Defining Safe Automated Driving

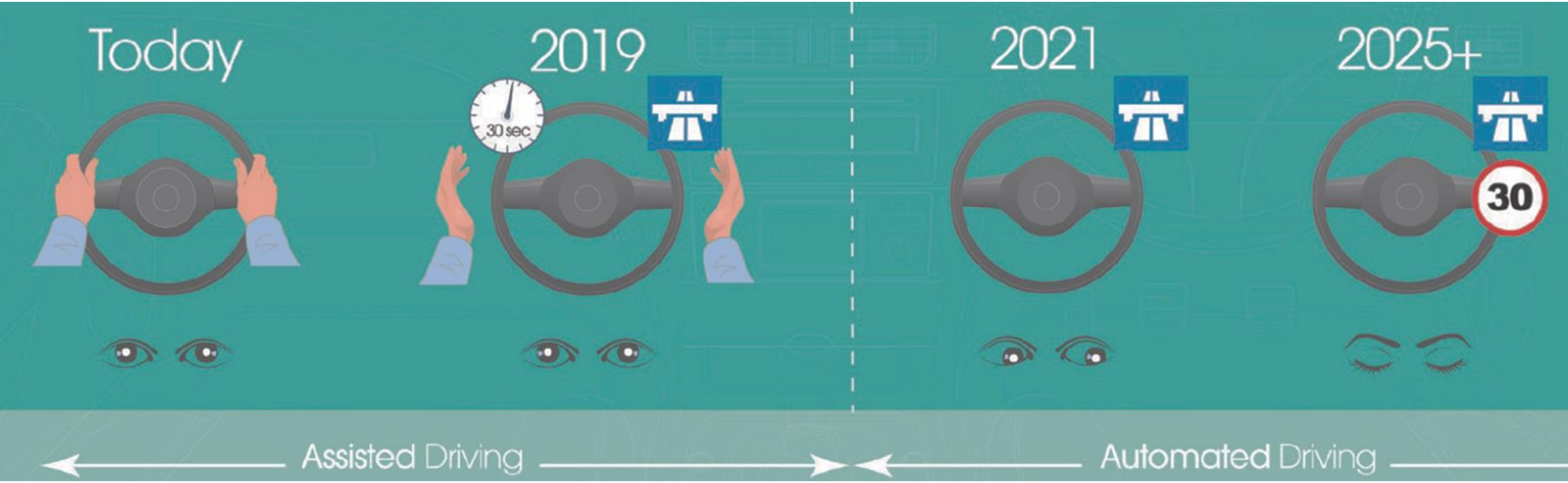
The Insurer View

ABI

Thatcham Research

A Journey to Automation

- The Insurer View – Assisted or Automated



Defining Safe Automated Driving

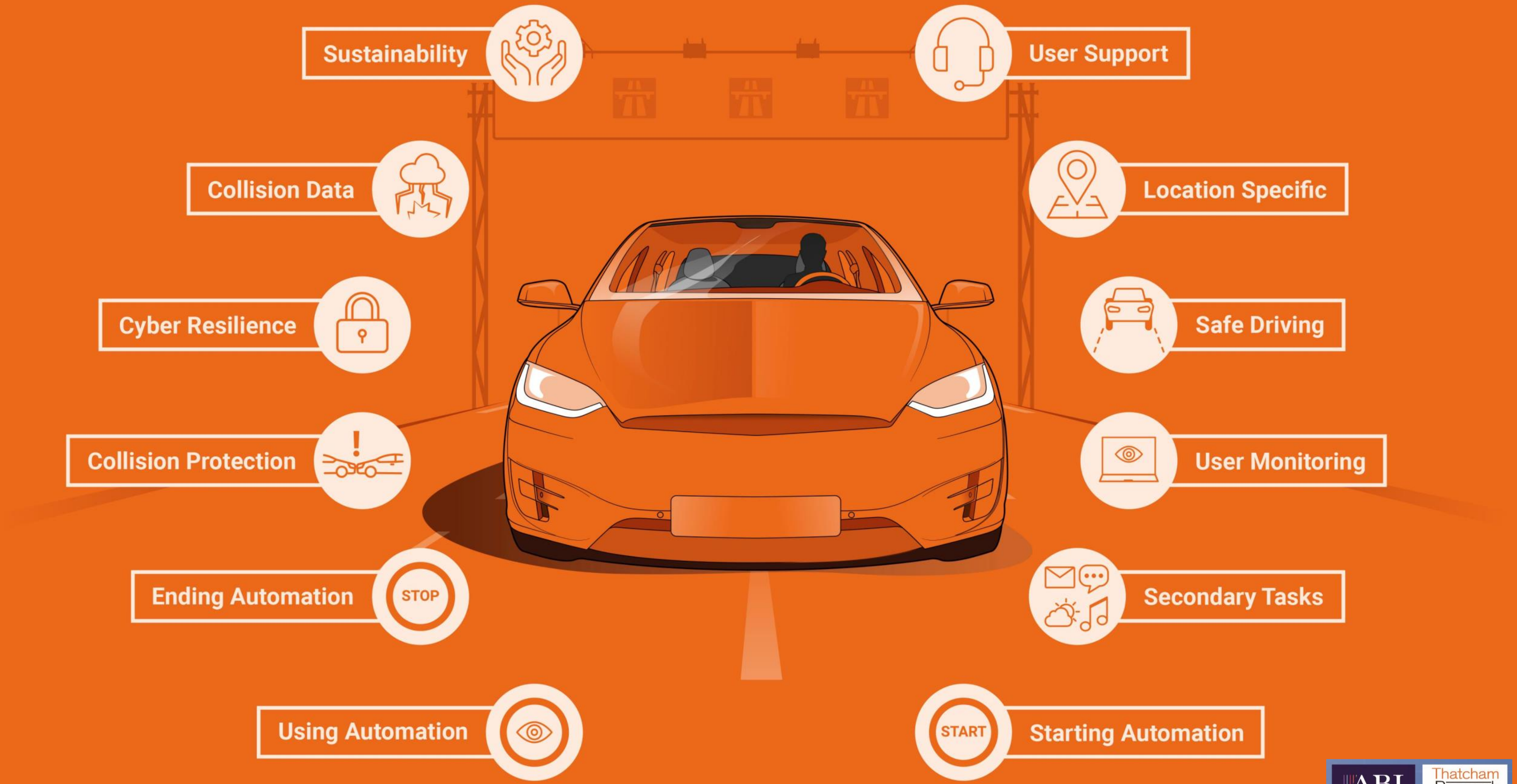
Insurer Requirements for Highway Automation

Thatcham Research

ABI

Automated Driving – Keeping it Safe

- UK Automated and Electric Vehicle Act **AEVA** facilitates Automated Driving by 2021
- Allows “user in charge” to undertake “secondary tasks”
- Insurers liability moves from the person to the car
- Changes to UK **Road Traffic Act** to allow public use
- Act defines Automated Vehicles – UN GRVA provides basis of functional definition
- International Insurers have defined “Safe Automation”– *www.abi.org.uk/defining-safe-automation.pdf*
- Identifies **12** Key requirements



