards enhancing TARA either by combining it to other risk assessment methodologies, by tweaking its threat modeling or by extending its risk factors.

Agrawal et al. [7] proposed Threat/Hazard Analysis and Risk Assessment (THARA) to unify security and safety concepts within a single assessment methodology. The framework combines TARA 1.0 and HARA as the authors posited that the former fails in comprehensively addressing attacks related to safety-critical functionalities specially in L3 onwards CAVs. Such improvement consists of integrating the controllabity metric from ASIL [177] in HARA to TARA. Similarly, Vogt et al. [443] designed a joint risk assessment where the FMEA from HARA is integrated to TARA for more quantitative risk analysis. Besides, Dobaj et al. [114] provided a model combining TARA 1.0 and Automotive Software Process Improvement and Capability dEtermination (A-SPICE) [332] where an iterative workflow on deriving cybersecurity requirements was proposed. While these frameworks are designated for ITS as a broad scope of CAVs, concrete demonstrations of the models remain lacking.

With a focus on CAV's perception systems, Ghosh et al. [178] proposed a framework joining TARA 1.0 and STPA-Sec [313], a generic threat modeling designed for cyber-physical systems. By merging the two approaches' steps, the authors aimed to overcome their limitations in comprehensively assessing threats related to perception systems. In addition to the merging, the authors proposed a refinement of the risk calculation by embedding both a robustness factor, representing the performance of AI-based algorithms involved in the assessed perception systems, and a mitigation factor addressing the influences of mitigation solutions on the risk prioritisation.

While the aforementioned research works opted for joint models, others improved TARAs through the automation of certain aspects of their processes. Schmittner, Schrammel and Konig [396] and Ebrahimi et al. [121] proposed a refinement of the threat modeling stage by automating the threat scenarios and attack paths generation respectively using ThreatGet tool. Similarly, Zelle et al. [465] proposed a semi-automated attack paths generation using a different software entitled ThreatSurf. Nevertheless, the suggested tools rely on additional manual work for the input preparation.

7.7.5 Demonstrated TARA

Understanding how to execute a TARA in CAV's environment is crucial for valid risk treatment and cybersecurity requirements elicitation. However, with the multiple sub-steps and the collection of factors including impact, likelihood, and attacker profiles analysis, TARA 1.0 is foreseen as complex and no-ready-to-use methodology [443]. Several works exist in the domain of automotive cybersecurity aiming to address this shortcoming through step-by-step demonstrations as depicted through the last column of Table 7.15 . For instance, Abuabed, Alsadeh and Taweel [4] proposed a compliant framework with an in-depth threat modeling. Plappert et al. [374] demonstrated fine-grained attack feasibility analysis. While the authors demonstrated TARA 1.0 over modern cars at a large scope, they neglected to conduct similarly detailed analysis for the remaining steps of the assessment process. Loskin [302] brought out insight on how to clearly implement TARA 1.0 while depicting all the required work products in terms of sample sheets and documents. Albeit the author presented a detailed methodology, the assessment outcome was not published due to its classification as company confidential. In a more thorough work, Lautenbach, Almgren and Olovsson [285] proposed an improved version of HEAVENS [201] where all the assessment steps were enhanced to meet the ISO/SAE 21434 requirements. Although the authors proclaimed their framework as applicable to automotive, medical, and industrial systems, the level of automation and the extent of human intervention remain at a high level of abstraction.

It is noteworthy to mention that demonstrating the TARA framework remains a common concern among the majority of publications cited within the present section as showcased in Table 7.15. Nevertheless, this subsection is constrained to research work whose principle aim is to demonstrate TARA 1.0 as it is, without proposing any enhancement to the process.

7.7.6 Related work summary

The present section asserts that there is a rich literature attempting to enhance the framework from different angles and aiming to demonstrate TARA 1.0. From Table 7.15, we deduce that there is a substantial race to comply with the ISO/SAE 21434. Additionally, given that various researchers have highlighted limitations in TARA 1.0, multiple efforts have been invested towards enhancing the process. However, these efforts are primarily focused on joining safety and security factors within the assessment or on automating the threat modeling step within the TARA. Moreover, limited attention has been given to privacy or automation level concerns. Furthermore, assessing the experts objectivity is recorded more in other domains (like statistics [354]) but has not yet been incorporated into the execution of TARA.

From the demonstration perspective, existing research works remain limited to high level implementations or to partial demonstration of the TARA process where, for instance, the focus is put only on threat modeling steps or risk calculation. This is where our enhanced TARA 2.0 brings its innovation through simplified and granular demonstration, considering privacy, SAE level and the experts objectivity at the front line.

7.8 conclusions

The number of threats to consider in the CAV landscape grows substantially with the system size, complexity and type of processed data. In this context, TARA 2.0 is crucial to ensure a privacy-aware, efficient and near to objective threat modeling and establish a cost-effective risk analysis. TARA 2.0 can be applied in a systematic way as it consists of a set of guidelines regarding each TARA step, and thoroughly addresses the CAV's properties.

The present research work is threefold: (i) propose enhancements avenues, through TARA 2.0, to make the traditional TARA more privacy-centric and to address L4 and L5 CAVs's properties; (ii) provide guidelines in a step-by-step manner to conduct a TARA for L4 and L5 CAVs; and (iii) demonstrate a granular TARA per AP rather than conducting high level analysis at the level of damage scenarios. Our analysis shows that proposed framework captures additional privacy threat classes, assesses fine-grained privacy impact and incorporates the SAE level as a metric influencing the attack likelihood. Additionally, with the consideration of the experts' objectivity index, our framework pushes towards reliable risk analysis supporting risk decision makers and CAV's stakeholders in determining appropriate cybersecurity goals and claims. The illustrative application of TARA 2.0 that is given in the format of a PoC showcased the approach's feasibility. Our findings are elevated further through a comparative analysis between TARA 1.0 and TARA 2.0, followed by an outline of future efforts envisioned as part of ongoing research.

Appendix: STRIDE & LINDDUN threat classes

To provide more insight on threat classes considered in Section 7.5.4, Tables7.16 and 7.17 determine both STRIDE and LINDDUN categories respectively. Based on the definitions provided in ISO/IEC 27000 [203] as well as the documentation from Microsoft Threat Modeling tool[329] and LINDDUN organisation[459], the threat classes were mapped to the cybersecurity and data privacy compromised properties accordingly. Furthermore, additional supplementary materials, including full list of assets, damage scenarios, STRIDE report, risk analysis of attack paths are available on the online repository, located at [https://isec.unige.ch/].

Table 7.16: STRIDE security threat categories

ID	Class	Compromised property	Designation
S	Spoofing	Authenticity (Confidentiality)	Impersonating an entity to interact with a system.
T	Tampering	Integrity	Unauthorised data or functions modification.
R	Repudiation	Accountability	Not being able to trace back the author of a performed action.
I	Information Disclosure	Confidentiality	Exposing confidential data.
D	Denial of Service	Availability	Degrading service and making it unavailable to legitimate users.
E	Elevation of Privilege	Authorisation (Confidentiality)	Conducting unauthorised actions.

Table 7.17: LINDDUN privacy threat categories

Class	Compromised property	Designation	
L	Linkability	Unlikability	Inferring items of interest about data subjects from protected data.
I’	Identifiability	Unlikability	Identifying data subjects identity.
N	Non-repudiation	Accountability	Being able to trace claimed events as well as their action owner.
D’	Detectability	Accountability	being able to detect the existence of an item of interest relted to a data subject.
D	Disclosure of Information	Confidentiality	Exposing confidential data.
U	Unawareness	Confidentiality	Not being aware about the consequence of sharing their own sensitive data.
N	Non-Compliance	Compliance	Not complying with data protection legislations or the required users’ consents.

Part V

Conclusions

Chapter 8

Discussion and conclusions

Contents

This chapter provides an overall discussion of the research outcomes. It synthesises the answers to the RQs, summarises the scientific contributions, acknowledges the research limitations, proposes future orientations that are foreseen for the near term, and finally concludes the thesis.

8.1 Answers to research questions

RQ1: How to efficiently mitigate cybersecurity and data privacy threats related to CAVs according to a holistic view of all eventual risks?

Answer: This question was thoroughly examined in Chapter 2 and Chapter 3. Initially, we identified the CAV's components to facilitate the determination of potential threat vectors. This initial step allowed us to compile an in-depth knowledge about attack surfaces and supported in mapping them to existing technical mitigation solutions which vary from applying redundancy, fusion and randomisation to perception systems, implementing cryptography and blockchain for network authentication to integrating effective IDSs. Our investigations revealed that, in addition to technical countermeasures, the SDOs efforts also play an essential role mitigating the existing cybersecurity and data privacy risks. While combined mitigation strategies contribute to enhancing the CAV's resilience, it is crucial to recognise that achieving a zero-risk environment in this context can never be attainable. Although existing mitigation measures address known threats, the risk of unknown attacks remain important to consider especially with the CAV's dynamic and interconnected nature. Furthermore, the efficiency of mitigation strategies fluctuate with time. For instance, we demonstrated in Chapter 3 how data anonymisation can get weaker with time if systems are not maintained against de-anonymisation risks.

RQ2: By implementing the published standards, and assuring the compliance to the existing regulations, how robust the CAVs would be from both security and data protection perspectives?

Answer: The answer to this question is gleaned with the response provided for RQ1. It is also linked to the studies conducted in Chapter 2, Chapter 3 and Chapter 4. While the compliance to key regulations and standards pushes towards more resilient systems, a compliant system does not equate a fully protected environment. Our investigations in Chapter 3 showcased how compliance to GDPR just assists in reducing the risks and not to completely preserve privacy. Similarly, compliance to UNECE R155 and ISO/SAE 21434 does not imply a perfectly shielded environment by acknowledging their limitations, explored in Chapter 4, which includes their broadness and inappropriateness regarding L4 and L5 CAVs properties.

RQ3: How the existing standards and regulations can be upgraded to cope with the CAVs technological evolution and legal requirements?

Answer: To better tackle the L4 and L5 CAV, several improvements should be taken into consideration as raised in Chapter 2 and Chapter 3. First, accelerating the legislative process would significantly impact maintaining standards and regulations in alignment with the rapid technological advancements and evolving threats in the CAV's landscape. Second, there is a need to consolidate the WGs efforts, as currently, certain CAV components, such as software updates, receive duplicated attention, while others, like vehicle audits, are overlooked. Consequently, enhancing the collaboration among WGs can ensure equitable distribution of efforts across all CAV's layers and SAE levels. Third, bridging researchers, OEM and SDO efforts will bring a potential harmonisation in standards and regulations development, enabling their continuous and unified updates. Such insight all brings us to the conclusion that efficient standards and regulations is bound to the close collaboration among CAVs stakeholders and a granular understanding of the L4 and L5 particularities.

RQ4: What factors drive the wide adoption of TARA from ISO/SAE 21434?

Answer: The ISO/SAE 21434 is a key standard that has been advertised by mandatory regulations such as UNECE R155 and R156, as pointed out Chapter 5, Chapter 6 and Chapter 7. The standard is set as the core of the automotive cybersecurity governance since it proposes guidelines in cybersecurity management throughout the entire life-cycle, outlines generic road map to conduct TARA, and introduces the foundations of other standards like ISO/SAE 8477, ISO/SAE 8475 and ISO/PAS 5112. Advancing on these concepts involved comparing TARA from ISO/SAE 21434 (TARA 1.0) with existing methodologies in Chapter 5 and implementing that TARA in Chapter 6. This process granted the possibility to verify our theoretical assumption of the standard's limitation in approaching L4 and L5 CAVs despite its strong reference on the SDO's publications.

RQ5: How to build the most auspicious security assessment model based on TARA approaches with respect to the CAVs landscape?

Answer: This question was thoroughly examined in Chapter 5, Chapter 6 and Chapter 7. Compliance to TARA 1.0 and hence to ISO/SAE 21434 guided several researchers in proposing security assessment methodologies which intend to address CAV's particularities. Our studies enabled the possibility of identifying the existing methodologies limitations, more particularly in incorporating data privacy assessments, in reflecting the SAE level throughout the risk analysis and in tackling the experts knowledge involvement throughout the assessment process. Such findings guided the proposal of TARA 2.0 as a potential methodology which addresses the predefined limitations. However, as both technology and threats do not remain frozen on time, even TARA 2.0 would require further improvements as foreseen in Section 8.4.

RQ6: To what extent TARA methodology can be adapted to the highly automation properties of SAE L4 and L5 and the data privacy challenges?

Answer: The present RQ was examined through Chapter 7. Our studies and implementations showed that TARA is a powerful architecture-level analysis methodology. However, to conduct it over L4 and L5 CAV's architectures, a further adaptation is required as demonstrated through TARA 2.0. Our findings emphasised the criticality of modeling both privacy and cybersecurity threats whithin an ecosystem characterised by extensive data exchanges. They highlighted the indispensable inclusion of human controllabity factors through the incorporation of the SAE level in the TARA process. Moreover, our research demonstrated how conducting a granular assessment at the AP level differs significantly from a high-level analysis by damage scenario. This granularity not only facilitates a comprehensive risk analysis but also enables the elicitation of appropriate mitigation strategies, particularly within an environment that is AI dominated, perceived by sensors and driven by a software.

8.2 Summary of scientific contributions

We synthesise the scientific artefacts of the present thesis as follows:

- Provide clarity on cybersecurity and data privacy threat vectors and serve as a referential for researchers and CAV's actors.
- Outline the mandatory obligations versus the nice to have guidelines from the regulatory and standardisation perspectives as well as their pitfalls in addressing the CAV security requirements.
- Increase the awareness on data privacy concerns related to the extensive data exchange associated to every mile driven by a CAV and shed light on the PET challenges.
- Map the existing SDOs efforts, including published legislation and WIP standards, to the CAV's layers and assets.
- Spotlight existing TARA methods, their consistency and limitations with regard to L4 and L5 readiness.
- Define the path towards conducting an appropriate security assessment to the CAV's architecture based on TARA methodology.
- Propose an enhanced TARA which incorporates privacy threat modeling, an agile impact rating, an expanded attack feasibility computation and an extended risk matrix.
- Simplify the TARA process through a step-by-step guide for future replications.
- Bridge research and SDOs through sharing scientific findings within relevant EU projects and WGs standards from ISO, ITU and Swiss Association for Autonomous Mobility (SAAM).

8.3 Limitations

Despite the advancements that this research work is providing, there is of course much that we have not been able to cover within the PhD journey. On that note, the present subsection outlines the primary constraints of this thesis.

8.3.1 Evolving technology and standards

The CAV's technology is promptly advancing with sensors, AI and V2X evolution and upgrades. Concurrently, the attack vectors and mitigation strategies also expand with such advancements. Thereupon, what may serve as an effective countermeasure today can rapidly become limited or inadequate as attackers refine their methods respectively. For instance, a risk that is assessed to be low today with the current technology setup and mitigation strategies, may escalate to high with the evolved attackers capabilities. On that note, our thesis findings reflect the attack surfaces and risk analysis on the assessed vehicle configuration at the time of the elaboration of our experiments. However, given the dynamic nature of CAV technologies and threats landscape, these findings require iterative updates to remain relevant and effective.

Similarly, the regulation and standardisation efforts attempt to keep pace with the technologies advancements but at a different rate. What constitutes an efficient standard today, may become outdated very shortly. It is noteworthy to acknowledge the tremendous SDOs efforts in issuing new legislation, amendments and updates to cope with the rapid evolving cybersecurity and data privacy concerns. However, given the development stages involved in each regulation or standard, several years are counted from initiation to adoption [202]. For instance, in the ISO process, a rapid standard publication takes two to three years in the best case, and up to seven years under less optimal circumstances. The ISO standard development stages consist of [239]: (i) new proposal (NP) (ii) working draft (WD) (iii) committee draft (CD) (iv) draft international standard (DIS) (v) final draft international standard (FDIS) (vi) publication Each stage involves several review sessions, commenting and balloting by relevant technical committees and member countries which have a direct impact on the overall duration of the standard development. While the DIS is limited to 12 weeks, and the FDIS to eight weeks, each of the other stages length is not fixed and depend on the time required to reach consensus among the involved members [239]. Additionally, collaboration with external WGs, like IEC and SAE, can add more delays and contribute to the overall timeline of the standard development. Hence, through the standard development life-cycle, several changes may occur to the standard scope, guidelines or even relevance. Consequently, the changes on the SDOs publications leads to a notable limitation of the SCM proposed in the present thesis. Albeit, two iterations were provided through an initial publication [39] and a second one [38], further recurrent updates should apply to address new changes.

8.3.2 Confidential systems' architectures

Due to the CAV's market rivalry and race towards mature technologies, system architectures remain a sensitive topic that every OEM would keep confidential. Albeit the partnership through EU projects helped in having close discussions with experts on real systems flows, we were constrained to generalise the assessed systems during the articles publication process. The generalisation was achieved by omitting undisclosed components, assets or data flows. While such adjustment impacts the assessment granularity, it respects the confidentiality clauses with the project partners.

On the same note, the alignment to the partners clauses applied also while conducting attack simulations and penetration tests. Any physical access to the vehicle on-board computer as well as any publication revealing cybersecurity vulnerabilities, required formal approvals from the OEM's top management. As a countermeasure, only remote attacks were simulated with respect to the OEMs security procedures and approvals.

8.4 Future work

In the course of this thesis, several future works were raised in the initial articles and have been either partially or fully tackled through the consecutive publications. To illustrate, the envisioned efforts on privacy-preserving techniques, initially outlined as future work in Article I (Chapter 2), were realised through the findings presented in Article II (Chapter 3). Similarly, enhancements to TARA, initially proposed as future work in Article IV (Chapter 5) and Article V (Chapter 6), were successfully achieved in Article VI (Chapter 7). However, additional efforts are planned in the near future to address further challenges.

8.4.1 Towards a proactive and automated TARA

After the accomplishment of TARA 2.0, our aim is to further advance our model into a more automated and proactive framework. To reduce the manual efforts required from the experts in the TARA process and increase its results objectivity, it is planned to integrate a comprehensive tool-assisted threat modeling incorporating both STRIDE and automated LINDDUN along with synthesised threat scenarios. Additionally, the integration of automated risk assessment tools will expedite risk calculation, saving time and effort. This integration will significantly reduce the manual efforts required from experts, leading to more consistent results. Furthermore, we intend to incorporate continuous risk monitoring tools into the TARA 2.0 process allowing for proactive risk mitigation strategies to be implemented before the attack occurrence.

8.4.2 TARA generalisation to other CPS systems

While the present thesis proposes TARA 2.0 as an improved and a customised TARA for L4 & L5 CAVs, we intend to generalise it to any CPS. Although, TARA has been promoted by ISO/SAE 21434 as an automotive evaluation methodology, TARA can be used in any CPS where physical and software components interact [396]. Consequently, and as a part of our future work, we aim to generalise TARA 2.0 to fit different environments. Such generalisation focuses on offering a customisable interface for attack feasibility parameters. For instance, in TARA 2.0, the SAE Lx has been used to reflect the automation level which makes the TARA specific to CAVs. In a generalised TARA, such parameter will be substituted by the DS factor which will reflect a particularity of the assessed domain. For instance, in agricultural systems, the

DS parameter can be a crop-related factor, while in healthcare systems, it may represent a medical parameter. This approach enables a flexible and customisable application of TARA 2.0 across various cyber-physical domains.

8.4.3 Further attack simulations

From the attacks simulations perspectives, it is planned to conduct further penetration tests, in different modes, and targeting various CAV's components. Considering the ongoing collaborations with the SAAM association bridging academic partners to industrial parties, grey- or white-box attack simulations, with access to the onboard computer, can become tangible. In such attack simulation mode, the access to the vehicle logs will become possible allowing a deep understanding of the vehicle behaviour upon an attack as well as the resilience of the mitigation techniques in place. The reporting of such pentests is aimed to take the form of CVEs reports with a mapping to known vulnerabilities from the National Vulnerability Database (NVD) database [343] and patching recommendations.

