Potential Sources of Sensor Data Anomalies for Autonomous Vehicles: An Overview from Road Vehicle Safety Perspective

Xiangmo Zhao [a, b] (xmzhao@chd.edu.cn), Yukun Fang [a] (fangyukun@chd.edu.cn), Haigen Min [a, b*] (hgmin@chd.edu.cn), Xia Wu [a, b] (wuxia@chd.edu.cn), Wuqi Wang [a] (wuqiwang@chd.edu.cn), Rui Teixeira [c] (rui.teixeira@ucd.ie)

[a] School of Information Engineering, Chang’an University, Xi’an 710064, China.
[b] Collaborative Innovation Center for Western China Traffic Safety and Intelligent Cooperative Control, Xi’an 710012, China.
[c] School of Civil Engineering, University College Dublin, Dublin D04 V1W8, Ireland.

[*] **Corresponding author: Haigen Min**
School of Information Engineering, Chang’an University, Xi’an, China
Email: hgmin@chd.edu.cn
Address: Weishui Campus of Chang’an University, Shangyuan Road, Weiyang District, Xi’an, Shaanxi Province, China. Zipcode: 710018

CRediT authorship contribution statement

Xiangmo Zhao: Conceptualization, Methodology, Resources, Supervision, Funding acquisition. **Yukun Fang:** Writing – original draft & review, Conceptualization, Methodology. **Haigen Min:** Writing – review, Conceptualization, Project administration, Funding acquisition. **Xia Wu:** Writing – review & editing, Funding acquisition. **Wuqi Wang:** Methodology, Writing – review & editing. **Rui Teixeira:** Writing –review & editing, Methodology.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research is supported in part by National Key Research and Development Program of China (2021YFB2501200), National Natural Science Foundation of China (61903046), Shaanxi Province Innovation Capability Support Plan-Innovative Talent Promotion Plan (2023KJXX-020), Natural Science Foundation of Shaanxi Province (2022JQ-663), Shaanxi Key R & D Program (2021GY-290), Youth Talent Lift Project of Shaanxi Association for Science and Technology (20200106), Fundamental Research Funds for the Central Universities, CHD (300102243202, 300102243501, 300102243711, 300102242103), European Union Horizon Europe (101103695), and China Scholarship Council (202206567012).

Abstract

Outstanding steps towards intelligent transportation systems with autonomous vehicles have been taken in the past few years. Nevertheless, the safety issue in autonomous vehicles is critical and remains to be fully solved. Sensor data provide information about the internal status of the system and the impact of its external environment, where the occurrence of sensor data anomalies indicates the existence of potential safety risks. Therefore, in this work, a taxonomy for potential sensor data anomaly sources from the perspective of road vehicle safety is proposed, motivated by the lack of a unified comprehensive taxonomy of sensor data anomaly identification for autonomous vehicles. In this context, sources are divided into; 1) fault or failure of the components or subsystems; 2) failure of the adaptability to the external environment; 3) cyber-attacks; and 4) faults or design deficiencies of sensors. Based on the taxonomy proposed, related works, and in particular, countermeasures for the four potential sources of sensor data anomalies in autonomous vehicles are then reviewed. In the context of providing a comprehensive discussion, other taxonomies of potential sources causing sensor data anomalies for autonomous vehicles and the issue of interpretability of sensor data anomalies are also discussed, providing insight into the strengths of the proposed taxonomy.

Keywords: autonomous vehicles, road vehicle safety, sensor data anomaly sources

Potential Sources of Sensor Data Anomalies for Autonomous Vehicles: An Overview from Road Vehicle Safety Perspective

Xiangmo Zhao[a,b], Yukun Fang[a], Haigen Min[a,b*], Xia Wu[a,b], Wuqi Wang[a], Rui Teixeira[c]

[a]*School of Information Engineering, Chang'an University, Xi'an, China*
[b]*Collaborative Innovation Center for Western China Traffic Safety and Intelligent Cooperative Control*
[c]*School of Civil Engineering, University College Dublin, Dublin, Ireland*

Abstract
Outstanding steps towards intelligent transportation systems with autonomous vehicles have been taken in the past few years. Nevertheless, the safety issue in autonomous vehicles is critical and remains to be fully solved. Sensor data provide information about the internal status of the system and the impact of its external environment, where the occurrence of sensor data anomalies indicates the existence of potential safety risks. Therefore, in this work, a taxonomy for potential sensor data anomaly sources from the perspective of road vehicle safety is proposed, motivated by the lack of a unified comprehensive taxonomy of sensor data anomaly identification for autonomous vehicles. In this context, sources are divided into; 1) fault or failure of the components or subsystems; 2) failure of the adaptability to the external environment; 3) cyber-attacks; and 4) faults or design deficiencies of sensors. Based on the taxonomy proposed, related works, and in particular, countermeasures for the four potential sources of sensor data anomalies in autonomous vehicles are then reviewed. In the context of providing a comprehensive discussion, other taxonomies of potential sources causing sensor data anomalies for autonomous vehicles and the issue of interpretability of sensor data anomalies are also discussed, providing insight into the strengths of the proposed taxonomy.

Keywords: autonomous vehicles, road vehicle safety, sensor data anomaly sources

1. Introduction

Autonomous vehicles (AVs) have been developed for decades and are expected to enable higher mobility, traffic efficiency, and environmental sustainability in transportation systems (Eskandarian, Wu, & Sun, 2021; Taiebat, Brown, Safford, Qu, & Xu, 2018). Regardless, issues of safety in autonomous vehicles still delay their full deployment, and safety risks with origin in both their internal systems and external environments need to be resolved. Sensor data provide observations about the operation status of the system and the impact of its external environment. These form the basis of the decision-making and control processes of autonomous vehicles. Anomalies in this context are defined as observations that deviate considerably from some established concept of normality (Ruff et al., 2021). In the context of autonomous driving, multiple works focus on sensor data anomaly detection but mostly lack the necessary insight into the interpretation of the identified anomalies (Alotibi & Abdelhakim, 2021; Fang, Min, Wang, Xu, & Zhao, 2020; Shi & Zhang, 2021; Wyk, Wang, Khojandi, & Masoud, 2020; Wang, Masoud, & Khojandi, 2021; Xiong et al., 2022). In such cases, technicians are able to know the existence of anomalies but may fail to understand what these anomalies indicate, which may then compromise adequate and efficient decision-making for the vehicle. Investigation of potential sources of sensor data anomalies combining the domain knowledge of autonomous driving is one of the alternatives to establish robust interpretation (Fang et al., 2023). However, at the moment there is still a lack of a unified comprehensive taxonomy for the sources of sensor data anomalies in autonomous driving. Thus, a taxonomy of potential sensor data anomaly sources for autonomous vehicles is proposed in the present work from the road vehicle safety perspective. Road vehicle safety means the absence of unreasonable risks of being involved in a vehicle accident (Koopman & Wagner, 2017), and sensor data anomalies indicate potential road vehicle safety risks. As a result, a taxonomy for the source of sensor data anomalies with such a perspective provides guidance for reducing safety risks, facilitating the exploration of the intrinsic relationship between road vehicle safety risks and sensor data anomalies as well as the design of countermeasures for each anomaly source that mitigate safety risks.

Once anomaly instances are captured, identifying the sources that have resulted in these facilitates the development of adequate corresponding countermeasures, reducing the overall potential safety risks for the vehicle. Such problem can be expressed as:

From the symptoms of sensor data in the autonomous driving scenario, can the possible sources that potentially lead to such sensor data anomalies be identified?

Note D as the data domain and S as the source domain. $a_1, a_2, \ldots, a_i, \ldots \in D$ are anomaly symptoms of the sensor data; $s_1, s_2, \ldots, s_j, \ldots \in S$ are potential sources that may lead to sensor data anomalies. There exists a complex mapping between the data domain D and the source domain S, and the question raised above can be summarized as finding a mapping f which maps the anomaly symptom a_i in the data domain to s_j in the source domain, formulated as

$$s_j = f(a_i) \tag{1}$$

$a_i \in D$ and $s_j \in S$ are not expected to be simple one-to-one mapping. Usually, a specific symptom a_i can be caused by different sources. Thus, using the symptom information from the data domain only (without any other domain knowledge) is commonly not sufficient to identify the specific source(s). The construction of the mapping f can be considered from the following two aspects:

1). To explore the potential sources that may lead to sensor data anomalies in the context of autonomous driving, narrowing the search scope in the definition of f.

2). To investigate the specific sources and construct corresponding domain knowledge for f.

Regarding 1), since the existence of anomalies indicates safety risks, potential sources of sensor data anomaly for autonomous driving can be considered from the road vehicle safety view and categorized in terms of it. As for 2), investigation of specific sources of sensor data anomaly for autonomous driving facilitates to establish the relationship between the sources and the anomalies, and is informative to design specific countermeasures for each source. In view of the above analysis, a taxonomy for sensor data anomaly sources is illustrated using a road vehicle safety perspective and countermeasures for each anomaly source are reviewed in this paper. The contribution of this overview is threefold:

- Illustration of the relation between road vehicle safety risk and sensor data anomalies.
- A taxonomy of potential sources that may lead to sensor data anomalies for autonomous vehicles from road vehicle safety perspective.
- A review of the current works in literature for each potential source and corresponding countermeasures.

As guidance, the proposed taxonomy that uses a road vehicle safety perspective is illustrated in Section 2, followed by the review of countermeasures for each potential sensor data anomaly source in Section 3. Some issues of relevance are discussed in Section 4, and finally, the main conclusions of the analysis developed are presented in Section 5.

2. Taxonomy of Potential Sensor Data Anomaly Sources with a Road Vehicle Safety Perspective

To respond to the issue formalized in Equation (1), the primary question that needs to be comprehensively answered is:

What can be the potential sources of sensor data anomalies in the context of autonomous driving?

Considering that the existence of anomalies indicates potential safety risks in the light of autonomous vehicles, the analysis of this issue can be started using a perspective centered on safety risks. In the context of road vehicle safety, unreasonable risks derive from insufficient measures that ensure, functional safety, safety of the intended functionality (SOTIF), and cybersecurity.

Functional safety, as described in ISO 26262, means the absence of unreasonable risks due to hazards caused by the malfunctioning behavior of electrical and electronic (E/E) systems (Silva, Bagbaba, Hamdioui, & Sauer, 2019; Debouk, 2019), where the fault or failure of the components or subsystems leads to functional safety risks.

SOTIF, as described in ISO 21448, describes the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons (Götze, Witt, Willer, & Raisch, 2023). Functional insufficiencies are, in fact, the manifestation of the incapability to adapt and cope with the system's current external environment, which then leads to SOTIF risks.

Cybersecurity, as described in the ISO/SAE 21434, specifies engineering requirements for cybersecurity risk management regarding the concept, product development, production, operation, maintenance, and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces (Costantino, Vincenzi, & Matteucci, 2022). Cybersecurity risks may result in functional safety risks (i.e., subsystems failures due to the cyber-attack) and SOTIF risks (i.e., failure in the adaptability to the environment due to the cyber-attack), and cybersecurity emphasizes the measures to protect the information, networks, and data against internal or external threats, aiming to ensure that only authorized individuals have access to specific information (Li & Liu, 2021).

Sensor data anomalies indicate unreasonable risks that derive from these three aspects, specifically,

- Non-premeditated data anomalies that affect what the vehicle is capable to do in a foreseen or unforeseen scenario of operation, and what safety issues relate to these. In this case, sensor anomalies reflect the safety risks of the normal operation of the vehicle and its contribution to potentially compromising road vehicle safety, which is related to functional safety.
- Non-premeditated data anomalies that affect what the vehicle intends to do, not affecting what it is capable to do, and what are the foreseen or unforeseen ways that it may fulfil its fully capable functionality. In this case, sensor anomalies reflect the safety risks of the insufficiency of fulfilling the intended functionalities of the vehicle, and such insufficiency may disrupt road vehicle safety. This is related to the SOTIF.
- Premeditated anomalies that affect the vehicle capabilities and/or its intention, where the vehicle functionalities are affected by an intentional and malicious way. This is an issue of cyber-security or any other issue that relates to deliberate data manipulation.

Sensor data reflect the operation status of the system and the impact of the external environment only in the condition that the sensors themselves function normally (Min et al., 2023). In practice, the occurrence of sensor data anomalies indicates different underlying risks in distinct circumstances. A sensor may be working at its full functionality or not. If the sensor is healthy, then a data anomaly can indicate that something is effectively not functioning as expected in the system. This may generate a functional safety issue in the vehicles, and it describes the first source of potential data anomalies in autonomous vehicles, **1) fault or failure of the components or subsystems**. On the other hand, a sensor may still be working at its full functionality but have limited capability to produce a correct sensor reading in operation in specific circumstances (*e.g.*, perception sensors in extreme weather conditions). Hence it can be described that a correctly functioning sensor fails to collect required sensor readings owing to the breakdown in adaptability, such that the acquired quantity is unable to reflect the true status of the measured object, which originates the second type of source of anomalies in sensor readings, the **2) failure to adapt to the external environment**. This generates the risk of SOTIF, as the sensor is not able to fulfil its functionality despite operating as expected. However, sensors do not always function correctly, and data anomalies, may have sources with origin from incorrect functioning of the sensors. First, cyber-attacks can change the profile of data, and generate data anomalies that bypass sensors. The sensor in this circumstance may or may not be compromised, but its acquired data are intentionally tampered with, which generates the third source of data anomaly, **3) cyber-attacks**. Finally, a sensor may be simply faulty or have design deficiencies, which generate the fourth source of data anomalies, **4) faults or design deficiencies of sensors**. Both 3) and 4) can generate functional risk and/or SOTIF risks that compromise road vehicle safety. In terms of the above analysis, this paper summarizes from the road vehicle safety perspective the following four sources of sensor data anomalies in the context of autonomous vehicles (as illustrated in Fig. 1):

1) fault or failure of the components or subsystems;
2) failure of the adaptability to external environment;
3) cyber-attacks;
4) faults or design deficiencies of sensors.

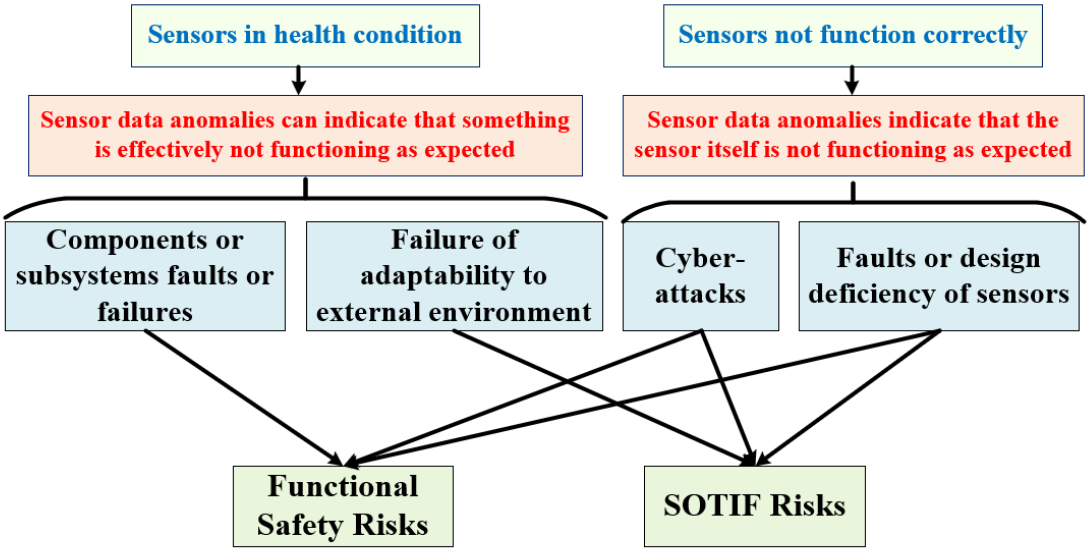

Fig. 1. Illustration of the sensor data anomaly sources for autonomous driving from the road vehicle safety perspective.

