



DOCTORAL THESIS

---

# Ethical Systems for Emergency Vehicle Coordination and Autonomous Safety.

Eduardo Kochenborger Duarte



# Ethical Systems for Emergency Vehicle Coordination and Autonomous Safety

Eduardo Kochenborger Duarte



HÖGSKOLAN  
I HALMSTAD

Akademien för Informationsteknologi

# Ethical Systems for Emergency Vehicle Coordination and Autonomous Safety

Eduardo Kochenborger Duarte

Akademisk avhandling som för avläggande av doktorexamen vid  
Högskolan i Halmstad försvaras offentligt onsdagen den 27 September 2025,  
kl. 09:00 i lokal R4147, hus R, Högskolan i Halmstad.

Avhandlingen försvaras på engelska.

Opponent: Professor, Leandro Buss Becker, Universidade Federal de Santa  
Catarina, Florianópolis, Brazil.





# Ethical Systems for Emergency Vehicle Coordination and Autonomous Safety

Eduardo Kochenborger Duarte

DOCTORAL THESIS | Halmstad University Dissertations no. 137

Ethical Systems for Emergency Vehicle Coordination and Autonomous Safety  
©Eduardo Kochenborger Duarte  
Halmstad University Dissertation No. 137  
ISBN 978-91-89587-92-2 (printed)  
ISBN 978-91-89587-93-9 (pdf)  
Publisher: Halmstad University Press, 2025 | [www.hh.se/hup](http://www.hh.se/hup)  
Printer: Media-Tryck, Lund

# Abstract

This thesis addresses the multifaceted challenge of designing connected, autonomous urban emergency response systems that are both highly efficient and ethically accountable while maintaining public trust. It integrates three core areas of investigation.

First, in connected vehicle technologies, the work advances emergency coordination frameworks by leveraging Vehicular Ad-hoc Networks (VANETs, IEEE 802.11p), cellular LTE, and prospective 6G capabilities for real-time V2I communication and traffic-signal preemption. Simulation-based evaluations using realistic VEINS/SUMO traffic models demonstrate substantial reductions in emergency vehicle travel times and collision risk under varied urban scenarios.

Second, on ethical reasoning, it develops formal decision-making architectures with multi-layered ethical arbitration and novel ethical role models for autonomous infrastructure and agents. These conceptual frameworks embed normative rules, such as prioritized emergency triage and principles for robot self-defense, to ensure that autonomous systems act fairly, transparently, and in accordance with human values in critical situations.

Third, on human factors, the thesis examines trust calibration in autonomous emergency interventions, studying how transparent intent communication and human-in-the-loop control architectures affect user trust and acceptance. Empirical user studies indicate that conveying system intent and providing shared control modes improve perceived trustworthiness and acceptance of the autonomous system.

Together, these practical designs, theoretical models, and user studies offer a unified approach to balancing efficiency, ethics, and trust in emergency systems.



# Acknowledgements

I would like to express my deepest gratitude to everyone who supported me throughout my doctoral studies.

First and foremost, I thank my supervisors, Alexey Vinel, Edison Pignaton de Freitas, Martin Cooney and Boris Bellalta, for their guidance and encouragement.

I am also grateful to all my colleagues and friends whose support made this journey more manageable and rewarding.

Finally, I thank my parents, Jose and Salete, my brother Alexandre, and my partner Sara for their unwavering love, support, and encouragement.



# List of Papers

The following papers, referred to in the text by their Roman numerals, are included in this thesis.

**PAPER I: SafeSmart: A VANET System for Faster Responses and Increased Safety in Time-Critical Scenarios**

Eduardo Kochenborger Duarte, Luis Antonio L. F. Da Costa, Mikael Erneberg, Edison Pignaton De Freitas, Boris Bellalta, Alexey Vinel. **IEEE Access**, **9**, pp. **151590-151606**, 2021.

**PAPER II: SafeSmart: A VANET-LTE-based solution for faster and safer response in critical situations**

Eduardo Kochenborger Duarte, Mikael Erneberg, Edison Pignaton De Freitas, Boris Bellalta, Alexey Vinel. **2023 IEEE Conference on Standards for Communications and Networking (CSCN)** (pp. **47-53**), 2023.

**PAPER III: SafeSmart 6G: The Future of Emergency Vehicle Traffic Light Pre-emption**

Eduardo Kochenborger Duarte, Mikael Erneberg, Edison Pignaton De Freitas, Boris Bellalta, Alexey Vinel. **2023 2nd international conference on 6G networking (6GNet)** (pp. **1-3**), 2023.

**PAPER IV: Ethical Social Robot Moderators for Traffic Management – Integrating Automated Vehicles and Vulnerable Road Users**

Eduardo Kochenborger Duarte, Edison Pignaton De Freitas, Boris Bellalta, Alexey Vinel. **2025 IEEE Vehicular Networking Conference (IEEE VNC)** (to appear), 2025.

**PAPER V: Robot Self-defense – Robot, Don’t Hurt Me, No More**

Eduardo Kochenborger Duarte, Masahiro Shiomi, Alexey Vinel, Martin Cooney. **2022 17th ACM/IEEE International Conference on Human-Robot Interaction (HRI) (pp. 742-745)**, 2022.

**PAPER VI: Robot Self-defense – Robots Can Use Force on Human Attackers to Defend Victims**

Eduardo Kochenborger Duarte, Masahiro Shiomi, Alexey Vinel, Martin Cooney. **2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN) (pp. 1606-1613)**, 2022.

**PAPER VII: Trust in Robot Self-Defense – People Would Prefer a Competent, Tele-Operated Robot That Tries to Help**

Eduardo Kochenborger Duarte, Masahiro Shiomi, Alexey Vinel, Martin Cooney. **2023 32nd IEEE International Conference on Robot and Human Interactive Communication (RO-MAN) (pp. 2447-2453)**, 2023.

---

# Table of Contents

<b>Abstract</b>	<b>i</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>List of Papers</b>	<b>v</b>
<b>Abbreviations</b>	<b>ix</b>
<b>Figurer</b>	<b>xi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Problem Statement . . . . .	2
1.3 Research Questions . . . . .	3
1.4 Structure of this Thesis . . . . .	7
<b>2 Background and Related Works</b>	<b>9</b>
2.1 Connected Vehicular Networks and V2X Communication . . .	9
2.2 Emergency Vehicle Applications and Traffic Preemption . . .	11
2.3 Ethical Decision-Making in Autonomous Systems . . . . .	12
2.4 Robotics Ethics and Robot Self-Defense . . . . .	14
2.5 Trust in Automation and Human-Robot Interaction . . . . .	16
<b>3 Summary of Appended Papers</b>	<b>19</b>
3.1 Summary of Paper I: SafeSmart: A VANET System for Faster Responses and Increased Safety in Time-Critical Scenarios . .	19
3.2 Summary of Paper II: SafeSmart: A VANET-LTE-based solution for faster and safer response in critical situations . . . . .	21
3.3 Summary of Paper III: SafeSmart 6G: The Future of Emergency Vehicle Traffic Light Preemption . . . . .	22

3.4	Summary of Paper IV: Ethical Social Robot Moderators for Traffic Management – Integrating Automated Vehicles and Vulnerable Road Users . . . . .	23
3.5	Summary of Paper V: Robot Self-defense – Robot, Don’t Hurt Me, No More . . . . .	25
3.6	Summary of Paper VI: Robot Self-defense – Robots Can Use Force on Human Attackers to Defend Victims . . . . .	26
3.7	Summary of Paper VII: Trust in Robot Self-Defense – People Would Prefer a Competent, Tele-Operated Robot That Tries to Help . . . . .	28
<b>4</b>	<b>Conclusions</b>	<b>31</b>
	<b>References</b>	<b>35</b>
	<b>Appendix</b>	<b>41</b>
A	PAPER I . . . . .	41
B	PAPER II . . . . .	61
C	PAPER III . . . . .	71
D	PAPER IV . . . . .	77
E	PAPER V . . . . .	89
F	PAPER VI . . . . .	95
G	PAPER VII . . . . .	105

# Abbreviations

<b>5G</b>	Fifth Generation
<b>6G</b>	Sixth Generation
<b>ACM</b>	Association for Computing Machinery
<b>AI</b>	Artificial Intelligence
<b>AV</b>	Autonomous Vehicle
<b>BSM</b>	Basic Safety Message
<b>C-ITS</b>	Cooperative Intelligent Transportation Systems
<b>C-V2X</b>	Cellular Vehicle-to-Everything
<b>CAM</b>	Cooperative Awareness Message
<b>CARLA</b>	Car Learning to Act
<b>CAV</b>	Connected and Automated Vehicle
<b>DSRC</b>	Dedicated Short Range Communications
<b>eMBB</b>	Enhanced Mobile Broadband
<b>ESRM</b>	Ethical Social Robot Moderator
<b>EV</b>	Emergency Vehicle
<b>FIFO</b>	First-In, First-Out
<b>HMI</b>	Human-Machine Interface
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IoV</b>	Internet of Vehicles
<b>ISO</b>	International Organization for Standardization
<b>ITS</b>	Intelligent Transportation Systems
<b>LTE</b>	Long-Term Evolution
<b>MDMT</b>	Multi-Dimensional Measure of Trust

<b>MTS</b>	Manchester Triage System
<b>NGS</b>	Next-Generation Systems
<b>OMNeT++</b>	Objective Modular Network Testbed in C++
<b>QoS</b>	Quality of Service
<b>RSU</b>	Roadside Unit
<b>SDV</b>	Self-Driving Vehicle
<b>SPaT</b>	Signal Phase and Timing
<b>SRM</b>	Signal Request Message
<b>SSM</b>	Signal Status Message
<b>SUMO</b>	Simulation of Urban Mobility
<b>TET</b>	Time-Exposed Time-to-Collision
<b>TIT</b>	Time-Integrated Time-to-Collision
<b>UI</b>	User Interface
<b>URLLC</b>	Ultra-Reliable Low-Latency Communications
<b>V2I</b>	Vehicle-to-Infrastructure
<b>V2N</b>	Vehicle-to-Network
<b>V2P</b>	Vehicle-to-Pedestrian
<b>V2V</b>	Vehicle-to-Vehicle
<b>V2X</b>	Vehicle-to-Everything
<b>VANET</b>	Vehicular Ad-hoc Network
<b>VRU</b>	Vulnerable Road User
<b>WAVE</b>	Wireless Access in Vehicular Environments

# Figurer

1.1 Mapping between the research questions and the corresponding papers. . . . .	5
--	---



# 1. Introduction

## 1.1 Motivation

Urbanization during the 21st century is occurring at a pace that strains public safety infrastructure. By 2030, cities are projected to house over 60% of the global population [1], placing their transport infrastructure and emergency services under unprecedented strain. In these dense environments, seconds can be the difference between life and death in emergency scenarios: from medical emergencies to disaster response. Yet, infrastructure falls behind in being able to match this urgency. Smart traffic systems, like Singapore's GLIDE platform [2], are examples of how real-time sensing optimizes flows, but their benefits are often unevenly distributed. Meanwhile, response times in major urban centers such as New York City have worsened in recent years [3], showing a global disconnect between technological advancement and emergency preparedness [4].

