Connected Places Catapult

Failure Mode and Effect Analysis for Testing in a Controlled Car Park

December 2019

Autonomous Valet Parking

Version Number	Reason for Update	Updated By	Date
0.1	First release	Richard Hillman	25/02/2019
1.0	Testing in a car park	Adrian Beford	21/11/2019
1.1	Ready for Publication	Maysun Hassanaly	17/12/2019

Description:

The FMEA is based on the functional architecture of the AVP system. Each possible fault that could occur within the system is considered and how that fault will affect the rest of the system, including any failures or other undesirable behaviours that the fault could cause the system as a whole to display. This is referred to as a 'bottom- up' or 'inductive' approach, as it starts with the fault (at a low level) and works up to the effect on the high-level behaviour of the system, as opposed to 'top-down' or 'deductive' analysis (e.g. Fault Tree Analysis), which starts at the high-level failure and works downward to identify the fault(s) that form the root cause.

A workshop was held with the project consortium, where participants were asked to identify what possible failures could occur in each sub-subsystem, what the local effect would be on the subsystem in which it resides, and whether this would result in any undesired vehicle-level behaviours.

It was decided not to apply severity and likelihood scores to each failure (this is commonly referred to as Failure Modes, Effects and Criticality Analysis, FMECA) due to the difficulty in estimating reasonable scores (each failure typically causes a low chance of a high severity accident, a higher chance of a lower severity accident, plus an infinite number of variations on the spectrum between these points), the limited resources available, and the fact that there would have been little that the creation of such prioritisation scores would achieve in the project anyway. However, Safety Goals (i.e. high-level requirements for what should be done to mitigate the risks) were logged for each fault, and these were incorporated into the Requirements Spreadsheet, with corresponding test cases and acceptance criteria being added.

Notice

By using this safety report ("the Report") produced by the Connected Places Catapult ("CPC") you accept this disclaimer in full.
The Report has been prepared in good faith on the basis of information, findings and analysis of our specific research activity entitled "Autonomous Valet Parking". All information contained in the Report is provided "as is" and CPC does not guarantee or warrant the accuracy, reliability or completeness of the information in the Report or its usefulness in achieving any particular outcome or purpose. CPC does not owe a duty of care to any third-party readers.
You are responsible for assessing the relevance and accuracy of the content of this publication. You must not rely on the Report as an alternative to seeking appropriate advice. and nothing in the Report shall to any extent substitute for consultation with an appropriately qualified advisor. You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of the Report.
To the fullest extent permitted by law, CPC excludes all conditions, warranties, representations or other terms which may apply to the Report or any content in it, whether expressed or implied. CPC will not be liable to any user for any loss or damage, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, including without limitation loss of or damage to profits, sale business, revenue, use, production, anticipated savings, business opportunity, goodwill, reputation or any indirect or consequential loss or damage. Nothing in the Report excludes or limits CPC's for any liability that cannot be excluded or limited by English law.
Any entity seeking to conduct autonomous vehicle trials will need to develop and publish a safety case specific to their own trials (as specified by the government's Centre for Connected & Autonomous Vehicles (CCAV) Code of Practice for Automated Vehicle Trialling) and gain permission to do so.

FUNDING:

The Autonomous Valet Parking project is part-funded by the Centre for Connected and Autonomous Vehicles (CCAV), delivered in partnership with Innovate UK. It is part of the government's £100 million Intelligent Mobility Fund, supporting the Future of Mobility Grand Challenge.
As a key part of the UK government's modern Industrial Strategy, the Future of Mobility Grand Challenge was announced in 2017 to encourage and support extraordinary innovation in UK engineering and technology, making the UK a world leader within the transport industries.
This includes facilitating profound changes in transport technologies and business models, to make the movement of people, goods and services across the nation greener, safer, easier and more reliable.

