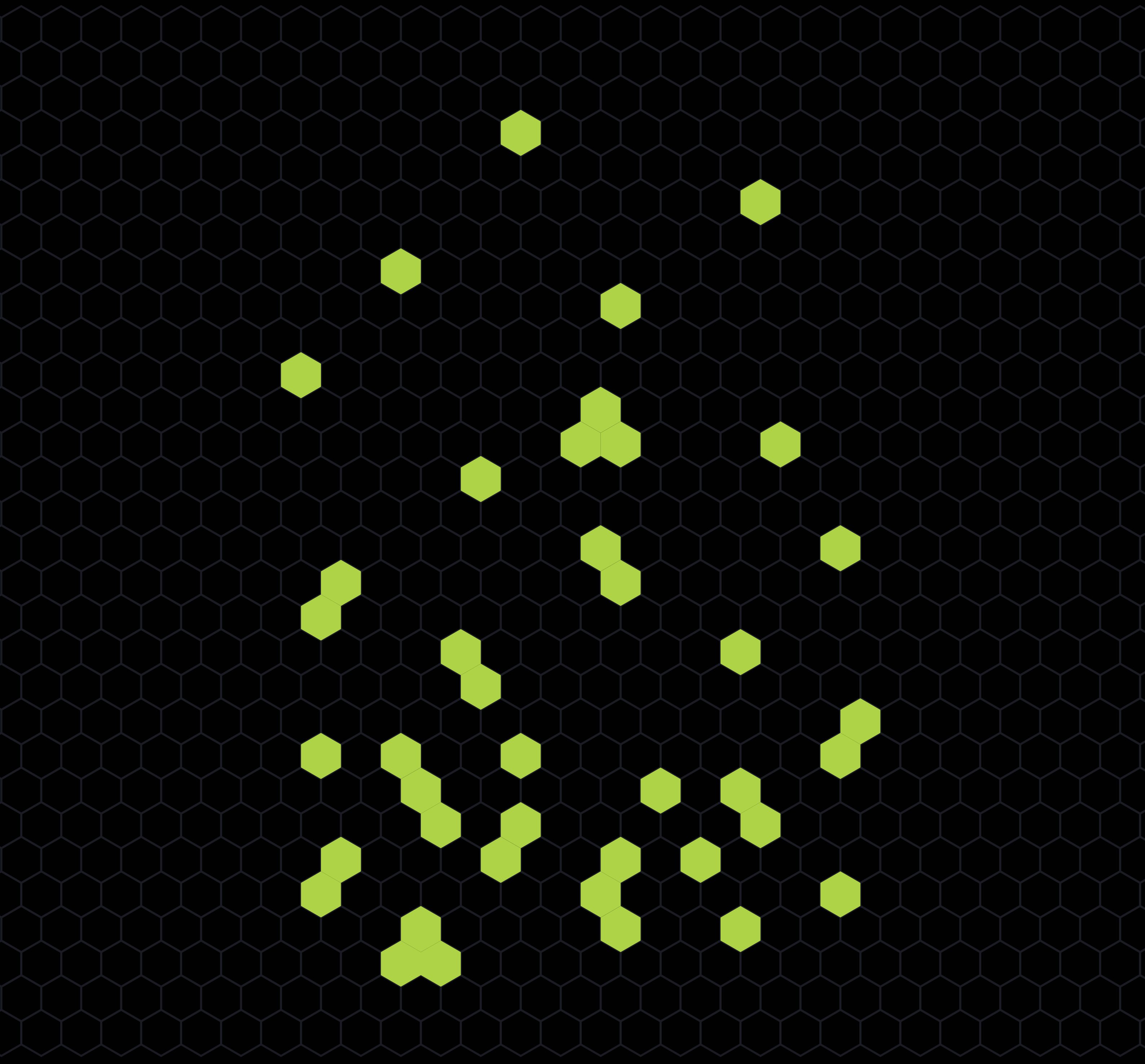
AUTONOMOUS TRIALS SAFETY CASE



Academy of Robotics

AUTONOMOUS TRIALS SAFETY CASE

HOUNSLOW PROJECT PARTIES

Lead Company
Academy of Robotics

Project Manager
William Sachiti

Trial Coordinator
Aaron Parsons

Press Manger
Jill Lloyd

Supporting Company
Eurovia UK

Project Manager
Joanne Saunders

Communications Manager
Shelley Benson

Supporting Company
4 Local Pharmacies

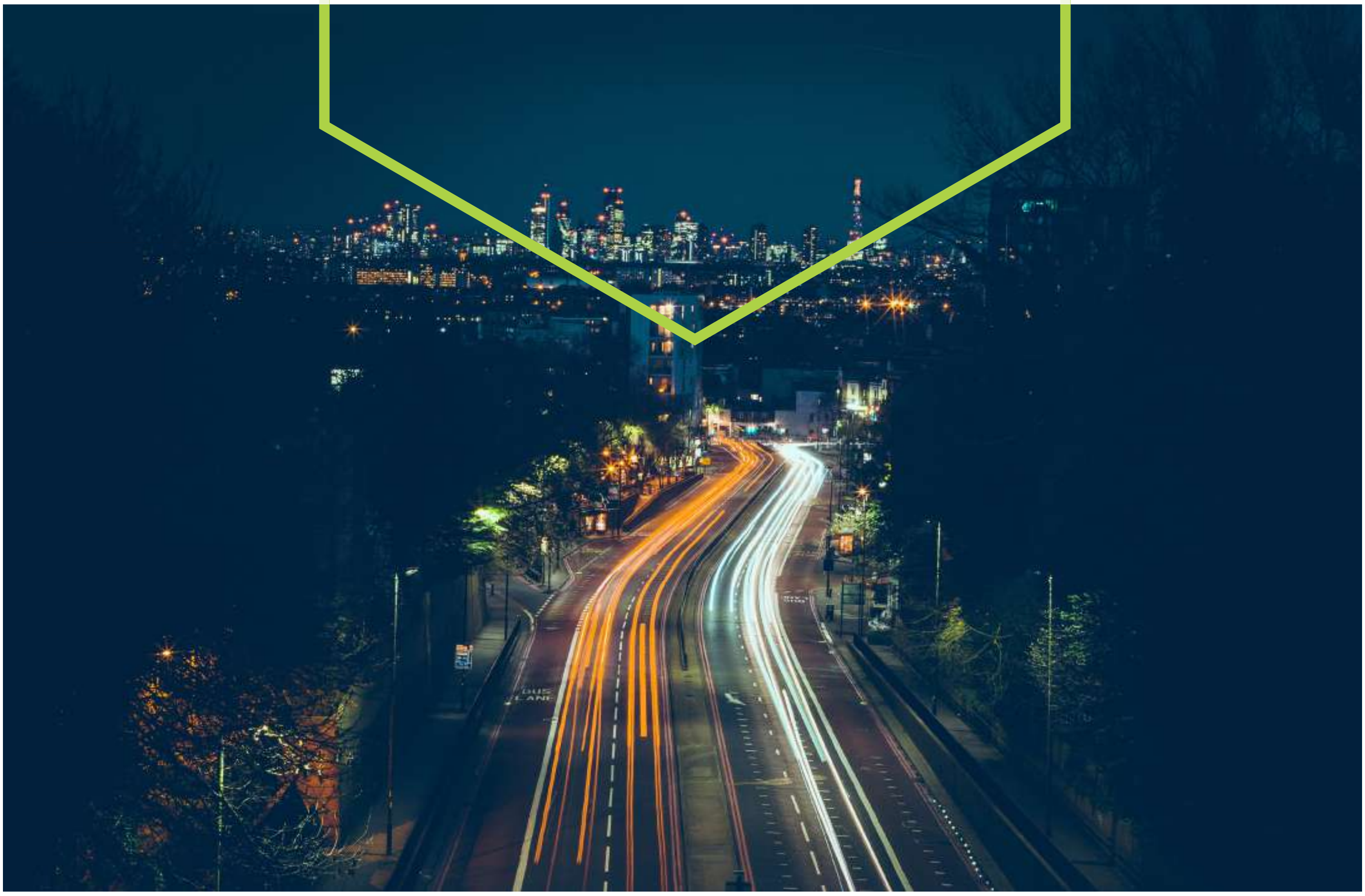
Location
Hounslow

Coordinator
Academy of Robotics

Supporting Company
2 Local Care Homes

Location
Hounslow

Coordinator
Academy of Robotics



CONTENT

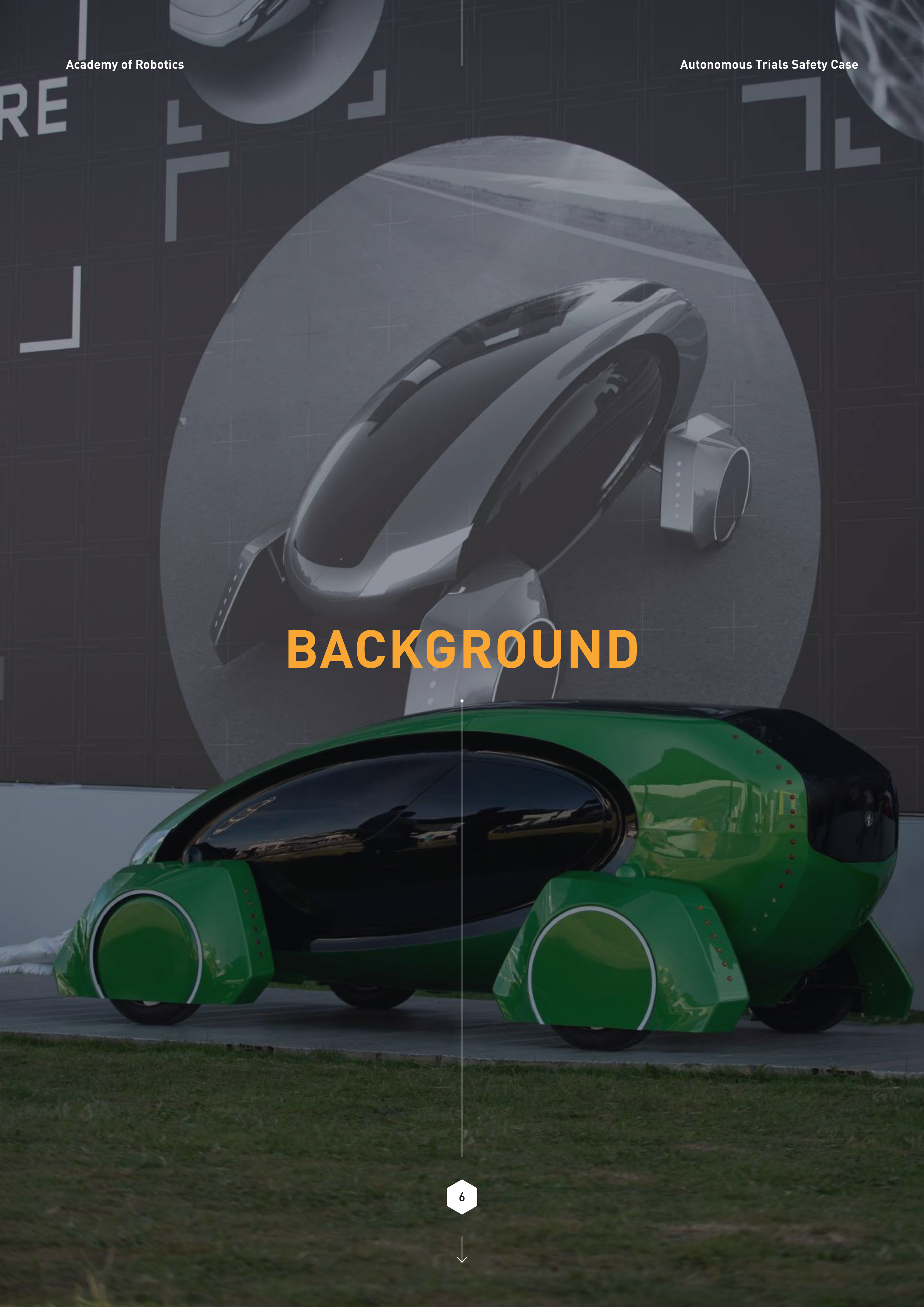
SEMI-AUTONOMOUS DELIVERY VEHICLE ROAD TRIALS, SURREY, 2020

The pilot will be carried out in accordance with the Centre for Connected & Autonomous Vehicles (CfCAVs) Code of Practice for Automated Vehicle Trialling.

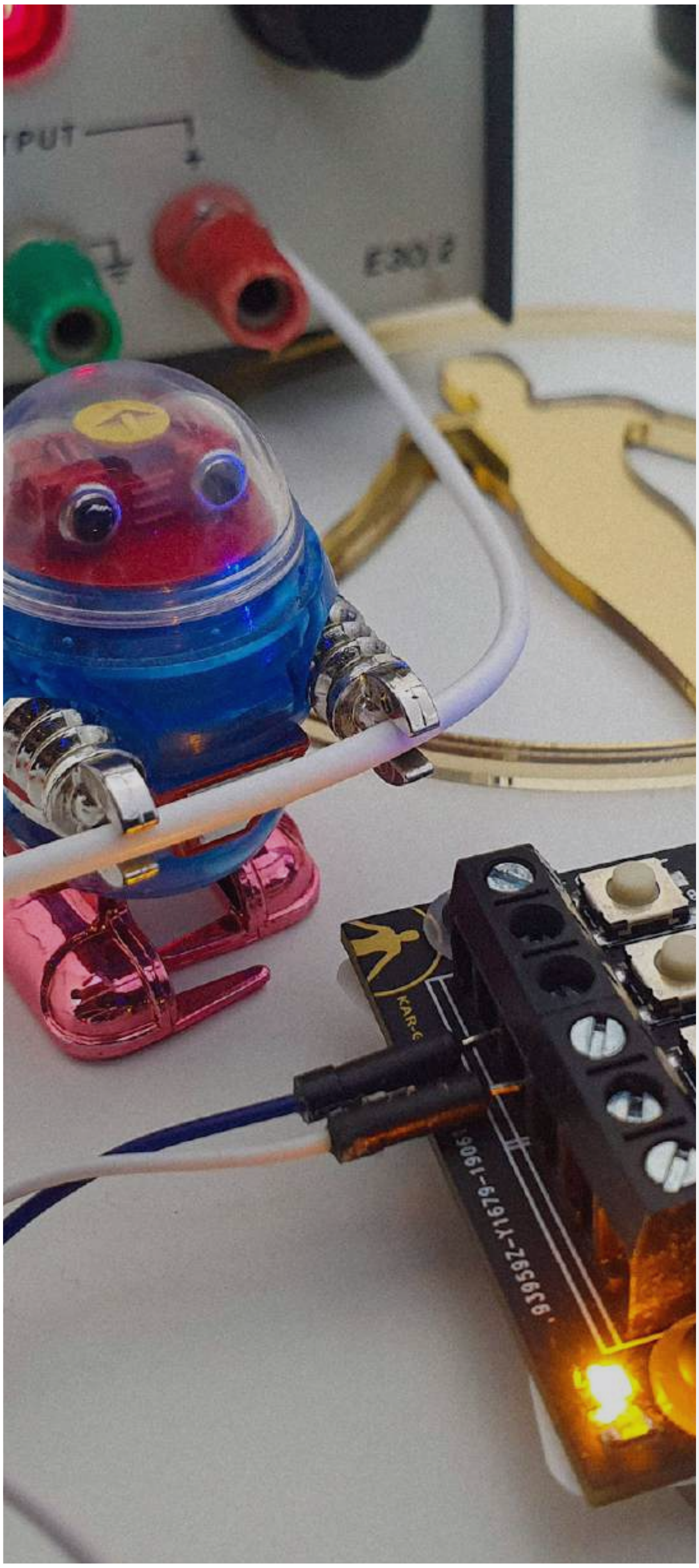
The UK Government has published stating that trialling any level of automated vehicle technology is possible on any UK road if carried out in line with UK law. Trialling organisations do not need to obtain permits or pay surety bonds when conducting trials in the UK. As part of complying with the law, they will need to ensure that they have:

- **a driver or operator, in or out of the vehicle, who is ready, able, and willing to assume control of the vehicle.**
- **a roadworthy vehicle.**
- **appropriate insurance in place.**

Newer legislation states that trialing organisations are expected to develop a detailed safety case before conducting trials which demonstrates that the trial activity can be conducted safely (with safety defined as the absence of unreasonable risk). This document, completed by Academy of Robotics, sets out the safety case for Kar-go's semi autonomous vehicle road trials.