Sustainability

Collision Data

Cyber Resilience

Collision Protection

Ending Automation

Using Automation

User Support

Location Specific

Safe Driving

User Monitoring

Secondary Tasks

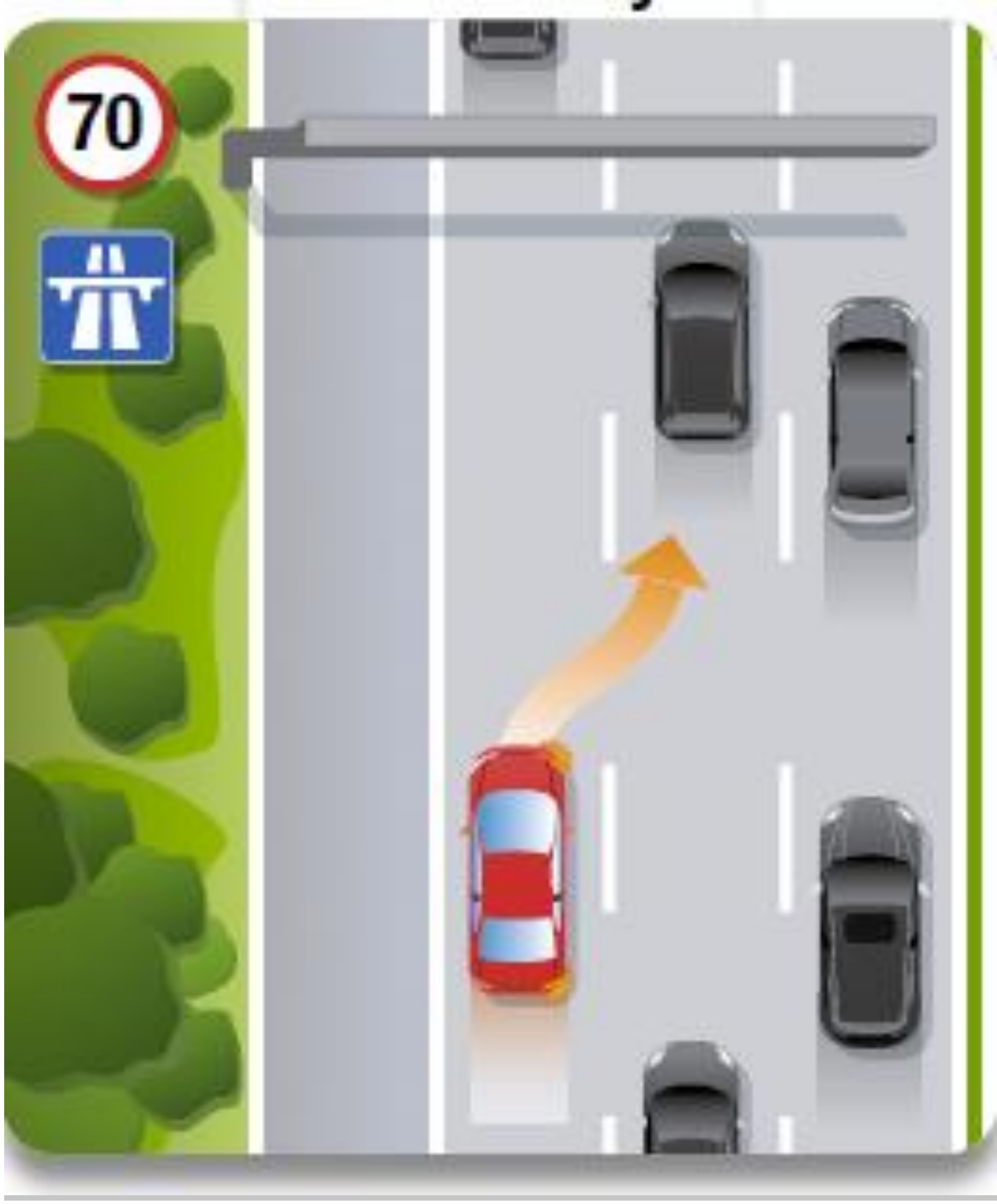
Starting Automation

#1 User Support
Naming and training

- Automated modes must be clearly differentiated from Assisted/Manual modes both in terms of information and implementation.
- The ADS must inform the driver of their obligations when using the system and the driver must accept these prior to using.
- Vehicle manufacturers must declare dynamic VIN level functionality data for individual vehicles including the latest software release to reflect changing capability.

#2 Location Specific –
Operational Design Domain (ODD)

- ODD requirements may include static (e.g. road type) and dynamic (e.g. traffic) features.
- The vehicle manufacturer must publish a definition of the ODD in which the ADS functions
- The ADS must be capable of accurately identifying when all conditions defining the ODD are met and predicting when they will be no longer met.



#3 Safe Driving

- The ADS must perceive and safely react to all foreseeable events encountered within the ODD.
- The ADS must interact and drive in a predictable and safe way with other safe and legal road users.
- Where software updates change capability or performance the VM must demonstrate that it complies with the required standards.

#4 User Monitoring

- Vehicles with ADS must have User-in-Charge monitoring systems capable of determining user status when starting, during and ending automation.
- During automation user attentiveness status must be used by the ADS to determine the best strategy for managing handover in a safe manner.
- When ending automation user monitoring must assess user status and the ADS must provide support until the user is reengaged with the dynamic driving task (DDT).

#5 Secondary Tasks

- The ability for a User-in-Charge to undertake distracting secondary tasks is a key motivation for using automation.
- Where the possibility exists for an **unplanned** handover from automation only tasks that link the user to the in-car infotainment system will be permitted. The use of nomadic devices, books, newspapers and sleeping will be prohibited.
- Where a **planned** handover can be ensured the use of nomadic devices will be permitted and in some circumstances sleeping may be permitted.