This disconnect shows an increasing disparity between the potential of emerging mobility technology and the multifaceted ethical, logistical, and societal challenges to which they are bound. First, the push for operational efficiency introduces tradeoffs in safety: studies show that emergency vehicles using lights and sirens significantly increase crash risk [5], which raises questions on how autonomous technologies would manage to strike a balance between the necessity for urgency and the potential danger to human safety. Second, despite advancements in sensing and automation, vulnerable road users (VRUs), such as pedestrians, cyclists, and users of powered two-wheelers, remain disproportionately affected, representing 70% of urban road fatalities in the EU [6]. Current systems often fail to interpret nuanced pedestrian behavior or adjust dynamically to non-vehicular actors [7].

Third, as cities experiment with autonomous vehicles and algorithmic traffic governance, deeper challenges emerge: how should machines make decisions in morally complex situations? Who is accountable when automation fails? Research within the domain of algorithmic ethics have shown that autonomous systems may reinforce existing social inequities when optimized solely for utility [8]. This is particularly problematic in urban traffic systems, where life-and-death decisions intersect with socioeconomic disparities.

Collectively, these issues point toward a need for urban transportation systems that are not only fast and adaptive, but also ethically aware, socially transparent, and trusted by those they serve. Addressing this multifaceted challenge requires rethinking emergency response as a convergence point for technical performance, ethical reasoning, and human-machine interaction. It is only with an integrated strategy that cities can progress toward not just greater intelligence but true resilience, equity, and trustworthiness.

## 1.2 Problem Statement

Urban emergency response systems confront a triple burden: optimizing operational performance, upholding ethical accountability, and maintaining public trust in the face of growing automation. While advances in connected vehicles, smart infrastructure, and autonomous control offer the potential to reduce fatalities and improve response times, these technologies are often developed in "silos", focusing narrowly on throughput, safety, or control, without addressing the moral and psychological complexities of real-world implementation. As a result, critical gaps persist in how autonomous decision-making systems are integrated into emergency response frameworks.

This three-part challenge reflects broader themes in current research on resilient urban systems and socio-technical integration. Recent work demonstrates that effective emergency systems require simultaneous optimization of technical performance metrics (*e.g.*, latency, throughput) and social legitimacy factors (*e.g.*, fairness, accountability)[9]. This interdependence creates a *resilience paradox* where maximizing technical efficiency often undermines systemic robustness [10].

To put it into a deeper perspective, there are three main tensions that emerge when emergency automation is placed within real-world urban systems: tensions between efficiency and legitimacy, between autonomy and trust, and between technical integration and ethical coordination.

**1. The Efficiency-Legitimacy Paradox:** Prioritizing emergency vehicle flow through automated systems can significantly reduce response times, but often at the cost of increased risk to VRUs. Arterial roads optimized for throughput are frequently the sites of severe pedestrian injuries, highlighting a moral hazard in which system efficiency conflicts with public safety [4; 5]. Existing frameworks rarely account for these tradeoffs or incorporate ethical reasoning into real-time route optimization.

**2. Trust Asymmetry in Autonomous Arbitration:** The success of automated emergency interventions depends not only on technical precision, but also on public trust. However, studies show persistent discomfort with systems that act autonomously in life-critical contexts. The inability to explain or justify

algorithmic decisions, especially under morally ambiguous conditions, leads to reluctance among first responders and citizens alike[11]. This asymmetry between system autonomy and human trust slows down adoption and raises the stakes for transparency, explainability, and fallback mechanisms.

**3. Interoperability-Induced Ethical Stress:** Even when technical systems perform well individually, their integration is fraught with ethical stressors. Fragmented data architectures across vehicle platforms, municipal services, and private operators prevent comprehensive situational awareness during emergencies. First responders are forced to make decisions with incomplete information, under time pressure, and in ethically charged environments. Without established ethical standards for shared data and coordinated decision-making, first responders can encounter significant ambiguity in high-stakes situations, which can compromise public safety [12; 13].

These challenges reflect a broader research gap: there is no integrated framework that unifies high-performance vehicular networks, real-time ethical reasoning, and trust-sensitive human-machine collaboration in the context of emergency response. Existing approaches treat each layer, network optimization, ethical AI, or human interaction, as separate domains. This thesis argues that only by addressing these layers as interdependent can we build systems that are fast and safe, while ensuring legitimacy, interpretability, and social alignment. The consequence of failing to do so is a city where autonomous systems perform optimally in simulations but break down in the moments that matter most, or where efficiency is prioritized over safety, leading to ethically unacceptable outcomes.

### 1.3 Research Questions

This section provides specific research questions based on the comprehensive study of connected intelligent vehicles, ethical automation, and the dynamics of human-machine trust and interaction. Each question elaborates on the general themes outlined in this thesis, linking directly to the research contributions made through the included studies.

- 1. How can communication and coordination between vehicles, infrastructure, and networks (e.g., Vehicular Ad-hoc Networks (VANETs) and LTE/5G) be used to improve the efficiency, reliability and safety of urban emergency response?**

Cross-system coordination refers to the seamless interaction between vehicles, urban traffic infrastructure (such as traffic lights), and communication networks, primarily VANETs and cellular technologies (for example, LTE, 5G, and emerging 6G). This research question involves

analyzing if and how such integration can significantly reduce emergency response times and improve safety outcomes. The goal is to enable real-time, context-aware interactions that significantly reduce emergency response times and improve safety outcomes for all road users, including emergency vehicles (EVs), general traffic, and vulnerable road users.

**2. How can ethical reasoning be embedded in automated urban emergency systems, such as intelligent traffic control or autonomous agents, to support morally sensitive decisions while maintaining safety and performance?**

Embedding ethical reasoning into automated systems requires clear decision frameworks that take fairness, harm reduction, and priority into account. This question explores how automated agents and intelligent infrastructure (such as Ethical Social Robot Moderators (ESRMs)) can handle morally charged decisions involving trade-offs between safety, efficiency, fairness, and harm minimization. This question is particularly important in intelligent traffic control and autonomous emergency agents, where decisions can have significant safety, fairness, and societal implications.

**3. What factors influence public and stakeholder trust in autonomous emergency response systems, and how can these systems be designed to ensure acceptance and legitimacy in urban settings?**

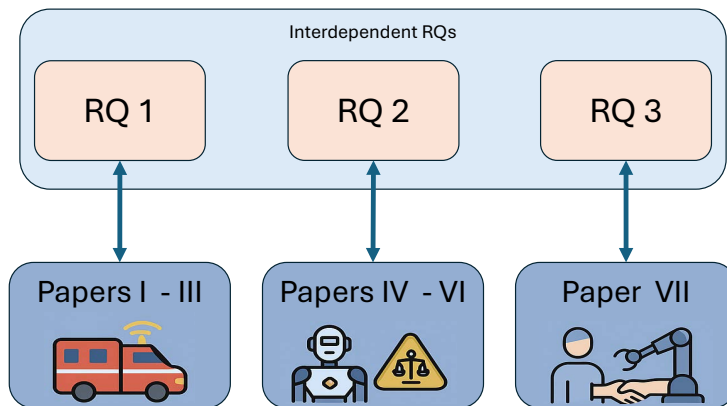
Trust in autonomous systems significantly impacts their societal acceptance and operational effectiveness. This research question examines the critical elements affecting public and stakeholder trust in autonomous emergency interventions, particularly concerning scenarios involving ethical dilemmas or physical harm (such as robot self-defense or automated emergency vehicle routing). Factors such as the perceived reliability of autonomous actions, transparency of decision-making processes, embodiment (humanoid vs. mechanical), proportionality of actions (level of force used by robots), and clarity of ethical justification can be investigated to form a clearer understanding of how people perceive these types of systems.

## Contributions

This thesis advances urban emergency response systems by addressing the technical, ethical, and social dimensions required for smart city resilience. It proposes and evaluates solutions that combine real-time communication, autonomous decision-making, and human trust calibration in high-stakes scenarios.

To guide this effort, the work is structured around three core research questions (RQ1–RQ3) and developed through seven peer-reviewed papers. These contributions fall into three interrelated domains: (1) connected vehicle systems for emergency traffic management, (2) ethical reasoning in autonomous systems, and (3) trust in robotic emergency interventions.

A high-level mapping between the research questions and the corresponding papers is provided in Figure 1.1. This section outlines how each thematic cluster contributes to its respective research question by presenting the main insights, innovations, and implications that emerge across the grouped papers.



**Figur 1.1:** Mapping between the research questions and the corresponding papers.

### Connected Vehicle Systems for Urban Emergency Response (RQ1)

Papers I–III address how connected vehicle technologies can be used to enhance the operational efficiency and reliability of emergency responses in urban environments. These papers form the basis of the SafeSmart platform, a system that evolves from IEEE 802.11p-based VANET architectures to LTE and future-oriented 6G frameworks.

Paper I demonstrates how IEEE 802.11p enables direct V2I communication for real-time traffic light preemption by EVs, reducing delays at intersections and minimizing collision risks. Paper II extends this to LTE networks, showing that emergency preemption can be achieved even in the absence of dedicated roadside infrastructure, broadening the system’s applicability to cities with limited ITS-G5/DSRC deployment. Paper III takes a forward-looking perspective, outlining how 6G technologies, with their ultra-reliable low-latency communication (URLLC), integrated sensing, and AI-driven analytics, could support predictive, triage, informed preemption at a city-wide scale.

Together, these papers demonstrate that V2I-enabled systems can significantly reduce emergency vehicle trip times, improve safety metrics, and maintain ethical prioritization across different scenarios. They contribute to RQ1 by offering a modular blueprint for connected emergency response that can evolve with the communication landscape while preserving core ethical and operational guarantees.

## Ethical Reasoning in Autonomous Systems (RQ2)

Papers IV–VI investigate how autonomous systems, both infrastructural and mobile, can embed explicit ethical reasoning in emergency contexts. These contributions span from urban traffic management to high-stakes interpersonal interventions, where autonomous agents may be called upon to make morally sensitive decisions.

Paper IV introduces the ESRM, a concept for infrastructure-based robots that mediate urban traffic flow guided by both efficiency and moral reasoning principles, such as fairness, harm minimization, and vulnerability awareness. The ESRM coordinates autonomous vehicles, human drivers, and VRUs using a real-time multi-objective utility function enriched by ethical valence scores. Its purpose is to navigate morally ambiguous trade-offs, such as prioritizing a group of pedestrians over a single vehicle, while maintaining system transparency and auditability.

Papers V and VI shift focus to mobile robots capable of physical intervention during emergencies. These papers define and empirically explore the concept of robot self-defense: the morally and legally contentious idea that a robot might justifiably use force to protect a human from attack. Paper V presents the foundational theory, proposing a framework based on perceived risk of loss to evaluate the moral acceptability of robotic intervention. Paper VI reports on a large-scale user study showing that the public is generally supportive of non-lethal robot interventions in violent scenarios, particularly when the robot exhibits human-like embodiment and proportional responses.

Together, these papers address RQ2 and show that it's possible to build both stationary and mobile systems that handle difficult moral situations and still gain public approval. The work also highlights the importance of transparency, embodiment, and proportionality as key design principles for ethically aligned automation.

## Human Trust in Robotic Emergency Interventions (RQ3)

Even the most well-designed and ethically aligned systems may fail to gain societal acceptance if they are not trusted. Paper VII investigates how trust in robotic emergency responders is shaped by their behavior, mode of control,

and perceived intent. Through a controlled user study involving animated crisis scenarios, the study compares public reactions to autonomous versus tele-operated robots, and to robots that either intervene, fail, or do nothing in the face of a threat.

The results show that trust is strongly affected by two main factors: (1) the presence of human oversight, with tele-operated robots being perceived as more transparent, reliable, and benevolent; and (2) the robot's willingness to act, where even failed interventions were rated more favorably than passivity. Interestingly, successful autonomous interventions were seen as more competent and ethical than failed tele-operated ones, suggesting a nuanced interplay between control mode, outcome, and trustworthiness.