BACKGROUND



BACKGROUND

Over the last four years, we've been working on a way to automate last-mile delivery. As a result, we built Kar-go. Kar-go is an electric autonomous last-mile delivery vehicle able to pick up a package and then take it to any target address. In summer 2019, we unveiled Kar-go at the Goodwood Festival of Speed. Kar-go, is the first of its kind, UK-made, and able to compete with US-owned systems such as Starship, Google, and Tesla's autonomy, but our vehicle works specifically with last-mile delivery in mind while being designed for use on UK roads.

Over the last 12 months, we had data gathering vehicles mapping roads and routes in and around Surrey, London, Italy, Germany and Brussels. We then used this data to train our vehicles to be able to drive on the roads we mapped but in virtual environments representing the mapped areas.

We have reached the stage where we are to perform human-operator supervised trials, in-which we use Kar-go to perform semi-autonomous last-mile delivery. The trial will see medicines delivered from pharmacies to care homes without human contact, simultaneously laying the groundwork for future fully autonomous delivery. This trial service will use one Kar-Go delivery vehicle.

We can split Kar-go's functionality into three key components:

a. A sender such as a pharmacist can insert a package into a tray then into the vehicle. A receiver can see that their delivery is on its way using a specialised app, then be notified when the package has arrived for them to collect outside. A hatch opens at the back of the vehicle and the receiver can pick up their specific delivery. The vehicle can hold several packages and can do this up to a dozen times with no additional human intervention. This allows for what we call, «non-human-contact delivery» This is all possible due to the custom logistics system in vehicles with automated onboard package-swapping.

b. This vehicle is packed with sensors and hardware which allows it to learn a specific route so that it can in the future, drive itself to perform pre-set delivery routes. Simultaneously, the vehicle performs data-gathering and route analysis.

c. The vehicle drives itself from the sender to the receiver.

The trial we are conducting focuses on part a) and part b) only, this means that the vehicle will be manually driven by a skilled operator at all times allowing us to test «non-human-contact delivery». We call this, Semi-Autonomous Delivery.

PHASES

The trial will take place across three phases:

Test 01 **Navigation of route whilst empty, trial runs.**

Test 02 **Autonomous pick up procedure testing, Autonomous Drop off procedure testing**

Test 03 **Live Trial - Test semi-autonomous delivery run.**

TIMESCALES

The pilot will take place in Summer 2020 with a duration of six months.

The primary aims of the project are to test:

- the autonomous vehicle technology on board Kar-go
- the case for autonomous delivery within 30 mins from sender to receiver.

Key Metrics

The measures of success have been categorised as follows:

Technical Operational (Kar-go)	Technical/ Operational
Kms travelled in the following categories: o Day/Night o Weather conditions Number of interventions to manual driving required (by category) Load carrying capacity Range vs Load Adaption to dynamic entry and exit points to locations Charge time	Time saved through autonomous delivery Ease of Loading Availability of charging points Time taken to load Kar-go Maintenance time
Public Acceptance	Environmental Benefits
Volume of press coverage Evaluation of public response, feedback etc i.e. level of acceptance	Emissions saved (local air quality)

TRIAL DOCUMENTATION AND COMMUNICATION

The trial will complete the following reports, logs and briefings in order to communicate during the trial process and present the outputs following the trial process.

Deliverables Report: In order to measure the success of this trial, a detailed report highlighting performance and level of success in meeting the trial deliverables will be conducted after the trial period. This will factor in all of the information contained in the trial

logs and after an assessment of the recorded metrics by the onboard vehicle software.

Daily Driver Logs: As specified, the driver will complete daily logs detailing experience with the vehicle. This will take place in conjecture with a daily briefing following trial activities which will allow for any concerns/ improvements to be voiced. The emergency mode operator will also be present and required to complete a similar log.

Daily Briefings: A briefing will take place each day both before the trial activities and following them. This will include a detailed list of the days tasks at the start and an opportunity to evaluate afterwards.

Engineering Report: In order to ensure that the vehicle is in safe operating capacity throughout the trial, engineers will evaluate the vehicle daily before and after the trial activities to assess any required maintenance actions.

LEGAL REQUIREMENT CHECKLIST

SAFETY DRIVER

Requirement - A driver is present, in or out of the vehicle, who is ready, able, and willing to assume control of the vehicle.
Response - There will be a safety driver inside the vehicle at all times, the safety driver will be able to take control of the vehicle on public roads and will allow autonomous arrival and departure procedure to delivery sites.

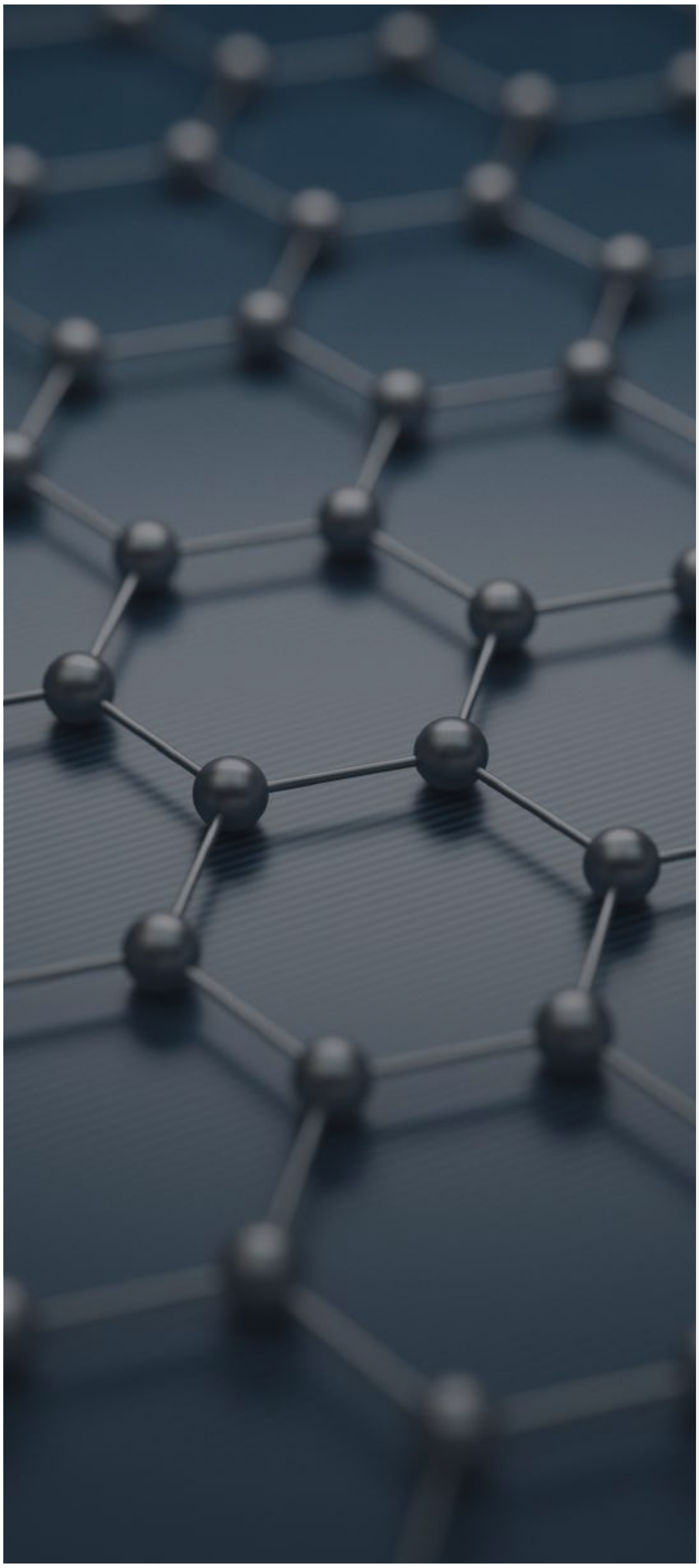
ROADWORTHINESS

Requirement - The vehicle is roadworthy
Response - The vehicle is a road-worthy vehicle which recently received approval via MSVA at the Driver Vehicle Standards Agency, a UK government body in 2020.

INSURANCE

Requirement - Appropriate insurance in place
Response - The vehicle is fully taxed and insured.

SAFE OPERATION AND CONTROL



SAFE OPERATION AND CONTROL

This section is concerned with demonstrating that control of the vehicle can always be maintained during trialling.

This trial will include a safety driver inside the vehicle and will focus on the 'no-contact' aspect of delivery. Utilising the vehicles package delivery system to test autonomous arrival and departure procedures and test being able to provide a delivery service with no contact between driver and recipient. However, as software will be operational relative to autonomous driving, we have considered necessary safety requirements relevant to 'semi-autonomous' delivery.

WHAT DOES THE SAFETY DRIVER DO?

The safety driver's main job is to take control of the vehile if required to do so. Inside the vehicle is a control panel which the safety driver is trained to use. The control panel has a series of buttons and a small screen which allows the safety driver to monitor all aspects of the vehicle as well as press buttons to log the journey, enable or disable onboard recording software/hardware for additional vehicle 'training'. The buttons also allow the vehicle to begin or cease its autonomous arrival/ departure/
delivery procedure.

HOW LONG DOES THE SAFETY DRIVER SIT IN THE VEHICLE?

Our trials are short and frequent, meaning that journeys and time in the vehicle will be less than 1 hour before a break. This mitigates driver fatigue, our test area is also located minutes away from our base station and remote monitoring facility.

VEHICLE'S IN BUILT SAFETY SYSTEMS (ADAS)

Advanced driver-assistance systems (ADAS), are electronic systems that help the vehicle driver while driving. When designed with a safe human-machine interface, they are intended to increase car safety and more generally road safety. Our vehicles are equipped with a range of sensors including camera, radar and lasers, to collect data about the environment in which it is operating. They then use sophisticated software to localise themselves within the environment and watch for hazards. While a safety driver is operating the vehicle, our ADAS software is also in operation. This allows the vehicle to perform emergency maneuvers such as automatically applying the brakes if it detects a collision hazard, notifying the driver of red lights, lane changes, pedestrian crossing etc. All this data is recorded and stored on the vehicle.

REMOTE CONTROL CENTRE

The company has built a command hub, which acts as an operational centre for additional team members to work from. While the vehicle is in operation, team members at the command hub receive real-time data from the vehicle including and not limited to video data streams, vehicle status, and data logs. This allows all test data to be stored not only in the vehicle but in real-time at the control centre a few miles away. The control centre is also able to remotely take full control of the vehicle should there ever be a need to do so.

Please see the supplement document titled 'The Command Hub' for more information on our control centre, how it works and how we use it to maximise safety.

PRE-TRIAL SAFETY & WORKFLOW

PRE-TRIAL SAFETY & WORKFLOW

SOFTWARE

While the vehicle is in operation and being driven, our on-board software will be running on the vehicle. The software is an ecosystem of modules, simulators and utility tools related to mostly vision based perception and control of autonomous vehicles. This software is what we use to monitor all aspects of the vehicle, the drive and most importantly, log data which we will then use to perform fully autonomous trials in the future.

Our testing workflow has followed a series of steps before we got to the current live testing stage in the target environments representative of typical U.K residential/high-street roads. To get to this stage the following outcomes were achieved.

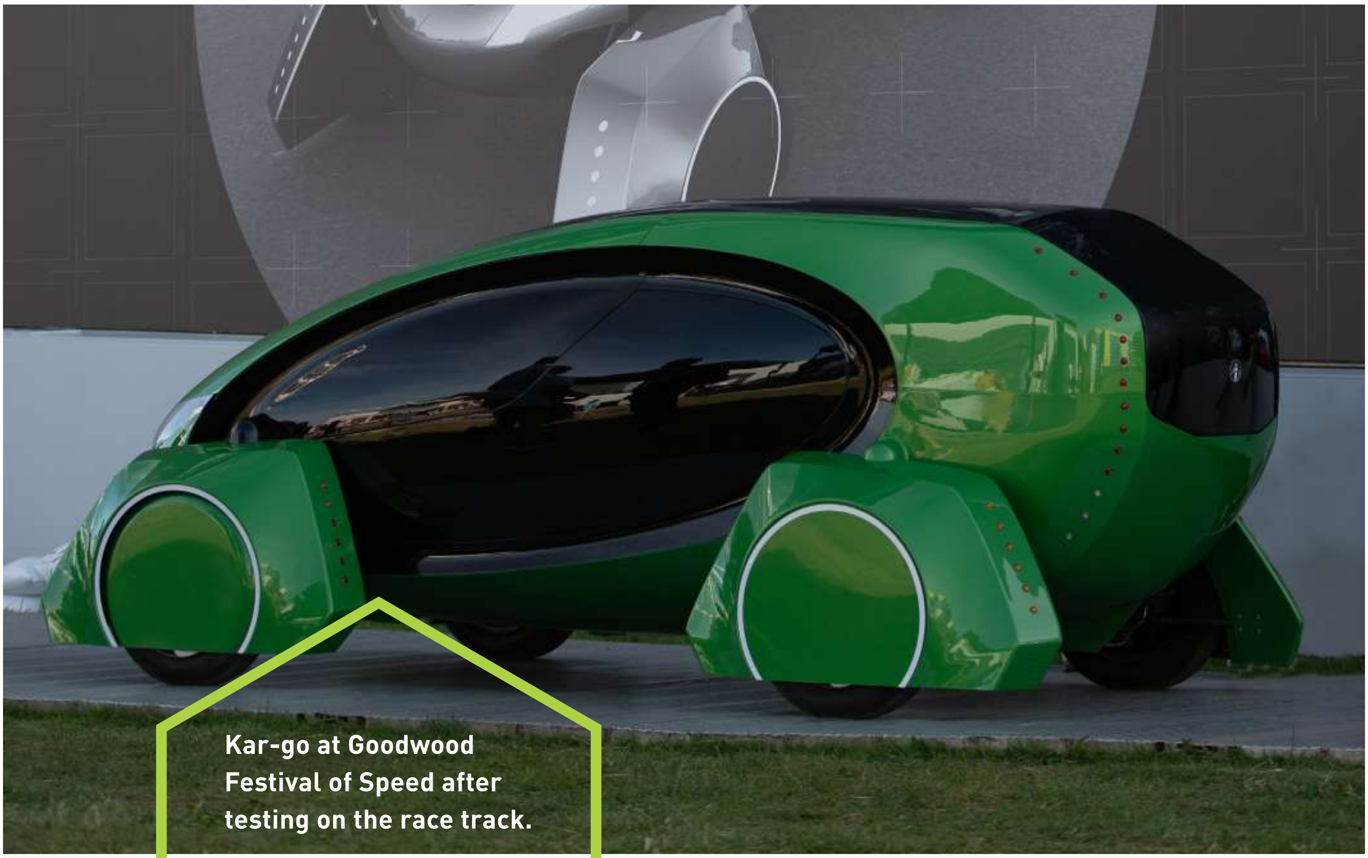
- Data gathering and network fine-tuning.
- Off-line validation, testing and simulation.
- Live testing with 100 % manual control. (Private Roads)
- Perception-control loop calibration.
- Autonomous testing in structured test road segments limited in length and duration.
- Autonomous testing in un-structured real-world segments limited in length and duration.
- Autonomous testing for transitions in real-world environments (these tests would entail, the vehicle choosing the correct intersection, behaviour at red lights).
- Autonomous testing for special behavioural routines (reversing, parking to space) and emergency mode response.
- Autonomous testing combining scenarios e, f and g. Here the vehicle is required to traverse a straight road segment, make a decision and transition into another segment (make a turn at intersection onto another road) and finally perform a special behavioural routine (park/halt at designated location.)

The current system is designed and capable of operating in these conditions. The vehicle has multiple layers of safety built in. At the base layer is the control circuit that interfaces the on-board computer with the vehicle. This has built in failsafes which include:

Halting the vehicle if the computer-controller connection broken, halt vehicle if interrupt signal from computer/remote received, speed limiting, activation of emergency lights

The entire electro-mechanical system will be thoroughly configured by our engineer(s) and technicians experienced in safety critical performance. On top of this we have the field of distance sensors as part of our emergency mode system which overrides any perception freespace estimatons. Moreover the perception-action pipeline can be interrupted resulting in a vehicle halt, by a remote signal from an external observer or action by the safety driver.

