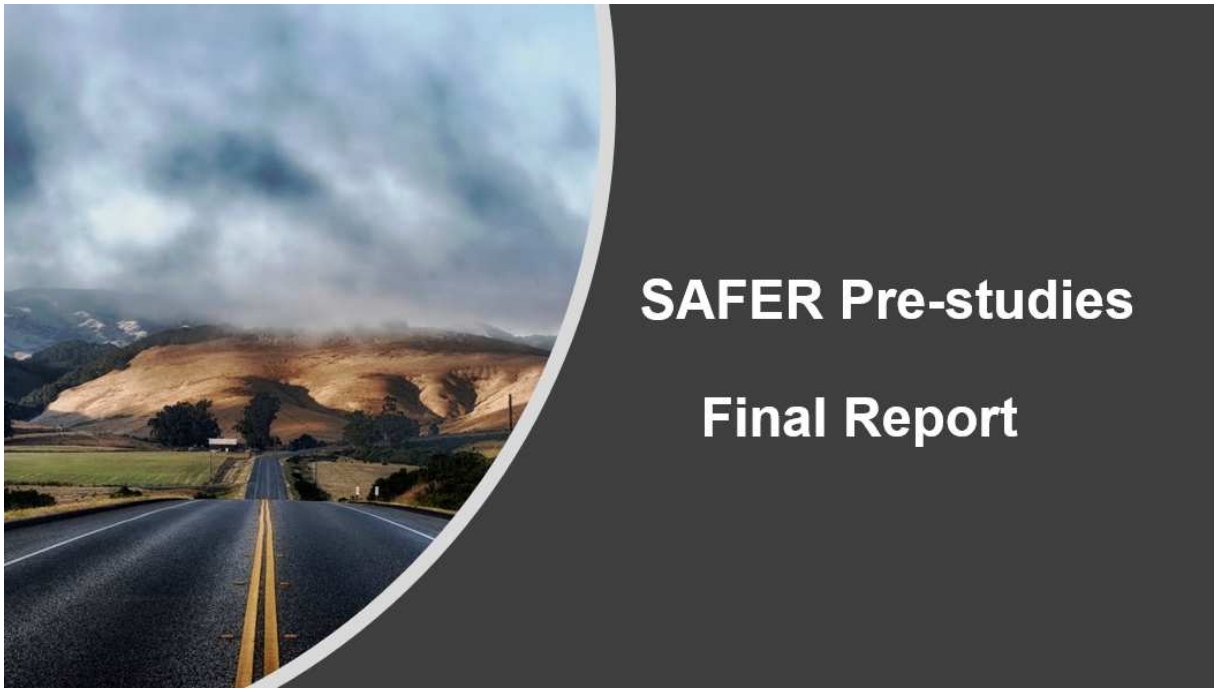


Reference	*AP70*
Project Title	Trustworthy AI from a Traffic Safety Perspective
Coordinator	*Malmeken AB*
Project Manager	*Trustworthy AI from a Traffic Safety Perspective*
Project Duration	2022-01-10 – 2022-06-30

Contents

Summary - *Trustworthy AI from a Traffic Safety Perspective*

This pre-study was initiated by Malmeken AB (Else-Marie Malmek, PM) and Blackbird Law AB (Kristina Lillieneke), and the Project Owner was Zenseact AB. The project was supported by a PhD student at VCC and also by Reveré and SAFER.

To create Trustworthy AI, it is imperative to ensure that the AI is not only technically safe and robust but also that it is ethically and legally compliant. In this pre-study project we aim to identify a) which data is collected by Autonomous Vehicles and b) which must be handled appropriately and c) which stakeholders to involve to address the legal and ethical risks and opportunities in data handling. If data handled correctly the results will create opportunities for SAFER and its partners to use AI in automated solutions which support fulfilling the UN Sustainable Development Goals and Vision Zero.

Trustworthy AI creates transparency, predictability and takes responsibility for how the algorithms are scaled in a broader ethical context. We have re-used "The SEVS Way", www.sevs.se , a strategic analysis methodology and process to handle complexity in a systematically way to address these issues.

One of our main conclusions is that it seems that the industry is fully occupied to have the AV functioning, so even if they think that Trustworthuy AI is important, they have to prioritize and therefore it seems that Trustworthy AI is not yet on top of their agendas.

