Connected Places Catapult

Hazard Analysis and Risk Assessment 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	12/12/2019

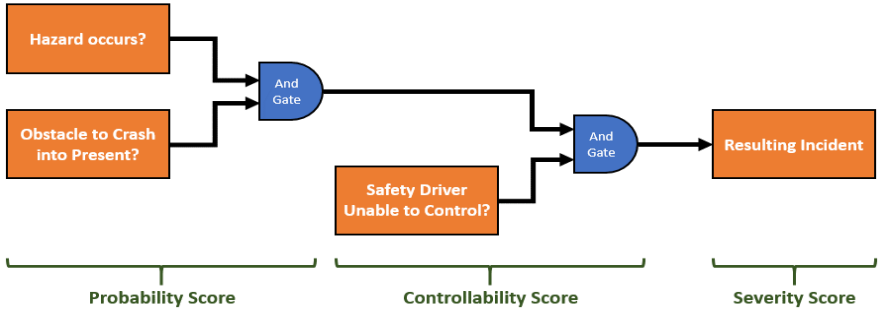
Description:

This document is a Hazard Analysis and Risk Assessment from the perspective of System Safety, as opposed to Operational Safety (i.e. it looks at faults within the system and how the system would respond if presented with a situation that is outside its limitations, but does not look at operational procedures for how tests are carried out; this is covered in the Risk Assessment & Method Statement for that particular test).

The possible vehicle level faults identified in the Failure Modes and Effects Analysis (FMEA) were used to generate hazards here; other hazards were identified via brainstorming, prior experience and knowledge of the system limitations.

Three separate risk assessments are provided for the same hazards, depending on whether the vehicle is deployed on a private track, in a secure area of a car park, or as part of a demonstration involving travelling through non-secure areas of the car park.

The Scoring for Probability (P) is based on both the probability of the hazard in column B occurring AND the probability that other traffic and obstacles around the vehicle poses a threat at the moment that the hazard is triggered such that it is reasonably possible for an incident to result. This is multiplied by the score for severity (S) of the resulting incident, and the controllability (C) a low score indicating that the driver has a good chance of being able to prevent or mitigate the incident, to obtain an overall Risk Score (R). A schematic of the approach is shown below, and the scoring system is detailed on the Risk Scoring tab.



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.

Project:	AVP		Activity/ task:	Car Park Testing		Company:	CPC		Created by:	M. Hassanaly		Reviewer:	Adrian Bedford			
Hazard Analysis					Risk Assessment				Risk Mitigation							
Hazard ID no.	Hazard Description	Existing Mitigation Measures	Hazard Type (Functional Safety, SOTIF, Operational etc.)	Hazard Target (Employees/ public/ both)	P Probability	S Severity	C Controllability	R Risk Level	Additional Mitigation Measures	P Probability	S Severity	C Controllability	R Risk Level	Rationale/ Notes	Review Comments	Accept Risk? (y/n)	Last Change Version
C1	**Sudden Loss of Autonomous Control**	* Safety driver ready and able to take control * Audible alert to inform driver of need to take over * Prior verification on test track to establish reasonable robustness prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of handover) * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF (e.g. sensor blinded by sun)	Both	3	4	2	**24**	* Driver to take control	3	4	2	**24**	*Probability low as even though handovers are likely to occur, there is unlikely to be anything present for the vehicle to collide with * Controllability if kept low because of alert given at time of loss of control, meaning safety driver gets feedback before vehicle goes off line, also deviation likely to be low, unless it happens on tight bend			**1.0**
C2	**Driver asked to take over, no immediate loss of autonomous control**	* Safety driver ready and able to take control * Audible alert to inform driver of need to take over * Prior verification on test track to establish reasonable robustness Prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of handover) * Vehicle able to maintain autonomous control for immediate driving task, giving safety driver sufficient time to take over - this hazard can only occur in the case of failure where there is redundancy. Only becomes problem if other layer of protection also fails * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety	Both	3	4	1	**12**	* Driver to take control pre-emptively	3	4	1	**12**	*Although loss of autonomous control is reasonably likely to happen at some point, probability is only a 3 as a hazardous traffic scenario (e.g. oncoming vehicle, nearby obstacle etc.) as well as the failure would be needed for an incident to occur			**1.0**
C3	**Incorrect steering**	* Safety driver ready and able to take control * Prior verification on test track to establish reasonable robustness Prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of error) * Safety driver to take over if other vehicles are behaving in an unusual or illegal manner * Control inputs limited to maximum values by MicroAutoBox * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF (e.g. sensor blinded by sun)	Both	3	4	2	**24**	* Driver to take control	3	4	2	**24**	* Hazard includes too much or too little steering - effect similar * Probability also takes into account that hazard would only result in accident if an obstacle is present			**1.0**
C4	**Inappropriate acceleration**	* Safety driver ready and able to take control * Prior verification on test track to establish reasonable robustness Prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of error) * Safety driver to take over if other vehicles are behaving in an unusual or illegal manner * Control inputs limited to maximum values by MicroAutoBox * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF (e.g. sensor blinded by sun)	Both	3	4	2	**24**	* Driver to take control	3	4	1	**12**				**1.0**
C5	**Inappropriate lack of acceleration**	* Safety driver ready and able to take control * Prior verification on test track to establish reasonable robustness Prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of error) * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF (e.g. sensor blinded by sun)	Both	2	2	1	**4**	* Driver to take control	2	2	1	**4**	* Risk of rear-ending scenario materialising is very small given nature of testing - could only happen if vehicle is being used outside limits intended, or someone acts inappropriately in test area			**1.0**
C6	**Inappropriate braking**	* Safety driver ready and able to take control * Prior verification on test track to establish reasonable robustness Prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of error) * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF (e.g. sensor blinded by sun)	Both	2	2	1	**4**	* Driver to take control	2	2	1	**4**	* Similar collision type to lack of acceleration, but higher probability as rapid deceleration could happen at any time * Injuries due to rear-ending accident unlikely to be severe			**1.0**