The final layer of safety comes from the perception software design itself. The use of multiple networks for critical functionalities and hierarchical representation of data greatly eliminates inaccuracies that may mandate such interventions.



Kar-go at Goodwood Festival of Speed after testing on the race track.

The particular route we have chosen for the trial is a route which we have had a team testing in simulations and calibrating on for over a year, this same team will be based in our control centre giving a high level of familiarity and deep understanding of the route, area and nuances.

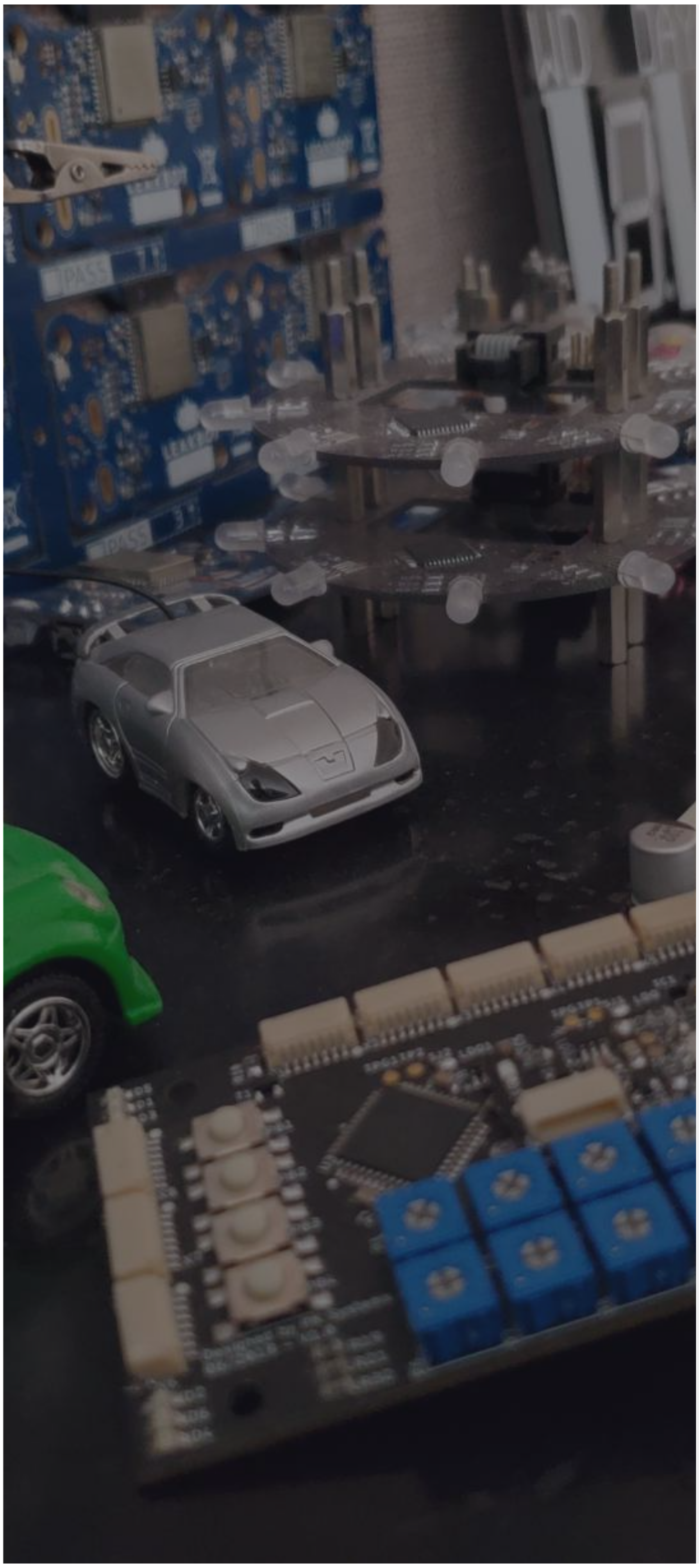
ROUTE

The activity of this trial will be conducting deliveries from pharmacies to care homes. This will take place along the following routes in Hounslow and Surrey in the UK;

Assurance of system safety

We work within the guidelines of ISO26262, ISO/PAS 21448 – Safety of the Intended Function, BSI PAS 1880 – Guidelines for developing and assessing control systems for automated vehicles. Our vehicles having passed an individual vehicle assessment has meant that the vehicle itself and driving has been deemed roadworthy by the relevant government body. Our experimental modules are being used for logging and not part of vehicle control.

DATA ACCESS AND RECORDING PLANS



DATA ACCESS AND RECORDING PLANS

In order to sustain safe practices and further improve on them, it is important to tailor data recording planning towards influencing future improvements. Data recording takes place in the following instances; ➔

- **Vehicle Data Recording:** Kar-Go, whilst operational (whether autonomous or not) constantly captures data in real time through its on-board cameras. This information provides a live feed that will ultimately be used to further develop the strengths of the autonomous software as well as improving upon any weaknesses potentially discovered. Information captured and recorded during the trial process will be made available to any interested parties, including overseeing authorities such as the Department of Transport where necessary, to help influence future guidelines and regulations set in place for the operation of autonomous vehicles. Video recorded footage will also be able to provide insight to developers on increasing Kar-Go's ability to adapt to changing requirements on roads during live autonomous driving. On board monitoring systems will also record key metrics where available, including distance travelled (Km.) Time to complete the route from specified points (For example, one delivery from depot A to site B) and the number of times manual intervention is required from a safety driver (If applicable.)

- **Supervised Metrics Recording:** In trial scenarios, particular key metrics will be recorded by supervising project coordinators and trial participants. These include charge time, number of interventions by manual safety driver and time to complete deliveries. Having a human presence to record particular data as well as the Kar-Go vehicle itself helps to ensure the best accuracy of data recording.

- **Trial Report Recording:** At each phase of the trials and operation testing, information collected is collated into reports that detail both results and information relevant to further trials and interested parties. This will include all previously summarised metrics as well as overviews of general performance, cost evaluations and assessments of value and further scope. This information will be made available with the intention of shaping future frameworks in the field of autonomous vehicle testing.

SUMMARY OF SPECIFIC VEHICLE METRICS RECORDED:

- Details of the automated system i.e. software version, hardware specifications;
- Whether the vehicle is operating in manual or automated mode;
- Longitudinal acceleration in the vehicle's direction of travel;
- Lateral acceleration when the vehicle moves sideways;
- Vertical acceleration when the vehicle mounts a kerb, central island, speed hump or other object which causes the vehicle to rise;
- Vehicle speed;

- Steering command and activation;
- Braking command and activation;
- Operation of the vehicle's lights and indicators;
- (If applicable) Operation of the vehicle's ignition;
- Geo-location;
- Connectivity, network access, and latency;
- Use of the vehicle's audible warning system (for example a horn);
- Sensor data concerning the presence of other road users or objects in the vehicle's vicinity;
- Remote commands which influence the vehicle's movement (if applicable); and
- Any intervention made by the safety driver or safety operator, including the time of such intervention

ACCESS PLAN FOR POLICE INVESTIGATORS AND EMERGENCY SERVICES

Understanding the need for emergency services and law enforcement to have detailed access to recorded data and the trial site itself, Academy of Robotics has devised the following access plan.

MAKE VIDEO FOOTAGE AVAILABLE AT REQUEST

Camera footage will be available from multiple sources during the many phases of vehicle operation and testing. Some of the ways that video data is captured includes;

- Cameras on-board the Kar-Go vehicle, able to capture everything in a 360 radius around itself in real-time.
- Video footage captured by on-site PR.
- Footage captured by trial participants in an evaluation capacity.
- Data captured by the Command Hub overseer.
- As such, Academy of Robotics agrees and understands the need to provide any and all required video footage to either police investigators and/or emergency services on request in a prompt and detailed fashion.

PRESERVE FORENSIC INTEGRITY OF DATA

All participants responsible for capturing video data footage will be briefed and provided with an 'Emergency Data Access Plan' in the instance of an incident in order to preserve the forensic integrity of data. This will also apply to non-video data and relevant workers responsible for its collection. A core component of this plan is to make the information available at request. Furthermore, to additionally commit to the promise of preserving the integrity of the data, in trial scenarios, an intermediary between the trial and emergency services can be provided with a secondary data feed to allow them also to view certain video footage (Kar-Go on-board cameras) in real time. A summary of the Emergency Data Access Plan includes;

1. **Collate:** Data is pooled together relative to relevance.
2. **Verify:** Data is verified as relevant and informative to requesting party.
3. **Privacy Check** - Ensure data required is relevant only to the pertaining incident and not unnecessarily out of scope in-order to protect the privacy of other parties. There may be a delay in providing information which legal council deems to breach third party or citizen privacy.
4. **Provide:** Data is provided to requesting parties, whether through physical hard drive transfer or digital transference.
5. **Assist:** Academy of Robotics will assist with providing additional data if required and answer general queries and further questions with the utmost transparency.

SECURITY

Academy of Robotics will complete a security assessment throughout the lifecycle of the trial and testing phases. Similar to an evolving risk register, this security analysis will cover the following three components;

- Cyber
- Physical
- Personnel

The security assessment has been developed with the - ISA/IEC 62443 (all parts), PAS 1885, and PAS 11281 - legislation as a guidance tool, which sets the standards that have been considered, when conducting the assessment.

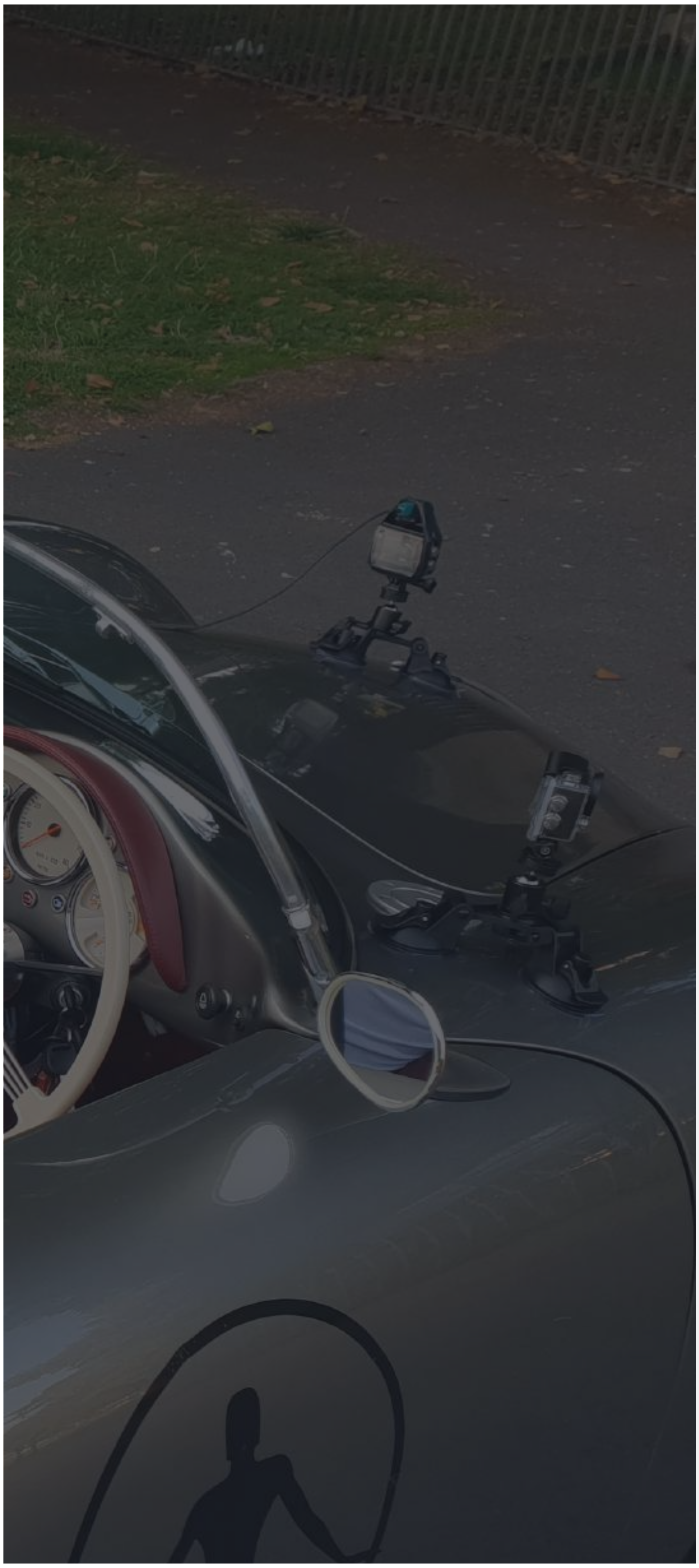
DATA PROTECTION

All captured data is anonymised, number plates blurred, facial features obscured, all stored data is encrypted. We follow GDPR guidelines for data gathering and retention.

Reference Stack:

- UK Vehicle Regulations and in-service requirements;
- 'The Road Vehicles (Construction and Use) Regulations 1986'
- DfT: The Pathway to Driverless Cars: A detailed review of regulations for automated vehicle technologies
- DfT Code of Practice: Automated Vehicle Trialling;
- The Highway Code and Road Traffic Law;
- General Data Protection Regulation (GDPR); and
- Relevant Cybersecurity Standards

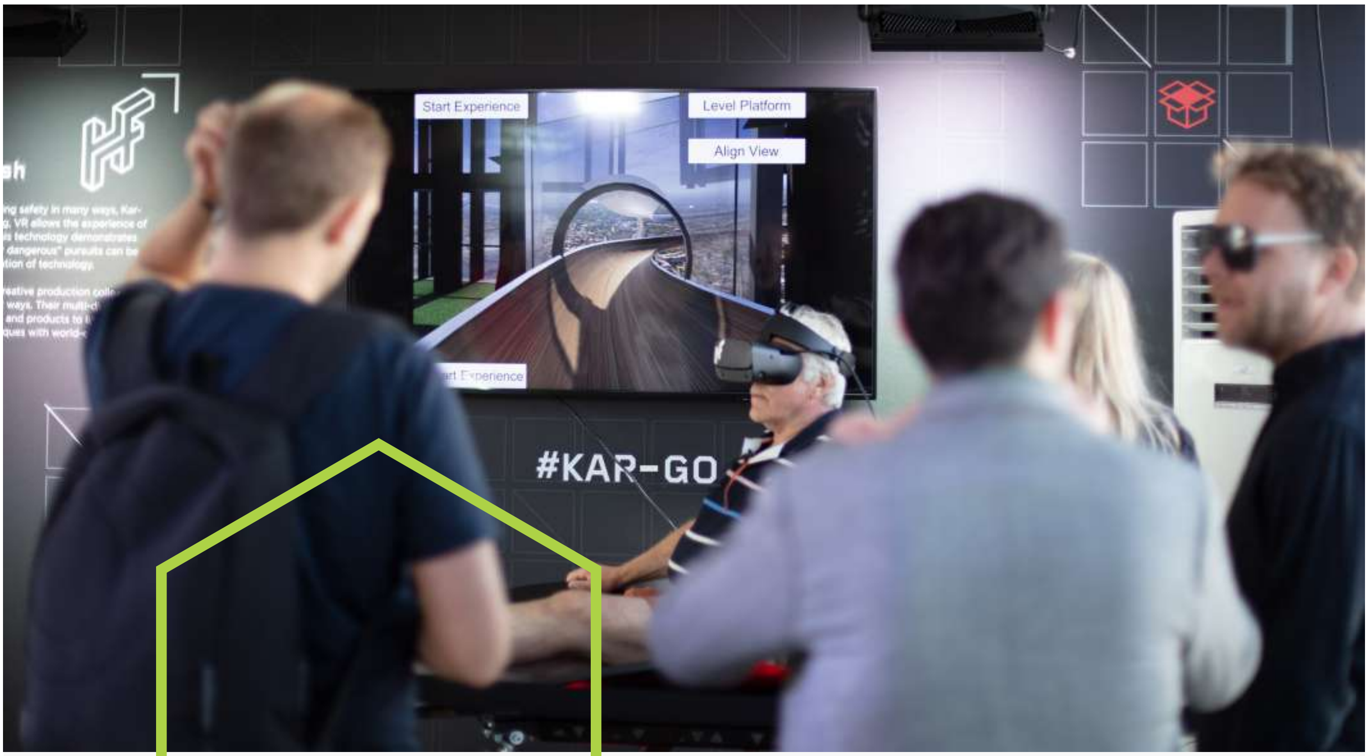
RISK ASSESSMENT AND ANALYSIS



RISK ASSESSMENT AND ANALYSIS

RISK ASSESSMENTS

On 01 of July 2020, we conducted four separate risk assessments. These assessments were conducted internally and the appropriate policies and procedures have been addressed and accounted for by all members of the Academy of Robotics team to ensure that we adhere to a high level of safety practice in our own capacity as well as looking towards public road live trials. These specific risk assessments are as follows; ➔



- **Kar-go Vehicle Operations:** This concerns all elements of risk associated with the active use of our Kar-Go vehicle. This pertains to both practice driving behind closed doors in test environments as well as in controlled spaces specified in more detail within relevant project plans relating to the location in which each trial takes place.