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
1	AVP	Entire AVP sub-system	N/A	No data output - No situational awareness	Hardware failure of entire AVP sub-system	No message to system	No input in the AVP system.	Vehicle remains in AD mode. Safety driver made aware of the failure via warning (visual) in order to stop the trial when safe to do so.	x							x	Visual alert given to the driver	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. (Already part of StreetDrone) • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured (Allready part of StreetDrone)
2	Parkopedia	Mission Control	User Input	No output	Failure in app/ failure of comms	Mission not requested	Vehicle does not respond	None									HMI	Alert / notification given to the user	N/A	N/A
3				Wrong output	Incorrect request sent/ failure in app/map not up to date	Mission planning plans wrong mission	Assuming no other failures, wrong mission will be carried out succesfully	Low safety risk, however need to consider whether marshalls will be caught out by unexpected journey, vehicle will leave controlled area etc.		x	x	x	x	x	x	x	Safety Driver identifies that vehicle is carrying the wrong manoeuvres	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
4			Mission Planning	Incorrect but plausible output - error not detectable by system	Computation error etc.	Incorrect route information passed to subsystems	Unsuitable path planned as a result of erroneous input. System unable to identify error	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or steering or brake input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented by StreetDrone calibration of full lock.

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
5				Malfunction - no output or unusable output	Electric failure, coms link failure, Mechanical failure, HMI failure	No predefined uploaded map	AVP system unable to provide a path to the vehicle System transitions from autonomous driving to manual driving	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice	x							x	Visual alarm when AD system disconnected	Highly trained safety driver Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation
6	Parkopedia	Connectivity	3G/4G	Malfunction- no connectivity	Coms link failure, network issues in car park	App cannot connect to the software and feed into the mission control module	The park, summon and stop functions cannot be activated via the app	No safety implications since the mission will not start					x	x	x	x	HMI	Driver takes over		• Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time
7				Cyber attack	Spoofing or man-in-the-middle attacks (privacy and security)	The app and safety engineer cannot control the vehicle	Vehicle reacts differently than expected	Potential collision/accident	x	x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver has to take control of vehicle as quickly as possible, if possible, or turn off the vehicle manually.	• Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time
8				User interface malfunction	Wrong function selected by error etc.	Incorrect command sent to the car via the app	Vehicle reacts differently than expected	Potential collision/accident		x	x	x	x	x	x	x	HMI	Safety Driver takes control		• Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time
9			VO/SLAM	Scale of odometry is wrong	Wrong calibration data used	Incorrect values calculated	Incorrect signal to sensor fusion	Vehicle loses position estimate								x	Detection of signal going above the threshold HMI	Stereo vision with known baseline supports allows accurate estimate of scale.		Avoid the safety drivert from having to intervene
10				Baysian probabilities produce "ghost" solutions	Noisy sensor measurement	Incorrect values calculated	Affect object/freespace proximity detection and tracking Planning, prediction, behaviour affected	Vehicle loses position estimate or gives estimate that is wrong									Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity	Safety Driver able to make manual control inputs to override the autonomous system		Avoid colision