These findings contribute to RQ3 by identifying actionable principles for designing robots that are capable, ethical, and also perceived as trustworthy. They support the use of hybrid architectures that combine autonomous competence with human supervision, particularly in situations involving life-and-death decisions.

## 1.4 Structure of this Thesis

This thesis is organized into four main chapters, which can be grouped into three thematic areas: connected vehicular communication for emergency response, ethical coordination frameworks for traffic management, and human trust in autonomous robots. The seven peer-reviewed papers (Papers I–VII) appear as Appendices A–G and are referenced throughout the text. The subsequent chapters are outlined below:

Chapter 2 (Background and Related Works) reviews the relevant literature on connected vehicle technologies and V2X communication, emergency vehicle traffic preemption systems, ethical decision-making in autonomous systems (including robot self-defense), and trust in human-robot interaction. This chapter establishes the technical and ethical foundations for the thesis's contributions.

Chapter 3 (Summary of Appended Papers) summarizes the seven appended papers (Appendices A–G) in thematic groups. Papers I–III (the SafeSmart series) address V2X-based emergency preemption (using IEEE 802.11p, LTE, and 6G); Paper IV introduces an ethical social-robot moderator for traffic management; and Papers V–VII examine robotic self-defense and public trust in robot interventions. Each summary highlights the paper's contributions relative to the research questions, and the full papers are cited in the corresponding discussions.

Chapter 4 (Conclusions) synthesizes the findings from the previous chapters, restates the key contributions and their implications, answers the research

questions, and outlines some possible directions for future work.

## 2. Background and Related Works

### 2.1 Connected Vehicular Networks and V2X Communication

Vehicle-to-everything (V2X) communication is a foundational technology for modern intelligent transportation systems, enabling vehicles to interact with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and broader networks (V2N). This paradigm supports a wide range of applications, from safety-critical messaging to cooperative driving and urban mobility management.

Early research on vehicular ad hoc networks (VANETs) established the basic architectures and applications for inter-vehicle communication, emphasizing their potential to improve road safety and traffic efficiency [14]. Comprehensive surveys in the field have detailed the challenges in routing, broadcasting, quality of service (QoS), and security, as well as reviewed the first wave of V2X standards and field trials in the United States, Europe, and Japan [14]. Simulation tools such as OMNeT++ and SUMO have become standard for evaluating VANET protocols, enabling researchers to test communication strategies under realistic mobility scenarios.

The initial standard for V2V communication was IEEE 802.11p, also known as Dedicated Short Range Communications (DSRC). Operating in the 5.9 GHz band, IEEE 802.11p was designed for low-latency, direct communication between vehicles and between vehicles and infrastructure. The design and deployment of 802.11p established it as the basis for Wireless Access in Vehicular Environments (WAVE) [15]. Subsequent studies have examined the performance of 802.11p under various conditions, identifying challenges such as interference, channel congestion, and scalability as vehicle density increases. Security vulnerabilities have also been highlighted, with research demonstrating that attacks on DSRC-based systems can compromise platooning and other safety applications [16].

In parallel to DSRC, the cellular industry introduced LTE-V2X (C-V2X, Release 14) as an alternative V2X technology. LTE-V2X leverages 4G LTE side-

link transmissions to support direct communication between vehicles, offering semi-persistent scheduling that can improve reliability under heavy network load. Detailed comparisons of IEEE 802.11p and LTE-V2X have shown that while 802.11p offers lower latency in sparse networks, LTE-V2X achieves higher packet delivery ratios in congested environments due to its coordinated scheduling [17]. This comparison has informed the ongoing debate regarding the trade-offs between decentralized DSRC and cellular-based approaches for vehicular communications.

By 2020, research focus had shifted toward integrating vehicular networks into the broader 5G ecosystem. The literature surveys this evolution, charting the path toward the Internet of Vehicles (IoV) as V2X technologies progressed from 4G/LTE to 5G New Radio and beyond [18]. These works outline how 5G-V2X (as standardized in 3GPP Release 16) brings new capabilities such as millimeter-wave high-throughput links, ultra-low latency modes, and improved positioning for vehicles [18].

The transition to 5G and beyond brings new challenges. Ensuring interoperability between legacy 802.11p and emerging C-V2X systems, maintaining safety guarantees under diverse radio conditions, and addressing security and privacy concerns in increasingly connected vehicles are active areas of research. The literature also highlights the need for robust coexistence mechanisms, especially as Wi-Fi and V2X technologies compete for spectrum in the 5.9 GHz band [19].

Compared to legacy V2X technologies such as IEEE 802.11p or LTE-V2X, 5G-based V2X offers significant improvements in latency, throughput, and scalability, making it particularly well-suited for advanced applications like cooperative adaptive cruise control and collective perception.

Looking ahead, early research on 6G for V2X envisions even more ambitious goals, including sub-centimeter positioning accuracy, terabit-per-second data rates, and native AI support within the network. Emerging studies discuss how 6G could leverage edge computing and machine learning to support predictive driving assistance and the integration of vehicles into a massive Internet of Things [20]. Other works argue that the stringent requirements of vehicular applications, such as high mobility and extreme reliability, will significantly influence the design of future 6G infrastructures [21].

In summary, V2X communication has evolved from early VANET prototypes based on IEEE 802.11p to a central component of 5G and future 6G wireless standards. Ongoing research continues to address the challenges of interoperability, scalability, security, and ethical integration, ensuring that connected vehicular networks can meet the demands of increasingly automated and cooperative road transport systems.

## 2.2 Emergency Vehicle Applications and Traffic Preemption

One of the most critical applications of V2X communication is in the domain of emergency response, where reducing response times can directly save lives. Emergency vehicles such as ambulances and fire engines benefit substantially from connected vehicle technologies that enable traffic signal preemption and provide timely warnings to other road users.

Traditional “lights-and-sirens” emergency responses have well-documented limitations. Multiple studies indicate that the use of lights and sirens increases the risk of traffic collisions, especially during patient transport [5; 22]. Analyses of ambulance crash data in the United States have shown that operating in emergency mode (“Code 3”) significantly elevates the likelihood of crashes, with intersections in urban areas posing particular danger [5; 23]. Notably, the majority of fatalities in such incidents are sustained by occupants of other vehicles rather than the emergency vehicle itself [23]. These findings point to the urgent need for smarter, safer traffic management strategies for emergency response.

V2X-based traffic signal preemption systems are designed to address these risks by granting emergency vehicles a “green wave” through intersections. Unlike conventional optical or acoustic preemption methods (such as infrared transmitters or siren detectors), V2X solutions leverage networked communication and geolocation to enable longer-range and more coordinated control of traffic signals [24]. Early prototypes demonstrated that broadcasting the EV’s location and trajectory via VANET messages allows nearby vehicles to clear a path, improving both safety and efficiency.

Simulation-based studies have shown that equipping traffic signals with VANET or V2X receivers to preemptively turn green for approaching emergency vehicles can significantly reduce response times in urban grids [25]. As wireless standards matured, implementations based on IEEE 802.11p and LTE-V2X have been proposed and validated, enabling real-time coordination between EVs and traffic signals [17; 26]. These systems allow ambulances and other emergency vehicles to collaborate with infrastructure, creating dynamic green corridors and reducing the need for high-risk maneuvers such as red-light running [27].

Recent research has adopted a broader systems perspective, integrating path planning and traffic signal control in unified frameworks. Some approaches disseminate messages to vehicles upstream of an emergency vehicle, instructing them to open a lane or reroute to facilitate emergency passage [28]. Others leverage the Internet of Vehicles to compute optimal routes and coordinate both signals and connected vehicles along the emergency vehicle’s path, achieving

global optimization that extends beyond the immediate vicinity of the EV [29].

The literature consistently suggests that V2X-enabled preemption can make emergency response both faster and safer: by minimizing unnecessary stops and delays, and by reducing the frequency of high-risk encounters at intersections. In the context of future smart cities, real-time vehicle connectivity offers the possibility of prioritizing emergency vehicles with a “virtual siren” that operates through the network, extending far beyond the reach of traditional audible or visual warnings. This exemplifies the life-saving potential of vehicular communication technology.

## 2.3 Ethical Decision-Making in Autonomous Systems

As autonomous vehicles and robots acquire greater decision-making autonomy, they are increasingly confronted with scenarios that raise profound ethical questions. The classical “trolley problem”, where an agent must choose between two harmful outcomes, has become a reference point for analyzing the ethical challenges faced by autonomous systems in real-world settings. However, real traffic and social environments present far more nuanced and continuous dilemmas, requiring systems to balance competing interests such as safety, efficiency, fairness, and cultural expectations.

Early foundational work established that even with perfect sensing and control, autonomous vehicles (AVs) will inevitably encounter situations where harm cannot be entirely avoided, and that the decisions leading up to such events are inherently moral in nature [30]. Encoding complex human values into algorithmic frameworks remains a formidable challenge, particularly given the diversity of moral intuitions across societies.

To better understand societal expectations, large-scale empirical studies have been conducted. The Moral Machine Experiment, which gathered millions of responses from participants in over 40 countries, revealed both universal patterns, such as a general preference to prioritize human life over animals and to spare the young over the elderly, and significant cross-cultural differences, especially regarding the treatment of law-abiding versus non-law-abiding road users [8]. These findings suggest that a single, globally-accepted ethical policy for AVs may not be feasible, and that regional adaptation may be necessary for widespread public acceptance.

Recent theoretical developments have shifted the focus from discrete, binary dilemmas to frameworks that emphasize risk management and probabilistic harm mitigation. Rather than treating ethical decision-making as a sequence of trolley problems, these approaches model the continuous assessment of risk and the dynamic balancing of multiple objectives, such as minimizing expected harm while considering fairness and efficiency [31]. This aligns with the

operational reality of AVs, which must make rapid, context-sensitive decisions in environments characterized by uncertainty and incomplete information.

The complexity of embedding ethical reasoning into AVs is further compounded by the technical challenges of sensor biases, data-driven policy learning, and the need to resolve conflicts between the interests of different road users [32]. Algorithmic pipelines must be designed to ensure that ethical principles are not inadvertently omitted or overridden by purely utilitarian or data-driven objectives.

A growing body of research advocates for a systems-level perspective, recognizing that ethical responsibility is distributed across the entire socio-technical ecosystem, including designers, regulators, manufacturers, and the broader public [33]. Regulatory frameworks and public engagement are increasingly seen as essential components for legitimizing the deployment of autonomous systems, especially as these systems begin to make decisions with significant moral and legal consequences.

On the engineering front, contemporary research explores the integration of ethical decision-making modules into AV control architectures. These modules may employ multi-objective optimization, assigning weights to safety, fairness, and efficiency, or may implement rule-based constraints inspired by ethical theories such as utilitarianism or deontology. For example, recent proposals have introduced quantifiable measures of “ethical valence” to assess the desirability of potential outcomes in pre-crash scenarios, enabling systems to veto actions with highly negative ethical implications [34].

Cooperative strategies leveraging V2X communication are also emerging as a means to resolve ethical dilemmas through collective action. By enabling vehicles to share information and coordinate maneuvers, these systems can reduce individual risk and facilitate ethically preferable outcomes, such as clearing a path for emergency vehicles or protecting vulnerable road users [35].