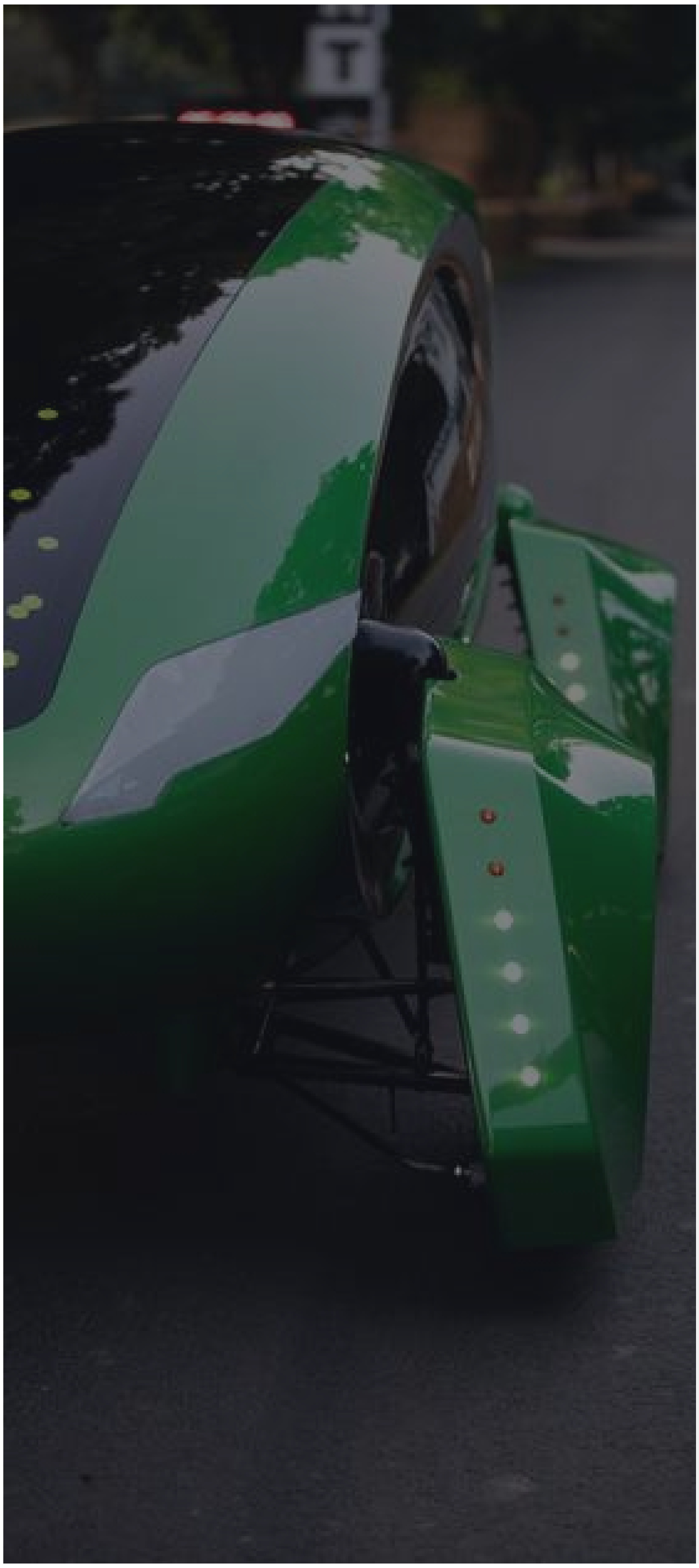
- **Software Risks:** These have been identified as stemming either directly the on-board perception-control software or indirectly through data handling processes and experiments. These may include error-prone performance, failure of trials and loss of data.

- **Electronics and Hardware Risks:** Risks that may arise due to faulty assembly, repairs and configuration of on-vehicle electronics and automotive hardware.

- **Personnel:** This is a general risk assessment that shows an understanding as well as actions taken to limit the general risk to staff and assisting personnel in multiple scenarios. This can range from general office duties such as administration and software development, to engineering a test scenario involving the use of equipment and vehicles that require the appropriate certifications.

Please see appendix 1 which has a safety chart.

THE VEHICLE



THE VEHICLE

MAKE: Kar-go
MODEL: Delivery Bot

PAYLOAD CAPACITY

Space within the Kar-Go vehicle is for up to 48 packages and additional space for a skilled operator working as the safety driver.

Our Autonomous Data Gathering Vehicle 2020

The Kar-Go Delivery Bot is a fully electric vehicle developed for the intent of completing autonomous deliveries and is compliant with UK MSVA requirements. On-board the vehicle are a number of hardware technologies, which include high fidelity 4k resolution cameras to capture video data in a 360 circle which can be stored both internally in the onboard computer and streamed directly to a remote operator. There are distance sensors and proximity sensors that when not operating autonomously can function alongside the cameras (which will run autonomous detection software regardless of manual driving,) to act as a sophisticated A.I ADAS system.

WHAT DO OUR CAMERAS SEE?

Camera data is processed through on-board perception-control software modules that provides perception and detection outputs in real-time whilst the cameras are operating. In autonomous driving, this information is used to distinguish objects around the vehicle, represented visually within colour coded boundary boxes, to perceive freespace areas on the road that the vehicle can navigate within and to detect. This software further allows the camera to perceive lane boundaries on roads. In 'semi-autonomous' driving, our camera systems function as an inbuilt ADAS system that provides data to the operator and the driver. These camera

We get Telemetry, Depth, Optical Flow, all from cameras

systems also record road video footage to be used in the further training of the perception and navigation software. Camera recording methodology is compliant with privacy laws. Different modules are also inter-linked to each other and arranged within an overall hierarchical structure. This can be seen in the diagram below, where image flow is visualized after being processed by the initial low level modules. The integrated freespace is used along with distance sensor data to calculate navigational commands. If in semi-autonomous mode these commands get logged as data.

WHAT DO OUR DISTANCE SENSORS DO?

Distance sensors are hardware components that act as a final level of safety when operating in autonomous and semi-autonomous mode. Despite what the visual perception software predicts, if an object is detected within the designated buffer zone by the distance sensors, the vehicle prioritizes this reading over camera perception and takes appropriate actions. Even if the camera image gets corrupted or an error occurs in the visual processing stack, the distance sensors provide a layer of redundancy against such a scenario.

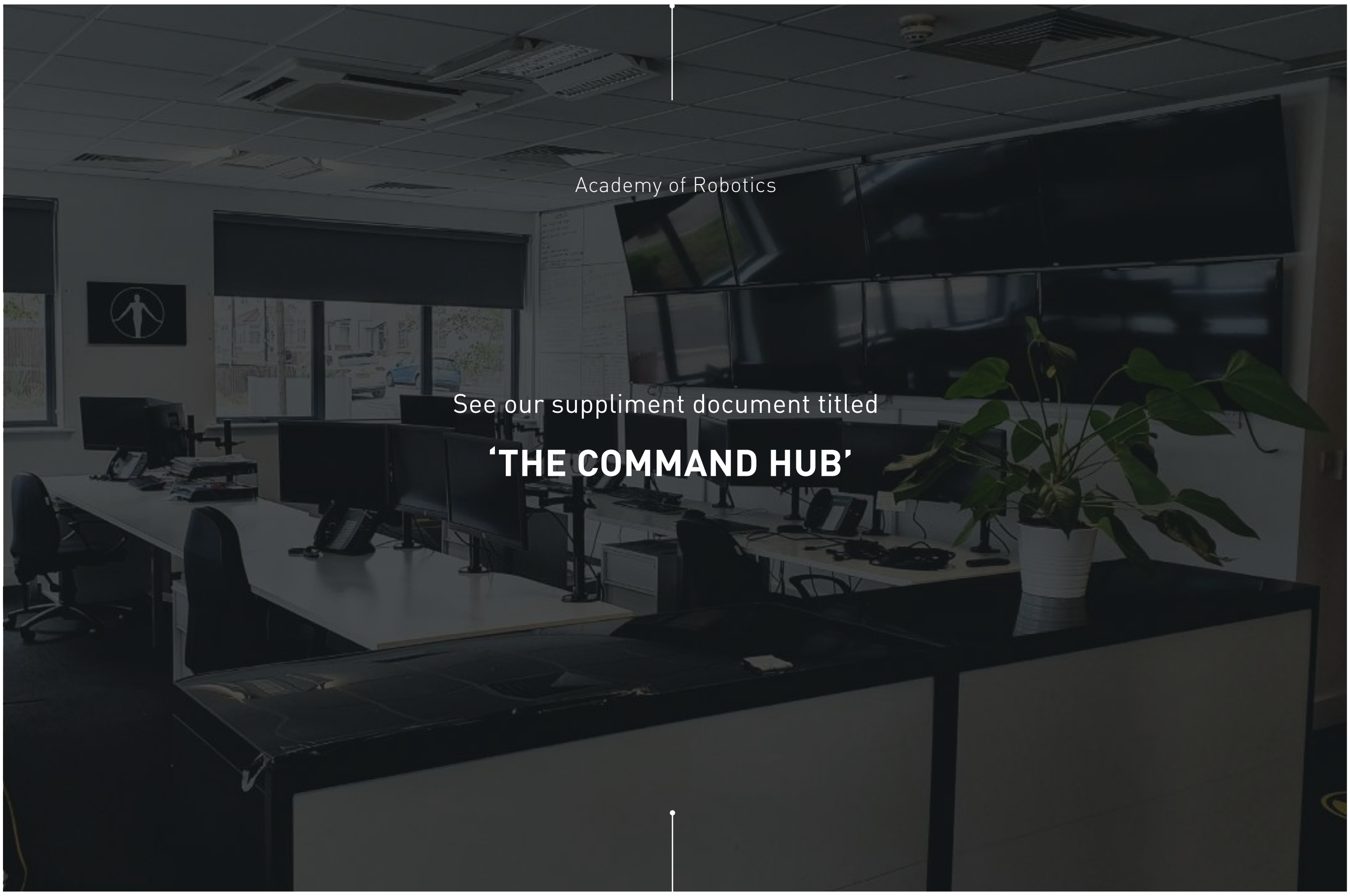
These sensors can also provide proximity information to a safety driver.

WHAT IS EMERGENCY MODE?

Emergency mode is an inbuilt feature that is triggered in the instance that any of the onboard software detects an exception to the parameters established for the safe operation of the vehicle. This process notifies the operator that it has entered emergency mode, then either;

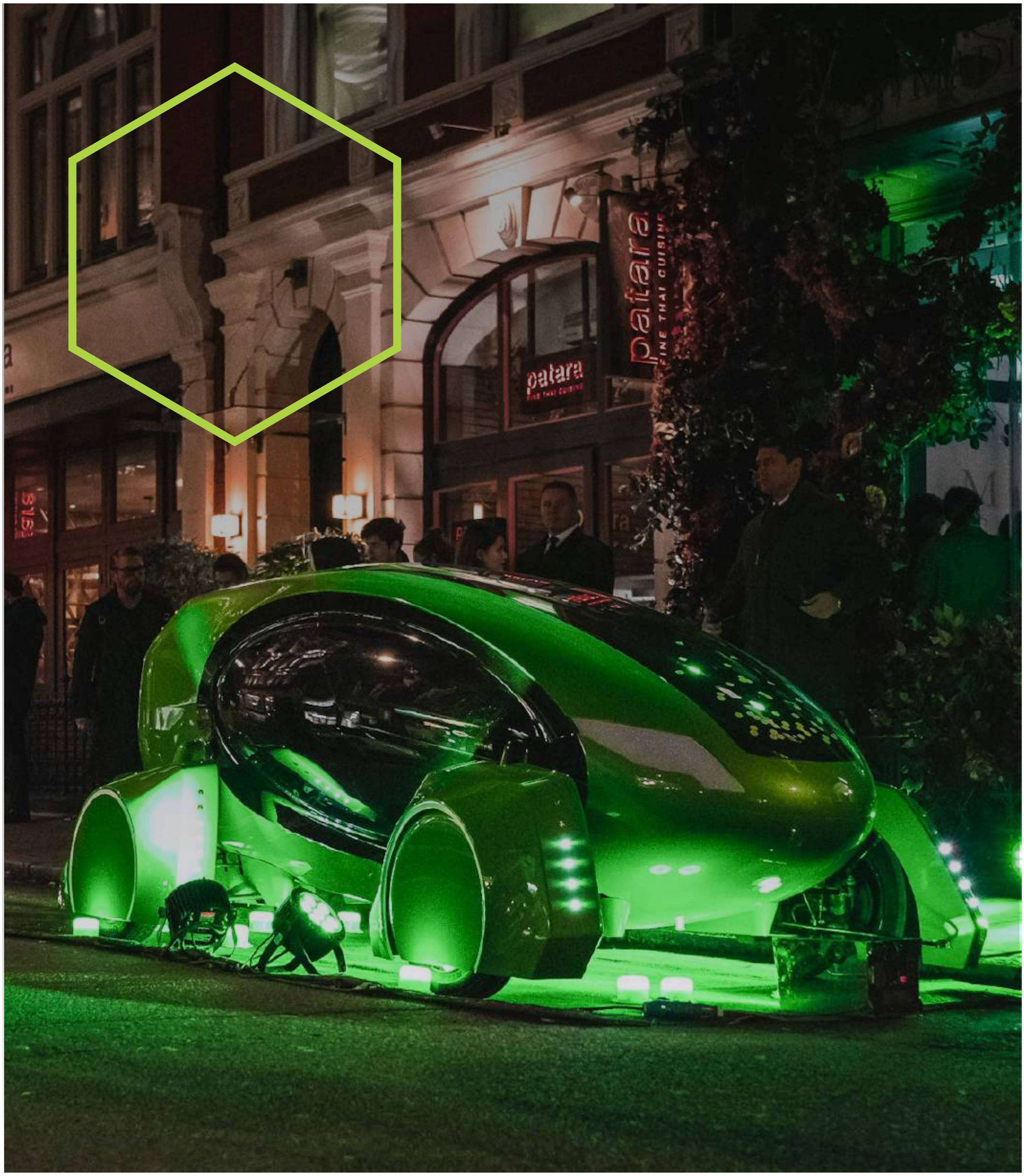
A. Provides manual control to the safety driver
B. Safely parks the vehicle
C. Allows remote control of the vehicle

Whilst 'semi-autonomous' driving, the triggering of emergency mode, which is the result of any of the vision-control system or sensor modules making a detection that requires emergency mode, or failing to make a detection in the instance of a fault. Will provide full control to the safety driver and disable autonomous driving features. In the case of full autonomy, emergency mode is able to pass remote control of the vehicle to a trained operator stationed at our command hub.



See our suppliment document titled

'THE COMMAND HUB'


patara
FINE THAI CUISINE
patara
FINE THAI CUISINE

HOW WAS THE VEHICLE TESTED?

The Kar-go Delivery Bot, has undergone a number of tests which include the presence of a safety driver in the vehicle at all times. Primarily, the testing has been conducted at the facility of Pilgrim Motorsports in Brighton, UK, both on a private track and stilts. Furthermore, vehicle testing has also been conducted on site at Goodwood during the Goodwood Festival of Speed 2019 as well as for several testing activities on privately owned roads in the region of Surrey, UK.

