IEEE Open Journal of
Intelligent Transportation Systems

Received 19 June 2021; revised 25 August 2021; accepted 20 October 2021. Date of publication 27 October 2021; date of current version 9 November 2021.

Digital Object Identifier 10.1109/OJITS.2021.3123305

Fault Injection in Model-Based System Failure Analysis of Highly Automated Vehicles

SAIF SALIH AND RICHARD OLAWOYIN

Industrial and Systems Engineering Department, Oakland University, Rochester, MI 48309, USA

CORRESPONDING AUTHOR: S. SALIH (e-mail: sysalih@oakland.edu)

ABSTRACT The active safety control systems of highly automated vehicles for SAE level 3 and higher are still not fully developed and facing some unresolved issues. The deployment of automated driving systems and the functional safety development present challenges in driver – machine control relationship when there is a system failure or malfunction. The current definition of the product development and controllability classes of the road vehicles functional safety (ISO26262) are not feasible in highly automated vehicles (HAV). This research developed an overview of fault or disturbance injection on the steering system of highly automated model to study the impact of steering system sensors malfunction. The approach was to study the fault propagation using a model-based engineering development in a virtual environment of MATLAB. Subsequently, the steering control system of automated vehicle was developed using an adaptive model predictive control structure to study the control system sensors failures on a system-feature level of the vehicle. It was concluded that the steering wheel angle sensor failure has a significant impact on the planned trajectory of the vehicle and thus it was classified as ASIL D, which represents the highest critical safety component and requires comprehensive safety mechanisms to meet the safety goals of the system. The study also introduced a new criterion for controllability classes suitable for highly automated systems based on the global vehicle position relative of the lane marker lines, to deal with the active safety systems and risk handling strategies. The drivers – vehicle control systems are changing significantly in SAE level 3 automated vehicle and above that driving functions are controlled by the vehicle control systems. This presents human factors challenge in this interactive system with moving to SAE levels 4 and 5. Hence, several human machine interfaces and scenario-based testing are introduced to mitigate any risk or safety uncertainty resulting from control handing-over between the driver and the vehicle control system.

INDEX TERMS Adaptive MPC, planned trajectory follow, fault injection, steering wheel angle sensor, controllability classes, human-machine interface (HMI) and ISO26262.

I. INTRODUCTION

AUTOMATED and intelligent transportation driving systems have attracted extensive attention and interest from academia, industry, and the public. The traffic safety, fuel efficiency and enhanced driver experience are the main motivations for automated and connected vehicles. The connected automated vehicles are considered as mitigations of issues such as traffic congestion, road safety, inefficient fuel consumption and pollutant emissions that current road transportation system suffers from [1]. There are still some challenges reported by the research group of [1] such as:

1. Ideal working conditions of the communication channel (e.g., no packet loss, communication failure, noise, etc.).
2. Perfect knowledge of vehicle dynamics (vehicle parameters, road friction conditions, etc.).
3. Perfect knowledge of the positions of the vehicles.

Hence, additional investigation is required to understand how the aforementioned uncertainties affect cooperating driving scenarios.

The society of automotive engineering (SAE) standard SAE J3016, also known as (surface vehicle **J3016** recommended practice), defines the dynamic driving

The review of this article was arranged by Associate Editor Fernando Auat Cheein.

task (DDT) as: "all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic" [2]. In the context of driving automation systems, SAE J3016 provides detailed definitions for six levels of driving automation, ranging from no driving automation (level 0) to full driving automation (level 5) clarifying the role of the (human) driver and/or the automated control system and the interaction between them. This leads to the definition of the automated driving system (ADS) that is defined as "the hardware and software components, subsystem and systems in forms of features that are collectively capable of performing the entire DDT on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD). Table 2.1 in SAE J3016 describes the higher driving automation system levels [2]. For instance, level 1 and 2 are defined as partial autonomy driving mode, which requires the driver to always execute or supervise the longitudinal and the lateral vehicle motion control (VMC). The conditional driving automation of level 3 is where the driver and the system can collaboratively exchange the vehicle control with the fallback feature if the automated system fails to hand over the control to the driver. Level 3 is considered as the breaking point between the low (level 1 and 2) and high (level 4 and 5) automation levels. Level 4 is referred to as a high driving automation, where the automated driving system performs all driving operation under specific driving modes and the fallback system can appropriately perform without any expectation of the driver to intervene. Full driving automation or level 5 is defined as sustained and unconditional performance by the automated driving system of the entire DDT and ODD. Thus, the driver, if presented, may perform other tasks while an onboard dedicated control system controls the vehicle's DDT or even there is no need for the driver in the vehicle at all [3]. The VMC is the system operative part of the object event detection and response (OEDR), it needs to be integrated in the ADS to provide status and feature capabilities of feasible maneuver and follow the planned trajectory from the start point A to the desired destination B. These subtasks are necessary to perform the DDT and to assure that the vehicle can be safely operated in higher automation mode such as SAE level 3, 4 or 5 [3]. The introduction of the on-board automated VMC increases the risks for hazards and hence the complexity of vehicle control architecture increases as well. The deployment of the automated VMC requires the capability to detect the environment, locate its position, and operate the vehicle to get to the specified destination safely without human input. This includes the perception system sensors such as camera, radars, light detection and ranging (LIDAR), global position systems (GPS), ultrasonic applications, and additional actuators such as active steering electric motors, electronic braking, and active suspensions systems. Vehicles equipped with these intelligent systems (perception, VMC and actuation) can identify obstacles on the road such as pedestrians or other moving vehicles such as blind zone detection and vehicle in the headway. Additionally, lane markers can be detected to keep the vehicle in the center of the lane by apply steering actuation to avoid lane departures, which is also known as lane keep assist (LKA) and lane departure warning (LDW).

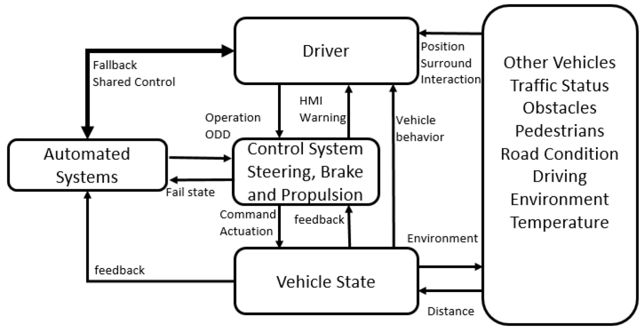

FIGURE 1. **Driving ecosystem interactions with boxes representation factors and arrows representing interaction direction and possibilities.**

Lin *et al.* [4] explained the architectural implications of autonomous driving system in detail from the perception perspective and lack any controller information because the perception system was linked to a planner and an action block [4]. A model-based safety analysis (MBSA) was performed for the autonomous driving system for the adaptive cruise control (ACC) controls longitudinal speed and LKA controls lateral trajectory [5]. It was concluded that the yaw rate and the longitudinal speed of ego vehicle are critical elements (because they appear in order 1 cutsets) of the simulated sequence events. Hence, they represent a single failure element and cause safety violation in case of malfunction and mishap. However, the main objective of the study was to study the traffic jam chauffeur using AltaRica language and Simfia software [5].

