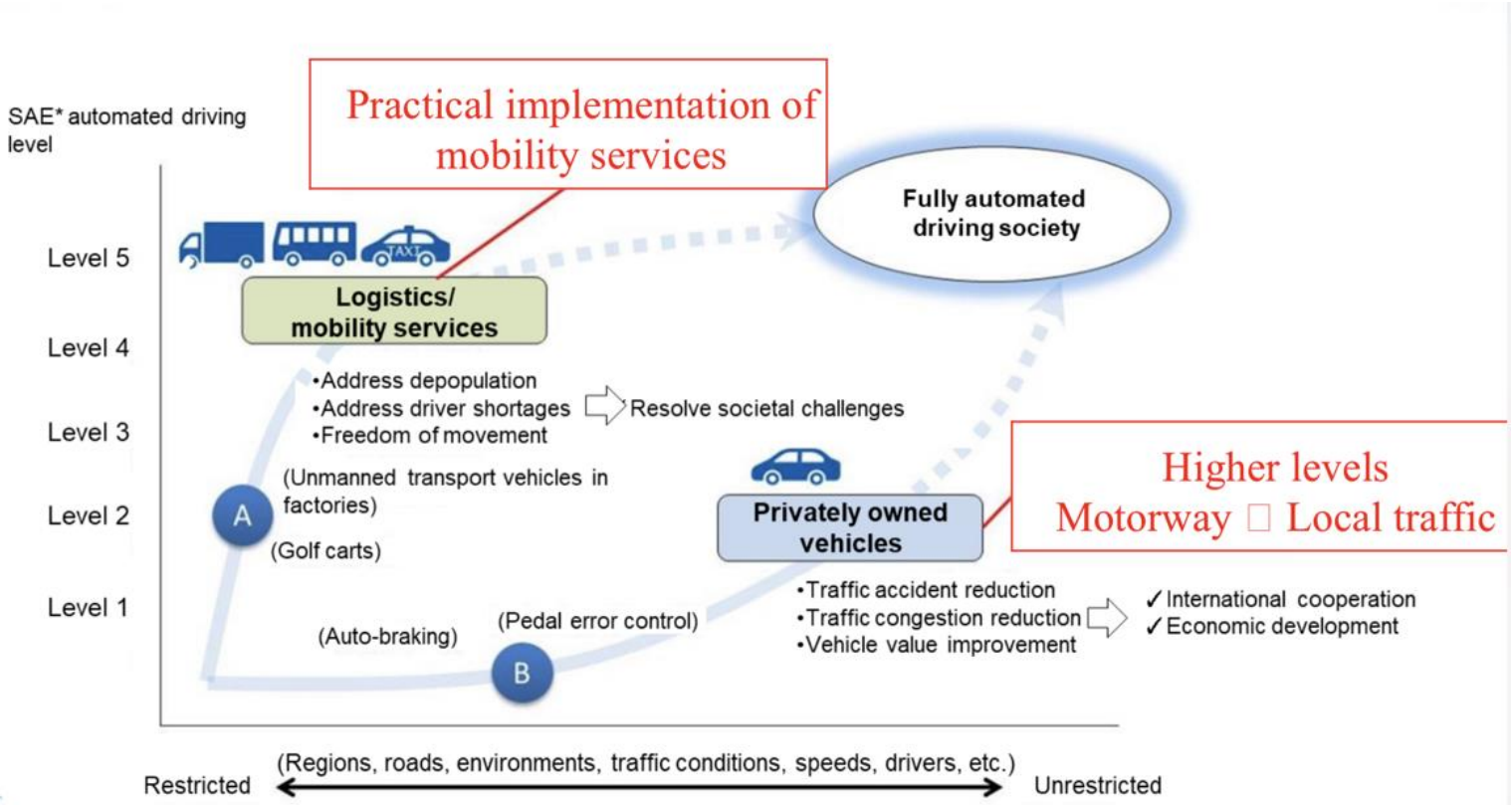
ITF Roundtable on Artificial Intelligence, Machine Learning and Regulation