WHAT HARDWARE/SOFTWARE FAILSAFES ARE IN PLACE?

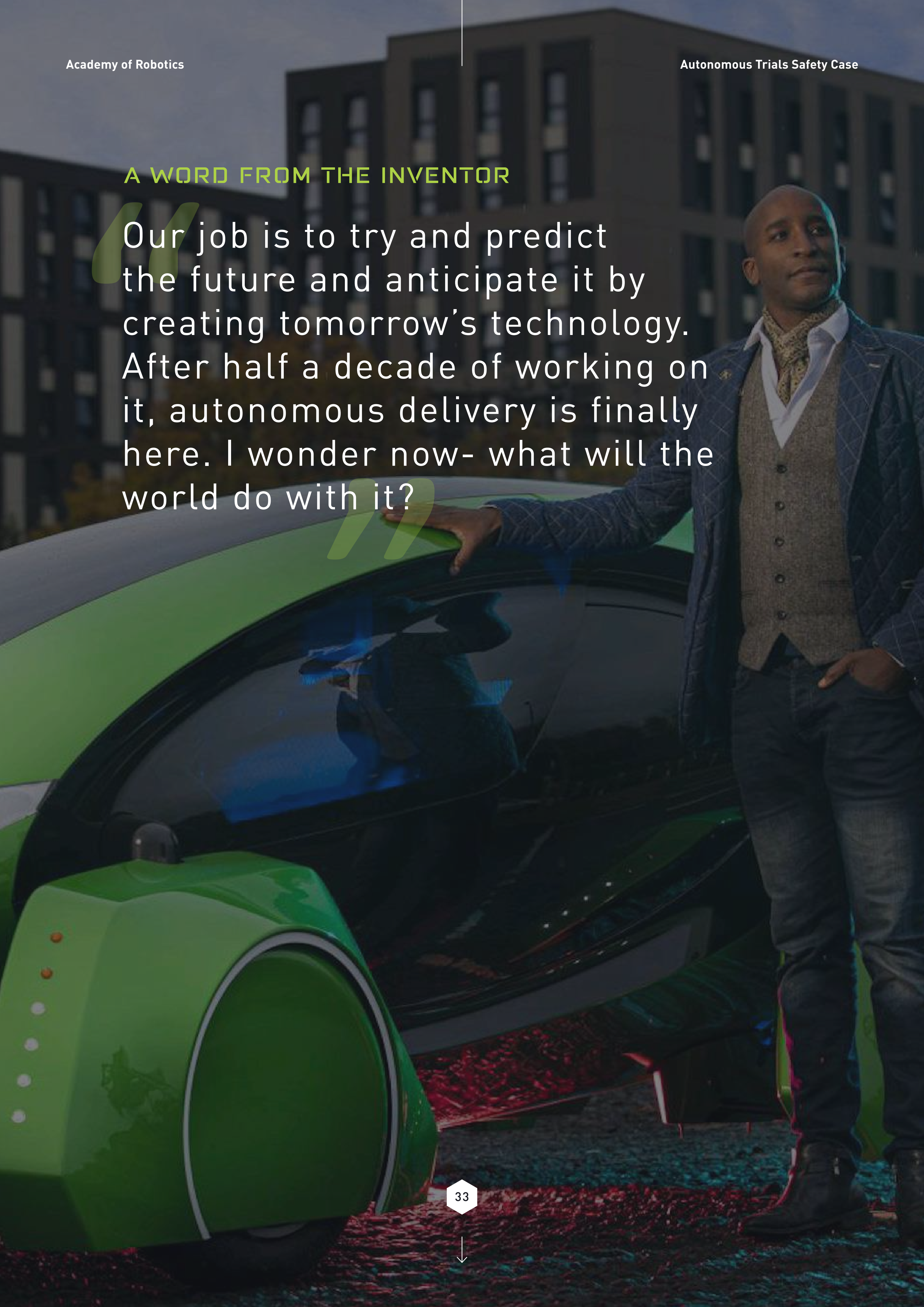
There are a number of failsafe mechanisms built in at different points of the system. This includes measures implemented from a software and mechatronics point of view. The perception software pipeline is implemented on the main computing server. The navigational values calculated are then sent to an interface controller circuit which sends motor & actuator commands to move the vehicle (if operating in autonomous mode.)

PERCEPTION SOFTWARE (ON-BOARD COMPUTER)

1. **Use of multiple modules with overlapping functionalities:** This ensures any detections or false predictions by a single module does not contribute to overall performance errors as other modules can counteract this with true predictions.
2. **Hierarchical software structure:** Modules are structured such that the detection of the first 'set' or 'level' is passed on for further processing by higher level modules. These higher level modules are trained to account for noise in the intermediate predictions from the lower level modules. Even if lower level modules (such as object detection, segmentation and lane detection) are subject to false detections, when processed by higher level modules (pilotnet, navigational-freespace) the capability exists to output the desired perceptual outputs despite this.
3. **Distance sensors:** These supplement the freespace calculations from the vision module. If an object is detected by the distance sensors but not accounted for by vision modules, the priority is given to the distance sensors.
4. **Command Center Signal:** If a signal is received by an operator outside the vehicle (in a command-control center) it is treated as a hard interrupt and the vehicle brought to a halt immediately with system shutdown.

VEHICLE CONTROLLER (CONTROL CIRCUIT)

1. **Autonomous to Manual Transition:** The control circuit has clearly defined rigid protocols for transfer of control from autonomous mode to manual driving.
2. **Data Sanity Check:** To ensure that any corrupted or false navigational values incoming from the main on-board server



A WORD FROM THE INVENTOR

“Our job is to try and predict the future and anticipate it by creating tomorrow’s technology. After half a decade of working on it, autonomous delivery is finally here. I wonder now- what will the world do with it?”

are not actioned.

3. **Angular velocity and acceleration limiting**: Vehicles cannot exceed these limits and this is implemented at the final layer, just before signals are sent to the motor/ actuator.
4. **State Machine:** A state machine is implemented at the control circuit level. This prevents operator errors while transitioning between different modes and also acts as a safety check during vehicle testing.
5. **PID Loop:** A final level of trajectory control is implemented to ensure the vehicle moves in-line with the navigational commands.

Connection Interrupt

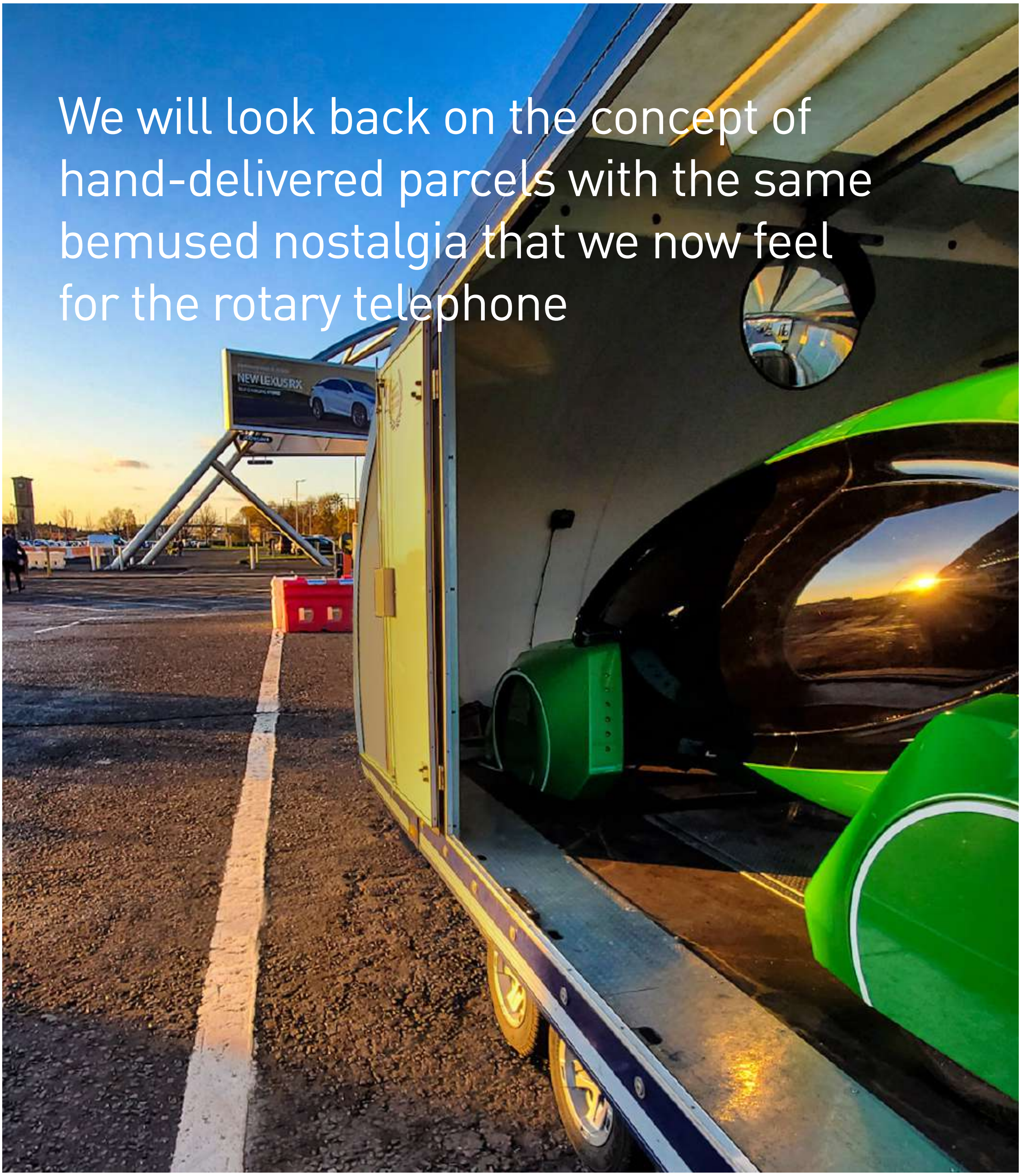
If any corruption in data fidelity or drop of connection between the main server and control circuit is sensed the vehicle is brought to an immediate halt and control handed over to the safety driver.

UNDERSTANDING MSVA

MSVA (Motorcycle Single Vehicle Approval) is a method of certification that applies to the Kargo Delivery Bot as a 4 wheeled light vehicle, or heavy quadricycle. The MSVA is a pre-registration inspection for vehicles that have not been type-approved to European standards. The main purpose of the MSVA is to ensure that the vehicle has been designed and constructed to modern safety and environmental standards before it can be used on a public road.

The Kargo Delivery Bot has been thoroughly tested for the following items;

- Mirrors (Bodied Vehicles)
- Mirror Field of View
- Speedometers
- Audible Warning
- Lighting
- Lighting Requirements
- Acceptable multi-lamp options for 3&4 wheeled vehicles not requiring two obligatory headlamps
- Unauthorized Use Preventions
- External Projections (Bodied Vehicles)
- Floor Line
- Rear Registration Plate Space
- Headlamp Aim (Bodied Vehicles)
- Design and Construction
- Tyres
- Tyre Load Indices
- Speed Categories
- Brakes
- Radio Suppression
- Exhaust System/Noise
- Exhaust Emissions - Spark Ignition
- Brake Performance
- Goods Vehicle Identification Plate
- Engine Power Restriction Information Plate
- Defrost/Demist
- Seat Belts and Anchorages
- Glazing
- Windscreen Wipers and Washers



We will look back on the concept of hand-delivered parcels with the same bemused nostalgia that we now feel for the rotary telephone

- Masses and Dimensions

Following the MSVA inspection, the Kargo vehicle is assigned an identification and registration number.

PROPOSED OPERATING LIMITS

Time	Work	Rest
3 hours 15 minutes	3 hours of work time	15 continuous minutes of rest time
12 hours	11 hours work time	60 minutes rest time in blocks of 15 continuous minutes
24 hours	11 hours work time	12 hours continuous stationary rest time

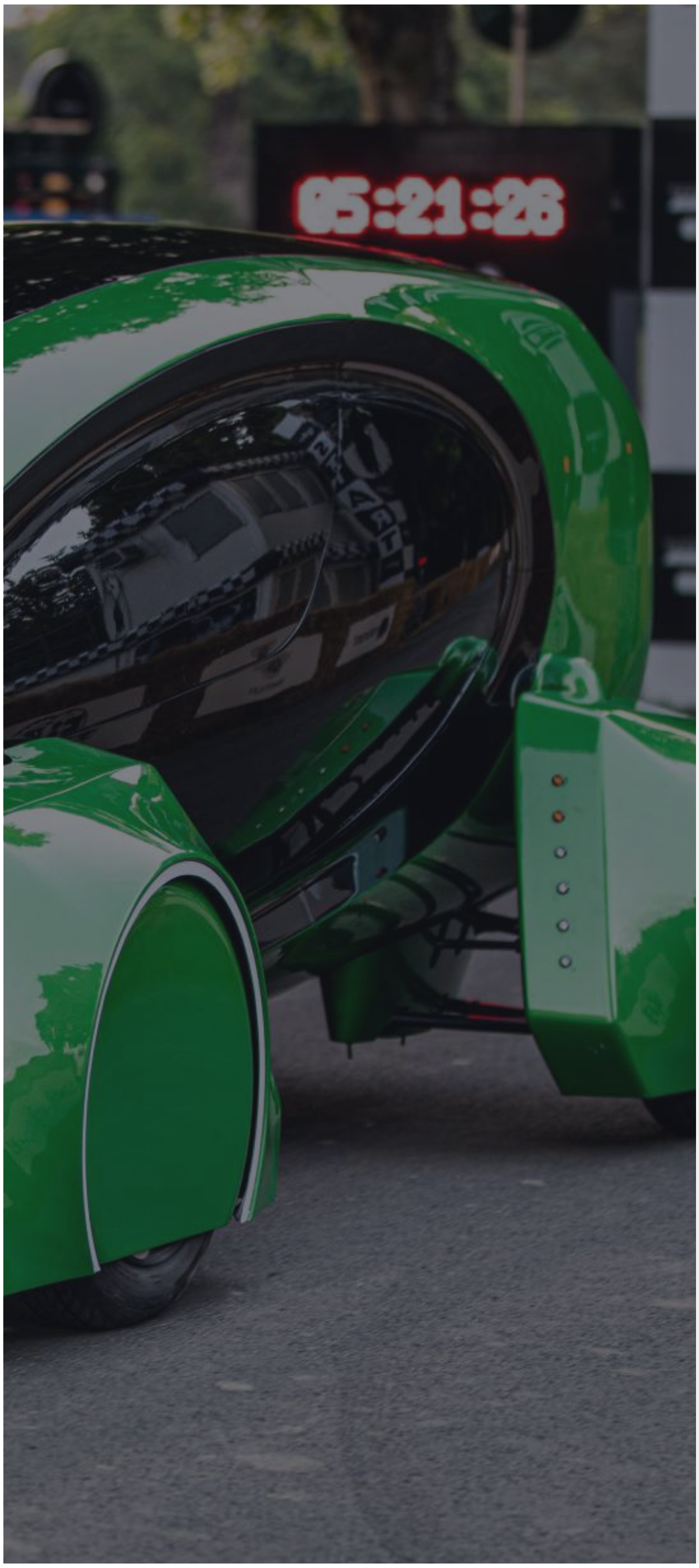
Safety Driver
This is a preliminary detailing of safe operational hours for the driver. Actual work/driving times will be determined closer to the trial period and considerations of idea delivery times/local traffic flow will be taken into account.

In accordance with the Automated and Electric Vehicles Act of 2018 the project plan will include details of the charging points available for the vehicle on the trial, the required power consumption and the expected charging time.