As our overall conclusion we can establish that for the industry to be able to develop Trustworthy AI they need to use multi-disciplinary teams right from the start. AI applications have multiple consequences that needs to be taken into account and does not only present us with technical challenges but also a vast amount of legal and ethical challenges.

The future is much too important to leave it up to technology engineers alone.

TRUSTWORTHY AI from a traffic safety perspective

1. Background

Connected and autonomous vehicles bring about a plethora of new technologies and generate vast amounts of data from the vehicles, its surroundings, the drivers and the passengers. AI is the main enabler for autonomous driving and AVs consist of numerous sets of complex interrelated AI-based systems. AVs will function through diverse technologies such as image recognition systems (using high powered smart cameras inside and outside of the cars), GPS, voice and sound recognition systems, neural networks and high-powered sensors. Inputs from there systems create an intelligent layer of insights and patterns that help AVs operate efficiently. The data will be gathered continuously and be further transmitted to the infrastructure in real-time and will sometimes be temporarily stored in the vehicle.

There are four main types of data that will be actively collected by AVs:

- **Non-sensitive data** – data such as congestion data, parking availability etc.
- **Personal data** – location, habits, opinions, conversations, behavioral patterns and other biometric details
- **Special category data** – data collected during a collision calling of the emergency services by the car – possible to share who is in the car and any specific needs
- **Commercial sensitive data** – data specific to the manufacturer and/or it's suppliers

The reason we initiated this pre-study is because the discussion around the handling of personal data and differentiation between different types of data for that matter seems to be getting too little attention. We were therefore interested in investigating how personal data is handled and if there are any measures taken or planned to ensure that personal data is handled in a legally and ethically compliant way. Collected data can be anonymized/encrypted/de-identified or fully visible/unmasked but it is unclear to what extent AI systems are actually differentiating different types of data, whether AI systems are being designed to anonymize personal data and it is also unclear how suppliers and OEMs work with legal and ethical requirements when developing AI for AVs.

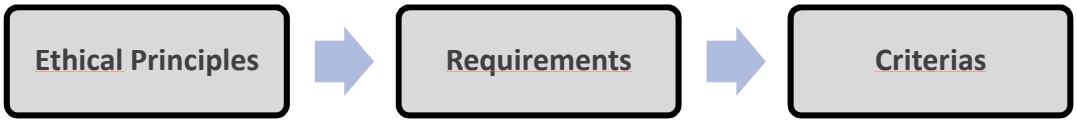
The term Trustworthy AI has become increasingly used in the last 2-3 years, most noteworthy since the EU published its report "Ethics guidelines for Trustworthy AI" in April 2019.[1] In the preface of the report the meaning of the term as well as the aim of the guidelines is stated to be:

[1] https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

"The aim of the Guidelines is to promote Trustworthy AI. Trustworthy AI has three components which should be met throughout the system's entire life cycle: (1) it should be lawful, complying with all applicable laws and regulations (2) it should be ethical, ensuring adherence to ethical principles and values and (3) it should be robust, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm. Each component in itself is necessary but not sufficient for the achievement of Trustworthy AI. Ideally, all three components work in harmony and overlap in their operation. If, in practice, tensions arise between these components, society should endeavor to align them."

Trustworthy AI is thus not a legal requirement but a preferred setup according to the EU. The first report applies to AI in general and does not specifically addresse the automotive industry. In December 2021, the EU however published a report titled "Trustworthy Autonomous Vehicles"[2] which aims at advancing the discussion around Trustworthy AI in the Automated/Autonomous Vehicles (AVs) domain. In the report five "Trustworthy stages" of an AV is specifically mentioned; Trustworthy Localization, Trustworthy Scene Understanding, Trustworthy Path Planning, Trustworthy Control and Trustworthy Interaction.

The report further states that the term Trustworthy AI should be interpreted as a global framework that includes multiple principles, requirements and criteria. The EU framework suggests taking on the issue of Trustworthy AI in accordance with the following order of steps:



The report defines four main Ethical Principles:

1. ***Respect for human autonomy (EP1):*** *humans interacting with AVs (whether they are vehicle users or external road users) must be able to maintain full self-determination over themselves. AI systems of AVs should not subordinate, coerce, deceive, manipulate, condition or herd humans (e.g., do not move them to unwanted destinations, do not comply with stop requests, etc.). Instead, they should be designed to augment, complement and empower human driving skills and mobility (e.g., extending mobility to vulnerable groups). Interactions between humans and AVs should follow human-centric design principles, securing human oversight of driving automation systems in AVs.*

2. ***Prevention of harm (EP2):*** *AVs should neither cause nor exacerbate harm or otherwise adversely affect human beings. This entails the protection of human dignity as well as physical, and even mental, integrity. AVs and the road environments in which they operate must be safe and secure. AVs must be technically robust and it should be ensured that they are not open to malicious use. Vulnerable users (both in- vehicle and external road users) should receive greater*

[2] https://publications.jrc.ec.europa.eu/repository/handle/JRC127051

attention and be considered in the development, deployment and use of AI systems of AVs.