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
11	Uni of Surrey	Localisation	Sensor Fusion	Faulty inputs	Increased uncertainty over position, belief becomes uniform. Effectively the same as kidnapped robot problem. Need to begin localisation from scratch	Incorrect values calculated	Affect object/freespace proximity detection and tracking Planning, prediction, behaviour affected	Vehicle loses position estimate or gives estimate that is wrong									Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity	Safety Driver able to make manual control inputs to override the autonomous system		Avoid colision
12				Incorrect output that is detectable (clearly wrong)	Computational error etc.	Incorrect data sent to navigation or route planning	Error messages provided to subsystems Vehicle unable to maintain autonomous control	Vehicle transitions immediately to manual driving mode. Safety driver made aware of the failure via warning (visual)	x							x	Visual alert given to the driver	Safety Driver able to make manual control inputs to override the autonomous system asking: A. Can I match the surroundings with the map? B. Have I been here before? C. Is it the right sensor data? Are the sensors working correctly? D. Should I "be here"? E. Sensor fusion outcome/delays	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation
13				Incorrect but plausible output - error not detectable by system	Computational error etc.	Incorrect data sent to navigation or route planning	Incorrect path sent to the AVP system.	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x		Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity	Safety Driver able to make manual control inputs to override the autonomous system asking: A. Can I match the surroundings with the map? B. Have I been here before? C. Is it the right sensor data? Are the sensors working correctly? D. Should I "be here"? E. Sensor fusion outcome/delays	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
14				No output or uninterpretable/ clearly incorrect output	Computational error, electrical failure, coms link failure, etc.	No input data sent to navigation or route planning	Subsystems unable to function.No input to the AVP system. Vehicle unable to maintain autonomous control	Vehicle transitions immediately to manual driving mode.Safety driver made aware of the failure via warning (visual)	x							x	visual alert given to the driver	Safety Driver able to make manual control inputs to override the autonomous system asking: A. Can I match the surroundings with the map? B. Have I been here before? C. Is it the right sensor data? Are the sensors working correctly? D. Should I "be here"? E. Sensor fusion outcome/delays	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation
15			Scene Understanding	Malfunction - no output or no interpretable output	Computational error etc.	Erroneous/no message sent to navigation or route planning	Subsystems unable to function.No input to the AVP system. Vehicle unable to maintain autonomous control	Vehicle remains in AD mode. Safety driver made aware of the failure via warning (visual) in order to stop the trial when safe to do so.		x	x	x	x	x	x	x	Visual alert given to the driver HMI	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured
16				Misrepresentation of the environment - error NOT detectable (i.e. plausible output)	Computational error etc.	Erroneous/no message sent to navigation or route planning	Subsystems unable to function.No input to the AVP system. Vehicle unable to maintain autonomous control	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Visual alert given to the driver HMI	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured
17				Misrepresentation of the environment - error detectable (i.e. implausible signal)	Computational error etc.	Erroneous/no message sent to navigation or route planning	Subsystems unable to function.No input to the AVP system. Vehicle unable to maintain autonomous control	Vehicle remains in AD mode. Safety driver made aware of the failure via warning (visual) in order to stop the trial when safe to do so.		x	x	x	x	x	x		Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured. • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
18	Parkopedia			Incorrect but plausible output - error not detectable by system	Computational error etc.	Incorrect data sent to navigation and route planning	Incorrect path would be sent to navigation and route planning	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
19				Incorrect output that is detectable (clearly wrong)	Computational error etc.	Incorrect data sent to navigation and route planning	Error messages provided to AVP system, vehicle unable to maintain autonomous control	Vehicle transitions immediately to manual driving mode. Safety driver made aware of the failure via warning (visual)	x							x	visual alert given to the driver	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation
20				Segmentation fault	Close match to another shape	Hazard not identified	Continue to drive a path towards a hazard	Incorrect and potentially dangerous behaviour			x	x	x		x	x	Safety driver to take control	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation
21				Misrepresentation of the distances - error not detectable	LIDAR/UT/Radar malfunction or failure	Wrong distances computed/ erroneous messages sent to safety cage module and path planning	System does not stop when it should	Accident/incident		x	x	x	x	x	x	x	Safety Driver takes over Alert HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
22		Perception	Proximity Detection	Malfunction - no output or no interpretable output	Computational error etc.	No input to behaviour planning or mission planning	System safe stop fails. Unsuitable path planned	Vehicle remains in AD mode. Safety driver made aware of the failure via warning (visual) in order to stop the trial when safe to do so.								x	visual alert given to the driver HMI	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • Visual alert shall be provided to the Safety Driver
23				Misrepresentation of the environment - error NOT detectable (i.e. plausible output)	Computational error etc.	No input to behaviour planning or mission planning	System safe stop fails. Unsuitable path planned	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x		Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
24				Misrepresentation of the environment - error detectable (i.e. implausible output)	Computational error etc.	No input to behaviour planning or mission planning	System safe stop fails. Unsuitable path planned	Vehicle remains in AD mode. Safety driver made aware of the failure via warning (visual) in order to stop the trial when safe to do so.								x	visual alert given to the driver HMI	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate • Visual alert shall be provided to the Safety Driver
25				No ouput	Power loss, broken connection etc	No input to behaviour planning or mission planning	Autonomous control not possible	Safety driver made aware of the failure via warning	x							x	Safety Driver takes over HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
26	Parkopedia		Prediction	Plausible but incorrect data	Corrupted data, design limitations or system etc	Mission planning and behaviour planning fed incorrect data	Behaviour may be wrong, prediction would have no effect (object well away from path may have no influence anyway)	Vehicle may adopt wrong path/speed. Safety Driver perceives and corrects		x	x	x	x	x	x	x	Safety Driver takes over HMI	Safety Driver able to make manual control inputs to override the autonomous system asking: A. Can I match the surroundings with the map? B. Have I been here before? C. Is it the right sensor data? Are the sensors working correctly? D. Should I "be here"? E. Sensor fusion outcome/delays		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate • Visual alert shall be provided to the Safety Driver
27			Behaviour Planning	Malfunction - no output or no interpretable output	Computational error etc.	Erroneous signal to Path Planner	Erroneous signal to rest of system	Safety Driver made aware of the failure via warning (visual) in order to stop the trial when safe to do so.								x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficcient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
28				Misrepresentation of the environment - error NOT detectable (i.e. plausible output)	Computational error etc.	Erroneous signal to Path Planner	Incorrect path sent	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x		visual alert given to the driver HMI	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate ie when the covariance produced by the localisation method is greater than 3 sigma • Visual alert given to the driver
29				Misrepresentation of the environment - error detectable (i.e. implausible output)	Computational error etc.	Erroneous signal to Path Planner		Safety Driver made aware of the failure via warning (audio/visual) in order to stop the trial when safe to do so.								x	visual alert given to the driver HMI	Safety Driver able to make manual control inputs to override the autonomous system		• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when autonomous control unavailable. • Visual alert given to the driver