Having an explicit description of these four potential sources is informative to design specific countermeasures for each type of potentially road vehicle safety compromising issue based on data anomalies. At the same time, having the explicitly defined four sources of sensor data anomalies in a taxonomy is insightful for the transversal design of countermeasures, as when designing methods to diagnose sensor data anomalies, it is important to be aware of potential sources of data anomaly such that robust measures can be designed. As such, the following section reviews previous works on the countermeasures for sensor data anomalies deriving from each source, where the employed strategies for each case are discussed in depth.

3. Countermeasures for Potential Sensor Data Anomaly Sources

With the potential sources of sensor data anomalies for autonomous vehicles being classified, it is then possible to investigate these sources and construct corresponding domain knowledge for each category. In the present section, related works of the four potential sources, i.e., sensor data anomalies caused by 1) fault or failure of the components or subsystems; 2) failure of the adaptability to external environment; 3) cyber-attack; 4) faults or design deficiencies of sensors, and corresponding countermeasures for each are investigated. Related works from journal and conference papers were searched, and database or searching tools including *IEEE Xplore*, *Science Direct*, *Web of Science*, *ACM Digital Library*, *Scopus*, *arXiv*, and *Google Scholar* were utilized for literature collection. A two-level keywords tree (Guo et al., 2017; Zhang et al., 2022) was constructed to collect related published papers, shown in Fig. 2.

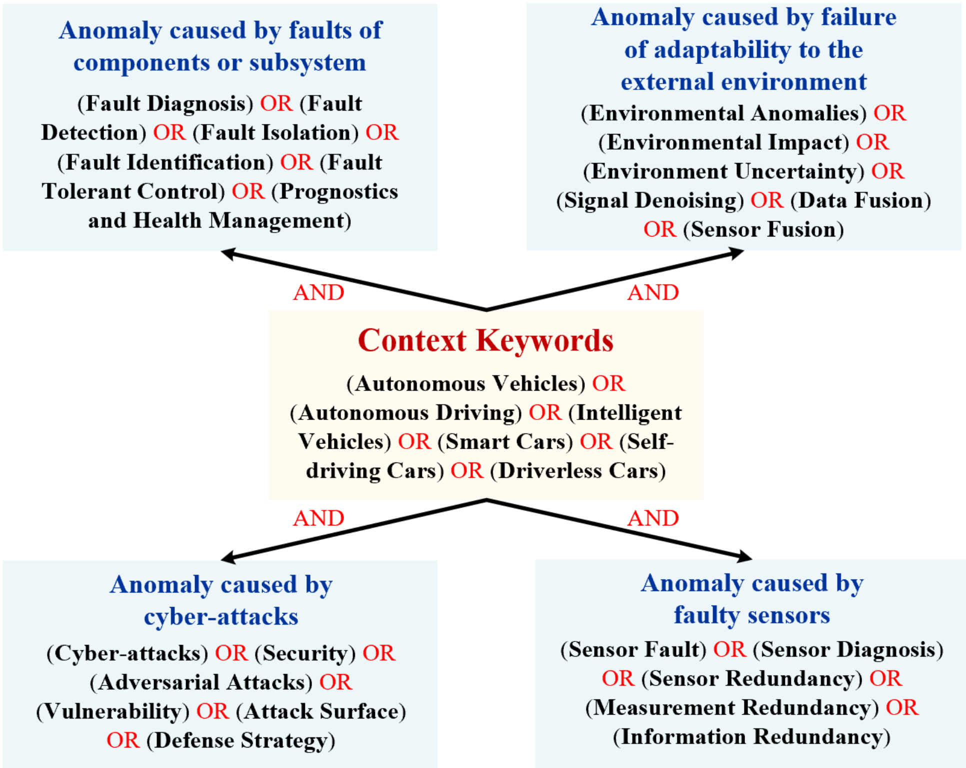

Fig. 2. The two-level keywords tree for the collection of related published papers.

3.1 Countermeasures for Anomalies Caused by Faults of Components or Subsystems

A fault is defined as an unpermitted deviation of at least one characteristic property or parameter of the system from the acceptable/usual/standard condition (Schrick, 1997), and failures can be regarded as severe faults of a system. Faults or failures bring safety risks to the normal operation of the vehicle and lead to anomalies in the observations, which is related to functional safety. Fault diagnosis, fault-tolerant control (FTC), and prognostic health management (PHM) are the three most employed countermeasures to handle the safety risk caused by the fault or failure of specific components or subsystems.

3.1.1 Fault Diagnosis

Fault diagnosis is to determine what faults occur, involving interpreting the current status of the system given sensor readings and specific domain knowledge (Ardakani et al., 2016). It aims to provide available information about the faults or failures and generally comprises three main tasks: 1) fault detection, 2) fault isolation, and 3) fault identification. Fault detection involves checking whether there are malfunctions or faults in the system; fault isolation involves locating the faulty components/subsystems in the system, or the faulty variables in a monitored process; and fault identification involves determining the type, severity, and/or causes of the faults (Gao, Cecati, & Ding, 2015a). The fault diagnosis methods in practice are categorized as model-based, signal-based, data-driven, and knowledge-based methods, related to the way through which the designers develop knowledge about the fault in a system or a process, and to the techniques used to process the data (Gao, Ding, & Cecati, 2015). Definitions and characteristics (i.e., pros and cons) of these four categories are summarized in Table 1.

Table 1. Taxonomy of fault diagnosis methods

Category	Definition	Pros and Cons
Model-based	Monitor the consistency between the model-predicted outputs and the measured values of the system.	· Only a small amount of real-time data is required. · An explicit model representing the input–output relationship is required.
Signal-based	Extract features from the raw signals and compare the discrepancy between extracted features and that of the healthy system or process.	· Do not require an explicit or complete model. · Pays less attention to system dynamic inputs, whose diagnosis performance may be degraded under unknown input disturbances (Gao, Cecati, et al., 2015a).
Data-driven	Use a large volume of historical data to learn the underlying features of healthy system/process performance. Consistency between the features of an instance and that of the learned features is then checked for fault diagnosis.	· Do not require an explicit or complete model. · Highly depend on historic data and suffer from high computational costs.
Knowledge-based	Use a pre-existing knowledge base with facts, and an inference engine that applies reasoning methods to the known facts as means of fault diagnosis (Chi, Dong, Wang, Yu, & Leung, 2022).	· Do not require an explicit or complete model. · Establishment of the knowledge base can be challenging.

Model-based methods require a system model which explicitly describes the relationship among the system variables. With such a model, fault diagnosis algorithms are developed to monitor the consistency between the model-predicted outputs and the measured values of the system (Gao, Cecati, et al., 2015a). Table 2 summarizes several recent advances of model-based methods for fault diagnosis for autonomous vehicles. Models contain prior knowledge of a system or a process, and the literature in the context of autonomous vehicles indicates that such models can be established to describe the prior knowledge of :

1) **components/subsystems of an autonomous vehicle**, where the model depicts the properties of specific components or the dynamics of a particular system (Boulkroune, Aalst, Nunen, & Descas, 2019);

2) **a single autonomous vehicle,** where the model depicts the properties of a single vehicle from at least one of its facets, e.g., the kinematic and dynamic models to describe the motion characteristics of an autonomous vehicle (Fang, Min, et al., 2020; Lee et al., 2022; Oh & Yi, 2017);

3) **a group of collaborative autonomous vehicles**, where the model depicts the interaction relationship among these agents (Alotibi & Abdelhakim, 2021).

Table 2. Several recent advances of model-based methods for fault diagnosis of autonomous vehicles

Work	Summary	The object being modeled
Oh & Yi, 2017	Given the information of the preceding vehicle, a sliding mode observer based on the vehicle longitudinal kinematic model is employed to diagnose the acceleration faults.	· The vehicle longitudinal kinematic characteristics of a single vehicle
Boulkroune et al., 2019	An observer based on the electric drivetrain model was proposed to generate the residual signals and diagnose actuator and sensor faults for the electric vehicle.	· The dynamic characteristics of the electric drivetrain
Fang, Min, et al., 2020	A Kalman filter observer is proposed based on the linear kinematic vehicle bicycle model to predict the current position of the vehicle, and residuals between the prediction and the measurement are calculated to monitor whether the trajectory of the autonomous vehicle deviates from the expected trajectory.	· The kinematic characteristics of an autonomous vehicle
Alotibi & Abdelhakim, 2021	Vehicle kinematics and a cooperative adaptive cruise control (CACC) model were applied for fault diagnosis by checking the difference between the vehicle's own speeding decision and the platoon leader's, as well as the unexpected deviations between the output of the kinematic model and the leader's information.	· The kinematic characteristics of a single vehicle · The cooperative model between multiple agents (i.e., the CACC model)
Lee et al., 2022	A sliding mode observer based on the vehicle longitudinal kinematic model was developed for fault detection of the chassis system of an autonomous vehicle.	· The vehicle longitudinal kinematic model

Signal-based methods assume that faults of a system or process can be reflected in the measured signals, which extract features from the raw signal and a diagnostic decision is then made based on the symptom analysis and prior knowledge of the symptoms of the healthy systems (Gao, Cecati, et al., 2015a). Several related works using signal-based methods for fault diagnosis in the applications of autonomous vehicles are listed in Table 3, and from the table, it can be seen that signal processing techniques are usually applied to diagnose specific components or subsystems, for example, the vehicle engine (Wang, Ma, Zhu, Liu, & Zhao, 2013), the wheel system (Li, Liu, Guo, Zhang, & Wang, 2015), the battery system (Wang, Hong, Liu, & Zhang, 2017), the inertial measurement unit (Fang, Cheng, Dong, Min, & Zhao, 2020), etc. Besides, considering the complexity of the autonomous vehicles, signal processing techniques are often combined with other methods especially data-driven methods for fault diagnosis of autonomous vehicles, and it is usually employed for data preprocessing or feature extracting (Fang, Cheng, et al., 2020; Min, Fang, Wu, Xu, & Zhao, 2021; Wang et al., 2013).

Another potential application of signal-based techniques for fault diagnosis of autonomous vehicles is active fault diagnosis (AFD), where a suitably designed input signal is allowed to be injected into the dynamic processes so that faulty modes can be distinguished from normal modes, improving the detectability of potential faults (Gao, Cecati, & Ding, 2015b; Puncochar & Skach, 2018). To instantiate, Zhang et al. (2013) proposed an active fault diagnosis approach to isolate and evaluate the fault in the wheel system of the vehicle. Lopes & Araujo (2020) presented an active fault diagnosis method for the detection and identification of faults of vehicles in a platoon formation, where a probing signal was introduced as an auxiliary input that would be actively excited when necessary. In this method, a supervisor was designed to monitor the platoon behavior and activate the auxiliary input whenever the system's natural excitation was insufficient for a clear fault diagnosis, enhancing the detectability of potential faults in the system.

Table 3. Several related works using signal-based methods for fault diagnosis in the applications of autonomous vehicles

Work	Summary	Methodological approach & Object being diagnosed
Wang et al., 2013	Empirical mode decomposition (EMD) was applied to extract the fault features of the vehicle engine, and these features were then utilized to train a support vector machine (SVM) classifier to identify potential engine faults.	· EMD for fault feature extraction as the preceding procedure for SVM · Vehicle engine
Li et al., 2015	Wavelet packet autoregressive spectrum techniques were employed to diagnose the health status of the wheel system for an autonomous vehicle.	· Wavelet packet autoregressive spectrum · Wheel system of an autonomous vehicle
Wang et al., 2017	Shannon entropy was analyzed for the voltage signal to achieve the fault diagnosis and prognosis of the battery systems for an autonomous vehicle.	· Shannon entropy · Battery systems of an autonomous vehicle
Fang, Cheng, et al., 2020	Discrete wavelet transform (DWT) was applied for feature extraction and denoising for the inertial measurement unit (IMU) data to train an extreme learning machine (ELM) based autoencoder (AE) for fault detection.	· DWT for fault feature extraction and denoising for training data as the preceding procedure for ELM-based AE · Inertial measurement unit (IMU)
Min et al., 2021	EMD and DWT were adopted to filter the noise contained in the inertial navigation system (INS) data which were later utilized to train the Long Short-term Memory (LSTM) network for fault detection.	· EMD and DWT for signal denoising for training data as the preceding procedure for LSTM · Inertial navigation system (INS)

Data-driven methods start from where only a large volume of historic data is available, where such methods learn the underlying features of a system/process in terms of the historic data. Based on what the data-driven method has learned, consistency between the observed behavior and the learned one is checked to implement fault diagnosis (Gao, Cecati, et al., 2015b). Data-driven methods can be primarily categorized as statistical-analysis-based and nonstatistical-analysis-based methods. The former captures the key characteristics of the process by using statistical analysis, *i.e.*, it uses data to define statistics of interest for the process that can then be monitored for detection. The latter captures the features of a system or process by learning the patterns and dependencies in the data and searching for underlying changes to identify any potential deviations (without explicit statistical or probability quantities) from the known normal behavior of the system or process. Both approaches demand a large amount of data for accurate inference. Several recent advances of data-driven methods for fault diagnosis of autonomous vehicles are listed in Table 4, and it can be concluded that

1) Deep learning methods (i.e., varieties of deep neural networks) for fault diagnosis of autonomous vehicles have been widely investigated in the literature because of the powerful ability in nonlinear approximation and adaptive learning (Bahavan et al., 2020; Fang, Cheng, et al., 2020; Fang et al., 2023; Gomes & Wolf, 2019; Xiong et al., 2022; Xu & Lian, 2018; Zhang, Zhang, Liu, & Guo, 2018).

2) The objects to be diagnosed using data-driven methods can be: the components or subsystems of an autonomous vehicle (Bahavan et al., 2020; Ben Lakhal, Adouane, Nasri, & Slama, 2019; Fang, Cheng, et al., 2020; Gomes & Wolf, 2019; Xiong et al., 2022; Xu & Lian, 2018), a single autonomous vehicle (Fang, Min, et al., 2020; Fang et al., 2023; Senapati, Swain, Swain, & Khilar, 2023), or a group of collaborative autonomous vehicles (Zhang et al., 2018).