8.4.4 SAE automation levels granularity

As a fundamental input to the present thesis, the SAE levels definition guided the overall progress of our scientfic findings. The actual six levels provide valuable foundations for assimilating the driver and the ADS capabilities in each level. However, the SAE levels require further refinement to capture more granular distinctions in the CAV capabilities. While Article VI (Chapter 7) points out to L4* and L4** mirroring the status of the fall-back operator to be remote or inside the vehicle, we believe that additional distinctions are applicable to infer L4 and L5 sub-levels. The incorporation of other factors capturing finer environmental conditions (like resistance to extreme temperatures), traffic density (as per mixed driving in city centers, or light weighted traffic in suburbs) and CAV setup (like speed limitation to <20km/h), could fine-tune and help to adapt the SAE levels to real-world driving scenarios. To that end, it is planned to provide a review on enhancing SAE granularity to better guide the CAV's development and deployment.

8.4.5 European regulations

From a regulatory standpoint, it is intended to conduct a study evaluating the relevance of the recent EU acts to L4 & L5 CAVs. For instance, the new data act [151], effective from January 2024, introduces data sovereignty clauses granting enhanced rights to data subjects to access produced data. Further more, the CRA [144], also entering into force in 2024, complements the NIS2 directive and aims to increase the end-users' awareness of cybersecure services and devices. As IoT systems fall into the scope of these new regulations, further investigations are needed to understand their implications on CAV's stakeholders, their obligations regarding open systems, and the required security measures to grant such openness.

8.5 Conclusion

This thesis delves into cybersecurity, data privacy as well as regulations and standards challenges associated to the CAV's deployment. It presents the current state-of-the art of these three pillars laying the groundwork in understanding the existing threat vectors, mitigation strategies and the standards limitations as theoretical foundations of the entire thesis. The consolidated insights led to the importance of conducting cybersecurity and data privacy assessments based on standardised methodologies to reach a resilient environment.

Among the assessment methodologies examined, TARA emerges as the most suitable framework. However, even prominent methodologies like TARA from ISO/SAE 21434 exhibit limitations in addressing L4 and L5 properties, as showcased by analytics and experimental studies. These findings motivated the proposal and the establishment of an enhanced framework which puts privacy at the forefront, incorporates the SAE level, and quantifies the experts subjectivity. The conceptualisation and implementation of the proposed framework was validated through a PoC supporting its feasibility. Additionally, our solution is presented with a comprehensive step-by-step demonstration, simplifying the process workflow for future replication.

Despite confidentiality clauses in OEMs agreements limiting publication or access to full CAV architectures, our implementations ensured granular analysis of the ADS as a common asset in all CAV's systems to preserve the agreements with the OEM partners. Besides, it is noteworthy to mention that our work extends beyond the presentation of this thesis. It is intended to turn the enhanced TARA into more automated framework with the conversion of the experts dependent steps into tools-based. This future direction aligns with plans for further attack simulations, facilitating proactive TARA testing and refinement.

References

[1] 5GAA. *5GAA Efficient Security Provisioning System White Paper*. Tech. rep. 5GAA, May 2020.

[2] 5GAA. *Privacy by Design Aspects of C-V2X*. Tech. rep. 5GAA, Oct. 2020.

[3] Ahmed Abdo et al. 'Cybersecurity on Connected and Automated Transportation Systems: A Survey'. In: *IEEE Transactions on Intelligent Vehicles* (2023). ISSN: 23798858. DOI: 10.1109/TIV.2023.3326736.

[4] Zaina Abuabed, Ahmad Alsadeh and Adel Taweel. 'STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles'. In: *Computers and Security* 133 (Oct. 2023). ISSN: 01674048. DOI: 10.1016/j.cose.2023.103391.

[5] ACEA. *ACEA comments EDPB guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*. Tech. rep. ACEA, 2020.

[6] aepd. *Ten Misunderstandings Related to Anonymisation*. Tech. rep. 1. AEPD, Dec. 2019. DOI: 10 . 1038 / s41467 - 019 - 10933 - 3. URL: https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

[7] Vivek Agrawal et al. 'Threat/Hazard Analysis and Risk Assessment: A Framework to Align the Functional Safety and Security Process in Automotive Domain'. In: *SAE Int. J. Transp. Cyber. and Privacy* (Dec. 2021). DOI: 10.4271/2021-01-0148.

[8] Ijaz Ahmad et al. 'Security for 5G and beyond'. In: *IEEE Communications Surveys and Tutorials* 21.4 (2019), pp. 3682–3722. ISSN: 1553877X. DOI: 10.1109/COMST.2019.2916180.

[9] Jaagup Ainsalu et al. 'State of the art of automated buses'. In: *Sustainability (Switzerland)* 10.9 (2018). ISSN: 20711050. DOI: 10.3390/su10093118.

[10] Abdullah Al Mamun, Md Abdullah Al Mamun and Abdullatif Shikfa. 'Challenges and Mitigation of Cyber Threat in Automated Vehicle: An Integrated Approach'. In: *2018 International Conference of Electrical and Electronic Technologies for Automotive, AUTOMOTIVE 2018* (2018), pp. 1–6. DOI: 10.23919/EETA.2018.8493171.

[11] Christopher Alberts, Audrey Dorofee and James Stevens. *OCTAVE -S Implementation Guide, Version 1.0*. Tech. rep. Pittsburg: Carnegie Mellon Software Engineering Institute, Jan. 2005.

[12] Ikram Ali and Fagen Li. 'An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs'. In: *Vehicular Communications* 22 (2020), p. 100228. ISSN: 22142096. DOI: 10.1016/j.vehcom.2019.100228. URL: https://doi.org/10.1016/j.vehcom.2019.100228.

[13] Khattab M Ali Alheeti and Klaus Mc Donald-Maier. 'Intelligent intrusion detection in external communication systems for autonomous vehicles'. In: *Systems Science and Control Engineering* 6.1 (2018), pp. 48–56. ISSN: 21642583. DOI: 10.1080/21642583.2018.1440260.

[14] Alissa Knight. *Hacking Connected Cars: Tactics, Techniques and Procedures*. 2020. ISBN: 978-1-119-49173-6. URL: https://www.wiley.com/en-us/Hacking+Connected+Cars%3A+Tactics%2C+Techniques%2C+and+Procedures-p-9781119491736.

[15] Sultan Almuhammadi and Clifford Neuman. 'Security and privacy using one-round zero-knowledge proofs'. In: *Proceedings - Seventh IEEE International Conference on E-Commerce Technology, CEC 2005* 2005 (2005), pp. 435–438. DOI: 10.1109/ICECT.2005.78.

[16] Philip Andersson. 'Penetration Testing of an In-Vehicle Infotainment System'. PhD thesis. Stockholm: KTH ROYAL INSTITUTE OF TECHNOLOGY, July 2022. URL: http://kth.diva-portal.org/smash/record.jsf?aq2=%5B%5B%5D%5D&c=9&af=%5B%5D&searchType=LIST_LATEST&sortOrder2=title_sort_asc&query=&language=en&pid=diva2%3A1708534&aq=%5B%5B%5D%5D&sf=all&aqe=%5B%5D&sortOrder=author_sort_asc&onlyFullText=false&noOfRows=50&dswid=3357.

[17] Oluwasefunmi T. Arogundade et al. 'Enhancing Misuse Cases with Risk Assessment for Safety Requirements'. In: *IEEE Access* 8 (2020), pp. 12001–12014. ISSN: 21693536. DOI: 10.1109/ACCESS.2019.2963673.

[18] Article 29 Data Protection Working Party. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Tech. rep. Brussels: Article 29 WP, Feb. 2018. URL: https://ec.europa.eu/newsroom/article29/items/612053.

[19] Article 29 Data Protection Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Tech. rep. Article 29 Data Protection Working Party, Oct. 2017. URL: https://ec.europa.eu/newsroom/article29/items/611236.

[20] Article 29 Data Protection Working Party. *Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) - 217/EN - WP 252*. Tech. rep. October. Article 29 Data Protection Working Party, 2017, pp. 1–14.

[21] Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*. Tech. rep. April. Article 29 Working Party, 2014, pp. 1–37. URL: http://ec.europa.eu/justice/data-protection/index_en.htm%0Ahttp://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[22] Mamoona N. Asghar et al. 'Visual surveillance within the eu general data protection regulation: A technology perspective'. In: *IEEE Access* 7 (2019), pp. 111709–111726. ISSN: 21693536. DOI: 10.1109/ACCESS.2019.2934226.

[23] Philip Asuquo et al. 'Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures'. In: *IEEE Internet of Things Journal* 5.6 (2018), pp. 4778–4802. ISSN: 23274662.

[24] NTC Australia. *Regulating Government Access to C-ITS and Automated Vehicle Data*. Tech. rep. September. National Transport Commission, 2018.

[25] Auto-ISAC. *Best Practices*. URL: https://automotiveisac.com/best-practices/.

[26] AUTOSAR. *Autosar 402 Specification of Crypto Service Manager*. Tech. rep. AUTOSAR, 2009.

[27] AUTOSAR. *Autosar 438 Specification of Crypto Abstraction Library*. Tech. rep. AUTOSAR, 2009.

[28] AUTOSAR. *Autosar 654 Specification of Secure Onboard Communication*. Tech. rep. AUTOSAR, 2017, pp. 1–28.

[29] AUTOSAR. *Autosar 664 Overview of Functional Safety Measures in AUTOSAR*. Tech. rep. Autosar, 2015, pp. 1–96.

[30] Naila Azam et al. 'Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR Perspective'. In: *IEEE Transactions on Big Data* (Apr. 2022). ISSN: 23327790. DOI: 10.1109/TBDATA.2022.3227336.

[31] David Bailey. 'Quantitative Cybersecurity Risk Management for Autonomous Vehicle Systems'. PhD thesis. Technical University of Munich, Oct. 2018. URL: https://mediatum.ub.tum.de/doc/1482036/992686146856.pdf.

[32] Paolo Balboni et al. 'Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility'. In: *WAIEL2020*. Athens, Sept. 2020. URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&.

[33] Mohammad Baqer and Axel Krings. 'Reliability of VANET Bicycle Safety Applications in Malicious Environments'. In: *27th Telecommunications Forum, TELFOR 2019* (2019), pp. 2019–2022. DOI: 10.1109/TELFOR48224.2019.8971200.

[34] Daniel Bastos, Fadi El-Mousa and Fabio Giubilo. 'GDPR Privacy Implications for the Internet of Things'. In: *4th Annual IoT Security Foundation Conference*. London, 2018. URL: https://www.researchgate.net/publication/331991225.

[35] P Bec et al. 'Study of vulnerabilities in designing and using automated vehicles based on SWOT method for chevrolet camaro'. In: *IOP Conference Series: Materials Science and Engineering*. Vol. 898. 1. 2020, p. 12008.

[36] Giampaolo Bella, Pietro Biondi and Giuseppe Tudisco. 'A Double Assessment of Privacy Risks Aboard Top-Selling Cars'. In: *Automotive Innovation* (2023). ISSN: 25228765. DOI: 10.1007/s42154-022-00203-2.

[37] Gueltoum Bendiab et al. 'Autonomous Vehicles Security: Challenges and Solutions using Blockchain and Artificial Intelligence'. In: *IEEE Transactions on Intelligent Transportation Systems* 24 (2023), pp. 3614–3637.

[38] Meriem Benyahya, Anastasija Collen and Niels Alexander Nijdam. 'Analyses on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap'. In: *Transportation Engineering* 14 (Dec. 2023). ISSN: 2666691X. DOI: 10.1016/j.treng.2023.100205.

[39] Meriem Benyahya, Anastasija Collen and Niels Alexander Nijdam. 'Cybersecurity and Data Privacy Certification Gaps of Connected and Automated Vehicles'. In: *Transportation Research Procedia*. Ed. by Elsevier. Vol. 72. Lisbon: Elsevier, Nov. 2023, pp. 783–790. DOI: 10.1016/j.trpro.2023.11.468. URL: https://linkinghub.elsevier.com/retrieve/pii/S2352146523007664.

[40] Meriem Benyahya et al. 'A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles'. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*. Vol. 1. New York, NY, USA: ACM, Aug. 2023, pp. 1–10. DOI: 10.1145/3600160.3605084. URL: https://dl.acm.org/doi/10.1145/3600160.3605084.

[41] Meriem Benyahya et al. 'Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments'. In: *Computers & Security* 122 (Nov. 2022), p. 102904. ISSN: 01674048. DOI: 10.1016/j.cose.2022.102904. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404822002978.

[42] Meriem Benyahya et al. 'Driving Towards Resilience: Advancements in Threat Analysis and Risk Assessment for Connected and Automated Vehicles'. 2024.

[43] Meriem Benyahya et al. 'Symbiotic Analysis of Security Assessment and Penetration Tests Guiding Real L4 Automated City Shuttles'. In: *Telecom* 4.1 (Mar. 2023), pp. 198–218. ISSN: 2673-4001. DOI: 10.3390/telecom4010012. URL: https://www.mdpi.com/2673-4001/4/1/12.

[44] Meriem Benyahya et al. 'The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis'. In: *Applied Sciences* 12.9 (Apr. 2022), p. 4413. ISSN: 2076-3417. DOI: 10.3390/app12094413. URL: https://www.mdpi.com/2076-3417/12/9/4413.

[45] Anatolij Bezemskij et al. 'Detecting Cyber-Physical Threats in an Autonomous Robotic Vehicle Using Bayesian Networks'. In: *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017* 2018-Janua (2018), pp. 98–103. DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.20.

[46] Bharat Bhargava et al. 'A systematic approach for attack analysis and mitigation in V2V networks'. In: *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 7.1 (2016), pp. 79–96. ISSN: 20935382. DOI: 10.22667/JOWUA.2016.03.31.079.

[47] Narayan Bhusal, Mukesh Gautam and Mohammed Benidris. 'Cybersecurity of electric vehicle smart charging management systems'. In: *arXiv* (2020). ISSN: 23318422.

[48] Anushka Biswas and Hwang-Cheng Wang. 'Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain'. In: *Sensors* 23.4 (Feb. 2023), p. 1963. ISSN: 1424-8220. DOI: 10.3390/s23041963. URL: https://www.mdpi.com/1424-8220/23/4/1963.

[49] Anastasia Bolovinou et al. 'TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems'. In: *2019 IEEE Intelligent Vehicles Symposium (IV)*. Paris: IEEE, June 2019, pp. 8–13. ISBN: 978-1-7281-0560-4. DOI: 10.1109/IVS.2019.8813999. URL: https://ieeexplore.ieee.org/document/8813999/.

[50] Richard Bonichon et al. *Computer Safety, Reliability, and Security*. Vol. 6894. Turku: Springer, Sept. 2019, pp. 85–98. ISBN: 978-3-642-24269-4. DOI: 10.1007/978-3-642-24270-0.

[51] Patrick M Bösch et al. 'Cost-based analysis of autonomous mobility services'. In: *Transport Policy* 64.February (2018), pp. 76–91. ISSN: 1879310X. DOI: 10.1016/j.tranpol.2017.09.005.

[52] Aymen Boudguiga et al. 'RACE: Risk analysis for cooperative engines'. In: *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*. Paris, France: IEEE, July 2015, pp. 1–5. ISBN: 978-1-4799-8784-9. DOI: 10.1109/NTMS.2015.7266516. URL: http://ieeexplore.ieee.org/document/7266516/.

[53] Azzedine Boukerche, Abdul Jabbar Siddiqui and Abdelhamid Mammeri. 'Automated vehicle detection and classification: Models, methods, and techniques'. In: *ACM Computing Surveys* 50.5 (2017), pp. 1–39. ISSN: 15577341. DOI: 10.1145/3107614. URL: https://dl.acm.org/doi/10.1145/3107614.

[54] Elizabeth A Brasher. 'Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation'. In: *Columbia Business Law Review*. Heinonline, 2018, pp. 209–253.

[55] BSI. *PAS 11281 Connected and autonomous vehicles (CAVs)*. Tech. rep. BSI, 2018.

[56] BSI. *PAS 1880 Guidelines for developing and assessing control systems for automated vehicles*. Tech. rep. BSI, 2020.

[57] BSI. *PAS 1881: Assuring the safety of automated vehicle trials and testing-Specifi cation Publishing and copyright information*. Tech. rep. BSI, 2020.

[58] BSI. *PAS 1885:2018 how to improve and maintain vehicle security*. Tech. rep. BSI, 2018.

[59] C-Roads. *Platform: C-Roads*. 2021. URL: https://www.c-roads.eu/platform.html.

[60] C. McCarthy, K. Harnett and A. Carter. *Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach*. Tech. rep. National Highway Traffic Safety Administration (NHTSA), Oct. 2014. URL: www.ntis.gov.

[61] C2A-SEC LTD. *C2A security: The First Cybersecurity Lifecycle Management Platform*. 2024. URL: https://c2a-sec.com/autosec/.

[62] Canonica. *Enterprise Open Source and Linux Ubuntu*. Jan. 2023. URL: https://ubuntu.com.

[63] Yulong Cao et al. 'Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving'. In: *arXiv* (2019), pp. 2267–2281.

[64] Yulong Cao et al. 'You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks'. In: *arXiv* (Oct. 2022). DOI: 10.48550/arXiv.2210.09482.

[65] Félix Carreyre et al. 'On-Demand Autonomous Vehicles in Berlin: A Cost–Benefit Analysis'. In: *Transportation Research Record: Journal of the Transportation Research Board* (Aug. 2023). ISSN: 0361-1981. DOI: 10.1177/03611981231186988.

[66] Valentina Casola et al. 'Towards automated penetration testing for cloud applications'. In: *Proceedings - 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2018*. Institute of Electrical and Electronics Engineers Inc., Oct. 2018, pp. 30–35. ISBN: 9781538669167. DOI: 10.1109/WETICE.2018.00012.

[67] CellMapper. *Swisscom (Switzerland) - Cellular Coverage and Tower Map*. Jan. 2023. URL: https://www.cellmapper.net/.

[68] CEN. *CEN/CLC/JTC 13 - Cybersecurity and Data Protection*. 2021. URL: https://standards.cen.eu/.

[69] CEN-CENELEC. *About us - CEN-CENELEC*. 2021. URL: https://www.cencenelec.eu/aboutus/Pages/default.aspx.

[70] Cen-CENELEC. *Work programme 2021*. Tech. rep. May. CEN-CENELEC, 2020, pp. 1–16.

[71] CEN/TC278. *CEN/TC 278 Intelligent transport systems*. 2021. URL: https://www.itsstandards.eu/aboutus/.

[72] CEN/TC278. *Cooperative intelligent transport systems (C-ITS) Guidelines on the usage of standards*. Tech. rep. CEN and ISO, 2021.

[73] CEN/TC278. *European Standardization in Support of urban Intelligent Transportation and Mobility*. Tech. rep. CEN, 2018. URL: https://www.cen.eu/news/brochures/brochures/Urban_Intelligent_Transport_CEN-TC-278.pdf.

[74] Center for Strategic and International Studies. *European Union Releases Draft Mandatory Human Rights and Environmental Due Diligence Directive*. Mar. 2022. URL: https://www.csis.org/analysis/european-union-releases-draft-mandatory-human-rights-and-environmental-due-diligence.

[75] Shi Cho Cha et al. 'Privacy enhancing technologies in the internet of things: Perspectives and challenges'. In: *IEEE Internet of Things Journal* 6.2 (Apr. 2019), pp. 2159–2187. ISSN: 23274662. DOI: 10.1109/JIOT.2018.2878658.

[76] Badreddine Chah et al. 'Privacy Threat Analysis for connected and autonomous vehicles'. In: *Procedia Computer Science*. Vol. 210. C. Elsevier B.V., 2022, pp. 36–44. DOI: 10.1016/j.procs.2022.10.117.

[77] Kuei-Hu Chang. 'Integrating Subjective–Objective Weights Consideration and a Combined Compromise Solution Method for Handling Supplier Selection Issues'. In: *Systems* 11.2 (Feb. 2023), p. 74. ISSN: 2079-8954. DOI: 10.3390/systems11020074.

[78] Raghu Changalvala and Hafiz Malik. 'LiDAR Data Integrity Verification for Autonomous Vehicle'. In: *IEEE Access* 7 (2019), pp. 138018–138031. ISSN: 21693536. DOI: 10.1109/ACCESS.2019.2943207.

[79] Kyong Tak Cho and Kang G Shin. 'Error handling of in-vehicle networks makes them vulnerable'. In: *Proceedings of the ACM Conference on Computer and Communications Security* 24-28-Octo (2016), pp. 1044–1055. ISSN: 15437221. DOI: 10.1145/2976749.2978302.