The vehicle to everything (V2E) and the Cooperative Systems (CS) are the most promising technology within the Intelligent Transportation Systems (ITS) framework. The word "cooperative" indicates that vehicles are collaborating with each other and with the surrounding environment and infrastructure, exploiting wireless communications such as vehicle to vehicle (V2V) feature using a dedicated short range communication (DSRC) protocol. The vehicle onboard active safety control systems are integrated with the Cooperative Systems architecture to mitigate any potential risk or hazards due to mishap or malfunction of the control systems. The interaction between the driver, control system and the environment in the driving ecosystem can be seen in Figure 1 [6].

It is clear that the driver and the automated system collaboratively exchange the ODD and the operation task to control the vehicle (bold bidirectional arrow), which represents the cooperative systems in the ITS framework.

The model predictive control (MPC) technology is an effective control strategy that can be systematically taken into consideration the future prediction, patterns and the system operation constrains in design and operation stages [7]. The capabilities of the MPC for controlling multivariable plants (vehicle actuators) and parameters using the initial state of the plant within every application-imposed constraint, i.e., minimum, and maximum values of speed, acceleration, steering positions, make it a suitable choice for autonomous driving applications, where the system faces dynamically changing environment and must satisfy crucial safety constraints. The current control action is obtained by solving on one at each sampling instant using an optimizer unit, starting with the initial state to generate a finite horizon open loop. The optimization yields an optimal control sequence and the first control in this sequence is applied to the plant. This is the main difference from the conventional control strategy, which utilizes a precomputed control law [8]. The first of such optimal moves is the control action applied to the plant at time t. At a time, t + 1, a new optimization is solved over a predefined and shifted prediction horizon [9]. Therefore, it operates in a receding horizon fashion, meaning that at each time step new measurements of the system and new predictions into the future are made by solving multi input datasets applied to the system which allows predicting the future system states based on the current states and control input [7], [10].

The main objective of the this research is to address the emerging technology challenges of the higher automated and electric vehicles steering system architecture integrated with the framework of the road vehicles functional safety standard ISO 26262 in the presence of the human machine interface (HMI). This requires special means in system design and validation during the run time of the automated vehicle control system. Therefore, the current work developed an adaptive MPC model to simulate the longitudinal and the lateral motion of the vehicle and follow a trajectory path using the adaptive MPC optimizer and prediction capabilities complaint with the ISO 26262 standard- Part 4 (Product development at the system level) implementation of the safety related function and behavior.

Due to the complexity and higher degree of freedom (DOF) level of the vehicle dynamic system motion, the multi-input, multi-output (MIMO) control system represented by the adaptive MPC block was chosen to satisfy the manipulated parameters out of the adaptive MPC controller such as: ego speed, steering wheel angle (SWA), and brake signal, etc. within the predefined constrains and limits that represent the traffic policy, the driving situation, trajectory and the minimum and maximum control parameters. The stability analysis of the vehicle dynamic is a major problem in the automotive technology that requires sophisticated control systems, optimizers and tuning capabilities with efficient implementation scheme and formation. Therefore, the steering system of higher automated vehicles has more safety challenges as the role of the driver (human) in vehicle control has been reduced.

In Section II, the research methodology was presented in this work and the high level of the adaptive MPC was explained. Two driving scenarios were generated and validated in a fully virtual environment and the model was deemed to be ready to perform the fault injection tests both in velocity and the steering wheel angle sensors. A new controllability criterion was introduced and defined based on the higher automated driving systems when the driver might not be part of the control loop in Section III. In conclusion, the human machine interaction in the highly automated driving system represents new challenges in this interactive systems.

II. METHODOLOGY

With the deployment of the new technology of the advanced driver assistant systems (ADAS) and autonomous vehicles (AV) controlling systems during the last decade, the concept of sensor fusion has been used in the higher automated vehicles, in which multiple channels and sources of surrounding information are connected and processed [11]. It enables the vehicle control modules to anticipate future events beforehand based on the pattern recognition and dataset training using the adaptive MPC block, fuzzy logic, and recurrent neural network (RNN) strategies [12]. Consequently, it alerts the driver before performing any maneuver or action to avoid any potential danger or risk. In the higher automated driving level such as SAE level 3 or above, the electronic control units (ECU) can make a controlling decision based on the perception input that feeds the programmed algorithm, which resides in their microcontrollers (μc) and systems on the chip (SoC) to make a control decision and send it to the actuators. This is where the artificial intelligence (AI) and machine learning (ML) have effectively played a key role to build a vehicular sensory platform with sensor fusion, decision making and actuation streams and pipelines in real time basis. This requires super-fast data computing and processing systems, more memory resources, low latency communication to support the self-driving cars with zero tolerance for systematic error in the driving control system and acceptable reduced risk in complaint with ISO26262 and safety regulations.

The parallel advancement and innovation in theory and hardware computing systems (HCS) have enabled a range of applications such as adaptive MPC and AI to be executed in real-time basis in automotive applications such intelligent steering and electronic braking systems using Ethernet protocols in machine to machine communications. Using the state-of-the-art of math optimization solvers and rapid prototyping, systems have enabled the control modules to perform complex calculations at a sufficient rate to meet the safety requirements of highly automated vehicles with 360° surrounding coverage.

To deal with the change of the vehicle dynamics in the HAV with SAE level 3 or above, the adaptive MPC provides a new linear planar model at each time step as the operating conditions change; therefore, it makes more accurate prediction for the new operating conditions of the vehicle trajectory maneuver.

The adaptive MPC can then control.

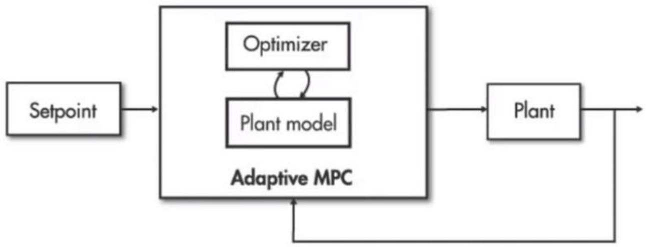

FIGURE 2. High-level schematic of using the adaptive MPC in the automotive longitudinal velocity and lateral position in the real time simultaneously and it shows the plant model connected with an embedded optimizer to update the operation conditions for the current time step and predict the next time step.

1- The longitudinal velocity as the driver sets it in the ACC automated system.

2- The lateral position of the vehicle by following a predefined trajectory or LKA following system.

In Figure 2, the adaptive MPC computes the longitudinal velocity and the steering angle position and rate and provides them as commands to the plant. Then, the real-time vehicle state parameters such as longitudinal velocity, lateral position and yaw rate are the real-time states representing the plant or the vehicle on the road.

Another advantage of deploying the adaptive MPC in the controller is that the plant model connected to an embedded optimizer can be updated in each time step in the runtime for the current operation conditions.