Table 4. Several recent advances of data-driven methods for fault diagnosis of autonomous vehicles

Work	Summary	Methodological approach & Object being diagnosed
Xu & Lian, 2018	Fully CNN was adopted to detect the faults for a multi-source integrated navigation system, using the measuring residual among multiple sources as the input.	· Convolutional neural network (CNN) · Diagnosis of the vehicle navigation system
Zhang et al., 2018	A threshold-based fault detection and repairing scheme using a dynamic Bayesian network (DBN) model was proposed, where the fault detection and repairing are achieved based on the temporal and spatial correlations of vehicles in a cooperative group.	· Dynamic Bayesian network (DBN) · Diagnosis of the vehicle in a cooperative group
Lakhal et al., 2019	Principal component analysis (PCA) was employed in the adaptive cruise control (ACC) system of the autonomous vehicle to diagnose the faults of a navigation system.	· Principal component analysis (PCA) · Diagnosis of the vehicle navigation system
Gomes & Wolf, 2019	A fault detection and diagnosis framework for autonomous vehicles in lateral and longitudinal controllers was presented using a Bayesian network.	· Bayesian network · Diagnosis of the lateral and longitudinal controllers
Fang, Min, et al., 2020	One-Class support vector machine (OCSVM) was adopted to train the boundary that separates the normal states and anomalous states of the vehicle to detect the potential operational state faults of autonomous vehicles.	· One-Class support vector machine (OCSVM) · Diagnosis of the status of a single autonomous vehicle
Fang, Cheng, et al., 2020	A reference model of the brake system for an autonomous vehicle was approximated through the training of a neural network that diagnoses the status of the brake system.	· Fully connected neural network · Diagnosis of the vehicle brake system
Bahavan et al., 2020	An LSTM-based forecaster was developed to diagnose the faults of the IMU, which predicted the next IMU vector using the previous three ones, and the prediction error that greater than a threshold indicated the potential IMU faults.	· Long Short-term Memory (LSTM) network · Diagnosis of the inertial measurement unit (IMU)
Xiong et al., 2022	An adaptive denoising residual network is proposed for fault diagnosis of steering actuators with reduced noise interference and improved accuracy.	· Residual network · Diagnosis of the steering actuator

Fang et al., 2023	An adversarial training technique (i.e., the generative adversarial network (GAN) architecture) was introduced in training a denoising shrinkage autoencoder to improve the performance of fault detection for an autonomous vehicle.	· GAN architecture & Autoencoder · Diagnosis of the status of a single autonomous vehicle
Senapati et al., 2023	A framework for automatic fault detection and classification using a cloud-based vehicular ad hoc network (VANET) was constructed, where support vector machine (SVM) and logistic regression were adopted for fault identification.	· SVM & Logistic regression · Fault identification of the vehicle based on VANET

Knowledge-based methods require a knowledge base with facts and an inference engine that applies reasoning methods to the known facts to diagnose the faults qualitatively or quantitatively, and are particularly well-suited for complex or multi-component systems/processes for which detailed mathematical models are not available (Chi et al., 2022). Applications of knowledge-based methods for fault diagnosis of autonomous vehicles are comparatively scarce in the literature due to the difficulty of the establishment of a knowledge base for the faults in autonomous driving applications. Some related works are listed in Table 5, and it can be seen that expert systems (Sandoval-Pillajo, Tarupi, Basantes, Granda, & García-Santillán, 2019), fuzzy systems (Gomez-Penate et al., 2018), failure mode effects and criticality analysis (FMECA) (Peng, Nie, Wang, Zhu, & Liu, 2020), and fault tree analysis (FTA) (Chen, Chen, Bisantz, Shen, & Sahin, 2023) are the potential tools for fault diagnosis of autonomous vehicles using knowledge-based methods.

Table 5. Several related works using knowledge-based methods for fault diagnosis of autonomous vehicles

Work	Summary	Methodological approach & Object being diagnosed
Gomez-Penate et al., 2018	A Takagi-Sugeno (TS) fuzzy system was employed to diagnose the components faults of the vehicle, where the proposed TS model considers the nonlinearity of the longitudinal velocity of the vehicle and parametric variation induced by the slope of the road.	· Fuzzy system · Diagnosis of components faults of a vehicle
Sandoval-Pillajo et al., 2019	An expert system module consisting of the stages of knowledge extraction, creation of the inference engine, and writing of production rules were proposed for the diagnosis of autonomous vehicle failures.	· Expert System. · Diagnosis of the failure of a single autonomous vehicle.
Peng et al., 2020	Failure mode effects and criticality analysis (FMECA) was adopted to qualitatively analyze the impact of several known faults on autonomous driving and isolate the faulty components or subsystems.	· Failure mode effects and criticality analysis (FMECA) · Diagnosis of several known faults of autonomous driving qualitatively
Chen et al., 2023	Fault tree analysis (FTA) was adopted to identify potential failure sources that led to the failure of the takeover when human interventions were required.	· Fault tree analysis (FTA) · Diagnosis of the factors that result in the failure of the takeover

Hybrid methods- Fault diagnosis methods in each category have their own advantages and disadvantages (see Table 1 and the above introduction of each). To leverage the strength of different fault diagnosis methods, an integration or combination of two or more categories is often exploited, which is often called a hybrid fault diagnosis approach. Several current works using hybrid methods for fault diagnosis of autonomous vehicles are listed in Table 6. From the table, it can be concluded that: 1) model-based and data-driven methods have been the most widely applied and are often combined to diagnose the faults in the applications of autonomous vehicles (Liao, Hashemi, Wang, & Yang, 2021; Shi & Zhang, 2021; Wang et al., 2021); 2) signal-based methods are often combined with other methods and utilized for data preprocessing or feature extracting (Fang, Cheng, et al., 2020; Gultekin, Cinar, Ozkan, & Yazici, 2022; Min et al., 2021; Wang et al., 2013); and 3). Knowledge-based methods are currently rarely seen in the literature for the combination with other methods in fault diagnosis of autonomous vehicles due to the difficulty in establishing the required knowledge base for various faults and efficient knowledge representation (Chi et al., 2022).

Table 6. Several recent works using hybrid methods for fault diagnosis of autonomous vehicles

Work	Summary	Methodological approach & Object being diagnosed
Wang et al., 2021	A car-following model was employed to describe the interaction among the vehicles in a platoon, and faults were detected and identified through employing previously-trained One-class SVM models utilizing the leading vehicle's information.	· Car-following model & One-class SVM · Diagnosis of a platoon consisting of a group of autonomous vehicles
Liao et al., 2021	A fault detection and recovery framework for automated driving systems was developed based on the combination of the vehicle dynamic model and multitask one-dimensional convolutional neural networks (MONN), where dynamic relations among measured physical quantities depicted by the vehicle dynamic model were introduced in the MONN as partial input features to train such a network.	· Vehicle dynamic model & CNN. · Diagnosis of a single autonomous vehicle.
Shi & Zhang, 2021	A system model to describe the dynamics of the autonomous vehicle is established, and this model is then applied to generate residual signals as the training data to train a support vector machine (SVM) classifier to diagnose faults.	· Vehicle dynamic model & SVM. · Diagnosis of a single autonomous vehicle.
Gultekin et al., 2022	A CNN-based data fusion approach that uses a short-time Fourier Transform is proposed for the detection and identification of operational faults in autonomous transfer vehicles.	· CNN & short-time Fourier Transform · Diagnosis of operational faults for autonomous transfer vehicles

3.1.2 Fault-tolerant Control

Fault tolerance is defined as the ability of a system to continue its operation regardless of faults (Amin & Hasan, 2019). A control system that can automatically compensate for a fault effect of the system components while maintaining the system functionality along with the desired level of overall performance is called a fault-tolerant control (FTC) system (Abbaspour, Mokhtari, Sargolzaei, & Yen, 2020; Yu & Jiang, 2015). FTC can be categorized as passive or active according to the dependency on the fault information. Passive FTC does not rely on fault information to control the system and is related to robust control, where a fixed controller is designed to be robust against a predefined fault in the system (Abbaspour et al., 2020; Yu & Jiang, 2015) and redundancy is integrated into the passive fault-tolerant control design to make it robust to potential faults (Yu & Jiang, 2015). Whereas, active FTC requires fault information provided by the fault diagnosis module. With the fault information, a supervisory controller decides how to modify the control structure and parameters to compensate for the influence of the occurred fault in the system (Abbaspour et al., 2020; Yu & Jiang, 2015). Several recent advances of FTC in the applications of autonomous vehicles are listed in Table 7, from which it can be inferred that both passive or active approaches to FTC have been widely employed in the applications of autonomous vehicles, ranging from applications to a single vehicle to a group of cooperative vehicles, and always aiming to guarantee the safety and stability of the system.

Table 7. Several recent advances of fault-tolerant control in the applications of autonomous vehicles

Work	Summary	Type, Approach & Object of FTC
Boukhari, Chaibet, Boukhnifer, & Glaser, 2019	A scheme for autonomous vehicle reliable spacing control was presented, where a nonlinear longitudinal model of the vehicle was described by a Lipschitz representation, and a state feedback integral controller was designed in terms of the representation.	· Passive FTC · State feedback integral controller · FTC for a single vehicle
Guo, Li, & Hao, 2020	An improved quadratic spacing policy was proposed to tackle the occurrence of actuator faults for the fault-tolerant control of a heterogeneous vehicular platoon.	· Passive FTC · Quadratic spacing policy · FTC for a heterogeneous vehicular platoon considering actuator faults
Cao, Tian, Ji, & Qiu, 2021	An FTC strategy for path trajectory guidance of autonomous vehicles considering faults in the braking actuator was developed, where a robust gain-scheduling linear parameter-varying (LPV) synthesis H_∞ fault-tolerant controller was designed to ensure the autonomous vehicle stability and safety in operation.	· Passive FTC · H_∞ controller · FTC for an autonomous vehicle considering faults in the braking actuator

Zhang et al., 2016	An active fault-tolerant control method for an electric vehicle with independent drive in-wheel motors was proposed, where a reconfigurable controller would be switched on to achieve optimal postfault performance after the fault was detected and estimated by the fault diagnosis mechanism.	· Active FTC · Fault-tolerance achieved by controller switch · FTC for an electric vehicle
Li, Zhang, & Wang, 2020	A data-driven lateral fault-tolerant control method consisting of a data-driven off-policy combined with adaptive control. The adaptive parameters were adjusted online to compensate for the actuator faults automatically.	· Active FTC · Data-driven off-policy & adaptive control · FTC for a single vehicle considering actuator faults
Zhang, Liang, & Zhang, 2020	An active fault tolerant control model of the ACC system was established based on both the fault-free dynamics and the fault dynamics of the system using model predictive control (MPC) framework, considering vehicle-borne millimeter wave radar faults.	· Active FTC · Fault-tolerance achieved by controller switch to adapt different dynamics · FTC for adaptive cruise control (ACC) system

3.1.3 Prognostic Health Management

Prognostic Health Management (PHM) is an integrated approach that elaborates on knowledge, information and data of structures, systems and components (SSCs) operation and maintenance, to enable 1) detecting equipment and process anomalies, 2) diagnosing degradation states and faults, 3) predicting the health state of the system in the future and estimate its remaining useful life (RUL) (Hu, Miao, Si, Pan, & Zio, 2022; Zio, 2022). PHM generally includes fault diagnosis and failure prognosis (Vachtsevanos, Lewis, Roemer, Hess, & Wu, 2006). It tends to emphasize the prognosis processes (Calabrese, Regattieri, Botti, & Galizia, 2019; Kordestani, Saif, Orchard, Razavi-Far, & Khorasani, 2021), with diagnosis as a prerequisite to prognosis. Considering that fault diagnosis for autonomous vehicles has already been discussed in Section 3.1.1, only the content concerning failure prognosis in autonomous vehicles will be surveyed in this section. Failure prognosis means prediction of the future status of the faulty component(s) and estimation of the remaining useful lifetime based on the available information, highlighting prediction of the future state of damage rather than focusing on the diagnosis of the current state of damage (Mojtaba Kordestani, Samadi, Saif, & Khorasani, 2018). Some related works about prognostic health management in the applications of autonomous vehicles are listed in Table 8. From these works, it can be inferred that:

1) Most of the current research about PHM for autonomous driving focuses on the prognosis of specific components or subsystems (Lee, Sung, Han, Yoo, & Lee, 2023; Makke & Gusikhin, 2019; Venkatesan, Manickavasagam, Tengenkai, & Vijayalakshmi, 2019; Zhang, Tang, DeCastro, Roemer, & Goebel, 2014) and works of PHM for the whole vehicle are comparatively rare in the literature (Gomes & Wolf, 2021; Safavi, Safavi, Hamid, & Fallah, 2021). The review paper provided by Nguyen et al. (2019) further validates this inference, and in which the prognosis of battery systems and suspension systems was then particularly discussed;

2) The taxonomy presented in Table 1 (i.e., model-based methods, signal-based methods, data-driven methods, and knowledge-based methods) also suits PHM (Kordestani et al., 2021).

Table 8. Several previous works about prognostic health management in the applications of autonomous vehicles

Work	Summary	Object being prognosed & Methodological approach
Zhang et al., 2014	The prognosis of the battery was integrated into a mission planning scheme, where the state-of-charge of a battery was monitored and predicted by a particle-filtering-based prognostic algorithm, and the predicted state-of-charge and remaining useful life of the battery was used in the mission planning to minimize mission failure risk.	· Prognosis of the battery · Particle-filtering for RUL prediction

Makke & Gusikhin, 2019	A modeling framework for connected vehicle prognosis for dynamic systems that allows addressing connectivity limitations and memory constraints was demonstrated, which was based on a hybrid prognostic approach combining in-vehicle physics-based data aggregation model and cloud-based data-driven prognosis leveraging cross-vehicle and external data sources.	· Prognosis of the dynamic systems of connected vehicles · In-vehicle physics-based data aggregation model & Cloud-based data-driven methods
Venkatesan et al., 2019	The health monitoring and prognosis of a permanent magnet synchronous motor (PMSM) of the vehicle is developed by creating an intelligent digital twin, where an artificial neural network and fuzzy logic were used for mapping inputs distance, time of travel of the vehicle, outputs casing temperature, winding temperature, time to refill the bearing lubricant, percentage deterioration of magnetic flux to compute RUL of the permanent magnet.	· Prognosis of the permanent magnet synchronous motor · Artificial neural network and fuzzy logic for RUL prediction
Safavi et al., 2021	A CNN was used to capture the features of faulty signals and construct a health index (HI) for the system, and a Temporal Fusion Transformer (TFT) network was then employed to forecast the system's health status.	· Prognosis of a single autonomous vehicle · Temporal Fusion Transformer (TFT) for predicting the future health status of the system
Gomes & Wolf, 2021	A hierarchical component-based health system with fault detection, diagnosis, and prognosis was presented, where Dynamic Bayesian Network (DBN) was employed for the prognosis of the vehicle using the health monitoring data from different components.	· Prognosis of a single autonomous vehicle · Dynamic Bayesian Network (DBN) for predicting future states of the system
Lee et al., 2023	The process to diagnose the anomaly and to evaluate the remaining useful life of the chassis system of the vehicle under autonomous driving conditions was established, where deteriorated behavior was monitored with KNN (K-nearest neighbor) and GMM (Gaussian Mixture Model), and the remaining useful life was estimated by a Gaussian process.	· Prognosis of the chassis system of the vehicle · KNN and GMM for status monitoring and Gaussian process for RUL prediction

3.2 Countermeasures for Anomalies Caused by the Failure of Adaptability to the External Environment

The lack of capability to adapt to the external environment indicates the insufficiency of specific functions of the system, leading to the mentioned SOTIF risks and resulting in sensor data anomalies. For example, the positioning data provided by the Global Navigation Satellite System (GNSS) receiver in the scenarios of tunnel or urban canyon navigation can be inaccurate due to the functionality limitations of the GNSS system, and not due to any intrinsic failure of components. Improving the adaptability to the external environment of an autonomous vehicle, in fact, enhances the functionality of the system to deal with the uncertainties raised by the environment. The impact of the environment on the perception sensors should be particularly researched as they are the direct interfaces of the autonomous vehicle to the external environment. In this context, the transversal design of countermeasures can be considered from the following aspects:

1) Exploring the impact of particular environmental factors on specific perception sensors and compensating the performance to account for it;

2) Characterizing the uncertainty introduced by the external environment and developing strategies to deal with the uncertainty such that it does not compromise functionality.