[80] Mashrur Chowdhury, Mhafuzul Islam and Zadid Khan. 'Security of connected and automated vehicles'. In: *Bridge* 49.3 (2019), pp. 46–56. ISSN: 07376278.

[81] Christoph Schmittner et al. 'A Preliminary View on Automotive Cyber Security Management Systems'. In: EDA Consortium, 2020. ISBN: 9783981926347.

[82] Ge Chu and Alexei Lisitsa. 'Penetration Testing for Internet of Things and Its Automation'. In: *Proceedings - 20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018*. Institute of Electrical and Electronics Engineers Inc., Jan. 2019, pp. 1479–1484. ISBN: 9781538666142. DOI: 10.1109/HPCC/SmartCity/DSS.2018.00244.

[83] CITS. *Secure Firmware Update*. 2017. URL: https://cts-labs.com/secure-firmware-update.

[84] Guillaume Collard et al. 'A definition of Information Security Classification in cybersecurity context'. In: *Proceedings - International Conference on Research Challenges in Information Science*. IEEE, 2017, pp. 77–82. ISBN: 9781509054763. DOI: 10.1109/RCIS.2017.7956520.

[85] Lisa Collingwood. 'Privacy implications and liability issues of autonomous vehicles'. In: *Information and Communications Technology Law* 26.1 (2017), pp. 32–45. ISSN: 14698404. DOI: 10.1080/13600834.2017.1269871.

[86] Common Criteria. *Common Methodology for Information Technology Security Evaluation Evaluation methodology*. Tech. rep. 2017.

[87] Congress. *H3388- Self Drive Act*. Tech. rep. US Government, 2017. URL: https://www.congress.gov/bill/115th-congress/house-bill/3388/text.

[88] Congress. *S.2181 Spy Car Act*. Tech. rep. US Government, 2019. URL: https://www.congress.gov/bill/116th-congress/senate-bill/2182/text.

[89] Consortium. *ULTIMO Advancing Sustainable User-centric Mobility with Automated Vehicles*. 2023. URL: https://ultimo-he.eu/partners/.

[90] Graham Cormode. 'Personal privacy vs population privacy: Learning to attack anonymization'. In: *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (2011), pp. 1253–1261. DOI: 10.1145/2020408.2020598.

[91] Federico Costantini et al. 'Autonomous vehicles in a GDPR era: An international comparison'. In: *Advances in Transport Policy and Planning* 5 (2020). ISSN: 25429116. DOI: 10.1016/bs.atpp.2020.02.005.

[92] Costas Lambrinoudakis et al. *Compendium of Risk Management Frameworks with Potential Interoperability*. Tech. rep. ENISA, Jan. 2022.

[93] Joseph Cox. *Surprise! Scans Suggest Hackers Put IMSI-Catchers All Over Defcon*. Nov. 2022. URL: https://www.vice.com/en/article/vv7zn9/surprise-scans-suggest-hackers-put-imsi-catchers-all-over-defcon.

[94] Daniel A Crane, Kyle D Logue and Bryce C Pilz. 'A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles'. In: *SSRN Electronic Journal* 23.2 (2017). ISSN: 1528-8625. DOI: 10.2139/ssrn.2807059.

[95] Alexandru Csete. *Welcome to gqrx*. Jan. 2023. URL: https://gqrx.dk.

[96] Jin Cui and Giedre Sabaliauskaite. 'On the Alignment of Safety and Security for Autonomous Vehicles'. In: *Cyber 2017: The Second International Conference on Cyber-Technologies and Cyber Systems*. Barcelona, Spain: IARIA XPS Press, 2017, pp. 59–64. ISBN: 9781612086057.

[97] Jin Cui and Biao Zhang. 'VeRA: A Simplified Security Risk Analysis Method for Autonomous Vehicles'. In: *IEEE Transactions on Vehicular Technology* 69.10 (Oct. 2020), pp. 10494–10505. ISSN: 19399359. DOI: 10.1109/TVT.2020.3009165.

[98] Jin Cui et al. 'A review on safety failures, security attacks, and available countermeasures for autonomous vehicles'. In: *Ad Hoc Networks* 90 (2019). ISSN: 15708705. DOI: 10.1016/j.adhoc.2018.12.006.

[99] Curia Caselaw. *Judgment of The Court*. June 2018. URL: https://curia.europa.eu/juris/document/document.jsf?docid=202543&doclang=EN.

[100] Curia Caselaw. *Judgment of the Court on Facebook Ireland Ltd*. July 2019. URL: https://curia.europa.eu/juris/document/document.jsf?docid=216555&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=4232790.

[101] Cymotive Technologies Ltd. *Automotive Vulnerability Management for the Full Vehicle Lifecycle*. 2022. URL: https://www.cymotive.com/wp-content/uploads/2022/08/CYMOTIVE-Vulnerability-Management-Solution-Brief.pdf.

[102] Kevin Daimi and Mustafa Saed. 'Securing Tire Pressure Monitoring System'. In: *The Fourteenth Advanced International Conference on Telecommunications*. c. Barcelona, Spain, 2018, pp. 32–37. ISBN: 978-1-61208-650-7.

[103] George Danezis et al. *Privacy and Data Protection by Design - from policy to engineering*. Tech. rep. ENISA, Jan. 2015. DOI: 10.2824/38623. URL: http://arxiv.org/abs/1501.03726%20http://dx.doi.org/10.2824/38623.

[104] Daniel J. Fagnant and Kara Kockelman. 'Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations'. In: *Transportation Research Part A* 77 (2015), pp. 167–181.

[105] Sagar Dasgupta et al. 'Prediction-Based GNSS Spoofing Attack Detection for Autonomous Vehicles. (arXiv:2010.11722v1 [cs.RO])'. In: *arXiv Computer Science* 864 (2021), pp. 1–16.

[106] Data for Road Safety. *Partners Safety Related Traffic Information Ecosystem*. 2021. URL: https://www.dataforroadsafety.eu/.

[107] DATEX-II. *Datex II developments*. URL: https://datex2.eu/datex2/developments.

[108] DATEX-II. *Datex II Specifications*. URL: https://datex2.eu/datex2/specifications.

[109] Yves-Alexandre De Montjoye et al. 'Unique in the Crowd: The privacy bounds of human mobility'. In: *Scientific Reports* (2013). DOI: 10.1038/srep01376. URL: www.nature.com/scientificreports.

[110] by Deborah Lamm Weisel. *The Sequence of Analysis in Solving Problems*. Tech. rep. 2003, pp. 115–146.

[111] Johannes Deichmann et al. *Autonomous driving's future: Convenient and connected*. Tech. rep. Atlanta: McKinsey, Jan. 2023.

[112] Department for Transport. *The Pathway to Driverless Cars*. Tech. rep. February 2015. Department of Transport, UK, 2015.

[113] Mahdi Dibaei et al. 'Attacks and defences on intelligent connected vehicles: a survey'. In: *Digital Communications and Networks* 6.4 (2020), pp. 399–421. ISSN: 23528648. DOI: 10.1016/j.dcan.2020.04.007. URL: https://doi.org/10.1016/j.dcan.2020.04.007.

[114] Jürgen Dobaj et al. 'Towards a security-driven automotive development lifecycle'. In: *Journal of Software: Evolution and Process* (Nov. 2021), pp. 1–22. ISSN: 2047-7473. DOI: 10.1002/smr.2407. URL: https://onlinelibrary.wiley.com/doi/10.1002/smr.2407.

[115] Jürgen Dobaj et al. 'Towards Integrated Quantitative Security and Safety Risk Assessment'. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11699 LNCS (2019), pp. 102–116. ISSN: 16113349. URL: https://link.springer.com/chapter/10.1007/978-3-030-26250-1_8.

[116] Derrick Dominic et al. 'Risk Assessment for Cooperative Automated Driving'. In: *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. New York, NY, USA: ACM, Oct. 2016, pp. 47–58. ISBN: 9781450345682. DOI: 10.1145/2994487.2994499. URL: https://dl.acm.org/doi/10.1145/2994487.2994499.

[117] Faábio Duarte and Carlo Ratti. 'The Impact of Autonomous Vehicles on Cities: A Review'. In: *Journal of Urban Technology* 25.4 (Oct. 2018), pp. 3–18. ISSN: 1063-0732. DOI: 10.1080/10630732.2018.1493883.

[118] Phap Duong-Ngoc, Tuy Nguyen Tan and Hanho Lee. 'Efficient NewHope Cryptography Based Facial Security System on a GPU'. In: *IEEE Access* 8 (2020), pp. 108158–108168. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3000316.

[119] Cynthia Dwork, Nitin Kohli and Deirdre Mulligan. 'Differential Privacy in Practice: Expose your Epsilons!' In: *Journal of Privacy and Confidentiality* 9.2 (Oct. 2019). DOI: 10.29012/jpc.689. URL: https://journalprivacyconfidentiality.org/index.php/jpc/article/view/689.

[120] Cynthia Dwork and Aaron Roth. 'The algorithmic foundations of differential privacy'. In: *Foundations and Trends in Theoretical Computer Science* 9.3-4 (2013), pp. 211–487. ISSN: 15513068. DOI: 10.1561/0400000042.

[121] Masoud Ebrahimi et al. 'Identification and Verification of Attack-Tree Threat Models in Connected Vehicles'. In: *SAE Threat Modeling 2022*. Dec. 2022. DOI: 10.4271/2022-01-7087.

[122] EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Tech. rep. EDPB, July 2020.

[123] David Elliott, Walter Keen and Lei Miao. 'Recent advances in connected and automated vehicles'. In: *Journal of Traffic and Transportation Engineering (English Edition)* 6.2 (2019), pp. 109–131. ISSN: 20957564. DOI: 10.1016/j.jtte.2018.09.005.

[124] ENISA. *Data Pseudonymisation: advanced Techniques & Use Cases*. Tech. rep. ENISA, Jan. 2021. DOI: 10.2824/860099. URL: www.enisa.europa.eu..

[125] Joseph M Ernst and Alan J Michaels. 'LIN bus security analysis'. In: *Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society* (2018), pp. 2085–2090. DOI: 10.1109/IECON.2018.8592744.

[126] ETSI. *EN 302 637-2 - V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*. Tech. rep. ETSI, 2014.

[127] ETSI. *ETSI TR 102 893 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*. Tech. rep. ETSI, 2010.

[128] ETSI. *ETSI TR 103 257-1 V1.1.1 Intelligent Transport Systems (ITS); Access Layer; Part 1: Channel Models for the 5,9 GHz frequency band*. Tech. rep. ETSI, 2019.

[129] ETSI. *ETSI TR 103 415 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management*. Tech. rep. ETSI, 2018.

[130] ETSI. *ETSI TS 102 165 Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)*. Tech. rep. Sophia Antipolis: ETSI, Oct. 2017.

[131] ETSI. *ETSI TS 102 731 v2 Intelligent Transport Systems (ITS); Security; Security Services and Architecture; Release 2*. Tech. rep. ETSI, Nov. 2022.

[132] ETSI. *ETSI TS 102 940 V1.3.1 - Security; ITS communications security architecture and security management*. Tech. rep. ETSI, 2018, pp. 1–42.

[133] ETSI. *TS 102 165-1 - V4.2.3 - Method and proforma for Threat, Risk, Vulnerability Analysis*. Tech. rep. ETSI, Mar. 2011.

[134] ETSI. *TS 102 941 - V1.3.1 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*. Tech. rep. ETSI, 2019.

[135] ETSI. *TS 102 942 - V1.1.1 Intelligent Transport Systems (ITS); Security; Access Control Technical Specification*. Tech. rep. ETSI, 2012. URL: http://portal.etsi.org/chaircor/ETSI_support.asp.

[136] ETSI. *TS 102 943 V1.1.1 Intelligent Transport Systems (ITS); Security; Confidentiality services Technical Specification*. Tech. rep. ETSI, 2012.

[137] ETSI. *TS 103 097 - V1.3.1 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats*. Tech. rep. ETSI, 2017.

[138] European Automotive Manufacturers Association (ACEA). *ACEA Principles of Automobile Cybersecurity*. Tech. rep. September. ACEA, 2017.

[139] European Automotive Manufacturers Association (ACEA). *Roadmap for the Deployment of Automated Driving in the European Union*. Tech. rep. ACEA, 2019.

[140] European Comission. *ULTIMO - Advancing Sustainable User-centric Mobility with Automated Vehicles*. 2022. URL: https://cordis.europa.eu/project/id/101077587/fr.

[141] European Commission. *A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles | nIoVe Project | Fact Sheet | H2020 | CORDIS | European Commission*. 2022. URL: https://cordis.europa.eu/project/id/833742/fr.

[142] European Commission. *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*. Tech. rep. June. European Commission, 2018, pp. 1–79.

[143] European Commission. *E-safety Vehicle Intrusion proTected Applications EVITA Project*. URL: https://cordis.europa.eu/project/id/224275.

[144] European Commission. *EU Cyber Resilience Act*. 2024.

[145] European Commission. *Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements*. Tech. rep. Brussels: European Comission, Sept. 2022, pp. 1–87.

[146] European Commissopn. *Cooperative, connected and automated mobility (CCAM) Mobility and Transport*. URL: https://ec.europa.eu/transport/themes/its/c-its.

[147] European Data Protection Board. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*. Tech. rep. January. EDPB, 2020, pp. 1–31.

[148] European Data Protection Board. *Opinion of EDPB on Interplay between ePrivacy Directive and GDPR*. Tech. rep. March. EDPB, 2019, pp. 1–25. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

[149] European data Protection Board. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*. Tech. rep. March. EDPB, 2021, pp. 1–36.

[150] European Data Protection Supervisor. *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725*. Tech. rep. EDPS, Nov. 2019. URL: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

[151] European Parliament and of the Council. *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)*. Tech. rep. Brusseks: European Parliament and of the Council, Dec. 2023, pp. 1–71. URL: http://data.europa.eu/eli/reg/2023/2854/oj.

[152] European Parliament and the Council of the European Union. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Tech. rep. European Parliament and the Council of the European Union, 2002, pp. 37–47.

[153] European Union Agency for Cybersecurity. *Data Protection Engineering*. Tech. rep. ENISA, Jan. 2022. URL: www.enisa.europa.eu..

[154] European Union Agency for Network and Information Security (ENISA). *Cyber security and resilience of smart cars. Good practices and recommendations*. Tech. rep. December. ENISA, 2017, p. 84.

[155] European Union Agency for Network and Information Security (ENISA). *Cyber security for Smart Cities*. Tech. rep. December. ENISA, 2015, pp. 249–252.

[156] European Union Agency for Network and Information Security (ENISA). *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*. Tech. rep. ENISA and JRC, 2021.

[157] European Union Agency for Network and Information Security (ENISA). *Cybersecurity Stocktaking in the CAM*. Tech. rep. November. ENISA, 2020. DOI: 10.2824/24902.

[158] European Union Agency for Network and Information Security (ENISA). *ENISA good practices for the security of smart cars*. Tech. rep. November. ENISA, 2019, p. 103.

[159] European Union Agency for Network and Information Security (ENISA). *Guidelines for Securing the Secure supply chain for IoT*. Tech. rep. November. ENISA, 2020.

[160] Tatjana Evas and Aleksandra Heflich. *Artificial intelligence in road transport*. Tech. rep. European Parliament, Jan. 2021, p. 28. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/654212/EPRS_STU(2021)654212_EN.pdf.

[161] Authors Fabian Biegel et al. *GAIA-X: Driver of digital innovation in Europe*. Tech. rep. GAIA-X, 2020.

[162] Federal Ministry for Economic Affairs and Energy. *GAIA-X: The European project kicks off the next phase*. Tech. rep. GAIA-X, 2020.

[163] Federal Office for Information Security. *BSI-Standard 100-4 Business Continuity Management*. Tech. rep. Bonn: Federal Office for Information Security (BSI), 2009.

[164] Pietro Ferrara et al. 'Static analysis for discovering IoT vulnerabilities'. In: *International Journal on Software Tools for Technology Transfer* 23.1 (Feb. 2021), pp. 71–88. ISSN: 14332787. DOI: 10.1007/s10009-020-00592-x.

[165] Akif Fidanoglu, Ilgin Gokasar and Muhammet Deveci. 'Integrating shared autonomous vehicles in Last-Mile public transportation'. In: *Sustainable Energy Technologies and Assessments* 57 (June 2023). ISSN: 22131388. DOI: 10.1016/j.seta.2023.103214.

[166] FIRST. *Common Vulnerability Scoring System SIG*. 2023. URL: https://www.first.org/cvss/.

[167] Trond Foss and Knut Evensen. *ITS standardisering*. Tech. rep. Statens vegsen, 2019. URL: https://its-norway.no/wp-content/uploads/2021/01/ITS-standardisering-SVV-rapport-482-4MB.pdf.

[168] Daniel S. Fowler et al. 'A Method for Constructing Automotive Cybersecurity Tests, a CAN Fuzz Testing Example'. In: *Proceedings - Companion of the 19th IEEE International Conference on Software Quality, Reliability and Security, QRS-C 2019*. Institute of Electrical and Electronics Engineers Inc., July 2019, pp. 1–8. ISBN: 9781728139258. DOI: 10.1109/QRS-C.2019.00015.

[169] Jack Freund and Jack Jones. 'The FAIR Risk Ontology'. In: *Measuring and Managing Information Risk*. Elsevier, 2015, pp. 25–41. DOI: 10.1016/B978-0-12-420231-3.00003-8. URL: https://linkinghub.elsevier.com/retrieve/pii/B9780124202313000038.

[170] Simon Furst and Markus Bechter. 'AUTOSAR for Connected and Autonomous Vehicles: The AUTOSAR Adaptive Platform'. In: *Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN-W 2016* (2016), pp. 215–217. DOI: 10.1109/DSN-W.2016.24.

[171] Konstantinos Fysarakis et al. 'Security Concerns in Cooperative Intelligent Transportation Systems'. In: *Taylor & Francis*. Boca Raton, FL, USA: CRC Press, Sept. 2017, pp. 487–522. ISBN: 978-1-31530583-7. DOI: 10.1201/b21885-16.

[172] David Gabay, Kemal Akkaya and Mumin Cebe. 'Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs'. In: *IEEE Transactions on Vehicular Technology* 69.6 (June 2020), pp. 5760–5772. ISSN: 0018-9545. DOI: 10.1109/TVT.2020.2977361.

[173] GAIA-X. *GAIA-X: A Federated Data Infrastructure for Europe*. URL: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

[174] Maria Cristina. Galassi et al. *ERA - JRC Workshop on Safety certification and approval of automated driving functions : analogies and exchange of best practices between railway and automotive transport sectors.* Tech. rep. European Commision, Joint Research Centre, 2021.

[175] Kevin Gavigan et al. *Vehicle Information Service Specification*. Tech. rep. W3C, 2018. URL: https://www.w3.org/TR/2018/CR-vehicle-information-service-20180213/#introduction.

[176] Damian George, Kento Reutimann and Aurelia Tamò -Larrieux. 'GDPR bypass by design? Transient processing of data under the GDPR'. In: *International Data Privacy Law* 9.4 (Nov. 2019), pp. 285–298. DOI: https://doi.org/10.1093/idpl/ipz017. URL: https://www.wired.de/collection/business/real-.

[177] Youcef Gheraibia et al. 'An Overview of the Approaches for Automotive Safety Integrity Levels Allocation'. In: *Journal of Failure Analysis and Prevention* 18.3 (June 2018), pp. 707–720. ISSN: 1547-7029. DOI: 10.1007/s11668-018-0466-9.

[178] Subhadip Ghosh et al. 'An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System'. In: *IEEE Access* 11 (2023), pp. 14752–14777. ISSN: 21693536. DOI: 10.1109/ACCESS.2023.3243906.

[179] Anastasios Giannaros et al. *Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions*. Sept. 2023. DOI: 10.3390/jcp3030025.

[180] Mansi Girdhar et al. ‘Post-Accident Cyberattack Event Analysis for Connected and Automated Vehicles’. In: *IEEE Access* 10 (2022), pp. 83176–83194. ISSN: 21693536. DOI: 10.1109/ACCESS.2022.3196346.