A. ADAPTIVE MPC DESIGN IN MATLAB CONTROL TOOLBOX

The traditional or classical MPC control toolbox uses a constant internal plant model, which limits its capability for real time updating and optimization. However, the adaptive MPC that was used and deployed in the research work utilizes the new version of the MATLAB control toolbox (Version 2020) that has an embedded optimizer that linked to the internal plant model, which updates every time step when executed in real time basis. This makes the adaptive MPC effective and suitable for the HAV steering systems to change the lane and follow a planned trajectory by controlling the steering angle input to the plant. At each time step, the Adaptive MPC updates the internal plant model with the same structure of the optimization problem across different operating points according to the programmed numbers of states and constraints. Therefore, the adaptive MPC is computationally complex because it solves an optimization problem at each time step in a real-time basis of the vehicle maneuver. In addition, the adaptive MPC computation gets more complicated with the increase of states constraints and the length of the control horizon and prediction horizons.

To build and simulate the virtual driving environment, the driving scenario designer of automotive application in MATLAB was used to generate roads, lanes and define maneuvers and the driving scenarios and other traffic predefined operating conditions. A passenger car was added to the driving scenario and two maneuvers were generated as follows.

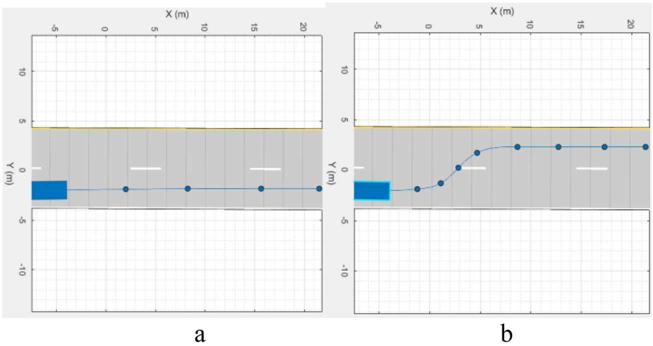

FIGURE 3. The driving environment, roads, lanes and maneuvers scenario were generated virtually using the Driving Scenario Designers in the automotive applications of MATLAB. a (left) is straight maneuver and b (right) is left lane change maneuver.

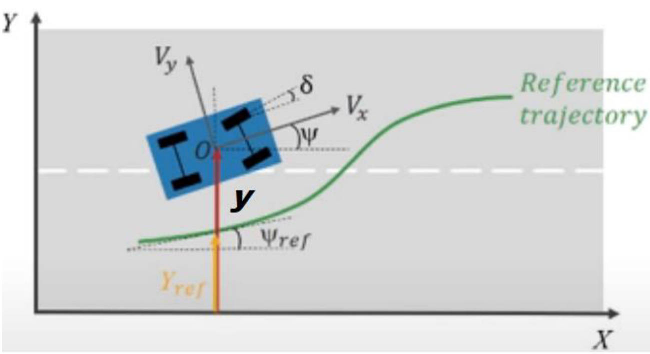

FIGURE 4. Left lane change reference trajectory and vehicle parameters and the referenced X_{ref} and Y_{ref} (Longitudinal dimension to the vehicle motion direction).

1- Straight trajectory in which the adaptive MPC will be deployed to control the longitudinal trajectory and velocity of the vehicle as shown in Figure 3a.

2- Lane change trajectory in which the adaptive MPC will be deployed to control the lateral global position or trajectory and velocity of the vehicle as shown in Figure 3b.

The vehicle was set as an ego car in the model. The sub model was saved and converted to a MATLAB function and exported to the workspace of the main MATLAB command window in the form of .mat extension file. This is an effective approach for utilizing vehicle dynamic models, which has emerged recently in the automotive industry for the ADAS applications development, Verification and validation (V&V) demonstration purposes in the early phase of the vehicle development. It moves the vehicle product development engineering towards the left side of the V model, which reduces time, cost, and utilizes control toolbox more efficiently.

The plant (vehicle) was developed as a state space model representing the lateral vehicle dynamic. The input to the plant is the vehicle longitudinal speed and the steering wheel angle and the outputs are the lateral position and the yaw angle.

In Figure 4, the horizontal axis denoted as X-axis [m] to represent the longitudinal distance of the headway of the ego vehicle while the vertical Y-axis represents the driving lane

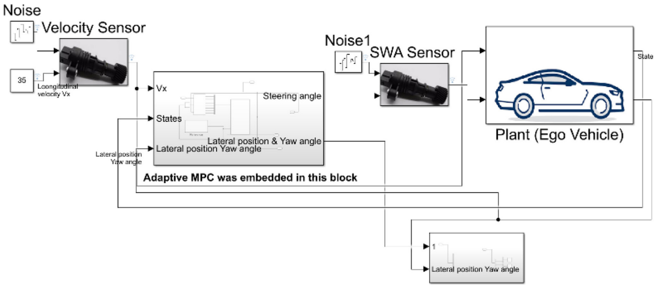

FIGURE 5. **The adaptive MPC controller block, seniors, noise blocks and monitors connected the plant vehicle model.**

width [m]. There are the referenced X_{ref} and Y_{ref}that will be used in the model. In addition, $\boldsymbol{x}$ and $\boldsymbol{y}$ are the global parameters that represent the vehicle position as the ego vehicle moves in the headway road based on the X_{ref} and Y_{ref}. This predefined path or trajectory will be the referenced path that the vehicle shall follow with the deployed adaptive MPC. Which controls the vehicle longitudinally and laterally as will be explained in more detail in the next section. The referenced values of the lateral position and the yaw angle are calculated with respect to the referenced horizontal X_{ref} axis as shown in Figure 4.

B. ADAPTIVE MPC AND VEHICLE PARAMETERS

MATLAB SIMULINK package library was utilized to create the adaptive MPC block and connected to the plant (ego vehicle) as shown in Figure 5.

Two lanes with 4m wide each were defined in the driving scenario designer. The plant (vehicle) was developed as a state space model representing the lateral vehicle dynamic using the bicycle model as the following equations (1) and (2) which are used in the first step to calculate the state space matrices of the vehicle velocity V_x and the vehicle position$\boldsymbol{y}$. Then it computes the discrete model to update the nominal conditions of the discrete time plant of the current operation conditions in the same order that was created inside the MATLAB function through the signals bus that was connected to the adaptive MPC block.

Lateral dynamic as a state space model

$$\frac{d}{dt}\begin{bmatrix} y \\ \psi \\ \psi' \end{bmatrix} = \begin{bmatrix} -\frac{2C_{\alpha f}+2C_{\alpha r}}{mV_x} & 0 & -V_x-\frac{2C_{\alpha f}l_f-2C_{\alpha r}l_r}{mV_x} \\ 0 & 0 & 0 \\ -\frac{2l_fC_{\alpha f}-2l_rC_{\alpha r}}{I_zV_x} & 0 & -\frac{2\,l_f^2C_{\alpha f}+2l_r^2C_{\alpha r}}{I_zV_x} \end{bmatrix}\begin{bmatrix} y \\ \psi \\ \psi' \end{bmatrix} + \begin{bmatrix} \frac{2C_{\alpha f}}{m} \\ 0 \\ \frac{2l_f}{C}{}_{\alpha f}I_z \end{bmatrix}\boldsymbol{\delta} \tag{1}$$

Global $\boldsymbol{y}$ position

$$\boldsymbol{y} = V_x\ \psi + \ V_y \tag{2}$$

where;

$\boldsymbol{y}$ is the global vehicle lateral position at a time t measured from the reference.