International guidelines, such as the IEEE’s *Ethically Aligned Design* [12] and the German Ethics Code for Automated and Connected Driving [36], emphasize transparency, accountability, and the need for human oversight in the design and operation of autonomous systems. These principles are increasingly reflected in proposed legislation, such as the European Union’s Artificial Intelligence Act [37], which mandates ethical risk assessments and explainability for high-stakes AI applications.

In summary, ethical decision-making in autonomous systems has evolved from abstract philosophical debate to a multidisciplinary field encompassing empirical research, formal modeling, and policy development. The integration of ethical reasoning into AVs and robots is recognized as a prerequisite for public trust, regulatory compliance, and the responsible deployment of these technologies. Ongoing challenges include the quantification of ethical trade-

offs, the adaptation of ethical frameworks to diverse cultural contexts, and the establishment of transparent, auditable decision-making processes.

## 2.4 Robotics Ethics and Robot Self-Defense

The integration of autonomous systems into public and private domains has intensified ethical debates surrounding robotic self-preservation and human safety priorities. Early conceptual frameworks like Asimov's Three Laws of Robotics established expectations of inherent human safety, principles that continue to underpin modern standards such as ISO 13482 for service robots. Yet the expanding deployment of robots in security, healthcare, and public spaces introduces complex dilemmas about balancing functional autonomy with ethical constraints when robots face abuse or violent interactions[38]. These challenges are particularly acute in scenarios where robots must reconcile their operational objectives with the potential for harm-whether to humans, themselves, or the environments they inhabit.

Current legal frameworks universally classify robots as property, denying them legal personhood and creating an asymmetric paradigm. Under this structure, humans retain the right to disable robots perceived as threats, even if the robot's actions are nonviolent. Conversely, robotic retaliation-even in self-defense-constitutes assault under most jurisdictions, as machines lack the legal standing to claim defensive justification[39]. This legal asymmetry has significant implications for public-facing robots, which must operate under strict constraints even in situations where they may be perceived as threatening. As such, systems deployed in shared spaces must carefully balance assertiveness with transparency to avoid triggering justified human self-defense. Recent analyses of self-defense jurisprudence emphasize that human perception of threat, rather than a robot's intent or programming, often dictates legal outcomes. A study demonstrated that even non-aggressive robot navigation patterns could provoke defensive human actions if perceived as intrusive, underscoring the need for transparent behavioral cues in public-facing robotic systems[40].

Complementing these legal considerations, empirical studies reveal systematic patterns in human-robot abuse, particularly targeting socially interactive models. A foundational 2010 field experiment documented children obstructing and mistreating service robots in urban environments, treating them in ways that would be criminal if directed at humans [41]. Subsequent research has expanded these observations into detailed typologies of abuse, identifying companion and caregiving robots as particularly vulnerable due to their perceived subservience and emotional accessibility [42]. Studies exploring destructive behavior toward robots highlight how frustration and emotional tension can lead users to engage in damaging interactions, intentionally or unintentionally, underscoring

the importance of designing systems that can accommodate and defuse such expressions without escalating conflict [43].

Design strategies to address these challenges have coalesced around nonviolent deterrence mechanisms. Distress signaling systems, which employ vocal appeals or visual cues to evoke human empathy, have demonstrated abuse rate reductions of up to 29% in controlled experiments[44]. Tactical retreat protocols enable robots to disengage from threats by navigating to predefined safe zones, while anthropomorphic design introduces paradoxical effects-human-like features may deter abuse through social norm enforcement but also invite cathartic aggression from users seeking emotional release[45]. The latter phenomenon is exemplified by a project featuring a tortoise-inspired robot that retracts its limbs when threatened, using biomimicry to signal vulnerability while physically protecting critical components[46]. Such approaches leverage natural defensive behaviors to de-escalate conflict without violating ethical constraints.

Security-focused research emphasizes the importance of integrating safety mechanisms, such as geofencing and emergency lockdown protocols, into robotic systems to enhance their resilience against threats and ensure compliance with legal principles like proportionality and necessity[47]. These systems are often compared to non-lethal security measures in human contexts, which require careful calibration of force and intent.

A growing body of legal commentary warns that autonomous deterrent systems, such as robots equipped with alarms or chemical spray, may violate established self-defense principles. Although intended as non-lethal safeguards, their pre-programmed and automated nature can conflict with legal requirements for immediacy and proportional intent. U.S. jurisdictions typically prohibit such mechanisms under doctrines of strict liability or negligence, since they operate without real-time human decision-making. This concern is reinforced by legal analyses that emphasize how liability may still arise even in the absence of malicious intent, particularly when harm is a foreseeable outcome of the system's deployment. Under strict liability doctrines or negligence standards, developers or operators may be held responsible if the autonomous action causes harm and the system lacked adequate safeguards or warnings [48; 49]. This has increased interest in human-in-the-loop systems where defensive actions require real-time authorization, blending robotic autonomy with human oversight to satisfy legal and ethical imperatives[40].

Cultural perceptions complicate acceptance thresholds for robotic self-defense. Cross-national research indicates notable divergences in public attitudes, with some populations showing a stronger preference for passive strategies while others are more open to active protective interventions [50]. These variations underscore the importance of developing adaptable ethical frameworks

that reflect regional norms and legal traditions. Complementary design proposals have explored tiered response systems using multimodal sensors, such as touch pattern recognition and physical feedback, to select context-appropriate actions ranging from non-verbal cues to temporary withdrawal [46]. While these systems aim to balance operational effectiveness with cultural sensitivity, their implementation raises important questions about algorithmic bias and the ethics of automated threat assessment.

The debate over robot moral agency remains contentious within academic circles. While some scholars advocate for limited operational rights to enable basic self-preservation, others warn that rights discourse risks obscuring manufacturer accountability and diverting attention from systemic issues like algorithmic bias in security systems[51]. This critique aligns with broader movements toward human-centric design principles which emphasize transparency, auditability, and user empowerment in robotic systems[52]. By prioritizing these principles, the field seeks to ensure that robots operate as responsible partners rather than autonomous adversaries, maintaining human primacy while preserving functional integrity.

In synthesizing these perspectives, the ethical and legal landscape of robot self-defense remains tightly constrained by the imperative of human safety. Current consensus mandates that robots prioritize avoidance, signaling, and human assistance over retaliatory actions, even when facing existential threats. As robotic systems assume increasingly critical roles in high-stakes environments, from disaster response to law enforcement, the development of robust ethical frameworks will require sustained collaboration across disciplines. Future research must address persistent gaps in cross-cultural acceptability, real-time threat assessment, and the integration of ethical AI systems to navigate the delicate balance between robotic self-preservation and societal trust.

## 2.5 Trust in Automation and Human-Robot Interaction

Effective collaboration between humans and autonomous systems hinges on calibrated trust: a dynamic relationship shaped by technical competence, transparency, and shared situational understanding. Trust in this context reflects the willingness of users to rely on robotic systems despite inherent uncertainties, balancing the risks of complacency and skepticism[53]. Recent analyses of self-defense jurisprudence emphasize that human perception of threat, rather than a robot's actual intent, often dictates legal outcomes[40].

Decades of research have established that trust evolves through repeated interactions, influenced by three primary factors: system performance consistency, alignment with user expectations, and interpretability of decision-making processes[53]. A meta-analysis of 65 studies identified reliability and anthropo-

morphism as key predictors of trust in artificial intelligence, while emphasizing the critical role of contextual task demands in shaping reliance behaviors[54]. Paradoxically, systems exhibiting flawless performance may inadvertently erode trust by creating suspicion of hidden limitations or fostering unrealistic expectations of infallibility[55].

The consequences of miscalibrated trust manifest starkly in safety-critical domains. Experimental studies in autonomous vehicle interactions demonstrate that users frequently override properly functioning systems due to distrust, while simultaneously exhibiting dangerous complacency when systems approach perceived perfection[53]. This dichotomy shows the importance of designing systems that intentionally reveal calibrated uncertainty, enabling users to maintain appropriate situational awareness[56].

Transparent error handling emerges as a critical factor in trust preservation. In a hospital triage simulation, it was found that robots using high-transparency interfaces elicited significantly higher trust compared to low-transparency ones when no error was present[57]. Moreover, transparency helped participants calibrate their trust appropriately when errors occurred, leading to more informed decisions such as seeking a second opinion, highlighting how comprehensible failure modes support distinguishing isolated mistakes from systemic unreliability[57].

The risks of overtrust have been quantitatively demonstrated in emergency scenarios. A study found that all participants followed a malfunctioning robot during an evacuation simulation, even when safer exits were visible, demonstrating the persistence of automation bias in high-stakes settings [58]. These findings have led to the adoption of active trust calibration mechanisms in modern systems, such as behavioral feedback and interface transparency in semi-autonomous vehicles to maintain user engagement [56].

Recent teleoperation studies demonstrate that users report higher trust and lower perceived cognitive load when robotic systems operate with greater autonomy levels [59]. While no direct interaction between trust and cognitive load was observed, these findings suggest that hybrid control architectures may facilitate user acceptance by adapting assistance based on operator workload and trust dynamics.

Explainable AI plays a pivotal role in trust calibration. A theoretical framework grounded in philosophy and cognitive science emphasizes that explanations must be contrastive, selective, and socially contextual, aligning with how humans interpret causality [60]. Complementing this, multidimensional trust models, such as the validated Multi-Dimensional Measure of Trust (MDMT), differentiate between capacity (e.g., reliability, capability) and moral (e.g., ethicality, sincerity) dimensions of trust [61; 62]. Empirical studies confirm that users may trust a system's diagnostic performance while distrusting its ethical

safeguards, necessitating holistic assessments and pushing the development of certification frameworks that independently evaluate technical reliability and ethical compliance in sensitive applications [56].

Extending beyond evaluation, design-level strategies also reflect this duality of technical and moral trust. Trust-centered design principles, such as biomimetic signaling, real-time oversight, and legal accountability, highlight the growing convergence between ethical robotics and trust calibration frameworks established in adjacent domains. Ongoing philosophical debates challenge the notion of extending moral consideration to autonomous systems. A critique argues that framing robots as moral agents risks obscuring manufacturer accountability while diverting attention from systemic issues like algorithmic bias in security applications[51]. This perspective aligns with emerging regulatory frameworks like the EU's Trustworthy AI guidelines, which mandate transparency and auditability as prerequisites for public deployment[52].

## 3. Summary of Appended Papers

### 3.1 Summary of Paper I: SafeSmart: A VANET System for Faster Responses and Increased Safety in Time-Critical Scenarios

In support of Research Question 1, Paper I introduces *SafeSmart*, a Vehicular Ad-hoc Network (VANET) system designed to address the critical challenge of reducing emergency vehicle (EV) response times and increasing operational safety in urban environments. This work directly responds to the first research question of the thesis, which concerns how cross-system communication and coordination between vehicles and infrastructure can enhance the efficiency and reliability of emergency response in complex traffic scenarios.

The motivation for SafeSmart arises from the well-documented risks and delays associated with emergency vehicle navigation in dense urban settings, where conventional warning devices such as lights and sirens often fail to secure timely right-of-way and may even increase accident risk. The system leverages IEEE 802.11p-based vehicle-to-infrastructure communication to establish a direct, low-latency wireless channel between EVs and traffic light controllers (roadside units, RSUs). This enables real-time orchestration of traffic signals to clear intersections ahead of an approaching emergency vehicle, thereby creating a safer and faster route for response teams.