[181] GitHub. *GSM Description*. Jan. 2023. URL: https://github.com/0xh4di/GSMDecryption.

[182] GitHub. *Software-Defined GPS Signal Simulator*. Jan. 2023. URL: https://github.com/osqzss/gps-sdr-sim.

[183] Dorothy J Glancy. ‘Privacy in Autonomous Vehicles’. In: *Number 4 Article* 52.4 (2012), pp. 12–14.

[184] GNU Radio project. *GNU Radio - The Free & Open Source Radio Ecosystem GNU Radio*. Sept. 2022. URL: https://www.gnuradio.org.

[185] Google play. *GPS Test Applications sur Google Play*. Jan. 2023. URL: https://play.google.com/store/apps/details?id=com.chartcross.gpstest.

[186] UK-Government. *Automated and Electric Vehicles Act 2018*. Tech. rep. UKAct2018, 2018.

[187] Daniel Grimm et al. ‘Gap analysis of ISO/SAE 21434-Improving the automotive cybersecurity engineering life cycle’. In: *IEEE 26th International Conference on Intelligent Transportation Systems*. Ed. by IEEE. Bilbao, Bizkaia, Spain: IEEE, Sept. 2023. URL: http://www.ieee.org/documents/opsmanual.pdf.

[188] Dominique Gruyer et al. ‘Are Connected and Automated Vehicles the Silver Bullet for Future Transportation Challenges? Benefits and Weaknesses on Safety, Consumption, and Traffic Congestion’. In: *Frontiers in Sustainable Cities* 2 (Jan. 2021). ISSN: 26249634. DOI: 10.3389/frsc.2020.607054.

[189] GRVA UNECE. *Proposal for the Interpretation Document for UN Regulation No. [155] on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. Tech. rep. UNECE, 2020. URL: https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/WP29-182-05e.pdf.

[190] Pengwenlong Gu et al. ‘Vehicle driving pattern based sybil attack detection’. In: *Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016* (2017), pp. 1282–1288. DOI: 10.1109/HPCC-SmartCity-DSS.2016.0182.

[191] Rajesh Gupta et al. ‘Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review’. In: *Computers and Electrical Engineering* 86 (Sept. 2020). ISSN: 00457906. DOI: 10.1016/j.compeleceng.2020.106717.

[192] Trung Ha et al. ‘Differential Privacy in Deep Learning: An Overview’. In: *2019 International Conference on Advanced Computing and Applications (ACOMP)*. IEEE, Nov. 2019, pp. 97–102. ISBN: 978-1-7281-4723-9. DOI: 10.1109/ACOMP.2019.00022.

[193] Debiao He et al. 'An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks'. In: *IEEE Transactions on Information Forensics and Security* 10.12 (2015), pp. 2681–2691. ISSN: 15566013. DOI: 10.1109/TIFS.2015.2473820.

[194] Qiyi He, Xiaolin Meng and Rong Qu. 'Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles'. In: *Journal of Advanced Transportation* 2020 (2020). ISSN: 20423195. DOI: 10.1155/2020/6873273.

[195] Richard Lubomir Hes and John J. Borking. 'Privacy-Enhancing Technologies: The Path to Anonymity'. In: *Computer Science*. 1988. URL: https://www.semanticscholar.org/paper/Privacy-Enhancing-Technologies%3A-The-Path-to-Hes-Borking/b3d3c3dd5281a8625b026920d28cfdda6e39ad67.

[196] HM Government. *The key principles of vehicle cyber security for connected and automated vehicles*. Tech. rep. Department of Transport, UK, 2017.

[197] Erik Hohmann et al. 'Expert Opinion Is Necessary: Delphi Panel Methodology Facilitates a Scientific Approach to Consensus'. In: *Arthroscopy: The Journal of Arthroscopic & Related Surgery* 34.2 (Feb. 2018), pp. 349–351. ISSN: 07498063. DOI: 10.1016/j.arthro.2017.11.022. URL: https://linkinghub.elsevier.com/retrieve/pii/S0749806317314421.

[198] ICDPPC. *Resolution on Data Protection in Automated and Connected Vehicles The 38th International Conference of Data Protection and Privacy Commissioners*. Tech. rep. ICDPPC, 2017.

[199] Calin Iclodean, Nicolae Cordos and Bogdan Ovidiu Varga. 'Autonomous shuttle bus for public transportation: A review'. In: *Energies* 13.11 (2020). ISSN: 19961073. DOI: 10.3390/en13112917.

[200] Philokypros P Ioulianou et al. 'A Signature based Intrusion Detection System for the Internet of Things'. In: *Information and Communication Technology Form*. 2018.

[201] Mafijul Md. Islam et al. 'A Risk Assessment Framework for Automotive Embedded Systems'. In: *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*. New York, NY, USA: ACM, May 2016, pp. 3–14. ISBN: 9781450342889. DOI: 10.1145/2899015.2899018. URL: https://dl.acm.org/doi/10.1145/2899015.2899018.

[202] ISO. *Conformity assessment for standards writers Do's and don'ts*. Tech. rep. Geneva: International Organization for Standardization, 2015, pp. 1–24. URL: https://www.iso.org/publication/PUB100303.html.

[203] ISO. *International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and*. Tech. rep. 19. ISO/IEC, 2018, pp. 45–55. URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.

[204] ISO. *ISO - ISO 24014-1:2021 - Public transport — Interoperable fare management system — Part 1: Architecture*. Jan. 2021. URL: https://www.iso.org/standard/72507.html.

[205] ISO. *ISO - ISO/AWI TR 19560 Intelligent transport systems - Information interface framework between automated driving system and user*. Tech. rep. ISO, 2023. URL: https://www.iso.org/standard/85901.html.

[206] ISO. *ISO - ISO/SAE PAS 22736:2021 - Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*. Tech. rep. ISO, Aug. 2021.

[207] ISO. *ISO 15118-20:2022 Road vehicles - Vehicle to grid communication interface*. Tech. rep. ISO, Apr. 2022.

[208] ISO. *ISO 20077-2:2018*. 2018. URL: https://www.iso.org/standard/67597.html.

[209] ISO. *ISO 20078-3:2019*. 2019. URL: https://www.iso.org/standard/67579.html.

[210] ISO. *ISO 22737:2021*. Tech. rep. ISO, 2021. URL: https://www.iso.org/standard/73767.html.

[211] ISO. *ISO 22741-1:2022 Intelligent transport systems - Roadside modules AP-DATEX data interface*. Tech. rep. ISO, Feb. 2022.

[212] ISO. *ISO 23150:2021 Road vehicles - Data communication between sensors and data fusion unit for automated driving functions - Logical interface*. Tech. rep. ISO, May 2021.

[213] ISO. *ISO 24089 - Road vehicles - Software update engineering*. Tech. rep. ISO, Feb. 2022.

[214] ISO. *ISO 26262 Road vehicles - Functional safety*. Tech. rep. ISO, 2018.

[215] ISO. *ISO 31000:2018 - Risk management - Guidelines*. Tech. rep. ISO, 2018.

[216] ISO. *ISO 9001:2015*. 2015. URL: https://www.iso.org/standard/62085.html.

[217] ISO. *ISO/AWI 21734*. 2021. URL: https://www.iso.org/standard/71520.html.

[218] ISO. *ISO/AWI PAS 8800 Road Vehicles - Safety and artificial intelligence*. Tech. rep. ISO, 2023.

[219] ISO. *ISO/AWI TR 23254*. 2021. URL: https://www.iso.org/standard/75089.html.

[220] ISO. *ISO/AWI TS 22726*. Tech. rep. ISO, 2021. URL: https://www.iso.org/standard/73747.html.

[221] ISO. *ISO/AWI TS 5083 Road vehicles - Safety for automated driving systems - Design, verification and validation*. Tech. rep. ISO, 2023.

[222] ISO. *ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Introduction and general model*. Tech. rep. ISO, Aug. 2022.

[223] ISO. *ISO/IEC 17065: Conformity assessment - Requirements for bodies certifying products, processes and services*. Tech. rep. ISO, 2012.

[224] ISO. *ISO/IEC 18045: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation*. Tech. rep. ISO, Aug. 2022.

[225] ISO. *ISO/IEC 27001:2022, Information security management systems*. Tech. rep. ISO, Oct. 2022.

[226] ISO. *ISO/IEC 29134:2017 Information technology - Security techniques - Guidelines for privacy impact assessment*. Tech. rep. ISO, 2017.

[227] ISO. *ISO/IEC AWI 5888 Information security, cybersecurity and privacy protection - Security requirements and evaluation activities for connected vehicle devices*. Tech. rep. ISO, 2023.

[228] ISO. *ISO/IEC20243*. Tech. rep. ISO/IEC, 2018.

[229] ISO. *ISO/NP 7856*. Jan. 2022. URL: https://genorma.com/en/project/show/iso:proj:82951.

[230] ISO. *ISO/PAS 21448:2019*. 2019. URL: https://www.iso.org/standard/70939.html.

[231] ISO. *ISO/PAS 5112 - Guidelines for auditing cybersecurity engineering*. Tech. rep. ISO, Mar. 2022.

[232] ISO. *ISO/PWI TR 5255-2*. Apr. 2020. URL: https://genorma.com/en/project/show/iso:proj:81070.

[233] ISO. *ISO/SAE 21434 Road vehicles-Cybersecurity engineering*. Tech. rep. ISO/SAE, Aug. 2021.

[234] ISO. *ISO/SAE AWI 8475 - Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF)*. Tech. rep. ISO, 2023.

[235] ISO. *ISO/SAE DIS 21434*. 2021. URL: https://www.iso.org/standard/70918.html.

[236] ISO. *ISO/SAE PWI 8477 Road vehicles - Cybersecurity verification and validation*. Tech. rep. ISO, 2023.

[237] ISO. *ISO/TR 21186*. Tech. rep. CEN and ISO, 2021.

[238] ISO. *ISO/TS 21177:2019*. Tech. rep. ISO, 2019.

[239] ISO. *Stages and resources for standards development*. 2024. URL: https://www.iso.org/stages-and-resources-for-standards-development.html.

[240] ISO/IEC. *ISO/IEC 29100:2011 Information technology - Security techniques-Privacy framework*. Tech. rep. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2011. URL: https://www.iso.org/fr/standard/45123.html.

[241] ISO/TC204. *ITS Standardization Activities of ISOTC 204*. Tech. rep. ISO, 2019.

[242] ITU-T. *Focus Group on AI for autonomous and assisted driving*. 2023. URL: https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx.

[243] ITU-T. *ITU-T Recommendations*. 2021. URL: https://www.itu.int/ITU-T/recommendations/.

[244] ITU-T. *X. 1371 Security threats to connected vehicles*. Tech. rep. ITU-T, 2020.

[245] ITU-T. *X.1372 Security guidelines for vehicle-to-everything (V2X) communication*. Tech. rep. ITU-T, 2020.

[246] ITU-T. *X.1373 Secure software update capability for intelligent transportation system communication devices*. Tech. rep. ITU-T, 2017.

[247] ITU-T. *X.1374 Security requirements for external interfaces and devices with vehicle access capability*. Tech. rep. ITU-T, 2020.

[248] ITU-T. *X.1375 Guidelines for an intrusion detection system for in-vehicle networks*. Tech. rep. ITU-T, 2020.

[249] ITU-T. *X.1376 Security-related misbehaviour detection mechanism using big data for connected vehicles*. Tech. rep. ITU-T, 2021.

[250] IWGDPT. *International Working Group on Data Protection in Telecommunications*. Tech. rep. IWGDPT, 2018. URL: https://fpf.org/wp-content/uploads/.

[251] J-Auto-ISAC. *J-Auto-ISAC For the safety and security of the automobile society*. URL: https://j-auto-isac.or.jp/.

[252] JasPar. *JasPar*. 2021. URL: https://www.jaspar.jp/en.

[253] Jueun Jeon, Jong Hyuk Park and Young Sik Jeong. 'Dynamic Analysis for IoT Malware Detection with Convolution Neural Network Model'. In: *IEEE Access* 8 (2020), pp. 96899–96911. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.2995887.

[254] Rahul Johari et al. 'Penetration Testing in IoT Network'. In: *Proceedings of the 2020 International Conference on Computing, Communication and Security, ICCCS 2020*. Institute of Electrical and Electronics Engineers Inc., Oct. 2020. ISBN: 9781728191805. DOI: 10.1109/ICCCS49678.2020.9276853.

[255] Joshua Joy and Mario Gerla. 'Privacy risks in vehicle grids and autonomous cars'. In: *CarSys 2017 - Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services, co-located with MobiCom 2017* October (2017), pp. 19–23. DOI: 10.1145/3131944.3133938.

[256] Jiawen Kang et al. 'Location privacy attacks and defenses in cloud-enabled internet of vehicles'. In: *IEEE Wireless Communications* 23.5 (2016), pp. 52–59. ISSN: 1536-1284. DOI: 10.1109/MWC.2016.7721742.

[257] Min Joo Kang and Je Won Kang. 'Intrusion detection system using deep neural network for in-vehicle network security'. In: *PLoS ONE* 11.6 (2016), pp. 1–17. ISSN: 19326203. DOI: 10.1371/journal.pone.0155781.

[258] Arijit Karati et al. ‘Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments’. In: *IEEE Internet of Things Journal* 5.4 (2018), pp. 2904–2914. ISSN: 23274662. DOI: 10.1109/JIOT.2017.2741580.

[259] Bikram Karki and Myounggyu Won. ‘Characterizing Power Consumption of Dual-Frequency GNSS of Smartphone’. In: *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., Dec. 2020. ISBN: 9781728182988. DOI: 10.1109/GLOBECOM42002.2020.9322317.

[260] Stamatis Karnouskos and Florian Kerschbaum. ‘Privacy and integrity considerations in hyperconnected autonomous vehicles’. In: *Proceedings of the IEEE* 106.1 (2018), pp. 160–170. ISSN: 15582256. DOI: 10.1109/JPROC.2017.2725339.

[261] Yusuke Kawamoto and Takao Murakami. ‘On the Anonymization of Differentially Private Location Obfuscation; On the Anonymization of Differentially Private Location Obfuscation’. In: *2018 International Symposium on Information Theory and Its Applications (ISITA)* (2018).

[262] Yasuyuki Kawanishi et al. ‘A Comparative Study of JASO TP15002-Based Security Risk Assessment Methods for Connected Vehicle System Design’. In: *Security and Communication Networks* 2019 (Feb. 2019), pp. 1–35. ISSN: 1939-0114. DOI: 10 . 1155 / 2019 / 4614721. URL: https://www.hindawi.com/journals/scn/2019/4614721/.

[263] Shah Khalid Khan, Nirajan Shiwakoti and Peter Stasinopoulos. ‘A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles’. In: *Accident Analysis and Prevention* 165 (Feb. 2022). ISSN: 00014575. DOI: 10.1016/j.aap.2021.106515.

[264] Shah Khalid Khan et al. ‘Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions’. In: *Accident Analysis and Prevention* 148.October (2020), p. 105837. ISSN: 00014575. DOI: 10.1016/j.aap.2020.105837.

[265] Shah Zahid Khan, Mujahid Mohsin and Waseem Iqbal. ‘On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions’. In: *PeerJ Computer Science* 7 (2021), pp. 1–35. ISSN: 23765992. DOI: 10.7717/PEERJ-CS.507.

[266] Shapla Khanam et al. ‘A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things’. In: *IEEE Access* 8 (2020), pp. 219709–219743. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3037359.

[267] Siddartha Khastgir et al. ‘Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems’. In: *Safety Science* 99 (Nov. 2017), pp. 166–177. ISSN: 18791042. DOI: 10.1016/j.ssci.2017.03.024.

[268] Marzana Khatun, Michael Glass and Rolf Jung. 'An Approach of Scenario-Based Threat Analysis and Risk Assessment Over-the-Air updates for an Autonomous Vehicle'. In: *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*. Xi'an, China: IEEE, Feb. 2021, pp. 122–127. ISBN: 978-1-6654-0469-3. DOI: 10.1109/ICARA51699.2021.9376542. URL: https://ieeexplore.ieee.org/document/9376542/.

[269] Kyounggon Kim et al. 'Cybersecurity for autonomous vehicles: Review of attacks and defense'. In: *Computers and Security* 103 (2021), p. 102150. ISSN: 01674048. DOI: 10.1016/j.cose.2020.102150.

[270] Seokmo Kim, R. Young Chul Kim and Young B. Park. 'Software Vulnerability Detection Methodology Combined with Static and Dynamic Analysis'. In: *Wireless Personal Communications* 89.3 (Aug. 2016), pp. 777–793. ISSN: 1572834X. DOI: 10.1007/s11277-015-3152-1.

[271] Shiho Kim and Rakesh Shrestha. *Automotive Cyber Security*. Singapore: Springer Singapore, 2020. ISBN: 978-981-15-8052-9. DOI: 10.1007/978-981-15-8053-6.

[272] Barbara Kitchenham and Stuart M Charters. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Tech. rep. Durham, UK: Software Engineering Group School of Computer Science and Mathematics Keele University, 2007. URL: https://www.researchgate.net/publication/302924724.

[273] Dan Klinedinst and Christopher King. *On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle*. Tech. rep. March. 2016, p. 21.

[274] Hideaki Kobayashi et al. *Approaches for Vehicle Information Security*. Tech. rep. IPA, 2013. URL: https://www.ipa.go.jp/files/000033402.pdf.

[275] Mihai Kocsis, Raoul Zöllner and Gheorghe Mogan. 'Interactive System for Package Delivery in Pedestrian Areas Using a Self-Developed Fleet of Autonomous Vehicles'. In: *Electronics (Switzerland)* 11.5 (Mar. 2022). ISSN: 20799292. DOI: 10.3390/electronics11050748.

[276] Alyzia Maria Konsta et al. 'Survey: Automatic generation of attack trees and attack graphs'. In: *Computers and Security* 137 (Feb. 2024). ISSN: 01674048. DOI: 10.1016/j.cose.2023.103602.

[277] Dimitri Konstantas. 'From Demonstrator to Public Service: The AVENUE Experience'. In: *The Robomobility Revolution of Urban Public Transport*. Ed. by Sylvie Mira-Bonnardel, Fabio Antonialli and Danielle Attias. Springler, 2021, pp. 107–130. DOI: 10.1007/978-3-030-72976-9{_}5. URL: https://link.springer.com/10.1007/978-3-030-72976-9_5.

[278] Philip Koopman. *SAE J3016 User Guide*. Sept. 2021. URL: https://users.ece.cmu.edu/~koopman/j3016/.

[279] Anna Kosovac, Brian Davidson and Hector Malano. 'Are We Objective? A Study into the Effectiveness of Risk Measurement in the Water Industry'. In: *Sustainability* 11.5 (Feb. 2019), p. 1279. ISSN: 2071-1050. DOI: 10.3390/su11051279.

[280] KPMG. *Assessing the preparedness of 30 countries and jurisdictions in the race for autonomous vehicles 2020 Autonomous Vehi cl es Readi ness I ndex*. Tech. rep. KPMG, 2020.

[281] Ioannis Krontiris et al. 'Autonomous Vehicles: Data Protection and Ethical Considerations'. In: *Proceedings - CSCS 2020: ACM Computer Science in Cars Symposium* (2020). DOI: 10.1145/3385958.3430481.

[282] Santosh Kumar, Ashish Joshi and Aditya Raturi. 'Study on Smart Security Measures in Threat and Risk Assessment'. In: *ICAN 2022 - 3rd International Conference on Computing, Analytics and Networks - Proceedings*. Rajpura, Punjab, India: Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1–4. ISBN: 9781665499446. DOI: 10.1109/ICAN56228.2022.10007166.

[283] Immanuel Kunz and Andreas Binder. 'Application-Oriented Selection of Privacy Enhancing Technologies'. In: *Annual Privacy Forum*. Ed. by Springer. Cham: Springer International Publishing, May 2022, pp. 75–87. DOI: 10.1007/978-3-031-07315-1{_}5.

[284] Costas. Lambrinoudakis et al. *Interoperable EU risk management framework*. Tech. rep. ENISA, Jan. 2022.

[285] Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson. 'Proposing HEAVENS 2.0 – an automotive risk assessment model'. In: *Computer Science in Cars Symposium*. New York, NY, USA: ACM, Nov. 2021, pp. 1–12. ISBN: 9781450391399. DOI: 10.1145/3488904.3493378. URL: https://dl.acm.org/doi/10.1145/3488904.3493378.