V_x is the longitudinal velocity at center of gravity of vehicle
m is the total mass of vehicle
I_z is the yaw moment of the vehicle inertia
l_f is the longitudinal distance from the center of the gravity to front tires
l_r is the longitudinal distance from the center of the gravity to rear tires
C_α is the cornering stiffness of tire
$\boldsymbol{\delta}$ is the front steering angle
ψ is the yaw angle.

The adaptive MPC block receives the predefined trajectory that was already defined in the driving scenario designer from the reference block that was embedded in the adaptive MPC block in Figure 5. The predefined trajectory represents the lateral position of the vehicle maneuver. Another input is the current or the real position of the vehicle, which are feedback from the plant (ego vehicle) as lateral position and yaw angle that will change as the vehicle dynamic changes so that the adaptive MPC controls the vehicle trajectory as close as the desired trajectory and at the same time, controls the longitudinal velocity as close as to the set point velocity. The advantage of the adaptive MPC is that it is a multivariable controller that controls the outputs simultaneously by considering all the interactions between system variables within the predefined constrains and ranges of these variables. Constrains such as steering wheel rate, velocity increase step, are important because constrain violations can lead to undesired consequences. Therefore, the adaptive MPC can handle multi-input multi-out (MIMO) systems and this makes it suitable for high-level automation and autonomous vehicle applications. In addition, another feature of the adaptive MPC is its preview capability, which is similar to feedforward control technique to control upcoming events accurately.

Another output variable from the plant (vehicle) is the state of the vehicle, which represents the actual longitudinal velocity, and lateral position of the vehicle. The state estimator is part of the feedback loop to the adaptive MPC to measure the vehicle velocity and position incrementally in each time step and adjust the output accordingly.

The adaptive MPC updates the plant (vehicle) each time step T_s with the below operation conditions and parameters values used to design the adaptive MPC setting in this work are shown in Table 1.

The adaptive MPC uses an internal plant model to make predictions and optimization iterations to find the optimal control actions utilizing fixed and variable horizon optimizers. In order to calculate the next step decision, the controller operates in two phases.

1- Estimate the current state which includes the true value of the controlled vehicle parameters such as the long. vehicle speed and the steering wheel angle. This is very crucial to make an intelligent move in the future step

TABLE 1. Adaptive MPC parameters.

Parameters	Explanation
T_s	Execution time step update = 0.1 sec
T	Simulation duration =15 sec
Prediction Horizon	Controller prediction of the sample time = 1
Constraints	Represent the physical limitation of vehicle Steering wheel turns at of 15 degree/sec
Weights	Set the input and output parameters to value Such yaw angle to 0.1 and position to 1
Response	Ramp input
Plant Input	The long. speed V_x and the front steering angle $\boldsymbol{\delta}$
Plant Measured output	Lateral position $\boldsymbol{y}$ Yaw angle ψ
State Estimator	Default Kalman Filter
Vehicle mass	1575 Kgs

TABLE 2. ISO 26262 active safety implementation.

Methods	ASIL			
	A	B	C	D
Requirements-Based Test	++	++	++	++
Fault Injection Test	+	++	++	++
Back-to-Back Test	+	+	++	++

TABLE 3. Fault models.

Type	Examples
Data errors	Data integrity, Data processing, Data exchange corruption, interruption, loss, manipulation and byte flip
Timing errors	Violation of specific timing behavior of the executed SW
Program flow errors	Erroneous sequence or execution order
HW errors	Faulty hardware parts in the system

based on the current and past measurements. The state estimator in this study was a default Kalman Filter.

2- Optimize the values of the set points, measured disturbance and constraints specified over the finite horizon of the future sampling instants T+1, T+2, … The adaptive MPC control action at time T is obtained by solving the optimization problem and the cost function as explained in the MATLAB user guide of the adaptive MPC Toolbox [13].

The selection of magnitudes and values of the adaptive MPC is important as they affect not only the controller performance but also the computational complexity of the adaptive MPC algorithm that solves an online optimization problem at each time step. In automotive applications, the sample time (Ts) of the adaptive MPC determines the rate at which the controller executes the control algorithm and command the actuators based on the predefined algorithm and calculation. In the same time, too small Ts requires excessive computational load on the system resources and memories that add more design complexity, constrains and cost. The adaptive MPC computations get more complex and resource demanded with the increasing number of vehicle states, constraints, length of control, and the prediction horizon. The vehicle dynamic optimization processes and solving the cost function need to be solved within small sampling intervals in the order of milliseconds (msec) execution time to converge results through iteration.

C. ISO 26262 ACTIVE SAFETY REQUIREMENTS

This framework for developing a fault injection test methodology at the system level of the vehicle motion controller is complaint with the ISO 26262 standard – Part 4 product development at the system level. It requires evidence for the correct implementation of the safety related functions and behavior on the system level (HW & SW) combination as shown in Table 2. However, it does not specify whether the tests need to be done in virtual environment or real scenarios and maneuvers. ASILs B, C and D require fault injection test in the run time while the control system is deployed. It is considered one of the effective methods to test the robustness of the active safety control system after integrating the HW and the SW components of the system [14]. Consequently, this provides an evidence that system elements interact correctly with an adequate level of confidence that unintended behaviors (that could violate a safety goal), are absent from the current integration design.

A fault injection test uses corrupted and false data and means to introduce faults into the steering system during the run time of the vehicle was performed on the developed MATLAB model. Most of the suppliers and testers are moving towards the virtual hardware in the loop (VHIL) technology for verification and validation of the ADAS applications and their active safety mechanisms. Therefore, it would be feasible to perform a preliminary fault injection test in the early phase of the development process to understand the system behavior and address any design issues as early as possible. Therefore, this work would serve as a fully virtual fault injection test was done in a fully virtual environment of a model based to study the behavior of the active safety system. This would address any issues easily and costly effective before the prototype implementation and execution phases.

Faults were generated in the model of the steering system and injected in the interface of the adaptive MPC to improve the test coverage in a fully virtual environment of the steering sensors and adaptive MPC block. The injected fault in form of noise needs to cover the data corruption, timing, program flow and sequences. The SW architecture design goal is to be able to detect, isolate and recover from the faults and maintain a safe and highly available architecture.

Table 3 shows examples of fault models and types.