3. ***Fairness (EP3):*** *the development, deployment and use of AVs must be fair, ensuring equal and just distribution of both benefits and costs, and ensuring that individuals and groups are free from unfair bias, discrimination and stigmatization. The use of AVs should never lead to people being deceived or unjustifiably impaired in their freedom of choice. Fairness entails the ability to contest and seek effective redress against decisions made by AVs and by the humans operating them. In order to do so, the entity accountable of the AV decisions must be identifiable, and the decision-making processes (e.g., local path planning) should be explainable.*

4. ***Explainability (EP4):*** *is crucial for building and maintaining users' trust in AVs. This means that driving automation systems need to be transparent, the capabilities and purpose of AI systems that enable vehicle automation must be openly communicated, and AV decisions - to the extent possible - explainable to those directly and indirectly affected. Without such information, the decisions and behavior of the AVs cannot be duly contested. Cases in which an explanation is not possible (i.e., "black box" algorithms) require additional measures (e.g. traceability, auditability and transparent communication on system capabilities).*

The EU report further defines 7 requirements:

Code	Requirements
KR1	Human agency and oversight [Mänsklig handlingsfrihet och tillsyn]
KR2	Technical robustness and safety
KR3	Privacy and data governance
KR4	Transparency
KR5	Diversity, non-discrimination and fairness
KR6	Societal and environmental well-being
KR7	Accountability

Lastly the report suggests how to measure such requirements according to a number of defined criteria. See example below:

Table 3: Assessment Criteria for a Trustworthy AI: key requirement 1.

Req.	Code	Criteria
KR1		**Human agency and autonomy**
	CR1.1	Affects humans or society
	CR1.2	Confusion as to whether the interaction is with a human or an AI
	CR1.3	Overreliance
	CR1.4	Unintended and undesirable interference with end-user decision-making
	CR1.5	Simulation of social interaction
	CR1.6	Risk of attachment, addiction and user behaviour manipulation
		Human oversight
	CR1.7	Self-learning or autonomous / Human-in-the-Loop / Human-on-the-Loop / Human-in-Command
	CR1.8	Training on how to exercise oversight
	CR1.9	Detection and response mechanisms for undesirable adverse effects
	CR1.10	Stop button
	CR1.11	Oversight and control of the self-learning or autonomous nature of the AI system

Figure 1: criteria

The legal and ethical considerations of AVs must thus be carefully considered throughout the entire value chain. It is the authors view that different types of data also has to be handled in different ways and that primary use of data (in the moment use) and secondary use (processing of historically collected data) must also be differentiated to assess whether the legal and ethical requirements are fulfilled. The more data that is collected by suppliers and OEMs the more complex the legal and ethical challenges become. In this context we wanted to investigate how the ecosystem players are developing and handling data today.

When reviewing personal data handling it is important to understand how such data, and big data, is handled currently and how the actors in the field address privacy challenges. Using collected data, an AV can build strategies for many possible situations on the road. Smart cars pass information from all their sensors to a cloud server and respond to conditions which is great for technical robustness but which can also constitute a privacy risk as data is not only collected for driving. Mobility intelligence uses machine learning and data science to create a digital twin with unique indicators that allow predictive real-world modelling. It is a tool for assessing different facets of mobility and analyzing different real-world personas, and it provides context that can be transformed into actionable insights. But it also poses complex legal and ethical challenges. Big data is also a rich source of behavioral insights such as consumer patterns. This information can and is being used in marketing, sales, and customer service.