[286] Le Conseil fédéral. *Protection de récepteurs GPS contre des cyberattaques*. Nov. 2022. URL: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-69896.html.

[287] Michael Lee and Travis Atkison. 'VANET applications: Past, present, and future'. In: *Vehicular Communications* 1 (2020), p. 100310. ISSN: 22142096.

[288] Wonsuk Lee et al. *Vehicle Information Access API*. Tech. rep. W3C, 2021. URL: https://rawgit.com/w3c/automotive/master/vehicle_data/vehicle_spec.html.

[289] Changle Li et al. 'Vehicle Position Correction: A Vehicular Blockchain Networks-Based GPS Error Sharing Framework'. In: *IEEE Transactions on Intelligent Transportation Systems* PP (2020), pp. 1–15. ISSN: 1524-9050. DOI: 10.1109/tits.2019.2961400.

[290] Huaxin Li et al. 'Analyzing and Preventing Data Privacy Leakage in Connected Vehicle Services'. In: *SAE Technical paper* (Apr. 2019). DOI: 10.4271/2019-01-0478.

[291] Jianping Li, Chunbing Bao and Dengsheng Wu. 'How to Design Rating Schemes of Risk Matrices: A Sequential Updating Approach'. In: *Risk Analysis* 38.1 (Jan. 2018), pp. 99–117. ISSN: 15396924. DOI: 10.1111/risa.12810.

[292] Zhen Li et al. 'A comparative study of deep learning-based vulnerability detection system'. In: *IEEE Access* 7 (2019), pp. 103184–103197. ISSN: 21693536. DOI: 10.1109/ACCESS.2019.2930578.

[293] Hazel Si Min Lim and Araz Taeihagh. 'Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications'. In: *Energies* 11.5 (2018), p. 1062. ISSN: 19961073. DOI: 10.3390/en11051062.

[294] Jaemin Lim et al. 'Preserving Location Privacy of Connected Vehicles With Highly Accurate Location Updates'. In: *IEEE Communications Letters* 21.3 (2017), pp. 540–543. ISSN: 10897798. DOI: 10.1109/LCOMM.2016.2637902.

[295] Bing-Rong Lin and Dan Kifer. 'Towards a Systematic Analysis of Privacy Definitions'. In: *Journal of Privacy and Confidentiality* 5.2 (2014), pp. 57–109. DOI: 10.29012/jpc.v5i2.631.

[296] Kun Li Lin, Chi Sheng Daniel Shih and Jia Ru Li. 'From rail to railless: Retrofitting servicing buses for safe autonomous public transportation'. In: *2019 IEEE International Conference on Embedded Software and Systems, ICESS 2019* (2019), pp. 1–8. DOI: 10.1109/ICESS.2019.8782530.

[297] Václav Linkov et al. 'Human factors in the cybersecurity of autonomous vehicles: Trends in current research'. In: *Frontiers in Psychology* 10.MAY (2019), pp. 1–7. ISSN: 16641078. DOI: 10.3389/fpsyg.2019.00995.

[298] Todd Litman. *Autonomous Vehicle Implementation Predictions*. Tech. rep. Victoria Transport Policy Institute, Jan. 2013. URL: https://www.vtpi.org/avip.pdf.

[299] Suolan Liu, Lizhi Kong and Hongyuan Wang. 'Face detection and encryption for privacy preserving in surveillance video'. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11258 LNCS (Nov. 2018), pp. 162–172. ISSN: 16113349. DOI: 10.1007/978-3-030-03338-5{_}14.

[300] Sascha Löbner et al. 'Comparison of De-Identification Techniques for Privacy Preserving Data Analysis in Vehicular Data Sharing'. In: *Computer Science in Cars Symposium*. New York, NY, USA: ACM, Nov. 2021, pp. 1–11. ISBN: 9781450391399. DOI: 10.1145/3488904.3493380.

[301] Brigitte Lonc and Pierpaolo Cincilla. 'Cooperative ITS security framework: Standards and implementations progress in Europe'. In: *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks* (2016). DOI: 10.1109/WoWMoM.2016.7523576.

[302] Ilona Loskin. 'TARA+AD Threat Analysis and Risk Assessment for Automated Driving'. PhD thesis. Jyvaskyla, Finland: University of Jyvaskyla, 2023.

[303] Manuel Lozano and Mateo Sanguino. 'Review on V2X, I2X, and P2X Communications and Their Applications: A Comprehensive Analysis over Time'. In: *Sensors* Figure 1 (2019), pp. 1–29.

[304] Zhaojun Lu, Gang Qu and Zhenglin Liu. 'A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy'. In: *IEEE Transactions on Intelligent Transportation Systems* 20.2 (2019), pp. 760–776. ISSN: 15249050. DOI: 10.1109/TITS.2018.2818888.

[305] Feng Luo et al. *Cybersecurity Testing for Automotive Domain: A Survey*. Dec. 2022. DOI: 10.3390/s22239211.

[306] Feng Luo et al. 'Threat Analysis and Risk Assessment for Connected Vehicles: A Survey'. In: *Security and Communication Networks* 2021 (Sept. 2021). Ed. by George Drosatos, pp. 1–19. ISSN: 1939-0122. DOI: 10.1155/2021/1263820. URL: https://www.hindawi.com/journals/scn/2021/1263820/.

[307] Katharine J. Mach et al. 'Unleashing expert judgment in assessment'. In: *Global Environmental Change* 44 (May 2017), pp. 1–14. ISSN: 09593780. DOI: 10.1016/j.gloenvcha.2017.02.005.

[308] Georg Macher et al. 'A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context'. In: *35th International Conference, SAFECOMP 2016*. Vol. 9922 LNCS. Trondheim: Springer, Cham, Sept. 2016, pp. 130–141. ISBN: 9783319454764. URL: https://link.springer.com/chapter/10.1007/978-3-319-45477-1_11.

[309] Georg Macher et al. 'ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell'. In: *Computer Safety, reliability, and Security*. Springer, Cham, 2020, pp. 123–135.

[310] Georg Macher et al. 'SAHARA: A Security-Aware Hazard and Risk Analysis Method'. In: *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015*. New Jersey: IEEE Conference Publications, 2015, pp. 621–624. ISBN: 9783981537048.

[311] Ralph Mader et al. 'The Car's Electronic Architecture in Motion: The Coming Transformation'. In: *42 nd International Vienna Motor Symposium 2021*. Vienna, 2021, pp. 1–17.

[312] Tambiana Madiega. *EU Legislation in Progress Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts Committees responsible*. Tech. rep. Brussells: European Parliamentary Research Service, 2023.

[313] Logan O. Mailloux et al. 'A Top Down Approach for Eliciting Systems Security Requirements for a Notional Autonomous Space System'. In: *2019 IEEE International Systems Conference (SysCon)*. IEEE, Apr. 2019, pp. 1–7. ISBN: 978-1-5386-8396-5. DOI: 10.1109/SYSCON.2019.8836929. URL: https://ieeexplore.ieee.org/document/8836929/.

[314] Shahida Malik and Weiqing Sun. ‘Analysis and Simulation of Cyber Attacks against Connected and Autonomous Vehicles’. In: *2020 International Conference on Connected and Autonomous Driving*. Institute of Electrical and Electronics Engineers Inc, Feb. 2020, pp. 62–70. ISBN: 9781728160597.

[315] Marco Mangialardo et al. ‘The full Potential of an Autonomous GNSS Signalbased Navigation System for Moon Missions’. In: Oct. 2021, pp. 1039–1052. DOI: 10.33012/2021.18040.

[316] D Manivannan, Shafika Showkat Moni and Sherali Zeadally. ‘Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)’. In: *Vehicular Communications* 25 (2020), p. 100247. ISSN: 22142096. DOI: 10.1016/j.vehcom.2020.100247.

[317] Carsten Maple et al. ‘A connected and autonomous vehicle reference architecture for attack surface analysis’. In: *Applied Sciences (Switzerland)* 9.23 (2019). ISSN: 20763417. DOI: 10.3390/app9235101.

[318] Pablo Marin-Plaza et al. ‘Project ARES: Driverless Transportation System. Challenges and Approaches in an Unstructured Road’. In: *Electronics* 10.15 (July 2021), p. 1753. ISSN: 2079-9292. DOI: 10.3390/electronics10151753.

[319] Stefan Marksteiner and Slava Bronfman. ‘Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing’. In: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Ed. by IEEE. 2021, pp. 123–128. DOI: 0.1109/EuroSPW54576.2021.00020.

[320] Stefan Marksteiner and Zhendong Ma. ‘Approaching the automation of cyber security testing of connected vehicles’. In: *ACM International Conference Proceeding Series* (2019), pp. 4–6. DOI: 10.1145/3360664.3360729.

[321] Stefan Marksteiner et al. ‘A Process to Facilitate Automated Automotive Cybersecurity Testing’. In: *2021 IEEE 93rd Vehicular Technology Conference*. Vol. 2021-April. IEEE Inc, Apr. 2021, pp. 1–7. ISBN: 9781728189642.

[322] Stefan F Marksteiner et al. ‘From TARA to Test: Automated Automotive Cybersecurity Test Generation Out of Threat Modeling’. In: *Proceedings of the 7th ACM Computer Science in Cars Symposium*. New York, NY, USA: ACM, Dec. 2023, pp. 1–10. ISBN: 9798400704543. DOI: 10.1145/3631204.3631864. URL: https://dl.acm.org/doi/10.1145/3631204.3631864.

[323] Tomás de J. Mateo Sanguino, José M Lozano Domínguez and Patrícia de Carvalho Baptista. ‘Chapter Four - Cybersecurity certification and auditing of automotive industry’. In: *Policy Implications of Autonomous Vehicles*. Ed. by Dimitris Milakis, Nikolas Thomopoulos and Bert van Wee. Vol. 5. Advances in Transport Policy and Planning. Academic Press, 2020, pp. 95–124. DOI: 10.1016/bs.atpp.2020.01.002.

[324] Matt Lewis. *The Automotive Threat Modeling Template*. July 2016. URL: https://research.nccgroup.com/2016/07/20/the-automotive-threat-modeling-template/.

[325] Sahar Mazloom et al. 'A security analysis of an in vehicle infotainment and app platform'. In: *10th USENIX Workshop on Offensive Technologies, WOOT 2016* (2016).

[326] Scott McLachlan et al. 'Tempting the Fate of the furious: cyber security and autonomous cars'. In: *International Review of Law, Computers and Technology* 36.2 (2022), pp. 181–201. ISSN: 13646885. DOI: 10.1080/13600869.2022.2060466.

[327] METI. *Cyber Security Measures in Automated Driving Systems*. Tech. rep. Ministry of Economy, Trade and Industry, 2018.

[328] Jonas Meyer et al. 'Autonomous vehicles: The next jump in accessibilities?' In: *Research in Transportation Economics* 62 (2017), pp. 80–91. ISSN: 07398859. DOI: 10.1016/j.retrec.2017.03.005.

[329] Microsoft. *Microsoft Threat Modeling Tool*. 2023. URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model.

[330] Charlie Miller and Chris Valasek. 'Remote Exploitation of an Unaltered Passenger Vehicle'. In: *Defcon 23* 2015 (2015), pp. 1–91.

[331] Jean Philippe Monteuuis et al. 'Sara: Security automotive risk analysis method'. In: *CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-located with ASIA CCS 2018*. New York: Association for Computing Machinery, Inc, May 2018, pp. 3–14. ISBN: 9781450357555. DOI: 10.1145/3198458.3198465.

[332] Noha Moselhy and Ahmed Adel Mahmoud. 'Standardization of Cybersecurity Concepts in Automotive Process Models: An Assessment Tool Proposal'. In: *FICC 2023: Advances in Information and Communication*. Cham: Springer, Mar. 2023, pp. 635–655. DOI: 10.1007/978-3-031-28073-3{_}44.

[333] Lama J. Moukahal, Mohammad Zulkernine and Martin Soukup. 'Vulnerability-Oriented Fuzz Testing for Connected Autonomous Vehicle Systems'. In: *IEEE Transactions on Reliability* 70.4 (Dec. 2021), pp. 1422–1437. ISSN: 15581721. DOI: 10.1109/TR.2021.3112538.

[334] Khan Muhammad et al. 'Secure surveillance framework for IoT systems using probabilistic image encryption'. In: *IEEE Transactions on Industrial Informatics* 14.8 (Aug. 2018), pp. 3679–3689. ISSN: 15513203. DOI: 10.1109/TII.2018.2791944.

[335] T. Mulder and N. Vellinga. 'Handing over the wheel, giving up your privacy?' In: *13th ITS Europe Congress*. 2019.

[336] Trix Mulder and Nynke E. Vellinga. 'Exploring data protection challenges of automated driving'. In: *Computer Law and Security Review* 40 (2021), p. 105530. ISSN: 02673649. DOI: 10.1016/j.clsr.2021.105530. URL: https://doi.org/10.1016/j.clsr.2021.105530.

[337] Takao Murakami. ‘A Succinct Model for Re-identification of Mobility Traces Based on Small Training Data; A Succinct Model for Re-identification of Mobility Traces Based on Small Training Data’. In: *2018 International Symposium on Information Theory and Its Applications (ISITA)* (2018).

[338] Erion Murati and Manjola Hënkoja. ‘Location Data Privacy on MaaS under GDPR’. In: *European Journal of Privacy Law & Technologies* (2019). ISSN: ISSN 2704-8012.

[339] Suntherasvaran Murthy et al. ‘A Comparative Study of Data Anonymization Techniques’. In: *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. 2019, pp. 306–309. ISBN: 9781728100067. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00063.

[340] Muhammad Faheem Mushtaq et al. ‘A Survey on the Cryptographic Encryption Algorithms’. In: *IJACSA International Journal of Advanced Computer Science and Applications* 8.11 (2017), pp. 333–344. DOI: 10.14569/IJACSA.2017.081141.

[341] Clare Mutzenich et al. *Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles*. Dec. 2021. DOI: 10.1186/s41235-021-00271-8.

[342] National Aeronautics and Space Administration. *NASA’s Archive of Space Geodesy Data*. 2023. URL: https://cddis.nasa.gov/.

[343] National Institute of Standards and Technology and US Department of Commerce. *National Vulnerability Database*. URL: https://nvd.nist.gov/vuln/full-listing.

[344] National Science and Technology Council and the United States Department of Transportation. *Ensuring American Leadership in Automated Vehicle Technologies, Automated Vehicles 4.0*. Tech. rep. January. US Government, 2020, p. 56. URL: https://www.transportation.gov/av/4.

[345] T K Nayak, S A Adeshiyan and C Zhang. ‘A Concise Theory of Randomized Response Techniques for Privacy and Confidentiality Protection’. In: *Handbook of Statistics* 34.December (2016), pp. 273–286. ISSN: 01697161. DOI: 10.1016/bs.host.2016.01.015.

[346] Hoang Nga Nguyen et al. ‘Developing a QRNG ECU for automotive security: Experience of testing in the real-world’. In: *Proceedings - 2019 IEEE 12th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2019*. Institute of Electrical and Electronics Engineers Inc., Apr. 2019, pp. 61–68. ISBN: 9781728108889. DOI: 10.1109/ICSTW.2019.00033.

[347] Kim Thuat Nguyen, Maryline Laurent and Nouha Oualha. ‘Survey on secure communication protocols for the Internet of Things’. In: *Ad Hoc Networks* 32 (Sept. 2015), pp. 17–31. ISSN: 15708705. DOI: 10.1016/j.adhoc.2015.01.006.

[348] NHTSA. *Automated Driving Systems A vision for Safety*. Tech. rep. NHTSA, 2017.

[349] NHTSA. *Automated Vehicles for Safety*. Oct. 2022. URL: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

[350] NHTSA. *Vehicle Cybersecurity*. 2021. URL: https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.

[351] Calvin Nobles et al. 'Driving Into Cybersecurity Trouble With Autonomous Vehicles'. In: *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems*. Mar. 2023, pp. 255–273. DOI: 10.4018/978-1-6684-7207-1.ch013.

[352] Jaewon Noh, Sangil Jeon and Sunghyun Cho. 'Distributed blockchain-based message authentication scheme for connected vehicles'. In: *Electronics (Switzerland)* 9.1 (2020). ISSN: 20799292. DOI: 10.3390/electronics9010074.

[353] Nuand. *bladeRF x40*. Jan. 2023. URL: https://www.nuand.com/product/bladerf-x40.

[354] Anthony O'Hagan. 'Expert Knowledge Elicitation: Subjective but Scientific'. In: *American Statistician* 73.sup1 (Mar. 2019), pp. 69–81. ISSN: 15372731. DOI: 10.1080/00031305.2018.1518265.

[355] Lubna Obaid et al. 'Environmental impacts of the transition to automated vehicles: A life cycle perspective'. In: *Sustainable Materials and Technologies* 38 (Dec. 2023). ISSN: 22149937. DOI: 10.1016/j.susmat.2023.e00725.

[356] Office fédéral de la communication OFCOM. *Perturbateurs (jammers)*. Nov. 2022. URL: https://www.bakom.admin.ch/bakom/fr/page-daccueil/appareils-et-installations/equipements-particuliers/perturbateurs-jammers.html.

[357] Office feédeéral des routes. *Complément au Rapport final de l'étude de suivi HEIA-FR*. Tech. rep. Transports publics fribourgeois, May 2020. URL: https://www.astra.admin.ch/dam/astra/fr/dokumente/abteilung_strassennetzeallgemein/marly-mic-complement-rapport-final.pdf.download.pdf/Compl%C3%A9ment%20au%20Rapport%20final%20de%201%E2%80%99%C3%A9tude%20de%20suivi%20HEIA-FR.pdf.

[358] Chuka Oham et al. 'B-FERL: Blockchain based framework for securing smart vehicles'. In: *Information Processing and Management* 58.1 (2021), p. 102426. ISSN: 03064573. DOI: 10.1016/j.ipm.2020.102426. URL: https://doi.org/10.1016/j.ipm.2020.102426.

[359] OneTrust Data Guidance. *Comparing privacy laws: GDPR vs PIPEDA*. Tech. rep. OneTrust DataGuidance, 2019. URL: https://www.dataguidance.com/sites/default/files/gdpr_v_pipeda.pdf.

[360] openpilot. *Open source advanced driver assistance system*. 2023. URL: https://comma.ai/openpilot.

[361] Zakariae El Ouazzani and Hanan El Bakkali. 'A Classification of non-Cryptographic Anonymization Techniques ensuring Privacy in Big Data'. In: *International Journal of Communication Networks and Information Security (IJCNIS* 12.1 (2020).

[362] Oxford English dictionary. *Home : Oxford English Dictionary*. 2021. URL: https://www.oed.com/.

[363] L. Pan et al. 'Cyber security attacks to modern vehicular systems'. In: *Journal of Information Security and Applications* 36 (2017), pp. 90–100. ISSN: 22142126. DOI: 10.1016/j.jisa.2017.08.005. URL: https://doi.org/10.1016/j.jisa.2017.08.005.

[364] Sebastian Pape et al. 'A Systematic Approach for Automotive Privacy Management'. In: *7th ACM Computer Science in Cars Symposium (CSCS)*. Association for Computing Machinery (ACM), Dec. 2023, pp. 1–12. ISBN: 9798400704543. DOI: 10.1145/3631204.3631863.

[365] Seonghyeon Park et al. 'A real-time high-speed autonomous driving based on a low-cost RTK-GPS'. In: *Journal of Real-Time Image Processing*. Vol. 18. 4. Springer Science and Business Media Deutschland GmbH, Aug. 2021, pp. 1321–1330. DOI: 10.1007/s11554-021-01084-0.

[366] Seunghyun Park and Hyunhee Park. 'PIER: cyber-resilient risk assessment model for connected and autonomous vehicles'. In: *Wireless Networks* (Aug. 2022). ISSN: 1022-0038. DOI: 10.1007/s11276-022-03084-9. URL: https://link.springer.com/10.1007/s11276-022-03084-9.

[367] Simon Parkinson et al. 'Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges'. In: *IEEE Transactions on Intelligent Transportation Systems* 18.11 (2017), pp. 2898–2915. ISSN: 15249050. DOI: 10.1109/TITS.2017.2665968.