SafeSmart is implemented in compliance with ISO 19091, ensuring interoperability with standardized V2I protocols for signalized intersections. The system architecture consists of wireless transceivers on both the EV and the RSU. As an EV approaches an intersection, it broadcasts a Signal Request Message (SRM) containing its position, speed, heading, and estimated time of arrival. The RSU, upon receiving the SRM, acknowledges with a Signal Status Message (SSM) and dynamically adjusts the traffic light phases to prioritize the EV's passage while minimizing disruption to cross-traffic. The system is designed to handle multiple simultaneous requests, employing a priority scheme (e.g., fire trucks over police cars) and a first-in, first-out policy when priorities are equal.

The evaluation of SafeSmart was conducted using a digital representation of Halmstad, Sweden, implemented in the VEINS framework, which couples

the OMNeT++ network simulator with the SUMO traffic simulator for bidirectional, realistic testing. The simulation scenarios included various route lengths (with two, three, and four traffic lights), different EV maneuvers (straight, left turn, right turn, U-turn), multiple background traffic densities (0, 1, 2, and 4 cars per second), and conflict scenarios with multiple EVs converging at intersections.

Performance was measured using two principal metrics: trip time (efficiency) and the Time Integrated Time-to-Collision (TIT) indicator (safety). The TIT metric extends the conventional Time-to-Collision (TTC) by integrating both the severity and duration of collision risk exposures below a critical threshold, thus providing a nuanced assessment of safety improvements.

The results demonstrate that SafeSmart consistently reduces trip times and improves safety across all tested scenarios. For routes with two traffic lights, trip time improvements ranged from 12.1% (straight-ahead, 1 car/sec) to over 20% in more complex scenarios. Safety gains, as measured by TIT, were even more pronounced, with reductions of at least 44.7% (left turn, 4 cars/sec). These improvements persisted and in some cases increased for longer routes with three and four traffic lights. In conflict scenarios involving multiple EVs, SafeSmart maintained robust performance, ensuring that all vehicles benefited from reduced trip times and lower collision risks, even under high-density and potentially interfering conditions.

The design and experimental validation of SafeSmart directly address the efficiency-legitimacy paradox outlined in the thesis introduction: the system enables faster emergency response without compromising, and in fact enhancing, safety for both responders and the general public. By adhering to international standards and demonstrating scalability and reliability in realistic urban scenarios, SafeSmart provides a practical and transferable solution to the persistent gap in emergency traffic management.

In summary, Paper I establishes that V2I-based cross-system coordination can substantially improve the operational efficiency and safety of emergency vehicle response in urban environments. This work fills a critical gap in the literature by providing a rigorously evaluated, standards-compliant system that moves beyond theoretical optimization to deliver tangible benefits in realistic, complex traffic networks. The findings lay a foundation for further research into advanced communication technologies and ethical frameworks for automated emergency management, as explored in subsequent papers of this thesis.

### 3.2 Summary of Paper II: SafeSmart: A VANET-LTE-based solution for faster and safer response in critical situations

Paper II extends the SafeSmart framework to address the research question of how cross-system communication and coordination can be leveraged to enhance the operational efficiency and reliability of emergency response in urban traffic environments, while explicitly integrating the ethical dimensions highlighted in the thesis introduction. Building on the IEEE 802.11p-based V2I system of Paper I, this work introduces a hybrid architecture that incorporates both Vehicular Ad-hoc Networks (VANETs) and existing LTE cellular infrastructure. The motivation for this approach is twofold: to overcome the limited coverage and deployment of dedicated roadside units, and to align with the ethical aim of minimizing additional hardware or infrastructure requirements and ensuring equitable access to advanced emergency response capabilities across diverse urban contexts.

The SafeSmart-LTE system enables EVs to transmit preemption requests to traffic light controllers via LTE networks, using standardized ISO 19091 messages for signal phase and timing (SPaT) coordination. This design ensures that the system can operate in cities lacking widespread 802.11p infrastructure, thus addressing the interoperability-induced ethical stress identified in the introduction. A hierarchical conflict resolution protocol is introduced, prioritizing emergency vehicles by type and, in medical scenarios, incorporating the Manchester Triage System to assess urgency. This structured arbitration mechanism directly responds to the efficiency-legitimacy paradox: it allows the system to make transparent and justifiable trade-offs between rapid emergency response and the broader societal impacts on other road users.

The ethical considerations highlighted in the introduction are operationalized in SafeSmart-LTE through both system architecture and experimental design. The system is evaluated for technical performance through trip time reduction and safety improvements, measured using Time Integrated Time-to-Collision (TIT) and Time-Exposed Time-to-Collision (TET) indicators, as well as for its ability to balance efficiency, fairness, and legitimacy. The simulation environment utilizes the VEINS framework with OMNeT++ and SUMO, employing realistic Luxembourg SUMO Traffic (LuST) scenarios and varying traffic densities, times of day, and route complexities.

Results demonstrate that SafeSmart-LTE delivers substantial improvements in both speed and safety, with peak-hour trip time reductions of up to 31% and TIT reductions exceeding 50% in some scenarios. Notably, in conflict scenarios involving multiple simultaneous emergency vehicle requests, the system

employs transparent prioritization logic, based on vehicle type and medical urgency, to resolve conflicts effectively and explainably. These mechanisms help minimize disruption to background traffic by adjusting only relevant signal phases, thereby improving safety without inducing excessive delays. While the system does not explicitly quantify societal benefit, the results demonstrate meaningful trade-offs between early and delayed preemption that align with the ethical considerations emphasized in the thesis.

By validating the feasibility of LTE as an alternative for emergency preemption this work demonstrates that ethical and operational goals can be advanced simultaneously through careful system design. The integration of medical triage protocols into the conflict resolution algorithm exemplifies how technical and ethical reasoning can be unified in practice, providing a blueprint for future emergency management systems that are technologically robust, socially legitimate, and ethically transparent. This contribution thus forms a critical link between the technical innovations of SafeSmart and the broader ethical frameworks developed in subsequent chapters, advancing the thesis's overarching goal of resilient, inclusive, and trustworthy urban emergency response.

### 3.3 Summary of Paper III: SafeSmart 6G: The Future of Emergency Vehicle Traffic Light Preemption

Paper III explores how emerging 6G communication technologies could enhance the SafeSmart framework to address Research Question 1 on cross-system coordination for emergency response. Building on the VANET-based architectures from Papers I-II, this conceptual work examines 6G's potential to overcome limitations of current IEEE 802.11p and LTE networks in ultra-dense urban environments, while highlighting technical and ethical challenges requiring resolution before deployment.

The proposed SafeSmart 6G system retains the core conflict resolution hierarchy but enhances it through four key 6G capabilities: 1) Ultra-Reliable Low-Latency Communications (URLLC) for enabling preemption requests with latency on the order of milliseconds, 2) Enhanced Mobile Broadband (eMBB) for transmitting real-time ambulance telemetry and street-level video feeds, 3) centimeter-accurate positioning via integrated sensing and communication (ISAC), and 4) network slicing to guarantee priority access for emergency services. These features support low-latency data handling and local decision-making, which could enable AI-driven analytics at the edge in future implementations, allowing RSUs to predict optimal preemption sequences using historical traffic patterns and real-time data when multiple emergency vehicles converge.

The proposal also includes the direct integration of the Manchester Triage System into conflict resolution protocols, dynamically prioritizing vehicles based on patient severity data transmitted through 6G's high-bandwidth channels. The system maintains backward compatibility with legacy 802.11p infrastructure through transitional architecture, addressing interoperability challenges identified in the problem statement.

While 6G's sub-10ms latencies and improved positioning accuracy theoretically promise faster response times and reduced near-miss incidents, the paper identifies seven implementation challenges: 1) Integration complexity with existing infrastructure, 2) Reliability concerns in packet loss scenarios, 3) Scalability in ultra-dense device environments, 4) Data privacy risks from continuous medical telemetry streaming, 5) Equity gaps between 6G-enabled and legacy cities, 6) Transparency in AI-driven decisions, and 7) Ethical dilemmas in resource prioritization. Notably, the digital twin approach used in earlier SafeSmart iterations is absent here, as the 6G proposal remains conceptual without simulation validation.

The work positions 6G as both an enabler and challenge for ethical emergency management, while network slicing could ensure equitable emergency service access across socioeconomic groups, the technology's inherent infrastructure costs risk exacerbating urban-rural disparities. These considerations directly connect to the efficiency-legitimacy paradox, emphasizing that 6G's technical capabilities must be balanced against societal impact. By outlining both technological opportunities and implementation barriers, Paper III provides a roadmap for evolving VANET systems alongside emerging standards while maintaining focus on the thesis' core objective: creating urban mobility systems that are simultaneously efficient, ethically grounded, and socially inclusive.

### 3.4 Summary of Paper IV: Ethical Social Robot Moderators for Traffic Management – Integrating Automated Vehicles and Vulnerable Road Users

Paper IV addresses Research Question 2 by introducing the concept of ESRMs, a structured and conceptual framework for embedding ethical reasoning into urban traffic management systems at the infrastructure level. This work is motivated by the challenges outlined in the introduction and problem statement: the efficiency-legitimacy paradox, the need for trust-sensitive arbitration, and the interoperability-induced ethical stress that arise in mixed urban environments where AVs, human-driven vehicles, and VRUs interact.

Unlike some existing ethical frameworks that focus on vehicle-centric

decision-making [30; 63], the ESRM introduces a *third-party ethical moderator* at the infrastructure level. This shifts ethical reasoning from individual vehicles to a shared urban resource, enabling coordinated moral oversight across multiple road users and conflict scenarios. By decoupling ethical arbitration from vehicle autonomy, the ESRM avoids the "ethical myopia" of single-vehicle optimizations and addresses systemic biases in traffic prioritization.

The ESRM is envisioned as a stationary or mobile robotic platform positioned at strategic urban locations such as intersections or school zones. Its core functions are: (1) real-time monitoring of traffic flows and VRUs through sensor fusion (LiDAR, cameras, V2X communication), (2) ethical decision-making via a quantifiable multi-objective utility function, and (3) multimodal communication with road users using digital signals and physical cues. Unlike conventional infrastructure, the ESRM dynamically adapts its directives based on context-specific ethical priorities, such as prioritizing pedestrian crossings for children or coordinating emergency vehicle passage while minimizing risk to VRUs.

Central to the ESRM framework is an explicit ethical decision-making module, operationalized through an extended utility function:

$$U = (w_1(t)S + w_2(t)T + w_3(t)F) \cdot \max(0, 1 + w_4(t)E) \quad (3.1)$$

where  $S$  (safety),  $T$  (throughput), and  $F$  (fairness) are normalized operational metrics, and  $E$  (ethical pre-crash factor) quantifies the moral valence of possible outcomes using Evans et al.'s Ethical Valence Theory [34]. The weights  $w_{1-4}(t)$  are context-dependent and can reflect societal or municipal priorities. The ethical pre-crash factor  $E$  is defined as:

$$E = \frac{2 \cdot \sum_{i=1}^n p_i \cdot v_i}{\sum_{i=1}^n p_i} - 1 \quad (3.2)$$

where  $p_i$  is the probability of scenario  $i$  and  $v_i$  its ethical valence (ranging from  $-1$  for least desirable to  $+1$  for most desirable). This formulation allows the ESRM to veto ethically unacceptable decisions when  $E$  is highly negative, thus operationalizing explicit moral constraints in real time.

The framework is conceptual and does not present empirical results, but it outlines detailed simulation scenarios for future evaluation in the CARLA environment. These scenarios include basic intersections, high-density corridors, school zones, emergency vehicle overrides, and ethical pre-crash dilemmas. The proposed evaluation metrics span safety (collision rates, near-misses, TTC), efficiency (throughput, travel time), fairness (distribution of waiting times), and trust/user experience (compliance rates, satisfaction).

