STREETDRONE

Abridged Safety Case

Summer 2022 Demo Trials & Demonstration

Prepared by Abdullah Baig

Autonomous Safety Engineer – StreetDrone

Document Version Control		
Version Number	**Date Created**	**Notable Changes**
1.0	14/06/2022	First Draft

Prepared By	Abdullah Baig	Autonomous Safety Engineer
Reviewed by	Ross James	Lead Safety Engineer

1 Introduction

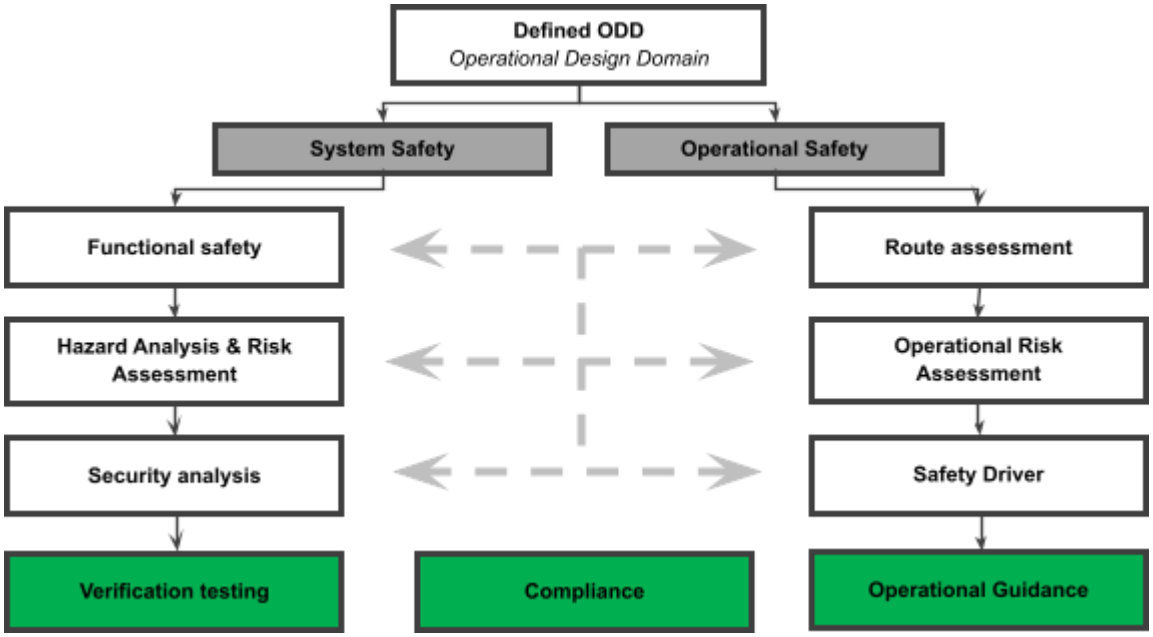
This safety case is developed and owned by StreetDrone as the organisation responsible for managing and conducting autonomous vehicle demonstrations at Osney Mead, Oxford, UK as part of the Summer 2022 Demo project.

The Summer 2022 Demo project will demonstrate only the first portion of the ENCODE project which took place at Osney Mead. Connected and Automated Vehicle (CAV) developer StreetDrone aims to reduce time to market for connected and automated vehicle technology in the movement of goods. The project centres on the use of "multi-driver" vehicles, and accompanying security and safety assurance, to enable StreetDrone and the UK to be first to market in the automation of the freight supply chain. A "multi-driver" vehicle is one which can be driven via in-vehicle driver, remote driver, or autonomous driving stack (ADS). This Demo will examine the safe and secure integration of "teleoperation", the ability for a remote driver to assist a CAV when the situation deems it necessary. StreetDrone provides an open, end-to-end solution to bring autonomy to urban environments. Making it faster, easier and safer for cities to deploy, learn and scale autonomous urban vehicle trials towards commercial application.