[368] Shakila Bu-Pasha. 'Location Data, Personal Data Protection and Privacy in Mobile Device Usage: An EU Law Perspective'. PhD thesis. Helsink: Faculty of Law, Dec. 2018. ISBN: 978-951-51-4660-1. URL: https://researchportal.helsinki.fi/en/publications/location-data-personal-data-protection-and-privacy-in-mobile-devi.

[369] Jo Ann Pattinson, Haibo Chen and Subhajit Basu. 'Legal issues in automated vehicles: critically considering the potential role of consent and interactive digital interfaces'. In: *Humanities and Social Sciences Communications* 7.1 (2020). ISSN: 26629992. DOI: 10.1057/s41599-020-00644-2.

[370] Personal Information Protection Commission. *Amended Act on the Protection of Personal Information*. Tech. rep. PPC, 2016. URL: https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf.

[371] Mert D. Pesé, Karsten Schmidt and Harald Zweck. 'Hardware/Software Co-Design of an Automotive Embedded Firewall'. In: *SAE Technical Papers*. Vol. 2017-March. March. SAE International, Mar. 2017. DOI: 10.4271/2017-01-1659.

[372] Jonathan Petit and Steven E Shladover. ‘Potential Cyberattacks on Automated Vehicles’. In: *IEEE Transactions on Intelligent Transportation Systems* 16.2 (2015), pp. 546–556. ISSN: 15249050. DOI: 10.1109/TITS.2014.2342271.

[373] Jonathan; Petit et al. ‘Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR’. In: *Blackhat.com* (2015), pp. 1–13.

[374] Christian Plappert et al. ‘Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain’. In: *Proceedings - 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2021*. Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 266–275. ISBN: 9781665414555. DOI: 10.1109/PDP52278.2021.00050.

[375] Preeti Wadhwani and Prasenjit Saha. *Autonomous Bus Market Trends 2022-2028, Size Analysis Report*. Tech. rep. Global Market Insights, 2021. URL: https://www.gminsights.com/industry-analysis/autonomous-bus-market.

[376] PyPi. *Welcome to the rfcat project*. Jan. 2023. URL: https://pypi.org/project/rfcat.

[377] Marvin Rausand and Stein Haugen. *Risk Assessment*. 2020th ed. New Jersey: Wiley, Mar. 2020. ISBN: 9781119377238. DOI: 10 . 1002 / 9781119377351. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119377351.

[378] Kui Ren et al. ‘The Security of Autonomous Driving: Threats, Defenses, and Future Directions’. In: *Proceedings of the IEEE* 108.2 (2020), pp. 357–372. ISSN: 15582256. DOI: 10.1109/JPROC.2019.2948775.

[379] Elena Reshetova and Michael McCool. *Web of Things (WoT) Security and Privacy Guidelines*. Tech. rep. W3C, 2019. URL: https://www.w3.org/TR/2019/NOTE-wot-security-20191106/.

[380] Zeinab El-Rewini et al. ‘Cybersecurity challenges in vehicular communications’. In: *Vehicular Communications* 23 (2020), p. 100214. ISSN: 22142096. DOI: 10.1016/j.vehcom.2019.100214.

[381] Sergio Luís Ribeiro and Emilio Tissato Nakamura. ‘Privacy Protection with Pseudonymization and Anonymization in a Health IoT System: Results from OCARIoT’. In: *Proceedings - 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering, BIBE 2019*. Institute of Electrical and Electronics Engineers Inc., Oct. 2019, pp. 904–908. ISBN: 9781728146171. DOI: 10.1109/BIBE.2019.00169.

[382] Alastair R Ruddle and Michael Friedewald. *Security requirements for automotive on-board networks based on dark-side scenarios*. Tech. rep. European Commission, Mar. 2009. URL: https://www.researchgate.net/publication/46307752.

[383] Rebecca Russell et al. 'Automated Vulnerability Detection in Source Code Using Deep Representation Learning'. In: *Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018* Ml (2019), pp. 757–762. DOI: 10.1109/ICMLA.2018.00120.

[384] Aiman Al-Sabaawi et al. 'Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges'. In: *Malware Analysis Using Artificial Intelligence and Deep Learning*. Cham, Switzerland: Springer, Dec. 2020, pp. 97–119.

[385] SAE. *J3016B Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Tech. rep. SAE, 2018, p. 35.

[386] SAE. *SAE J2735 Surface Vehicle Standard*. Tech. rep. SAE, Nov. 2020.

[387] SAE. *SAE J3061- Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Tech. rep. Society of Automotive Engineering, Dec. 2021.

[388] SAE. *Surface Vehicle Information Report*. Tech. rep. SAE, July 2021.

[389] SAE International. *SAE J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Tech. rep. SAE international, Apr. 2021.

[390] S. Sangeetha and G. Sudha Sadasivam. 'Privacy of Big Data: A Review'. In: *Handbook of Big Data and IoT Security* (2019), pp. 5–23. DOI: 10.1007/978-3-030-10543-3{_}2. URL: https://link.springer.com/chapter/10.1007/978-3-030-10543-3_2.

[391] Arman Sargolzaei. *Security of Cyber-Physical Systems*. Ed. by Arman Sargolzaei. MDPI, May 2022. ISBN: 978-3-0365-4145-7. DOI: 10 . 3390 / books978 - 3 - 0365 - 4145 - 7. URL: https://www.mdpi.com/books/pdfview/book/5448.

[392] Ankur Sarker et al. 'A Review of Sensing and Communication, Human Factors, and Controller Aspects for Information-Aware Connected and Automated Vehicles'. In: *IEEE Transactions on Intelligent Transportation Systems* 21.1 (2020), pp. 7–29. ISSN: 15580016. DOI: 10.1109/TITS.2019.2892399.

[393] Christian Schlager et al. 'Consistency of Cybersecurity Process and Product Assessments in the Automotive Domain'. In: *Communications in Computer and Information Science*. Vol. 1890 CCIS. Springer Science and Business Media Deutschland GmbH, 2023, pp. 343–355. ISBN: 9783031423062. DOI: 10.1007/978-3-031-42307-9{_}24.

[394] Christoph Schmittner, Zhendong Ma and Paul Smith. 'FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles'. In: *International Conference on Computer Safety, Reliability, and Security SAFECOMP 2014*. Cham: Springer, 2014, pp. 282–288. URL: http://link.springer.com/10.1007/978-3-319-10557-4_31.

[395] Christoph Schmittner and Georg Macher. 'Automotive Cybersecurity Standards - Relation and Overview'. In: *Lecture Notes in Computer Science*. Vol. 11699 LNCS. Springer, Cham, Sept. 2019, pp. 153–165. ISBN: 9783030262495.

[396] Christoph Schmittner, Bernhard Schrammel and Sandra Konig. 'Asset Driven ISO/SAE 21434 Compliant Automotive Cybersecurity Analysis with ThreatGet'. In: *European Conference on Software Process Improvement EuroSpi2021*. Ed. by Springer Nature Switzerland AG. Vol. 1442. Cham: Springer Nature Switzerland AG, 2021, pp. 548–563. ISBN: 9783030855208.

[397] Christoph Schmittner et al. 'Using SAE J3061 for automotive security requirement engineering'. In: *International Conference on Computer Safety, Reliability, and Security*. Vol. 9923 LNCS. Springer Verlag, 2016, pp. 157–170. ISBN: 9783319454795.

[398] Erwin Schoitsch and Christoph Schmittner. 'Ongoing Cybersecurity and Safety Standardization Activities Related to Highly Automated/Autonomous Vehicles'. In: *Intelligent System Solutions for Auto Mobility and Beyond*. Springer, Cham, Dec. 2020, pp. 72–86. ISBN: 978-3-030-65871-7.

[399] Barry Sheehan et al. 'Connected and autonomous vehicles: A cyber-risk classification framework'. In: *Transportation Research Part A: Policy and Practice* 124 (2019), pp. 523–536. ISSN: 09658564. DOI: `10.1016/j.tra.2018.06.033`.

[400] Hocheol Shin et al. 'Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications'. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10529 LNCS (2017), pp. 445–467. ISSN: 16113349. DOI: `10.1007/978-3-319-66787-4{\_}22`.

[401] Show Consortium. *Show project*. 2022. URL: https://show-project.eu/.

[402] Charlie Simpson et al. *Mobility 2030: Transforming the mobility landscape*. Tech. rep. KPMG, Feb. 2019.

[403] Laurens Sion. 'Automated Threat Analysis for Security and Privacy'. PhD thesis. Leuven, Belgium: KU Leuven, Oct. 2020, pp. 1–232.

[404] Laurens Sion et al. 'Solution-aware data flow diagrams for security threat modeling'. In: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. New York, NY, USA: ACM, Apr. 2018, pp. 1425–1432. ISBN: 9781450351911. DOI: `10.1145/3167132.3167285`.

[405] Mirosław Śmieszek and Magdalena Dobrzańska. 'Application of Kalman filter in navigation process of automated guided vehicles'. In: *Metrology and Measurement Systems* 22.3 (2015), pp. 443–454. ISSN: 23001941. DOI: `10.1515/mms-2015-0037`.

[406] Göran Smith and Göran Smith. *Making Mobility-as-a-Service*. Gothenburg: Chalmers University of Technology, 2020. ISBN: 9789179052973.

[407] Florian Sommer, Jürgen Dürrwang and Reiner Kriesten. 'Survey and classification of automotive security attacks'. In: *Information (Switzerland)* 10.4 (2019). ISSN: 20782489. DOI: `10.3390/info10040148`.

[408] Standardization Administration of PRC. *GB/T 20984-2007 Information security technology - Risk assessment specification for information security*. Tech. rep. General Adminstration of Quality Supervision Inspection and Quarantine, 2007. URL: https://www.chinesestandard.net/PDF.aspx/GBT20984-2007.

[409] Kim Strandberg, Tomas Olovsson and Erland Jonsson. ‘Securing the Connected Car: A Security-Enhancement Methodology’. In: *IEEE Vehicular Technology Magazine* 13.1 (Mar. 2018), pp. 56–65. ISSN: 15566072. DOI: 10.1109/MVT.2017.2758179.

[410] Sang-Bum Suh. *Understanding the UNECE WP.29 Cybersecurity Regulation | PERSEUS*. 2020. URL: https://cyberperseus.com/understanding-the-unece-wp-29-cybersecurity-regulation/.

[411] Aifen Sui and Gordon Muehl. ‘Security for Autonomous Vehicle Networks’. In: *ICEICT 2020 - IEEE 3rd International Conference on Electronic Information and Communication Technology*. Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 67–69. ISBN: 9781728190457.

[412] Xiaoqiang Sun, F. Richard Yu and Peng Zhang. ‘A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)’. In: *IEEE Transactions on Intelligent Transportation Systems* 23.7 (July 2022), pp. 6240–6259. ISSN: 1524-9050. DOI: 10.1109/TITS.2021.3085297.

[413] Dajiang Suo et al. ‘Location-Based Schemes for Mitigating Cyber Threats on Connected and Automated Vehicles: A Survey and Design Framework’. In: *IEEE Transactions on Intelligent Transportation Systems* (2020), pp. 1–19. ISSN: 15580016. DOI: 10.1109/TITS.2020.3038755.

[414] Chitanut Tachepun and Sotarat Thammaboosadee. ‘A Data Masking Guideline for Optimizing Insights and Privacy Under GDPR Compliance’. In: *Proceedings of the 11th International Conference on Advances in Information Technology*. New York, NY, USA: ACM, July 2020, pp. 1–9. ISBN: 9781450377591. DOI: 10.1145/3406601.3406627.

[415] Araz Taeihagh and Hazel Si Min Lim. ‘Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks’. In: *arXiv* (2018).

[416] Junko Takahashi et al. ‘Automotive attacks and countermeasures on LIN-Bus’. In: *Journal of Information Processing* 25.3 (2017), pp. 220–228. ISSN: 18826652. DOI: 10.2197/ipsjjip.25.220.

[417] Nazanin Takbiri et al. ‘Limits of location privacy under anonymization and obfuscation’. In: *IEEE International Symposium on Information Theory - Proceedings* (2017), pp. 764–768. ISSN: 21578095. DOI: 10.1109/ISIT.2017.8006631.

[418] Akiyoshi Tashiro et al. ‘A secure protocol consisting of two different security-level message authentications over CAN’. In: *2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017* 2018-Janua (2018), pp. 1520–1524. DOI: 10.1109/CompComm.2017.8322794.

[419] The Avenue Consortium. *AVENUE – EU funded project under Horizon 2020*. 2022. URL: https://h2020-avenue.eu/.

[420] The Data Protection WG of the C-ITS Platform. *C-ITS Platform Final Report*. Tech. rep. C-ITS Platform, 2016.

[421] The European Parliament and of the Council. *Regulation (Eu) 2019/2144*. Tech. rep. 715. European Union, 2019, ANNEX II.

[422] The European Parliament and the Council of the European Union. *Directive (EU) 2016/ 1148 of the European Parliament and of the Council - NIS Directive 1*. Tech. rep. European Commission, 2016.

[423] The European Parliament and the Council of the European Union. *Proposal for a Directive (EU) 2016/ 1148 of the European Parliament and of the Council - NIS Directive 2*. Tech. rep. Brussels: European Commission, 2020.

[424] The European Parliament and the Council of the European Union. *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. Tech. rep. European Commission, 2016, pp. 16–32.

[425] The UK Centre for Connected and Autonomous Vehicles. *Innovation is Great: connected and automated vehicles*. Tech. rep. Department of Transport, UK, 2020.

[426] Jonay Toledo et al. 'Improving odometric accuracy for an autonomous electric cart'. In: *Sensors (Switzerland)* 18.1 (2018). ISSN: 14248220. DOI: 10.3390/s18010200.

[427] Ceara Treacy, John Loane and Fergal McCaffery. 'A Developer Driven Framework for Security and Privacy in the Internet of Medical Things'. In: *Communications in Computer and Information Science*. Vol. 1251 CCIS. Springer, 2020, pp. 107–119. ISBN: 9783030564407. DOI: 10.1007/978-3-030-56441-4{_}8.

[428] Tony Ucedavélez and Marco M. Morana. *Risk Centric Threat Modeling*. Hoboken, NJ, USA: John Wiley & Sons, Inc, June 2015. ISBN: 9781118988374. DOI: 10.1002/9781118988374.

[429] UNECE. *Proposal for draft guidelines on cyber security and data protection Submitted by the Informal Working Group on Intelligent Transport Systems / Automated Driving**. Tech. rep. UNECE, 2016.

[430] UNECE. *R155*. Tech. rep. UNECE, 2020, pp. 1–194.

[431] UNECE. *R156*. Tech. rep. April. UNECE, 2020, pp. 1–194.

[432] UNECE. *Revised Framework document on automated/autonomous vehicles*. Tech. rep. UNECE, 2019. URL: https://undocs.org/ECE/TRANS/WP.29/2019/34/REV.2.

[433] Upstream Security. *Global Automotive Cybersecurity Report 2019*. Tech. rep. Upstream Security, 2018, p. 28.

[434] Upstream Security Ltd. *Upstream: Threat Analysis and Risk Assessment Tool*. 2024. URL: https://upstream.auto/threat-analysis-and-risk-assessment/.

[435] USBKill. *USBKill V4*. Nov. 2022. URL: https://usbkill.com/products/usbkill-v4?variant=32836117397586.

[436] Vijay K. Vaishnavi, Vijay K. Vaishnavi and William Kuechler. *Design Science Research Methods and Patterns*. CRC Press, May 2015. ISBN: 9780429172205. DOI: 10.1201/b18448.

[437] Félicien Vallet. 'The GDPR and Its Application in Connected Vehicles—Compliance and Good Practices'. In: *Electronic Components and Systems for Automotive Applications*. Springer, 2019, pp. 245–254. DOI: 10.1007/978-3-030-14156-1{_}21.

[438] DImitri Van Landuyt and Wouter Joosen. 'A descriptive study of assumptions made in LINDDUN privacy threat elicitation'. In: *Proceedings of the ACM Symposium on Applied Computing*. Association for Computing Machinery, Mar. 2020, pp. 1280–1287. ISBN: 9781450368667. DOI: 10.1145/3341105.3375762.

[439] Franco Van Wyk et al. 'Real-time sensor anomaly detection and identification in automated vehicles'. In: *IEEE Transactions on Intelligent Transportation Systems* 21.3 (2020), pp. 1264–1276. ISSN: 15580016. DOI: 10.1109/TITS.2019.2906038.

[440] Vector. *VectorCAST: Software Test Automation for High Quality Software*. 2024. URL: https://www.vector.com/int/en/products/products-a-z/software/vectorcast/#c88480.

[441] Viktoras Kabir Veitas and Simon Delaere. 'In-vehicle data recording, storage and access management in autonomous vehicles'. In: *arXiv* May (2018). ISSN: 23318422.

[442] Gorka Velez et al. '5G beyond 3GPP release 15 for connected automated mobility in cross-border contexts'. In: *Sensors (Switzerland)* 20.22 (Nov. 2020), pp. 1–19. ISSN: 14248220. DOI: 10.3390/s20226622.

[443] Tom Vogt et al. 'A Comprehensive Risk Management Approach to Information Security in Intelligent Transport Systems'. In: *SAE International Journal of Transportation Cybersecurity and Privacy* 4.1 (May 2021), pp. 11–04. ISSN: 2572-1054. DOI: 10 . 4271 / 11 - 04 - 01 - 0003. URL: https://www.sae.org/content/11-04-01-0003/.

[444] Kerstin N. Vokinger, Daniel J. Stekhoven and Michael Krauthammer. 'Lost in Anonymization — A Data Anonymization Reference Classification Merging Legal and Technical Considerations'. In: *Journal of Law, Medicine and Ethics* 48.1 (Mar. 2020), pp. 228–231. ISSN: 1748720X. DOI: 10.1177/1073110520917025.

[445] W3C. *Documents published at W3C*. URL: https://www.w3.org/standards/types#eddraft-note.

[446] Zhiguo Wan et al. ‘Zk-AuthFeed: How to feed authenticated data into smart contract with zero knowledge’. In: *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019* (2019), pp. 83–90. DOI: 10.1109/Blockchain.2019.00020.

[447] Fei Wang et al. ‘2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET’. In: *IEEE Transactions on Vehicular Technology* 65.2 (2016), pp. 896–911. ISSN: 00189545. DOI: 10.1109/TVT.2015.2402166.

[448] Jinbao Wang, Zhipeng Cai and Jiguo Yu. ‘Achieving Personalized k-Anonymity-Based Content Privacy for Autonomous Vehicles in CPS’. In: *IEEE Transactions on Industrial Informatics* 16.6 (June 2020), pp. 4242–4251. ISSN: 19410050. DOI: 10.1109/TII.2019.2950057.

[449] Yiyang Wang, Neda Masoud and Anahita Khojandi. ‘Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors’. In: *arXiv* 21.3 (2019), pp. 1264–1276. ISSN: 1524-9050. DOI: 10.1109/tits.2020.2970295.

[450] Yue Wang, Xintao Wu and Donghui Hu. ‘Using randomized response for differential privacy preserving data collection’. In: *CEUR Workshop Proceedings* 1558 (2016). ISSN: 16130073.

[451] Yunpeng Wang et al. ‘A Systematic Risk Assessment Framework of Automotive Cybersecurity’. In: *Automotive Innovation* 4.3 (Aug. 2021), pp. 253–261. ISSN: 25228765. DOI: 10.1007/s42154-021-00140-6.

[452] Yunpeng Wang et al. ‘A Systematic Risk Assessment Framework of Automotive Cybersecurity’. In: *Automotive Innovation* 4.3 (Aug. 2021), pp. 253–261. ISSN: 25228765. DOI: 10.1007/s42154-021-00140-6.

[453] David Ward and Paul Wooderson. *Automotive Cybersecurity: An Introduction to ISO/SAE 21434*. SAE International, Dec. 2021, pp. i–xii. ISBN: 9781468600810. DOI: 10.4271/9781468600810.

[454] Ta Chun Wen et al. ‘A flexible risk assessment approach integrating subjective and objective weights under uncertainty’. In: *Engineering Applications of Artificial Intelligence* 103 (Aug. 2021). ISSN: 09521976. DOI: 10.1016/j.engappai.2021.104310.

