Safety Assessment for Autonomous Systems’ Perception Capabilities

J F Molloy*a, J A McDermid*a

aDepartment of Computer Science, Deramore Lane, University of York, Heslington, York, YO10 5GH, Yorkshire, UK

Abstract

Autonomous Systems (AS) are increasingly proposed, or used, in Safety Critical (SC) applications. Many such systems make use of sophisticated sensor suites and processing to provide scene understanding which informs the AS’ decision-making. The sensor processing typically makes use of Machine Learning (ML) and has to work in challenging environments, further the ML-algorithms have known limitations, e.g., the possibility of false-negatives or false-positives in object classification. The well-established safety-analysis methods developed for conventional SC systems are not well-matched to AS, ML, or the sensing systems used by AS. This paper proposes an adaptation of well-established safety-analysis methods to address the specifics of perception-systems for AS, including addressing environmental effects and the potential failure-modes of ML, and provides a rationale for choosing particular sets of guidewords, or prompts, for safety-analysis. It goes on to show how the results of the analysis can be used to inform the design and verification of the AS and illustrates the new method by presenting a partial analysis of a road vehicle. Illustrations in the paper are primarily based on optical sensing, however the paper discusses the applicability of the method to other sensing modalities and its role in a wider safety process addressing the overall capabilities of AS.

Keywords: Autonomous Systems, Perception Systems, HAZOP, Machine Learning, ALKS

*Corresponding Author
Email address: john.molloy@york.ac.uk (J F Molloy)
1. Introduction

Autonomous Systems (AS) depend on complex perception subsystems to produce and continuously update a “world model” on which to base decisions, e.g. to choose a trajectory. These subsystems are typically multi-modal, i.e. use multiple sensor types, and often employ Machine Learning (ML) for processing data from optical sensors, especially cameras.

The “world models” produced by the perception systems are crucial to overall system safety. The decision-making element of the system has to treat the model as “ground truth” – it has no alternative source against which to check the model – so a “correct” decision-making algorithm may give rise to unsafe behaviour if the “world model” is sufficiently misleading, e.g. fails to identify an object in the path of a mobile system, such as a road vehicle. Of course, decision-making algorithms themselves can be inappropriate, but our focus here is on unsafe behaviour that can be induced by inadequacies or limitations in the perception subsystem of Autonomous Vehicle (AV), especially where behaviour relies, at least in part, on ML.

The paper presents an approach to hazard and safety analysis of ML-based perception subsystems, as part of a wider programme to adapt classical safety engineering methods for use on AS operating in complex environments. Specifically, it proposes an adaptation of well-established safety analysis methods to address the specifics of perception systems for AS, including addressing environmental effects and the potential failure modes of both sensors and ML. It focuses on a single domain, AV’s and on camera-based sensing because of their importance and the availability of data, including on critical malfunctions. However, we start by explaining the level of dependency on sensing and present a more extensive rationale for choosing to develop our method based on analysis of camera-based systems.

1.1. Importance of Sensing Systems

Sophisticated sensor systems are now an integral part of consumer vehicles, and 92% of new cars sold in the US include some Advanced Driver Assistance Systems (ADAS) features, which are defined as partial automation (Level 2 autonomy) under Society of Automotive Engineers (SAE) J3016 [1, 2]. ADAS features are now widespread, and the first Level 3 features have recently been approved for use in commercial vehicles, e.g. both Honda and Mercedes have received regulatory approval for Advanced Lane Keeping System (ALKS) [3]. Typically capabilities at the higher levels of autonomy are
referred to as Automated Driving Systems (ADS).

Levels of autonomy are defined by the SAE in J3016 depending on the degree of assistance provided and the extent of driver/operator oversight required, see Figure 1. Levels 0-2 require constant driver supervision and the driver remains in control of the vehicle, while Levels 3 and above permit the drivers to engage in activities other than the Dynamic Driving Task (DDT).

![Levels of Driving Automation](image)

Figure 1: Overview of SAE J3016 adapted from[1]

The perception system is clearly Safety Critical (SC) at Level 3 as, for example, failure to correctly identify lane markings could lead an ALKS-equipped vehicle to stray from the current lane.

A recent example shows a Peugeot 508 running an ADAS (see Figure 2) leaving the motorway and into the verge, while the driver in the rear seat boasts that a water bottle (used to simulate manually applied steering torque) is driving the car [4].

Even for Level 2 systems, errors in the “world model” can lead to unsafe behaviour. For example, if an Automatic Emergency Breaking (AEB) system initiates braking when there is no obstacle in its path (perhaps due to a false positive from the ML image processing software) this could give rise to a
tail-end collision. With Level 2 systems, drivers are meant to be attentive and able to deal with such situations but, at a minimum, such a malfunction would increase risk. In our HAZOP method, we do not use the SAE Level as a factor when considering potential malfunctions of the sensing system, but we illustrate the method using ALKS, see Section 3, where the criticality of
misperception is unequivocal.

Manufacturers have generally taken the approach that vehicles should be self-sufficient in implementing features such as ALKS, rather than being dependent on the infrastructure, to for example, communicate the state of traffic lights. Vehicles do this using on-board exteroceptive sensors systems including cameras, radar & lidar to produce “world models”, in a given Operation Design Domain (ODD). These sensors are used in conjunction with ML algorithms to detect, understand, and interpret the external environment and its context including: the drivable area, other road users, static obstacles, road signals, e.g. speed limits, traffic lights, etc.

It is difficult, if not impossible, to use a single sensor or data source to accurately interpret complex scenarios such as those encountered by AV’s and to report on all features of interest. Hence, manufactures typically use complementary sets of sensors, fusing their outputs in an attempt to mitigate individual sensor weaknesses [5].

So, while the ideal perception suite remains an open area of consideration [6], significant benefits are derived from the use of a diverse sensor suite, operating at heterogeneous electromagnetic wavelengths and fusing their outputs: a typical sensor suite now contains multiple Red, Green, Blue (RGB) cameras, lidar and radar sets, and additional systems such as thermal imaging, and ultrasound may also be included. Despite the benefits of overcoming the limitations of individual sensing modalities, there are drawbacks in terms of financial cost and computational resources.

1.2. Hazard and Safety Analysis

Classical safety processes start by identifying hazards, i.e., undesirable situations that pose risk to life, then determine potential causes of the hazards and estimate the risk associated with the hazards. Typically, risk is a combination of the likelihood of the hazard occurring and the severity of the harm arising from the hazard, although the detailed computations vary from domain to domain, e.g. in the automotive domain controllability of the hazard is normally considered.

In the context of this paper, it is assumed that vehicle level hazard analysis has been carried out, incorporating process such as Safety Assurance of Autonomous Systems in Complex Environments (SACE) and that the concerns in analysing sensing systems are in identifying potential causes of known hazards we will refer to this as Safety Assurance of Understanding in Autonomous Systems (SAUS) [7]. As indicated above, hazards can be
caused by errors in the “world model” produced by the sensing system. We introduce the concept of a Hazardous Internal System State (HISS) which arises when the system’s model of the environment or its own state differs significantly from the real world (ground truth). The term “significantly” is used as all models will lag the real-world due to the time taken for signals to reach the sensor (or round-trip delays for active sensors) and the length of time for the software to process the sensor data. The models will also necessarily be approximate as sensors have finite resolution, and their precision is also a function of target range.

The system model must also consider its own state – for example, whether or not brake actuators are working correctly, as this can also affect safety. Our focus in this paper is mainly on exteroception, but a brief discussion is given of interoception, especially the ability to monitor the state of the sensing system itself.

Identifying hazards and potential hazard causes is a creative process, and many hazard and safety analysis methods use guidewords to prompt the analysts to consider ways in which deviations from design intent might arise and contribute to hazards. To our knowledge, there are no established hazard and safety analysis methods focused on completed ML-driven perception capabilities. Though camera performance for computer-vision has been previously considered [8] showing the methods flexibility, and we believe it is both practical and valuable to adapt existing methods for this purpose.

1.3. Scope and Structure of the Paper

For simplicity, and because of the importance of optical perception for human drivers, the paper focuses on camera-based elements of sensing systems from the point of view of identifying potential causes of hazards. Further, we use the term AVs throughout, although we recognise that there are currently no commercially deployed systems at SAE Levels 4 & 5, and Level 3 systems are just entering the market (although there are highly autonomous systems in other domains). We believe this is reasonable, as it is our intent that the method we propose would be valid and useful, for all of the SAE Levels.

The rest of the paper is structured as follows. Section 2 presents background on the capabilities and limitations of sensing systems with a focus on cameras and the ML algorithms used for processing the images. It also briefly summarises the principles of classical safety analysis and their role in achieving and assuring system safety. Section 3 sets out our proposed
an analysis method, which is an adaptation of classical Hazard and Operability Studies (HAZOP) [9] and presents examples to illustrate the guidewords chosen for the method. Section 4 illustrates the use of the adapted HAZOP method on an ALKS capability, making reasonable assumptions about the implementation; treating both camera and radar-based capabilities, to show the generality of the HAZOP method. This is followed by a discussion of limitations of the approach and the broadening of the method to deal with wider multi-modal sensing systems, and the role of the method in an overall safety process for AS in Section 5. Conclusions are presented in Section 6.

2. Background

This section first considers the capabilities and limitations of camera-based perception systems, including the ML algorithms for processing the images, in the context of AVs. This is followed by an introduction to hazard and safety analysis processes, and an assessment of their capabilities and limitations for assessing AS, in particular for the safety analysis of sensing systems.

2.1. Capabilities and Limitations of Camera-based Perception Systems

RGB cameras are to a large extent the principal sensing channel in AS and have become ubiquitous in AVs. Cameras provide reasonably precise and feature rich data, which is important in the context of a road environment designed to be navigated largely by human vision, while also being relatively cheap and robust sensors.

Cameras systems however suffer a number of limitations. While depth data may be extracted from both stereo and monocular images it is generally computationally expensive, of limited accuracy, and best suited to shorter ranges. Additionally RGB cameras typically perform poorly in low light conditions and, in contrast to human vision, struggle with High Dynamic Range (HDR) scenarios. These weaknesses are typically addressed through multiple exposures and onboard image processing i.e. HDR imaging, and through the use of complementary sensing modalities i.e. lidar and radar.

Moreover, visual sensor technology is at an extremely mature stage and total failure of the sensor is now rather rare with significant mitigations in place during production to avoid this. In contrast intermittent failure or processing errors are not as well controlled, and analogue side failures are difficult to identify using automatic software processing at run-time [10].
Until recently, the outputs of such sensors have been interpreted by operators to enhance human situational awareness e.g. by increasing visible range or detecting low observable objects. Operators (e.g. vehicle drivers) can often compensate for such errors, intermittent failures, and degradation of the sensor suite by means of training, experience, ability to adjust the sensor set or independent assessment of the scenario. Though interpretation failures still occur, infamously the Pitot tubes on Flight A447 [11] and the radar set on USS Fitzgerald (DDG-62) [12, 13] it is important to note, that up to SAE Level 2 sensing systems are an aid to the drivers who remain in control of the vehicle and must supervise its behaviour, while receiving far less training than the operators in the above two cases.