Reporting Structure
Risk Assessments will be conducted prior to the beginning of the trial and as part of the safety case in order to highlight the perceived risks of the trial activity. The following tablature highlights

Report Type	Daily	Weekly	Post-Trial	Pre-Trial
Driver Log	X	X	X	
Operator Log	X	X	X	
Hardware Report		X	X	
Deliverable Report			X	
Performance Report		X	X	
Risk Assessment				X
Trial Coordinator Report		X	X	
Engineering Report	X	X		
Project Plan				X

CHANGE CONTROL



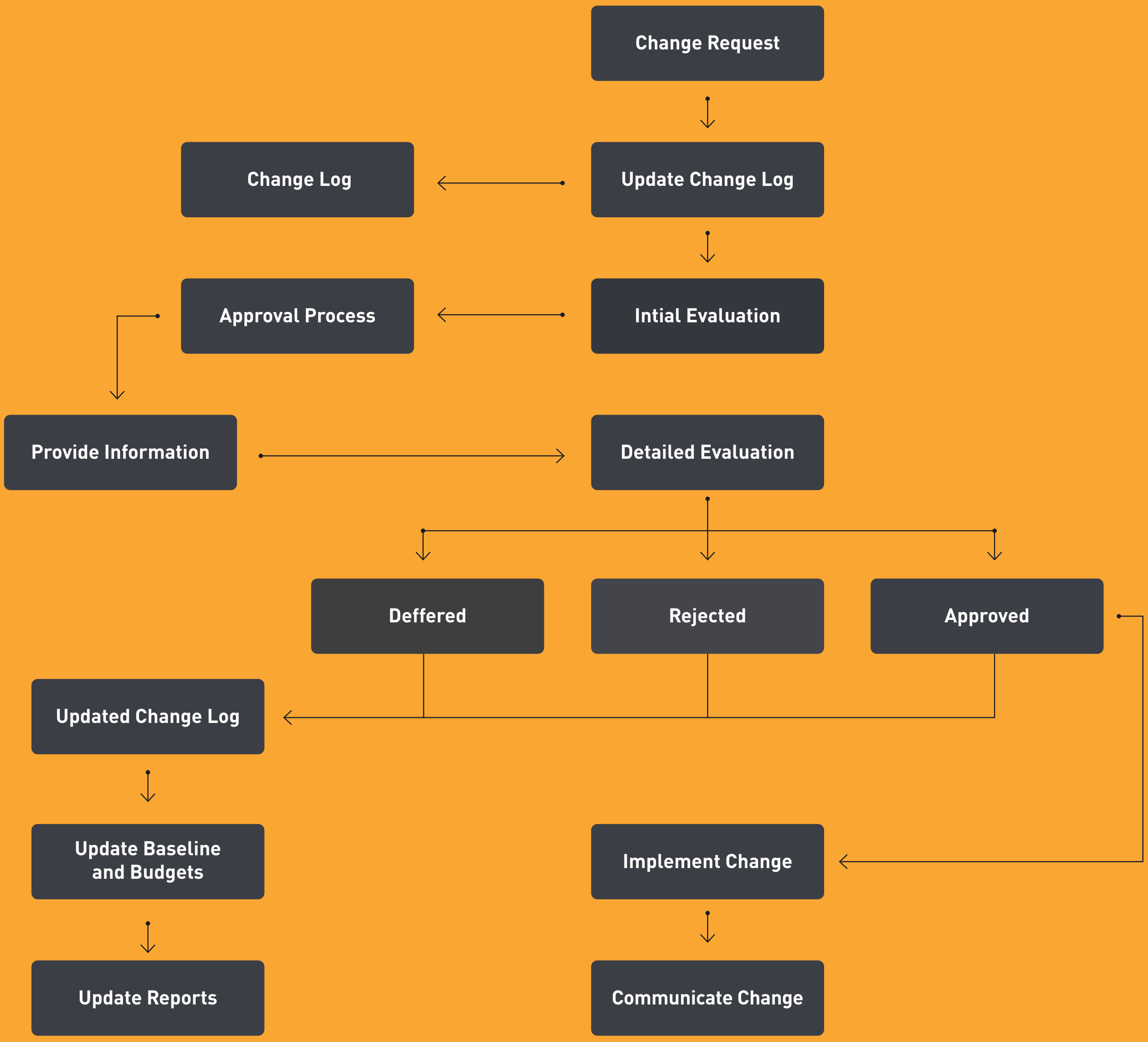
CHANGE CONTROL

WHAT IS CHANGE CONTROL?

This section provides an overview of the change control process utilised for the trial. Change control is a process that defines what events trigger a review of the safety case (and those that do not.) This further includes a process for documenting and communicating changes. Changes may include hardware or software changes as well as operational changes such as increasing the number of vehicles, a new route or different test scenarios. ➔

CHANGE PROCESS FLOW

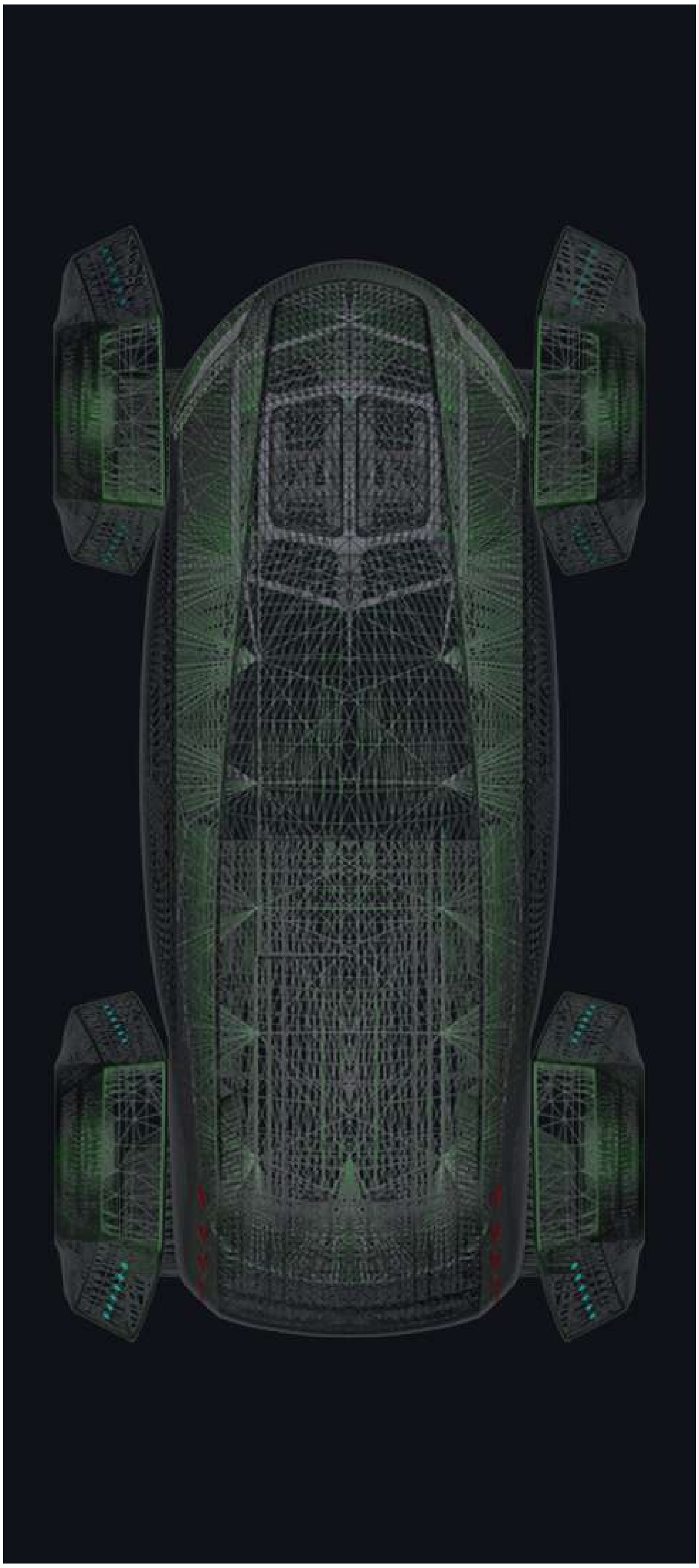
Potential changes that have been considered are logged in a change template. All changes are recorded in a project change log and all key members of the project team consult proposed changes as part of the initial evaluation and detailed evaluation stages. The process flow diagram illustrates the process flow that takes place after a change is suggested.



Area of Project	Change	Impact
Resource	Several changes in resources may occur that require change. These range from Software/Hardware replacements/upgrades as a result of trial report feedback or unforeseen malfunctions and maintenance requirements. Furthermore, additional relevant resources such as staff may require changes in the case of illnesses/ unforeseen circumstances.	Software/Hardware resource changes are likely to result in impacts on the overall project budget. Some of which may be catered for but others may lead to additional budgetary needs and potential rescheduling of trial activity days and pre-trial deadlines to accommodate replacement/upgrading of software/hardware. In order to combat the need to upgrade, all software/hardware will be evaluated and the necessary changes made prior to the start of trial activities.
Budget	Changes to the budget may be required following advice of project team members and reporting on trial needs. In some cases, the budget may be foreseen to exceed its allocations and alternatives will need to be considered and implemented to fit into the financial parameters of the trial.	Budget issues may cause significant delay and as such must be carefully considered as a risk when operating with experimental, high-end technology and hardware. As such, specialists in their respective fields will observe and monitor all equipment to ensure its operating capacity and condition.
Quality	During trial activities, the quality of results or a process may be highlighted as change-worthy. Similar changes may also be suggested from outputs of pre-trial work packages.	Evaluation within the change process-flow is fundamental in the instance of suggested quality changes. If a process or result can be significantly improved then changes can be made provided they do not interfere with budgetary or timeframe parameters.

Area of Project	Change	Impact
Timeframe	Several factors may lead to required changes with the timeframe. Especially relative to the driving segment of the project. These factors include; • Extreme weather • Road works/collisions • High Traffic Flow Furthermore, delays in established project work packages may see requirements for deadlines to be extended to ensure that all work packages are complete.	Impacts on the timeframe relative to driving activities may result in delays and rescheduling which can be managed between the cooperating parties. Delays in work package completion can be evaluated and if additional resources cannot be provided to meet the deadline, extensions can be discussed.
Operational	Operational changes include scenarios such as route changing or the introduction of new test scenarios.	Route changes can be accounted for in the surveying stages, where route data is taken of the proposed route and the surrounding area as to pre-train both vehicle and safety driver to the surrounding area in the instance of a required route change, as to prevent delays and a reschedulement. New test scenarios would not be a factor unless discussed prior to the beginning of driving activities, in which case these scenarios would be evaluated for their potential deliverables and ability to be completed within the allotted time frame for the operational aspect of the trial.

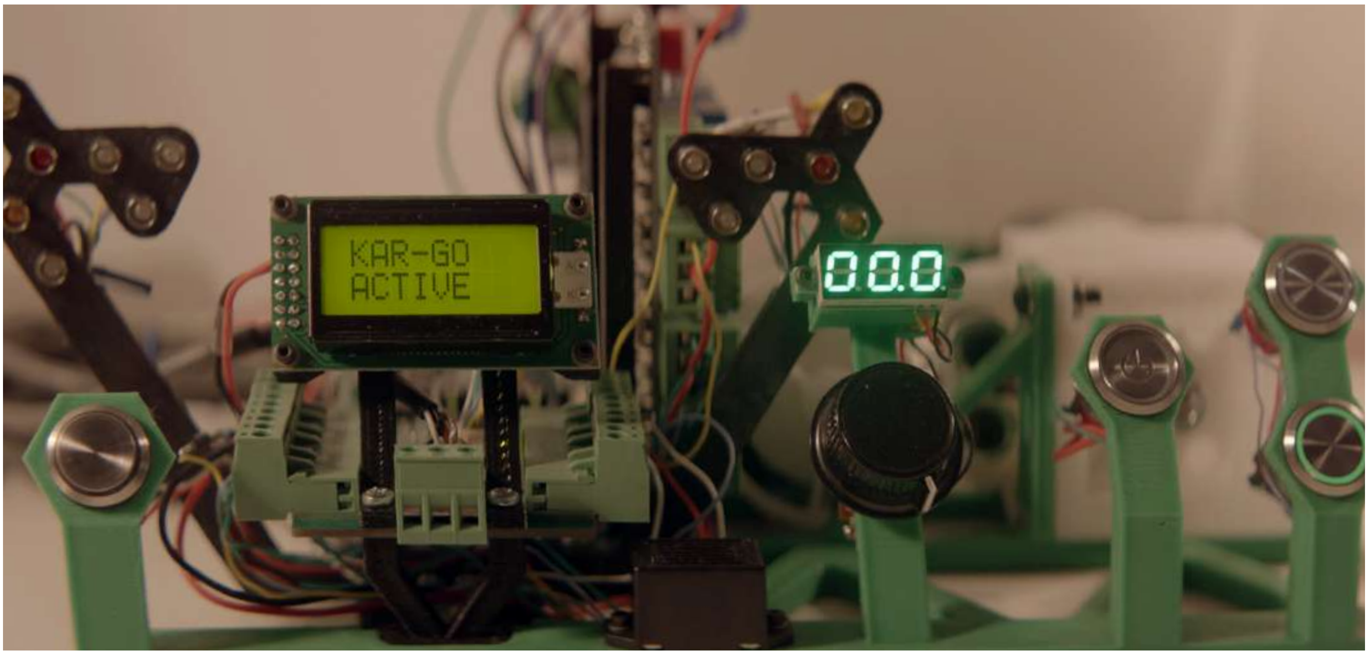
MODELLING AND SIMULATION STUDIES



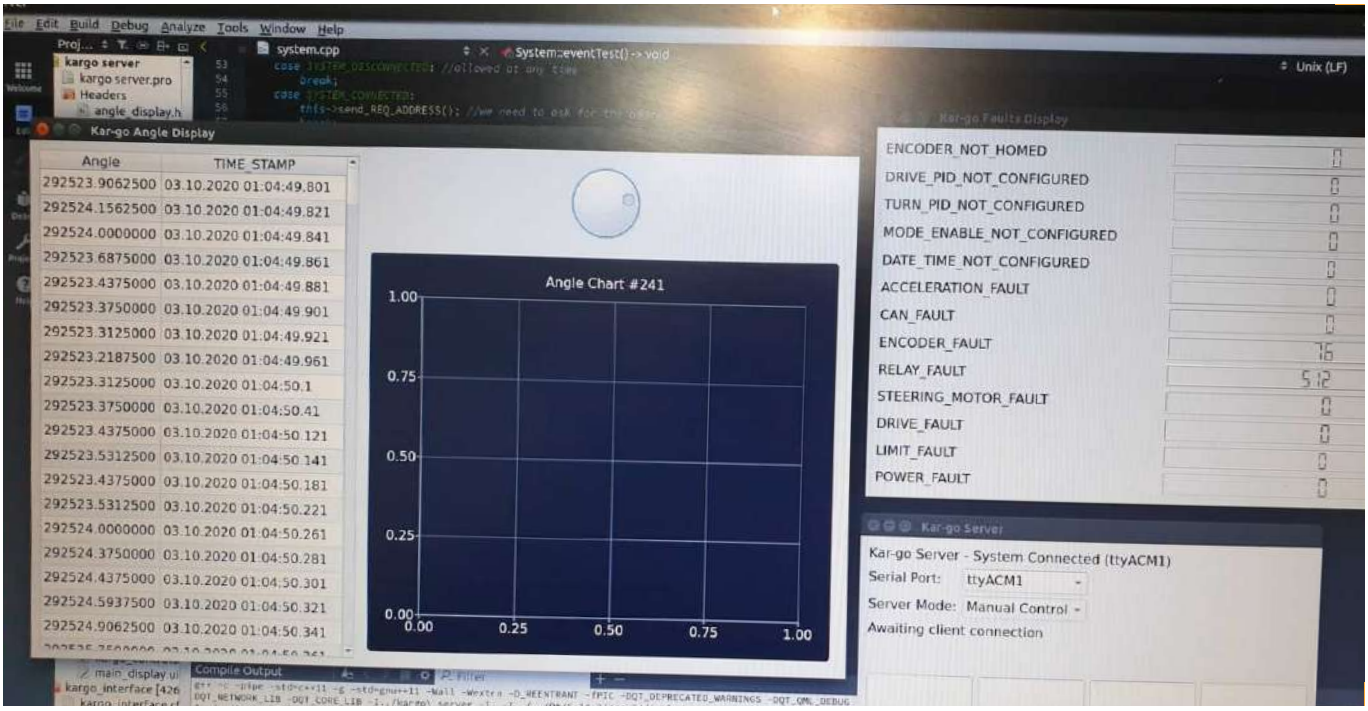
MODELLING AND SIMULATION STUDIES

All trialing is initially conducted in a virtual simulation environment as well is using hardware simulation. This is where custom routes and environments are constructed to test the vehicle in a safe, virtual environment. This virtual testbed is used to simulate safety parameters and test the vehicle's theoretical execution of routes relevant to the trial location. Further simulation tests are also conducted using an inhouse control sim; a vehicle dynamics and obstacle avoidance simulator platform that is used to further test the effectiveness of vehicle control strategies and emergency mode responses.