3.2.1 Exploring the Impact of Environmental Factors on Perception Sensors

The purpose of exploring the impact of particular environmental factors on specific perception sensors is to enhance the functionality of the system to deal with negative impacts caused by the external environment. Related works are listed in Table 9, where it can be inferred that the sensitivity of each perception sensor to diverse factors varies. For example, the performance of the sensors using radio waves to perceive the environment will degrade due to the multipath effect (He, Guo, Lu, & Lu, 2014), and cameras are particularly sensitive to illumination conditions (Venkata & Naskar, 2018). An overview of the physical fundamentals, electromagnetic spectrum, and principle of operation for the sensors in an autonomous vehicle's perception system was presented in (Vargas, Alsweiss, Toker, Razdan, & Santos, 2021), where effects of different weather conditions (precipitation, fog, lightning, dust storm, etc.) on sensors were analyzed in-depth. The interested reader is directed to the work of (Vargas et al., 2021) for a more comprehensive description of this issue.

Table 9. Some previous works exploring the impact of particular environmental factors on specific perception sensors in the applications of autonomous vehicles

Work	Summary	Studied Sensor & Environmental Factors
Ruike, Xiaobo, Kexiang, & Huihui, 2012	The influence of the rain backscattering enhancement on millimeter-wave (MMW) radar detection performance was studied, and the experimental results showed that the MMW radar detection performance could be degenerated severely due to the backscattering enhancement of rain.	· Millimeter-wave radar · Impact of the rain backscattering on MMW radar
He et al., 2014	The effects of multipath propagation on the positioning performance of received GNSS signals were researched, with results indicating the degradation of positioning performance when multipath signals were present, causing position error from several meters to tens of meters.	· GNSS receiver · Impact of the multipath propagation on GNSS signals
Filgueira, Gonzalez-Jorge, Laguela, Diaz-Vilarino, & Arias, 2017	Experiments of quantifying the impact of rain on LiDAR measurements were conducted, with results showing that the detected LiDAR intensity and the sampled points would attenuate with the increase of the rain intensity.	· LiDAR · Impact of the rain intensity on the LiDAR intensity
Jokela, Kutila, & Pyykonen, 2019	The impact of fog and snow on the LiDAR performance was investigated, where performance decreased the denser the fog and the further the target in the fog chamber tests, and viewing distance was shortened in the turbulent snow tests.	· LiDAR · Impact of the fog and snow on LiDAR performance
Abdo, Hamblin, & Chen, 2022	LiDAR sensors were tested in adverse weather conditions (i.e., fog, rain, and snow) to understand how extreme weather affects data collection, with the results indicating that fog severely affected lidar performance; rain too had some effect on the performance; snow did not affect lidar performance.	· LiDAR · Impact of adverse weather conditions (i.e., fog, rain, and snow) on LiDAR performance
Venkata & Naskar, 2018	Experiments to assess the impact of illumination conditions on cameras were implemented and proposed an image filtering-based technique to eliminate the adverse effects of scene illumination.	· Camera · Impact of illumination conditions on cameras
Vargas et al., 2021	The effects of different weather conditions (precipitation, fog, lightning, dust storm, etc.) on the perception systems (including RADAR, LiDAR, ultrasonic, camera, and GNSS) of an autonomous vehicle were addressed, where physical fundamentals, electromagnetic spectrum, and principles of operation of these perception sensors were utilized to quantify the impact of different weather conditions on the performance of these sensors.	· RADAR, LiDAR, ultrasonic, camera, and GNSS · Impact of the precipitation, fog, lightning, and dust storm on these sensors

3.2.2 Strategies Dealing with the Environmental Uncertainty

Uncertainty was described as a state of limited information where it is impossible to exactly describe the studied agent (Hullermeier & Waegeman, 2021). Environmental uncertainty can be understood as the lack of complete information about the environment. Uncertainty also arises from the natural randomness of processes. It is usually categorized as aleatory (may appear in the context of autonomous driving described as statistical) uncertainty and epistemic (may appear in the context of autonomous driving described as systematic) uncertainty. The former refers to the notion of randomness, that is, the variability in the outcome of an experiment which is due to inherently random effects; the latter refers to uncertainty caused by a lack of knowledge, i.e., the lack of information of the epistemic state for an agent (Hullermeier & Waegeman, 2021; Kiureghian & Didevsen, 2009). Noise introduced in the sensor data during the signal acquisition process may be a source of aleatory uncertainty, as it is related to natural randomness that appears in the experiments. In fundament, it relates to the fact that the same experiments repeated may still lead to different results, and it is a type of uncertainty that can be characterized through experience. On the other hand, the malfunction of certain sensors to provide information or calibration issues may lead to a source of epistemic uncertainty, as it clearly describes a state of limited knowledge about a certain acquired system variable. In such a case, further acquisition of information may lead to its reduction as a better state of knowledge about a variable or process can be achieved. Methods to reduce the uncertainty caused by the environment in the applications of autonomous driving primarily include, but are not exclusive to,

1) *signal denoising*;

2) *data fusion*;

These have the ultimate goal of achieving redundancy and highly accurate information systems that mitigate both aleatory and epistemic uncertainties. Signal denoising allows the aleatory uncertainty to be reduced, while data fusion allows the epistemic uncertainty with data from different sources and at different fidelities to be decreased (Teixeira, Nogal, & O'Connor, 2021). Both techniques are widely employed in autonomous driving and several recent advances that include application of these two are listed in Table 10 and Table 11, respectively. Other alternatives to reduce the effects of uncertainty may include measures for updated information acquisition or control of uncertainty and its propagation. It is also noted that there is a number of research on sensor signal denoising and sensor data fusion that can inform further research in these topics and in the scope of autonomous vehicles. The interested reader is directed to the works of (Han, Meng, Omisore, Akinyemi, & Yan, 2020; Krishnamurthi, Kumar, Gopinathan, Nayyar, & Qureshi, 2020; Rasti, Scheunders, Ghamisi, Licciardi, & Chanussot, 2018; Xie, Colonna, & Zhang, 2021) for reviews on signal denoising and (Gupta & Fernando, 2022; Meng, Jing, Yan, & Pedrycz, 2020; Munir, Blasch, Kwon, Kong, & Aved, 2021; Zhang, Jiang, Yue, Wan, & Guizani, 2022) for reviews on sensor data fusion, with application to other areas, and that may provide further insight on applications to autonomous vehicles.

For signal denoising in the applications of autonomous vehicles, it can be inferred from Table 10 that denoising techniques can be developed in different domains, such as the time domain (Fang et al., 2023), and the time-frequency domain (Fang, Cheng, et al., 2020). Machine learning methods, and in particular deep learning, are also widely researched in the literature on this topic (Dodda et al., 2023; Duan, Yang, & Li, 2021; Fuchs, Rock, Toth, Meissner, & Pernkopf, 2021; Liu et al., 2022; Wang et al., 2021).

For data fusion in the applications of autonomous driving, it can be inferred from Table 11 that, the data to be fused can be from either the vehicle sensors (e.g. LiDAR, camera, GNSS, IMU, etc.) or other sources, like the roadside infrastructure (Manogaran et al., 2021) or cloud information (Liu et al., 2022). The data fusion approaches show great diversity (including but not limited to, Kalman filter based methods, weight-based methods, machine learning methods, in particular, deep learning techniques), and the selection of the methods should consider multiple factors, such as the characteristics of the sensor data, the computation cost, the rapidness of its response, among others.

Table 10. Several recent advances on uncertainty reduction through signal denoising in applications of autonomous vehicles

Work	Summary	Object being denoised & Methodological approach
Fang, Cheng, et al., 2020	Discrete wavelet transform (DWT) was employed to denoise the micro-electro-mechanical system inertial measurement unit (MEMS-IMU) data.	· Denoising for MEMS-IMU data · Discrete wavelet transform (DWT)
Duan et al., 2021	An adaptive radius outlier removal filter based on principal component analysis (PCA) was developed for denoising point cloud data.	· Denoising for LiDAR point cloud data · An outlier removal algorithm based on PCA

Wang et al., 2021	A de-raining and denoising convolutional neural network (CNN) was proposed to improve the accuracy of object detection in rainy conditions.	· Denoising for image data · Convolutional neural network (CNN)
Fuchs et al., 2021	A Complex-Valued Convolutional Neural Network (CVCNN) was proposed for radar signal denoising, where the issue of mutual interference between radar sensors was addressed.	· Denoising for radar data · CNN-based
Roriz, Campos, Pinto, & Gomes, 2022	A weather denoising method called Dynamic light-Intensity Outlier Removal (DIOR) was proposed, which combines two approaches of the state-of-the-art, i.e., the dynamic radius outlier removal (DROR) and the low-intensity outlier removal (LIOR).	· Denoising for LiDAR point cloud data · Outlier removal algorithms
Liu et al., 2022	A lightweight network for large-scale point cloud denoising was proposed, which combines the *k*-nearest neighbors (KNN) algorithm, the multi-layer perceptron (MLP), and the long short-term memory network (LSTM).	· Denoising for LiDAR point cloud data · Artificial neural network based methods combining KNN, MLP, and LSTM
Fang et al., 2023	Savitzky–Golay filters were applied for online denoising of the inertial measurement unit (IMU) data.	· Denoising for IMU data · Savitzky–Golay filters
Dodda et al., 2023	A fully unsupervised network (i.e., U-Net) was proposed to denoise the photon-counted 3D sectional images under extremely low light level conditions.	· Denoising for image data · U-Net under extremely low light level conditions

Table 11. Several recent advances on uncertainty reduction through data fusion in applications of autonomous vehicles

Work	Summary	Data being fused & Methodological approach
Geng & Liu, 2020	An improved weight assignment method for multi-sensor data fusion was presented, where GNSS, visual odometer, and LiDAR data were fused for robust fault-tolerant path tracking.	· Fusion of GNSS, visual odometer, and LiDAR data · Weight assignment fusion
Pi et al., 2020	A cooperative tracking framework was presented, where data from GNSS, IMU, camera, and V2X communication were fused based on Kalman filtering for security enhancement.	· Fusion of GNSS, IMU, camera, and V2X communication data · Kalman filtering
Manogaran et al., 2021	Data from the vehicle sensors and road sensors were fused based on the proposed multi-variate diffusion algorithm in the connected environment, focused to diminish errors in assimilating data in different time variations and input sources.	· Fusion for the data from vehicle sensors and road sensors · Multi-variate diffusion algorithm
Bai, Li, Huang, & Chen, 2021	A robust multi-object detection and tracking method for moving objects was proposed, using the maximum posterior estimation method for radar and camera data fusion	· Fusion of radar and camera data · Maximum posterior estimation
Liu et al., 2022	Data fusion for radar and camera data based on the joint data probabilistic data-association (JPDA) method was developed to deal with severe weather.	· Data fusion for radar and camera data · Joint data probabilistic data-association (JPDA)
Cui et al., 2022	Methods of image and point cloud data processing using deep learning techniques were reviewed, where camera-LiDAR fusion methods in depth completion, object detection, semantic segmentation, tracking, and online cross-sensor calibration were illustrated in detail.	· Data fusion for image and point cloud data · Review of deep learning methods for image and point cloud data fusion
Xiao, Codevilla, Gurram, Urfalioglu, & Lopez, 2022	A fusion scheme of RGB information (provided by the camera) and depth information (provided by LiDAR) based on convolutional neural network (CNN) architecture was presented, which learned a direct mapping from input raw sensor data to vehicle control signals.	· Data fusion for image data and LiDAR data · Convolutional neural network (CNN)
Liu et al., 2022	A vision-cloud data fusion architecture was proposed, integrating camera image and Digital Twin information from the cloud, where a depth evaluation algorithm and a distance matching algorithm were proposed for the fusion.	· Fusion of camera image and Digital Twin information from the cloud · Depth evaluation algorithm & Distance matching algorithm
Roy et al., 2023	Several deep learning based frameworks (including MLPs and CNNs) of fusing different modalities (image, radar, acoustic) were developed through the exploitation of complementary latent embeddings for surrounding vehicle detection and tracking.	· Fusion of image, radar, and acoustic data · Multi-layer perceptron (MLP) & convolutional neural network (CNN)
Gao, Zhang, & Xiong, 2022	A multi-scale selective kernel fusion (MSSKF) method was proposed, where the techniques of multi-scale convolution and selective kernel were employed to complete the fusion of camera and LiDAR data.	· Fusion of camera and LiDAR data · Multi-scale convolution & Selective kernel

3.3 Countermeasure for Anomalies Caused by Cyber-Attacks

Cyber-attacks lead to cybersecurity risks that can further cause functional safety risks (e.g., software faults due to a cyber-attack) and SOTIF risks (e.g., degradation of specific functions due to falsification of data), leading to sensor data anomalies. The cyber-security of autonomous driving is a source of vulnerabilities and several components of an autonomous vehicle can be targets of a cyber-attack, such as the on-board diagnostic port (OBD), controller area network (CAN), electronic control units (ECUs), and varieties of sensors including LiDAR, Radar, GNSS, Camera, among other. Cyber-attacks can be launched through either physical or remote access. Several attack models specific to autonomous vehicles have been summarized in (Pham & Xiong, 2021), listed in Table 12.

