A Dynamic Synchronous Interactive Functional Validation Approach for Electric Vehicles

Ci Liang, Mohamed Ghazel, Chi Xie, Wei Zheng, Wei Chen

A Dynamic Synchronous Interactive Functional Validation Approach for Electric Vehicles

Ci Liang, *Senior Member, IEEE*, Mohamed Ghazel, Chi Xie, Wei Zheng, Wei Chen, *Senior Member, IEEE*

***Abstract*—Functional safety is crucial for Electric Vehicles (EVs) as it ensures that the EV systems operate correctly and safely. This paper aims to propose an efficient and holistic approach to verify functionality and ensure the functional safety of EVs. A holistic closed-loop dynamic synchronous functional validation (CL-DSFV) methodology is proposed. The CL-DSFV methodology consists of a set of sequential analysis/modeling methods: use case analysis, functional concept analysis, functional state/transition modeling, simulation method of the user interaction based on dynamic synchronous interconnection between the FSM and the user behavior simulation platform, verification method of checking correctness and completeness of functions according to the user behavior cover list and test cases. Moreover, a novel transition engine with usage and functionality features is originally developed to constrain the switching between functional states of the FSM. UIG algorithm is originally proposed to generate functional validation configurations automatically and further achieve the automation of dynamic synchronous validation. Superiority of the CL-DSFV is verified through the comparison with several referred relevant existing methods. Furthermore, CL-DSFV is applied to functional validation of the product function "Electrical Energy Management" (EEM) of EVs. The outcomes attest that the CL-DSFV allows for effectively ensuring the completeness and correctness of the considered functions, and helps ensure the traceability of function decomposition.**

***Index Terms*—Electric vehicle, functional safety, functional state interconnection, user intention, dynamic synchronous validation.**

I. Introduction

A. Background

OWING to the rapid development of electric vehicle (EV) technologies, we are on the cusp of a revolution in transportation on a scale not seen since the introduction of automobiles a century ago. As a solution to help tackle the global climate change problem, the development of EVs has been attracting worldwide attention from industries, government agencies, professional organizations and academic institutions. The number of EVs has increased dramatically in recent years. In China, the sales trend of EVs has soared since 2018. Specifically, EV sales increased to 141,000 in the first quarter of 2018, which leads to the fact that China has become the principal market of EVs all over the world. In 2019, the production and possession quantity of EVs in China reached more than 1.3 million and 3.4 million, respectively, which accounted for more than 60% of the world figures in terms of both production and possession [1]. The U.S. remains the second-largest EV market in terms of sales. The number of new EV registrations in the first quarter of 2019 in the U.S. rose to 61,000. Across Europe, one can notice that Norway and Germany currently have the most EVs registered. The number of newly registered EVs has exceeded 23,300 since 2019 in both countries [2]. Global EV sales doubled in 2021 from the previous year to a new record of 6.75 million [3, 4]. Besides, nearly 10% of global car sales were electric in 2021. This brought the total number of operated electric cars worldwide to about 16.5 million, triple the amount in 2018. In 2022, global EV sales have kept accelerating with 2 million sold solely in the first quarter, which went up 75% from the same period in 2021 [5].

Meanwhile, safety issues related to EVs have become prominent along with the increasing inventory of EVs. It is worth mentioning that since EVs are safety-critical systems, ensuring the correctness of their functional design and preventing malfunctions are of primary importance [6]. Therefore, functional safety is a core concern for EVs, due to the high complexity of EV systems, which incorporate battery cells, the battery management system (BMS), the electrical energy management system (EEMS, our focus in this paper), power electronics and electric powertrain [7–9]. Moreover, a high level of functional safety is required to protect passengers, pedestrians and the environment. As witnessed by the statistics from various countries, severe accidents related to EVs have occurred and given rise to serious human and material damages in the past decade. According to the investigation conducted by the National Highway Traffic Safety Administration (NHTSA) in the U.S., numerous plug-in EV fire accidents have occurred since the introduction of mass production of plug-in EVs [10]. On August 15, 2016, a new Tesla Model S 90D spontaneously caught fire during a promotional test drive in Biarritz, France. Following a sudden loud noise, the dashboard presented the driver with a warning of a "charging" problem. A few moments later, the vehicle started burning, and the fire completely destroyed the vehicle within 5 minutes. Fortunately, the driver and passengers safely exited the vehicle in time. The investigations conducted by Tesla subsequently showed that a bolted electrical connection of the vehicle had not been tightened properly, which led to the charging

Ci Liang (First author, Corresponding author) is with the School of Transportation Science and Engineering, Harbin Institute of Technology, Harbin, 150001, China (e-mail: ciliang.lc@gmail.com).