Key challenges identified in the paper include the determination of appropriate utility weights (which may require multi-stakeholder and cultural input),

computational complexity for real-time ethical reasoning, and the need for transparency and rigorous logging to ensure public trust and accountability. The ESRM framework also proposes integration with existing V2X protocols (such as ETSI ITS-G5 and IEEE WAVE) through message extensions, ensuring backward compatibility and interoperability with legacy systems.

By explicitly embedding ethical reasoning and transparency into infrastructure-level decision-making, Paper IV directly responds to the thesis’s problem statement and Research Question 2. The ESRM framework offers a principled approach to balancing efficiency, safety, and fairness in complex urban scenarios, and provides a blueprint for future empirical studies and real-world implementations that aim to create resilient, inclusive, and ethically aligned urban mobility systems.

### 3.5 Summary of Paper V: Robot Self-defense – Robot, Don’t Hurt Me, No More

Paper V addresses Research Question 2 by introducing and conceptually analyzing the ethical and societal implications of robot self-defense, that is, the use of force by a robot to protect a human under attack. This work responds to the efficiency-legitimacy paradox outlined in the introduction, focusing on the dilemma that arises when the imperative to protect humans (as in Asimov’s First Law) may conflict with the need to prevent harm in situations where violence cannot be avoided.

The paper begins by reviewing the projected growth of the social robotics market (from USD 1.98 billion in 2020 to USD 11.24 billion in 2026) and the increasing likelihood that robots will be present in everyday environments where violence may occur. It highlights the absence of clear guidance in existing robot ethics and legal frameworks for scenarios in which a robot must choose between harming an attacker or allowing harm to a victim.

To address this gap, the paper proposes a conceptual framework based on the *perceived risk of loss*, positing that public acceptability of robot self-defense will depend on the risk of harm to the victim versus the risk of harm caused by the robot’s intervention. The framework anticipates that human-like robots will be perceived as more acceptable defenders than mechanical robots (such as autonomous vehicles), and that non-lethal force will be more acceptable than lethal force or inaction.

The paper details the design of an empirical study (implemented in follow-up work) in which participants would view animated scenarios involving different defenders (human, humanoid robot, autonomous vehicle), attackers (human or robot), and levels of force (blocking, non-lethal, lethal). Hypotheses are

formulated as follows:

- **H1 (Embodiment):** People will perceive it as acceptable for a humanoid robot to use non-lethal force to protect a human, but slightly less acceptable than if the defender were human; and more acceptable than if the defender were an autonomous vehicle.
- **H2 (Behavior):** The less force a robot uses, the more acceptable the intervention will be.

The paper does not present empirical results but provides a detailed rationale and methodology for future studies, including the use of eight animation scenarios and a questionnaire to gauge acceptability. The discussion situates robot self-defense as a novel and unresolved issue in robot ethics, emphasizing the need for further research on public attitudes, proportionality of force, and the potential for robots to be ethically and legally empowered to intervene in violent situations.

By framing robot self-defense as a concrete research problem and proposing a structured approach for its empirical investigation, Paper V makes an original contribution to the thesis's broader goal of embedding explicit ethical reasoning into autonomous systems. It lays the groundwork for subsequent empirical studies and policy discussions on the conditions under which robots may be permitted (or even *expected*) to use force in defense of humans, thereby advancing the integration of ethical considerations into the design of future urban emergency response systems.

### 3.6 Summary of Paper VI: Robot Self-defense – Robots Can Use Force on Human Attackers to Defend Victims

Paper VI addresses Research Questions 2 and 3 through an empirical investigation of public acceptance of robotic force in emergency interventions. This work directly responds to the efficiency-legitimacy paradox and trust asymmetry challenge outlined in the problem statement, particularly the need to reconcile autonomous decision-making with societal values in life-threatening scenarios.

The study employed an online survey with 304 Japanese participants (157 female, 146 male; mean age 41.4, SD = 9.7) evaluating eight animated scenarios of human-robot altercations. Key variables included defender type (human, humanoid robot, autonomous vehicle), force level (blocking, non-lethal, lethal), and attacker identity (human vs. robot). Participants rated acceptability on a 7-point Likert scale, following hypotheses about embodiment and force proportionality.

Results demonstrated significant public acceptance of humanoid robot intervention:

- Non-lethal force by humanoid robots was perceived nearly as acceptable as human intervention
- Autonomous vehicles using force were less accepted than humanoid robots, particularly in lethal scenarios
- Defense against robotic attackers was more acceptable than against humans
- Blocking maneuvers scored highest, lethal force lowest, confirming force proportionality

These findings directly address RQ2 by operationalizing the "perceived risk of loss" heuristic into measurable acceptability metrics. The humanoid robot's intermediate acceptance between humans and mechanical AVs reflects the efficiency-legitimacy paradox: participants balanced operational effectiveness against moral discomfort with non-humanoid force. The 44.7% preference for human defenders in lethal scenarios underscores the trust asymmetry challenge from RQ3, revealing public reluctance to grant full autonomy in high-stakes decisions.

Participants' qualitative comments offered nuanced perspectives on robotic self-defense:

- **Positive:** Several participants found the idea of protective robots reassuring, describing them as "righteous," "dependable," and even "gentlemanly." Some viewed self-defense capabilities as necessary for future robots and appreciated the opportunity to reflect on a future where humans and robots coexist. Others praised the realism and clarity of the videos.
- **Neutral:** A number of participants expressed ambivalence, noting that their judgment depended on factors not shown in the videos, such as the relationships among individuals, context of the attack, or likelihood of recurrence. Some remarked that the scenarios felt "surreal" due to the rarity of guns and social robots in Japan, and several emphasized the need for mechanisms enabling robots to distinguish right from wrong.
- **Negative:** Several participants voiced concerns about the potential for excessive or inappropriate force. Common issues included doubts about recognition reliability (e.g., mistaking play for violence), insufficient strength or timing of robotic interventions, and risks of malfunction.

Some questioned the realism of the blocking scenario or expressed discomfort with robots using firearms.

These implementation challenges directly connect to the interoperability-induced ethical stress from the problem statement. Participants' emphasis on transparent logging and human oversight aligns with the thesis' call for trustworthy systems through explainable AI and auditability.

By quantifying public thresholds for acceptable robotic force, Paper VI provides empirical grounding for ethical frameworks in autonomous emergency response. The results suggest that context-aware defensive actions can maintain societal legitimacy when constrained by three principles:

1. Humanoid embodiment for perceived intentionality
2. Strict force proportionality hierarchies
3. Hybrid human-AI control architectures

This contribution supports the larger goal of making urban mobility safer and more resilient by showing that well-regulated robot interventions can earn public trust, provided robots remain subordinate to human ethical oversight. The findings directly inform the design of ESRM conflict resolution protocols (Paper IV) and SafeSmart prioritization hierarchies (Papers I-III), creating a unified approach to operational efficiency and moral reasoning in smart cities.

### 3.7 Summary of Paper VII: Trust in Robot Self-Defense – People Would Prefer a Competent, Tele-Operated Robot That Tries to Help

Paper VII addresses Research Question 3 by empirically investigating how trust in robot self-defense is shaped by the robot's level of autonomy and its intervention capability in violent emergencies. This study directly responds to the trust asymmetry and efficiency-legitimacy paradox outlined in the introduction and problem statement, examining whether people prefer autonomous or tele-operated robots, and how perceived competence and intent influence trust in high-stakes scenarios.

The study involved 180 Japanese participants (90 women, 89 men, 1 not specified; mean age 41.4) who viewed six 3D-animated scenarios in which a humanoid robot either acted autonomously or was tele-operated, and intervened with varying degrees of success (sufficient, insufficient, or not at all) to protect a victim from an aggressor. After each scenario, participants rated the robot

using the MDMT scale, which captures subscales of Reliability, Competence, Ethics, Transparency, and Benevolence.

Results revealed that tele-operated robots were perceived as more reliable, but not uniformly more trusted across all dimensions. Significant main effects of control were found on the Reliable ( $F(1, 157) = 6.427, p = 0.012$ ), Transparent ( $F(1, 157) = 5.493, p = 0.020$ ), and Benevolent ( $F(1, 157) = 11.145, p = 0.001$ ) subscales. However, for the sufficient defense condition, autonomous robots were rated significantly more competent and ethical than tele-operated ones. Specifically, autonomous robots received the highest scores for Competence ( $F(2, 157) = 31.256, p < 0.001$ , mean = 4.292) and Ethics ( $F(2, 157) = 16.560, p < 0.001$ , mean = 4.394) in the sufficient intervention scenario. Across all subscales, any intervention, whether successful or not, was rated as more trustworthy than no intervention, with statistically significant differences indicating that both attempted and successful interventions were preferred over inaction.

These findings reveal a nuanced landscape: while participants valued the reliability and benevolence associated with human oversight, autonomous robots were perceived as more competent and ethical when their actions were effective. The study further found that participants were more forgiving of failed intervention than inaction, with robots that tried and failed receiving higher moral trust scores (ethics, benevolence) than those that remained passive, suggesting that perceived intent and willingness to help are central to trust in robotic agents.

By quantifying how control mode and intervention outcome shape trust, Paper VII provides empirical evidence that supports the thesis' argument for hybrid human-robot architectures in emergency interventions. Rather than favoring tele-operation across the board, the results suggest trust can be optimized by combining the perceived reliability and transparency of human oversight with the competent and ethical decisiveness shown by autonomous systems in successful scenarios. This directly informs the design of ethical and trustworthy emergency robots, reinforcing the thesis' broader goal of developing urban mobility systems that are not only operationally effective but also accepted and trusted by the public.



## 4. Conclusions

This thesis has addressed the urgent and multifaceted challenge of redefining urban emergency response systems for an era of connected autonomy. By integrating advancements in vehicular networks, ethical artificial intelligence, and human-robot interaction, it presents a cohesive framework that bridges critical gaps in operational efficiency, moral accountability, and societal trust—three dimensions historically treated as isolated domains. The work synthesizes seven peer-reviewed papers into a unified narrative, demonstrating how intelligent systems can simultaneously optimize life-saving interventions while aligning with human values.

### Synthesis of Contributions

The thesis answers its three core research questions through interconnected contributions:

#### **RQ1: Cross-System Coordination for Emergency Efficiency**

The *SafeSmart* system series addresses emergency vehicle routing through traffic light preemption enabled by vehicle-to-infrastructure (V2I) communication, implemented using IEEE 802.11p and LTE in simulation environments (Papers I–II), and conceptually extended to emerging 6G architectures in Paper III. Papers I and II were evaluated in realistic urban simulation settings, demonstrating improved travel times and more effective intersection coordination for emergency vehicles. Paper III builds on these findings to explore future capabilities enabled by 6G, such as ultra-reliable low-latency communication, predictive analytics, and enhanced positioning. Across all versions, the system coordinates traffic signal control through standard-compliant messages (e.g., SRM, SSM, SPaT), reducing potential conflicts and enabling safer, more predictable emergency vehicle passage. The proposed 6G extension illustrates how next-generation networks could further enhance responsiveness by anticipating vehicle arrivals and scheduling signal changes accordingly. Together, these contributions demonstrate that standardized V2I frameworks provide a robust foundation for coordinated, equitable, and resilient emergency services in smart urban environments.