The error can be defined as the incorrect state of the subsystem that is caused by the fault can lead to failure mode. The failure is the termination of the ability of the system or the function unit. This loss of function can appear

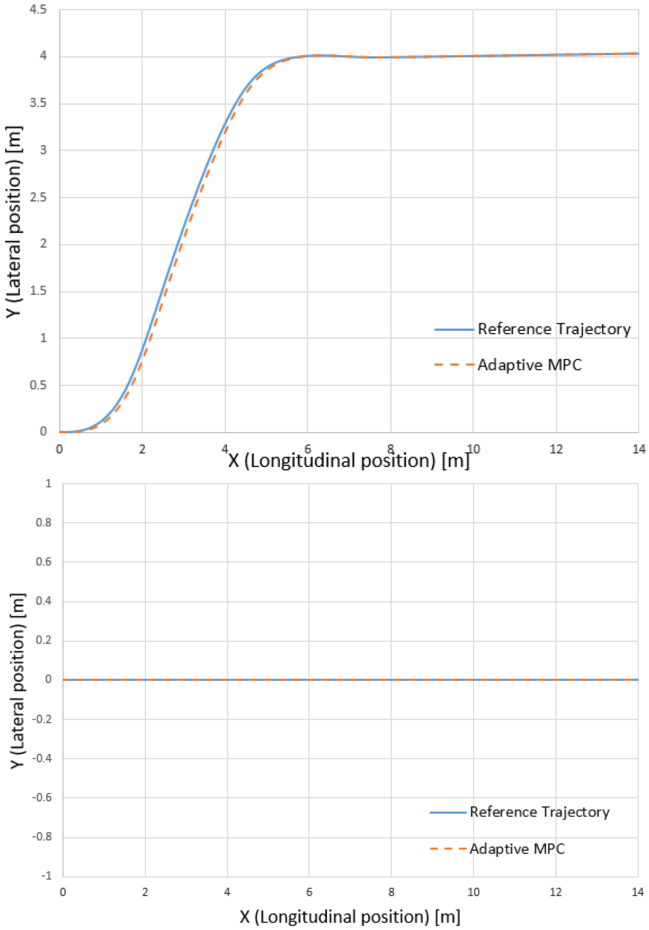

FIGURE 6. **The SIMULINK model of the adaptive MPC ego vehicle results following the reference trajectory of left lane change (Upper) and stay in the same straight maneuver (bottom).**

as abnormal behavior such as an unintended vehicle path and loss of assist. Consequently, hazardous event could lead to an accident with negative potential inherited from this set of conditions. Personal injuries and property damage can be caused and experienced which depend on the severity of the hazard and the environment of the drivers, passengers and other road users.

III. RESULTS

A. ADAPTIVE MPC AND VEHICLE TRAJECTORY VALIDATION

The SIMULINK model was ran with two driving scenarios; the first scenario was a left lane change from the host lane and continue the maneuver in the left lane. The second scenario was driving the ego vehicle in same host lane straightforward both with longitudinal velocity of 35 m/sec, which was fed in the reference trajectory. The adaptive MPC of the ego vehicle follows the reference trajectory lane change very closely as shown in Figure 6 orange dotted line. The implementation of the adaptive MPC in the ego vehicle integrated in the SIMULINK explains the combination of controlling of the longitudinal speed, which is known a full range speed adaptive cruise control (FRSACC) across a wide range of different speeds. In addition, following the lateral reference trajectory vehicle position, which fulfils the third level of the SAE automation level, where the vehicle's control system can drive the vehicle longitudinally and laterally simultaneously and follow a defined path from point A to point B. The deployment of the adaptive MPC model achieves level SAE 3 automation in this research work. Consequently, the adaptive MPC application can be considered as a suitable solution in HAV control system integrated with other localization, perception, positioning and mapping applications that can be optimized for the reference path utilizing artificial intelligence and machine learning platforms and constitute layers covering vehicle control [15]. The model was deemed fully validated against the driving scenarios that were generated virtually using the driving scenario designer of automotive application in MATLAB.

B. CONTROLLABILITY OF ADAPTIVE MPC AND SYSTEM FAILURES

After validating the adaptive MPC integrated in the vehicle model by matching the reference and vehicles paths as shown in Figure 6, the longitudinal velocity and steering hand wheel angle sensors failures or degradation event were performed in the SIMULINK model by injecting a predefined percentage of noise or disturbance (faults) on the signals to evaluate the fault injection metric of the ISO26262. In addition, this represents an end-to-end (E2E) performance test coverage of the adaptive MPC block. The chosen evaluation of the noise or disturbance impact considers the longitudinal and lateral vehicle motion and position. The ACC, LKA and the automatic lane change assist (LCA) are the features on the system level that can be impacted by any functional failure or signal disturbance in these sensors due to the injected faults. Two noise or disturbance blocks or sources were linked to the longitudinal velocity sensor and the steering hand wheel angle sensor as shown in Figure 5. The band-limited white noise block generates normally distributed random numbers that are suitable for use in continuous or hybrid systems with sample time of 0.1 sec to represent malfunction or degradation of the sensors or the transmitted signal from the sensor to the adaptive MPC module block.

The first case involved tracing the longitudinal velocity sensor output without any noise as shown in blue color in Figure 7, which is clear that the longitudinal signal sensor is fully functional, and the signal is stable at 35 m/sec. The orange trace in the same figure shows manipulated velocity with a random noise of 10% of the original longitudinal velocity, which represents a fault or sensor degradation that causes the transmitted velocity signal to be unstable as shown in Figure 7.

It was found that the injection of 10% of noise or disturbance on the vehicle velocity does not impact the adaptive MPC model following the reference trajectory because the velocity sensor path or trace in the model is totally separate from the lateral position control path. According to the

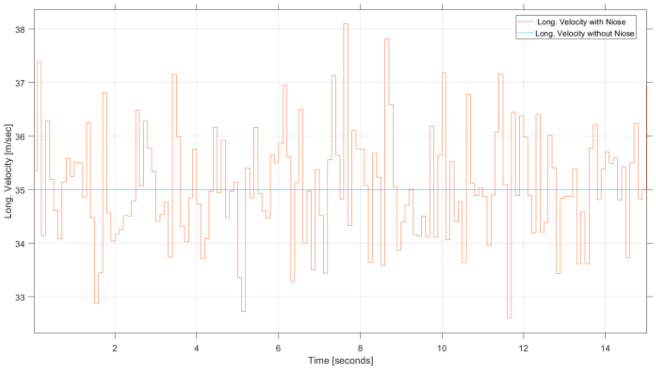

FIGURE 7. Longitudinal velocity sensor signal without any noise or disturbance (blue color) and with 10% noise (orange color).

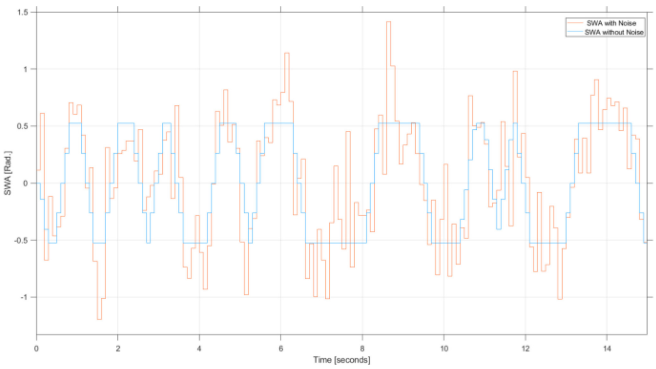

FIGURE 8. Steering wheel angle sensor signal without any noise or disturbance (blue color) and with 10% noise (orange color).