#6 Starting Automation

- The ADS must continuously monitor the vehicle and environment to assess whether the ODD requirements for automation are met.
- Automation will be offered only where the requirements for the ODD are achieved. The driver will not be able to request automation.
- When met the ADS can be activated with a clear *‘Offer and Confirm’* process.

#7 Using Automation

- During automation the vehicle must continuously indicate the ADS status.
- During automation the user may engage in appropriate secondary tasks.
- The user monitoring system must manage the user attentiveness to ensure they are ready for handover at the appropriate time.

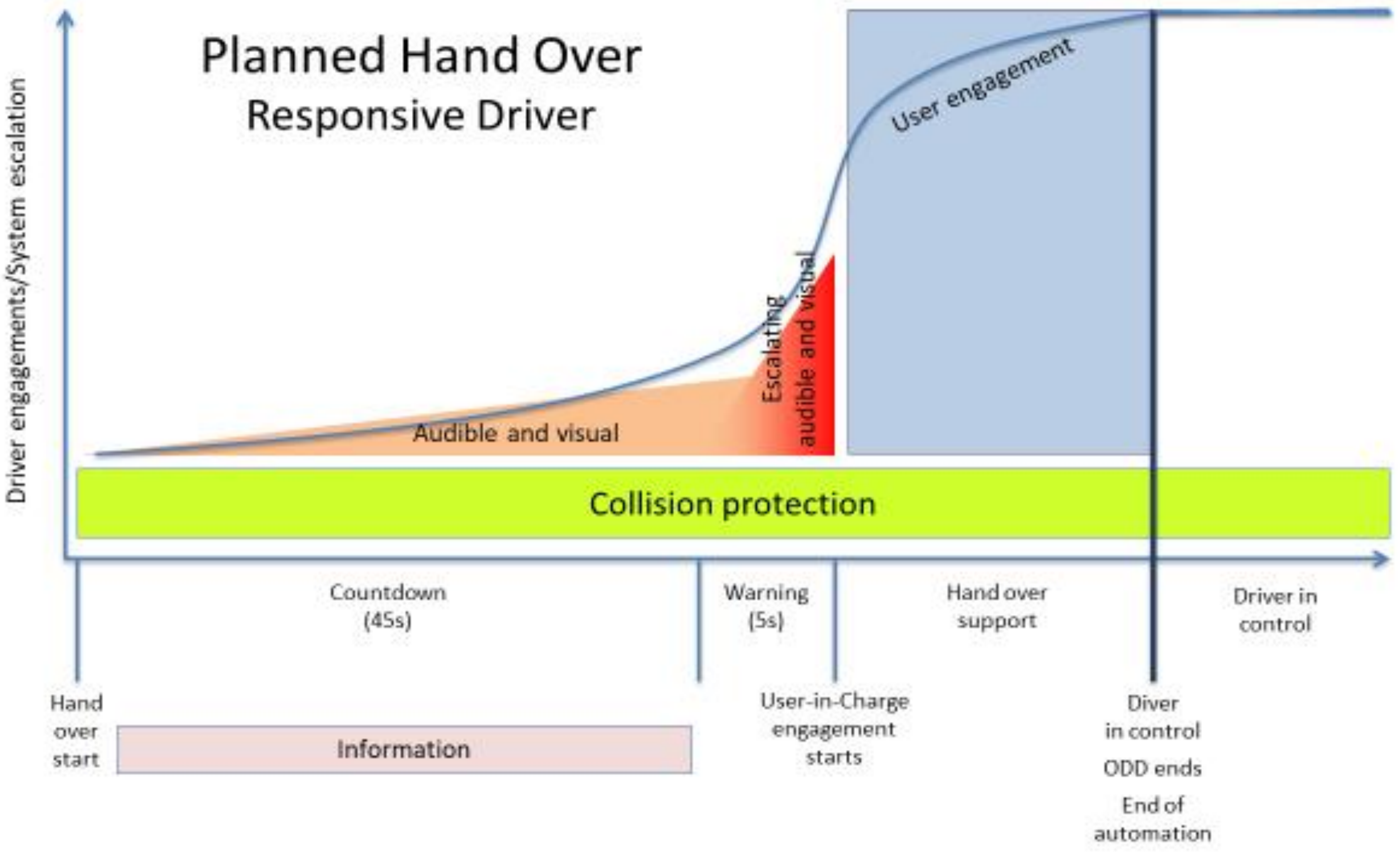
#8 Ending Automation

- **Planned** – ADS initiates a scheduled handover of control giving the User-in-Charge sufficient time to reengage with the DDT.