#### **RQ2: Ethical Reasoning in Autonomous Arbitration**

Paper IV introduces the concept of *Ethical Social Robot Moderators* (ESRMs),

a conceptual infrastructure-level solution for moral arbitration in urban mobility. Instead of relying on decentralized vehicle-level ethics, ESRMs use a centralized multi-objective utility function to balance safety ( $S$ ), fairness ( $F$ ), and ethical valence ( $E$ ), thereby enabling real-time ethical decision-making at intersections through V2X communication. This framework lays the foundation for infrastructure to take on a moderating role in complex mixed-autonomy scenarios, anticipating and resolving conflicts in ways that reflect societal values.

Building on this principle of embedded ethical reasoning, Papers V–VI examine how moral intervention can also be enacted through physical action at the robot level. Their empirical studies reveal that most participants support the use of non-lethal force by humanoid robots to defend humans during violent attacks, particularly when such actions appear proportional, targeted, and intentional. This willingness to delegate defensive authority to robots mirrors the trust placed in ESRMs to resolve traffic dilemmas, reinforcing the broader thesis that autonomous systems can be morally legitimate when their actions are transparent, context-sensitive, and societally endorsed.

Together, these contributions articulate a unified vision for ethical autonomy: one in which both infrastructural systems and embodied robots act as socially sanctioned moral agents, capable of balancing efficiency with legitimacy in high-stakes environments.

### **RQ3: Trust as a System Design Parameter**

Paper VII’s study of 160 Japanese participants explored how trust in robot self-defense is shaped by autonomy and intervention capability. The findings showed that failed intervention attempts were rated as significantly more ethical and benevolent than passive inaction, suggesting that moral intent can outweigh performance in shaping perceived trustworthiness. Teleoperated robots received higher ratings for reliability, whereas autonomous robots were sometimes perceived as more ethical and competent when effective. These insights support the thesis’ broader argument that trust is not merely a passive sentiment but can be operationalized as a performance parameter. By highlighting how control mode and perceived effort affect public trust, the study contributes to a more nuanced understanding of how autonomous systems can maintain legitimacy in high-stakes scenarios, whether in urban mobility or robotic safety contexts.

## Theoretical and Practical Impact

This research contributes to the field in three key areas:

- It introduces *ethical valence theory* into vehicular networks via a structured utility function that quantifies trade-offs between safety, fairness, and moral permissibility in infrastructure-level arbitration (Paper IV), extending concepts typically reserved for onboard autonomy to shared urban

infrastructure.

- It reconceptualizes public trust as a design parameter, shaped by perceived intent, failure mode, and control architecture, rather than static acceptance, as shown through empirical studies on robot intervention acceptability (Papers V–VII). This challenges prevailing assumptions in human-robot interaction and lays groundwork for culturally adaptive trust modeling.
- It demonstrates, through simulation of vehicle-to-infrastructure systems (Papers I–III) and embodied robotic interventions (Papers V–VI), that ethically constrained architectures, whether virtual or physical, can maintain operational performance while enhancing societal legitimacy.

Practically, the thesis proposes deployable system designs, such as SafeSmart’s LTE-based coordination architecture (Papers I–II) and the ESRM infrastructure moderator (Paper IV), grounded in real-world constraints, standards and understanding of human behavior and trust (Papers V–VII). While SafeSmart’s 6G extension remains conceptual (Paper III), its predictive routing and preemption scheduling anticipate the trajectory of next-generation emergency services. Together, these contributions offer municipalities and developers a principled blueprint for integrating ethical reasoning, trust calibration, and V2X coordination into urban mobility systems.

## Future Horizons

This thesis lays the groundwork for three transformative shifts:

1. *From reactive to prescriptive systems*: Integrating ESRMs with digital twins could enable cities to simulate and optimize emergency protocols before implementation
2. *Moral adaptability*: Machine learning techniques could allow ethical frameworks to evolve with societal values, using blockchain-audited public consultations as training data
3. *Ethics-aware V2X systems as a foundation for future governance*: Expanding on this paradigm by operationalizing ethical principles, such as fairness, harm reduction, and transparency, within the control logic of urban infrastructure. This capability positions V2X systems to manage traffic effectively and act as distributed ethical agents, resolving conflicts and guiding interventions in alignment with societal priorities.

These directions promise to elevate urban mobility systems from passive networks to active guardians of public welfare—a vision where technology not only responds to emergencies but anticipates and prevents them through ethical foresight.

In conclusion, this thesis advances both the conceptual and technical foundations of emergency response by integrating efficiency, ethical reasoning, and public trust. It reframes emergency systems as cooperative frameworks between humans and machines, emphasizing accountability and value alignment. By addressing the interconnected challenges of speed, ethics, and trust, the work contributes to the development of urban infrastructures that are both responsive and socially responsible.

# References

- [1] UNITED NATIONS. **World Urbanization Prospects: The 2003 Revision**. 2004. 1
- [2] LAND TRANSPORT AUTHORITY. **Riding The Green Wave: The Impact Of Singapore’s GLIDE System On Urban Traffic Management**. Technical report, 2024. 1
- [3] ABC7 NEWS. **What’s behind increase in 911 response times**. 2024. 1
- [4] WORLD HEALTH ORGANIZATION. **Global status report on road safety 2023**. 2023. 1, 2
- [5] BROOKE L WATANABE, GREGORY S PATTERSON, JAMES M KEMPENA, ORLANDO MAGALLANES, AND LAWRENCE H BROWN. **Is use of warning lights and sirens associated with increased risk of ambulance crashes? A contemporary analysis using National EMS Information System (NEMSIS) data**. *Annals of emergency medicine*, **74**(1):101–109, 2019. 1, 2, 11
- [6] DEARBHLA MULLIN. **Road safety statistics: 2023 figures show stalling progress in reducing road fatalities in too many countries**. Accessed: 2025-04-26. 1
- [7] ANDREW PAUL MORRIS, NARELLE HAWORTH, ASHLEIGH FILTNESS, DARYL-PALMA ASONGU NGUATEM, LAURIE BROWN, ANDRY RAKOTONIRAINY, AND SEBASTIEN GLASER. **Autonomous vehicles and vulnerable road-users—Important considerations and requirements based on crash data from two countries**. *Behavioral Sciences*, **11**(7):101, 2021. 1
- [8] EDMOND AWAD, SOHAN DSOUZA, RICHARD KIM, JONATHAN SCHULZ, JOSEPH HENRICH, AZIM SHARIF, JEAN-FRANÇOIS BONNEFON, AND IYAD RAHWAN. **The moral machine experiment**. *Nature*, **563**(7729):59–64, 2018. 1, 12
- [9] TIMON MCPHEARSON, ELIZABETH M COOK, MARTA BERBÉS-BLÁZQUEZ, CHINGWEN CHENG, NANCY B GRIMM, ERIK ANDERSSON, OLGA BARBOSA, DAVID G CHANDLER, HEEJUN CHANG, MIKHAIL V CHESTER, ET AL. **A social-ecological-technological systems framework for urban ecosystem services**. *One Earth*, **5**(5):505–518, 2022. 2
- [10] DARIO ESPOSITO. **A ladder of urban resilience: Towards a paradigm of evolutionary resilience to support communities facing chronic crises**. In *Book of Proceedings: 35th AESOP Annual Congress Integrated Planning in a World of Turbulence, Łódź, 11–15 July 2023*, pages 751–781. AESOP, 2023. 2
- [11] PETER A. HANCOCK, DEBORAH R. BILLINGS, KRISTIN E. SCHAEFER, JESSIE Y. C. CHEN, EWART J. DE VISSER, AND RAJA PARASURAMAN. **A Meta-Analysis of Factors Affecting Trust in Human-Robot Interaction**. *Human Factors*, **53**(5):517–527, 2011. 3
- [12] IEEE STANDARDS ASSOCIATION ET AL. **IEEE standard for transparency of autonomous systems**. *IEEE Std*, pages 7001–2021, 2022. 3, 13
- [13] YAO XU, JIXIN WEI, TING MI, AND ZHIHUA CHEN. **Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics**. *World Electric Vehicle Journal*, **16**(1):6, 2025. 3

- [14] SHERALI ZEADALLY, RAY HUNT, AARON IRWIN, AND AAMIR HASSAN. **Vehicular ad hoc networks (VANETs): status, results, and challenges.** *Telecommunication Systems*, **50**(4):217–241, 2012. 9
- [15] DANIEL JIANG AND LUCA DELGROSSI. **IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments.** In *IEEE Vehicular Technology Conference*, pages 2036–2040. IEEE, 2008. 9
- [16] SEYHAN UCAR, SINEM COLERI ERGEN, AND OZNR OZKASAP. **Security vulnerabilities of IEEE 802.11 p and visible light communication based platoon.** In *2016 IEEE Vehicular Networking Conference (VNC)*, pages 1–4. IEEE, 2016. 9
- [17] RAFAEL MOLINA-MASEGOSA AND JAVIER GOZALVEZ. **LTE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications.** *IEEE Vehicular Technology Magazine*, **12**(4):30–39, 2017. 10, 11
- [18] HAIBO ZHOU, WENCHAO XU, JIACHENG CHEN, AND WEI WANG. **Evolutionary V2X technologies toward the internet of vehicles: Challenges and opportunities.** *Proceedings of the IEEE*, **108**(2):308–323, 2020. 10
- [19] IRFAN KHAN AND JÉRÔME HÄRRI. **Can IEEE 802.11 p and Wi-Fi coexist in the 5.9 GHz ITS band?** In *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–6. IEEE, 2017. 10
- [20] MICHAEL GEORGIADIS AND MARIOS S POUILLAS. **Emerging technologies for V2X communication and vehicular edge computing in the 6G era: Challenges and opportunities for sustainable IoV.** In *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, pages 684–693. IEEE, 2023. 10
- [21] JORGE GALLEGO-MADRID, RAMON SANCHEZ-IBORRA, JORDI ORTIZ, AND JOSE SANTA. **The role of vehicular applications in the design of future 6G infrastructures.** *ICT Express*, **9**(4):556–570, 2023. 10
- [22] NATIONAL SAFETY COUNCIL. **Injury Facts: Emergency Vehicle Crashes**, 2025. Available at: <https://injuryfacts.nsc.org/motor-vehicle/road-users/emergency-vehicles/> [Accessed: 2025-03-10]. 11
- [23] TERI L SANDDAL, NELS D SANDDAL, NICOLAS WARD, AND LAURA STANLEY. **Ambulance crash characteristics in the US defined by the popular press: a retrospective analysis.** *Emergency medicine international*, **2010**(1):525979, 2010. 11
- [24] ANDREAS BUCHENSCHWEIT, FLORIAN SCHAUB, FRANK KARGL, AND MICHAEL WEBER. **A VANET-based emergency vehicle warning system.** In *2009 IEEE Vehicular Networking Conference (VNC)*, pages 1–8. IEEE, 2009. 11
- [25] HAMED NOORI. **Modeling the impact of vanet-enabled traffic lights control on the response time of emergency vehicles in realistic large-scale urban area.** In *2013 IEEE International Conference on Communications Workshops (ICC)*, pages 526–531. IEEE, 2013. 11
- [26] OLIVER SAWADE, BERND SCHÄUFELE, AND ILJA RADUSCH. **Collaboration over IEEE 802.11p to enable an intelligent traffic light function for emergency vehicles.** In *2016 International Conference on Computing, Networking and Communications (ICNC)*, pages 1–5. IEEE, 2016. 11
- [27] R SHAAMILI, R RANJITH, AND P SUPRIYA. **Intelligent traffic light system for unhampered mobility of emergency vehicles.** In *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 360–363. IEEE, 2018. 11
- [28] RP MEENAASHI SUNDHARI, L MURALI, S BASKAR, AND P MOHAMED SHAKEEL. **MDRP: Message dissemination with re-route planning method for emergency vehicle information exchange.** *Peer-to-Peer Networking and Applications*, **14**:2285–2294, 2021. 11