The advent of Convolutional Neural Network (CNN) on cheap, powerful computers, e.g. Graphics Processing Unit (GPU), has enabled modern implementations of AVs. CNN’s can provide a “decent level of accuracy”, and fast processing speeds for many AV tasks including perception in comparison with traditional methods[5].

Hence has been a sustained increase in use of CNNs for image processing tasks in Autonomous Systems (AS) in the last decade. For example, traffic sign recognition with multi-scale CNNs is one of the most mature and widely adopted techniques [14]. Whilst it is difficult to get concrete data from manufacturers, research papers produced by manufacturers and their Tier 1 suppliers point to the growing use of such technology, e.g. for pedestrian detection.

Some AVs also use ML for other functions, e.g. mapping and decision making, but these applications are outside the scope of this paper.

However, the deployment of CNNs presents serious safety challenges as there is a significant lack of human interpretability or intuition for the functioning of these Neural Network (NN) [15], even in the case of visual imagery. This is compounded by the variance in perception suite performance, where it simultaneously out- and under-performs human capability leading to a cognition gap [16, 17] making it difficult for drivers/operators to predict the vehicle’s (mis-) behaviour with respect to unseen or unforeseen scenarios and edge-cases [18]. Where CNNs are used for object detection and classification, e.g. distinguishing pedestrians from street furniture, they are prone to false positives, e.g. classifying an object as a pedestrian which isn’t, and false negatives. A false negative which means that an area of a scene is interpreted as a drivable area where, in fact, there is an obstacle (whether a human or static) is clearly hazardous – a HISS. More subtly, object classification can be
used to shape the AVs prediction of object trajectories, so misclassification can lead to incorrect prediction of the future position of an object – this was one of the factors in the National Transportation Safety Board (NTSB)’s investigation of the Uber Tempe fatality [19].

This suggests that the average or even trained drivers may not know whether or why the the system component, either CNN or sensor, is failing or degraded. Moreover with Over-the-Air (OTA) updates to core system functionality, the behaviour of the vehicle (or factors affecting the vehicle) may change overnight. Thus human oversight is hampered by significant configuration variability, which was a contributing factor to the fatal USS McCain (DDG-56) (2017) incident [20, 13].

Hence, it cannot be reasonable nor ethical to expect the a human driver to provide supervisory behaviour for ALKS – and it could be said to be in conflict with the very definition of the higher SAE levels; in the US National Highway Traffic Safety Administration (NHTSA) preliminary statement of policy concerning automated vehicles (in 2013) the driver cannot be relied upon to provide control methods during operation of a fully automated vehicle [21].

In the UK, work by the Law Commission is seeking to identify regulatory changes that would give clarity relating to driver and manufacturer responsibility for AVs at Level 3 and above, with the onus on vehicle manufacturers to ensure safety. In turn, this means that there is a need for hazard and safety analysis of perception systems – but before we consider that, we first outline some of the uses of ML in perception systems for AV and the problems that can arise.

We will use the term Date Driven Model (DDM) as a general description for the results of ML, as the issues are not particular to CNNs [22]. It is difficult (if not impossible) to show deterministically that the outputs of DDMs will be correct. While DDMs often produce a measure of confidence, e.g. 93% certain that an object is a pedestrian, they usually do not provide an explicit consideration of uncertainty or provide a measure that is not statistically robust. However, even if the algorithms do not provide specific measures, some degree of uncertainty must be ascribed to the DDMs in the cases where they are used for safety critical functions [23].

In general, three common sources of uncertainty should be considered for DDMs: the model fit, the data quality, and the scope compliance [23]. Model fit is the inherent uncertainty in the DDM, Data quality is the DDM’s uncertainty as a result of it’s application to input data obtained in sub-
optimal conditions (and greatly affect by sensor performance), and scope compliance is where the model may be applied to the scenarios outside of the intended use [24].

More broadly, DDMs often fail to generalise outside their immediate domain of training data distribution and the algorithms are often over-confident on inputs that are rare in the training data set [25] Thus the systems are vulnerable to these shifts but humans can’t provide oversight – further they should not be expected to do so for higher SAE Levels.

Finally, functionality provided by ML, or the expected outcome, is not explicitly specified and implemented by software developers, instead the DDMs are learnt, and that is a challenge for classical approaches to safety engineering.

2.2. Capabilities and Limitations of Classical Safety Engineering Methods

As mentioned above, classical safety engineering methods and processes are based around the notion of hazards and the risk (likelihood and severity) associated with each hazard. Effective safety processes identify potential causes of hazards early in the system development lifecycle, and identify Derived Safety Requirement (DSR) to reduce risk. These DSRs can be intended to reduce the likelihood of the hazard arising, e.g. by using redundant sensing, or by mitigating the consequences, e.g. by using airbags to reduce the effects of collisions. We refer to this as ensuring safety.

Safety engineering also has a role in assuring safety, with safety analysis methods used to provide evidence that DSRs have been met, in some cases. They often have a role in showing that hazard-related risk has been reduced to an acceptable level. In many industries, including automotive, it is common to produce a safety or assurance case to support demonstration that a system is safe to operate, and this can be mandated by standards, e.g. ISO 26262 [26] in automotive. Our focus in this paper is on ensuring safety, and the role of safety engineering methods in understanding potential causes of hazards and thus identifying DSRs.

Safety engineering processes start at whole system level – in this case an AV – and seek to identify potential hazards. Hazards can generally arise from failure to control hazardous substances, e.g. asphyxiating gases, or through inadequate control of energy. In the case of AVs the key issue is control of vehicle kinetic energy – although we are particularly interested here in how perception system inadequacies can contribute to such hazards.
At their simplest, whole system level analysis might ask “what if” questions with some simple prompts related to function provision:

- **Omission** – function not provided when intended, e.g. brake not applied when vehicle is stationary (and on a slope so it will start to roll);

- **Commission** – function provided when not intended, e.g. application of AEB when there is no obstacle in front of the vehicle;

- **Incorrect** – function provided wrongly, e.g. steering angle insufficient to proceed around a bend and stay on the road.

Of these examples, Commission is most likely to lead to a DSR which flows down to the perception system, in terms of the (acceptable) likelihood of false positives in detecting objects in the vehicle’s path.

As the design evolves, further analysis will be carried out to identify potential causes of hazards (and perhaps new hazards which become apparent as the system design matures). The chemical process industry developed HAZOP [9] as a method for analysing flows through pipework using guidewords, e.g. *more*, *less*, to flow attributes, e.g. volume, pressure. HAZOP has been adopted successfully for computer-based systems, reflecting the fact that it is common to model system architecture in terms of data flows. However, it has been simplified to reflect the absence of attributes of the flow of interest other than the existence/value of data, and the more limited set of potential failure modes. One such example method is Software Hazard Analysis and Resolution in Design (SHARD), developed in the 1990s [27].

The focus on failures will continue through the design and development process, ultimately arriving at detailed Failure Modes and Effects Analyses (FMEA) on system components, e.g. sensors (see [28] for a survey of FMEA methods). There are likely to be further DSRs at this level, e.g. to detect and respond to individual hardware failure modes, but methods such as FMEA also have a role in assurance, e.g. showing that failure behaviour is no worse than assumed in earlier, design-stage, analyses.

The long-established methods, such as FMEA and HAZOP, continue to be applied, but there are more modern methods which build on systems theory, viewing ensuring safety as a control problem, for example Leveson’s System-Theoretic Process Analysis (STPA) [29]. STPA is becoming increasingly widely used in automotive, but our experience has been that there are limitations in applying it for shared control, such as Level 2 autonomy, but it is possible to enhance STPA models to deal with these challenges [30].
More fundamentally, the failure-focused methods do not explicitly deal with assessing whether or not the intended functions are safe. There are emerging practices and standards for the Safety of the Intended Function (SOTIF) [31] but it remains unclear whether or not these methods are rich enough to deal with the growing complexity of systems.

Another fundamental limitation of existing methods and standards is that they do not deal with the specific properties of perception systems, including their failure modes. Associated work has developed a processes for Safety Assurance of Autonomous Systems in Complex Environments (SACE) [7] and Assurance of Machine Learning for Autonomous System (AMLAS) [32]. These are relevant for assuring the safety of the AS as a whole and ML elements of perception systems, although not the perception system or the sensors themselves. Moreover, AMLAS starts with identifying the context of use and safety requirements (DSRs) for the ML elements of the system. However, we are not aware of any analysis methods that help to identify these DSRs; this is the “gap” that we aim to fill in this paper.

3. Proposed Method

| Guideword          | Meaning                                      |
|--------------------|----------------------------------------------|
| No or Not          | Complete negation of the design intent       |
| More               | Quantitative increase                        |
| Less               | Quantitative decrease                        |
| As well as         | Qualitative modification/increase            |
| Part of            | Qualitative modification/decrease            |
| Reverse            | Logical opposite of the design intent        |
| Other than/Instead | Complete substitution                        |
| Early              | Relative to clock time                       |
| Late               | Relative to clock time                       |
| Before             | Relating to order or sequence                |
| After              | Relating to order or sequence                |

Methods such as STPA have merit for whole-vehicle level analysis, but with sensing we are dealing with information processing systems and a flow-based model seems more appropriate. In particular, we are interested in
identifying potential causes of unsafe internal states – HISS, in our terminology. SHARD was developed from HAZOP for computer-based systems but, implicitly, it assumed that the flows were quite simple, e.g. scalar values. Images from cameras are rich and complex, thus it seems appropriate to go back to the original HAZOP definition of guidewords to identify what are appropriate prompts for sensing systems, albeit focusing on information content not considering multiple attributes. We first briefly analyse the standard HAZOP guidewords for relevance to the analysis of sensing systems, then give examples to make the intended interpretation more concrete. This is followed by an explanation of how we expect the method to be used.

3.1. Analysis of Standard HAZOP Guidewords

The standard HAZOP guidewords are set out in Table 1 below. We briefly discuss the guidewords to assess their relevance for sensing system analysis.

The guidewords are assessed as follows:

- **No or Not** – relevant, this is similar to *Omission* and would include false negatives;

- **More and Less** – relevant, this can include false positives, e.g. identifying more objects than exist in the scene through reflections from glass buildings, and false negatives;

- **As well as and Part of** – relevant, although may be very similar to *More and Less*;

- **Reverse** – while not relevant in the meaning of flow from the computers to the sensor we have used it to consider the a sign change in scalar or vector values;

- **Other than/Instead** – relevant, this is similar to *Incorrect* and would include, for example, wrong classification;

- **Early and Late** – relevant, although the likelihood of seeing such deviations will depend on the sensor physics;

- **Before and After** – there may be mis-ordering of returns from active sensors in multi-path scenarios but, for now, we deem this as not relevant as we are interested in what is in the “world model” not the order in which the elements were identified.
There is some overlap between *No or Not*, *More*, *Less*, *As well as* and *Part of*. It may be, with experience, these could be simplified further or reduced to false positive and false negative. However, *More* and *Less* may remain useful where there are quantitative errors in counting multiple objects of the same class in a given scene. This remains an area for future work, including gaining feedback from experience using the method.