Mohamed Ghazel is with the COSYS/ESTAS Department, Université Gustave Eiffel (ex-IFSTTAR), Villeneuve-d'Ascq, 59650, France (e-mail: mohamed.ghazel@univ-eiffel.fr).

Chi Xie is with the School of Transportation Engineering and Urban Mobility Institute, Tongji University, Shanghai, 201804, China (e-mail: chi.xie@tongji.edu.cn).

Wei Zheng is with Collaborative Innovation Center of Railway Traffic Safety, and School of Automation and Intelligence, Beijing Jiaotong University, Beijing, 100044, China (email: wzheng1@bjtu.edu.cn).

Wei Chen is with Ruijie Network Co. LTD., Beijing, 100000, China.

failure [11]. Moreover, upon several reported Tesla-related EV accidents, the NHTSA opened a probe, in 2019, into all Tesla Model S and X cars manufactured between 2012 and 2019. The probe collected a wide range of information regarding details on the engineering and production of the specified vehicles, which involves the functions of battery management, electrical energy management (EEM, our focus in this paper) and thermal management during or after charging [12]. In 2021, Electrek, an American news website dedicated to electric transportation and sustainable energy, compiled a list of 19 Chevrolet Bolt EV related fires [13]. The frequent fire related accidents resulted in a recall of around 110,000 Chevrolet Bolt and Bolt EUV EVs produced between 2017 and 2022. According to the U.S. highway vehicle fire report, EV fire accidents are mainly a result of mechanical problems, electrical failures or malfunctions, ranging from a faulty design of relevant functions to an improperly installed device [14]. The investigation on EV fire accidents in 2020 in China shows that mechanical failures and malfunctions of battery cells, BMS and EEMS are the leading contribution factors towards the EV fire accidents [15–17].

Based on the aforementioned overview of EV related accidents, it is plain that the functional safety of EEM is crucial to ensure the whole safety of EVs. Besides, there is a pressing need for efficient modeling methods of functional safety validation to assure EV safety, so as to improve road safety as a whole. The contributions discussed in the present paper fall within this context as detailed in the following section.

B. Contributions and outline

Since EVs are safety-critical systems, ensuring the correctness of their functional design and preventing malfunctions are of primary importance. In this paper, we propose a closed-loop dynamic synchronous functional validation (CL-DSFV) methodology based on the functional state model and interconnected synchronous simulation. The proposed CL-DSFV is applied to validating the completeness and correctness of the EEM function of the EV as an experiment. According to the outcomes of the application, the CL-DSFV allows us to achieve bidirectional validation with a dynamic synchronous visualization. Namely, we investigate whether each user behavior can trigger one transition and activate the corresponding functional state, and whether each state and transition can be covered by at least one user behavior. Specifically, the primary contributions of the present paper focus on the following aspects:

1) **Novel and holistic closed-loop dynamic process:** providing a holistic and closed-loop dynamic feedback functional validation process, which allows us to achieve bidirectional validation with a dynamic synchronous interaction. Such a holistic closed-loop dynamic process was rarely achieved in the relevant state of the art.
2) **Original transition engine and UIG algorithm:** developing a novel transition engine (TE) considering Usage Intention, Lifecycle State, User Location and Vehicle Status, to formalize the constraints on the transitions between the functional states of the FSM. Such comprehensive aspects related to usage and vehicle functionality features of the transition engine have not been completely taken into account in similar studies. Moreover, the original UIG algorithm (see Section III-D) is proposed to generate functional validation configurations automatically and achieve the automation of dynamic synchronous validation, which decreases time and labor cost.
3) **User intention oriented dynamic synchronous interaction:** creating dynamic synchronous interaction between the FSM and the user intention oriented simulation. Such one has not been achieved and applied in the functional validation of automobile industry, to the best of the authors' knowledge.

The remainder of this paper is organized as follows. Section II gives a review on related work in terms of functional safety analysis and validation. Section III elaborates on the proposed CL-DSFV methodology while going through the various stages of this methodology. Section IV is dedicated to the application of CL-DSFV framework on the considered EEM function. In Section V, we discuss the main outcomes of the application. Finally, concluding remarks and future work are outlined in Section VI.

