School of Mechanical Engineering
FACULTY OF ENGINEERING

UNIVERSITY OF LEEDS

MECH5170M
Connected and Autonomous Vehicles Systems

Regulation and legal requirement

Kris Kubiak (k.kubiak@leeds.ac.uk)

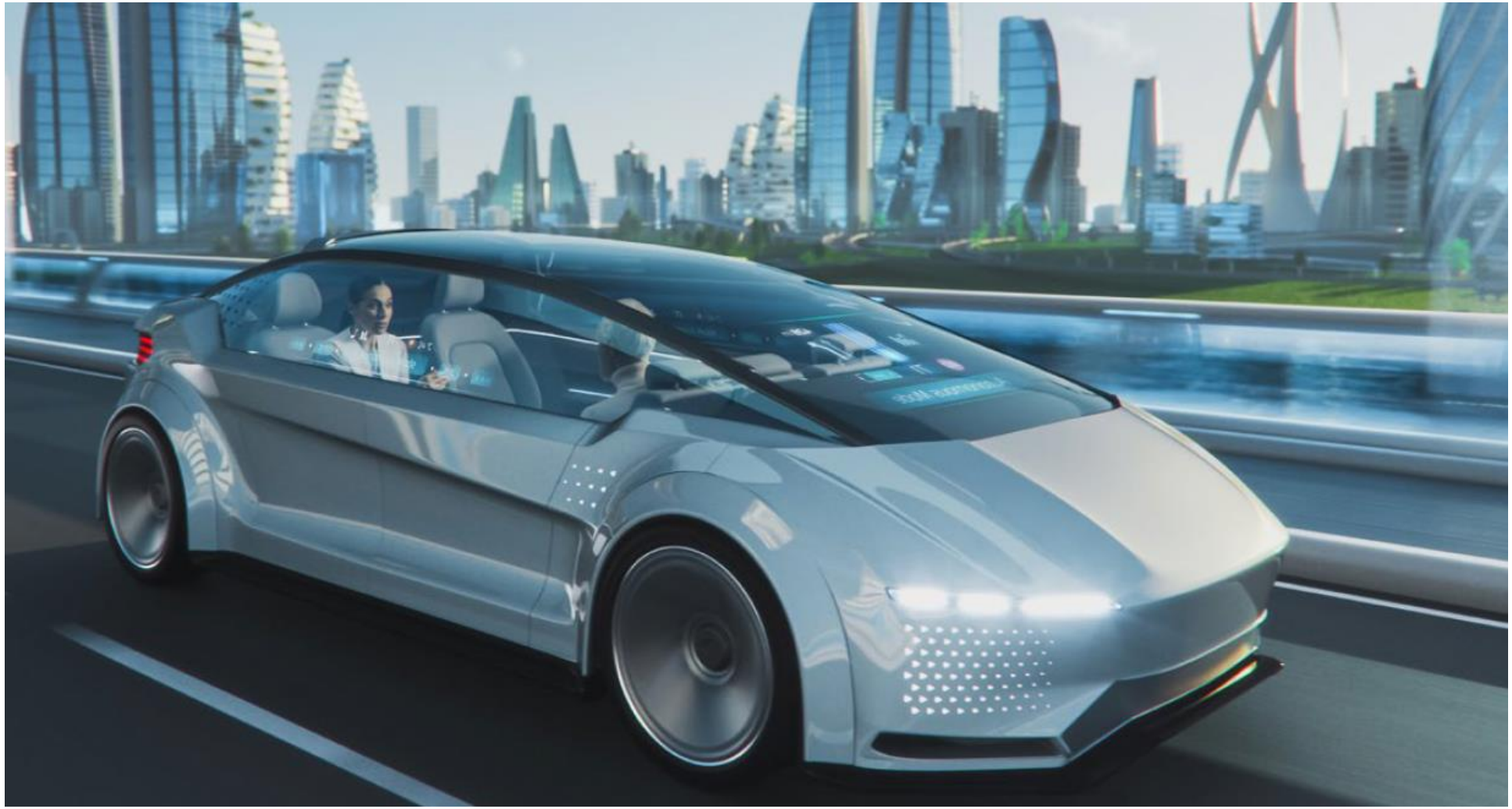
Introduction

- **10 million** autonomous vehicles will hit the roads by 2025
- **In 10 years** fully autonomous vehicles will be the norm
- AVs will generate a **£7 trillion** annual revenue stream worldwide by 2050
- Widespread adoption of AVs could lead to a **90% reduction** in vehicle crashes