Project:	AVP		Activity/ task:	Car Park Testing		Company:	CPC		Created by:	M. Hassanaly		Reviewer:	Adrian Bedford			
Hazard Analysis					Risk Assessment				Risk Mitigation							
Hazard ID no.	Hazard Description	Existing Mitigation Measures	Hazard Type (Functional Safety, SOTIF, Operational etc.)	Hazard Target (Employees/ public/ both)	P Probability	S Severity	C Controllability	R Risk Level	Additional Mitigation Measures	P Probability	S Severity	C Controllability	R Risk Level	Rationale/ Notes	Review Comments	Accept Risk? (y/n)	Last Change Version
C7	**Inappropriate lack of braking**	* Safety driver ready and able to take control * Prior verification on test track to establish reasonable robustness Prior to road testing * Safety driver to take over pre-emptively if scenario outside ODD is perceived (possible cause of error) * Safety driver to be aware of range limits of sensors/ processing and brake for vehicle if scenario is outside system capability (e.g. may not be able to react to stationary objects early enough when travelling at high speed) * Safety driver given instructions not to wait longer than is safe to see if system reacts (to avoid temptation/ pressure to leave override until last moment to find out if the vehicle would have intervened in the end) * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF (e.g. sensor blinded by sun)	Both	3	4	2	24	Safety driver takes appropriate action in the same way as driving manually	3	4	2	24				1.0
C8	**Failure of Low-Level Control System to limit control inputs to reasonable levels (e.g. steering torque too high for driver to fight against)**	* Safety driver able to disconnect system so AVP vehicle effectively becomes a manual vehicle * Driver to be given waring if failure is detected in Low Level Controller (CONFIRM IF TRUE!!!) - incident would therefore only occur if fault is undetected or if system makes excessive control input after warning but before driver can take control * Base vehicle has physically connected braking and steering controls to production robustness levels * Steering and braking also limited by production vehicle actuators - whilst thresholds may not be perfectly calibrated with MicroAutoBox, they can be relied upon to provide a reasonable backup, as ASIL rated components * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety	Both	2	4	4	32	Any small torque on the steering will cause the StreetDrone to return to manual mode.	1	4	4	16	Need to confirm whether vehicle has an ability to limit maximum steering, acceleration and braking inputs to reasonable values (to reduce likelihood of uncontrollable manoeuvre if system makes an error). StreetDrone may already have this in place, hopefully with test data to back it up	Any steering input torque from driver will imediately bring SD out of autonomous mode.		1.0
C9	**Another car park user (e.g. pedestrian, car, cyclist etc.) performs a dangerous or illegal manoeuvre in vicinity of AVP vehicle**	* Safety driver to intervene if other road users are behaving in a dangerous or illegal manner * Safety driver to intervene if needed to prevent an accident * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Operational	Both	2	4	3	24	Safety driver takes appropriate action in the same way as driving manually	2	4	3	24		We won't run if any other users are nearby.		1.0
C10	**Safety driver unable to monitor vehicle properly (e.g. fatigue)**	* Safety driver limited to half an hour without a break * Engineer present on test site and able to monitor safety driver attentiveness and take care of tasks that could distract safety driver * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access * Safety driver to hold a current UK driving license and be fit to drive	Operational	Both	1	4	4	16	Any members of the test team can call for a break, not just the driver.	1	4	4	16	Controllability reflects engineer in car having ability to monitor safety driver and take action. Probability is based on driver qualifications and required breaks.			1.0
C11	**Vehicle required to react to scenario that is outside the ODD (Operational Design Domain)**	* Safety driver to be familiar with ODD * Safety driver to take manual control pre-emptively if event outside ODD occurs (before system is exposed to hazard if possible) * Testing will not commence if weather is unsuitable * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety SOTIF	Both	3	4	2	24	* Safety driver to take control pre-emptively if there is insufficient space to correct steering errors (mitigates against events outside ODD causing dangerous steering inputs, permutation most likely to cause harm) * Other personnel on site familiar with ODD and able to provide backup observation of hazards/ events outside ODD when not engaged in other tasks (able to mitigate some, but not all, hazards)	3	4	1	12	Events or conditions out of ODD almost certain to be encountered multiple times. However, probability is lower as this is unlikely to occur in a situation where it could cause an accident			1.0
C12	**Failure of Mechanisms to Deactivate the Autonomous System**	* Multiple methods available to deactivate system * Speed not to exceed 5mph * RAMS to include procedures to ensure test environment is well managed with no unauthorised access	Functional Safety	Both	1	4	4	16	Verification testing (AVP or Streetdrone) to confirm robustness of ability to cancel autonomous control	1	4	4	16	* E-stop button etc. expected to have high level of robustness due to simplicity of design and well established approaches. * Controllability given high score (i.e. difficult to control), but not maximum, as driver will still be able to immediately overcome system due to physical connection of brakes and steering and the StreetDrone reverting to manual control.			1.0