There are enormous benefits to be had from big data analytics, but such analytics also highlights the serious privacy problems and there is massive potential for unwanted exposure, monitoring and tracking that can result in anything from embarrassment, discrimination to controlling behaviors.[3][4] Corporations such as Israeli Otonomo already monetize the big data generated by connected vehicles. Otonomo has built a vehicle data platform and marketplace where they sell the data from 16 OEMs, fleets and more than 100 service providers. The platform ingests

[3] Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach, Alexandros Nikitas, Na Liu, Simon Parkinson
[4] ENISA Good Practices for Security of Smart Cars (2019)

more than 4 billion data points per day from over 40 million global connected vehicles, then reshapes and enriches them and sell the data. Otonomo's platform creates new revenue streams by enabling the utilization of the vast amounts of data vehicles generate on a daily basis and that OEMs are required to store and maintain. It is unclear how the drivers/passengers have been informed of the collection of personal data and given their consent to the monetization of the personal data generated by themselves. It is also unclear which legal and ethical considerations have been taken into account not only by Otonomo but the OEMs providing them with raw data.

As vehicles are becoming increasingly geared towards being service platforms, behavioral insights can be converted into direct revenue for premium services, infotainment offers, or even partnerships with third parties. But where is and should the line bee drawn between privacy and revenue generating data sales? Who shall own the data and biometric information generated? That is an issue that is not being discussed enough.

In addition to the above mentioned data collection we can add technologies such as "Precise Point Positioning". Geely has developed so called "Real-Time Kinematic-services" (PPP-RTK). These services build on Geely's own satellites that they have launched and which track all vehicles in real time. The tracking data is then transferred and stored in a network of stations throughout China. It is unclear if any other personal data is collected through this system. Geely plans their "Future Mobility Constellation" to consist of 240 satellites when the whole system is up and running. Services such as this, and the fact that such monitoring is being made by a dictatorship that has many human rights and freedoms issues adds another dimension to the privacy issue.

Trust takes years to build, seconds to break, and forever to repair. It's no secret that trust is the new brand equity, yet it's no small feat to maintain. Based on issues such as the ones mentioned above we wanted to understand how/if responsible data handling is a key factor when developing AI applications. We also wanted to see if there is a distinction between collected data and how possible problems are addressed and lastly how the actors in the field are addressing the legal and ethical challenges.

Considering that OEMs are moving from being product manufacturers to service providers that provide their customers not with vehicles, but with "mobility-as-a-service", monetization of data has become an important component. There would be no striving for autonomy without revenue generating big data. The global connected car market is projected to grow from $59.70 billion in 2021 to $191.83 billion in 2028[5]. Intel estimates that each autonomous vehicle will use and generate around 4000 GB of data per day. Thus data revenues are the key component in autonomous driving and software that helps to analyze big data is being used without any legal limitations on how personal data is handled within the EU.

[5] https://www.fortunebusinessinsights.com/industry-reports/connected-car-market-101606

2. Project set up

2.3 Purpose

AVs are part of the solutions to achieve the Vision Zero but with AI solutions there also comes the risks to personal data due to the handling of a huge amount of data gathered by the AVs as well as from its surroundings. We initiated this pre-study since we had identified possible legal and ethical risks when handling huge amount of personal data, and we also know that this is a relatively unexplored area within the automotive industry. There are business benefits to be had by creating Trustworthy AI which will give OEMs a competitive advantage if are proactive and can show that personal data is handled in an acceptable way we think that this is an area worth exploring also for the OEMs. Therefore we took the initiative to analyze the Swedish automotive industry's work around Trustworthy AI and wanted to engage the Swedish automotive industry to co-operate and to build new knowledge in this field.

In the context of AI, there is a critical underlying assumption: "No trust, No Use". Since AI holds great promises (as well as dangers), autonomous drive-companies and AI enthusiasts must concern themselves with the question of how to create trust in their AI to foster adoption and usage. Without trust there will be no adoption. Trust in AI does not only mean trust in a technical functioning and robustness. Those aspects are considered "hygiene-factors" without which there will be no product in the first place. To truly create trust in AI and autonomous vehicles the legal and ethical aspects of how personal data is captured and handled must be trusted (Trustworthy AI).

This pre-study aims at identifying ethical and legal challenges posed by personal data in AI and autonomous driving and suggest directions for how to continue investigating and solving these issues to be able to create Trustworthy AI.

2.4 Objectives

This pre-study aimed to investigate the interest of SAFER's partners and other stakeholders to build a strong consortium and to apply for a scale-up project. Since this pre-study is a SAFER project with a focus on autonomous drive and safety, the FFI call **"Trafiksäkerhet och automatiserade fordon" - FFI – 2022-06-21,** was the most relevant call to prepare for.