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
30				Incorrect waypoints/path	Wrong file selected	Erroneous data to Path Planner	Erroneous commands produced	Wrong areas or fail to reach target Lead to undrivable route or hit obstacles								x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when autonomous control unavailable. • Visual alert given to the driver
31			Camera	Misalignment, improper lighting - erroneous output	Mechanical Failure	Erroneous absolute depth measurement accuracy and depth resolution	Camera self-diagnoses failure and/ or AVP subsystems detect invalid input System transitions from autonomous driving to manual driving	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice	x							x	Visual and audible alarm when AD system disconnected HMI	Highly trained Parkopedia safety driver Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation
32				Misalignment - erroneous output, failure NOT detectable	Mechanical Failure	Erroneous absolute depth measurement accuracy and depth resolution	Unsuitable path planned as a result of erroneous input.	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x		Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
33				Malfunction	Low/very bright light conditions	V/O fails, scene understanding fails	Unsuitable path planned as a result of erroneous input.	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
34				Malfunction	Sudden contrast change	Misinterpretation of object detection	Unsuitable path planned as a result of erroneous input.	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
35				Malfunction - no output or unusable output for Data Recording	Electric failure, coms link failure, Mechanical failure, etc.	No recording of the environment	No effect on AV control Alert when there is a problem with recording data Test to cease, not appropriate to continue without data recording - Safety Driver to take manual control as soon as it is safe to do so	None								x	Alert	N/A	N/A	N/A
36				Malfunction - no output	Electric failure, coms link failure, etc.	No output	System transitions from autonomous driving to manual driving	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice	x							x	Visual and audible alarm when AD system disconnected HMI	Highly trained Parkopedia safety driver Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time Localisation system monitored for error and staleness of information.	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate Heart beat monitor for timelyness and staleness of information