- **Unplanned** – ADS initiates a warning process to engage the User-in-Charge with the DDT immediately.
- **User-in-charge initiated –** User–in-Charge initiates an unplanned handover**.** Follows a multipath offer-and-confirm process to resume the DDT.
- **System Failure** – ADS initiates a warning process to engage the User-in-Charge with the DDT immediately. The system must maintain the capability to perform an MRM.

#8a Ending Automation

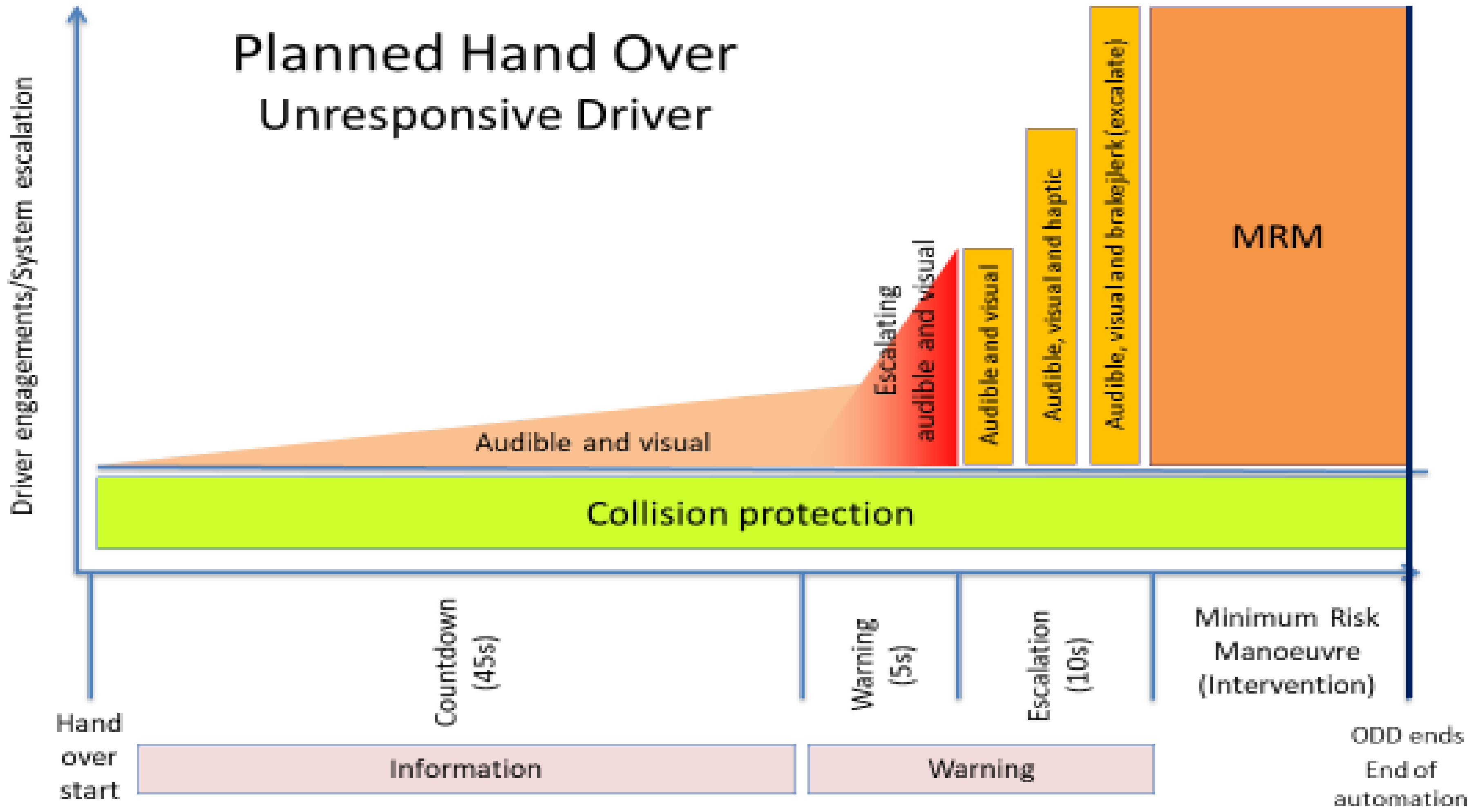
Responsive driver

- A **planned** handover**:** e.g. when a static, predictable ODD condition such as a highway exit is approached.
- ADS initiates a **planned** handover of control informing the user-in-charge with sufficient time to reengage with the Dynamic Driving Task (DDT).
- User monitoring must assess user status and the ADS must provide support until the user-in-charge is reengaged with the DDT.