Ahead of the proposed trials, simulations of similar routes and negative road scenarios



Hardware Simulator allowing us to test Kar-go control systems



```
case SYSTEM_DISCONNECTED: //allowed at any time
    break;
case SYSTEM_CONNECTED:
    this->send_REQ_ADDRESS(); //we need to ask for the addr
```

Angle	TIME_STAMP
292523.9062500	03.10.2020 01:04:49.801
292524.1562500	03.10.2020 01:04:49.821
292524.0000000	03.10.2020 01:04:49.841
292523.6875000	03.10.2020 01:04:49.861
292523.4375000	03.10.2020 01:04:49.881
292523.3750000	03.10.2020 01:04:49.901
292523.3125000	03.10.2020 01:04:49.921
292523.2187500	03.10.2020 01:04:49.961
292523.3125000	03.10.2020 01:04:50.1
292523.3750000	03.10.2020 01:04:50.41
292523.4375000	03.10.2020 01:04:50.121
292523.5312500	03.10.2020 01:04:50.141
292523.4375000	03.10.2020 01:04:50.181
292523.5312500	03.10.2020 01:04:50.221
292524.0000000	03.10.2020 01:04:50.261
292524.3750000	03.10.2020 01:04:50.281
292524.4375000	03.10.2020 01:04:50.301
292524.5937500	03.10.2020 01:04:50.321
292524.9062500	03.10.2020 01:04:50.341
292525.2500000	03.10.2020 01:04:50.361

ENCODER_NOT_HOMED	0
DRIVE_PID_NOT_CONFIGURED	0
TURN_PID_NOT_CONFIGURED	0
MODE_ENABLE_NOT_CONFIGURED	0
DATE_TIME_NOT_CONFIGURED	0
ACCELERATION_FAULT	0
CAN_FAULT	0
ENCODER_FAULT	16
RELAY_FAULT	512
STEERING_MOTOR_FAULT	0
DRIVE_FAULT	0
LIMIT_FAULT	0
POWER_FAULT	0

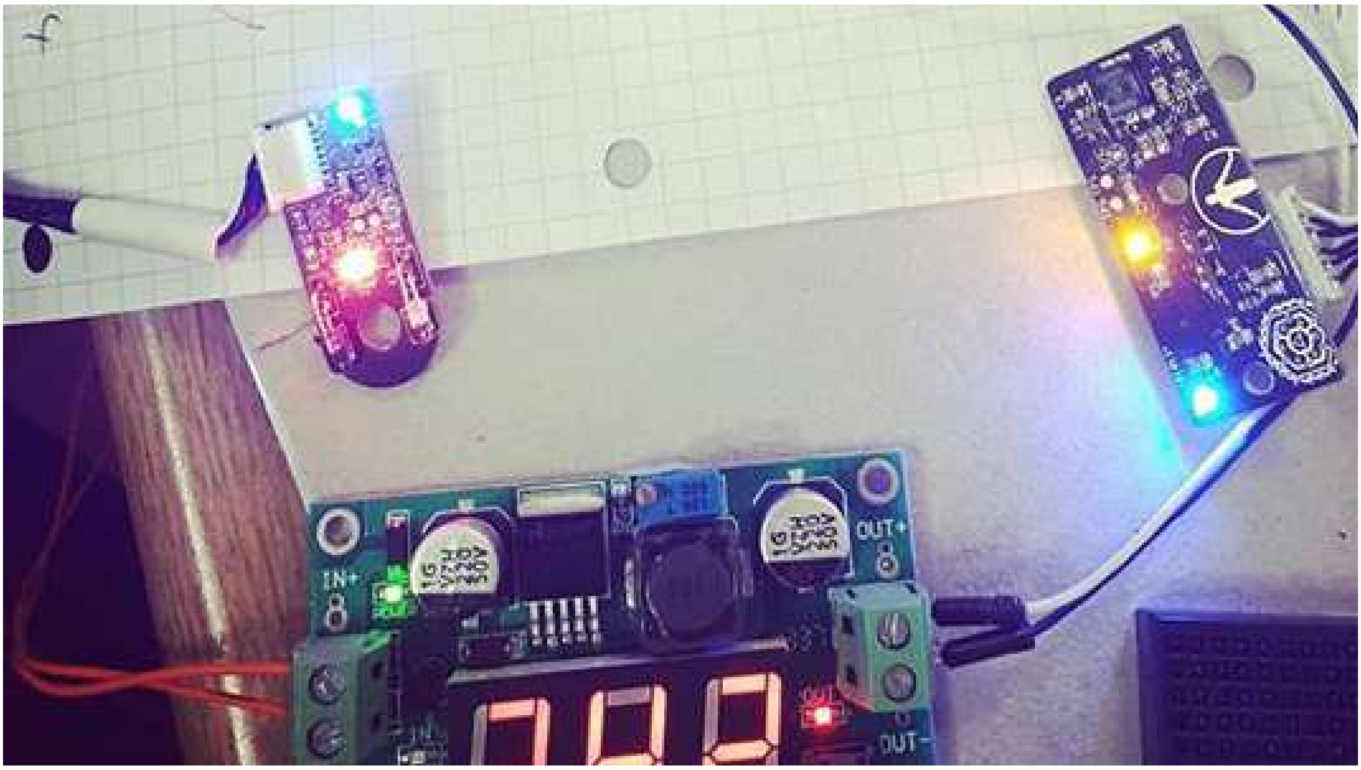
Kar-go Server - System Connected (ttyACM1)

Serial Port: ttyACM1

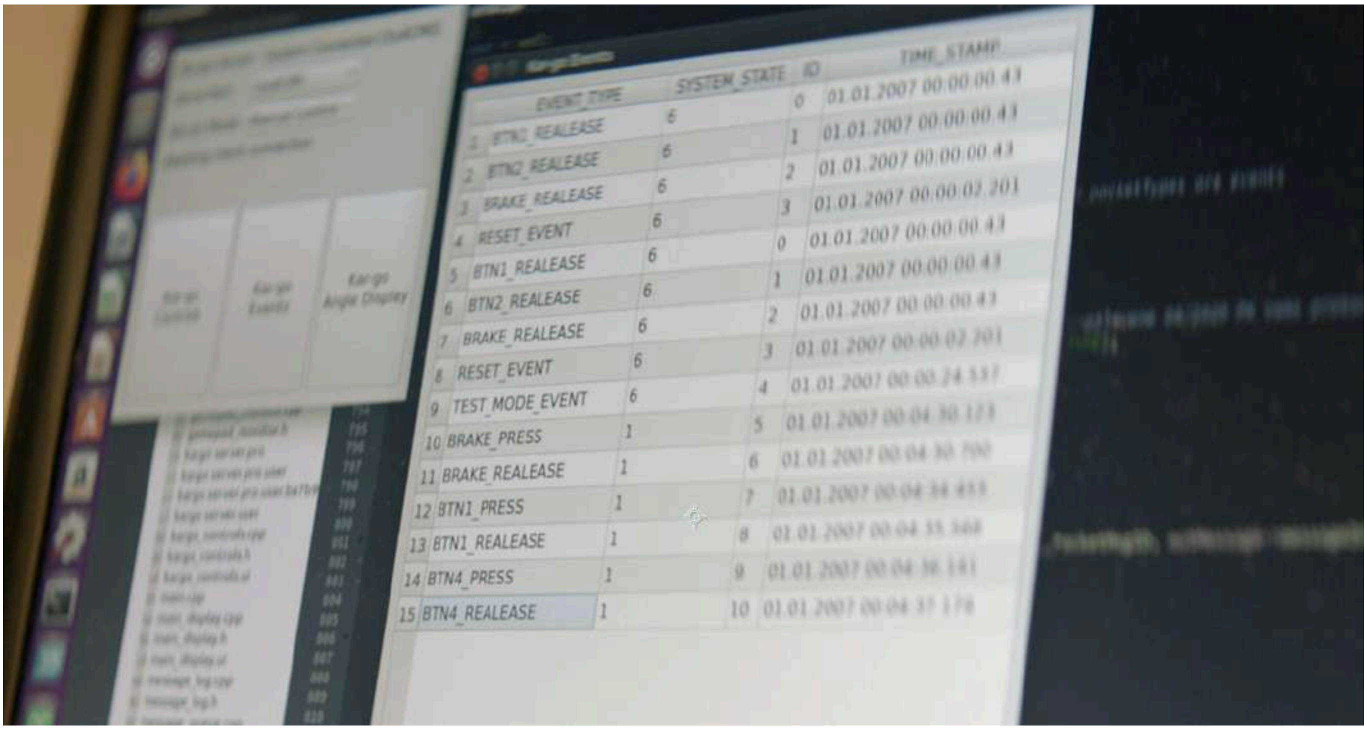
Server Mode: Manual Control

Awaiting client connection

Rigorous testing of thehardware safety layer.



Vehicle Control Dynamics Simulator



	EVENT_TYPE	SYSTEM_STATE	ID	TIME_STAMP
1	BTN1_REALEASE	6	0	01.01.2007 00:00:00.43
2	BTN2_REALEASE	6	1	01.01.2007 00:00:00.43
3	BRAKE_REALEASE	6	2	01.01.2007 00:00:00.43
4	RESET_EVENT	6	3	01.01.2007 00:00:02.201
5	BTN1_REALEASE	6	0	01.01.2007 00:00:00.43
6	BTN2_REALEASE	6	1	01.01.2007 00:00:00.43
7	BRAKE_REALEASE	6	2	01.01.2007 00:00:00.43
8	RESET_EVENT	6	3	01.01.2007 00:00:02.201
9	TEST_MODE_EVENT	6	4	01.01.2007 00:00:24.537
10	BRAKE_PRESS	1	5	01.01.2007 00:04:30.173
11	BRAKE_REALEASE	1	6	01.01.2007 00:04:30.700
12	BTN1_PRESS	1	7	01.01.2007 00:04:34.453
13	BTN1_REALEASE	1	8	01.01.2007 00:04:35.568
14	BTN4_PRESS	1	9	01.01.2007 00:04:36.141
15	BTN4_REALEASE	1	10	01.01.2007 00:04:37.178

OPERATIONAL DESIGN DOMAIN

OPERATIONAL DESIGN DOMAIN

WHAT IS THE OPERATIONAL DESIGN DOMAIN (ODD?)

The ODD refers to the operating conditions in which a driving automation system or feature is specifically designed to function ➔

ODD (OPERATIONAL DESIGN DOMAIN) OF THE VEHICLE

Academy of Robotics has developed a clear set of parameters that make up the operational design domain of the Kar-Go vehicle. These parameters act as the guidelines which determine a safe, planned for, environment in which the vehicle can operate.

Kar-Go's is designed to function semi-autonomously under these conditions:

- With a safety driver present in the driving seat and a specialist member of the team overseeing the operation from the control centre
- Only along the routes within the region specifically addressed in the route assessment section of the safety case
- Following the complete approval of the engineering team that oversees maintenance of the vehicle and its systems, this will be conducted before any trial delivery run
- During daylight hours and permitting that visibility is clear enough for detections to be made by the perception software and sensors.
- If weather is not deemed extreme and detections can still be made and their is no risk presented by the current weather
- Only in an 'on-road' environment

OPERATIONAL DESIGN DOMAIN OF THE TRIAL:

As this trial will feature a safety driver and thus, semi-autonomous driving, it will predominantly be at the drivers discretion how the vehicle is driven and the ADAS software will act as supporting technology. However, it is important to note the high-level boundaries of this project, which are as follows;

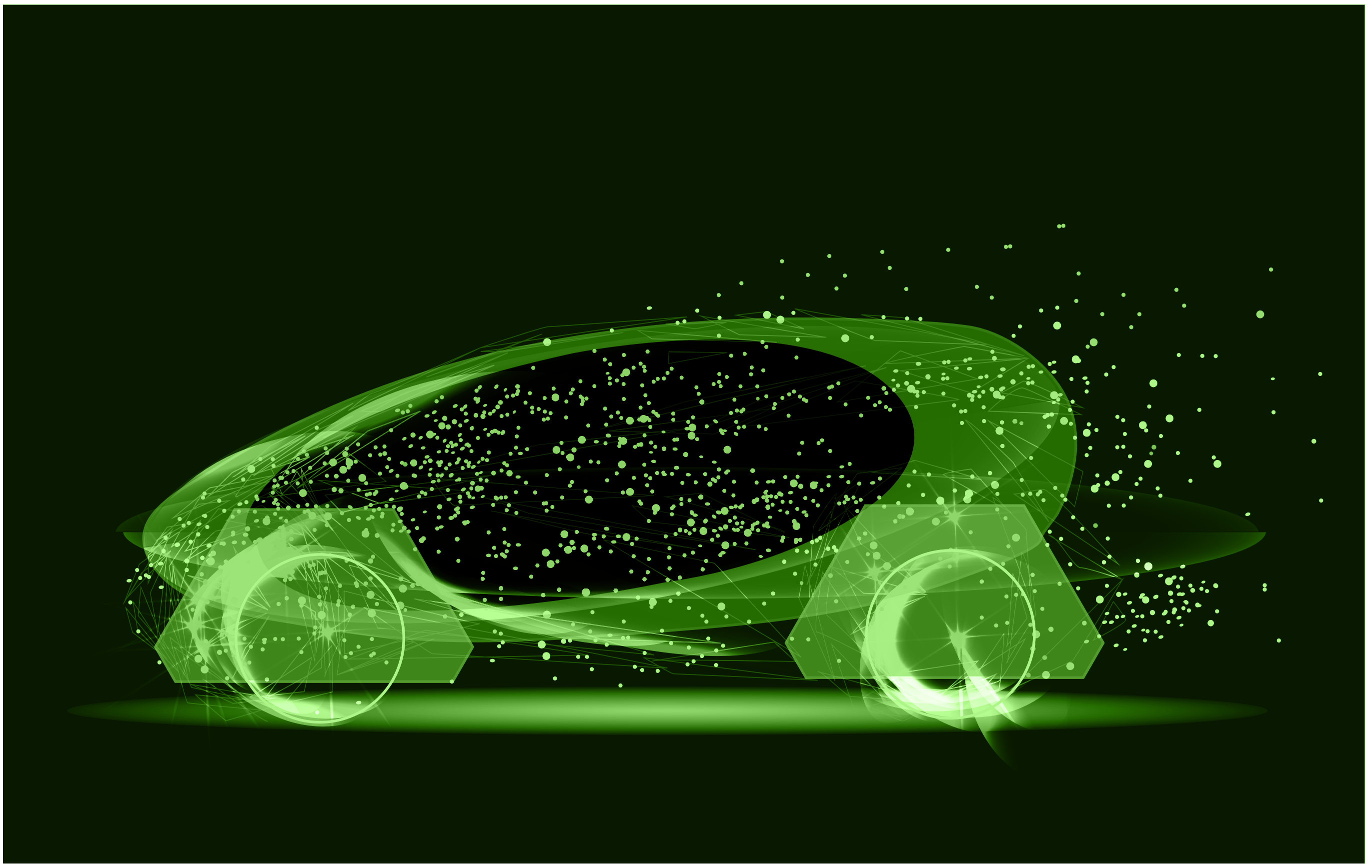
Whilst ADAS is different to ADS (automated driving system,) the software within Kar-Go means that the ADAS is a byproduct of the overall ADS. As such, within this documentation it can be assumed that both ADAS and ADS are interchangeable as terms since they are both connected to the autonomous software on-board. The perception and detection software within the vehicle is capable of distinguishing lane boundaries and road markings around it. This is the result of previous surveying and pre-training of the ADAS system that has allowed for the system to be calibrated for urban and suburban residential areas. As such, the delineation of lanes and understanding of road-markings as well as its pre-trained knowledge of the specified routes within the trial area, will inform it whether or not it is operating within the ODD. The safety driver and safety operator, stationed within the control centre, are also aware of the ODD.

The aforementioned control centre acts as an observation ground from which a safety operator can monitor the vehicle ADS remotely. This safety operator, who is trained extensively in the functions of the system and the correct intervention procedures, has the full capacity to intervene if required. Furthermore, the safety driver is also provided with a display to monitor the vehicle ADS while driving.