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
37	Parkopedia	Sensor Interface	Wheel Odometry	Miscalibration: over or underestimate of distance travelled	Lose connection to sensor	Wrong output	Wrong localisation output.	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Steering actuation beyond specification shall be prevented
38			DBW Sensors	Erroneous output, fault detectable	Computation error etc.	Erroneous vehicle sensor data passed to subsystems	CAN network and associated sensors/ systems self-diagnose failure	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice	x								Visual and audible alarm when AD system disconnected HMI	Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. any other vehicle means a stop and restart of the test)	• Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single switch when not satisfied with the safety of the current situation • Safety Driver is able to take control of steering and braking without turning switch.
39				Erroneous output, fault NOT detectable	Electric failure, coms link failure, Mechanical failure, etc.	Erroneous vehicle sensor data passed to subsystems	Unsuitable path planned as a result of erroneous input. AVP system unable to identify error	Vehicle remains in AD mode and attempts to adopt improper trajectory or speed		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. any other vehicle means a stop and restart of the test) If this information is used in a future algorithm then a monitor of the timelyness or staleness should be created.	• Detection of driver intervention shall be ensured • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single switch when not satisfied with the safety of the current situation • Safety Driver is able to take control of steering and braking without turning switch. • Steering actuation beyond specification shall be prevented
40				No output	Electric failure, coms link failure, Mechanical failure, etc.	No output	AVP subsystems detect no input from CAN network, and pass error message. System transitions from autonomous driving to manual driving	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice		x	x	x	x	x	x	x	Visual and audible alarm when AD system disconnected HMI	Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. any other vehicle means a stop and restart of the test)	Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single switch when not satisfied with the safety of the current situation • Safety Driver is able to take control of steering and braking without turning switch.

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
41			GPS/IMU	No GPS signal	Covered car park	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin) Safety heart beat check for staleness of the messages.	False input into the navigation	Unecessary stops/swerves, collisions		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. any other vehicle means a stop and restart of the test) If this information is used in a future algorithm then a monitor of the timelyness or staleness should be created.	Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single switch when not satisfied with the safety of the current situation • Safety Driver is able to take control of steering and braking without turning switch.
42				IMU error	Loose on its mounting	Affects sensor fusion	False input into the navigation	Unecessary stops/swerves, collisions		x	x	x	x	x	x	x	Safety Driver identifies that vehicle has deviated from a reasonable trajectory/ velocity HMI	Safety Driver able to make manual control inputs to override the autonomous system	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to react to the alert and gain full control before an incident (e.g. any other vehicle means a stop and restart of the test) If this information is used in a future algorithm then a monitor of the timelyness or staleness should be created.	Safety Driver to be provided with visual alert when the vehicle transitions from AD to MD mode due to a fault • Safety Driver to take manual control where they feel the error margin is insufficient to allow them to detect and correct an error in time • Safety Driver able to transition instantaneously from AD to MD mode with a single switch when not satisfied with the safety of the current situation • Safety Driver is able to take control of steering and braking without turning switch.
43				Misalignment - erroneous output, failure detectable	Mechanical failure	Irregular and sparse nature of the collected point cloud	System transitions from autonomous driving to manual driving	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice	x							x	Visual and audible alarm when AD system disconnected HMI	Highly trained Parkopedia safety driver Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time Localisation system monitored for error and staleness of information.	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate Heart beat monitor for timelyness and staleness of information