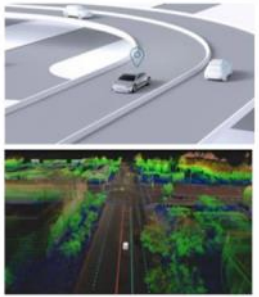
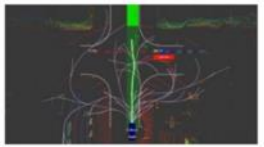
Session 4 – Institutional & Regulatory Aspects

Martin Russ, AustriaTech

The 2 „main pathways of automated mobility“



AV domains powered by one/more AI systems

Localization	Dynamic Scene Understanding	Path planning	Control	User Interaction
	 	 	 	 
Where am I? *Where am I heading?* *HD maps (static objects)* Trustworthy Localization	*Dynamic agents* *Action/trajectory prediction* *Free space* Trustworthy Scene Understanding	*Trajectories* *Environment* *Future agents' trajectories (predictions)* Trustworthy Path Planning	*Steering* *Speed* *Lateral & Longitudinal Control* Trustworthy Control	*User commands* *Request to intervene* *Other agents' interaction* Trustworthy Interaction

+

Trustworthy

Societal

Impact

??

Source: Trustworthy Autonomous Vehicles, 2021, EC JRC

SET-UP

The key challenge is how to ensure the **safety** of an automated system that employs Artificial Intelligence (AI) and Machine Learning (ML) for **scene interpretation and decision-making processes**

Session 4 should focus on how to build an **effective management system** within service providers and supervising authorities to ensure the **robustness, reliability and security of AI systems**.

What will be the **right level of human oversight** and how to **shift governance and liability frameworks** based on human-operated systems to those operated by AI?

→ *When discussing the right institutional framework and governance structure, it seems important to tackle **regulatory challenges for AI operated systems**.*

→ In general, when regulating AVs and setting up an **appropriate** institutional **framework**, we should come to an approach, where we **also** start with "**where it makes sense?**" (with regard to environment, inclusiveness, access,…), instead of just asking "where and how can we guarantee safety?"

GENERALS QUESTIONS – TO BE UPDATED/ADAPTED DURING THEMATIC DISCUSSIONS…

- What roles and responsibilities do each level of government need to take to ensure the safety of safety-critical systems?
- What knowledge and skills gaps must be addressed, how should this be done and which actors/institutions are concerned?
- How do institutions affect the social acceptance of automated AI-based systems?
- How to reflect these institutional factors in the regulation of AI and automated systems?

AI IS DIFFERENT – HOW TO TACKLE?

austriatech

Q: What's different when regulating AI?

- explainability / transparency
- trustability
- Accountability
- *data usage & scalability*.

→ So different kind of KPIs/norms/standards will be needed
→ What can we learn from actual state of regulating?

Q: how to approach: a full visionary perspective (e.g. map of laws) vs. step by step learning?

- Where is AI vs non-AI the right denominator? When is it just Legacy vs. New?
- Is this depending on the use case and framework conditions (ODDs)

AI is blurring boundaries of our regulatory approaches

ᔓ Strict limits of single aspects vs. performance of system (AI)

Q: do we start/allow to start everywhere, or within certain domains, that

a) guarantee fast/effective learning

b) really show a necessity/sense (with regard to societal impacts, system enhancements) for using AI (assisting technology, easy/repetitive tasks)

APPLYING EUROPEAN AI RULES IN TRANSPORT?

Although **existing legislation provides some protection**, it is insufficient to address the specific challenges AI systems may bring.