Further objectives were:

- Investigate weather Trustworthy AI is considered through legal and ethical compliance in the context of assisted and automated system solutions.
- Form a theory of where the line should be drawn between public and private interests.
- Investigate which data is collected by critical AI applications that must and should be filtered out from retention and second hand use from a legal and ethical perspective.
- To further develop and strengthen SAFER's Open Innovation Platform SEVS, www.sevs.se.

2.5 Project period

2022-01-10 – 2022-06-30

2.6 Partners

Zenseact AB, Malmeken AB, Blackbird Law AB

3. Method and activities

We have used "The SEVS Way" as the tool for our work, It is a strategic analysis methodology to handle complexity in a structural way. The methodology is a result from earlier FFI-project[6] and consists of a result driven process and a set of tools e.g. a stakeholder analysis, identified difficult questions, a driving force model, use cases and scenarios. It also includes a sustainability assessment step in the form of a Multi Criteria Analysis.

In this pre-study we aim to accomplish only the first two steps in The SEVS Way: a simplified stakeholder analysis and identification of the challenges and "difficult questions" related to ethical and legal aspects regarding the handling of personal data in conjunction with AV. Based on this, the plan was to define 3-4 use cases as a base for a scale-up phase 2 project.

Initially we planned to have 3-4 workshops where a number of invited participants, based on the stakeholder analysis, met in cross functional teams and discussed legal and ethical issues and define the challenges and so called "difficult questions".

As it proved impossible to get all participants together at any dates, we decided to conduct separate online semi-structured interviews with different stakeholders from the industry, academy and authorities instead. We have personally reached out to 53 individuals by email or in person. 18 of these individuals declined participation, 20 did not answer at all, and 14 individuals agreed and did participate. 10 of these participants were representatives from the automotive industry, while 4 were representatives from academy/governmental authorities. We tried to reach out to two insurance companies but unfortunately they declined to participate. Two were female and 12 were male.

Since this was a small pre-study, we were not able to apply this systematic and more time consuming approach to our interviewees. The interviews were instead conducted for 45 minutes - 1,5 hour, and we had only time to discuss a few general questions. We prepared the interviewees by sending the questions in advance.

[6] https://www.vinnova.se/m/fordonsstrategisk-forskning-och-innovation/

Questions asked to the interviewees:

1. What does Trustworthy AI mean to you/your company?
2. In what way do you/your organization work with Trustworthy AI?
3. Which are the main challenges and difficult questions?
   a) Technical/robustness?
   b) Social/ethical?
   c) Political/legal?
   d) Spatial/different markets? (Asia-EU-US, Rural/Ural areas)?
4. Who are the main stakeholders?

We had also prepared for some more deeper questions, which we were able to ask to a few of the interviewees. See ANNEX 1.

In parallel to the interviews we have read a lot of scientific reports and articles, we have also attended several seminars and conferences mainly on-line but also physically e.g the GAIA conference 2022, https://conference.gaia.fish/.

4. Results and Deliverables

The low number of participants makes it impossible to draw any definite conclusions, but nonetheless we are able to conclude that Trustworthy AI is not yet a prioritized area, apart from the robustness and functionality aspects.

From our interviews the main conclusion we can draw is that the question of how to differentiate different types of data and handle personal data is not a prioritized one. Only one of the companies developing AI was working with legal and ethical requirements even though the issue was labelled “interesting” by all interviewees. As AI solutions and AVs have proven harder to develop than anticipated technical robustness is the primary, and only, aim currently (Criteria KR2). There is no differentiation on how different types of collected data is handled. There is also no differentiation on the primary in the moment handling of data and the secondary use of historic data. This will most likely prove problematic as it will be ineffective, time consuming and more expensive to try to incorporate such features after a solution already has been developed. And if launched solutions prove untrustworthy customers trust will take a very long time to rebuild if it is even ever possible.

Due to the fact that almost no respondent, whom are all from different corporations and/or institutions, work to ensure that legal and ethical requirements are fulfilled it has not been possible to answer any of the questions we were looking to answer. Since they were not working with Trustworthy AI they could not answer any questions about it. It also proved impossible to locate anyone with knowledge on all forms of data collected or even provide us with information on which suppliers collect personal data through their applications. All development is being done separately without any cooperation between different teams and seemingly without any organization to help coordinate such work.