#8 Ending Automation

Unresponsive driver



#9 Collision Protection

- Automated vehicles must be equipped with emergency collision avoidance technology that can react to all foreseeable critical situations in the driving domain.
- Emergency collision avoidance technology must engage when ADS is operating.
- Vehicles will require state-of-the-art passive safety protection.

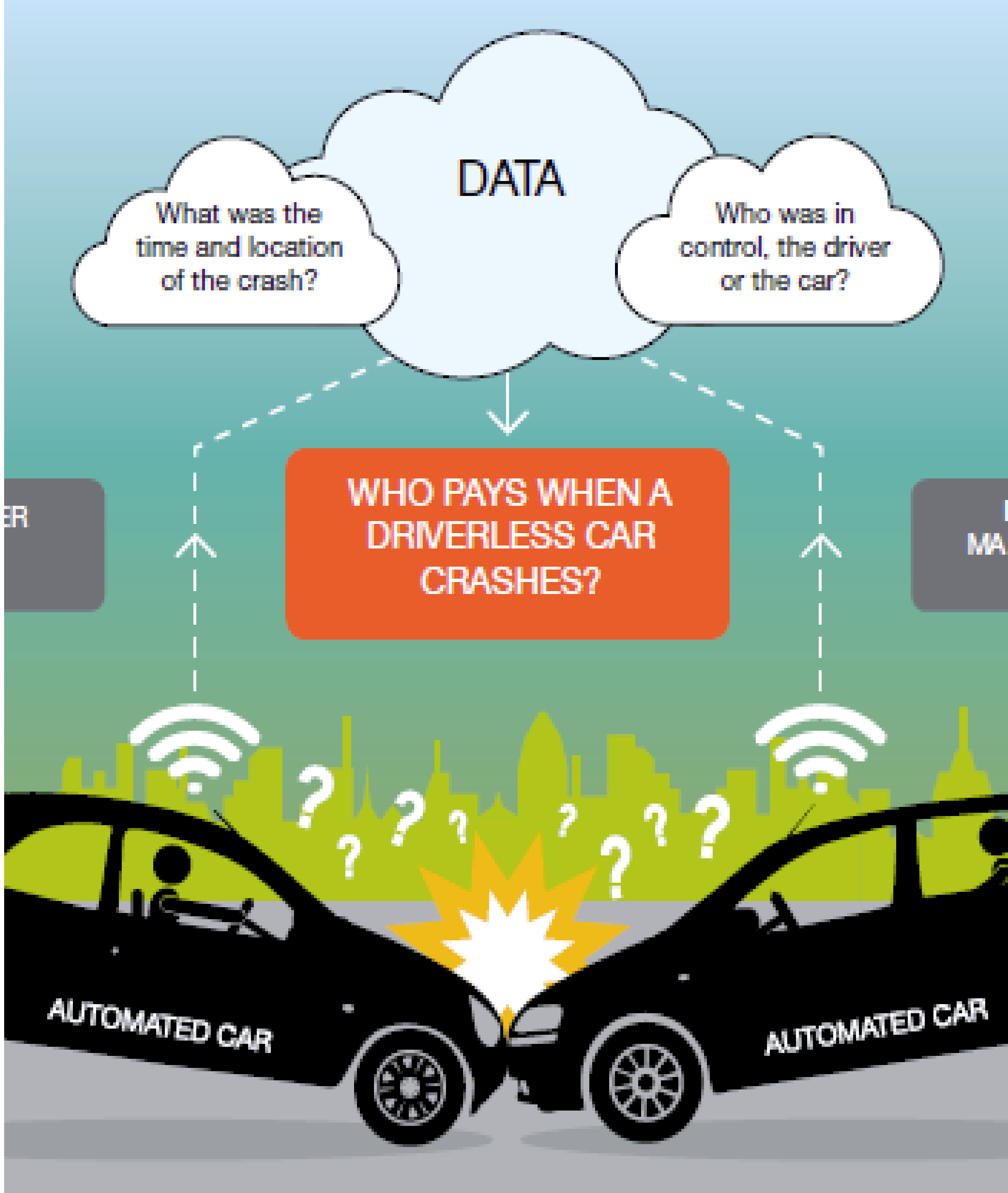
#10 Cyber Resilience

- ADS must be designed, developed and maintained to minimise the vulnerabilities and the consequences of cyber intrusion.
- ADS must meet UN ECE WP 29 regulations on cyber security and over-the-air software updates.
- Vehicle manufacturers, sub-brands, supply chains and vehicles must meet the ISO/SAE 21434 Automotive Cyber Security standard (due 2020).

#11 Collision Data

- Vehicle manufacturers must make a limited data set available to insurers confirming whether the ADS or the driver was in control leading up to a collision which must trigger in all collision situations

- GPS-event time stamp
- Activation status of each automated driving feature