StreetDrone deploys a safety-first principle, and this safety case has been produced in accordance with the Centre for Connected & Autonomous Vehicles, *Code of Practice: Automated vehicle trialling* [1]. This safety case has been developed to incorporate UK good practice and is based on both the *Safety Case Framework – a report by Zenzic* [2] and *PAS 1881:2020 Assuring safety for automated vehicle trials and testing – Specification* [3] and *PAS 1883:2020 Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification*. [9]

The purpose of this document is to summarise the body of evidence produced to ensure any hazards are identified and all risks are mitigated or minimised to a level As Low As Reasonably Practicable. This document acts as a central link to all the relevant information that constitutes the safety case. Where detailed information is not written within this document, links are provided to the latest or frozen versions of relevant documentation.

This document outlines StreetDrones methodology for ensuring an acceptable level of safety is achieved for those involved in the trials and demonstration and for members of the public. Figure 1 provides an overview of the approach followed by StreetDrone with respect to assessing both system safety – the safety of the autonomous functionality of the vehicle, and operational safety – the assessments and resulting guidance documents focussing on the wider demonstration environment.



The overriding mitigation against risk throughout StreetDrones demonstration(s) is the presence of a Safety Driver who is always ready to take instant control of the vehicle at all times, as such, the key consideration when preparing this safety case is to ensure there are no hazardous events under which the Safety Driver is unable to regain control of the vehicle.

2 Operational Design Domains (ODD)

Complete definition of the Operational Design Domain is key to building the wider safety case as it sets out the conditions under which the vehicle is permitted to drive either autonomously or teleoperated within, ensuring the safety driver has a clear understanding of the ODD also ensures they know when to regain manual control.

Many factors contribute to building a comprehensive ODD, for StreetDrone these include geographic location, site accessibility, maximum speed, weather, and local environment features to name but a few. StreetDrone has developed a detailed ODD to cover the planned demonstration(s) on Osney Mead.

Ensuring that the ODD is fully defined is important when deploying autonomous systems safely, the safety driver is responsible for dynamic monitoring of the ODD during automated operation, hence making it as clear as possible when the conditions fall within the ODD or not enables the Safety Driver to swiftly react and take control when conditions fall outside of the operational domain.

3 Route selection and assessment

This section documents the considerations given when selecting the route for the planned trial

3.1.1 Osney Mead, Oxford – Route Overview

This trial/demonstration route shall consist of a small section of public road on Osney Mead, Oxford, the route has been selected based on the following criteria:

- Must be such that travelling at speeds of up to 10mph would not cause any unnecessary hazard to other road users.
- Should be such that safety driver overrides are reduced to a minimum.
- Should be such that minimal opportunities arise for encountering dynamic objects / hazards.
- Should incorporate straight sections of road >100m and turns, preferably both left and right hand.
- Carriageway must be wide enough for the e-NV200 and another vehicle to pass, >4.5m.

Once a suitable route had been selected (Figure 2), a route assessment was conducted to identify any hazards that increase the level of risk posed during testing. Several methods were used to make assessments of the route including but not limited to, a walk-through route assessment, route measurements and data search. All results from the route assessment were fed into the Hazard Analysis and Risk Assessment and Operational Risk Assessment.

As shown in Figure 4 some sections of the route will be driven manually, this is based on limitations of the Driving Automation and Teleoperation Systems and ensuring the safety driver has control of the vehicle during manoeuvres which present higher risks, such as performing a U turn.