But from the lack of answers and clarifications we can however make some conclusions. One conclusion is that ethical guidelines have no real impact. Disregarding ethical aspects have no legal consequences and leaving the ethical aspects up to the individual corporations is not sufficient. AI ethics—or ethics in general—lacks mechanisms to reinforce its own normative claims. Of course, the enforcement of ethical principles may involve reputational losses in the case of misconduct, or restrictions on memberships in certain professional bodies. Yet altogether, these mechanisms are rather weak and pose no eminent threat. Ethics guidelines for the AI industry serve to suggest to legislators that internal self-governance is sufficient, and that no specific laws are necessary to mitigate possible technological risks and to eliminate scenarios of abuse. This does not seem to be the case though. In addition there are not even claims that the developers of AI differentiate between i.e. vehicle data and personal data, or differentiate between "primary in-the-moment" use of personal data and secondary use of personal data. Ethics guidelines, as well as other concepts of self-governance, seems to only serve to pretend that accountability is taken as no mitigating measures are actually implemented and embedded.

Due to this fact we can also draw the conclusion that unwanted side effects of the use of AI will be present if a change of focus is not made within the team developing the AI solutions. Such effects already occur in various areas. If unmonitored forms of AI experiments are released into society, individuals will suffer from data breaches, unfair uses, biased algorithms, surveillance and much more. All in all, very little attention is paid to the potential misuse of AI systems, even though massive damage can be done with those systems.

We are not opposed to internal AI ethics boards. But it is clear that individuals enforcing ethics and legal requirements has to be included in the development teams and the management of the companies. Ideally there should also be an organization that could set joint requirements and coordinate efforts to create Trustworthy AI. These are hard problems, and discussing best practices for algorithmic systems raises awareness of their potential flaws and helps finding solutions. But based on the lack of attention to these issues it is fair to say that society is not safe from the most harmful effects of new AI technologies and we need to give these issues the proper attention and we need to take the appropriate measures to protect personal data.

We have identified a number of primary challenges that must be addressed by OEMs and suppliers alike:

Ethical challenges:
(1) Designing a clear process for informed consent to use personal data, and limitations for collection of personal data,
(2) differentiated consent to use different types of personal data-sets,
(3) ability to use an AV without giving blanket consent to all form of data collection,
(4) data safety and transparency on what the data will be used for, which entities your personal data is sold to and for what purposes, including a specification of "legitimate interest" under GDPR and the ePrivacy directive,
(5) algorithmic fairness and biases,

(6) de-identification, anonymization and encryptions of data,
(7) Ethical dilemmas e.g. traffic safety vs privacy and pointing out disables, and
(8) prohibition on surveillance, use of biometric data to monitor individuals and secondary use of personal data.

Legal challenges:
(1) lack of sufficient legal protection for individuals and personal data in an AI/connected vehicle setting,
(2) lack of regulations and legal requirements on data collectors and resellers,
(3) unclear responsibility, control of & consent for automotive sub-supplier's personal data collection (such as Google, Smart Eyes etc),
(4) cybersecurity breaches,
(5) intellectual property law (data ownership), and
(6) Rules for data transfer to different countries.

Ethical principles and legal requirements have to be taken into account when designing AI systems and other connected vehicle functions. If the data handling is not designed with consideration taken to human autonomy, prevention of harm, with fairness and is possible to explain trust can (will) be lost.

We have realized that it is probably possible to use existing Safety methodologies and approaches e.g.: "Design for Safety" – "Design for integrity/privacy, use of Safety Performance Index (SPI) – Integrity Performance Index (IPI). One of the interviewees suggested defining "Integrity Cases" compared to "Safety Cases".

It is crucial that a human-centric perspective gets at the forefront of development efforts. This is a major challenge as it involves conflicting perspectives and interests that require compromise solutions.

5. Conclusions, Lessons Learnt and Next Steps

Unfortunately, we did not manage to engage enough stakeholders from the automotive industry to be able to submit an application to FFI in June 2022. Hopefully we may mobilize for an application to FFI in December 2022. However, we do have a dilemma. The FFI/Vinnova calls are directed primarily to the automotive industry while AI calls are more general. When writing this final report there does not seem to be any relevant Vinnova calls for Trustworthy AI in the AV setting.