ISO 26262, the functional safety of the road vehicles, the malfunction of the longitudinal velocity sensor due to faulty signals would not be considered as a high risk because the absence of the unreasonable risk when the velocity sensor fails. In addition, it is known as safe faults, which is unable to violate the safety goal of the system because the safe faults cannot propagate to the relevant paths of the lateral control logic gates or the internal registers. Consequently, it is unable to affect the design function so the system is tolerant for this type of faults. It might be still uncomfortable maneuver or experience for the driver or the road users, but still not a high-risk failure in the E/E system of the vehicle velocity sensor.

The second case involved tracing the SWA sensor output signal with 1% noise or disturbance as shown in orange color with respect to the original steering hand wheel angle signal without noise as shown in blue color in Figure 8. The steering wheel angle unit used in the model was chosen in radians (1 rad. = 57.29 degrees) and this is the reason that a noise magnitude of 1 % was selected in the work to investigate the small increment of the SWA failure in the order of 0.5729 degrees and evaluate its impact on the adaptive MPC model following the reference trajectory. Again, the orange trace shows a random noise distribution across the run time of the simulation of real time run of the ego vehicle.

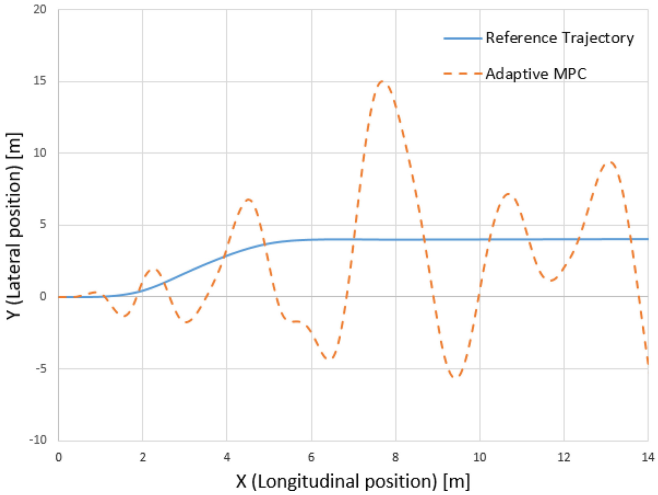

FIGURE 9. Adaptive MPC model result with 1% noise added to the steering wheel angle sensor [rad].

The added noise or disturbance representing faults was injected on the trace of the SWA sensor to study SWA failure and erroneous scenario that can degrade the function of the sensor and sending faulty signals. Consequently, this faulty signal propagates through the plant or the vehicle causing it to jitter in the right and left directions, which drives the ego vehicle out of the intended path as shown in Figure 9 even before the vehicle starts the lane change. The ego vehicle in this scenario can be described as non-controllable vehicle due to SWA sensor failure in the host lane, lane change and the target lane (the left lane in this study). This is the reason that the SWA sensors are categorized as a high safety critical component with ASIL D classification, that ISO 26262 recommends fault injection test as shown in Table 1. This is an example of a single point fault that can propagate through the controller and violate the safety goal and no safety mechanism can detect, control and mitigate it. Therefore, ISO 26262 recommends to perform a fault propagation analysis (FPA) to test the safety mechanism and the diagnostic coverage of single fault point metric (SFPM) to satisfy the SPFM and ASIL B,C and D targets as shown in Table 4 [16].

In addition, the highest spike of the noisy signal causes the vehicle to deviate further from the reference trajectory or path around the running time of 8 sec as shown in Figures 8 and 9. This presents a clear evidence that the lateral vehicle motion was badly impacted by the quality of the SWA signal to keep the vehicle in the intended path. The SWA signal oscillation that is caused by the added noise maneuvers the ego vehicle out of the intended path and the host lane until it reaches to the furthest point of 15 m off the road.

Then, the negative spike of the SWA signal drives the vehicle towards the intended path again and departs the intended path in the other side or direction. This requires developing a safety goal and diagnostic coverage to detect and mitigate any potential failure in the SWA sensor such as HW

FIGURE 10. Rating scale of controllability and uncontrollability and human feeling categorization and response to disturbance and steering system malfunction.

TABLE 4. ISO26262 single point fault metric and asil b,c and d target [16].

Methods	ASIL			
	A	B	C	D
Single-Point Fault Metric	–	≥ 90%	≥ 97%	≥ 99%

redundancy, cyclic redundancy check (CRC) and checksum counters, built in safety test (BIST) to capture these failures before they propagate to the control path and cause catastrophic consequences [5], [6].

C. DISTURBANCE RATING SCALE

The SWA faults that were injected in the automated steering system by adding noise or disturbance on the sensor output signal can be rated by their impact on the vehicle intended trajectory deviation as shown in Figure 9. The continuous injection process of faults causes the adaptive MPC vehicle to bounce in sinusoidal behavior, which can be seen as jitters or spikes anomalies from the intended path in both directions. Most of the ADAS and active safety applications sensors run in a synchronous mode. This means that the oscillators that generate the signals in a defined pattern and frequency in the sensors need to match the ECU input requirements to keep the synchronous mode operation. The system level scale that measures the SWA disturbance is characterized by a unique defined tolerance limit of the vehicle lateral position with respect to the lane marker lines. Rating on the vehicle lateral dynamic position is strongly influenced by the steering control system sensors, ECUs and actuators functionalities and safety goals in case of any malfunction while being deployed in the field. In addition, the vehicle lateral acceleration plays a key role in this scale. In order to give a common sense of the proposed scale, the concept of vehicle steering system controllability should be redefined, described and what is the threshold to say whether the vehicle is controllable or non-controllable with respect to the intended path in the host lane.

In ISO 26262 standard, the controllability (C) is categorized into four classes C0-C3 with the main difference in the probability from one C class to the next class in the order of magnitude, i.e., C1 is associated with 99%, C2 with 90-90%, C3 with less than 90% of the driver can control the malfunction and avoid the accident or the crash. This definition does not hold true in case of complex automated driving system being deployed in controlling the vehicle maneuver due to the extreme difference between the human and the computer systems nature such as response time and influence by other driving ecosystem components. This difference can be understood as the comparison between human machine interaction (HMI) and computer machine interaction (CMI). The human or the driver can distinguish more clearly between controllable and non-controllable scales such as unnoticeable, noticeable, disturbing and even dangerous as shown in Figure 10.

For the steering system and lateral vehicle control that the driver or the human is in the control loop, the controllability is defined as the estimated probability of the driver to gain the lateral vehicle control by rotating the steering wheel to keep the vehicle in the intended path. The system allows the driver to steer the vehicle very easily and comfortably under all driving conditions by providing up to 80% of the required steering wheel torque (SWT). So, the driver is expected to provide the remaining 20% of the required SWT [17], [18]. Therefore, there are two scenarios.