Table 12. Classification of cyber-attack models specific to autonomous vehicles (Pham & Xiong, 2021)

Cyber-attack Model	Target Component	Access Mode
Malicious OBD Devices	OBD	Physical
CAN Attacks through OBD	CAN	Physical
CAN Attack through Telematics ECUs	CAN	Remote
ECU Attacks through CAN	ECU	Physical
Attacks on Telematics ECUs	ECU	Remote
LiDAR Spoofing	LiDAR	Remote
LiDAR Jamming	LiDAR	Remote
Radar Spoofing	Radar	Remote
Radar Jamming	Radar	Remote
GNSS Spoofing	GNSS	Remote
GNSS Jamming	GNSS	Remote
Camera Blinding	Camera	Remote
Adversarial Images	Camera	Remote
Falsified Information on Network	Connection Mechanism	Remote
Network Denial of Service	Connection Mechanism	Remote

Significant research interest has been put on cyber-attacks specific to (connected and) autonomous vehicles, and several recently published surveys in this field are listed in Table 13. These outline the issue of cyber-security in autonomous vehicles as well as their countermeasures. Table 13 identifies some characteristics of the research on cyber-attacks specific to (connected and) autonomous vehicles, including:

1) Classifications of cyber-attack models are diverse. The attack model can be classified from the perspective of components (or subsystems), access modes, attack motives, employed attacking methods (Kim, Kim, Jeong, Park, & Kim, 2021; Limbasiya, Teng, Chattopadhyay, & Zhou, 2022; Pham & Xiong, 2021), among others.

2) The cybersecurity issue for (connected and) autonomous vehicles has the characteristics of both the traditional cybersecurity problems (e.g., the attacks on the communication interfaces and networks) and its specific cases (e.g., the adversarial attacks on deep learning models).

3) The objects being attacked are various, which can be the components or subsystems of the vehicle (Jing, Gao, Shahbeigi, & Dianati, 2022; Kim et al., 2021), the communication interfaces or networks (Dibaei et al., 2020; Jo & Choi, 2022), even the model/algorithms (Deng et al., 2021; Ilahi et al., 2021; Qayyum, Usama, Qadir, & Al-Fuqaha, 2020).

Table 13. Recently published works surveying cyber-attacks specific to (connected and) autonomous vehicles

Work	Summary	Key Points
Qayyum et al., 2020	A comprehensive analysis of the challenges posed by adversarial machine learning (ML) attacks for CAVs was illustrated, where ML used in CAVs, the taxonomy of the adversarial ML threats for CAVs, and surveys of adversarial ML attacks and defences were discussed.	· Attack and defence specific to adversarial machine learning (ML)

Dibaei et al., 2020	Attacks and defences for connected vehicles were addressed, where major security attacks on connected vehicles were illustrated, including denial-of-service (DoS) attacks, black-hole attacks, replay attacks, pseudospoofing attacks, impersonation attacks, malware, falsified-information attacks, and timing attacks, and available defences against these attacks were classified into four categories: cryptography, network security, software vulnerability detection, and malware detection.	· Attacks and defences for connected vehicles · Defence strategies including cryptography, network security, software vulnerability detection, and malware detection
Pham & Xiong, 2021	Taxonomies of attack models and defence strategies were presented respectively, where the former was classified from the perspective of CAV components (or subsystems), access modes, and attack motives, and the latter were generally divided into anomaly/intrusion detection-based methods, external information-based methods (i.e., getting information from other evolved entities, like other CAVs or connected infrastructures), and encryption methods.	· Taxonomy of attack models from the perspective of CAV components (or subsystems), access modes, and attack motives · Defence strategies including anomaly/intrusion detection-based methods, external information-based methods, and encryption methods
Kim et al., 2021	A taxonomy from the perspective of components tightly related to autonomous driving was presented, where the components were classified into the subsystem of autonomous control system (e.g., ECU, CAN, etc.), autonomous driving sensors (e.g., LiDAR, Radar, Camera, GNSS, etc.), and V2X communication, and the corresponding forms of attacks and defences were illustrated.	· Taxonomy from the perspective of components tightly related to autonomous driving · Attacks and defences for the components or subsystems
Deng et al., 2021	The attack and defence of deep learning-based autonomous driving systems were investigated, where cyber-attacks on onboard sensors, cloud service, and adversarial attacks were discussed, and countermeasures for each category were comprehensively discussed.	· Attacks and defences of deep learning-based autonomous driving systems · Attacks in this case including the cyber-attacks on onboard sensors, cyber-attacks on cloud service, and adversarial attacks
Ilahi et al., 2021	Adversarial attacks on deep reinforcement learning (DRL) based autonomous driving systems and the potential countermeasures to defend against attacks by these were investigated.	· Attack and defence specific to deep reinforcement learning (DRL) based autonomous driving systems
Jo & Choi, 2022	Attacks on CAN were surveyed, where attack surfaces including physical access-based attacks and wireless access-based attacks were illustrated in detail, and comprehensive attack models for automotive CAN were provided. Existing countermeasures were then divided into four categories: 1) preventative protection, 2) intrusion detection, 3) authentication, and 4) post-protection.	· Attacks and defences for CAN · Defence strategies including 1) preventative protection, 2) intrusion detection, 3) authentication, and 4) post-protection
Jing et al., 2022	Integrity monitoring (IM) frameworks for safety-critical navigation applications of connected autonomous vehicles were reviewed, where IM methods for GNSS and INS were underlined, as well as IM frameworks for map-assisted and wireless signal-augmented navigation systems.	· Integrity monitoring (IM) frameworks against the attacks on navigation system
Limbasiya et al., 2022	Attack detection and prevention strategies for connected and autonomous vehicles (CAVs) were systematically reviewed, where possible attacks in CAVs were introduced in terms of the employed attacking methods, and corresponding prevention strategies were then illustrated.	· Attacks and defences classified in terms of the attacking techniques for CAVs

3.4 Countermeasure for Anomalies Caused by Faulty Sensors

Sensor data reflects the operation status of the system and the impact of the external environment only in the condition that the sensors themselves function adequately. However, sensors themselves may also suffer from functional safety risks (e.g., sensor components faults) and SOTIF risks (e.g., functional insufficiencies because of design deficiencies), and malfunction of sensors can lead to unreasonable risks for autonomous driving, generating anomalous sensor data and lead to unexpected consequences in autonomous driving if the abnormal data are directly employed. Therefore, confirming the status of specific sensors is indispensable before using their outputs. Abbaspour et al. (2020) defined sensor faults as substantial errors in sensor readings while the plant (or measured object) properties remained the same, i.e., the sensor readings are unable to precisely reflect the operation status of the measured object. Gaddam et al. (2019) defined sensor faults as impaired data readings from failed or faulty sensors which were embedded within a device, addressing that the abnormal readings were caused by sensors, not by the attribute change of the measured object. Thus, the sensor status diagnosis problem can be described as:

How to diagnose the status of a specific data provider using the data provided by itself and/or other data providers?

Once the abnormal data patterns of an independent sensor's output are detected, it would be difficult to determine whether these are caused by sensor faults or some other reasons, given no prior knowledge. Therefore, enough information redundancy should be provided for sensor status diagnosis. Some related works that diagnose the sensor faults are listed in Table 14, with the literature indicating that potential redundancy information providers in the applications of autonomous vehicles can include 1) prior knowledge of a sensor or measured object, 2) redundant measurements, and 3) external information providers.

For redundant information provided by known facts (i.e., prior knowledge), the monitoring algorithm should diagnose the health status of the sensor based on the sensor's output and the given prior knowledge. The sources of the prior knowledge can be diverse, like the historical data (Mori, Sugiura, & Hattori, 2019), the knowledge base (Biswa Ranjan Senapati, Swain, & Khilar, 2022), etc.

Measurement redundancy can be utilized to detect and isolate a specific faulty sensor by checking the consistency of the redundant measurements, which can be provided by either homogeneous or heterogeneous sensors. The underlying assumption of faulty sensor isolation via consistency checking is that incorrect measurements are relatively rare, and correct measurements are likely to be consistent with one another (Duta & Henry, 2005). For a measurand with redundancy, each redundant measurement is independently representative of this measurand, and the variation tendency of each sensor output should be consistent when the measurand changes. Thus, any minority of measurements inconsistent with the majority is regarded as being incorrect, and the corresponding faulty sensors can be also isolated (Chen et al., 2016).

For information redundancy provided by external sources, the redundant information can be either stored in advance, like the prior knowledge of the vehicle stored in the cloud (Biswa Ranjan Senapati et al., 2022), or sent by specific entities with relations to the ego vehicle (e.g., vehicles in the same platoon, etc.) via vehicle-to-everything (V2X) communication (Biron, Dey, & Pisu, 2017; Qin, He, Yan, Deng, & Zhou, 2019).

Table 14. Several previous works on sensor fault diagnosis in the applications of autonomous vehicles

Work	Summary	Information Redundancy Provider
Jeong et al., 2015	Data provided by four-wheel speed sensors were utilized as redundancy, and the mean value of four speed sensors was used as a reference to distinguish failed wheel speed sensors. A sensor that had an excessive deviation compared with the reference would be regarded as faulty.	Speed sensors of four wheels
Biron et al., 2017	Information about other vehicles in a homogeneous platoon under a CACC strategy was applied as the reference to diagnose the sensor faults of the ego vehicle via vehicle-to-vehicle (V2V) communication.	Other vehicles in a platoon through V2V communication
Xu, Yan, Jia, Ji, & Liu, 2018	A multiple sensor consistency check scheme to enhance the security of autonomous vehicles was presented, which utilized the redundancy information from different sensors about the position of the vehicle to detect the inconsistency and found out faulty sensors.	Different sensors that collect vehicle position information
Qin et al., 2019	A distributed sensor fault detection and isolation scheme for the multi-vehicle system was presented, where each vehicle updated the state of the distributed observer by employing the measurements of itself and the transmitted state estimations from its neighbors. With this, the distributed fault detection observer in each vehicle was able to be sensitive to the faults of all vehicles in the system.	Neighbors that transmit state estimations of the ego-vehicle

Mori et al., 2019	A sensor fault diagnosis for an autonomous vehicle using a Student's *t*-distribution-based adaptive unscented Kalman filter was proposed, where the proposed filter evaluated each sensor by Hotelling's T^2 test utilizing the predicted sensor output based on the vehicle bicycle model and its covariance to assess the correlation between the data that was generated within the same sensor. Those with low correlation were regarded as faulty sensors.	Historical sensor data, specifically the correlation between data generated within the same sensor
Pan, Sun, Sun, & Gao, 2021	A sensor reliability evaluation method for an autonomous vehicle was proposed by calculating the global and local confidence of sensors, where the temporal and spatial correlation between sensor data was utilized to diagnose the local and global confidence level of sensor data in real-time, eliminate the fault data, isolate the faulty sensors, and ensure the accuracy and reliability of data fusion.	Temporal and spatial correlation between data from different sensors
Biswa Ranjan Senapati et al., 2022	A vehicular cloud was applied for fault diagnosis of the vehicle sensors, where the faulty sensors were isolated through check the consistency between the information provided by the onboard sensor and the prior knowledge stored in the cloud.	Prior knowledge stored in the cloud
Fang, Min, Lei, & Zhao, 2022	A residual consistency checking algorithm was proposed to quickly detect and isolate the failed sensor, where the vehicle attitude data provided by different sensors were utilized to calculate the residual and check the consistency between the output of one sensor and that of other sensors.	Different sensors that collect vehicle attitude information

3.5 Epilogue

To summarize, based on the taxonomy that categorizes the potential sources of sensor data anomalies as 1) fault or failure of the components or subsystems; 2) failure of the adaptability to external environment; 3) cyber-attack; 4) faults or design deficiencies of sensors, countermeasures for each potential sensor data anomaly source were reviewed in this section, and a brief summary of the countermeasures for each source is presented in Table 15. Having a review of these existing countermeasures is informative and insightful for the transversal design of the strategies to enhance the functionality of the system and reduce the road vehicle safety risks for autonomous vehicles.

Table 15. Summary of the potential anomaly sources in the context of autonomous vehicles, with countermeasures for each

Potential Source	Countermeasures	Summary
Faults of components or subsystems	Fault diagnosis	· To determine what faults occur, involving interpreting the current status of the system given sensor readings and specific domain knowledge (Ardakani et al., 2016) · Three main tasks: 1) fault detection, 2) fault isolation, and 3) fault identification · Taxonomy of fault diagnosis methods: 1) model-based, 2) signal-based, 3) data-driven, and 4) knowledge-based
	Fault-tolerant control (FTC)	· The ability of a system to continue its operation regardless of faults · Types: 1) passive FTC, and 2) active FTC
	Prognostic and health management (PHM)	· An integrated technology that elaborates on knowledge, information and data of structures, systems and components (SSCs) operation and maintenance, to enable 1) detecting equipment and process anomalies, 2) diagnosing degradation states and faults, 3) predicting the health state of the system in the future and estimate its remaining useful life (RUL) (Hu et al., 2022; Zio, 2022)
Failure of adaptability to the external environment	Exploring the impact of particular environmental factors on specific perception sensors	· To enhance the functionality of the system to deal with the negatives caused by the external environment and compensate the performance to account for it
	Characterizing the uncertainty introduced by the external environment and developing strategies to deal with the uncertainty	· Signal denoising to mitigate the aleatory uncertainty · Data fusion to reduce the epistemic uncertainty
Cyber-attacks	Investigating the attack model and corresponding defense strategies	· Potential objects being attacked: 1) components or subsystems; 2) communication interfaces or networks; 3) model/algorithms · Potential countermeasures: 1) cryptography, 2) network security, 3) software vulnerability detection, and 4) malware detection
Sensor faults or deficiency	Sensor self-diagnosis	· Enough information redundancy being provided for sensor self-diagnosis · Potential redundancy information providers: 1) prior knowledge of a sensor or measured object, 2) redundant measurements, and 3) external information providers

4. Discussion

4.1 Different Perspectives to Classify Sensor Data Anomaly Sources for Autonomous Vehicles

In the previous section, using a road vehicle safety perspective, potential sources causing sensor data anomalies in the applications of autonomous vehicles were identified to be: 1) fault or failure of the components or subsystems; 2) failure of the adaptability to the external environment; 3) cyber-attacks; 4) faults or design deficiencies of sensors. Sensor data provide the observations of the internal status and external surroundings of a system, and identification of anomaly sources for sensor data in a structured and systematic form is critical for the development of autonomous vehicles. Only when the source that causes data anomalies is pinpointed, can the design of the decision-making strategies be more tailored so as to ensure the safety and reliability of the system in operation. This drives the need for a structured taxonomy. To elaborate, if it is the fault or failure of the components/subsystems that causes the data anomalies, the focus should be on the faulty or failed modules, and corresponding fault diagnosis, fault-tolerant control, and prognostic health management strategies should be designed in terms of the characteristics of these modules. If it is the failure of the adaptability to the external environment that causes anomalies, the strategy to tackle these can range from applying methods that are robust to the environmental disturbances to designing algorithms that can improve the data quality, like sensor data fusion. If it is the cyber-attack that leads to data anomalies, countermeasures can involve enhancing encryption ability or updating the data security mechanisms. If it is a faulty sensor(s) that causes data anomalies, the focus should be on the sensor(s) and the mitigation decision-making strategies can involve abandoning the data obtained from the faulty ones.