We hope this will change as this is an area that needs a lot more attention as it has become apparent that currently the legal and ethical aspects of the AI applications that are being developed are almost not considered at all. There is a need to determine through a larger study how the Ethical and Legal challenges can be met in particular around these four areas:

1. Respect for human autonomy and privacy

2. Prevention of harm

3. Fairness

4. Explainability

During the spring, when conducting this pre-study, we have noticed several Swedish "incidents" regarding violation of data privacy, e.g. Apotea, Apoteket, Kry. All of the corporations involved in these violations have sold their customers´ sensitive data to third parties (Facebook) without their customers knowledge or informed consent. If similar violations are being done by OEMs and AV it might hinder the acceptance and implementation of AVs. Citizens are becoming more aware of the risks associated with personal data handling, tracking, monitoring and misuse.

6. Dissemination and Publications

Since this was only a small pre-study we have not yet published any articles. We submitted an application to a workshop proposal to SCSSS2022 , but unfortunately the application were rejected.

7. Acknowledgement

We would like to thank Håkan Sivencrona at Zenseact who listened and believed in us and who has taken the time to support us so that we had the opportunity to apply and carry out this feasibility study. If the interviewees had not taken the time to be interviewed without any compensation whatsoever, there would have been no report, so of course we also want to thank them. Finally, we also want to thank SAFER who also considered Trustworthy AI to be an interesting and important area within Traffic Safety and an opportunity to contribute to the Global Sustainability Goals.

ANNEX 1

KR1: Human agency and oversight
Interactions between humans and AVs should follow human-centric design principles, securing human oversight of driving automation systems in AVs.
Risks/opportunities? Human-centric design principles is this something you apply in your company? How to ensure human oversight? Communication between the human and the vehicle?

KR2: Technical robustness and safety
These requirements are linked to the principle of harm prevention, with a strong impact on user acceptance. Attack resilience and security of AVs must be addressed from a heterogeneous, constantly updated approach, starting from security by design. There is a lack of scenarios to assess human agency and oversight, as well as transparency and fairness.
Risks/opportunities? Security by design - what does that mean to your company? How to evaluate/assess (continuously)? Lack of scenarios?

KR3: Privacy and data governance
New innovative approaches have to be implemented to ensure data protection without negatively affecting the safety of AVs, including agent specific data anonymization and de-identification techniques, while preserving relevant attributes of agents. Consent to the processing of personal data for drivers and passengers, including the exchange of data with other vehicles and infrastructures.
Risks/opportunities? Privacy by design – Is this something you apply in your company? How?

- Consent to the processing of data (drivers and passengers)? Consent to what? Data handling towards 3:rd party? Suppliers consent? If not consent? How to hinder misuse of personal data?

KR4: Transparency
New explainable models and methods should be developed, focusing on explanations to internal and external road users, i.e. new research related to explainable human-vehicle interaction through new HMI and eHMI. Explainability as a requirement for vehicle type-approval frameworks will enhance the assessment of safety, human agency and oversight, and transparency, but will require new test procedures, methods and metrics.
Risks/opportunities? How does your company explain the human-vehicle interaction? How do you communicate risks with the customers? Explainability as a vehicle type-approval framework? Approve to what?

KR5: Diversity, non-discrimination and fairness
To avoid discrimination in decision making, AVs must avoid any kind of estimation based on potential social values of some groups over others (e.g., dilemmas) and must be designed to maintain the same level of safety for all road users. Efforts are needed to identify possible sources of discrimination in state-of-the-art perception, different inequity attributes such as sex, age, skin, tone, group behaviour, type of vehicle, colour, etc.
Risks/opportunities? How to secure? Procurement/sourcing requirements and supplier evaluations?
AVs opens up new autonomous mobility systems, services and products. How to secure 3rd party service and product provider? How to secure non-bias?

KR6: Societal and environmental well-being

Understanding and estimating the impact of AVs on the environment and society is a highly multidimensional and complex problem, involving many disruptive factors, for which we can only make predictions based on as yet uncertain assumptions.
Risks/opportunities? Is this something your company has a responsibility for? How and in what way?

KR7: Accountability [Ansvar]
As a safety-critical application, AVs must be audited by independent external auditors. Establishing the minimum requirements for third parties to audit systems without compromising intellectual and industrial property is a major challenge. The adoption of AVs will entail new risks. Policymakers should define new balanced and innovative frameworks to accommodate insurance and liability costs between consumers and injured parties on the one hand, and AVs providers on the other.
Risks/opportunities?
How to insure when OTA and continuously up-dates (vehicle/driver)?

--- end of document ---