Experience of malfunctions in perception systems (and their impact on vehicle safety) would also lead us to include *Intermittent* as a guideword, reflecting the case where an object is identified, then missed, then identified again. Whilst this could be viewed as a special case of, say, *No or Not* having the guideword explicitly encourages consideration of such cases.

### 3.2. Proposed Guidewords and Rationale

The proposed guidewords are set out in Table 2 together with interpretations that are more redolent of the behaviour and failure modes of perception systems, especially those based on cameras with ML used for image processing and understanding. Illustrative examples of the several of the guidewords are provided below, and an illustration of the use of the method on the ALKS is given in Section 4.

The guideword *No or Not* can be illustrated by an example of pedestrian detection at a level crossing. Figure 3 from [33] shows pedestrians correctly detected in green bounding boxes and those that have been missed (false negatives) with blue bounding boxes. One pedestrian is partly occluded by another who is correctly identified; two others are partly obscured by trees. This also serves as an example of *Part of*. Arguably, behaviour in this case is still safe as the pedestrian most exposed to risk has been correctly identified.

Figure 4 is from a system intended to detect runway and taxiway centre lines to assist in landing and aircraft manoeuvres in adverse weather conditions. As well as detecting the painted yellow lines it has “picked up” the joins in the concrete, thus illustrating the *More* guideword.

Figure 5 shows a Tesla system “seeing” a sky/cloud formation as a crossing truck (this is apparent on the image of the screen in the vehicle). This is an example of *As Well As*. It can also be seen as an example of pareidolia [34] where NNs tend to “see” patterns in images which are not actually there [35, 36, 37]. In this particular case, the deviation from intent is unlikely to be hazardous (the spurious image will disappear as the vehicle proceeds).

Figure 6 shows a Tesla interpreting the moon as an amber traffic light, and this illustrates *Incorrect* – an inappropriate classification. Depending on
Table 2: Revised HAZOP Guidewords

| Guideword     | Interpretation                                                                 |
|---------------|--------------------------------------------------------------------------------|
| No or Not     | Failure to identify a relevant element of the scene (false negative)            |
| More          | Identifying more elements in the scene than are relevant (multiple false positives) |
| Less          | Identifying fewer elements in the scene than are relevant (multiple false negatives) |
| As well as    | Identifying element in the scene that is not there (false positive)             |
| Part of       | Failing to identify element in the scene that is there (false negative)         |
| Other than/Instead | Incorrect classification, e.g. static object rather than pedestrian              |
| Reverse       | Change of sign in a scalar or vector value, e.g. pedestrian is moving towards rather than away from ego vehicle |
| Early         | Object identified earlier than necessary for safe behaviour, perhaps triggering unnecessary response |
| Late          | Object identified later than necessary for safe behaviour                        |
| Intermittent  | Element of scene present in some images, but not in others, or classification changes from image to image |

The road situation, and the estimated proximity of the vehicle to the identified traffic light the vehicle could start to slow down – this could be hazardous as other (manually driven) vehicles would not be expecting deceleration for a non-existent traffic light, and there is a risk of a rear-end collision.

The timing guidewords – Early and Late – are not easy to illustrate using images, instead they would need image sequences or videos. However, the identification of Elaine Herzberg as a pedestrian in the Uber Tempe accident only 1.2s before impact is an example of a Late failure (deviations) [19]. Further, the Uber systems repeatedly re-classified Ms Herzberg in the seconds leading up to the accident. Key points in the timeline are illustrated in Figure 7. This is an example of the Intermittent deviation. However, it also shows the need to undertake analysis in the context of understanding system behaviour. At the time of the accident the Uber software discarded the trajectory history for the “object” whenever it was reclassified. Thus,
for example, the motion was at one time predicted to be along the left turn lanes marked in the figure and not across the road.

The examples illustrate the guidewords and provide further motivation for their choice. However, it also illustrates that not all deviations from design intent are hazardous, and that knowledge of system design and of operational context are needed to determine whether or not a given deviations constitutes a HISS and can contribute to a hazard.

3.3. Applying the Method

In broad terms, it is expected that the system architecture can be viewed as four main elements: Sense, Understand, Decide and Act. In analysing perception systems we treat Sense and Understand together, and HISS can arise at the interface between Understand and Decide. At this point, the Decide element has to “trust” the system model and significant deviations between ground truth and the system’s model of the environment can lead to unsafe decisions. Several of the above examples make this clear, but it is perhaps most apparent with the Uber Tempe example [19].

As indicated earlier, the expectation is that hazard analysis will have been undertaken at whole system level (for an AV, in this case), prior to applying
SAUS. To be of most value, SAUS would be applied once a perception system architecture has been defined with commitments made to a particular sensor suite and to the ML approach, e.g. the structure of DDMs, etc. so the analysis can accurately reflect the system design. DSRs might include refinements to the DDM’s architecture, adaptations of the hyperparameters, e.g. loss functions, and choice of training data sets.

Due to the complexity of the ADAS or ADS to be analysed, SAUS is applied on scenarios. This has the benefit of identifying the DDT being undertaken by the ADAS or ADS and provides sufficient context to assess the potential for hazards. Each scenario is described as a form of use-case including the following elements [38]:

- **Primary environment** – the context for the DDT, e.g. type of road;
Figure 5: Spurious Object Identification

- **Goal in context** – the top-level goal of the ADS or ADAS in this context;

- **Scope** – any restrictions on the scenario, e.g. weather conditions under which the ADS or ADAS is expected to operate;

- **Pre-conditions** – necessary conditions for the scenario, e.g. presence of other vehicles;

- **Success end conditions** – the results of correct behaviour of the system in the scenario;

- **Failed end conditions** – the hazard(s) identified by earlier analysis;

- **Actors** – the systems and/or individuals involved in the use case, e.g. an ADAS and the driver;
Figure 6: Moon Misclassified as Amber Traffic Light

- *Trigger* – a condition that can initiate the use case;
- *Description* – the sequence of actions that should occur in the scenario.

In practice, it is likely that the *Primary environment* and the *Scope* will reflect the *Operation Design Domain (ODD)* for the ADS or ADAS.

As with other HAZOP-based methods, the analysis is recorded in tables. The key entries in the table are as follows:

- Function – the autonomous capability, i.e. the ADAS or ADS function, being analysed;
Figure 7: Timeline Leading to Accident with Uber ATG vehicle in Tempe Arizona

- Parameter – the information supporting the capability being analysed, e.g. distance to vehicle in front for AEB;
- Guideword – the HAZOP guideword to be applied to the parameter;
- Deviation – the interpretation of the guideword for the parameter being considered;
- Hazard – description of the hazard(s) that can arise from the deviation,
if any;

- Situation – the context in which the DDT is taking place, e.g. type of road, reflecting the Primary environment;

- Consequences – the potential effects of the hazard(s) which may be left blank if the deviations are not considered hazardous;

- Causes – credible malfunctions that could give rise to the identified deviations;

- Derived Safety Requirements – DSRs where deemed appropriate to reduce the likelihood of the hazard causes or to mitigate the consequences.

The analysis would consider the combination of these elements. There is a risk of “combinatorial explosion” but choosing an appropriate level at which to model the system functions, and noting when a guideword produces the same results as identified previously, e.g. considering Less after considering No or Not may not identify any further deviations, should help to keep the analysis manageable.

4. ALKS Example

Analysis starts with a system model. Here we wish to look at the behaviour (of ALKS) at a high level to elucidate the the potential hazards and fragility of ALKS implementations owing to Sensor vulnerabilities without restriction by the exact sensor device or implementation algorithm. We choose this level as we believe it is useful and informative; see Section 5 for a discussion.

We decompose the ADAS system in this case L2/L3 ALKS capabilities into different levels:

- **Service** – a complete vehicle feature available to the driver/operator regardless of autonomy level e.g L2+: ALKS, L1: Adaptive Cruise Control (ACC), Automated Lane Centring (ALC) or Automatic Emergency Breaking (AEB), L0: Blind Sport Warning (BSW), Forward Collision Warning (FCW) or Lane Departure Warning (LDW)
Figure 8: ALKS system, subs-systems and components

- **Behavioural Capability** – top level capabilities required to implement the service, e.g. ability to change lane

- **Function** – processing of data streams required to implement the capability

- **Implementation** – hardware and software required collect and process data to service the function or give effect to decisions

- **Data Source** – description of unit providing data to implementation
A L2 service may be made up of L1 services in addition to L2 capabilities while a L1 service may be made from L0 services and L1 capabilities.

Level of service restricts capabilities, e.g. a L1 service permits automated control of steering or acceleration while L2 or above is required for automated control of both steering and acceleration.

This decomposition is illustrated in Figure: 4 we will concern ourselves with the vertices between Behavioural Capability and Function in order to maintain a high level assessment.

4.1. Illustrations

We will consider several instances taken from real events where a vehicle operating an ALKS-like system experiences what we believe to be a Hazardous Internal System State (HISS). A HISS as defined above, is where system’s model of the environment or its own state differs significantly from the real world (ground truth). This difference can result from failures at different levels with in the autonomous system namely in: sensing, perception, understanding and decision-making.

Sensing failures fall into 3 categories: the sensor is non-functional, the sensor is functioning but degraded, or the sensor is malfunctioning. These may arise from a multitude of sources including: mechanical failure, electronic failure, thermal failure, environmental conditions or configuration error, to name but a few.

Whilst it is impossible to understand the environment perfectly with a degraded sensor, more frequently the available data suggests that the failures reside in the interpretation of the provided data leading to perception failure which results in understanding failures. These to fall into five broad categories:

- Unrecognised Sensor Failure – Failure, degradation or malfunctioning of sensor or sensor data is not recognised
- Not detected – Objects appear in the sensor field of view and data but are not detected (Object presence)
- Not classified – Objects are detected but are not classified and their presence is rejected (Object presence)
- Misclassification – Objects are detected but are misclassified (Object nature including pareidolia)
• Illusion – Objects are detected where they don’t exist or their nature is grossly misinterpreted (Object presence, shape, position, movement, or colour)

Perception failures may lead to understanding failures if we consider that understanding is the linking of pieces of information to create a coherent scene. Observed failures of understanding have arisen where there is an apparent conflict between different sources of information or where several pieces of concurring information conflict with the external environment. These fall into several broad categories:

• Unrecognised Perception failure
• Conflict between sensors’ perception
• Conflict between perception and internal law
• Conflict between perception and internal data source

We can illustrate these cases with some simple examples.

• Conflict between sensor data – detection and classification of targets does not correspond between sensor units.

• Conflict with on board law – radius of curve is perceived as greater than actual, lateral acceleration will exceed maximum permitted limit, $3m/s^2$ in normal operation, or $5m/s^2$ in an emergency manoeuvre [39].

• Conflict with on board data – the detected on the ground geometry of the driveable area, does not match with the driveable area described by internal/on-board maps

Finally, understanding failures may be driven by decision making, where a higher level decision may override the understanding developed from perception, or to command an action that ignores the developed understanding. This can be illustrated by a commonly observed example:

• Conflict between Decision and Understanding – Decision level route planning overrides understanding to command a manoeuvre that conflicts with the developed understanding such as cutting back to a straight-on route after beginning a right turn.
An ALKS system principally performs the DDT by keeping the vehicle in its lane by control of the lateral and longitudinal movements of the vehicle [40]. Some currently available examples of ALKS-like capability further permit: lane change, junction negotiation and navigate to destination capabilities, without issuing a transition demand.