II. Related work

In the literature, various methodologies are developed for the modeling and analyzing processes with the aim to validate functional safety and identify risks in complex systems. In early studies, for the sake of combining qualitative and quantitative analysis, the fault tree analysis (FTA) has been widely used for functional validation and risk analysis in various domains. FTA is a deductive top-down method, which aims at analyzing the possible combinations of initiating faults and events that may give rise to some feared events and providing the designer with an intuitive high-level abstraction of the system [18]. The failure mode and effects analysis (FMEA) has also been broadly used in various industrial domains to investigate the functional safety and reliability of high-risk systems [19]. FMEA is an inductive bottom-up analysis method aimed at analyzing the effects of single component/function failures on subsystem/equipment level. Compared with FMEA, FTA is more useful in showing how resistant a system is to single or multiple initiating faults. However, one obvious disadvantage of FTA is that it does not tell enough about the failure mechanism since, generally, the causal relationships between events are not a simple binary link (Yes or No). In addition, traditional static fault trees cannot handle the sequential interaction and functional dependencies between the system components. Consequently, it is necessary to employ dynamic methodologies to overcome these limitations [18].

Afterwards, to deal with the functional safety of complex and safety-critical systems, semi-formal/formal modeling approaches have been widely adopted, in particular for functional validation, reliability analysis and fault diagnosis. Among the notations that are commonly used in this context, one can cite the unified modeling language (UML) [20–23], state machines (SMs) [24–26] and Petri net (PN) [27–30]. Nowadays,

functional safety analysis and validation methodologies are required to deal with increasingly complex real-time systems with a large number of configuration parameters. To this end, such techniques should be equipped with the following characteristics [31]:

- having strong modeling ability,
- providing simple and efficient means to specify functional scenarios,
- having high computational efficiency,
- integrating domain expertise and causal knowledge,
- providing dynamic synchronized validation.

In this regard, new functional validation modeling methods based on the combination of semi-formal/formal modeling, fuzzy theory (FT), evidence theory (ET), neural networks (NN) and simulation have emerged in recent studies [24, 28, 30, 32–36, 38]. [24] proposed a neural-dynamic tracking framework to implement functional validation based on deep convolutional neural networks (Deep CNN, DCNN) and finite state machines (finite SMs). Namely, the DCNN acts as a key component to recognize patterns from a complex and changing environment, while the finite SM translates the recognized patterns into states and controls, and validates the functional behavior of the tracker tested in this study. A weighted fuzzy neural Petri net (WFNPN) was proposed by [28] to implement functional safety analysis and fault diagnosis of microgrids. This method created dynamic functional fault diagnosis models by means of PNs, and train specific parameters via the fuzzy neural network without excessive reliance on human experience. [30] proposed a novel dynamic PN model based on Dempster-Shafer (D-S) evidence theory to integrate knowledge inference for functional reliability modeling and validation of complex mechanical systems. This approach was applied to a satellite driving mechanism system, and the functional validation/evaluation process was improved due to the learning efficiency and knowledge accuracy of the developed dynamic PN model. [32] developed a systematic functional validation approach based on Stochastically and Dynamically Coloured Petri Nets (SDCPN) to validate the interactions between pilots and the Airborne Collision Avoidance System (ACAS). This model takes into account the technical, human and procedural elements relevant to the ACAS, which allows for assessing the fulfillment of the ACAS operation requirements and achieving the system functional confidence. A functional validation method was proposed in [33] to identify the inconsistency of development requirements and to improve behavioral flows by cross-checking with the state transition model based on UML diagrams. [36] proposed an integrated simulation-based approach to model EV driver behaviors using a multi-agent simulation platform, and to simulate EV's functions of interactions in both road transport and electric power systems, which allows the evaluation of functional safety of EVs. [37] developed an effective functional safety V&V platform for Electric Drive System (EDS) based on X-in-the-loop, and used the fault injection test as an example to show the effectiveness of the proposed approach. [38] presents a functional validation methodology based on the statistical scenario testing for evaluating autonomous vehicles' safety-related functionality in simulated scenarios. In this work, the authors formulated Scenarios Domain as a list of scenario characteristics with specified distributions and hierarchical dependencies, which is imported to a automatic testing simulation platform implemented through the Procedural Scenario Generation (PSG) algorithm. The classification of reviewed works in terms of the methods used is shown in Fig. 1. The comparison among the reviewed works in terms of the following assessment metrics: "Functional Behavior Validation (FBV)", "User Behavior Validation (UBV)", "Scenario Based Simulation (SBS)", "Expertise and Causal Knowledge Integration (ECKI)" and "State-Behavior Interconnected Dynamic Synchronous Validation (SBIDSV)" is shown in Table I.

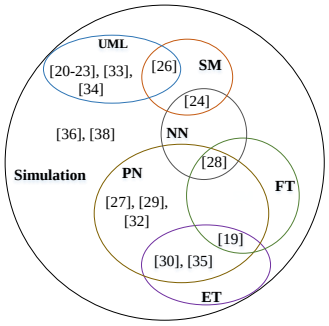


Fig. 1. The category of reviewed works in terms of methods.