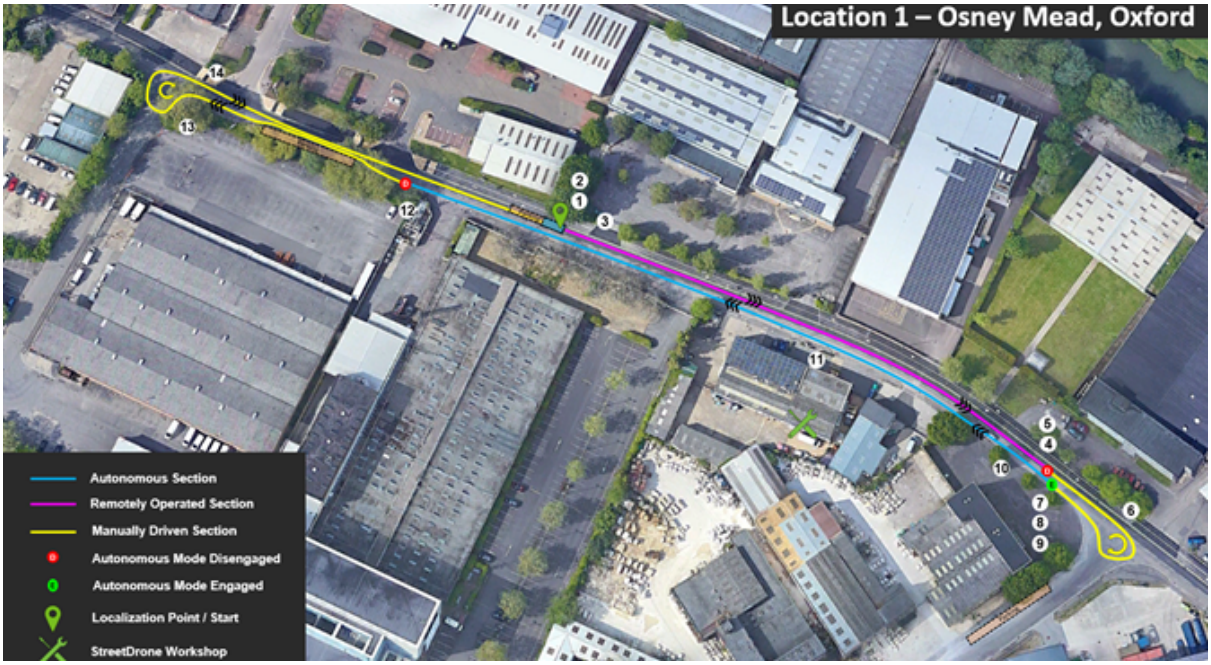


Figure 2 - Osney Mead Trial Route

4 Vehicle and automated system

The demonstration will take place using the StreetDrone Nissan e- NV200. Vehicle registration DK16 RTZ is owned by StreetDrone. The Nissan e-NV200 vehicle is type approved which have been modified by StreetDrone, modifications take the form of a Drive by Wire overlaid onto the existing base vehicle controls. Additional motors and actuators have been fitted to the steering column and brake system such that they can be activated based on signals sent from the XCU control system.

The vehicle is fully compliant with MOT, insurance and Construction and Use Regulations.

Figure 4 - Osney Mead Demonstration Route

4.1 Driving Automation System

The Nissan e-NV200 StreetDrone vehicle operates at SAE level 2 [6], the below description is taken directly from the SAE J3016 and applies to both vehicles.

> *The sustained and ODD-specific execution by a driving automation system of both the lateral and longitudinal vehicle motion control subtasks of the DDT with the expectation that the driver completes the OEDR subtask and supervises the driving automation system.*

NOTE: A level 2 driving automation feature is capable of only limited OEDR, meaning that there are some events that the driving automation system is not capable of recognizing or responding to. Therefore, the driver supervises the driving automation system performance by completing the OEDR subtask of the DDT. See Figure 1 (discussing the three primary subtasks of the DDT).

Furthermore

NOTE 1: At levels 1 and 2, the conventional driver is expected to achieve a minimal risk condition as needed.

These definitions form the basis of the Driving Automation System design as well as all safety driver training. Subsequent sections outline the key functionalities of StreetDrones Driving Automation System.

4.1.1 Capabilities

- Following a pre-mapped route using pre-recorded waypoints.
- Maintaining a pre-determined consistent vehicle speed.
- Object detection validated on static objects.