1- In case of loss of assistance (LOA) due to EPS control unit malfunction or failure, the driver needs to compensate for the EPS assistance loss and perform the required SWT manually [19]. Otherwise, the vehicle will not be laterally controllable and lose the intended or safe trajectory and cause harm or accident. This is the reason that the vehicle steering control system is considered as a very critical safety component and requires a high availability system architecture design to mitigate any failure or malfunction. In addition, this includes avoiding risks and harm to other traffic participants such other vehicles' drivers, passengers, and pedestrians.

2- In can of the human driver who is in charge of the DDT does not perform the steering commands before the time to collision (TTC) in upcoming safety critical situation to maintain vehicle path and headway due to distraction, fatigue and alcohol impairment [20].

When the vehicle is equipped with the automated control system that deploys the computer platform to take the lateral control of the vehicle and follow the intended trajectory, here is a special case that the current ISO 26262 standard controllability class would not hold true anymore when it comes to controllability classification. The reason is that the human driver is not the active part of the control loop of the vehicle and therefore it is very difficult to measure the controllability of HAD systems based on the computer control system. In an alternative controllability class definition and categorization in the system level of HAD can be considered as shown in Table 5.

Figure 10 and Table 4 are in alignment for the highest level of uncontrollable steering system, which marks it as dangerous and life threating accident where the unreasonable risk is presented. Consequently, the control system is considered unrecoverable, and the accident is non-avoidable. In addition, it can be concluded from Figure 10 and Table 4 that from the controllability standpoint, the disturbing class failures whose effects are usually controllable by sensible human response and system reaction that could cause minor harm. It represents the conversion point where the system becomes out of control, which makes it dangerous because the system

TABLE 5. Controllability class definition for SAE LEVEL3 with higher automation and deployment driving level.

C0 (100%)	C1(99%)	C2(90-99)%	C3(< 90%)
Controllable (Unnoticeable)	Simply Controllable (Noticeable)	Normally Controllable (Disturbing)	Uncontrollable (Dangerous)
Maintain the intended driving path at all times (Vehicle is in the center of the lane)	Vehicle is still inside the intended lane and the front wheel end does not cross the inside end of the lane marker.	Vehicle front wheel crosses internal end of the lane marker but does cross out of the lane marker.	Loss of lateral control of the vehicle (Vehicle is uncontrollable and lost driving path) and it is outside of the intended lane (Oncoming traffic) or road shoulder. The front wheel crosses the outside end of the lane marker.
No Accident or harm	Avoidable accident and no harm	Partially avoidable accident with minor harm	Non avoidable accident and it causes severe harm
No risk	Minimal risk	Reasonable risk	Unreasonable risk
Recoverable by the vehicle controller	Recoverable by the vehicle controller	Partially recoverable by the driver vehicle controller	NON recoverable
Intervention is not needed	Intervention is partially needed	Intervention is required	Intervention is required
Unnoticeable	Noticeable	Disturbing	Dangerous

failure results in a safety critical situation. This represents the moment that the front vehicle departs the outside end of the lane marker line and continue towards oncoming traffic or same direction traffic. At this moment, the braking and evasive steering are the two options that the driver can rely on to avoid collision or accidents. The development of evasion systems is a challenge when it comes to HMI and the time-critical scenarios that require highly dynamic steering action within 200 msec [21]–[23].

D. HUMAN MACHINE INTERFACE AND STEERING SAFETY METRICS

The high system level hazard definition of steering system failure metric is the unintended steering motion or activation regardless of the vehicle propulsion system status (i.e., parked, neutral or any drive gear position). This happens when the steering system provides unexpected assist in the form of torque due to failure in the electronic control unit of the steering system or the transmitted signals and commands. Consequently, the vehicle loses the intended lateral path due to uncontrollable or excessive assist from the steering system while driving the vehicle. The vehicle is unable to be steered due to the operator being unable to overcome the steering wheel force necessary to rotate the steering wheel. Interestingly, in SAE level 3 when the vehicle control system is deployed to drive the vehicle, the driver must be able to take over the control at any time and be able to control the vehicle while the automated steering feature is active such as LKA, LCA and advanced parking assist. The loss of vehicle stability while moving due to steering malfunction may result in loss of control or vehicle roll over. Therefore, most of the OEMs and suppliers have developed safety metrics for the unintended steering wheel motion, which include:

1- The unintended steering wheel torque that comes from the assist shall not exceed more than 4 to 5 Nm [19], [24].
2- The unintended steering wheel movement rate shall not exceed defined threshold by the manufacturers (depends on the vehicle weight, center of gravity height and dynamic properties) [25], [26].

The steering safety metrics are applicable for all vehicle-operating conditions with the vehicle speed ranges from zero to maximum speed. If the steering safety metrics are violated for any reason, the operator will experience difficulty controlling the vehicle and remaining in the intended path of the host lane. For example, if the unintended steering wheel torque assist exceeds (5) Nm, consequently, the operator might lose the steering control causing to intended trajectory loss and vehicle can be described as uncontrollable. The steering torque assist that the EPS provides is calculated based on the vehicle speeds in the predefined programmable tables of the EPS controlling unit. With the higher vehicle speeds (i.e., 35 m/sec), the assist decreased due to the friction reduction between the front axle wheels and the road surface. This case of high importance and critical safety designation because even with minimal amount of unintended torque with the high vehicle speed scenario, the vehicle is highly susceptible to lose the intended path faster due to the vehicle high lateral acceleration that deviated the vehicle quickly out of the intended lane. This is the reason that active safety systems in higher automation SAE level 3 and above use different intervention strategies in case of failure of the control system to trigger the driver's response to take the vehicle control over from the automated control system. The interventions can be delivered to the driver via the HMI located in the cockpit such as displays, haptic devices, sound alert and flashing lights. The human drivers are still responsible for most of the road crashes even in SAE level 1 and 2 automated vehicles because these active safety-controlling systems are designed to hand the control over to the driver using the intervention HMI in case of malfunction or failure. This is the reason that the drivers – vehicle control systems are changing significantly in SAE level 3 automated vehicle and above that. Driving functions are controlled by the

TABLE 6. HMI modalities.

Visual	Auditory	Haptic
Color	Sound type (Speech, tone, auditory icon)	Vibration –Frequency
Symbol	Loudness (Absolute and relative to masking threshold)	Location
Text	Muting or partial muting of other sounds	Intensity
Size	Onset of offset	Direction
Brightness	Duration (pulse & interval)	Rhythm
Contrast	Musicality	
Flashing	Frequency	
Duration	Spatial location	

vehicle control systems and this presents human factors challenges in this interactive system with moving to level 4 and 5. HMI modalities can be divided into three main categories as shown in Table 6.

The visual HMI warnings are appropriate for primary warning information and lower priority attention. However, the auditory HMI warnings are suitable for high priority alerts and indicate the onset of system malfunction or limitation. In addition, the haptic HMI can be used to provide information that the auditory HMI is unlikely to be effective. The driver can get a specific information from the HMI about the required action such as braking, swerving or acceleration rather than just getting warning alerts.