Hence, the systematic taxonomy of potential sources that cause sensor data anomalies proposed facilitates clarification on the anomaly source once any anomalous symptoms are captured, providing support for decision-making. In this work, the proposed taxonomy is discussed from the road vehicle safety view, which is a primary driver of development for autonomous driving. Nevertheless, it is recognized that there are different ways to classify the sources from different angles, and some potential alternative taxonomies that can further boost the development of autonomous driving safe operation are discussed below.

Taxonomy from a complex system perspective - An autonomous vehicle can be regarded as a complex system, and from the perspective of a complex system, anomalies indicate the dissonance of multitudes of functions to adapt to complexity. For autonomous vehicles, complexity derives from both the system itself and its external environment. An autonomous vehicle consists of several modules and subsystems, and the scale and coupling of these subsystems lead to internal complexity. Moreover, the surroundings of road vehicles are highly dynamic with multiple uncertainties, which leads to further external complexity. Interactions among individual subsystems and between vehicles and their surrounding environment generate countless events whose combinatorial outcomes can exceed the response capacity of the system, leading to interaction complexity (Dekker, Cilliers, & Hofmeyr, 2011). Thus, in terms of the origin of complexity, anomaly sources can be further divided into: 1) internal subsystems, 2) external environment, and 3) interaction between the system and the environment.

Taxonomy based on the modules of autonomous vehicles- To achieve the function of autonomous driving, three basic modules are involved: perception, planning, and control. The perception module gathers information from the internal and external environment through various sensors. The planning module then computes the route and trajectory through decision-making based on the information provided by the perception module. The control module finally calculates the appropriate commands to control the actuators (e.g., steering wheel, gas pedal, brake pedal, etc.) that allow the vehicle to follow the trajectory (Eskandarian et al., 2021). Anomalies indicate malfunction, function insufficiency, or function dissonance in these modules. Therefore, according to the three primary modules involved in autonomous driving, anomaly sources can be categorized as: 1) perception module, 2) planning module, and 3) control module, as shown in Fig. 3

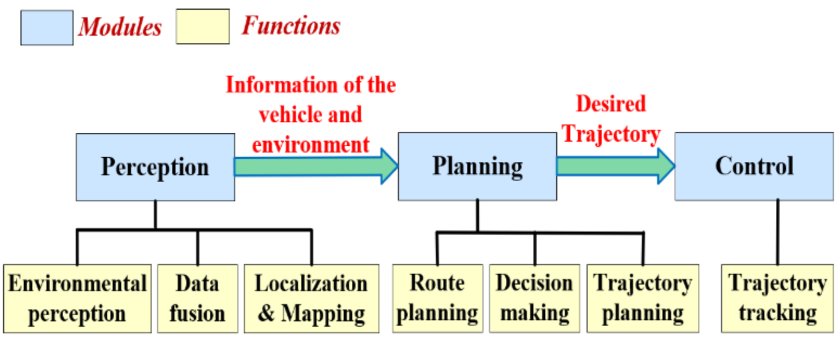

Fig. 3. Taxonomy for anomaly sources in terms of the modules of autonomous vehicles.

Taxonomy based on the control system perspective - Autonomous driving can be seen as a feedback process from the view of the automatic control, which gathers information about the ego-vehicle and the surroundings and adjusts the states of the system based on the information available and using specific algorithms to achieve the control objectives. This process can be depicted by a feedback control system in Fig. 4, consisting of the sensor, actuator, controller, and controlled object/process (Gao, Cecati, et al., 2015a). The controller here is understood as the combination of algorithms that handle internal and external information and generate decisions to achieve specific control objectives. Thus, from the control system perspective, anomalies for autonomous driving can be derived from: 1) sensors, 2) actuators, 3) controlled objects, and 4) algorithms that handle internal and external information and generate decision-making.

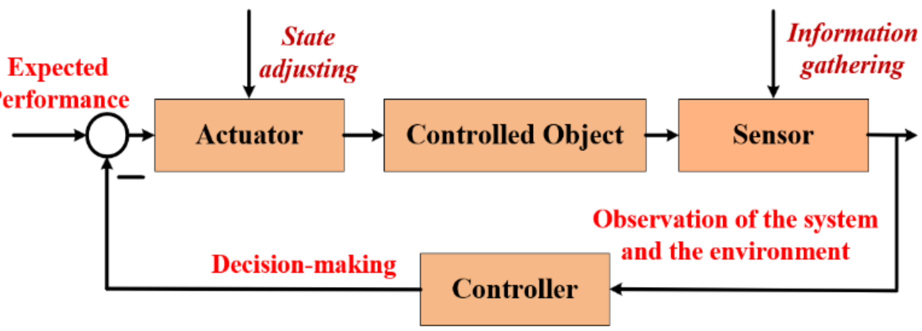

Fig. 4. Taxonomy for anomaly sources from the control system perspective.

To conclude, it is noted the proposed taxonomy and the taxonomies discussed above categorize sensor data anomaly sources for autonomous vehicles from different perspectives and correlate with each other, and the selection of the taxonomy should follow the characteristic of specific disciplines and applications to facilitate the design of strategies for guaranteeing safety and reliability. The proposed one is centered on road vehicle safety, which illustrates the relation between road vehicle safety risk and sensor data anomalies and benefits the transversal design of countermeasures to reduce unreasonable road vehicle safety risk.

4.2 Interpretability of Sensor Data Anomalies

As the sensor data anomalies are the output indicating safety risks, interpretation of the anomalies is particularly important in safety-critical areas, providing necessary information for decision-making. Interpretability of sensor data anomalies can be constructed primarily from two aspects (demonstrated in Fig. 5):

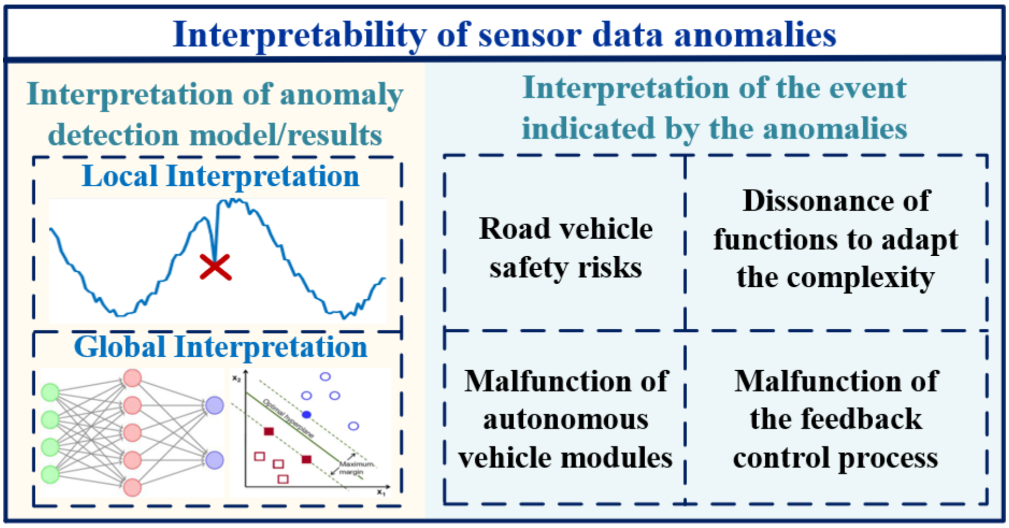

Fig. 5. Interpretability issue of sensor data anomalies for autonomous vehicles.

1) **interpretation of anomaly detection models and/or results, without considering the application background**.

It means to interpret the anomaly detection algorithms or models (especially the "black-box" models like artificial neural networks) and/or anomaly detection results. The former is referred as global interpretation, attempting to interpret the mechanism of anomaly detection algorithms/models, i.e., why the algorithms regard particular instances as anomalies; the latter can be referred as local interpretation, attempting to interpret why a specific data points are regarded as an anomaly (or, why a group of data points are regarded as anomalies) (Yepmo, Smits, & Pivert, 2022). Since the selection of algorithms or models can affect anomaly detection results, global and local interpretation are essential, especially for the "black-box" models, and interpretability, in this case, can be described as the ability to enable intuition and reasonability about the output of the algorithms to enhance end-users trust in the model output (Fang et al., 2023).

2) **interpretation of the event indicated by the anomalies, combining specific domain knowledge**.

It means to interpret the event indicated by the anomalies considering specific application background, where the event indicated by the anomalies can be interpreted from different perspectives. From the road vehicle safety view, sensor data anomalies indicate the existence of potential safety risks; from a complex system perspective, sensor data anomalies indicate the underlying dissonance of functions to adapt to the complexity; based on the modules of an autonomous vehicle, sensor data anomalies indicate the possible malfunction of autonomous vehicle modules; and from the control system perspective, sensor data anomalies indicate the potential malfunction of the control process. Clarifying anomaly sources and investigating each source combining the domain knowledge of autonomous driving is one of the critical aspects for seeking interpretation of the event indicated by the anomalies, facilitating the design of countermeasures to guarantee operation safety and reliability.

5. Conclusion

Focused on the issue of potential sources of sensor data anomaly for autonomous vehicles, a taxonomy of potential sensor data anomaly sources from the perspective of road vehicle safety is proposed, and corresponding countermeasures for each source are reviewed. It is motivated by the relevance between sensor data anomalies and road vehicle safety in autonomous driving, and the need for a systematic and structured approach to identify potential sensor data anomaly sources for further ensuing road vehicle safety. Since the existence of anomalies indicates potential safety risks, analysis of the sensor data anomaly sources can derive from the road vehicle safety perspective, including functional safety, SOTIF, and cybersecurity, with the sources being then divided, as proposed, into:

1) fault or failure of the components or subsystems;

2) failure of the adaptability to external environment;

3) cyber-attacks;

4) faults or design deficiencies of sensors.

Then, related works that cover countermeasures of the four potential sources are investigated. For anomalies caused by faults of components or subsystems, fault diagnosis, fault-tolerant control, and prognostic health management techniques in the applications of autonomous vehicles are reviewed. For anomalies caused by the failure of adaptability to the external environment, related works about exploring the relationship between specific perception sensors and environmental factors and measures to deal with environmental uncertainty are surveyed. For anomalies caused by cyber-attacks, several recently published reviews in this field are introduced to outline cyber-security issues in autonomous vehicles. For anomalies caused by faults or design deficiencies of sensors, countermeasures are reviewed considering strategies to provide information redundancy. Taxonomies of potential sources causing sensor data anomalies for autonomous vehicles and the issue of interpretability of sensor data anomalies are then further discussed. Alternative taxonomies are constructed and discussed, including 1) a complex system perspective, 2) an autonomous vehicle's module perspective, and 3) a control system viewpoint, providing insights to further boost developments in this field. Following, the interpretability of sensor data anomalies for autonomous vehicles is discussed, and two aspects are involved:

1) interpretation of anomaly detection models and/or results, without considering the application background;

2) interpretation of the event indicated by the anomalies, combining specific domain

knowledge.

For future work, the authors propose the continuation of the investigation of sensor data anomaly sources exploiting in a structured way on the basis of the proposed taxonomy, which can further extend and enrich the interpretability framework for sensor data anomalies for autonomous vehicle applications that are centered on safety issues, essential to the sustainable development of autonomous driving.

References

Abbaspour, A., Mokhtari, S., Sargolzaei, A., & Yen, K. K. (2020). A Survey on Active Fault-Tolerant Control Systems. *Electronics, 9*(9). doi:10.3390/electronics9091513

Abdo, J., Hamblin, S., & Chen, G. S. (2022). Effective Range Assessment of Lidar Imaging Systems for Autonomous Vehicles Under Adverse Weather Conditions With Stationary Vehicles. *ASME-ASME Journal of Risk and Uncertainty in Engineering Systems Part B-Mechanical Engineering, 8*(3). doi:10.1115/1.4052228

Alotibi, F., & Abdelhakim, M. (2021). Anomaly Detection for Cooperative Adaptive Cruise Control in Autonomous Vehicles Using Statistical Learning and Kinematic Model. *IEEE Transactions on Intelligent Transportation Systems, 22*(6), 3468-3478. doi:10.1109/Tits.2020.2983392

Amin, A. A., & Hasan, K. M. (2019). A review of Fault Tolerant Control Systems: Advancements and applications. *Measurement, 143*, 58-68. doi:10.1016/j.measurement.2019.04.083

Ardakani, M., Askarian, M., Shokry, A., Escudero, G., Graells, M., & Espuna, A. (2016). *Optimal Features Selection for Designing a Fault Diagnosis System*. Paper presented at the 26th European Symposium on Computer Aided Process Engineering (Escape), Pt A.

Bahavan, N., Suman, N., Cader, S., Ranganayake, R., Seneviratne, D., Maddumage, V., . . . Dehigaspitiya, S. (2020). Anomaly detection using deep reconstruction and forecasting for autonomous systems. *arXiv preprint arXiv:2006.14556*.

Bai, J., Li, S., Huang, L. B., & Chen, H. L. (2021). Robust Detection and Tracking Method for Moving Object Based on Radar and Camera Data Fusion. *IEEE Sensors Journal, 21*(9), 10761-10774. doi:10.1109/Jsen.2021.3049449

Ben Lakhal, N. M., Adouane, L., Nasri, O., & Slama, J. B. (2019). *Interval-based Solutions for Reliable and Safe Navigation of Intelligent Autonomous Vehicles*. Paper presented at the 2019 12th International Workshop on Robot Motion and Control (ROMOCO '19).

Biron, Z. A., Dey, S., & Pisu, P. (2017). *Sensor Fault Diagnosis of Connected Vehicles under Imperfect Communication Network*. Paper presented at the Proceedings of the ASME 9th Annual Dynamic Systems and Control Conference, 2016, Vol 1.

Boukhari, M. R., Chaibet, A., Boukhnifer, M., & Glaser, S. (2019). Two longitudinal fault tolerant control architectures for an autonomous vehicle. *Mathematics and Computers in Simulation, 156*, 236-253. doi:10.1016/j.matcom.2018.08.002

Boulkroune, B., van Aalst, S., van Nunen, E., & Descas, Y. (2019). *Fault detection and isolation system for four-wheels drive electric vehicles*. Paper presented at the 2019 4th Conference on Control and Fault Tolerant Systems (SYSTOL).

Calabrese, F., Regattieri, A., Botti, L., & Galizia, F. G. (2019). *Prognostic Health Management of Production Systems. New Proposed Approach and Experimental Evidences*. Paper presented at the 25th International Conference on Production Research Manufacturing Innovation: Cyber Physical Manufacturing.