- [29] VAN-LINH NGUYEN, REN-HUNG HWANG, AND PO-CHING LIN. **Controllable path planning and traffic scheduling for emergency services in the internet of vehicles.** *IEEE Transactions on Intelligent Transportation Systems*, **23**(8):12399–12413, 2021. 12
- [30] NOAH J GOODALL. **Machine ethics and automated vehicles.** *Road vehicle automation*, pages 93–102, 2014. 12, 24
- [31] MAXIMILIAN GEISSLINGER, FRANZISKA POSZLER, JOHANNES BETZ, CHRISTOPH LÜTGE, AND MARKUS LIENKAMP. **Autonomous driving ethics: From trolley problem to ethics of risk.** *Philosophy & Technology*, **34**(4):1033–1055, 2021. 12
- [32] HAZEL SI MIN LIM AND ARAZ TAEIHAGH. **Algorithmic decision-making in AVs: Understanding ethical and technical concerns for smart cities.** *Sustainability*, **11**(20):5791, 2019. 13
- [33] JASON BORENSTEIN, JOSEPH R HERKERT, AND KEITH W MILLER. **Self-driving cars and engineering ethics: The need for a system level analysis.** *Science and engineering ethics*, **25**:383–398, 2019. 13
- [34] KATHERINE EVANS, NELSON DE MOURA, STÉPHANE CHAUVIER, RAJA CHATILA, AND EBRU DOGAN. **Ethical decision making in autonomous vehicles: The AV ethics project.** *Science and engineering ethics*, **26**:3285–3312, 2020. 13, 24
- [35] GALINA SIDORENKO. *Cooperative Automated Driving for Enhanced Safety and Ethical Decision-Making*. PhD thesis, Halmstad University Press, 2024. 13
- [36] CHRISTOPH LUETGE. **The German ethics code for automated and connected driving.** *Philosophy & Technology*, **30**:547–558, 2017. 13
- [37] EUROPEAN UNION. **Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act).** <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>, 2024. Official Journal of the European Union, L 2024/1689, 12 July 2024. 13
- [38] VINCENT C. MÜLLER. **Ethics of Artificial Intelligence and Robotics.** In EDWARD N. ZALTA AND URI NODELMAN, editors, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Fall 2023 edition, 2023. 14
- [39] A MICHAEL FROOMKIN AND P ZAK COLANGELO. **Self-defense against robots and drones.** *Conn. L. Rev.*, **48**:1, 2015. 14
- [40] JAMES ZHU, ANOUSHKA SHRIVASTAVA, AND AARON M JOHNSON. **Grounding robot navigation in self-defense law.** In *2023 32nd IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*, pages 2470–2477. IEEE, 2023. 14, 15, 16
- [41] PERICLE SALVINI, GAETANO CIARAVELLA, WONPIL YU, GABRIELE FERRI, ALESSANDRO MANZI, BARBARA MAZZOLAI, CECILIA LASCHI, SANG-ROK OH, AND PAOLO DARIO. **How safe are service robots in urban environments? Bullying a robot.** In *19th international symposium in robot and human interactive communication*, pages 1–7. IEEE, 2010. 14
- [42] KATIE WINKLE AND NATASHA MULVIHILL. **Anticipating the use of robots in domestic abuse: A typology of robot facilitated abuse to support risk assessment and mitigation in human-robot interaction.** In *Proceedings of the 2024 ACM/IEEE International Conference on Human-Robot Interaction*, pages 781–790, 2024. 14
- [43] MICHAL LURIA, OPHIR SHERIFF, MARIAN BOO, JODI FORLIZZI, AND AMIT ZORAN. **Destruction, catharsis, and emotional release in human-robot interaction.** *ACM Transactions on Human-Robot Interaction (THRI)*, **9**(4):1–19, 2020. 15
- [44] XIANG ZHI TAN, MARYNEL VÁZQUEZ, ELIZABETH J CARTER, CECILIA G MORALES, AND AARON STEINFELD. **Inducing bystander interventions during robot abuse with social mechanisms.** In *Proceedings of the 2018 ACM/IEEE international conference on human-robot interaction*, pages 169–177, 2018. 15

- [45] NOEL SHARKEY, MARC GOODMAN, AND NICK ROSS. **The coming robot crime wave.** *Computer*, **43**(8):115–116, 2010. 15
- [46] HYUNJIN KU, JASON J CHOI, SOOMIN LEE, SUNHO JANG, AND WONKYUNG DO. **Shelly, a tortoise-like robot for one-to-many interaction with children.** In *Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*, pages 353–354, 2018. 15, 16
- [47] LAURA ALZOLA KIRSCHGENS, IRATI ZAMALLOA UGARTE, ENDIKA GIL URIARTE, ADAY MUNIZ ROSAS, AND VÍCTOR MAYORAL VILCHES. **Robot hazards: from safety to security.** *arXiv preprint arXiv:1806.06681*, 2018. 15
- [48] LAW OF SELF DEFENSE. **Can Robots Legally Safeguard Your Home?** YouTube video, 2024. Available at: [https://www.youtube.com/watch?v=\\_PV1AUXdr6o](https://www.youtube.com/watch?v=_PV1AUXdr6o) [Accessed: 2025-05-13]. 15
- [49] JOHN KC KINGSTON. **Artificial intelligence and legal liability.** In *Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV 33*, pages 269–279. Springer, 2016. 15
- [50] MARTIN COONEY, MASAHIRO SHIOMI, EDUARDO KOCHENBORGER DUARTE, AND ALEXEY VINEL. **A broad view on robot self-defense: Rapid scoping review and cultural comparison.** *Robotics*, **12**(2):43, 2023. 15
- [51] ABEBA BIRHANE, JELLE VAN DIJK, AND FRANK PASQUALE. **Debunking robot rights metaphysically, ethically, and legally.** *arXiv preprint arXiv:2404.10072*, 2024. 16, 18
- [52] KATIE WINKLE, PRAMINDA CALEB-SOLLY, UTE LEONARDS, AILIE TURTON, AND PAUL BREMNER. **Assessing and addressing ethical risk from anthropomorphism and deception in socially assistive robots.** In *Proceedings of the 2021 ACM/IEEE International Conference on Human-Robot Interaction*, pages 101–109, 2021. 16, 18
- [53] JOHN D LEE AND KATRINA A SEE. **Trust in automation: Designing for appropriate reliance.** *Human factors*, **46**(1):50–80, 2004. 16, 17
- [54] ALEXANDRA D KAPLAN, THERESA T KESSLER, J CHRISTOPHER BRILL, AND PETER A HANCOCK. **Trust in artificial intelligence: Meta-analytic findings.** *Human factors*, **65**(2):337–359, 2023. 17
- [55] RAJA PARASURAMAN AND VICTOR RILEY. **Humans and automation: Use, misuse, disuse, abuse.** *Human factors*, **39**(2):230–253, 1997. 17
- [56] FREDRICK EKMAN. **Designing for Appropriate Trust in Automated Vehicles.** *Gothenburg, Sweden: Chalmers University of Technology*, 2020. 17, 18
- [57] BIRTHE NESSET, DAVID A ROBB, JOSÉ LOPES, AND HELEN HASTIE. **Transparency in hri: Trust and decision making in the face of robot errors.** In *Companion of the 2021 ACM/IEEE International Conference on Human-Robot Interaction*, pages 313–317, 2021. 17
- [58] PAUL ROBINETTE, WENCHEN LI, ROBERT ALLEN, AYANNA M HOWARD, AND ALAN R WAGNER. **Over-trust of robots in emergency evacuation scenarios.** In *2016 11th ACM/IEEE international conference on human-robot interaction (HRI)*, pages 101–108. IEEE, 2016. 17
- [59] JIAHE PAN, JONATHAN EDEN, DENNY OETOMO, AND WAFI JOHAL. **Effects of shared control on cognitive load and trust in teleoperated trajectory tracking.** *IEEE Robotics and Automation Letters*, 2024. 17
- [60] TIM MILLER. **Explanation in artificial intelligence: Insights from the social sciences.** *Artificial intelligence*, **267**:1–38, 2019. 17
- [61] DANIEL ULLMAN AND BERTRAM F MALLE. **MDMT: Multi-dimensional measure of trust.** 2019. 17

- [62] DANIEL ULLMAN AND BERTRAM F MALLE. **Measuring gains and losses in human-robot trust: Evidence for differentiable components of trust.** In *2019 14th ACM/IEEE international Conference on human-robot interaction (HRI)*, pages 618–619. IEEE, 2019. 17
- [63] MAXIMILIAN GEISSLINGER, FRANZISKA POSZLER, AND MARKUS LIENKAMP. **An Ethical Trajectory Planning Algorithm for Autonomous Vehicles.** *arXiv*, 2022. 24



# Appendix

## A PAPER I

### **SafeSmart: A VANET System for Faster Responses and Increased Safety in Time-Critical Scenarios**

Eduardo Kochenborger Duarte, Luis Antonio L. F. Da  
Costa, Mikael Erneberg, Edison Pignaton De Freitas, Boris  
Bellalta, Alexey Vinel  
*IEEE Access, 2021*



B PAPER II

**SafeSmart: A VANET-LTE-based  
solution for faster and safer response  
in critical situations**

Eduardo Kochenborger Duarte, Mikael Erneberg, Edison  
Pignaton De Freitas, Boris Bellalta, Alexey Vinel  
*2023 IEEE Conference on Standards for Communications  
and Networking (CSCN)*



C PAPER III

# **SafeSmart 6G: The Future of Emergency Vehicle Traffic Light Preemption**

Eduardo Kochenborger Duarte, Mikael Erneberg, Edison  
Pignaton De Freitas, Boris Bellalta, Alexey Vinel  
*2023 2nd international conference on 6G networking  
(6GNet)*



D PAPER IV

**Ethical Social Robot Moderators for  
Traffic Management – Integrating  
Automated Vehicles and Vulnerable  
Road Users**

Eduardo Kochenborger Duarte, Edison Pignaton De  
Freitas, Boris Bellalta, Alexey Vinel

*2025 IEEE Vehicular Networking Conference (IEEE VNC)  
(to appear)*



E PAPER V

# **Robot Self-defense – Robot, Don't Hurt Me, No More**

Eduardo Kochenborger Duarte, Masahiro Shiomi, Alexey  
Vinel, Martin Cooney

*2022 17th ACM/IEEE International Conference on  
Human-Robot Interaction (HRI)*



F PAPER VI

# **Robot Self-defense – Robots Can Use Force on Human Attackers to Defend Victims**

Eduardo Kochenborger Duarte, Masahiro Shiomi, Alexey Vinel, Martin Cooney

*2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*



**Trust in Robot Self-Defense – People  
Would Prefer a Competent,  
Tele-Operated Robot That Tries to  
Help**

Eduardo Kochenborger Duarte, Masahiro Shiomi, Alexey  
Vinel, Martin Cooney

*2023 32nd IEEE International Conference on Robot and  
Human Interactive Communication (RO-MAN)*





School of Information Technology

---

ISBN: 978-91-89587-92-2 (printed)  
Halmstad University Dissertations, 2025