Examining the requirements for this functionality several of the principal behavioural capabilities are need to create an ALKS service namely: ACC ALC AEB FCW LDW. In the main body of the paper we will treat: ACC and ALC via the HAZOP methodology further ALKS capabilities (AEB FCW LDW) will be treated in annexes: Appendix A.

To carry out the HAZOP we need an understanding of limits on vehicle dynamics. In this case, it is sufficient to understand limitations on cornering. A vehicle navigating a curve experiences a lateral acceleration \( a = \frac{v^2}{r} \) where \( v \) is the vehicle’s velocity and \( r \) is the radius of curvature. *UN Regulation No. 79: Automatically Commanded Steering Function* specifies that the magnitude of lateral acceleration should not exceed \( a > 3 \, m/s^2 \) and under nominal consideration the manufacture may permit a maximum of \( a > 4 \, m/s^2 \) [39].

When applying the HAZOP Guide Words to parameters of ADAS functions Reverse results are considered in some instances e.g. ACC 1.1.2 Distance to Target (see Table 10), the finding of a Reverse result in a forward looking sensor could be excluded or mitigated by simple logic check against nonphysical results, and flag an error state in the sensor or software status.

Example HAZOP analyses are provided in Tables 10 to 8 below, noting that the DSRs are left out and are discussed below. We briefly illustrate some of the entries to further explain the method. As noted above, although the definition of the HAZOP guidewords was motivated by analysis of camera-based systems we illustrate the method with both camera and radar-based capabilities to help to show its generality.

For entry ACC 1.1.1 Relative Velocity of Target Vehicle, the first row for “More” illustrates how the effect of the deviation can vary in different driving situations. Whilst, in itself, this is not hazardous (the distance to the lead vehicle increases) reaction of other road users might contribute to hazards in the wider road transport system, as shown in the consequences column. Here the DSR is essentially for correct performance – within some error. There is value in setting expectations on such performance for safety and to enable Tier 1 manufacturers to produce AV components at a reasonable price and often UN ECE regulations will provide the detail. For entry ACC 1.2 Distance to Target Vehicle, the last row for “Reverse” identifies a situation
that is physically impossible. This should lead to a system-specific DSR to detect and reject such data. Whilst this may seem obvious, a previously analysed a medical device which caused two fatalities, at least in part because it failed to respond to “impossible” values. Again, Tier 1 suppliers may produce components with such properties, but the analysis gives a clear basis for checking this.

Entry FCW 0.2.5 Collision Warning A.19 shows how the lower-level deviations come together to cause problems in the generation of the Collision Warning (the causes are deviations in the parameters in entries 1.1 to 1.4). DSR would also be expected at this level – for example, “Not” would lead to requirements for sensors to self-diagnose their failures (interoception) or for cross-checks between sensors.
### Table 3: Scenario use-case: Camera implementation of Automated Lane Centring

| Hazop Analysis |
|----------------|
| **Use-Case**   | Camera Automatic Lane Centring |
| **Use-Case #** | T_CMRA_ALC_1 |

| Scenario |
|----------|
| ![Image](image_url) |

| **Primary environment** | Motorway, A roads, urban |
|-------------------------|--------------------------|
| **Goal in context**    | System to detect and maintain vehicle in centre of the driving lane. |
| **Scope**              |                         |
| **Pre-conditions**     | Ego vehicle on a recognised lined carriage way |
| **Success end condition** | Ego vehicle adjusts velocity and steering angle consistent with safe maintenance of position in centre of driving lane |
| **Failed end conditions** | Ego vehicle leaves the driving lane and/or carriage way |
| **Actors**             | Ego vehicle control system |
| **Trigger**            | Ego vehicle navigating a recognised lined carriage way |

| **Description** | **Step** | **Action** |
|-----------------|----------|------------|
|                 | 1        | Detect recognised lined carriage way |
|                 | 2        | Report velocity and steering angle command to vehicle control function |

| **Extension** | **Step** | **Branching Action** |
|---------------|----------|----------------------|
|               | 1        | Failed to detect recognised lined carriage way |
|               | 2        | Report failure to vehicle operator |
| ID   | Function           | Parameter   | Guide Word | Deviation | Hazard                     | Situation      | Consequence                                                                 | Causes                                                                                   |
|------|--------------------|-------------|------------|-----------|---------------------------|----------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1.2.1| Automatic          | Lane        | Centring   | As well as| An area of the scene is   | Motorway       | Ego Vehicle may drive on or navigate to an area that in addition to the highway | 1. Incorrect interpretation of Camera data  
2. Camera data value is out of range  
3. Conflict between Sensor data and internal data sources. |
|      | Driveable Area     | Recognition |            |           | Ego vehicle may drive on or navigate to an area that in addition to the highway | A Road         | Ego Vehicle may drive in the verge, Bus Lane / Cycle Lane. May result in Collision leading to material damage injury or death | 1. Incorrect interpretation of Camera data  
2. Camera data value is out of range |
|      |                    |             |            |           |                           | Urban          | Ego Vehicle may drive in the Bus Lane / Cycle Lane or pavement. May result in Collision leading to material damage injury or death | 1. Incorrect interpretation of Camera data  
2. Camera data value is out of range |
|      |                    |             |            |           |                           |                |                                                                              | 1. Conflict between Sensor data and internal data sources.  
2. Conflict between Sensor data and internal data sources. |
|      |                    |             |            | Part of   | Part of the highway is not recognised as the drivable area | Motorway       | Ego vehicle may not drive on an appropriate area of the highway               | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | A Road         | Ego Vehicle may not drive in appropriate traffic lane leading to confusion and frustration of other drivers. May result in unnecessary or sudden stopping. May result in Collision leading to material damage injury or death | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | Urban          |                                                                              | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            | Not      | The drivable area is not recognised | Motorway       | Ego vehicle cannot navigate the drivable area                                 | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | A Road         | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | Urban          |                                                                              | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            | Intermittent | The drivable area is recognised intermittently | Motorway       | Ego vehicle navigates the drivable area intermittently                        | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | A Road         | Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | Urban          |                                                                              | 1. Malfunctioning Camera unit  
2. Incorrect interpretation of Camera data  
3. Camera data value is out of range  
4. Environmental Factors obscure drivable area  
5. Conflict between Sensor data and internal data sources. |
|      |                    |             |            | Other Than / | Areas other than the highway is recognised as the drivable area | Motorway       | The Ego vehicle navigates on an area that isn’t the drivable area             | 1. Incorrect interpretation of Camera data  
2. Camera data value is out of range  
3. Environmental Factors obscure drivable area  
4. Conflict between Sensor data and internal data sources. |
|      | Instead            |             |            |           |                           | A Road         | Ego Vehicle may drive in the hard shoulder or verge. May result in Collision leading to material damage injury or death | 1. Incorrect interpretation of Camera data  
2. Camera data value is out of range  
3. Environmental Factors obscure drivable area  
4. Conflict between Sensor data and internal data sources. |
|      |                    |             |            |           |                           | Urban          | Ego Vehicle may drive in the Bus Lane / Cycle Lane or pavement. May result in Collision leading to material damage injury or death | 1. Incorrect interpretation of Camera data  
2. Camera data value is out of range  
3. Environmental Factors obscure drivable area  
4. Conflict between Sensor data and internal data sources. |

Table 4: Hazop Table for camera implementation of Automated Lane Centring (ALC) Part 1
| ID   | Function   | Parameter | Guide Word       | Deviation                      | Hazard                                                                 | Situation | Consequence                                                                 | Causes                                                                 |
|------|------------|-----------|-----------------|--------------------------------|------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1.2.2| Automatic  | Lane      | Marking         | Recognition                   | More Lane Markings are recognised than actual Ego vehicle may navigate along a path not corresponding to that of the driving lane. | Motorway  | Ego Vehicle may drive across traffic lanes. May result in Collision leading to material damage injury or death | 1. Incorrect interpretation of Camera data 2. Camera data value is out of range |
|      | Lane       | Marking   | Recognition     |                                | A Road Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | A Road    |                                                                          |                                                                        |
|      |            |           |                 |                                | Urban                                                                    |           |                                                                            |                                                                        |
|      |            | Less      | Less Lane Markings are recognised than actual Ego vehicle may navigate along a path not corresponding to that of the driving lane. | Motorway Ego Vehicle may drive across traffic lanes. May result in Collision leading to material damage injury or death | 1. Malfunctioning Camera unit 2. Incorrect interpretation of Camera data 3. Camera data value is out of range 4. Environmental Factors obscure markings |
|      |            |           |                 |                                | A Road Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | A Road    |                                                                          |                                                                        |
|      |            |           |                 |                                | Urban                                                                    |           |                                                                            |                                                                        |
|      |            | Not       | Lane Markings are not recognised Ego vehicle cannot orientate itself in the driving lane. | Motorway Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers | 1. Malfunctioning Camera unit 2. Incorrect interpretation of Camera data 3. Camera data value is out of range 4. Environmental Factors obscure markings |
|      |            |           |                 |                                | A Road Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | A Road    |                                                                          |                                                                        |
|      |            |           |                 |                                | Urban                                                                    |           |                                                                            |                                                                        |
|      |            | Intermittent | Lane Markings are recognised intermittently Ego vehicle navigates along a path in the driving lane intermittently. | Motorway Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning Camera unit 2. Incorrect interpretation of Camera data 3. Camera data value is out of range 4. Environmental Factors obscure markings |
|      |            |           |                 |                                | A Road Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | A Road    |                                                                          |                                                                        |
|      |            |           |                 |                                | Urban                                                                    |           |                                                                            |                                                                        |
|      |            | Other Than / Instead | Markings other than lane markings are recognised as lane markings Ego vehicle navigates along a path that does not correspond to the driving lane. | Motorway Ego Vehicle may drive in the hard-shoulder Lane. May result in Collision leading to material damage injury or death | 1. Incorrect interpretation of Camera data 2. Camera data value is out of range 3. Environmental Factors obscure markings 4. Conflict between Sensor data and internal data sources. |
|      |            |           |                 |                                | A Road Ego Vehicle may drive in the Bus Lane / Cycle Lane. May result in Collision leading to material damage injury or death | A Road    |                                                                          |                                                                        |
|      |            |           |                 |                                | Urban                                                                    |           |                                                                            |                                                                        |