4.1.2 Limitations

- Although any object within a certain proximity of the vehicle will cause it to stop, the system has not been designed or verified for dynamic objects.
- The vehicle has no capability to deviate from the fixed route along pre planned waypoints. Should the route be blocked by for example a parked vehicle, the Safety Driver must take over and navigate around the obstacle before reengaging automated mode.

4.1.3 e-NV200 Software Operation

Monitoring and control relating to the operation of the Driving Automation System is performed by a software engineer from row 2 of the vehicle, a screen has been fitted to the rear of the passenger seat for the purpose of carrying out the required activities.

4.2 Teleoperation system

As part of the multi-driver system developed for the Summer demo trial a Teleoperation system has been implemented to allow a remote driver to send steering, throttle, and brake commands through to the on-vehicle XCU control system. These commands are handled by the XCU in an identical way to commands coming from the Driving Automation System. When operating in teleoperation mode as with Automated driving mode the safety driver remains responsible for completing the OEDR subtask and supervising the commands being actuated.

Off-highway closed site testing has been performed to ensure the remote driver has an appropriate level of control over the vehicle equivalent to that of the Driving Automation System.

4.3 Switching between manual and automated and teleoperated modes

Switching between manual and automated/teleoperation mode requires a set procedure to be followed, this procedure is taught during the safety driver and remote driver training programme. Physical input is required from the safety driver to engage autonomous or teleoperation mode, once verbal confirmation has been received from the Software engineer that the vehicle has localised.

The Safety Driver has multiple available methods to regain manual control as outlined below, Safety Driving training covers the most appropriate method to use depending on the scenario.

- Manual input to steering wheel
- Manual input to brake pedal
- Manual input to accelerator pedal
- Switching the automated mode switch back to manual
- Pressing the e-stop button
- Turning the actuator master key

5 Functional safety

A complete functional safety analysis has been conducted by StreetDrone of the Drive by Wire system based upon principles described in functional safety standards such as IEC-61508 and ISO 26262. However due to the limited scope of deployment into society of small numbers of StreetDrone Twizy & e-NV200 vehicles (a modification of a production vehicle, not a new vehicle), full compliance with ISO 26262 is not proportionate nor a legal requirement.

6 Cyber Security

A full in-depth cyber security analysis of the StreetDrone Nissan e-NV200 has been completed, examining cybersecurity risks from a saboteur without physical access to the vehicle, i.e. across Wi-Fi™ or 4G connection, or by scrambling a signal input to a sensor. Also examined is the risk posed by a saboteur with physical access to the system, who can tamper, remove or damage equipment. Key requirements from this analysis are captured in the operational guidance documents.

7 Hazard Analysis and Risk Assessment

In order to provide high level assurance of system safety encompassing the whole Driving Automation and Teleoperation Systems, top level hazards were identified based on pre-existing knowledge of the system limits, these were fed into a HARA (Hazard Analysis and Risk Assessment).

The following hazardous scenarios or events were identified and fed into the HARA document.

- Front collision with oncoming traffic
- Front collision with ahead traffic
- Rear collision with trailing traffic
- Collision with another vehicle (parked)
- Collision with cyclist
- Collision with pedestrian
- Collision with obstacle / road furniture

The following potential causes or deviations relating to the hazardous scenarios above were analysed. All of the subsystems within the Driving Automation and Teleoperation Systems have been designed such that no failure shall result in the below causes occurring, however as this is an R&D vehicle, the HARA analysis has been conducted to ensure should any of these potential causes occur, appropriate mitigations are in place which means the previously mentioned hazardous events do not occur.