- Driver acceptance between automated/manual mode time stamp
- Record of Driver Intervention of steering, braking, accelerator or gear-shift
- Driver Seat Occupancy
- User Engagement Commenced
- Has Minimum Risk Manoeuvre (MRM) been triggered
- System status (linked to fault code)

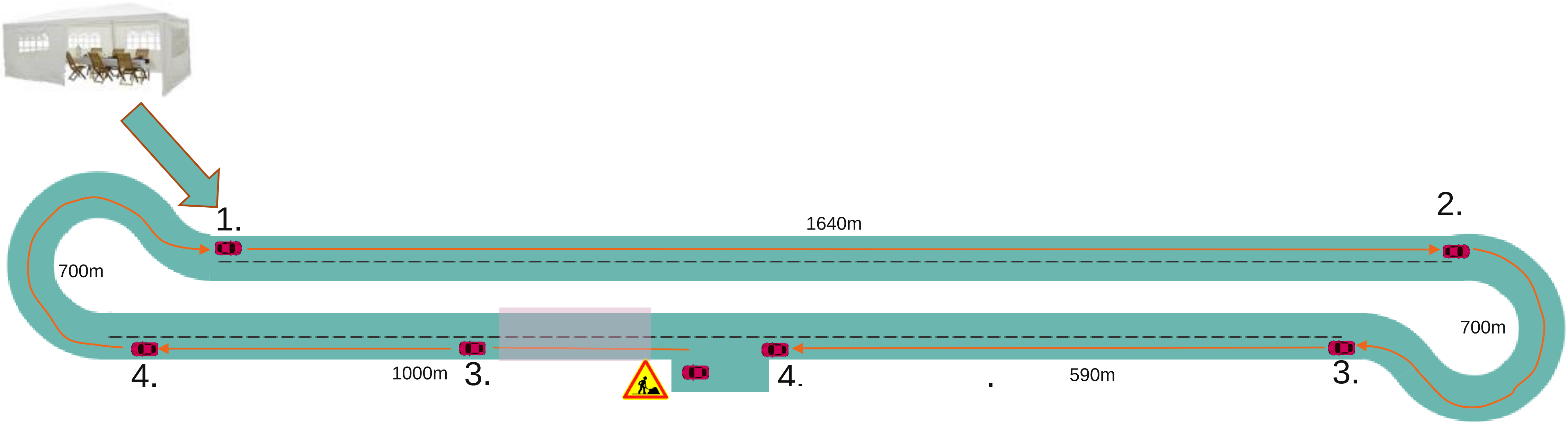

DATA
What was the time and location of the crash?
Who was in control, the driver or the car?
WHO PAYS WHEN A DRIVERLESS CAR CRASHES?
ER
MA
AUTOMATED CAR
AUTOMATED CAR

#12 Sustainability

- The emergency collision protection system shall be tolerant of sensor and vehicle degradation, maintaining full functional performance for at least 10 years incl software support
- Systems must be designed to be self-healing in case of minor damage or enable safe and cost-effective repair.
- A tell-tale must be displayed and system operation denied should system integrity checks detect a fault. This will be included in the data recording.

Thank You & Questions

Safe Automated Driving Demonstrations


1.
1640m
2.
700m
700m
4.
1000m
3.
4.
.
590m
3.