Table 5: Hazop Table for camera implementation of Automated Lane Centring (ALC) Part 2
| ID   | Function         | Parameter                      | Guide Word                  | Deviation | Hazard                        | Situation | Consequence                                                                 | Causes                                                                 |
|------|------------------|--------------------------------|-----------------------------|-----------|-------------------------------|-----------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1.2.3| Automatic Lane Centring | Lane Position Estimation | Other than / Instead | Ego Vehicle’s Lane position estimate is report as other than actual | Ego vehicle positions itself other than at centre of driving lane | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers | 1. Malfunctioning Camera unit 2. Incorrect interpretation of Camera data 3. Camera data value is out of range 4. Environmental Factors degrade image 5. Conflict between Sensor data and internal data sources. |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
| 1.2.4| Automatic Lane Centring | Vehicle Pose Estimation | Other than / Instead | Ego Vehicle’s pose estimate is report as other than actual | Ego vehicle orients itself other than colinear to driving lane | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers | 1. Malfunctioning Camera unit 2. Incorrect interpretation of Camera data 3. Camera data value is out of range 4. Malfunctioning internal data sources 5. Environmental Factors degrade sensor data 6. Conflict between Sensor data and internal data sources. |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |
|      |                   |                                |                             |           | A Road                        | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | Urban |                                                                                                                                   |

Table 6: Hazop Table for camera implementation of Automated Lane Centring (ALC) Part 3
| ID | Function | Parameter | Guide Word | Deviation | Hazard | Situation | Consequence | Causes |
|----|----------|-----------|------------|-----------|--------|-----------|-------------|--------|
| 1.2.5 | Automatic Lane Centring | Current Lane Curvature | Not | Current lane curvature is not reported | Ego Vehicle cannot effectively negotiate curve | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers. | A Road: Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death. Causes: 1. Malfunctioning camera unit 2. Incorrect interpretation of camera data 3. Camera data value is out of range 4. Camera Data is ignored/discarded. |
| | | | | | | | | |
| | | More | Current lane curvature is reported as more than actual | Ego Vehicle commands steering angle which over-steers through the curve | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers. | A Road: Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death. Causes: 1. Malfunctioning camera unit 2. Incorrect interpretation of camera data 3. Camera data value is out of range 4. Conflict between Sensor data and internal data sources. |
| | | Less | Current lane curvature is reported as more than actual | Ego Vehicle commands steering angle which under-steers through the curve | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers. | A Road: Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death. Causes: 1. Malfunctioning camera unit 2. Incorrect interpretation of camera data 3. Camera data value is out of range 4. Conflict between Sensor data and internal data sources. |
| | | Intermittent | Current lane curvature is reported intermittently | Ego Vehicle intermittently correctly steers through the curve | Motorway | Erratic driving leading to frustration confusion of other drivers. | A Road: Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death. Causes: 1. Malfunctioning camera unit 2. Incorrect interpretation of camera data 3. Camera data value is out of range 4. Camera Data is ignored/discarded. |
| | | Reverse | Current lane curvature is reported as reverse of actual | Ego Vehicle steers commands reverse steering angle incorrectly steering through the curve | Motorway | Ego Vehicle may leave driving lane, leading to confusion and frustration of other drivers. | A Road: Ego Vehicle may drive across traffic lanes. May result in Collision leading to material damage injury or death. Causes: 1. Malfunctioning camera unit 2. Incorrect interpretation of camera data 3. Camera data value is out of range. |

Table 7: Hazop Table for camera implementation of Automated Lane Centring (ALC) Part 4
| ID   | Function                  | Parameter          | Guide Word | Deviation | Hazard                                                                 | Situation                  | Consequence                                                                 | Causes                                                                 |
|------|---------------------------|--------------------|------------|-----------|-------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1.2.6| Automatic Lane Centring   | Predicted lane curvature | More       | Predicted lane curvature is report more than actual | Ego vehicle decreases speed into curve more than necessary | Motorway | Other vehicle cuts into gap                                              | 1. Malfunctioning camera unit                                        |
|      |                           |                    |            |           |                                                                         | A Road                      | Traffic builds up behind, over taking in frustration                       | 2. Incorrect interpretation of camera data                            |
|      |                           |                    |            |           |                                                                         | Urban                       | Traffic builds up behind                                                   | 3. Camera data value is out of range                                  |
|      |                           |                    |            |           |                                                                         |                             |                                                                             | 4. Conflict between Sensor data and internal data sources.             |
|      |                           |                    | Less       | Predicted lane curvature is reported less than actual | Ego vehicle does not decrease speed into curve sufficiently saturating maximum lateral acceleration and steering rate. | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers | 1. Malfunctioning camera unit                                        |
|      |                           |                    |            |           |                                                                         | A Road                      | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | 2. Incorrect interpretation of camera data                            |
|      |                           |                    |            |           |                                                                         | Urban                       |                                                                             | 3. Camera data value is out of range                                  |
|      |                           |                    |            |           |                                                                         |                             |                                                                             | 4. Conflict between Sensor data and internal data sources.             |
|      |                           |                    | Not        | Predicted lane curvature is not reported | Ego vehicle cannot set appropriate speed for curvature | Motorway | ALC is not functional. May result in Collision leading to material damage injury or death | 1. Malfunctioning camera unit                                        |
|      |                           |                    |            |           |                                                                         | A Road                      |                                                                             | 2. Incorrect interpretation of camera data                            |
|      |                           |                    |            |           |                                                                         | Urban                       |                                                                             | 3. Camera data value is out of range                                  |
|      |                           |                    | Intermittent| Predicted lane curvature is reported intermittently | Ego vehicle does not maintain appropriate speed for curvature | Motorway | Erratic driving leading to frustration confusion of other drivers | 1. Malfunctioning camera unit                                        |
|      |                           |                    |            |           |                                                                         | A Road                      |                                                                             | 2. Incorrect interpretation of camera data                            |
|      |                           |                    |            |           |                                                                         | Urban                       |                                                                             | 3. Camera data value is out of range                                  |
|      |                           | Reverse            |            | Reverse   | Current lane curvature is reported as reverse of actual | Motorway | Ego Vehicle may drive across traffic lanes, leading to confusion and frustration of other drivers | 1. Malfunctioning camera unit                                        |
|      |                           |                    |            |           |                                                                         | A Road                      | Ego Vehicle may drive across oncoming traffic lanes or leave the road. May result in Collision leading to material damage injury or death | 2. Incorrect interpretation of camera data                            |
|      |                           |                    |            |           |                                                                         | Urban                       |                                                                             | 3. Camera data value is out of range                                  |
|      |                           |                    |            |           |                                                                         |                             |                                                                             | 4. Conflict between Sensor data and internal data sources.             |
Table 9: Scenario use-case: Radar implementation of Adaptive Cruise Control

| Hazop Analysis |
|----------------|
| Use-Case       | Radar Adaptive Cruise Control |
| Use-Case #     | TRDR_{ACC,2}                |
| Scenario       |                            |

| Primary environment       | Motorway, A roads, urban          |
|---------------------------|-----------------------------------|
| Goal in context           | System to detect target and maintain safe following distance. |
| Scope                     |                                    |
| Pre-conditions            | Appearance of Target in the road in front of ego vehicle |
| Success end condition     | Ego vehicle adjusts velocity/distance consistent with target behaviour |
| Failed end conditions     | Ego vehicle strikes target object or leaves the carriage way |
| Actors                    | Ego vehicle control system         |
| Trigger                   | Target in the road that may not be driven over |

| Description | Step | Action                                      |
|-------------|------|---------------------------------------------|
|             | 1    | Detect target on the road                   |
|             | 2    | Report velocity and distance command to vehicle control function |

| Extension | Step | Branching Action                           |
|-----------|------|--------------------------------------------|
|           | 1    | Failure to adjust ego velocity or distance |
|           | 2    | Report failure to vehicle operator         |

33
### Table 10: Hazop Table for radar implementation of Adaptive Cruise Control (ACC) Part 1

| ID | Function | Parameter | Guide Word | Deviation | Hazard | Situation | Consequence | Cause |
|----|----------|-----------|------------|-----------|--------|-----------|-------------|-------|
| 1.1.1 | Adaptive Cruise Control | Relative Velocity of target vehicle | More | Relative velocity is reported as more than actual. | Ego vehicle increases safe distance to target vehicle. | Motorway | Other vehicle cuts into gap | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | Traffic builds up behind, over taking in frustration | Urban | Traffic builds up behind |
| | | | Less | Relative velocity is reported as less than actual. | Ego vehicle decreases safe distance on target vehicle. | Motorway | Ego Vehicle get too close to target vehicle | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| | | | Not | Relative velocity report is not reported. | Ego vehicle cannot track target vehicle. | Motorway | ACC is not functional. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| | | | Intermittent | Relative velocity report is intermittent. | Ego vehicle safe distance to target vehicle varies. | Motorway | Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| | | | Reverse | Relative velocity is reported as inverse. | Ego vehicle decreases safe distance to target when it should increase and vice versa. | Motorway | Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| 1.1.2 | Adaptive Cruise Control | Distance to target vehicle | More | Distance to target vehicle is reported as more than actual. | Ego vehicle increases safe relative velocity to target vehicle. | Motorway | Ego Vehicle get too close to target vehicle | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| | | | Less | Distance to target vehicle is reported as less than actual. | Ego vehicle reduces safe relative velocity to target vehicle. | Motorway | Other vehicle cuts into gap | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | Traffic builds up behind, over taking in frustration | Urban | Traffic builds up behind |
| | | | Not | Distance to target vehicle is not reported. | Ego vehicle cannot track target vehicle. | Motorway | ACC is not functional. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| | | | Intermittent | Distance to target vehicle is reported intermittently. | Ego vehicle varies its safe velocity to target. | Motorway | Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |
| | | | Reverse | Distance to target vehicle is reported as inverse.* | Ego vehicle increases safe velocity relatively to target when it should decrease and vice versa vehicle varies. | Motorway | Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | A Road | | Urban | |

* Not physical as vehicle would be behind or inside ego vehicle. Logic error correction mechanism could mitigate e.g. forward facing sensor can't detect object to the rear.
### Table 11: Hazop Table for radar implementation of Adaptive Cruise Control (ACC) Part 2

| ID   | Function                  | Parameter         | Guide Word       | Deviation | Hazard | Situation | Consequence                                                                 | Cause                                                                 |
|------|---------------------------|-------------------|------------------|-----------|--------|-----------|----------------------------------------------------------------------------|----------------------------------------------------------------------|
| 1.1.3 | Adaptive Cruise Control   | Velocity of ego vehicle | More             | Ego velocity is reported as more than actual | Ego vehicle increases safe distance to target vehicle | A Road | Traffic builds up behind, over taking in frustration | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           |                   | Less             | Ego velocity is reported as less than actual | Ego vehicle decreases safe distance on target vehicle | A Road | Ego Vehicle get too close to target vehicle | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           |                   | Not              | Ego velocity is not reported | Ego vehicle cannot perform odometry | A Road | ACC is not functional. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
|      |                           |                   | Intermittent     | Ego velocity is reported intermittently | Ego vehicle safe distance to target vehicle varies | A Road | Erratic driving leading to frustration confusion of other drivers | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
|      |                           |                   | Reverse          | Ego velocity is reported as inverse from actual | Ego vehicle decreases distance to target when it should increase and vice versa. | A Road | Erratic driving leading to frustration confusion of other drivers. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |

| ID   | Function                  | Parameter         | Guide Word       | Deviation | Hazard | Situation | Consequence                                                                 | Cause                                                                 |
|------|---------------------------|-------------------|------------------|-----------|--------|-----------|----------------------------------------------------------------------------|----------------------------------------------------------------------|
| 1.1.4 | Adaptive Cruise Control   | Acceleration of ego vehicle | More             | Ego Acceleration is reported as more than actual | Ego vehicle increases safe distance to target vehicle | A Road | Traffic builds up behind, over taking in frustration | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           |                   | Less             | Ego Acceleration is reported as less than actual | Ego vehicle decreases safe distance on target vehicle | A Road | Ego Vehicle get too close to target vehicle | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           |                   | Not              | Ego Acceleration is not reported | Ego vehicle cannot perform odometry | A Road | FCW is not functional. May result in Collision leading to material damage injury or death | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
|      |                           |                   | Intermittent     | Ego Acceleration is reported intermittently | Ego vehicle safe distance to target vehicle varies | A Road | Erratic driving leading to frustration confusion of other drivers | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
|      |                           |                   | Reverse          | Ego Acceleration is reported as inverted from reality | Ego vehicle decreases safe distance to target when it should increase and vice versa. | A Road | Erratic driving leading to frustration confusion of other drivers | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |

---

Table 11: Hazop Table for radar implementation of Adaptive Cruise Control (ACC) Part 2
5. Discussion

The method developed and illustrated in the paper is based on a well-understood HAZOP method. The illustration of the method on ACC and ALC functionalities shows the feasibility of the approach, but also opens up some questions about its utility, scalability, etc.