An automated Uber Volvo was involved in a crash in Tempe, Arizona (2017)

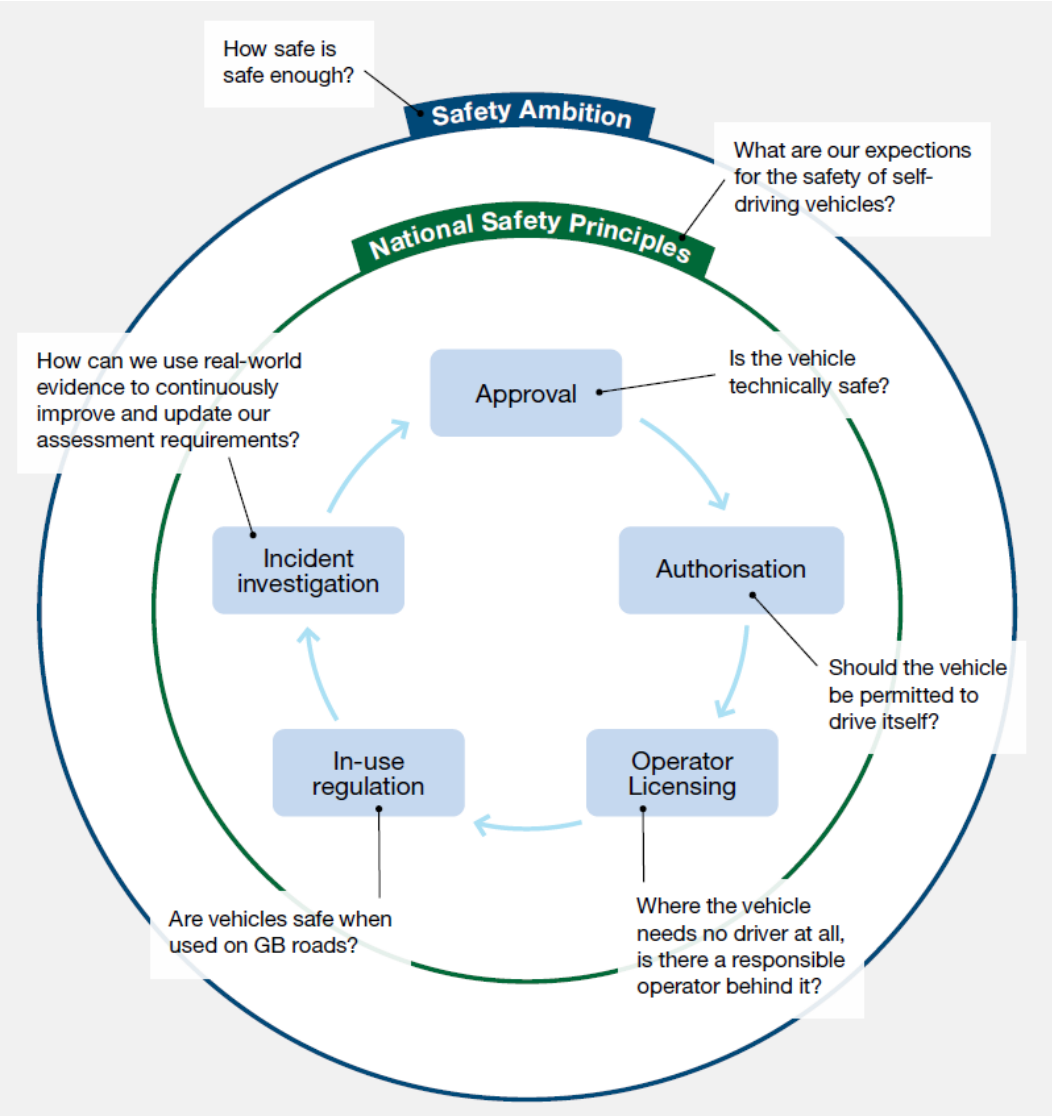
Self-driving car crash in Arizona: Red light runner hits Waymo van (2018)