- Incorrect steering
- Incorrect acceleration
- Inappropriate braking
- Inappropriate lack of braking
- Sudden loss of autonomous control
- Failure of mechanisms to deactivate the autonomous system

7.1 Overview of Mitigations

As set out previously within this document, a safety driver shall always be present and the major mitigation for any hazardous event is the ability of the safety driver to regain control immediately. In order to do this both the driving automation system and the teleoperation system contain elements of self-monitoring as well as a further level of monitoring within the drive-by-wire control system.

8 Operational risk assessment

Separate to the HARA, a complete operational risk assessment has been conducted which covers all additional risks associated with the trials/demonstration(s) not relating to Driving Automation or Teleoperation System errors.

In line with risk assessment best practice and guidance within PAS 1881, all risks have been reduced in line with the ALARP (As Low As Reasonably Practicable) principles and all mitigations identified have been implemented through clear operational guidance.

9 Compliance

A desk exercise has been completed to ensure the planned demonstration(s) are fully compliant in the following areas.

- DfT Code of Practice
- Highway Code & Road Traffic Laws
- Data Protection
- Insurance

9.1 Data Protection

To ensure any video and image data collected during the on-road trials/demonstrations complies with relevant conditions under the Data Protection Act / GDPR, StreetDrone has conducted a Data Privacy Impact Assessment as well as clear processes for secure transfer and storage of data.

10 Operational guidance

Operational guidance is based on the mitigations highlighted in the HARA, operational risk assessment, cyber security analysis & compliance study. The operational guidance takes the form of a series of instructional documents detailing how the demonstration(s) should be run.

The documents include:

- Defined roles and responsibilities
- Detailed safety driver policies covering training, behaviour, and monitoring
- Guidance on marshal positions
- Emergency response plan
- Method Statements

Prior to any demonstration day or phase, a method statement shall be disseminated to all trial staff detailing the relevant operational guidance documents alongside an overview of the testing and the key risks and mitigations. A briefing session shall also be held by the trial manager at the start of each day to highlight any important changes to the documents which have been disseminated.

11 Safety testing and acceptance process

StreetDrones software development follows the industry standard systems engineering V model.

A comprehensive suite of verification testing has been conducted prior to any public road testing.

11.1 Hardware & Software change control procedure

StreetDrone has a detailed change control procedure which shall be followed throughout the preparation and delivery of the demonstration(s). This procedure shall be adhered to throughout the project however it is of key importance after the hardware, software or safety case have been signed off as complete.

12 Monitoring, reporting and continuous improvement

Dashcams shall be fitted to all StreetDrone vehicles used for demonstration(s) these cameras are capable of recording a full day of video before overwriting. Should any incidents or near misses occur the memory card shall be secured by the Safety Driver and provided to the Trial Manager for review.

The Safety Driver is responsible for monitoring the ODD through the automated driving, should any conditions fall outside the ODD, the safety driver shall take control of the vehicle. The trial manager is responsible for monitoring the weather conditions in advance and informing all trial staff of any predicted weather which would fall outside of the ODD.

12.1 Incident and near miss reporting

Throughout the duration of the demonstration(s) StreetDrone's incident and near miss reporting procedure shall be followed by all trial staff members.

A safety steward shall be present within the front passenger seat of the vehicles to record any incidents or near misses.

13 Stakeholder consultation and engagement

Several key stakeholders have been consulted regarding the planned demonstration(s) to ensure everyone is aware of the activity and that any concerns can be raised and resolved prior to the demonstration, these include:

- Oxfordshire County Council iHUB Team
- Oxfordshire Fire and Rescue
- Oxfordshire County Council Emergency Planning
- Thames Valley Police
- Oxfordshire County Council Traffic Management
- CCAV

14 Point of Contact

Any questions relating to the abridged safety case or the demonstration(s) being conducted should be directed to info@streetdrone.com, where they will be forwarded on to the most relevant person for answering.

15 References

[1] https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public

[2] https://zenzic.io/insights/safety-case-framework-report/

[3] https://standardsdevelopment.bsigroup.com/projects/2019-00537?_ga=2.203258898.2092963123.1572208211-830469361.1548333176