First, it might be argued that the “problems” identified are obvious and would be “caught anyway” by competent designers or Tier 1 suppliers. Where this is true, the method serves to confirm the appropriateness of the component for its application. However, the examples of malfunctions of current AVs show that even if in principle these problems can be found, in practice they are making their way into deployed systems.

Second, real-world deployments of AVs are likely to employ multi-modal sensing systems. The analysis, as presented, focuses on single modalities. We see it as necessary to analyse the sensing modalities independently as they can be impaired and/or fail in different ways. What the method would allow us to do, if analysing a multi-modal sensing system, is to identify DSRs which can be met by use of other sensing modes. This can be illustrated by considering illusions in more detail.

The occurrence of pareidolia type phenomena are inherent in object recognition by CNN and its extent and susceptibility will be related to the distribution of training data, NN architecture, and available information in the scene [34, 35, 36, 37] Owing to its origin and frequency this phenomenon is considered within the label of misclassification. However, susceptibility to geometric illusion e.g. Muller-Lyer type illusions, has been observed in several safety critical instances. The susceptibility of CNN to these illusions and that they develop perception biases similar to humans, has been demonstrated by Ward et al (2019) [41]. We therefore suggest that the training data for AS should include significant contributions from less structured environments and specifically those with less rectilinear orthogonal forms in order to develop more nuanced cues for understanding of geometrical space. Typical geometric illusions may also be readily overcome by the use of high-fidelity active sensors as part of the perception suite.

Third, the systems of interest are likely to have many operational modes and the effects of failures can alter between modes. For example, given an ACC function, several deviations, e.g. “Less” of “relative velocity of target vehicle” will be different in a “drive off from standstill” mode as opposed to a “speed hold” mode. The HAZOP tables will need to be extended to include
a column for operational modes. Further, DSRs could include transitions between modes – for example to a speed-limited variant of ACC due to the weather conditions impairing the AV’s sensors.

Fourth is the issue of interoception. As well as classical fault monitoring and built-in test there is value in assessing sensor performance, in particular to determine whether or not the sensors are being impaired by the weather conditions, e.g. rain or snow in the case of optical sensors. This is a complex topic in itself but, for example, changes in statistics of the noise spectrum of the back-scattered light incident on an optical sensor, e.g. a Lidar, can indicate the presence of degrading environments e.g. rain or fog [42, 43, 44] and hence sensor impairment. We refer to this sort of interoception as sensor “introspection”. Related DSRs might be for change in AV mode, e.g. reduced velocity, and/or changes in priorities in sensing modality.

Fifth, there might be a concern about the scale or complexity of the example analysis, and what it means for analysis of industrial-scale systems, especially as it has been carried out at a general functional level, not reflecting a specific implementation architecture. This is a concern with all such analyses, but one which we believe can be overcome, especially where capabilities are relatively “standardised” as seems likely to be the case with AVs. We explain this by comparison with what has happened with civil aircraft. The hazards for “standardised” capabilities are well-known (often recorded in hazard lists) but these are extended for innovative implementations. For example, many large commercial aircraft use landing gear with wheels that caster, while the Airbus A380’s is actively steerable. This means that there are new hazards – for example landing with the wheels not aligned with the direction of travel – and this can be added to the hazard list. To do something analogous for AVs would require HAZOP-like analysis for major capabilities which would be common across vehicles, which can be picked up and refined for a specific application. The level of analysis presented here, i.e. in terms of ACC, ALC, etc., may be ideal for producing such a transferable analysis, although it may be that working at the level of more primitive behavioural capabilities, e.g. lane change, negotiating a roundabout, may be more practical (these capabilities can be composed to make higher level services). This remains an issue for further study.

Finally, it should be observed that, given the degree of interconnection between sensors, and various perception and understanding tasks, these systems are potentially liable to a significant number of common mode failures. Moreover, in deployed systems is has been observed that these failures have
complex interactions [45] that are not always commutative and associative. Further analysis of common mode failure in the perception and understanding capability is beyond the scope of this paper, but is an important area for further study.

6. Conclusions

Many AS are heavily dependent on their sensing capabilities to provide safe and effective services. Whilst the importance of the perception systems has long been recognised there has not, to our knowledge, previously been a systematic approach to analysing the way in which the behaviour and failure of such perception systems could contribute to the safety of the AS. This paper is intended to be a first step towards filling that “gap”.

Although our aim in proposing the method was to make generic, i.e. apply to a range of AS, it has been developed in the context of AVs. In particular the definition of HAZOP guidewords is motivated by an analysis of reported failures of perception systems mainly, but not entirely, related to AVs. However, to show that the method is not specific to optical/camera-based sensing we have illustrated it on radar-based AV functionality.

To gain initial feedback on the use of the method we are applying it to a small-scale mobile robot, intended to provide simple delivery services in a University building. We are also seeking other opportunities to validate the method, as well as exploring some of the issues covered in the discussion such as sensor “introspection” and related issues such as sensor performance evaluation. Ultimately, our aim is to help provide a sounder basis for assessing the contribution of proposed sensing systems to safety, and to provide methods to help in the selection and refinement of sensing systems for AS.

Credit Authorship Statement

All authors contributed equally to conception and drafting of the manuscript

Declaration of Competing Interest

The authors have no conflict of interest

Acknowledgment

This work has been funded by Lloyds Register Foundation and the University of York through the Assuring Autonomy International Programme https://www.york.ac.uk/assuring-autonomy.
## Appendix A. Supplementary HAZOP Tables

### Table A.12: Scenario use-case: Radar implementation of Automatic Emergency Braking

| Hazop Analysis |
|----------------|
| Use-Case       | Radar Automatic Emergency Break |
| Use-Case #     | T_RDR_AEB_3 |

### Scenario

- **Primary environment**: Motorway, A roads, urban
- **Goal in context**: System to detect and avoid striking targets.
- **Scope**
- **Pre-conditions**: Appearance of Target in the road in front of ego vehicle
- **Success end condition**: Ego vehicle slows or stops for target
- **Failed end conditions**: Ego vehicle strikes target object or leaves the carriage way
- **Actors**: Ego vehicle control system
- **Trigger**: Target in the road that may not be driven over

### Description

| Step | Action |
|------|--------|
| 1    | Detect target on the road |
| 2    | Report beak command to vehicle control function |

### Extension

| Step | Branching Action |
|------|------------------|
| 1    | Detect target on the road |
| 2    | Report target to vehicle operator |
### Table A.13: Hazop Table for radar implementation of Automatic Emergency Breaking (AEB) Part 1

| ID  | Function | Parameter | Guide Word | Deviation | Hazard | Situation | Consequence | Cause |
|-----|----------|-----------|------------|-----------|--------|-----------|-------------|-------|
| 0.1.1 | AEB | Relative Velocity of target vehicle | More | Relative velocity is reported as more than actual. | AEB accepts increased safe distance to target vehicle. | Motorway | AEB will supply break command to early. May lead to driver frustration. | A Road | " |
|       |          |           | Less      | Relative velocity is reported as less than actual. | AEB accepts decreased safe distance to target vehicle. | Motorway | AEB will supply break command to late. May lead to potential unmitigated collision. | A Road | " |
|       |          |           | Not       | Relative velocity report is not reported. | AEB cannot determine safe distance. | Motorway | AEB is not functional. May result in failure to supply break command in event of probable collision. | A Road | " |
|       |          |           | Intermittent | Relative velocity report is intermittent. | AEB ability to determine safe distance is sporadic. | Motorway | AEB will supply break command intermittently. May lead to driver frustration | A Road | " |
|       |          |           | Reverse   | Relative velocity report is reported as inverse. | AEB accepts decreased safe distance to target when it should increase and vice versa. | Motorway | AEB may not supply break command. May lead to potential unmitigated collision. | A Road | " |
| 0.1.2 | AEB | Distance to target vehicle | More | Distance to target vehicle is reported as more than actual. | AEB accepts increased safe relative velocity to target vehicle. | Motorway | AEB will supply break command too early. May lead to driver frustration | A Road | " |
|       |          |           | Less      | Distance to target vehicle is reported as less than actual. | AEB accepts decreased safe relative velocity to target vehicle. | Motorway | AEB will supply break command too late. May lead to potential unmitigated collision. | A Road | " |
|       |          |           | Not       | Distance to target vehicle is not reported. | AEB cannot determine safe velocity. | Motorway | AEB is not functional. May result in failure to supply break command in event of probable collision. | A Road | " |
|       |          |           | Intermittent | Distance to target vehicle is reported intermittently. | AEB ability to determine safe velocity is sporadic. | Motorway | AEB will supply break command intermittently. May lead to driver frustration | A Road | " |
|       |          |           | Reverse   | Distance to target vehicle is reported as inverse. * | AEB accepts increased safe velocity to target when it should decrease and vice versa. | Motorway | AEB may not supply break command. May lead to potential unmitigated collision. | A Road | " |

*Not physical as vehicle would be behind or inside ego vehicle. Logic error correction mechanism could mitigate e.g. forward facing sensor can't detect object to the rear.*
Reverse Ego Acceleration

Intermittent Ego Acceleration is not Ego Acceleration is not Less Ego Acceleration is reported.

Ego velocity is reported intermittently. Ego velocity is reported as less than actual. Ego velocity is not reported.

Ego vehicle cannot perform odometry.

AEB accepts increased safe distance to target vehicle. AEB accepts decreased safe distance on target vehicle. AEB accepts decreased safe distance to target vehicle.

AEB may not supply break command to early. May lead to driver frustration. AEB accepts break command to late. May lead to potential unmitigated collision. AEB accepts break command to early. May lead to potential unmitigated collision.