Self driving vehicles vision



A new safety framework UK

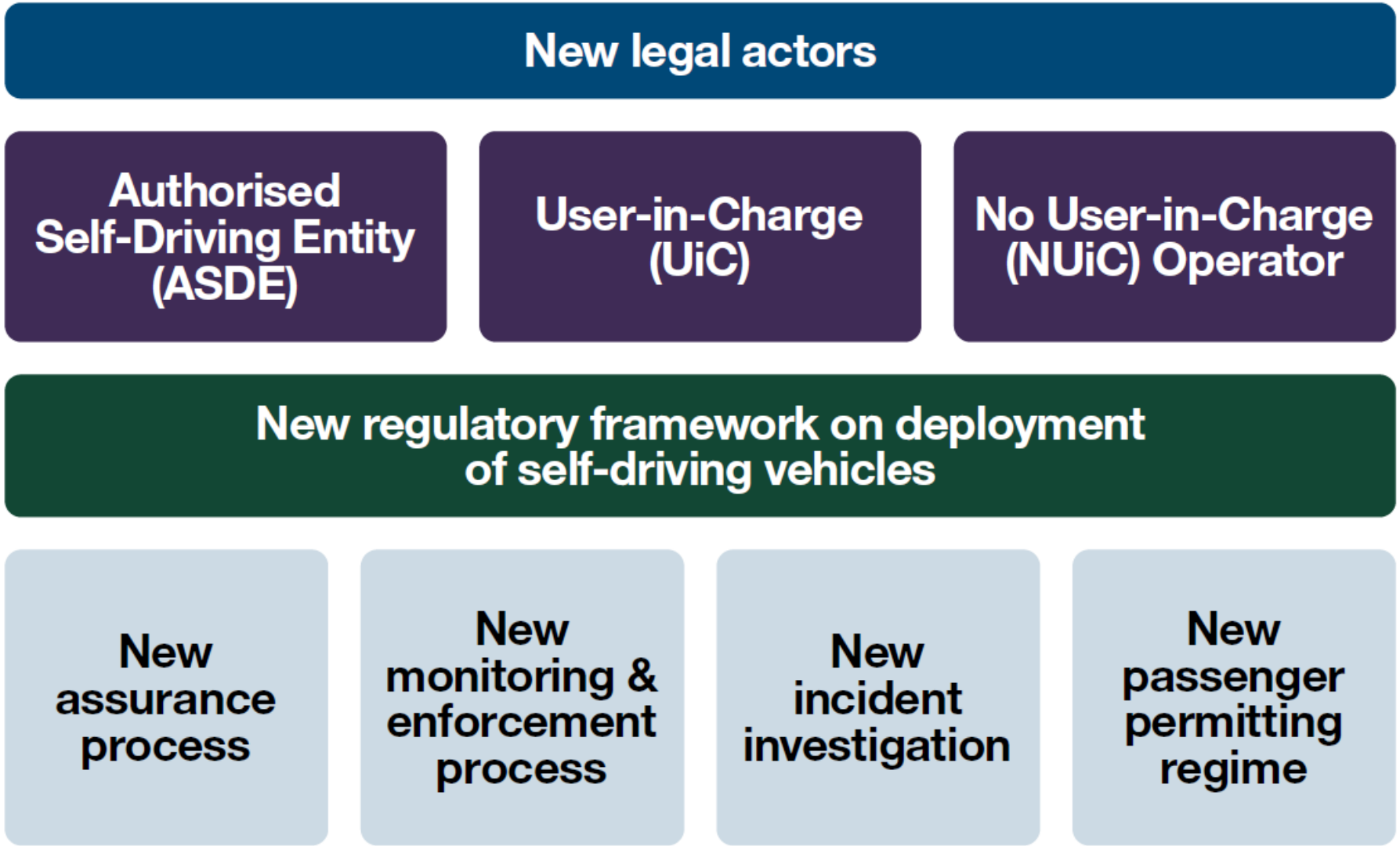