Any limitations of the vehicle ADS will not generate a risk to this trial as the vehicle will be driven semi-autonomously by a safety driver. Whilst the systems have been trained and designed with the ODD in mind and there are no perceived limitations. Instances where the ADS may struggle or underperform will be logged and subject to the feedback loop which will explore improvements to these systems in the final report and future post-trial research and development.

Engineering reports and maintenance checks will be dynamically conducted prior to and during the testing phase. This is to assess that the vehicle can safely operate within its ODD. This will involve an extensive examination of the vehicle and its system adhering to a maintenance checklist and taking into account feedback reporting by the safety driver in the drivers log. The lead engineer on the project will fulfil the role of approving the vehicle for safe operation. As the vehicle will be driven by a safety driver, there is no need for supporting vehicles in this trial. Furthermore, engineers will be present with the safety operator within the control centre to monitor and analyse vehicle safety during operation, allowing them to provide feedback.

Simulator training of the route and similar scenarios, along with feedback from private



testing of the vehicle ADS and intervention procedures in place, ensure that the system can operate safely within the ODD. This is further reinforced by the semi-autonomous nature of this trial, in which the focus will be on the no-contact delivery elements and so a safety driver will be in control for the full duration of this vehicle operation.

The minimal risk condition for the operation of the Kar-Go vehicle is a situation in which the ADAS detects an irregularity comparative to its pre-trained understanding of a road. This can be classified as;

- A detection that indicates an impending risk
- A signal from a software module(s) that indicates a potential risk
- A fault or malfunction in the software/hardware
- As a final layer of safety, a sensor detection that indicates a risk based on proximity.

In autonomous driving, minimal risk conditions would trigger emergency mode and a series of steps that can safely remove the vehicle from any risk conditions. However, as this trial is semi-autonomous, minimal risk conditions will be observed and can be acted upon by the safety driver and control centre safety operator.

MONITORING, REPORTING AND CONTINUOUS IMPROVEMENT

MONITORING, REPORTING AND CONTINUOUS IMPROVEMENT

INCIDENT LOGGING

In the instance of an incident, an incident log will function as a method of recording a detailed overview of the incident as well as the contributing factors that led to its occurrence. This log will be reviewed by responsible members of the team and made available to governing bodies at request. Incidents are recorded under the following categorization:

- Emergency
- Non-Emergency
- Near Miss
- Breakdown of vehicle
- Malfunction of software
- Malfunction of hardware
- Staff/Personnel Incident
- Undesired Event

All incidents are reported to the trial manager and trial coordinator. Incidents related to the vehicle ADS are also reported and recorded by the safety operator. Furthermore, the escalation of incidents is overseen by the project manager in conjecture with the trial coordinator.

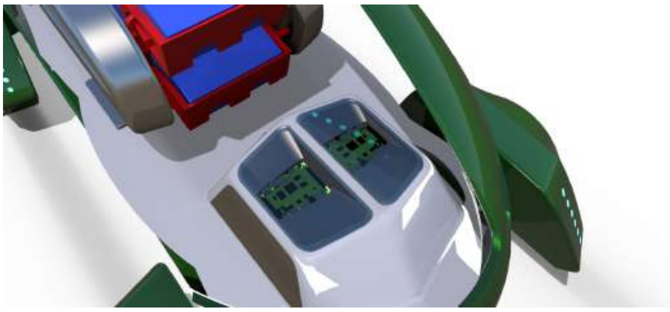
Whilst the vehicle will be driven semi-autonomously, if the vehicle ADS signals that it would trigger emergency mode and begin a disengagement process were it in control, this information would be logged by the safety operator. As all data is recorded and stored, this would enable a review of the perceived incident that triggered this process and an analysis of why this automatic disengagement action would have taken place.

HOW IS DATA MONITORED?

The data captured by the vehicle ADS is recorded and monitored by the safety operator. The safety data recorded is included in the summary of specific vehicle metrics recorded and is obtained from the camera software attributed to the Kar-Go vehicle, observations by safety driver and safety operator, and on-board monitoring systems that can determine the distance travelled, time taken and speed of the vehicle. Whilst the vehicle can record these metrics, the safety operator can act as an additional human recording resource.

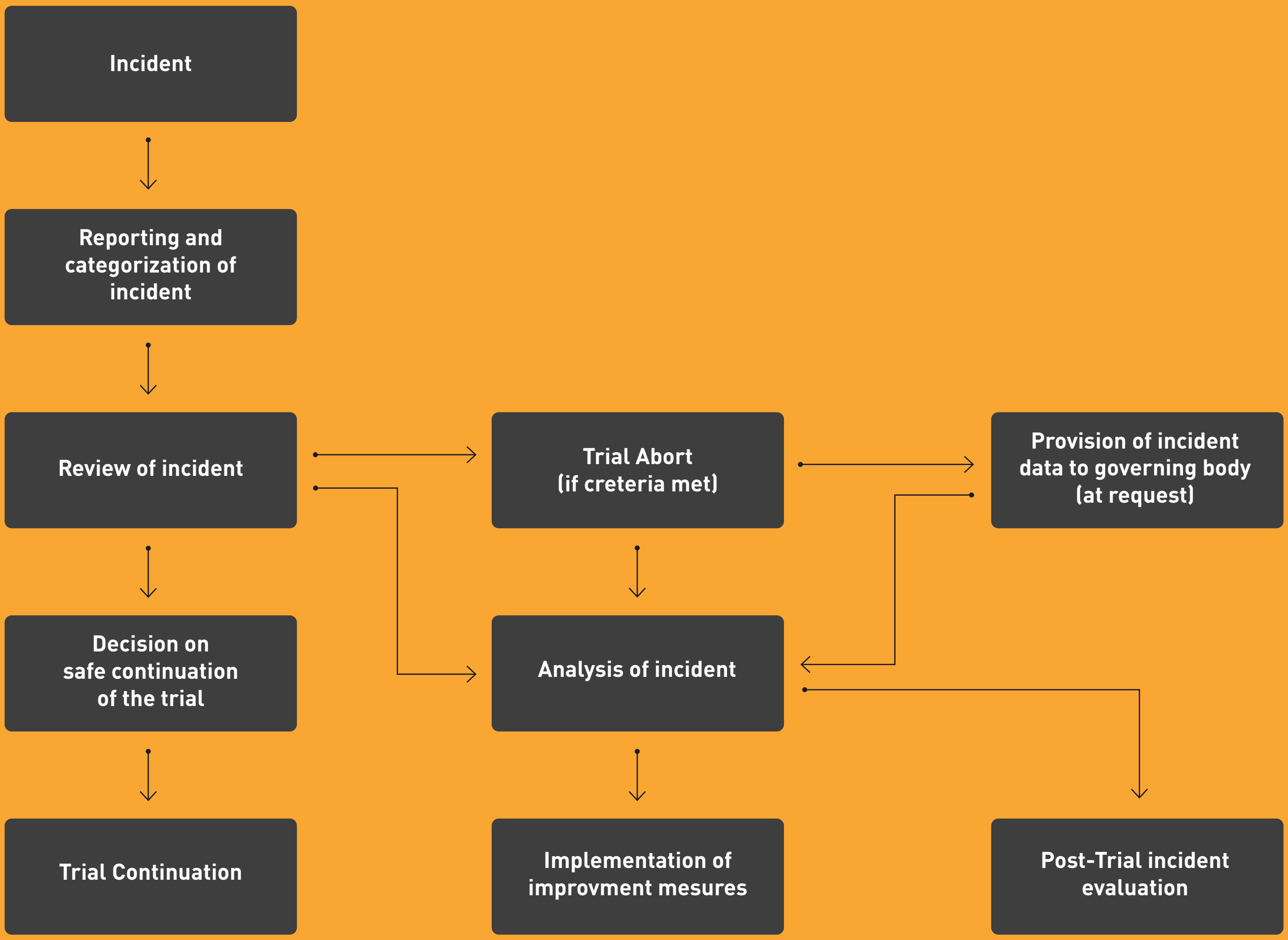
Data recording and logging will start when initiated by the safety driver as they begin operation on the route. This will end once the journey has been completed and be deactivated by the safety driver. The timeline of this data recording segment will be matched with the recorded duration of the trial run undertaken by a member of project personnel and matching timeframes will be verified to preserve the integrity of the data. To further assure that the data is not tampered with, security features are integrated into the data access interface that logs which user has accessed which information and at what time. Administrative access to this data is only provided to project developers with specialised knowledge of the system. Data is stored in the vehicle harddrive. The control center can connect to it and monitor the vehicle feed in real time. Post drive, the data is transferred to offline storage servers and catalogued along with raw driving logs from the controller circuit.

Dynamic hazards are monitored frequently and the route is surveyed prior to a delivery test run. This allows for the monitoring of any recently emerged hazards as well as an assessment of traffic flow. Weather will be consistently monitored throughout the trial period and expected weather on the day of a trial delivery run will be recorded and reviewed by all project team members.



LESSONS LEARNT AND CONTINUOUS IMPROVEMENT

This safety case shall function as a live, version-controlled document throughout the project and trial period. Lessons learnt, through a feedback loop, will be detailed along with an edit log that will be supplemented by an audit trail system that will provide a more detailed overview of implemented changes to the safety case, project, software and hardware.


Incident
Reporting and categorization of incident
Review of incident
Decision on safe continuation of the trial
Trial Continuation
Trial Abort (if creteria met)
Analysis of incident
Implementation of improvment mesures
Provision of incident data to governing body (at request)
Post-Trial incident evaluation

Incident reporting process:
The above diagram shows the incident reporting process in place throughout the trial.

ABORT CRITERIA

ABORT CRITERIA

WHAT LEVEL OF RISK TRIGGERS THE ABORT CRITERIA?

In the instance of an abort criteria being met, all trial activity will be ended and a complete review will be completed before further testing can resume. Abort criteria risks are tiered into levels which determine their potential impact and what that would mean for further testing after a safety review has been completed. ➔

HIGH-LEVEL RISKS (TESTING WILL NOT RESUME FOLLOWING A SAFETY REVIEW)

These risks include incidents in which endangerment was brought to human life, whether the safety driver, other road users, pedestrians or trial personnel. In the instance that it is required, a full investigation will be undertaken and cooperation and data will be provided to police investigators. Increased pandemic restrictions may also pose a high-level risk to the trial and the length of the restrictions may determine when, if at all, the trials may resume following a safety review.

MID-LEVEL RISKS (TESTING WILL LIKELY RESUME FOR FUTURE TRIALS)

These risks include malfunctions with the vehicle, hardware and software that in order to fix, would exceed the duration of the project. Replacement and maintenance will occur and the incident will be logged and the safety case reviewed, however the duration of these changes may result in exceeding the trial duration. This also applies to extreme weather scenarios in which driving is deemed unsafe for a significant period of time.

LOW-LEVEL RISKS (TESTING CAN RESUME WITHIN THE PROJECT DURATION)

These risks include brief road closures on all assessed routes, including reserve routes, brief extreme weather or low visibility that makes semi-autonomous driving unsafe (applicable to all road users.) Furthermore, malfunctions and maintenance required on the vehicle, software and hardware may present a situation where the vehicle cannot be driven for a brief period of time within the trial duration window. Maintenance provided to the vehicle will be logged, reviewed in accordance with the safety case (additions made where necessary) and the vehicle will be approved to resume trialing.

Low-level risks will be analysed in detail by the trial team before the operation of the vehicle continues within the trial window.

Risk	Who is harmed and how?	Risk Prevention Actions	Risk Rating
Risk of incident whilst Autonomous Driving (Vehicle Operation)	Members of the general public, trial operators and present safety drivers may be harmed as a result of vehicle collision or malfunctioning with autonomous navigation software. General automobile risks also apply.	a. Safety Driver training b. Controller design failsafes c. Software design failsafes d. Emergency Mode e. Trial on public roads only after route specialization f. Speed Limiting g. Pre-trial safety checklist h. In-house audits	Likelihood: 1 Consequence: 4 **Risk Level: 4**
Risk of incident whilst Full Manual Driving (Vehicle Operation)	Members of the general public, trial operators and present safety drivers may be harmed as a result of vehicle collision or malfunctioning with autonomous navigation software. General automobile risks also apply.	a. Approve driving by selected, trained staff only b. Training and pre-operation safety checks c. Pre-trial safety checklist	Likelihood: 1 Consequence: 4 **Risk Level: 4**
Vehicle Hardware Malfunction (Vehicle Operation)	Vehicle hardware either directly or indirectly related to autonomous technologies may malfunction and present threat to any vehicle occupant or surrounding presence	a. Ensure vehicle is compliant with DVLA and insurance requirements to be road worthy b. Thoroughly test autonomous software/hardware in controlled demo environment prior to road usage	Likelihood: 2 Consequence: 3 **Risk Level: 6**

Risk	Who is harmed and how?	Risk Prevention Actions	Risk Rating
Environmental Variability: Extreme Weather (Vehicle Operation/ Software)	In instances of extreme weather, the vehicle may be prone to damage or be presented with unsafe driving conditions that either; a. Cannot be tackled by autonomous software safely b. Cannot be tackled by a human driver safely	a. Comply with general safety standards for operating vehicles in incidents of extreme weather b. Ensure an active link between vehicle and command hub in the case of sudden weather change, to allow for emergency mode if required c. Available drivers have been trained on how to deal with adverse weather effects	Likelihood: 3 Consequence: 1 **Risk Level: 3**
Environmental Variability: Traffic Collision (Vehicle Operation/ Software	A road may be obstructed in a way that the vehicle is unable to detect and thus create a hazard when the autonomous navigation software attempts to navigate it. This may also mean scenarios where road closures affect the ability to proceed with the trial.	a. Exhaustive surveying before trial b. For initial trials have a manual drive first to scan route on the day c. sub-database of such scenarios and integrate them into training database such that the software is aware perceptually how to action such conditions.	Likelihood: 2 Consequence: 2 **Risk Level: 4**
Inaccurate Training/ Evolutionary Runs of A.I (Software	This will lead to either minor or catastrophic errors in the perception/ detection modules which will in turn have an adverse effect on vehicle navigation capabilities.	a. Multi-stage checking of training labels b. Execution of training runs by select personnel with appropriate know-how/training c. Post training checks	Likelihood: 2 Consequence: 1 **Risk Level: 2**

Risk	Who is harmed and how?	Risk Prevention Actions	Risk Rating
Perception Inaccuracies of Software (Software)	This will lead to either minor or catastrophic errors. Such a scenario may occur even without any inaccuracies in the trained networks, as this could simply be a failure to adapt to local/ dynamic noise.	a. Failsafes to mitigate effects if such a scenario does arise b. Emergency Mode/Buffer zone from distance sensors. c. Off-line tests on survey dataset of route	Likelihood: 3 Consequence: 2 **Risk Level: 6**
Software Corruption & Memory Faults (Software)	Minor and major faults during live operation and/or off-line testing which may either affect performance or cause data loss, software corruption.	a. Test, debugging and memory checks b. Thorough backup of software versions and data logs/results c. Vehicle Control design failsafes which causes immediate halt in case of interrupt signal and/or disengagement from on-board computer.	Likelihood: 1 Consequence: 4 **Risk Level: 4**
Power Faults short circuit, voltage surge, power loss (Hardware/ Circuit)	This is relevant to the prototype circuit chips. Such faults can completely destroy the circuit and render them unusable for trials.	a.Produce multiple circuits to account for backups b. Design and simulation of fault protection features c. ESD (Electrostatic Discharge) protection when working with microelectronic systems	Likelihood: 1 Consequence: 4 **Risk Level: 8**
FPGA production delays (Hardware/ Circuit)	Delays in production can arise from the need to redo aspects of circuit design, or detection of faults post production. Will have an impact on WP4 (tests)	a. Thorough simulation before final prototype production b. Planning accounts for delays upto 2 months for WP3	Likelihood: 2 Consequence: 3 **Risk Level: 6**

Likelihood: 0 (Totally Unlikely) - 5 (Very Probable); Consequence: 0 (No impact) - 5 (Severe Impact to project and/or associated work package), Risk = Likelihood x Consequence

hello@academyofrobotics.co.uk +44 1639 544 996 www.academyofrobotics.co.uk