Probability	
1	Very unlikely
2	Unlikely
3	Possible
4	Likely
5	Very Likely

Severity	
1	Minor injury – No first aid treatment required
2	Minor injury – Requires First Aid Treatment
3	Injury - requires GP treatment or Hospital attendance
4	Major Injury
5	Fatality

Probability considers the likelihood of 2 factors both required for an incident; how likely is the hazard to occur, and how likely is it that the surrounding environment will have the right combination of features to cause this hazard to result in an actual incident (e.g. oncoming traffic, pedestrian near vehicle etc.)

Controllability	
1	Very easily controllable
2	Easily controllable
3	Moderately controllable
4	Difficult to control
5	Not controllable

Overall Risk Scoring	
R >= 30	Unacceptable Risk - must be reduced before activity can begin
40 > R >= 30	Tolerable Risk (upper) - must be reduced if reasonably practicable within project resources
30 > R >= 18	Tolerable Risk (lower) - should be mitigated if possible to achieve with minimal additional burden
R < 18	Acceptable Risk - no further mitigation necessary
The overall Risk Level is scored by multiplying together the Probability, severity and (difficulty of) Controllability	

Controllability could be regarded as a measure of how difficult the scenario is for the safety driver to correct, i.e. the lower the score, the easier it is to control (the numbering was set out this was to allow multiplication to generate the Overall Risk Score

In line with Health And Safety Executive (HSE) Guidance, risks are rated as Unacceptable, Tolerable or Acceptable. However, the HSE approach advises that where risks are Tolerable, they should be demonstrated to be As Low As Reasonably Practicable (ALARP), assessed with techniques such as comparing the cost of fatalities to the cost per life saved of mitigation measures. For an R&D project, such an analysis isn't feasible, so it was deemed that a better approach to judging whether 'reasonably practicable' steps have been taken was to separate Tolerable risks into an Upper (amber) and Lower (yellow) band, with a higher burden of mitigation in the upper band.