IV. CONCLUSION

Analysis of model-based fault injection for the steering system of high-automated vehicles has shown that the steering wheel angle is of high importance and classified as ASIL D based on the risk assessment and control metrics that were developed in this study. The research also redefined the controllability classes or categories of high automated vehicles based on the vehicle global position related to the lane marker lines to accommodate for the machine in the loop controlling the DDT in autonomous vehicle maneuvering. There are however, human factors challenges in SAE level 4 and 5 and the interaction between the driver and the automated control system of the vehicle that require HMI modalities as explained in Table 2. The driver – automated control system engagement in the steering system of the vehicles is one of the crucial control complex scenario that add uncertainty and potential risk when handing over the steering control between the driver and-or the automated control system. Even when the driver is in full control of the steering system, the ESP is still responsible for approximately ($\sim$ 80%) of the SWT required to steer the vehicle. Therefore, the steering system design and functional safety metric require specific architecture redundancies in SW, HW and system level for high availability and risk mitigation mechanisms. This research highlighted the need to define the driver intervention in high-automated vehicle of SAE level 4 and 5 in order to sustain the traffic safety and keep the vehicle in the intended trajectory. This can be addressed by HMI and the human factor implementation in ISO 26262 to standardize the driver-machine relation with the DDT in real time and interactive environment. Both manual and automated driving modes demand the functional safety implementation of the steering system to mitigate any system malfunction or failure. Therefore, the fault injection concept supports the safety mechanism implementation and correctness of the system architectural design with respect to faults and failures during the runtime. This improves the test coverage of developing safe control system to operate as designed and meet the safety requirements in compliance with the OEMs and government regulations. Another aspect to consider in the future work is to utilize the HMI in ASIL D systems in ISO 26262 in more detail and include the HMI in the safety mechanism of the vehicle control system.

ACKNOWLEDGMENT

This work was part of the work in the Safety Engineering and Application Laboratory (SEAL) at Oakland University, Rochester, MI, USA. The authors would like to acknowledge the Safety Engineering and Applications Laboratory (SEAL), School of Engineering and Computer Science (SECS), Oakland University for helpful comments and insights in this work.

REFERENCES

[1] U. Montanaro *et al.*, "Towards connected autonomous driving: Review of use-cases," *Veh. Syst. Dyn.*, vol. 57, no. 6, pp. 779–814, 2018.

[2] SAE On-Road Automated Vehicle Standards Committee, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Warrendale, PA, USA: SAE Int., 2018.

[3] M. Jonasson and M. Thor, "Steering redundancy for self-driving vehicles using differential braking," *Veh. Syst. Dyn.*, vol. 56, no. 5, pp. 791–809, 2018.

[4] S.-C. Lin *et al.*, "The architectural implications of autonomous driving: Constraints and acceleration," in *Proc. 23rd Int. Conf. Archit. Support Program. Lang. Oper. Syst.*, 2018, pp. 751–766.

[5] M. Tlig *et al.*, "Autonomous driving system: Model based safety analysis," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Depend. Syst. Netw. Workshops (DSN-W)*, 2018, pp. 2–5.

[6] P. Lytrivis and A. Amditis, "Intelligent transport systems: Co-operative systems (vehicular communications)," in *Wireless Communications and Networks-Recent Advances*. Rijeka, Croatia: InTech, 2012.

[7] Y. Gao, "Model predictive control for autonomous and semiautonomous vehicles," Ph.D. dissertation, Dept. Doctor Philos., Univ. California, Berkeley, CA, USA, 2014.

[8] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. M. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[9] J. B. Froisy, "Model predictive control: Past, present and future," *ISA Trans.*, vol. 33, no. 3, pp. 235–243, 1994.

[10] M. Morari and J. H. Lee, "Model predictive control: Past, present and future," *Comput. Chem. Eng.*, vol. 23, nos. 4–5, pp. 667–682, 1999.

[11] T. Schmid, "Safety analysis for highly automated driving," in *Proc. IEEE Int. Symp. Sofw. Rel. Eng. Workshops*, 2018, pp. 154–157.

[12] V. S. Kumar, "P3/PPP in the context of autonomous driving vehicles," M.S. thesis, Dept. Civil Eng., North Carolina State Univ., Raleigh, NC, USA, 2017.

[13] A. Bemporad, M. Morari, and N. L. Ricker, *Model Predictive Control Toolbox: User's Guide (R2020a)*, MathWorks, Natick, MA, USA, 2020. [Online]. Available: https://instruct.uwo.ca/engin-sc/391b/downloads/mpc.pdf

[14] *Road Vehicles—Functional Safety—Part 4: Product Development at the System Level*, ISO Standard 26262-4, 2018.
[15] D. Watzenig and H. Martin, *Automated Driving: Safer and More Efficient Future Driving,* Springer, 2017.
[16] *Road Vehicles—Functional Safety—Part 5: Product Development at the Hardware (HW) Level*, ISO Standard 26262-4, 2018.
[17] "Bureau of Transportation Statistics; Motor and Vehicle Safety Data," U.S. Department of Transportation. [Online]. Available: https://www.bts.gov/content/motor-vehicle-safety-data (Accessed: 2018).
[18] National Center for Statistics and Analysis, "2018 fatal motor vehicle crashes: Overview. (Traffic Safety Facts)," U.S. Dept. Transp., National Highway Traffic Safety Administration, Washington, DC, USA, Rep. DOT HS 812 826, 2019.
[19] S. Salih and R. Olawoyin, "Computation of safety architecture for electric power steering system and compliance with ISO 26262," SAE, Warrendale, PA, USA, Tech. Paper 2020-01-0649, 2020.
[20] M. A. Regan, C. Hallett, and C. P. Gordon, "Driver distraction and driver inattention: Definition, relationship and taxonomy," *Accid. Anal. Prevent.*, vol. 43, no. 5, pp. 1771–1781, 2013.
[21] A. Marinik, R. Bishop, V. Fitchett, J. F. Morgan, T. E. Trimble, and M. Blanco, "Human factors evaluation of level 2 and level 3 automated driving concepts," U.S. Dept. Transp., Nat. Highway Traffic Safety Admin., Washington, DC, USA, Rep. DOT HS 812 044, 2014.
[22] M. Ellims and H. E. Monkhouse, "Agonising over ASILs: Controllability and the in-wheel motor," in *Proc. 7th IET Int. Conf. Syst. Safety Incorp. Cyber Security Conf.*, 2012, p. 52.
[23] N. Schneider, C. Purucker, and A. Neukum, "Comparison of steering interventions in time-critical scenarios," *Procedia Manuf.*, vol. 3, pp. 3107–3114, Jul. 2015.
[24] E. Thorn, S. C. Kimmel, M. Chaka, and B. A. Hamilton, "A framework for automated driving system testable cases and scenarios," U.S. Dept. Transp., Nat. Highway Traffic Safety Admin., Washington, DC, USA, Rep. DOT HS 812 623, 2018.
[25] R. Debouk, *Overview of the 2nd Edition of ISO 26262: Functional Safety—Road Vehicles*, General Motors Company, Warren, MI, USA, 2018.
[26] S. Singh, "Critical reasons for crashes investigated in the national motor vehicle crash causation survey," U.S. Dept. Transp., Nat. Highway Traffic Safety Admin., Washington, DC, USA, Rep. DOT HS 812 115, 2015.