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
44			LIDAR	Misalignment - erroneous output, failure NOT detectable	Mechanical failure	Irregular and sparse nature of the collected point cloud	System transitions from autonomous driving to manual driving Lidar safety cage may fail	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice		x	x	x	x	x	x	x	Visual and audible alarm when AD system disconnected HMI	Highly trained Parkopedia safety driver Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time Localisation system monitored for error and staleness of information.	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate Heart beat monitor for timelyness and staleness of information
45				Malfunction - no output	Electric failure, coms link failure, etc.	No output	System transitions from autonomous driving to manual driving Lidar safety cage may fail	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice		x	x	x	x	x	x	x	Visual and audible alarm when AD system disconnected HMI	Highly trained Parkopedia safety driver Safety driver alert at all time and with hands on steering wheel and foot on the pedal ready to take over at any point in time Localisation system monitored for error and staleness of information.	Safety driver to take manual control of the vehicle if they feel there is insufficient safety margin to allow time to detect and correct the deviation (e.g. oncoming vehicle with wide load meaning gap for passing will leave small error margin)	• Detection of driver intervention shall be ensured. • Display of actual operating mode and alarm in HMI when AVP control unavailable shall be ensured • AVP subsystem to have ability to recognise when output trajectory or velocity is clearly inappropriate Heart beat monitor for timelyness and staleness of information
46			Ultrasonic	False detection	Dirt on sensor. Rou	Wrong input to proximity detection	Auto safe stop is activated and vehicle stops.	AD system disconnects and reverts to Manual Driving Mode Safety driver has to take control of vehicle as quickly as possible, with no prior notice	x	x						x	HMI	Reduce false alarm rates so the system is kept switched on.	Choose a sutable surface and path staying away from obstructions.	Reduce false alarms so the system remains useful
47				Missed true detection	Opaque/ clear surfaces	No input to proximity detection	Auto safe stop not activated and possible collision	Could hit a threat					x			x	Safetry driver notices threat and brakes or evades it.	Test to provide assurance that the system works as expected Safety driver will switch to manual mode if the threat is missed.	Safety driver training and practice	Reduce chance of impacts with any threat objects

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
48	Parkopedia	Auto-Safe Stop	Fail Safe Recovery	No output	Total failure or false negative detecting heart beat	No stop message to mission planning	Vehicle keeps going when it should stop due to fault in other module	Test continues with 2 failures remaining latent (if second failure happens elsewhere)	x	x	x	x	x	x	x	x	HMI	Continuous or regular "ok" messages from failsafe recovery to mission planning, issue warning if messages not received	Since this is a to monitor other failures, its failure will not cause a dangerous action itself. "Who shall watch the watchmen themselves"	Reduce chance of impacts with any threat objects
49				Malfunction	False positive	Mission control told to stop vehicle	Vehicle stops unnecessarily	No safety risk	x	x	x	x	x	x	x	x	HMI	Continuous or regular "ok" messages from failsafe recovery to mission planning, issue warning if messages not received	Since this is a to monitor other failures, its failure will not cause a dangersou action itself. "Who shall watch the watchmen themselves"	Reduce chance of impacts with any threat objects
50				Unable to function	Power loss, physical damange, disconnection Sensor failure	No safety message to vehicle interface when hazard presents	Fault remains latent	Safety curtain doesn't work where needed Possible collision					x			x	Safetry driver notices threat and brakes or evades it.	Send "safe" messages to vehicle itnerface after continuously or at regular time period. If vehicle interface doesn't receive it, notify Safety Driver or fault		Reduce false alarms so the system remains useful
51	Parkopedia	Control	Path Following	False command - too big	Integral windup	Very high throttle request	High throttle request will be passed to SD	Very high acceleration or braking	x		x					x	Safety driver can easily detect sudden, unexpected changes	Filtering techniques Reset PID gain when stopped Set integral limit Limit torque command		Maintain safe autonomous control
52				False command - sudden change (eg.noise)	Electrical fault	Wrong sub system output	Wrong commands issued to SD	High acceleration or braking	x	x	x	x	x	x	x	x	With training and experience the safety driver can detect subtle differences and small deviations from the intended path	Filtering techniques Reset PID gain when stopped Set integral limit Limit torque command		Maintain safe autonomous control
53				Slow path degradation	Poor localisation	Controller not able to achieve desired trajectory	Wrong commands issued to SD	Collision		x	x	x	x	x	x	x	Monitoring system	Safety driver takes control Path following deviation check		Maintain safe autonomous control