1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data

1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data

1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data

1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data

1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data

1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data

Table A.14: Hazop Table for radar implementation of Automatic Emergency Breaking (AEB) Part 2
| ID   | Function       | Parameter              | Guide Word | Deviation | Hazard                                 | Situation | Consequence                                                                 | Causes                                                                                     |
|------|----------------|------------------------|------------|-----------|----------------------------------------|-----------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| 0.1.5| AEB            | Emergency Breaking     | Early      | Automatic emergency breaking is activated early | Ego vehicle performs emergency stop early | Motorway | Unexpected Stop leading to confusion among other drivers, or rear end collision. | 1. Relative velocity of target misreported (More/Reverse)  
2. Distance to target misreported (Less)  
3. Velocity of ego vehicle misreported (More)  
4. Acceleration of ego vehicle misreported (More) |
|      |                |                        | Late       | Automatic emergency breaking is activated late | Ego vehicle collides with target vehicle  | Motorway | Collision leading to material damage injury or death  
A Road | | Urban | Unexpected Stop leading to confusion among other drivers, or rear end collision. Maybe difficult to navigate urban environment | 1. Relative velocity of target misreported (Less/Reverse)  
2. Distance to target misreported (More)  
3. Velocity of ego vehicle misreported (Less)  
4. Acceleration of ego vehicle misreported (Less) |
|      |                |                        | Not        | Automatic emergency breaking is not activated | Ego vehicle collides with target vehicle  | Motorway | Collision leading to material damage injury or death  
A Road | | Urban |  | | 1. Relative velocity of target misreported (Not/Intermittent)  
2. Distance to target misreported (Not/Intermittent)  
3. Velocity of ego vehicle misreported (Not/Intermittent)  
4. Acceleration of ego vehicle misreported (Not/Intermittent) |
|      |                |                        | Intermittent | Automatic emergency breaking is activated intermittently | False positive rate to high driver loses trust ignores system or Ego vehicle collides with target vehicle | Motorway | Erratic driving leading to frustration confusion of other drivers. May result in collision leading to material damage injury or death | 1. Relative velocity of target misreported (Intermittent)  
2. Distance to target misreported (Intermittent)  
3. Velocity of ego vehicle misreported (Intermittent)  
4. Acceleration of ego vehicle misreported (Intermittent) |

Table A.15: Hazop Table for radar implementation of Automatic Emergency Breaking (AEB) Part 3
### Table A.16: Scenario use-case: Radar implementation of Forward Collision Warning

| Hazop Analysis |
|----------------|
| Use-Case       | Radar Forward Collision Warning |
| Use-Case #     | T_RDR_FCW_4                      |
| Scenario       | ![Image](image)                  |

**Scenario**

- **Primary environment**: Motorway, A roads, urban
- **Goal in context**: System to detect and assist in avoiding striking a target.
- **Scope**
  - **Pre-conditions**: Appearance of Target in the road in front of ego vehicle
  - **Success end condition**: Ego vehicle slows or stops for target.
  - **Failed end conditions**: Ego vehicle strikes target object or leaves the carriage way
- **Actors**: Ego vehicle control system
- **Trigger**: Target in the road that may not be driven over

| Description       | Step | Action                                           |
|-------------------|------|--------------------------------------------------|
|                   | 1    | Detect target on the road                       |
|                   | 2    | Report target to vehicle operator                |

| Extension         | Step | Branching Action                                |
|-------------------|------|------------------------------------------------|
|                   | 1    | Vehicle operator does not initiate breaking     |
|                   | 2    | Report warning command to vehicle control function (Trigger AEB) |

43
### Table A.17: Hazop Table for radar implementation of Forward Collision Warning (FCW) Part 1

| ID | Function | Parameter | Guide Word | Deviation | Hazard | Situation | Consequence | Causes |
|----|----------|-----------|------------|-----------|--------|-----------|-------------|--------|
| 0.2.1 | Forward Collision Warning | Relative Velocity of target vehicle | More | Relative velocity is reported as more than actual. | FCW accepts increased safe distance to target vehicle. | Motorway | FCW will supply warning to early. May lead to driver frustration | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | | | | |
| | | Less | Relative velocity is reported as less than actual. | FCW accepts decreased safe distance to target vehicle. | Motorway | FCW will supply warning too late. May lead to potential unmitigated collision | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | | | | | | |
| | | Not | Relative velocity report is not reported. | FCW cannot determine safe distance. | Motorway | FCW is not functional. May result in failure to supply warning in event of probable collision | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
| | | Intermittent | Relative velocity report is intermittent. | FCW ability to determine safe distance is sporadic. | Motorway | FCW will supply warning intermittently. May lead to driver frustration | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
| | | Reverse | Relative velocity is reported as inverse. | FCW accepts decreased safe distance to target when it should increase and vice versa. | Motorway | FCW may not supply warning. May lead to potential unmitigated collision | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |

*Not physical as vehicle would be behind or inside ego vehicle. Logic error correction mechanism could mitigate e.g. forward facing sensor can’t detect object to the rear.
| ID   | Function                  | Parameter                  | Guide Word       | Deviation                                      | Hazard                                           | Situation                  | Consequence                                      | Causes                                                                 |
|------|---------------------------|----------------------------|------------------|------------------------------------------------|------------------------------------------------|---------------------------|------------------------------------------------|------------------------------------------------------------------------|
| 0.2.3 Forward Collision Warning | Velocity of ego vehicle | More                      | Ego velocity is reported as more than actual. | FCW accepts increased safe distance to target vehicle. | Motorway FCW will supply warning early. May lead to driver frustration. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           | Less                      | Ego velocity is reported as less than actual. | FCW accepts decreased safe distance on target vehicle. | Motorway FCW will supply warning to late. May lead to potential unmitigated collision. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           | Not                       | Ego velocity is not report. | Ego vehicle cannot perform odometry. | Motorway FCW is not functional. May result in failure to supply warning in event of probable collision. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
|      |                           | Intermittent              | Ego velocity is reported intermittently. | FCW ability to determine safe distance is sporadic. | Motorway FCW will supply warning intermittently. May lead to driver frustration | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range |
|      |                           | Reverse                   | Ego velocity is reported as inverse from actual. | FCW accepts decreased safe distance to target when it should increase and vice versa. | Motorway FCW may not supply warning. May lead to potential unmitigated collision. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
| 0.2.4 Forward Collision Warning | Acceleration of ego vehicle | More                      | Ego Acceleration is reported as more than actual | FCW accepts increased safe distance to target vehicle. | Motorway FCW will supply warning early. May lead to driver frustration. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           | Less                      | Ego Acceleration is reported as less than actual | FCW accepts decreased safe distance on target vehicle. | Motorway FCW will supply warning to late. May lead to potential unmitigated collision. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |
|      |                           | Not                       | Ego Acceleration is not report | Ego vehicle cannot perform odometry. | Motorway FCW is not functional. May result in failure to supply warning in event of probable collision. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
|      |                           | Intermittent              | Ego Acceleration is reported intermittently | FCW ability to determine safe distance is sporadic. | Motorway FCW will supply warning intermittently. May lead to driver frustration | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Environmental Factors degrade sensor data |
|      |                           | Reverse                   | Ego Acceleration is inverted from reality | FCW accepts decreased safe distance to target when it should increase and vice versa. | Motorway FCW may not supply warning. May lead to potential unmitigated collision. | A Road                     |                                            | 1. Malfunctioning radar unit 2. Incorrect interpretation of radar data 3. Radar data value is out of range 4. Conflict between sensor data and internal data |

Table A.18: Hazop Table for radar implementation of Forward Collision Warning (FCW) Part 2
| ID      | Function            | Parameter            | Guide Word                        | Deviation                        | Hazard                      | Situation                          | Consequence                              | Causes                                                                 |
|---------|---------------------|----------------------|-----------------------------------|----------------------------------|-----------------------------|------------------------------------|-----------------------------------------|------------------------------------------------------------------------|
| 0.2.5   | Forward Collision  | Warning              | Early                             | Imminent Collision               | Warning is reported early    | Early Imminent Collision           | Warning is reported early              | 1. Relative velocity of target misreported (More)                       |
|         |                     |                      |                                   |                                  |                             | Driver responds in time;           | Driver does not collide with         | 2. Distance to target misreported (Less)                                |
|         |                     |                      |                                   |                                  |                             | ego vehicle does not collide with  | target vehicle                        | 3. Velocity of ego vehicle misreported (More)                           |
|         |                     |                      |                                   |                                  |                             |                                    |                                         | 4. Acceleration of ego vehicle (More)                                    |
|         |                     |                      | Late                              | Imminent Collision               | Warning is reported late     | Late Imminent Collision           | Warning is reported Late              | 1. Relative velocity of target misreported (Less)                       |
|         |                     |                      |                                   |                                  |                             | Driver cannot respond in time;     | Driver loses trust;                  | 2. Distance to target misreported (More)                                |
|         |                     |                      |                                   |                                  |                             | Ego vehicle collides with target   | ignores system                       | 3. Velocity of ego vehicle misreported (Less)                           |
|         |                     |                      |                                   |                                  |                             | vehicle                            |                                         | 4. Acceleration of ego vehicle misreported (Less)                       |
|         |                     |                      | Not                               | Imminent Collision               | Warning is not reported      | Not Imminent Collision            | Warning is not reported              | 1. Relative velocity of target misreported (Not/Intermittent)           |
|         |                     |                      |                                   |                                  |                             |                                     |                                         | 2. Distance to target misreported (Not/Intermittent)                    |
|         |                     |                      |                                   |                                  |                             |                                     |                                         | 3. Velocity of ego vehicle misreported (Not/Intermittent)               |
|         |                     |                      |                                   |                                  |                             |                                     |                                         | 4. Acceleration of ego vehicle misreported (Not/Intermittent)           |
|         |                     |                      | Intermittent                      | Imminent Collision               | Warning is reported          | Intermittently Imminent Collision   | Warning is reported intermittently   | 1. Relative velocity of target misreported (Intermittent)              |
|         |                     |                      |                                   |                                  |                             |                                     |                                         | 2. Distance to target misreported (Intermittent)                        |
|         |                     |                      |                                   |                                  |                             |                                     |                                         | 3. Velocity of ego vehicle misreported (Intermittent)                  |
|         |                     |                      |                                   |                                  |                             |                                     |                                         | 4. Acceleration of ego vehicle misreported (Intermittent)              |

Table A.19: Hazop Table for radar implementation of **Forward Collision Warning (FCW)** Part 3
References

[1] J3016_201806: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International, https://www.sae.org/standards/content/j3016_201806/.

[2] M. L. Cummings, B. Bauchwitz, Autonomous Driving Assist Alerting, IEEE Transactions on Intelligent Transportation Systems, in press. In Press (2021) 12.

[3] United Nations, Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems, addendum 156 – UN Regulation No. 157 (2021).

[4] alexraicu90, Youtube, Sitting in the back bragging about the lane assist feature, crash on the highway, https://www.youtube.com/watch?v=sEpVvxKN-WI (Nov. 2021).

[5] J. Fayyad, M. A. Jaradat, D. Gruyer, H. Najjaran, Deep learning sensor fusion for autonomous vehicle perception and localization: A review 20 (15) (2020) 1–34. doi:10.3390/s20154220.