UNIVERSITY OF LEEDS



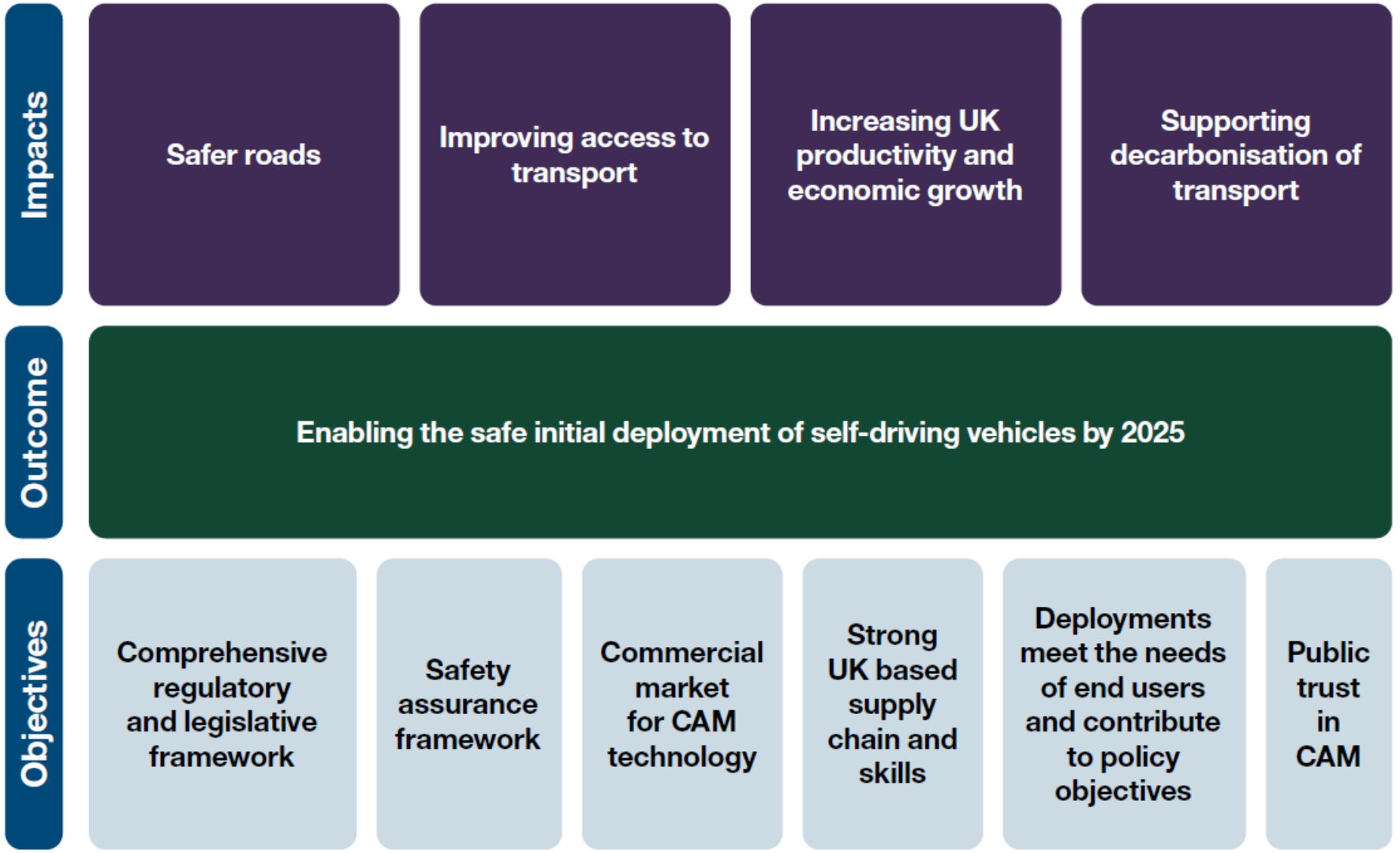
System pillars, which cover:

- Safe vehicles
- Safe road user behaviours
- Safe speeds
- Post collision care, including victim support

Primary legislation



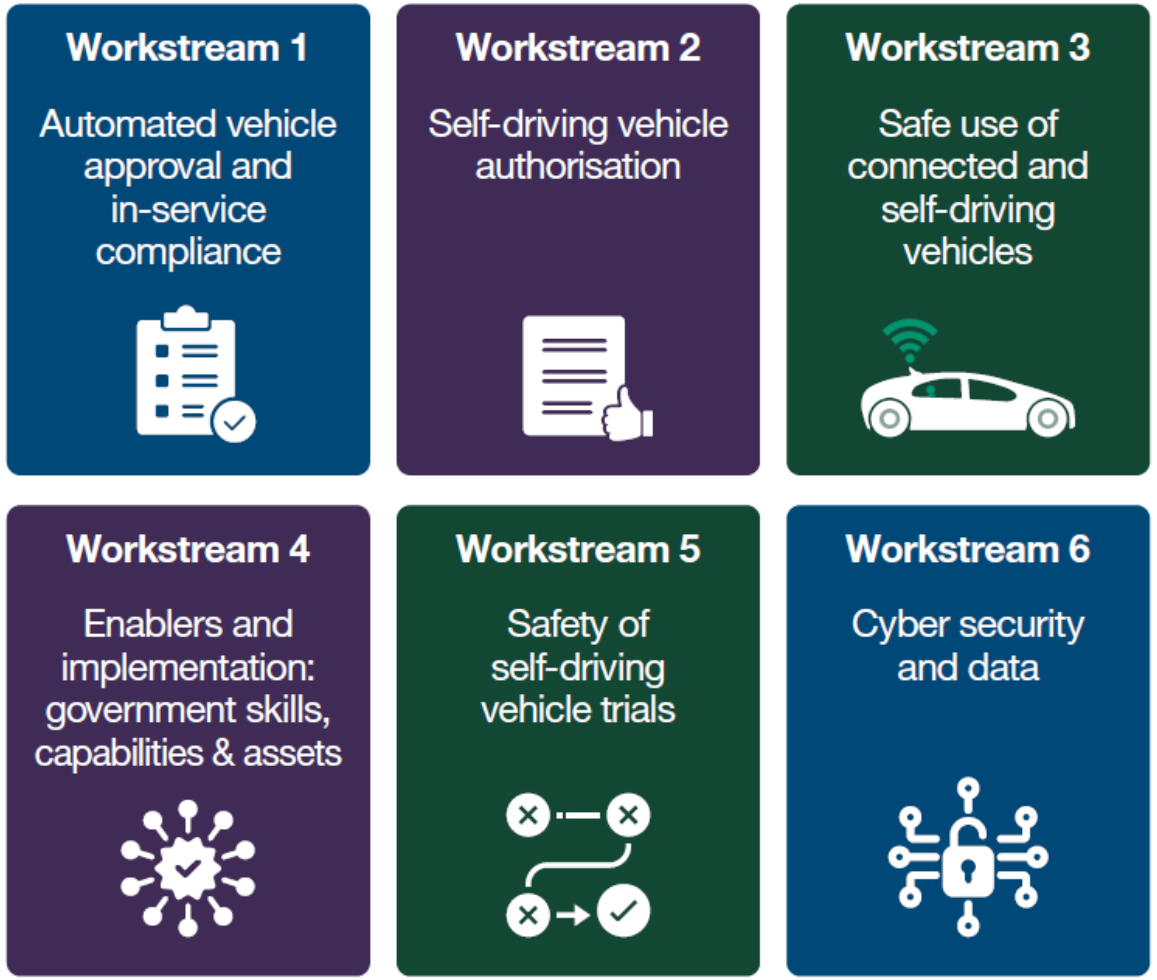
Theory of Change



CAVPASS workstreams

UNIVERSITY OF LEEDS

- Speed of the technology development
- Slow legal framework



Departments involved in legislation

- The Department for Transport ‘Transport Decarbonisation Plan’
- The Department for Transport ‘Transitioning to Zero Emission Cars and Vans: 2035 delivery plan’
- The Department for Transport ‘Future of Mobility: Urban Strategy’
- The Department for Transport ‘Future of Freight Strategy’
- The Department for Transport ‘Road Safety Strategy’
- The Department for Business, Energy & Industrial Strategy ‘Automotive roadmap: driving us forward’
- The Department for Business, Energy & Industrial Strategy ‘UK Innovation Strategy: leading the future by creating it’
- The Department for Business, Energy & Industrial Strategy ‘UK Research and Development Roadmap’
- The Department for Digital, Culture, Media and Sport 5G Testbeds and Trials Programme
- The Department for Digital, Culture, Media and Sport ‘Wireless Infrastructure Strategy’
- The Department for International Trade ‘Export Strategy’
- ‘Levelling up the United Kingdom’ White Paper
- The National Cyber Strategy
- The UK National AI Strategy
- The Department for Transport ‘Transport Employment and Skills Taskforce’
- Transport for Scotland ‘A CAV Roadmap for Scotland’

Case study: Wayve

UNIVERSITY OF LEEDS

Emerging as a spinout from the **University of Cambridge in 2017**, Wayve has since grown rapidly to become a globally competitive British automated vehicle start-up.

Based in London, the company has developed its ‘AV2.0’ technology that enables vehicles to ‘**learn’ to drive as a human would during testing on public roads**.

Wayve has recently partnered with Microsoft to design the supercomputing infrastructure required to accelerate this deep learning in self-driving vehicles. Using its ‘AV2.0’ technology, Wayve’s ambition is to be the first company to deploy selfdriving vehicles in 100 cities globally.

Company’s total equity over £258 million.

Liability for Autonomous Vehicle Accidents

Will courts treat autonomous vehicles as drivers and apply a negligence standard or as sophisticated technology and apply a product liability standard?

- How will liability be apportioned?
- Fleet Operator/Service Providers
- Vehicle manufacturers
- Technology companies/software manufacturers
- Local government's responsible for maintaining infrastructure