Cao, X. H., Tian, Y. T., Ji, X. W., & Qiu, B. (2021). Fault-Tolerant Controller Design for Path Following of the Autonomous Vehicle Under the Faults in Braking Actuators. *IEEE Transactions on Transportation Electrification, 7*(4), 2530-2540. doi:10.1109/Tte.2021.3071725

Chen, K. T., Chen, H. Y. W., Bisantz, A., Shen, S., & Sahin, E. (2023). Where Failures May Occur in Automated Driving: A Fault Tree Analysis Approach. *Journal of Cognitive Engineering and Decision Making, 17*(2), 147-165. doi:10.1177/15553434221116254

Chen, Y. S., Yang, J. L., Xu, Y. H., Jiang, S. D., Liu, X. D., & Wang, Q. (2016). Status Self-Validation of Sensor Arrays Using Gray Forecasting Model and Bootstrap Method. *IEEE Transactions on Instrumentation and Measurement, 65*(7), 1626-1640. doi:10.1109/Tim.2016.2540942

Chi, Y. F., Dong, Y. J., Wang, Z. J., Yu, F. R., & Leung, V. C. M. (2022). Knowledge-Based Fault Diagnosis in Industrial Internet of Things: A Survey. *IEEE Internet of Things Journal, 9*(15), 12886-12900. doi:10.1109/Jiot.2022.3163606

Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-depth exploration of ISO/SAE 21434 and its correlations with existing standards. *IEEE Communications Standards Magazine, 6*(1), 84-92.

Cui, Y. D., Chen, R., Chu, W. B., Chen, L., Tian, D. X., Li, Y., & Cao, D. P. (2022). Deep Learning for Image and Point Cloud Fusion in Autonomous Driving: A Review. *IEEE Transactions on Intelligent Transportation Systems, 23*(2), 722-739. doi:10.1109/Tits.2020.3023541

da Silva, F. A., Bagbaba, A. C., Hamdioui, S., & Sauer, C. (2019). *Combining Fault Analysis Technologies for ISO26262 Functional Safety Verification*. Paper presented at the 2019 IEEE 28th Asian Test Symposium (ATS).

Debouk, R. (2019). Overview of the Second Edition of ISO 26262: Functional Safety-Road Vehicles. *Journal of System Safety, 55*(1), 13-21.

Dekker, S., Cilliers, P., & Hofmeyr, J. H. (2011). The complexity of failure: Implications of complexity theory for safety investigations. *Safety Science, 49*(6), 939-945. doi:10.1016/j.ssci.2011.01.008

Deng, Y., Zhang, T. H., Lou, G. N., Zheng, X., Jin, J., & Han, Q. L. (2021). Deep Learning-Based Autonomous Driving Systems: A Survey of Attacks and Defenses. *IEEE Transactions on Industrial Informatics, 17*(12), 7897-7912. doi:10.1109/Tii.2021.3071405

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S. G., Zhang, Y. X., . . . Yu, S. (2020). Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks, 6*(4), 399-421. doi:10.1016/j.dcan.2020.04.007

Dodda, V. C., Kuruguntla, L., Elumalai, K., Chinnadurai, S., Sheridan, J. T., & Muniraj, I. (2023). A denoising framework for 3D and 2D imaging techniques based on photon detection statistics. *Scientific Reports, 13*(1). doi:10.1038/s41598-023-

27852-5
Duan, Y., Yang, C. A. C. A., & Li, H. B. (2021). Low-complexity adaptive radius outlier removal filter based on PCA for lidar point cloud denoising. *Applied Optics, 60*(20), E1-E7. doi:10.1364/Ao.416341
Duta, M., & Henry, M. (2005). The fusion of redundant SEVA measurements. *IEEE Transactions on Control Systems Technology, 13*(2), 173-184. doi:10.1109/Tcst.2004.840448
Eskandarian, A., Wu, C. X., & Sun, C. Y. (2021). Research Advances and Challenges of Autonomous and Connected Ground Vehicles. *IEEE Transactions on Intelligent Transportation Systems, 22*(2), 683-711. doi:10.1109/Tits.2019.2958352
Fang, Y. K., Cheng, C. Y., Dong, Z., Min, H. G., & Zhao, X. M. (2020). *A Fault Diagnosis Framework for Autonomous Vehicles Based on Hybrid Data Analysis Methods Combined with Fuzzy PID Control*. Paper presented at the Proceedings of 2020 3rd International Conference on Unmanned Systems (ICUS).
Fang, Y. K., Min, H. G., Lei, X. P., & Zhao, X. M. (2022). *A Self-Fault Diagnosis Framework for Sensors of Connected and Automated Vehicles with Dynamic Environmental Impact Quantification*. Paper presented at the 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC).
Fang, Y. K., Min, H. G., Wang, W. Q., Xu, Z. G., & Zhao, X. M. (2020). A Fault Detection and Diagnosis System for Autonomous Vehicles Based on Hybrid Approaches. *IEEE Sensors Journal, 20*(16), 9359-9371. doi:10.1109/JSEN.2020.2987841
Fang, Y. K., Min, H. G., Wu, X., Lei, X. P., Chen, S. X., Teixeira, R., & Zhao, X. M. (2023). Toward Interpretability in Fault Diagnosis for Autonomous Vehicles: Interpretation of Sensor Data Anomalies. *IEEE Sensors Journal, 23*(5), 5014-5027. doi:10.1109/JSEN.2023.3236838
Filgueira, A., Gonzalez-Jorge, H., Laguela, S., Diaz-Vilarino, L., & Arias, P. (2017). Quantifying the influence of rain in LiDAR performance. *Measurement, 95*, 143-148. doi:10.1016/j.measurement.2016.10.009
Fuchs, A., Rock, J., Toth, M., Meissner, P., & Pernkopf, F. (2021). *Complex-valued Convolutional Neural Networks for Enhanced Radar Signal Denoising and Interference Mitigation*. Paper presented at the 2021 IEEE Radar Conference (Radarconf21): Radar on the Move.
Gaddam, A., Wilkin, T., & Angelova, M. (2019). *Anomaly Detection Models for Detecting Sensor Faults and Outliers in the IoT - A Survey*. Paper presented at the 2019 13th International Conference on Sensing Technology (ICST).
Gao, X., Zhang, G. Y., & Xiong, Y. J. (2022). Multi-scale multi-modal fusion for object detection in autonomous driving based on selective kernel. *Measurement, 194*. doi:10.1016/j.measurement.2022.111001
Gao, Z. W., Cecati, C., & Ding, S. X. (2015a). A Survey of Fault Diagnosis and Fault-Tolerant Techniques-Part I: Fault Diagnosis With Model-Based and Signal-Based Approaches. *IEEE Transactions on Industrial Electronics, 62*(6), 3757-3767. doi:10.1109/Tie.2015.2417501
Gao, Z. W., Cecati, C., & Ding, S. X. (2015b). A Survey of Fault Diagnosis and Fault-Tolerant Techniques-Part II: Fault Diagnosis With Knowledge-Based and Hybrid/Active Approaches. *IEEE Transactions on Industrial Electronics, 62*(6), 3768-3774. doi:10.1109/Tie.2015.2419013
Gao, Z. W., Ding, S. X., & Cecati, C. (2015). Real-Time Fault Diagnosis and Fault-Tolerant Control. *IEEE Transactions on Industrial Electronics, 62*(6), 3752-3756. doi:10.1109/Tie.2015.2417511
Geng, K. K., & Liu, S. P. (2020). Robust Path Tracking Control for Autonomous Vehicle Based on a Novel Fault Tolerant Adaptive Model Predictive Control Algorithm. *Applied Sciences, 10*(18). doi:10.3390/app10186249
Gomes, I. P., & Wolf, D. F. (2019). *A Health Monitoring System with Hybrid Bayesian Network for Autonomous Vehicle*. Paper presented at the 2019 19th International Conference on Advanced Robotics (ICAR).
Gomes, I. P., & Wolf, D. F. (2021). Health Monitoring System for Autonomous Vehicles using Dynamic Bayesian Networks for Diagnosis and Prognosis. *Journal of Intelligent & Robotic Systems, 101*(1). doi:10.1007/s10846-020-01293-y
Gomez-Penate, S., Lopez-Estrada, F. R., Valencia-Palomo, G., Osornio-Rios, R., Zepeda-Hernandez, J. A., Rios-Rojas, C., & Camas-Anzueto, J. (2018). Sensor Fault Diagnosis Observer for an Electric Vehicle Modeled as a Takagi-Sugeno System. *Journal of Sensors, 2018*. doi:10.1155/2018/3291639
Götze, M., Witt, M., Willer, N., & Raisch, F. (2023). Safety in Use and Automated Driving in Consideration of the New ISO 21448. *ATZ worldwide, 125*(4), 38-43.
Gultekin, O., Cinar, E., Ozkan, K., & Yazici, A. (2022). Multisensory data fusion-based deep learning approach for fault diagnosis of an industrial autonomous transfer vehicle. *Expert Systems with Applications, 200*. doi:10.1016/j.eswa.2022.117055
Guo, G., Li, P., & Hao, L. Y. (2020). Adaptive Fault-Tolerant Control of Platoons With Guaranteed Traffic Flow Stability. *IEEE Transactions on Vehicular Technology, 69*(7), 6916-6927. doi:10.1109/TVT.2020.2990279
Guo, H. X., Li, Y. J., Shang, J., Gu, M. Y., Huang, Y. Y., & Bing, G. (2017). Learning from class-imbalanced data: Review of methods and applications. *Expert Systems with Applications, 73*, 220-239. doi:10.1016/j.eswa.2016.12.035
Gupta, A., & Fernando, X. (2022). Simultaneous Localization and Mapping (SLAM) and Data Fusion in Unmanned Aerial Vehicles: Recent Advances and Challenges. *Drones, 6*(4). doi:10.3390/drones6040085
Han, S. P., Meng, Z., Omisore, O., Akinyemi, T., & Yan, Y. P. (2020). Random Error Reduction Algorithms for MEMS Inertial Sensor Accuracy Improvement-A Review. *Micromachines, 11*(11). doi:10.3390/mi11111021
He, C. Y., Guo, J., Lu, X. C., & Lu, J. (2014). *Multipath Performance Analysis of GNSS Navigation Signals*. Paper presented at the 2014 IEEE Workshop on Electronics, Computer and Applications.
Hu, Y., Miao, X. W., Si, Y., Pan, E. S., & Zio, E. (2022). Prognostics and health management: A review from the perspectives of design, development and decision. *Reliability Engineering & System Safety, 217*. doi:10.1016/j.ress.2021.108063
Hullermeier, E., & Waegeman, W. (2021). Aleatoric and epistemic uncertainty in machine learning: an introduction to concepts and methods. *Machine Learning, 110*(3), 457-506. doi:10.1007/s10994-021-05946-3
Ilahi, I., Usama, M., Qadir, J., Janjua, M. U., Al-Fuqaha, A., Hoang, D. T., & Niyato, D. (2021). Challenges and countermeasures for adversarial attacks on deep reinforcement learning. *IEEE Transactions on Artificial Intelligence, 3*(2), 90-109.
Jeong, Y., Kim, K., Kim, B., Yoon, J., Chong, H., Ko, B., & Yi, K. (2015). *Vehicle Sensor and Actuator Fault Detection Algorithm for Automated Vehicles*. Paper presented at the 2015 IEEE Intelligent Vehicles Symposium (IV).
Jing, H., Gao, Y., Shahbeigi, S., & Dianati, M. (2022). Integrity Monitoring of GNSS/INS Based Positioning Systems for Autonomous Vehicles: State-of-the-Art and Open Challenges. *IEEE Transactions on Intelligent Transportation Systems, 23*(9), 14166-14187. doi:10.1109/Tits.2022.3149373
Jo, H. J., & Choi, W. (2022). A Survey of Attacks on Controller Area Networks and Corresponding Countermeasures. *IEEE Transactions on Intelligent Transportation Systems, 23*(7), 6123-6141. doi:10.1109/Tits.2021.3078740
Jokela, M., Kutila, M., & Pyykonen, P. (2019). Testing and Validation of Automotive Point-Cloud Sensors in Adverse Weather Conditions. *Applied Sciences, 9*(11). doi:10.3390/app9112341
Kim, K., Kim, J. S., Jeong, S., Park, J. H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security, 103*. doi:10.1016/j.cose.2020.102150

Kiureghian, A. D., & Didevsen, O. (2009). Aleatory or epistemic? Does it matter? *Structural Safety, 31*(2), 105-112. doi:10.1016/j.strusafe.2008.06.020

Koopman, P., & Wagner, M. (2017). Autonomous Vehicle Safety: An Interdisciplinary Challenge. *IEEE Intelligent Transportation Systems Magazine, 9*(1), 90-96. doi:10.1109/Mits.2016.2583491

Kordestani, M., Saif, M., Orchard, M. E., Razavi-Far, R., & Khorasani, K. (2021). Failure Prognosis and Applications-A Survey of Recent Literature. *IEEE Transactions on Reliability, 70*(2), 728-748. doi:10.1109/Tr.2019.2930195

Kordestani, M., Samadi, M. F., Saif, M., & Khorasani, K. (2018). A new fault prognosis of MFS system using integrated extended Kalman filter and Bayesian method. *IEEE Transactions on Industrial Informatics*.

Krishnamurthi, R., Kumar, A., Gopinathan, D., Nayyar, A., & Qureshi, B. (2020). An Overview of IoT Sensor Data Processing, Fusion, and Analysis Techniques. *Sensors, 20*(21). doi:10.3390/s20216076

Lee, J., Oh, K., Yoon, Y., Song, T., Lee, T., & Yi, K. (2022). Adaptive Fault Detection and Emergency Control of Autonomous Vehicles for Fail-Safe Systems Using a Sliding Mode Approach. *IEEE Access, 10*, 27863-27880. doi:10.1109/Access.2022.3155738

Lee, K.-W., Sung, D.-U., Han, Y. H., Yoo, Y., & Lee, J. (2023). *Diagnosis and Prognosis of Chassis Systems in Autonomous Driving Conditions* (0148-7191). Retrieved from

Li, G. F., Liu, Y., Guo, Y. C., Zhang, F. L., & Wang, T. (2015). *Research on the Wheel system Fault Diagnosis of Special Vehicle Based on Wavelet Packet-AR Model Spectrum Technique*. Paper presented at the Proceedings of 8th International Conference on Intelligent Computation Technology and Automation (ICICTA 2015).

Li, Y., Zhang, H., & Wang, Z. P. (2020). *Data-Driven Lateral Fault-tolerance Control of Autonomous Vehicle System Using Reinforcement Learning*. Paper presented at the 2020 IEEE 16th International Conference on Control & Automation (ICCA).

Li, Y. C., & Liu, Q. H. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. doi:10.1016/j.egyr.2021.08.126

Liao, Y. W., Hashemi, E., Wang, T., & Yang, B. (2021). A Learning-Aided Generic Framework for Fault Detection and Recovery of Inertial Sensors in Automated Driving Systems. *IEEE Systems Journal, 15*(2), 3001-3011. doi:10.1109/Jsyst.2020.3004805

Limbasiya, T., Teng, K. Z., Chattopadhyay, S., & Zhou, J. Y. (2022). A systematic survey of attack detection and prevention in Connected and Autonomous Vehicles. *Vehicular Communications, 37*. doi:10.1016/j.vehcom.2022.100515

Liu, K. C., Xiao, A. R., Huang, J. X., Cui, K. W., Xing, Y., & Lu, S. J. (2022). *D-LC-Nets: Robust Denoising and Loop Closing Networks for LiDAR SLAM in Complicated Circumstances with Noisy Point Clouds*. Paper presented at the 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS).