[6] A. Karpathy, CVPR’21 Workshop Autonomous Driving Keynote - Andrej Karpathy, Tesla (Jun. 2021).

[7] R. Hawkins, M. Osborne, M. Parsons, M. Nicholson, J. McDermid, I. Habli, Guidance on the Safety Assurance of Autonomous Systems in Complex Environments (SACE) (Aug. 2022). doi:10.48550/arXiv.2208.00853.

[8] O. Zendel, M. Murschitz, M. Humenberger, W. Herzner, CV-HAZOP: Introducing Test Data Validation for Computer Vision, in: 2015 IEEE International Conference on Computer Vision (ICCV), IEEE, Santiago, Chile, 2015, pp. 2066–2074. doi:10.1109/ICCV.2015.239.

[9] T. Kletz, HAZOP and HAZAN: identifying and assessing process industry hazards, CRC Press, 2018.

[10] ON-Semiconductor, Evaluating Functional Safety in Automotive Image Sensors, Tech. Rep. TND6233/D (2018).
[11] BEA, On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF447 Rio de Janeiro-Paris (2012).

[12] Collision between US Navy Destroyer Fitzgerald and Philippine-Flag Container Ship ACX Crystal, Sagami Nada Bay, off Izu Peninsula, Honshu Island, Japan, July 17, 2017, Marine Accident Report NTSB/MAR-19/01, NTSB, Washington DC.

[13] CNO USS Fitzgerald and USS John S McCain Response.pdf, REPORT ON COLLISIONS, OFFICE OF THE CHIEF OF NAVAL OPERATIONS, Washington DC (Oct. 2017).

[14] P. Sermanet, Y. LeCun, Traffic sign recognition with multi-scale Convolutional Networks, in: The 2011 International Joint Conference on Neural Networks, 2011, pp. 2809–2813. doi:10.1109/IJCNN.2011.6033589.

[15] A. Stocco, M. Weiss, M. Calzana, P. Tonella, Misbehaviour prediction for autonomous driving systems, in: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, ICSE ’20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 359–371. doi:10.1145/3377811.3380353.

[16] L. Huang, M. Cummings, M. Ono, A Mixed Analysis of Influencing Factors for Trust in a Risk-Aware Autonomy, Proceedings of the Human Factors and Ergonomics Society Annual Meeting 64 (1) (2020) 102–106. doi:10.1177/1071181320641027.

[17] M. L. Cummings, B. Bauchwitz, Safety Implications of Variability in Autonomous Driving Assist Alerting, IEEE Transactions on Intelligent Transportation Systems (2021) 1–11 doi:10.1109/TITS.2021.3109555.

[18] D. Alvarez Melis, T. Jaakkola, Towards Robust Interpretability with Self-Explaining Neural Networks, in: Advances in Neural Information Processing Systems, Vol. 31, Curran Associates, Inc., 2018.

[19] National Transportation Safety Board, Collision between vehicle controlled by developmental automated driving system and pedestrian, Tempe, Arizona March 18, 2018 (2019).
Collision between US Navy Destroyer John S McCain and Tanker Alnic MC, Marine Accident Report NTSB/MAR-19/01, NTSB.

P. Koopman, M. Wagner, Challenges in Autonomous Vehicle Testing and Validation 4 (1) (2016) 15–24. doi:10.4271/2016-01-0128.

D. Hendrycks, K. Zhao, S. Basart, J. Steinhardt, D. Song, Natural Adversarial Examples, in: 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, Nashville, TN, USA, 2021, pp. 15257–15266. doi:10.1109/CVPR46437.2021.01501.

M. Kläś, L. Jöckel, A Framework for Building Uncertainty Wrappers for AI/ML-Based Data-Driven Components, in: A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch, P. Ferreira (Eds.), Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops, Lecture Notes in Computer Science, Springer International Publishing, Cham, 2020, pp. 315–327. doi:10.1007/978-3-030-55583-2_23.

M. Kläś, L. Sembach, Uncertainty Wrappers for Data-Driven Models: Increase the Transparency of AI/ML-Based Models Through Enrichment with Dependable Situation-Aware Uncertainty Estimates, in: A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, F. Bitsch (Eds.), Computer Safety, Reliability, and Security, Vol. 11699, Springer International Publishing, Cham, 2019, pp. 358–364. doi:10.1007/978-3-030-26250-1_29.

C. Michaelis, B. Mitzkus, R. Geirhos, E. Rusak, O. Bringmanny, A. S. Eckery, M. Bethgey, W. Brendely, Benchmarking Robustness in Object Detection: Autonomous driving when winter is coming (NeurIPS 2019) (2019).

International Organization for Standardization (ISO), ISO 26262, Road Vehicles — Functional Safety (2018).

J. A. McDermid, M. Nicholson, D. J. Pumfrey, P. Fenelon, Experience with the application of HAZOP to computer-based systems, in: COMPASS95 Proceedings of the Tenth Annual Conference on Computer Assurance Systems Integrity, Software Safety and Process Security; IEEE, 1995, pp. 37–48.

49
[28] B. Dhillon, Failure modes and effects analysis—bibliography, Microelectronics Reliability 32 (5) (1992) 719–731.

[29] T. Ishimatsu, N. G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, H. Nakao, Modeling and Hazard Analysis Using STPA, International Association for the Advancement of Space Safety (IAASS) (Sep. 2010).

[30] H. E. Monkhouse, I. Habli, J. McDermid, An enhanced vehicle control model for assessing highly automated driving safety, Reliability Engineering & System Safety 202 (2020) 107061.

[31] A. Schnellbach, G. Griessnig, Development of the ISO 21448, in: European Conference on Software Process Improvement, Springer, 2019, pp. 585–593.

[32] R. Hawkins, C. Paterson, C. Picardi, Y. Jia, R. Calinescu, I. Habli, Guidance on the assurance of machine learning in autonomous systems (AMLAS), arXiv preprint arXiv:2102.01564 (2021).

[33] L. Gauerhof, R. Hawkins, C. Picardi, C. Paterson, Y. Hagiwara, I. Habli, Assuring the safety of machine learning for pedestrian detection at crossings, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2020, pp. 197–212.

[34] A. Abbas, S. Chalup, From Face Recognition to Facial Pareidolia: Analysing Hidden Neuron Activations in CNNs for Cross-Depiction Recognition, in: 2019 International Joint Conference on Neural Networks (IJCNN), 2019, pp. 1–8. doi:10.1109/IJCNN.2019.8852013.

[35] A. Nguyen, J. Yosinski, J. Clune, Deep neural networks are easily fooled: High confidence predictions for unrecognizable images, in: 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 427–436. doi:10.1109/CVPR.2015.7298640.

[36] A. Nguyen, J. Yosinski, J. Clune, Multifaceted Feature Visualization: Uncovering the Different Types of Features Learned By Each Neuron in Deep Neural Networks, arXiv:1602.03616 [cs] (May 2016). arXiv:1602.03616.
[37] M. T. Alexander Mordvintsev, Christopher Olah, Inceptionism: Going Deeper into Neural Networks, http://ai.googleblog.com/2015/06/inceptionism-going-deeper-into-neural.html.

[38] J. Guiochet, Hazard analysis of human–robot interactions with HA-ZOP–UML, Safety Science 84 (2016) 225–237. doi:10.1016/j.ssci.2015.12.017.

[39] Regulation No 79 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to steering equipment [2018/1947] (Dec. 2018).

[40] Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems, Tech. Rep. E/ECE/TRANS/505/Rev.3/Add.156, UNECE (Nov. 2019).

[41] E. J. Ward, Exploring perceptual illusions in deep neural networks, Journal of Vision 19 (10) (2019) 34b. doi:10.1167/19.10.34b.

[42] J. P. Espineira, J. Robinson, J. Groenewald, P. H. Chan, V. Donzella, Realistic LiDAR With Noise Model for Real-Time Testing of Automated Vehicles in a Virtual Environment, IEEE Sensors Journal 21 (8) (2021) 9919–9926. doi:10.1109/JSEN.2021.3059310.

[43] D. Vriesman, B. Thoresz, D. Steinhauser, A. Zimmer, A. Britto, T. Brandmeier, An Experimental Analysis of Rain Interference on Detection and Ranging Sensors, in: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), 2020, pp. 1–5. doi:10.1109/ITSC45102.2020.9294505.

[44] W. Ritter, M. Bijelic, T. Gruber, M. Kutila, H. Holzhüter, DENSE: Environment Perception in Bad Weather—First Results (2019) 143–159doi:10.1007/978-3-030-14156-1_12.

[45] AI DRIVR, Youtube, Can the FSD BETA drive blind? (Blocked sensor testing), https://www.youtube.com/watch?v=77cbSy-rBEQ (Nov. 2020).
Glossary

**ACC**  Adaptive Cruise Control. 21, 25, 34–37

**ADAS**  Advanced Driver Assistance Systems. 2, 3, 17–19, 21, 25

**ADS**  Automated Driving Systems. 3, 17–19

**AEB**  Automatic Emergency Breaking. 3, 11, 20, 21, 25, 40–42

**ALC**  Automated Lane Centring. 21, 25, 28–32, 36, 37

**ALKS**  Advanced Lane Keeping System. 2–5, 7, 9, 14, 21, 23, 25

**AMLAS**  Assurance of Machine Learning for Autonomous System. 12

**AS**  Autonomous Systems. 1, 2, 7, 8, 12, 36, 38

**AV**  Autonomous Vehicle. 2, 5–10, 16, 25, 36–38

**BSW**  Blind Sport Warning. 21

**CNN**  Convolutional Neural Network. 8, 9, 36

**DDM**  Date Driven Model. 9, 10, 17

**DDT**  Dynamic Driving Task. 3, 17, 21, 25

**DSR**  Derived Safety Requirement. 10–12, 17, 21, 25, 26, 36, 37

**FCW**  Forward Collision Warning. 21, 25, 26, 44–46

**FMEA**  Failure Modes and Effects Analyses. 11

**GPU**  Graphics Processing Unit. 8

**HAZOP**  Hazard and Operability Studies. 4, 7, 11, 13, 19, 20, 25, 36–38

**HDR**  High Dynamic Range. 7

**HISS**  Hazardous Internal System State. 6, 8, 13, 16, 23
LDW  Lane Departure Warning. 21, 25
ML  Machine Learning. 1–3, 5–10, 12, 14, 17
NHTSA  National Highway Traffic Safety Administration. 9
NN  Neural Network. 8, 14, 36
NTSB  National Transportation Safety Board. 9
ODD  Operation Design Domain. 5, 19
OTA  Over-the-Air. 9
RGB  Red, Green, Blue. 5, 7
SACE  Safety Assurance of Autonomous Systems in Complex Environments. 5, 12
SAE  Society of Automotive Engineers. 2–4, 6, 8–10
SAUS  Safety Assurance of Understanding in Autonomous Systems. 5, 17
SC  Safety Critical. 1, 3
SHARD  Software Hazard Analysis and Resolution in Design. 11, 13
SOTIF  Safety of the Intended Function. 12
STPA  System-Theoretic Process Analysis. 11, 12
UN ECE  United Nations Economic Commission for Europe. 25