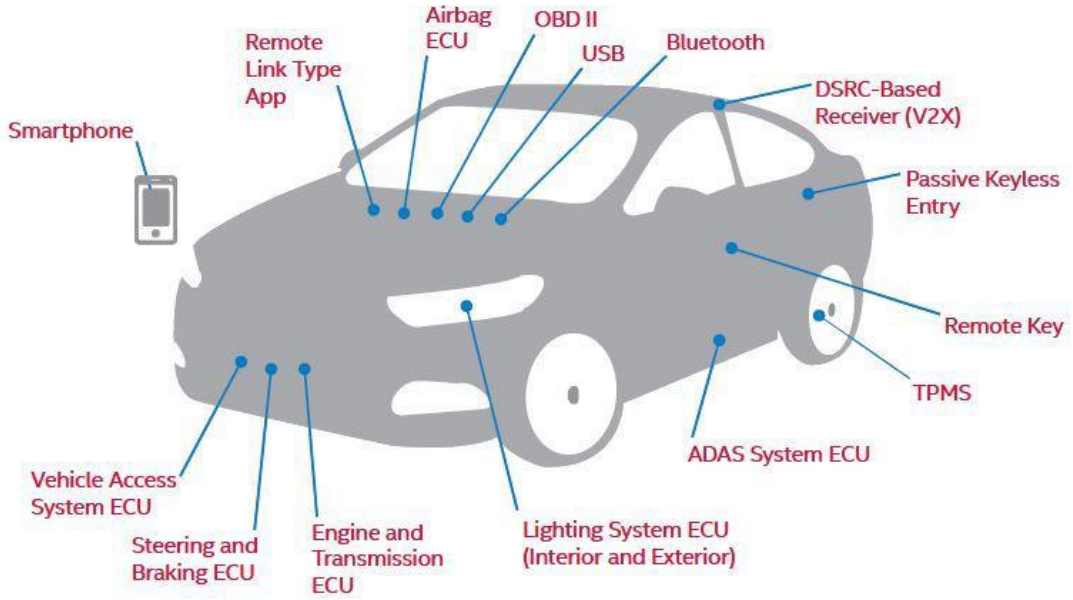
Managing Liability Among Parties

- Warranties should clearly define scope, responsibility and liability
- Responsibility for maintenance, repairs and updates should be defined
- Liability between automaker, technology company and vehicle owner/operator should be defined
- Responsibility for compliance with state and local laws and regulations should be defined

Cybersecurity

UNIVERSITY OF LEEDS

- Electrical Control Units (ECUs)
- Airbag, Advanced Driver Assistant System, Engine, Steering & Brakes, etc.
- On-Board Diagnostics (OBD) II Diagnostic Port
- Dedicated Short-Range Communications-Based Receiver
- USB Ports
- Passive Keyless Entry/ Remote Key
- Remote Link Type App
- Tire Pressure Monitoring System (TPMS)



Common Security Vulnerabilities

- **Software Glitches** – Connected vehicles today contain more than 100 million lines of code. More code means more opportunity for bugs and mistakes. Glitches, even when inadvertent, can be exploited.
- **No Single Source of Knowledge of or Control Over Source Code** – Software for different components of connected vehicles is being written by different developers, installed by different supplies, and no one source has knowledge of or control over the source code.
- **Increase Use of Apps Leave Vulnerabilities** – Consumers are using an increasing number of smartphone apps to interface with their connected cars and help run certain functions. Researchers have already demonstrated weaknesses in some of these apps. Likely to see spread in use of malware.
- **Need for Constant Updates May be Overlooked** – With the increased use of connected features comes an increased need for continuous updates to fix glitches and help protect vehicles. There is a risk these updates could be overlooked or that malicious actors could infect routine updates.

Privacy Concerns

"GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, profession, religious, and sexual associations. . . . I would take these attributes . . . into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."

"[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying on mundane tasks."

United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J. concurring).

Common Data Privacy Vulnerabilities

- **Data related to vehicle journeys** – Car makers, app developers, on-board assistance systems, etc. collect data regarding movements of vehicle. Length of time data is kept, who has access to it, and whether consumer has right to opt-out are key issues.
- **Data on consumer habits and preferences** – Data ranging from music preferences, news and radio selections, and other features is being used to target consumers. How this is done and whether consent is obtained will dictate potential ramifications.
- **Data from or related to children** – Collection, use, and storage of children's data is governed by special rules which should be considered.
- **Differences in regulations between markets** – Privacy regulations vary widely by region and market. For example, the EU implemented its data privacy and protection law, the GDPR, this May. The law includes a broad definition of personal information and strict requirements for consent and use and protection of such data. Companies working in the European market need to be prepared.

Insurance Considerations

Insurance of the **driver, vehicle, manufacturer, operator** ?

Changes required in the insurance industry:

- Recognize that rate of change
- Develop more technical underwriting capabilities
- Prepare for incremental changes to cost structures
- Navigate with insufficient or incomplete data
- Establish advanced analytics capabilities
- Plan for new products - including offering driverless car insurance

Summary

UNIVERSITY OF LEEDS

- A new safety framework required
- Local states legislation vs global requirement
- Cybersecurity
- Liability
- Privacy
- Insurance requirements

ANY QUESTIONS ???