[455] Konstanze Winter et al. ‘Identifying user classes for shared and automated mobility services’. In: *European Transport Research Review* 12.1 (Dec. 2020). ISSN: 18668887. DOI: 10.1186/s12544-020-00420-y.

[456] Wireshark. *About Wireshark*. Jan. 2023. URL: https://www.wireshark.org.

[457] Libing Wu et al. ‘Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks’. In: *International Journal of Distributed Sensor Networks* 13.3 (2017). ISSN: 15501477. DOI: 10.1177/1550147717700899.

[458] Wufei Wu et al. ‘A survey of intrusion detection for in-vehicle networks’. In: *IEEE Transactions on Intelligent Transportation Systems* 21.3 (2020), pp. 919–933. ISSN: 15580016. DOI: 10.1109/TITS.2019.2908074.

[459] Kim Wuyts and Wouter Joosen. *LINDDUN privacy threat modeling: a tutorial*. Tech. rep. Heverlee: Katholieke Universiteit Leuven, July 2015, pp. 1–38.

[460] Kim Wuyts, Laurens Sion and Wouter Joosen. *LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling*. Tech. rep. LINDDUN.org, 2020. URL: `https://adam.shostack.org/games.html`.

[461] Wenyuan Xu et al. 'Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles'. In: *IEEE Internet of Things Journal* 5.6 (2018), pp. 5015–5029. ISSN: 23274662. DOI: `10.1109/JIOT.2018.2867917`.

[462] Chen Yan, Wenyuan Xu and Jianhao Liu. 'Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle'. In: *DEFCON* 24.8 (2016), p. 109.

[463] YateBTS. *LTE & GSM mobile network components for MNO & MVNO*. Aug. 2021. URL: `https://yatebts.com`.

[464] Yakouta Zarouk and Ismahane Souici. 'Privacy Protection in Video Surveillance System using Enhanced Evolutionary Encryption Algorithm'. In: *2nd International Conference on Signal, Image, Vision and their Applications , SIVA'2013*. April 2020. Researchgate, 2013.

[465] Daniel Zelle et al. 'ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering'. In: *Microprocessors and Microsystems* 90.104461 (Apr. 2022), p. 104461. ISSN: 01419331. DOI: `10.1016/j.micpro.2022.104461`. URL: `https://linkinghub.elsevier.com/retrieve/pii/S0141933122000321`.

[466] Kexiong Zeng et al. 'All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems'. In: *Proceedings of the 27th USENIX Security Symposium* (2018).

[467] Tao Zhang, Helder Antunes and Siddhartha Aggarwal. 'Defending connected vehicles against malware: Challenges and a solution framework'. In: *IEEE Internet of Things Journal* 1.1 (2014), pp. 10–21. ISSN: 23274662. DOI: `10.1109/JIOT.2014.2302386`.

[468] Tao Zhang and Quanyan Zhu. 'Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs'. In: *IEEE Transactions on Signal and Information Processing over Networks* 4.1 (2018), pp. 148–161. ISSN: 2373776X. DOI: `10.1109/TSIPN.2018.2801622`.

[469] Shiying Zhou et al. 'Data Security Risk Assessment Method for Connected and Automated Vehicles'. In: *2022 IEEE 7th International Conference on Intelligent Transportation Engineering, ICITE 2022*. Beijin, China: Institute of Electrical and Electronics Engineers Inc., 2022, pp. 379–387. ISBN: 9781665460071. DOI: `10.1109/ICITE56321.2022.10101389`.

[470] Christian Zinckernagel and Emil Lutgens. *AVENUE: D2.2 Gap analysis and recommendations on autonomous vehicles for public service*. Tech. rep. Autonomous Mobility, Sept. 2019. URL: `https://h2020-avenue.eu/wp-content/uploads/2020/07/D2-2-`

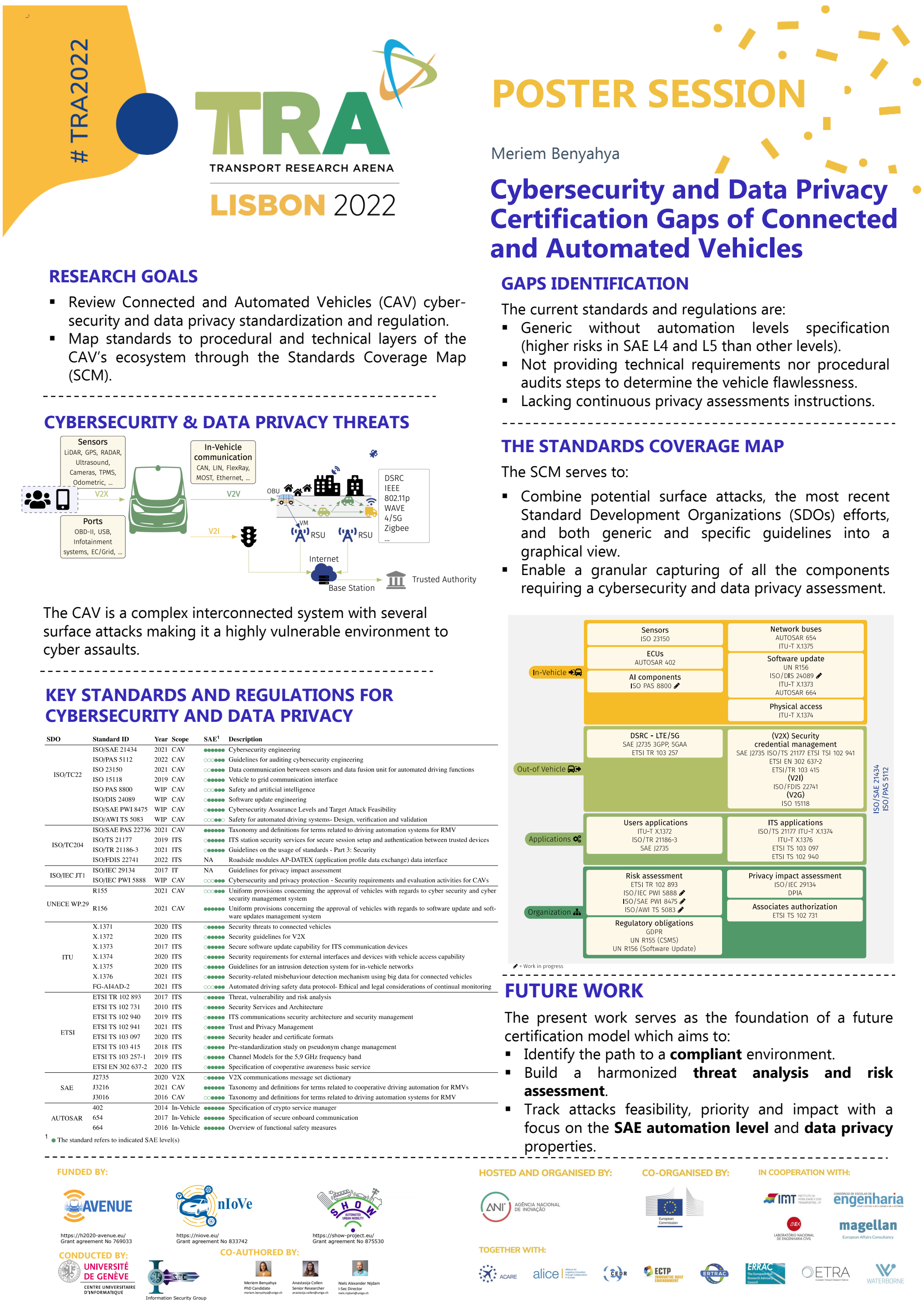
Second-Gap-analysis-and-recommendations-on-autonomous-vehicles-for-public-service.pdf.

[471] Zeljka Zorz. *Researchers hack BMW cars*. May 2018. URL: https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/.

Appendix A: TRA poster

Relevance

This poster reflects the efforts related to the article presented in Chapter 4. The content was debated with the TRA'22 experts through a presentation and a poster.



# TRA2022
TRA
TRANSPORT RESEARCH ARENA
LISBON 2022

POSTER SESSION

Meriem Benyahya

Cybersecurity and Data Privacy Certification Gaps of Connected and Automated Vehicles

RESEARCH GOALS

- Review Connected and Automated Vehicles (CAV) cybersecurity and data privacy standardization and regulation.
- Map standards to procedural and technical layers of the CAV's ecosystem through the Standards Coverage Map (SCM).

CYBERSECURITY & DATA PRIVACY THREATS

Sensors
LiDAR, GPS, RADAR, Ultrasound, Cameras, TPMS, Odometric, ...
In-Vehicle communication
CAN, LIN, FlexRay, MOST, Ethernet, ...
Ports
OBD-II, USB, Infotainment systems, EC/Grid, ...
V2X
V2V
V2I
OBU
VM
RSU
RSU
DSRC
IEEE
802.11p
WAVE
4/5G
Zigbee
...
Internet
Base Station
Trusted Authority

The CAV is a complex interconnected system with several surface attacks making it a highly vulnerable environment to cyber assaults.

KEY STANDARDS AND REGULATIONS FOR CYBERSECURITY AND DATA PRIVACY

SDO	Standard ID	Year	Scope	SAE[1]	Description
ISO/TC22	ISO/SAE 21434	2021	CAV	●●●●●●	Cybersecurity engineering
	ISO/PAS 5112	2022	CAV	○○○●●●	Guidelines for auditing cybersecurity engineering
	ISO 23150	2021	CAV	○○●●●●	Data communication between sensors and data fusion unit for automated driving functions
	ISO 15118	2019	CAV	○●●●●●	Vehicle to grid communication interface
	ISO PAS 8800	WIP	CAV	○○○●●●	Safety and artificial intelligence
	ISO/DIS 24089	WIP	CAV	○●●●●●	Software update engineering
	ISO/SAE PWI 8475	WIP	CAV	○●●●●●	Cybersecurity Assurance Levels and Target Attack Feasibility
	ISO/AWI TS 5083	WIP	CAV	○○○●●○	Safety for automated driving systems- Design, verification and validation
ISO/TC204	ISO/SAE PAS 22736	2021	CAV	●●●●●●	Taxonomy and definitions for terms related to driving automation systems for RMV
	ISO/TS 21177	2019	ITS	○●●●●●	ITS station security services for secure session setup and authentication between trusted devices
	ISO/TR 21186-3	2021	ITS	○●●●●●	Guidelines on the usage of standards - Part 3: Security
	ISO/FDIS 22741	2022	ITS	NA	Roadside modules AP-DATEX (application profile data exchange) data interface
ISO/IEC JT1	ISO/IEC 29134	2017	IT	NA	Guidelines for privacy impact assessment
	ISO/IEC PWI 5888	WIP	CAV	○○○●●●	Cybersecurity and privacy protection - Security requirements and evaluation activities for CAVs
UNECE WP.29	R155	2021	CAV	○○○●●●	Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system
	R156	2021	CAV	●●●●●●	Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system
ITU	X.1371	2020	ITS	○●●●●●	Security threats to connected vehicles
	X.1372	2020	ITS	○●●●●●	Security guidelines for V2X
	X.1373	2017	ITS	○●●●●●	Secure software update capability for ITS communication devices
	X.1374	2020	ITS	○●●●●●	Security requirements for external interfaces and devices with vehicle access capability
	X.1375	2020	ITS	○●●●●●	Guidelines for an intrusion detection system for in-vehicle networks
	X.1376	2021	ITS	○●●●●●	Security-related misbehaviour detection mechanism using big data for connected vehicles
	FG-AI4AD-2	2021	ITS	○○○●●●	Automated driving safety data protocol- Ethical and legal considerations of continual monitoring
ETSI	ETSI TR 102 893	2017	ITS	○●●●●●	Threat, vulnerability and risk analysis
	ETSI TS 102 731	2010	ITS	○●●●●●	Security Services and Architecture
	ETSI TS 102 940	2019	ITS	○●●●●●	ITS communications security architecture and security management
	ETSI TS 102 941	2021	ITS	○●●●●●	Trust and Privacy Management
	ETSI TS 103 097	2020	ITS	○●●●●●	Security header and certificate formats
	ETSI TS 103 415	2018	ITS	○●●●●●	Pre-standardization study on pseudonym change management
	ETSI TS 103 257-1	2019	ITS	○●●●●●	Channel Models for the 5,9 GHz frequency band
	ETSI EN 302 637-2	2020	ITS	○●●●●●	Specification of cooperative awareness basic service
SAE	J2735	2020	V2X	○●●●●●	V2X communications message set dictionary
	J3216	2021	CAV	●●●●●●	Taxonomy and definitions for terms related to cooperative driving automation for RMVs
	J3016	2016	CAV	○○●●●●	Taxonomy and definitions for terms related to driving automation systems for RMV
AUTOSAR	402	2014	In-Vehicle	●●●●●●	Specification of crypto service manager
	654	2017	In-Vehicle	●●●●●●	Specification of secure onboard communication
	664	2016	In-Vehicle	●●●●●●	Overview of functional safety measures

[1] ● The standard refers to indicated SAE level(s)

GAPS IDENTIFICATION

The current standards and regulations are:

- Generic without automation levels specification (higher risks in SAE L4 and L5 than other levels).
- Not providing technical requirements nor procedural audits steps to determine the vehicle flawlessness.
- Lacking continuous privacy assessments instructions.

THE STANDARDS COVERAGE MAP

The SCM serves to:

- Combine potential surface attacks, the most recent Standard Development Organizations (SDOs) efforts, and both generic and specific guidelines into a graphical view.
- Enable a granular capturing of all the components requiring a cybersecurity and data privacy assessment.

In-Vehicle

Sensors
ISO 23150

ECUs
AUTOSAR 402

AI components
ISO PAS 8800 ✎

Network buses
AUTOSAR 654
ITU-T X.1375

Software update
UN R156
ISO/DIS 24089 ✎
ITU-T X.1373
AUTOSAR 664

Physical access
ITU-T X.1374

Out-of Vehicle

DSRC - LTE/5G
SAE J2735 3GPP, 5GAA
ETSI TR 103 257

(V2X) Security credential management
SAE J2735 ISO/TS 21177 ETSI TSI 102 941
ETSI EN 302 637-2
ETSI/TR 103 415
(V2I)
ISO/FDIS 22741
(V2G)
ISO 15118

Applications

Users applications
ITU-T X.1372
ISO/TR 21186-3
SAE J2735

ITS applications
ISO/TS 21177 ITU-T X.1374
ITU-T X.1376
ETSI TS 103 097
ETSI TS 102 940

Organization

Risk assessment
ETSI TR 102 893
ISO/IEC PWI 5888 ✎
ISO/SAE PWI 8475 ✎
ISO/AWI TS 5083 ✎

Regulatory obligations
GDPR
UN R155 (CSMS)
UN R156 (Software Update)

Privacy impact assessment
ISO/IEC 29134
DPIA

Associates authorization
ETSI TS 102 731

ISO/SAE 21434
ISO/PAS 5112

✎ = Work in progress

FUTURE WORK

The present work serves as the foundation of a future certification model which aims to:

- Identify the path to a **compliant** environment.
- Build a harmonized **threat analysis and risk assessment**.
- Track attacks feasibility, priority and impact with a focus on the **SAE automation level** and **data privacy** properties.

FUNDED BY:

https://h2020-avenue.eu/
Grant agreement No 769033

https://niove.eu/
Grant agreement No 833742

https://show-project.eu/
Grant agreement No 875530

CONDUCTED BY:

UNIVERSITÉ DE GENÈVE
CENTRE UNIVERSITAIRE D'INFORMATIQUE

Information Security Group

CO-AUTHORED BY:

Meriem Benyahya
PhD Candidate
meriem.benyahya@unige.ch

Anastasija Collen
Senior Researcher
anastasija.collen@unige.ch

Niels Alexander Nijdam
I-Sec Director
niels.nijdam@unige.ch

HOSTED AND ORGANISED BY:

AGÊNCIA NACIONAL DE INOVAÇÃO

CO-ORGANISED BY:

European Commission

IN COOPERATION WITH:

IMT INSTITUTO DA MOBILIDADE E DOS TRANSPORTES, I.P.
CONSÓRCIO DE ESCOLAS DE engenharia
LABORATÓRIO NACIONAL DE ENGENHARIA CIVIL
magellan European Affairs Consultancy

TOGETHER WITH:

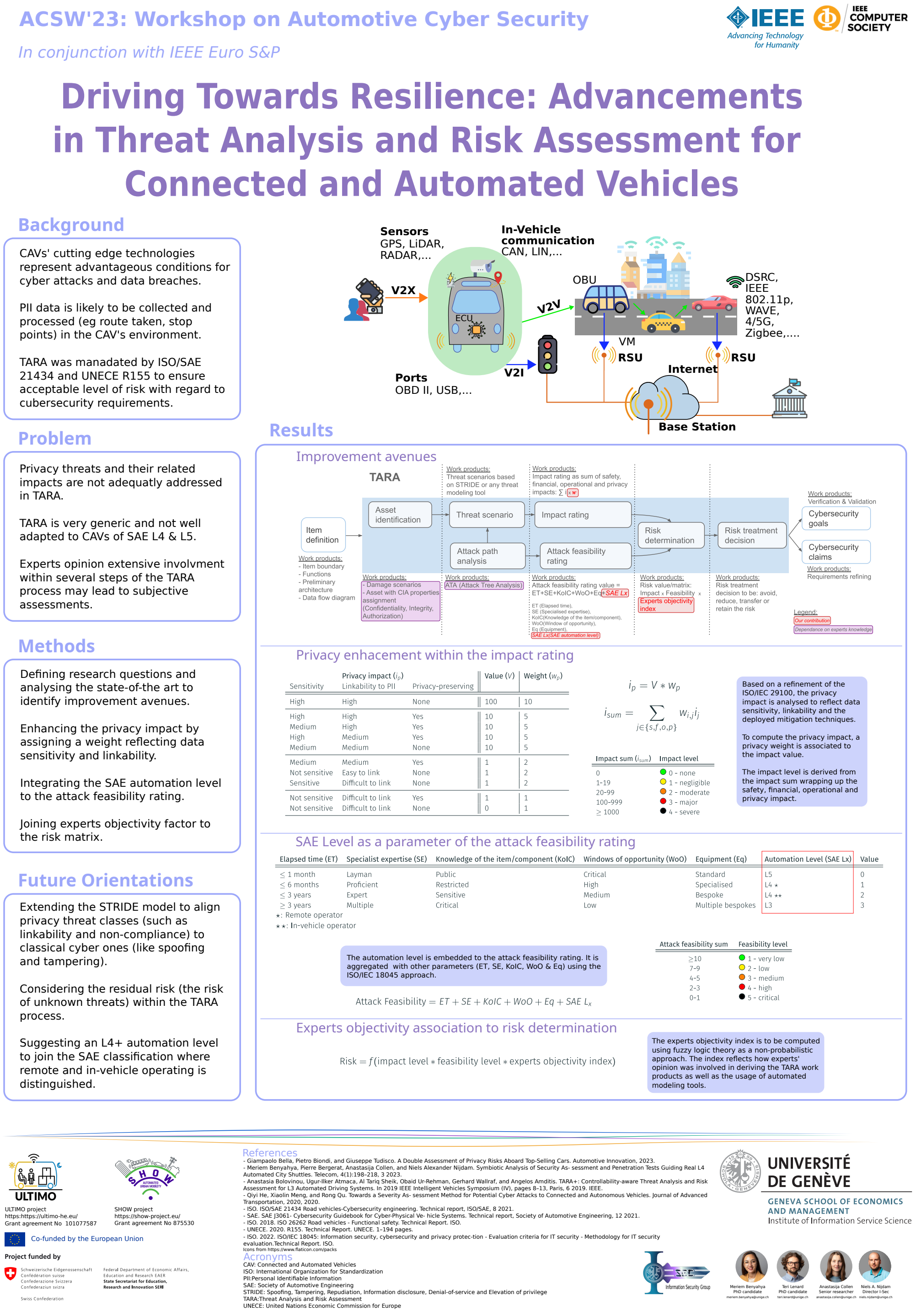
ACARE, alice, CEDR, ECTP INNOVATIVE BUILT ENVIRONMENT, ERTRAC, ERRAC The European Rail Research Advisory Council, ETRA, WATERBORNE

Figure 8.1: TRA'22 poster, Lisbon, November 2022.