Liu, Y. K., Wang, Z. R., Han, K., Shou, Z. Y., Tiwari, P., & Hansen, J. H. L. (2022). Vision-Cloud Data Fusion for ADAS: A Lane Change Prediction Case Study. *IEEE Transactions on Intelligent Vehicles, 7*(2), 210-220. doi:10.1109/TIV.2021.3103695

Liu, Z., Cai, Y. F., Wang, H., Chen, L., Gao, H. B., Jia, Y. Y., & Li, Y. C. (2022). Robust Target Recognition and Tracking of Self-Driving Cars With Radar and Camera Information Fusion Under Severe Weather Conditions. *IEEE Transactions on Intelligent Transportation Systems, 23*(7), 6640-6653. doi:10.1109/Tits.2021.3059674

Lopes, A., & Araujo, R. E. (2020). Active Fault Diagnosis Method for Vehicles in Platoon Formation. *IEEE Transactions on Vehicular Technology, 69*(4), 3590-3603. doi:10.1109/Tvt.2020.2968961

Makke, O., & Gusikhin, O. (2019). *Connected Vehicle Prognostics Framework for Dynamic Systems*. Paper presented at the Proceedings of the Third International Scientific Conference Intelligent Information Technologies for Industry (Iiti'18), Vol 1.

Manogaran, G., Balasubramanian, V., Rawal, B. S., Saravanan, V., Montenegro-Marin, C. E., Ramachandran, V., & Kumar, P. M. (2021). Multi-Variate Data Fusion Technique for Reducing Sensor Errors in Intelligent Transportation Systems. *IEEE Sensors Journal, 21*(14), 15564-15573. doi:10.1109/Jsen.2020.3017384

Meng, T., Jing, X. Y., Yan, Z., & Pedrycz, W. (2020). A survey on machine learning for data fusion. *Information Fusion, 57*, 115-129. doi:10.1016/j.inffus.2019.12.001

Min, H., Fang, Y., Wu, X., Xu, Z., & Zhao, X. (2021). Position prediction based on empirical mode decomposition and long short-term memory under global navigation satellite system outages. *China Journal of Highway Transport, 34*(7), 128. doi:10.19721/j.cnki.1001-7372.2021.07.010

Min, H. G., Fang, Y. K., Wu, X., Lei, X. P., Chen, S. X., Teixeira, R., . . . Xu, Z. G. (2023). A fault diagnosis framework for autonomous vehicles with sensor self-diagnosis. *Expert Systems with Applications, 224*. doi:10.1016/j.eswa.2023.120002

Mori, D., Sugiura, H., & Hattori, Y. (2019). *Adaptive Sensor Fault Detection and Isolation using Unscented Kalman Filter for Vehicle Positioning*. Paper presented at the 2019 IEEE Intelligent Transportation Systems Conference (ITSC).

Munir, A., Blasch, E., Kwon, J., Kong, J., & Aved, A. (2021). Artificial Intelligence and Data Fusion at the Edge. *IEEE Aerospace and Electronic Systems Magazine, 36*(7), 62-78. doi:10.1109/Maes.2020.3043072

Nguyen, V. D., Kefalas, M., Yang, K. F., Apostolidis, A., Olhofer, M., Limmer, S., & Back, T. (2019). A Review: Prognostics and Health Management in Automotive and Aerospace. *International Journal of Prognostics and Health Management, 10*(2).

Oh, K., & Yi, K. (2017). *A Longitudinal Model Based Probabilistic Fault Diagnosis Algorithm of Autonomous Vehicles Using Sliding Mode Observer*. Paper presented at the Proceedings of the Asme 26th Annual Conference on Information Storage and Processing Systems, 2017.

Pan, H. H., Sun, W. C., Sun, Q. M., & Gao, H. J. (2021). Deep Learning Based Data Fusion for Sensor Fault Diagnosis and Tolerance in Autonomous Vehicles. *Chinese Journal of Mechanical Engineering, 34*(1). doi:10.1186/s10033-021-00568-1

Peng, N., Nie, H., Wang, Q., Zhu, M., & Liu, Z. (2020). Study on the Fault Diagnosis System of Autonomous Vehicle and its Application. *Journal of Light Industry, 35*(05), 87-95. doi:10.12187/2020.05.012

Pham, M., & Xiong, K. Q. (2021). A survey on security attacks and defense techniques for connected and autonomous vehicles. *Computers & Security, 109*. doi:10.1016/j.cose.2021.102269

Pi, W., Yang, P. T., Duan, D. L., Chen, C., Cheng, X., Yang, L. Q., & Li, H. (2020). Malicious User Detection for Cooperative Mobility Tracking in Autonomous Driving. *IEEE Internet of Things Journal, 7*(6), 4922-4936. doi:10.1109/Jiot.2020.2973661

Puncochar, I., & Skach, J. (2018). A Survey of Active Fault Diagnosis Methods. *IFAC PapersOnline, 51*(24), 1091-1098. doi:10.1016/j.ifacol.2018.09.726

Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward. *IEEE Communications Surveys and Tutorials, 22*(2), 998-1026. doi:10.1109/Comst.2020.2975048

Qin, L. G., He, X., Yan, R., Deng, R. L., & Zhou, D. H. (2019). Distributed sensor fault diagnosis for a formation of multi-vehicle systems. *Journal of the Franklin Institute-Engineering and Applied Mathematics, 356*(2), 791-818. doi:10.1016/j.jfranklin.2017.11.020

Rasti, B., Scheunders, P., Ghamisi, P., Licciardi, G., & Chanussot, J. (2018). Noise Reduction in Hyperspectral Imagery: Overview and Application. *Remote Sensing, 10*(3). doi:10.3390/rs10030482

Roriz, R., Campos, A., Pinto, S., & Gomes, T. (2022). DIOR: A Hardware-Assisted Weather Denoising Solution for LiDAR Point Clouds. *IEEE Sensors Journal, 22*(2), 1621-1628. doi:10.1109/Jsen.2021.3133873

Roy, D., Li, Y. Y., Jian, T., Tian, P., Chowdhury, K., & Ioannidis, S. (2023). Multi-Modality Sensing and Data Fusion for Multi-Vehicle Detection. *IEEE Transactions on Multimedia, 25*, 2280-2295. doi:10.1109/Tmm.2022.3145663

Ruff, L., Kauffmann, J. R., Vandermeulen, R. A., Montavon, G., Samek, W., Kloft, M., . . . Muller, K. R. (2021). A Unifying Review of Deep and Shallow Anomaly Detection. *Proceedings of the IEEE, 109*(5), 756-795. doi:10.1109/Jproc.2021.3052449

Ruike, Y., Xiaobo, Z., Kexiang, L., & Huihui, M. (2012). *Study of the influence of rain backscattering enhancement on MMW radar performance.* Paper presented at the CSQRWC 2012.

Safavi, S., Safavi, M. A., Hamid, H., & Fallah, S. (2021). Multi-Sensor Fault Detection, Identification, Isolation and Health Forecasting for Autonomous Vehicles. *Sensors, 21*(7). doi:10.3390/s21072547

Sandoval-Pillajo, L., Tarupi, A., Basantes, A., Granda, P., & García-Santillán, I. (2019). *Expert system for diagnosis of motor failures in electronic injection vehicles.* Paper presented at the 2019 International Conference on Information Systems and Computer Science (INCISCOS).

Senapati, B. R., Swain, R. R., & Khilar, P. M. (2022). Hard and soft fault detection using cloud based vanet. In *Intelligent and Cloud Computing: Proceedings of ICICC 2021* (pp. 133-143): Springer.

Senapati, B. R., Swain, S., Swain, R. R., & Khilar, P. M. (2023). A heterogeneous fault diagnosis approach to enhance performance of connected vehicles. *International Journal of Communication Systems, 36*(4). doi:10.1002/dac.5414

Shi, Q., & Zhang, H. (2021). Fault Diagnosis of an Autonomous Vehicle With an Improved SVM Algorithm Subject to Unbalanced Datasets. *IEEE Transactions on Industrial Electronics, 68*(7), 6248-6256. doi:10.1109/Tie.2020.2994868

Taiebat, M., Brown, A. L., Safford, H. R., Qu, S., & Xu, M. (2018). A Review on Energy, Environmental, and Sustainability Implications of Connected and Automated Vehicles. *Environmental Science & Technology, 52*(20), 11449-11465. doi:10.1021/acs.est.8b00127

Teixeira, R., Nogal, M., & O'Connor, A. (2021). Adaptive approaches in metamodel-based reliability analysis: A review. *Structural Safety, 89*. doi:10.1016/j.strusafe.2020.102019

Vachtsevanos, G. J., Lewis, F., Roemer, M., Hess, A., & Wu, B. (2006). *Intelligent fault diagnosis and prognosis for engineering systems* (Vol. 456): Wiley Hoboken.

van Schrick, D. (1997). Remarks on terminology in the field of supervision, fault detection and diagnosis. *IFAC Proceedings Volumes, 30*(18), 959-964.

van Wyk, F., Wang, Y. Y., Khojandi, A., & Masoud, N. (2020). Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems, 21*(3), 1264-1276. doi:10.1109/Tits.2019.2906038

Vargas, J., Alsweiss, S., Toker, O., Razdan, R., & Santos, J. (2021). An Overview of Autonomous Vehicles Sensors and Their Vulnerability to Weather Conditions. *Sensors, 21*(16). doi:10.3390/s21165397

Venkata, U. S., & Naskar, R. (2018). Eliminating the effects of illumination condition in feature based camera model identification. *Journal of Visual Communication and Image Representation, 52*, 24-32. doi:10.1016/j.jvcir.2018.01.015

Venkatesan, S., Manickavasagam, K., Tengenkai, N., & Vijayalakshmi, N. (2019). Health monitoring and prognosis of electric vehicle motor using intelligent-digital twin. *Iet Electric Power Applications, 13*(9), 1328-1335. doi:10.1049/iet-epa.2018.5732

Wang, K., Chen, L., Wang, T., Meng, Q., Jiang, H., & Chang, L. (2021). *Image deraining and denoising convolutional neural network for autonomous driving.* Paper presented at the 2021 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS).

Wang, Y. S., Ma, Q. H., Zhu, Q., Liu, X. T., & Zhao, L. H. (2013). An intelligent approach for engine fault diagnosis based on Hilbert-Huang transform and support vector machine. *Applied Acoustics, 75*, 1-9. doi:10.1016/j.apacoust.2013.07.001

Wang, Y. Y., Masoud, N., & Khojandi, A. (2021). Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors. *IEEE Transactions on Intelligent Transportation Systems, 22*(3), 1411-1421. doi:10.1109/Tits.2020.2970295

Wang, Z. P., Hong, J. C., Liu, P., & Zhang, L. (2017). Voltage fault diagnosis and prognosis of battery systems based on entropy and Z-score for electric vehicles. *Applied Energy, 196*, 289-302. doi:10.1016/j.apenergy.2016.12.143

Xiao, Y., Codevilla, F., Gurram, A., Urfalioglu, O., & Lopez, A. M. (2022). Multimodal End-to-End Autonomous Driving. *IEEE Transactions on Intelligent Transportation Systems, 23*(1), 537-547. doi:10.1109/Tits.2020.3013234

Xie, J., Colonna, J. G., & Zhang, J. L. (2021). Bioacoustic signal denoising: a review. *Artificial Intelligence Review, 54*(5), 3575-3597. doi:10.1007/s10462-020-09932-4

Xiong, H. Y., Wang, Z. J., Wu, G. H., Pan, Y. L., Yang, Z. C., & Long, Z. N. (2022). Steering Actuator Fault Diagnosis for Autonomous Vehicle With an Adaptive Denoising Residual Network. *IEEE Transactions on Instrumentation and Measurement, 71*. doi:10.1109/Tim.2022.3199252

Xu, H. W., & Lian, B. W. (2018). Fault detection for multi-source integrated navigation system using fully convolutional neural network. *IET Radar Sonar and Navigation, 12*(7), 774-782. doi:10.1049/iet-rsn.2017.0424

Xu, W. Y., Yan, C., Jia, W. B., Ji, X. Y., & Liu, J. H. (2018). Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles. *IEEE Internet of Things Journal, 5*(6), 5015-5029. doi:10.1109/Jiot.2018.2867917

Yepmo, V., Smits, G., & Pivert, O. (2022). Anomaly explanation: A review. *Data & Knowledge Engineering, 137*. doi:10.1016/j.datak.2021.101946

Yu, X., & Jiang, J. (2015). A survey of fault-tolerant controllers based on safety-related issues. *Annual Reviews in Control, 39*, 46-57. doi:10.1016/j.arcontrol.2015.03.004

Zhang, B., Tang, L., DeCastro, J., Roemer, M., & Goebel, K. (2014). Autonomous vehicle battery state-of-charge prognostics enhanced mission planning. *International Journal of Prognostics Health Management, 5*(2).

Zhang, G. G., Zhang, H., Huang, X. Y., Wang, J. M., Yu, H., & Graaf, R. (2016). Active Fault-Tolerant Control for Electric Vehicles With Independently Driven Rear In-Wheel Motors Against Certain Actuator Faults. *IEEE Transactions on Control*

Systems Technology, 24(5), 1557-1572. doi:10.1109/Tcst.2015.2501354
Zhang, H., Liang, J., & Zhang, Z. Y. (2020). Active Fault Tolerant Control of Adaptive Cruise Control System Considering Vehicle-Borne Millimeter Wave Radar Sensor Failure. *IEEE Access, 8*, 11228-11240. doi:10.1109/Access.2020.2964947
Zhang, H. B., Zhang, Q., Liu, J. J., & Guo, H. Z. (2018). Fault Detection and Repairing for Intelligent Connected Vehicles Based on Dynamic Bayesian Network Model. *IEEE Internet of Things Journal, 5*(4), 2431-2440. doi:10.1109/Jiot.2018.2844287
Zhang, T. C., Chen, J. L., Li, F. D., Zhang, K. Y., Lv, H. X., He, S. L., & Xu, E. Y. (2022). Intelligent fault diagnosis of machines with small & imbalanced data: A state-of-the-art review and possible extensions. *ISA Transactions, 119*, 152-171. doi:10.1016/j.isatra.2021.02.042
Zhang, X., Cocquempot, V., Jiang, B., & Yang, H. (2013). *Active Fault Diagnosis based on Fault-Tolerant Control with Control Constraints for an Electric 4WD Vehicle*. Paper presented at the 2013 10th IEEE International Conference on Control and Automation (ICCA).
Zhang, Y., Jiang, C., Yue, B. L., Wan, J. F., & Guizani, M. (2022). Information fusion for edge intelligence: A survey. *Information Fusion, 81*, 171-186. doi:10.1016/j.inffus.2021.11.018
Zio, E. (2022). Prognostics and Health Management (PHM): Where are we and where do we (need to) go in theory and practice. *Reliability Engineering & System Safety, 218*. doi:10.1016/j.ress.2021.108119