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
54				Path provided exceed capabilities of vehicle (eg. turning circle too tight)	Path planning failure	Controller not able to achieve desired trajectory	Wrong path taken	Loss of vehicle control	x	x	x	x				x	Non applicable to detection method	Kinematic limit check in Autoware StreetDrone steering change rate limit		• Safety Driver to take manual control where they feel the turning circle is too tight
55			Vehicle Interface	Cannnot send CAN message/command to control the vehicle	loose connection	Safety cage and/or Path following	Possible collison	Vehicle cannot be stopped	x				x	x	x	x	Handshake message between PC PX2 and the vehicle	The StreetDrone will come out of autonomous mode and notify the driver with the red flashing light and an audible warning.		StreetDrone will alert driver audibly and visually when it returns control to the driver
56	Parkopedia	Global Services	Vehicle tf State Publisher	No output	No input	tf state not shown	Poses within the system will be wrong	System will not run					x	x	x		HMI	StreetDrone will not go into autonomous mode		StreetDrone will alert driver audibly and visually when it refuses autonomous mode
57				Wrong input	Malfunction/error/wrong input	Erroneous tf state shown	Navigation and Motion control	Incorrect path and location		x	x	x	x	x	x	x	Monitoring system	Safety driver to intervene		• Safety Driver to take manual control
58			Map Server	Malfunction - not able to accept or record inputs	Disk failure	No maps available to vehicle systems	Not run	System will not run									HMI	StreetDrone will not go into autonomous mode	The test will not run without a map	StreetDrone will alert driver audibly and visually when it refuses autonomous mode
59				Malfunction - not able to show outputs	Blank map	Maps available to vehicle systems but are of no use	Rviz cannot display	Incorrect path and location									HMI	Safety driver to intervene	The test will not run without a map	StreetDrone will alert driver audibly and visually when it refuses autonomous mode
60				No output	Malfunction	Maps cannot be downloaded	No route planning	System will not run									HMI	StreetDrone will not go into autonomous mode	The test will not run without a map	StreetDrone will alert driver audibly and visually when it refuses autonomous mode
61				Corrupted output indicated Emergency Braking required	Computational error etc.	Signal requiring Autonomous Emergency Braking sent to dbw system	Emergency braking request sent to braking system (Current assumption is that AEB will be possible) Vehicle performs emergency stop	Vehicle still in AD mode, brakes rapidly to a standstill Risk of incident if another vehicle is following closely behind or if vehicle is pulling out of a parking spot		x							Autonomous Emergency Braking will be obvious to Safety Driver	We won't be running when other vehicles are around. Highly trained safety driver able to override braking by switching to manual mode (black rotating switch to the right)	We won't be running when other vehicles are around. Ensure safety driver wareing seatbelt.	• Detection of driver intervention shall be ensured. • Safety Driver to prevent vehicle pulling out at a parking spot, where the gap would be insufficient for Safety Driver or other road users to respond in the event of undesired behaviour by the AVP vehicle • Safety driver to take manual control if a following vehicle is close enough to cause a significant risk of collision in the event of heavy braking by the AVP vehicle • Safety Driver able to transition instantaneously from AD to MD mode with a single button press or driving input when not satisfied with the safety of the current situation • Support vehicle to followAVP vehicle at a safe distance

System Description				Failure Mode	Possible Failure Causes	Failure Effect/Safety Impact			Potential Outcome								Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal
Ref	Owner	Sub-System	Sub-sub-system			Local	AVP System	Operational Situation with harm Safety Impact	Loss of AD Control	Unintended braking	Unintended Accel	Unintended Steering	Lacking of Braking	Lack of Accel	Lack of Steering	Driver take control				
62			Log File	Malfunction - not able to accept or record inputs	Electric failure, coms link failure, Mechanical failure, etc.	No recording of the data	No effect on AV control	None									Use HMI	N/A	No additional risk, but stop test if it is noted.	N/A