Appendix B: ACSW'23 poster

Relevance

This poster reflects the preliminary results related to the enhanced TARA 2.0. The content was presented within the Workshop on Automotive Cybersecurity (ACSW) workshop that took place in conjunction with IEEE EuroS&P in July 2023 in Delft, Netherlands. The findings were discussed with several automotive experts whose feedback was considered while elaborating the article from Chapter 7.



ACSW'23: Workshop on Automotive Cyber Security

In conjunction with IEEE Euro S&P

IEEE Advancing Technology for Humanity

IEEE COMPUTER SOCIETY

Driving Towards Resilience: Advancements in Threat Analysis and Risk Assessment for Connected and Automated Vehicles

Background

CAVs' cutting edge technologies represent advantageous conditions for cyber attacks and data breaches.

PII data is likely to be collected and processed (eg route taken, stop points) in the CAV's environment.

TARA was manadated by ISO/SAE 21434 and UNECE R155 to ensure acceptable level of risk with regard to cubersecurity requirements.

Problem

Privacy threats and their related impacts are not adequatly addressed in TARA.

TARA is very generic and not well adapted to CAVs of SAE L4 & L5.

Experts opinion extensive involvment within several steps of the TARA process may lead to subjective assessments.

Methods

Defining research questions and analysing the state-of-the art to identify improvement avenues.

Enhancing the privacy impact by assigning a weight reflecting data sensitivity and linkability.

Integrating the SAE automation level to the attack feasibility rating.

Joining experts objectivity factor to the risk matrix.

Future Orientations

Extending the STRIDE model to align privacy threat classes (such as linkability and non-compliance) to classical cyber ones (like spoofing and tampering).

Considering the residual risk (the risk of unknown threats) within the TARA process.

Suggesting an L4+ automation level to join the SAE classification where remote and in-vehicle operating is distinguished.

Results

Improvement avenues

TARA

Item definition

Work products:
- Item boundary
- Functions
- Preliminary architecture
- Data flow diagram

Asset identification

Work products:
- Damage scenarios
- Asset with CIA properties assignment (Confidentiality, Integrity, Authorization)

Threat scenario

Work products:
Threat scenarios based on STRIDE or any threat modeling tool

Attack path analysis

Work products:
ATA (Attack Tree Analysis)

Impact rating

Work products:
Impact rating as sum of safety, financial, operational and privacy impacts: ∑ i x *w*

Attack feasibility rating

Work products:
Attack feasibility rating value = ET+SE+KoIC+WoO+Eq+SAE Lx

ET (Elapsed time),
SE (Specialised expertise),
KoIC(Knowledge of the item/component),
WoO(Window of opportunity),
Eq (Equipment),
SAE Lx(SAE automation level)

Risk determination

Work products:
Risk value/matrix:
Impact x Feasibility x Experts objectivity index

Risk treatment decision

Work products:
Risk treatment decision to be: avoid, reduce, transfer or retain the risk

Work products:
Verification & Validation

Cybersecurity goals

Cybersecurity claims

Work products:
Requirements refining

Legend:
Our contribution
Dependance on experts knowledge

Privacy enhacement within the impact rating

Privacy impact (i_p)			Value (V)	Weight (w_p)
Sensitivity	Linkability to PII	Privacy-preserving		
High	High	None	100	10
High	High	Yes	10	5
Medium	High	Yes	10	5
High	Medium	Yes	10	5
Medium	Medium	None	10	5
Medium	Medium	Yes	1	2
Not sensitive	Easy to link	None	1	2
Sensitive	Difficult to link	None	1	2
Not sensitive	Difficult to link	Yes	1	1
Not sensitive	Difficult to link	None	0	1

$$i_p = V * w_p$$

$$i_{sum} = \sum_{j \in \{s,f,o,p\}} w_{i,j} i_j$$

Impact sum (i_{sum})	Impact level
0	● 0 - none
1-19	● 1 - negligible
20-99	● 2 - moderate
100-999	● 3 - major
≥ 1000	● 4 - severe

Based on a refinement of the ISO/IEC 29100, the privacy impact is analysed to reflect data sensitivity, linkability and the deployed mitigation techniques.

To compute the privacy impact, a privacy weight is associated to the impact value.

The impact level is derived from the impact sum wrapping up the safety, financial, operational and privacy impact.

SAE Level as a parameter of the attack feasibility rating

Elapsed time (ET)	Specialist expertise (SE)	Knowledge of the item/component (KoIC)	Windows of opportunity (WoO)	Equipment (Eq)	Automation Level (SAE Lx)	Value
≤ 1 month	Layman	Public	Critical	Standard	L5	0
≤ 6 months	Proficient	Restricted	High	Specialised	L4 ⋆	1
≤ 3 years	Expert	Sensitive	Medium	Bespoke	L4 ⋆⋆	2
≥ 3 years	Multiple	Critical	Low	Multiple bespokes	L3	3

⋆: Remote operator
⋆⋆: In-vehicle operator

The automation level is embedded to the attack feasibility rating. It is aggregated with other parameters (ET, SE, KoIC, WoO & Eq) using the ISO/IEC 18045 approach.

$$\text{Attack Feasibility} = ET + SE + KoIC + WoO + Eq + SAE\ L_x$$

Attack feasibility sum	Feasibility level
≥10	● 1 - very low
7-9	● 2 - low
4-5	● 3 - medium
2-3	● 4 - high
0-1	● 5 - critical

Experts objectivity association to risk determination

$$\text{Risk} = f(\text{impact level} * \text{feasibility level} * \text{experts objectivity index})$$

The experts objectivity index is to be computed using fuzzy logic theory as a non-probabilistic approach. The index reflects how experts' opinion was involved in deriving the TARA work products as well as the usage of automated modeling tools.

ULTIMO

ULTIMO project
https:https://ultimo-he.eu/
Grant agreement No 101077587

SHOW AUTOMATED URBAN MOBILITY

SHOW project
https://show-project.eu/
Grant agreement No 875530

Co-funded by the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

References

- Giampaolo Bella, Pietro Biondi, and Giuseppe Tudisco. A Double Assessment of Privacy Risks Aboard Top-Selling Cars. Automotive Innovation, 2023.
- Meriem Benyahya, Pierre Bergerat, Anastasija Collen, and Niels Alexander Nijdam. Symbiotic Analysis of Security As- sessment and Penetration Tests Guiding Real L4 Automated City Shuttles. Telecom, 4(1):198–218, 3 2023.
- Anastasia Bolovinou, Ugur-Ilker Atmaca, Al Tariq Sheik, Obaid Ur-Rehman, Gerhard Wallraf, and Angelos Amditis. TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems. In 2019 IEEE Intelligent Vehicles Symposium (IV), pages 8–13, Paris, 6 2019. IEEE.
- Qiyi He, Xiaolin Meng, and Rong Qu. Towards a Severity As- sessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles. Journal of Advanced Transportation, 2020, 2020.
- ISO. ISO/SAE 21434 Road vehicles-Cybersecurity engineering. Technical report, ISO/SAE, 8 2021.
- SAE. SAE J3061- Cybersecurity Guidebook for Cyber-Physical Ve- hicle Systems. Technical report, Society of Automotive Engineering, 12 2021.
- ISO. 2018. ISO 26262 Road vehicles - Functional safety. Technical Report. ISO.
- UNECE. 2020. R155. Technical Report. UNECE. 1–194 pages.
- ISO. 2022. ISO/IEC 18045: Information security, cybersecurity and privacy protec-tion - Evaluation criteria for IT security - Methodology for IT security evaluation.Technical Report. ISO.

Icons from https://www.flaticon.com/packs

Acronyms

CAV: Connected and Automated Vehicles
ISO: International Organization for Standardization
PII:Personal Identifiable Information
SAE: Society of Automotive Engineering
STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service and Elevation of privilege
TARA:Threat Analysis and Risk Assessment
UNECE: United Nations Economic Commission for Europe

UNIVERSITÉ DE GENÈVE
GENEVA SCHOOL OF ECONOMICS AND MANAGEMENT
Institute of Information Service Science

I-Sec Information Security Group

Meriem Benyahya
PhD candidate
meriem.benyahya@unige.ch

Teri Lenard
PhD candidate
teri.lenard@unige.ch

Anastasija Collen
Senior researcher
anastasija.collen@unige.ch

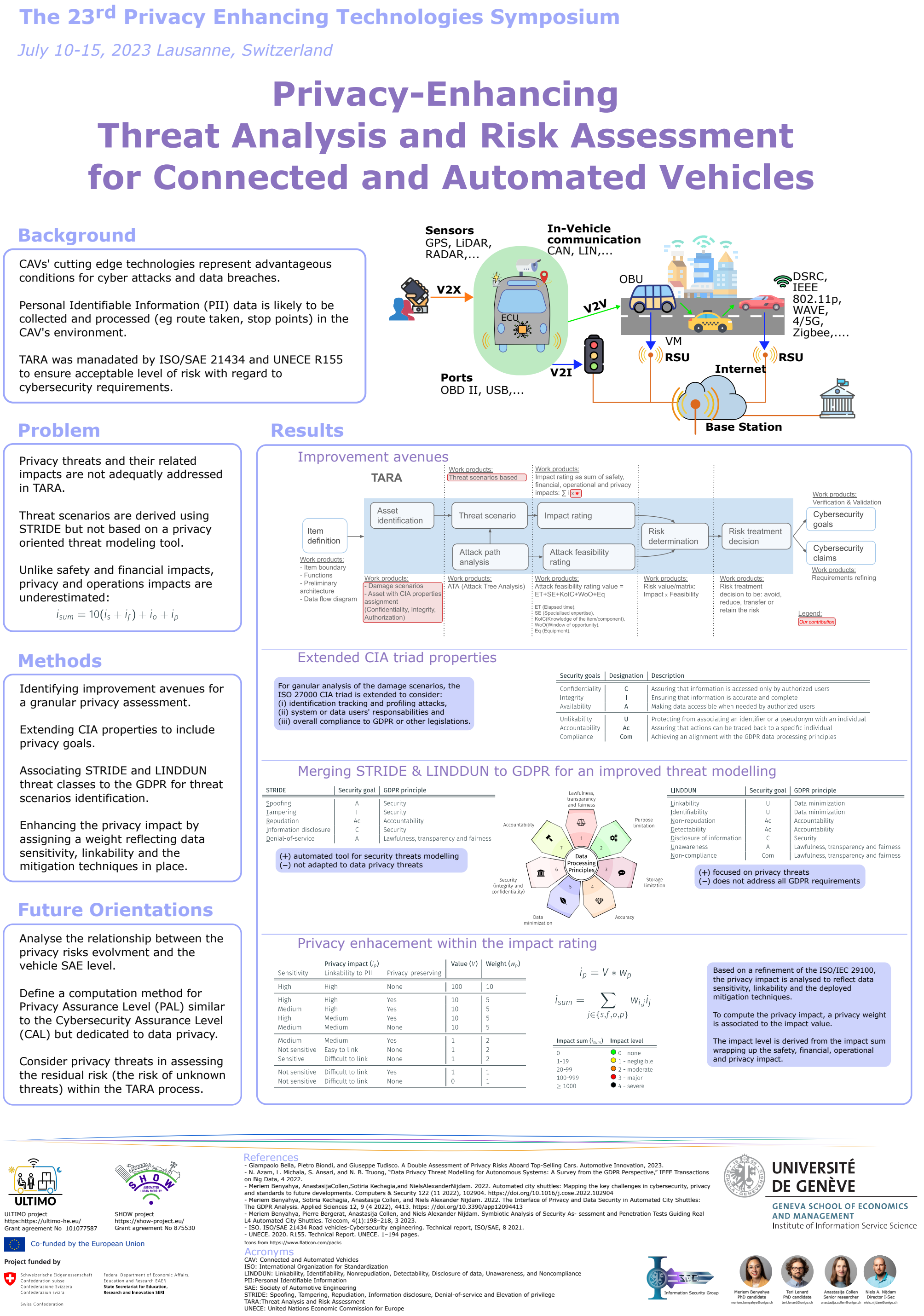
Niels A. Nijdam
Director I-Sec
niels.nijdam@unige.ch

Figure 8.2: ACSW'23 poster, Delft, Netherlands 2023.

Appendix C: PETS'23 poster

Relevance

Within the Privacy Enhancing Technologies Symposium (PETS), the present poster provided the opportunity to thoroughly discuss the privacy improvements related to our TARA 2.0 with privacy experts. The gathered insights supported in tweaking the methodology related to the article from Chapter 7.



The 23rd Privacy Enhancing Technologies Symposium

July 10-15, 2023 Lausanne, Switzerland

Privacy-Enhancing Threat Analysis and Risk Assessment for Connected and Automated Vehicles

Background

CAVs' cutting edge technologies represent advantageous conditions for cyber attacks and data breaches.

Personal Identifiable Information (PII) data is likely to be collected and processed (eg route taken, stop points) in the CAV's environment.

TARA was manadated by ISO/SAE 21434 and UNECE R155 to ensure acceptable level of risk with regard to cybersecurity requirements.

Problem

Privacy threats and their related impacts are not adequatly addressed in TARA.

Threat scenarios are derived using STRIDE but not based on a privacy oriented threat modeling tool.

Unlike safety and financial impacts, privacy and operations impacts are underestimated:

$$i_{sum} = 10(i_s + i_f) + i_o + i_p$$

Methods

Identifying improvement avenues for a granular privacy assessment.

Extending CIA properties to include privacy goals.

Associating STRIDE and LINDDUN threat classes to the GDPR for threat scenarios identification.

Enhancing the privacy impact by assigning a weight reflecting data sensitivity, linkability and the mitigation techniques in place.

Future Orientations

Analyse the relationship between the privacy risks evolvment and the vehicle SAE level.

Define a computation method for Privacy Assurance Level (PAL) similar to the Cybersecurity Assurance Level (CAL) but dedicated to data privacy.

Consider privacy threats in assessing the residual risk (the risk of unknown threats) within the TARA process.

Results

Improvement avenues

TARA

Item definition

Work products:
- Item boundary
- Functions
- Preliminary architecture
- Data flow diagram

Asset identification

Work products:
- Damage scenarios
- Asset with CIA properties assignment (Confidentiality, Integrity, Authorization)

Threat scenario

Work products:
Threat scenarios based

Attack path analysis

Work products:
ATA (Attack Tree Analysis)

Impact rating

Work products:
Impact rating as sum of safety, financial, operational and privacy impacts: ∑ i x *w*

Attack feasibility rating

Work products:
Attack feasibility rating value = ET+SE+KoIC+WoO+Eq

ET (Elapsed time),
SE (Specialised expertise),
KoIC(Knowledge of the item/component),
WoO(Window of opportunity),
Eq (Equipment),

Risk determination

Work products:
Risk value/matrix:
Impact x Feasibility

Risk treatment decision

Work products:
Risk treatment decision to be: avoid, reduce, transfer or retain the risk

Work products:
Verification & Validation

Cybersecurity goals

Cybersecurity claims

Work products:
Requirements refining

Legend:
Our contribution

Extended CIA triad properties

For ganular analysis of the damage scenarios, the ISO 27000 CIA triad is extended to consider:
(i) identification tracking and profiling attacks,
(ii) system or data users' responsabilities and
(iii) overall compliance to GDPR or other legislations.

Security goals	Designation	Description
Confidentiality	C	Assuring that information is accessed only by authorized users
Integrity	I	Ensuring that information is accurate and complete
Availability	A	Making data accessible when needed by authorized users
Unlikability	U	Protecting from associating an identifier or a pseudonym with an individual
Accountability	Ac	Assuring that actions can be traced back to a specific individual
Compliance	Com	Achieving an alignment with the GDPR data processing principles

Merging STRIDE & LINDDUN to GDPR for an improved threat modelling

STRIDE	Security goal	GDPR principle
Spoofing	A	Security
Tampering	I	Security
Repudation	Ac	Accountability
Information disclosure	C	Security
Denial-of-service	A	Lawfulness, transparency and fairness

(+) automated tool for security threats modelling
(–) not adapted to data privacy threats

Lawfulness, transparency and fairness
Purpose limitation
Storage limitation
Accuracy
Data minimization
Security (integrity and confidentiality)
Accountability
1
2
3
4
5
6
7
Data Processing Principles

LINDDUN	Security goal	GDPR principle
Linkability	U	Data minimization
Identifiability	U	Data minimization
Non-repudation	Ac	Accountability
Detectability	Ac	Accountability
Disclosure of information	C	Security
Unawareness	A	Lawfulness, transparency and fairness
Non-compliance	Com	Lawfulness, transparency and fairness

(+) focused on privacy threats
(–) does not address all GDPR requirements

Privacy enhacement within the impact rating

	Privacy impact (i_p)		Value (V)	Weight (w_p)
Sensitivity	Linkability to PII	Privacy-preserving		
High	High	None	100	10
High	High	Yes	10	5
Medium	High	Yes	10	5
High	Medium	Yes	10	5
Medium	Medium	None	10	5
Medium	Medium	Yes	1	2
Not sensitive	Easy to link	None	1	2
Sensitive	Difficult to link	None	1	2
Not sensitive	Difficult to link	Yes	1	1
Not sensitive	Difficult to link	None	0	1

$$i_p = V * w_p$$

$$i_{sum} = \sum_{j \in \{s,f,o,p\}} w_{i,j} i_j$$

Impact sum (i_{sum})	Impact level
0	● 0 - none
1-19	● 1 - negligible
20-99	● 2 - moderate
100-999	● 3 - major
$\geq$ 1000	● 4 - severe

Based on a refinement of the ISO/IEC 29100, the privacy impact is analysed to reflect data sensitivity, linkability and the deployed mitigation techniques.

To compute the privacy impact, a privacy weight is associated to the impact value.

The impact level is derived from the impact sum wrapping up the safety, financial, operational and privacy impact.

ULTIMO
ULTIMO project
https:https://ultimo-he.eu/
Grant agreement No 101077587

SHOW project
https://show-project.eu/
Grant agreement No 875530

Co-funded by the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

References
- Giampaolo Bella, Pietro Biondi, and Giuseppe Tudisco. A Double Assessment of Privacy Risks Aboard Top-Selling Cars. Automotive Innovation, 2023.
- N. Azam, L. Michala, S. Ansari, and N. B. Truong, "Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR Perspective," IEEE Transactions on Big Data, 4 2022.
- Meriem Benyahya, AnastasijaCollen,Sotiria Kechagia,and NielsAlexanderNijdam. 2022. Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. Computers & Security 122 (11 2022), 102904. https://doi.org/10.1016/j.cose.2022.102904
- Meriem Benyahya, Sotiria Kechagia, Anastasija Collen, and Niels Alexander Nijdam. 2022. The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis. Applied Sciences 12, 9 (4 2022), 4413. https: //doi.org/10.3390/app12094413
- Meriem Benyahya, Pierre Bergerat, Anastasija Collen, and Niels Alexander Nijdam. Symbiotic Analysis of Security As- sessment and Penetration Tests Guiding Real L4 Automated City Shuttles. Telecom, 4(1):198–218, 3 2023.
- ISO. ISO/SAE 21434 Road vehicles-Cybersecurity engineering. Technical report, ISO/SAE, 8 2021.
- UNECE. 2020. R155. Technical Report. UNECE. 1–194 pages.

Icons from https://www.flaticon.com/packs

Acronyms
CAV: Connected and Automated Vehicles
ISO: International Organization for Standardization
LINDDUN: Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of data, Unawareness, and Noncompliance
PII:Personal Identifiable Information
SAE: Society of Automotive Engineering
STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service and Elevation of privilege
TARA:Threat Analysis and Risk Assessment
UNECE: United Nations Economic Commission for Europe

UNIVERSITÉ DE GENÈVE
GENEVA SCHOOL OF ECONOMICS AND MANAGEMENT
Institute of Information Service Science

Information Security Group

Meriem Benyahya
PhD candidate
meriem.benyahya@unige.ch

Teri Lenard
PhD candidate
teri.lenard@unige.ch

Anastasija Collen
Senior researcher
anastasija.collen@unige.ch

Niels A. Nijdam
Director I-Sec
niels.nijdam@unige.ch

Figure 8.3: PETS'23 poster, Lausanne, Switzerland 2023.