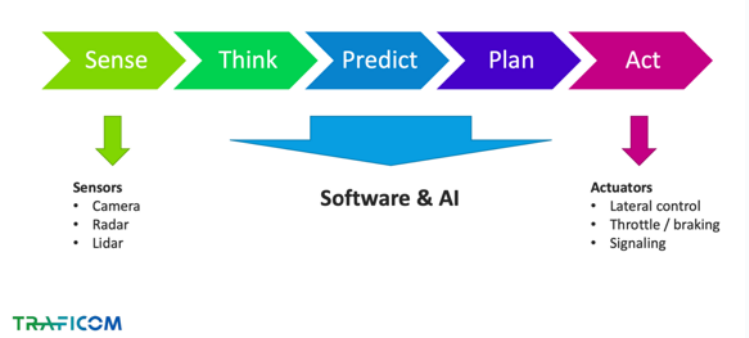
The proposed EU AI rules would:

- address risks specifically created by AI applications;
- propose a list of high-risk applications;
- set clear requirements for AI systems for high risk applications;
- define specific obligations for high risk applications;
- propose a conformity assessment before the AI system is put into service or placed on the market;
- propose enforcement after such an AI system is placed in the market;
- propose a governance structure at European and national level

APPLYING EUROPEAN AI RULES IN TRANSPORT?

So for Automated Transport (in narrower sense) this would mean….

- Risks: definition of common “edge cases” – risk catalogue for specific maneuvers (similar to early safety reports towards NHTSA
- High risk application – all driving/transport? Or specific use cases & maneuvers, specific ODDs/environments (e.g. schools)
- If high risk: how should an AI system act/ how should it be controlled (dual systems, learn from aviation, combination with classical control system, ?)
- Conformity assessment – based on edge cases?
- Enforcement: data recorder needed ?
- Governance structure? Adequate for all use cases applications (last mile, platooning, …)



austriatech

A RULE SET FOR AUTOMATED MOBILITY SYSTEMS/SERVICES?

For safety (and beyond)

- Integrate access, environment, where CCAM brings benefit for society
- Addressing benefits for systems performance – same/similar principles to be adopted?

Q: Can we/should we define specific focus areas to start with regulation?

AI enabled products & Services

- Sensing & Recognition
- Prediction & path planning
- Driving task
- In-vehicle-experience
- Predictive maintenance
- Fleet optimization
- Supply – demand matching
- Weather and environmental conditions
- Routing and traffic management
- Production & quality assurance
- Passenger/cargo demand prediction

INSTITUTIONAL/LEGAL PERSPECTIVES

- What **roles and responsibilities** do each level of government need to take to **ensure safety** of safety-critical systems?
- What **knowledge and skills gaps** must be addressed, how should this be done and which actors/institutions are concerned?
- How do institutions affect the **social acceptance** of automated AI-based systems?
- How to **reflect these institutional factors** in the regulation of AI and automated systems?
- How to develop/**establish an appropriate institutional landscape**? For law making, certification, operations and monitoring?
- Which **existing institutions** could be promoted / enhanced to fulfill those tasks? And how?
- **What's really different** when regulating AI?
- **How to approach**: a full visionary perspective (e.g. map of laws) vs. step by step learning?

INSTITUTIONAL/LEGAL PERSPECTIVES (2)

- **Where do we start**? “Everywhere”, or within certain domains?
- How and where to make use of a **uniform approach** of AI rules (EU AI Act/regulation) or do we need a **specific transport related approach** towards regulating AI? Can we agree on basic procedures & ingredients for different modes and applications/uses cases? If yes, which?
- Should we **define specific focus areas** of AI enabled products & services in mobility?
- Basic **procedures & ingredients for different modes** and applications/**uses cases**?
- How to **reflect key differences** of AI vs non-AI in our regulatory frameworks (data access/biases, ethical standards, performance metrics, ..)
- How could regulation/norming help in reducing the **tradeoff performance vs. trust**/safety
- Shouldn’t we just start with **safe testing of AI**? Are we there yet to lay out a **standardized rule set for future operations** of AI based systems?

Thank You

Martin Russ

Martin.Russ@austriatech.at

Kontaktadresse

Raimundgasse 1/6
1020 Wien, Österreich

T: +43 1 26 33 444
F: +43 1 26 33 444-10
office@austriatech.at