TABLE I The comparison among the reviewed works.

References	FBV	UBV	SBS	ECKI	SBIDSV
[20-23], [34, 35]	+	–	–	–	–
[19], [26], [30]	+	–	–	+	–
[24], [28], [38]	+	–	+	–	–
[27], [29]	+	–	–	–	–
[32]	+	+	–	–	–
[33]	+	+	+	–	–
[36]	+	+	–	–	–

+: Advantage, –: Limitation

Despite the aforementioned approaches that show a relatively strong modeling ability and high computational efficiency, there is still a lack of efficient means to practically formalize the functional transitions between functional states/scenarios, and these approaches rarely considered domain expertise or causal knowledge. Moreover, few works focus on the dynamic synchronous validation between the user behaviors and functional design. Indeed, although dynamic modeling self validation (such as state-reachable validation, etc.) was addressed in numerous existing research works, the dynamic synchronous validation between user behaviors and functional design is a different problem. Therefore, in the present study, we are inspired to tackle these issues in the context of functional validation, while reducing physical tests so as to achieve cost efficiency, with our proposed approach.

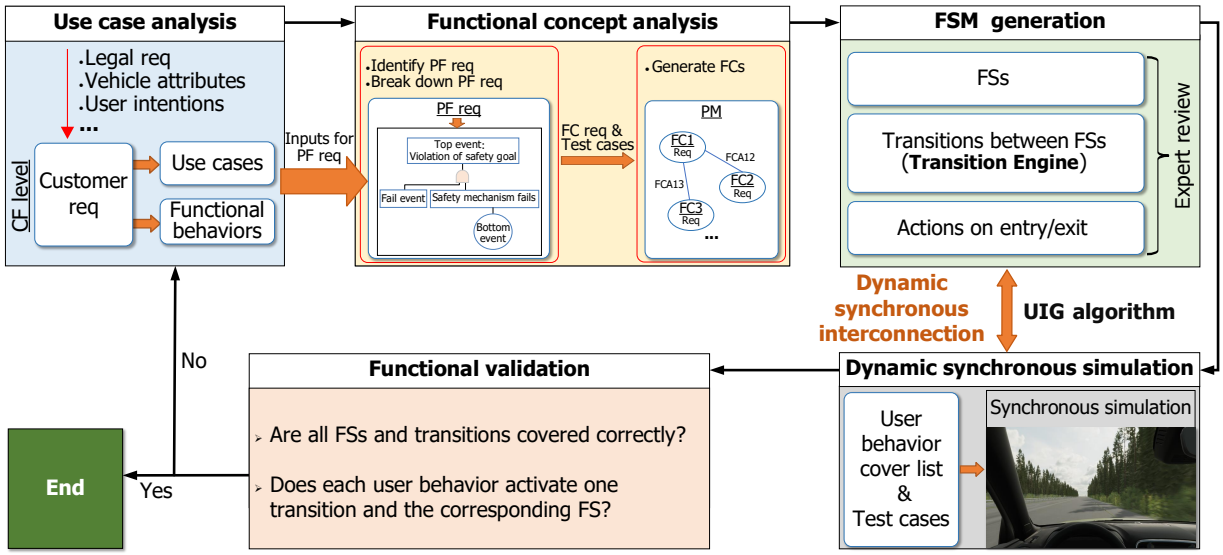


Fig. 2. The CL-DSFV pipeline ("PF", "PM", "FC", "FSM", "FS" and "req" represent product function, product module, functional capability, functional state model, functional state and requirement, respectively).

III. CL-DSFV FRAMEWORK

For a modeling paradigm to be efficient and relevant, it has to view an influential network not merely as passive parsimonious codes for storing factual knowledge, but also as a rational architecture for directing the causality flow of knowledge and representing characteristics of transitions between knowledge. While having in mind this principle, in this section, the CL-DSFV methodology is proposed. As shown in Fig. 2, the CL-DSFV framework consists of a set of sequential stages, namely starting from the use case analysis and functional concept analysis, going through the modeling description of functional states/transitions/actions on entry/exit, sequentially, simulating the user interaction with the system based on the dynamic synchronous interconnection between the functional state model (FSM) and the simulation platform, and ending with checking correctness and completeness of functions according to the user behavior cover list and test cases, followed by the iteration of functional design and validation when needed. The outputs of the last stage will be the inputs to the next stage. The CL-DSFV approach can achieve a holistic bidirectional validation through the closed-loop feedback pipeline to ensure the functional safety. The various stages of the framework, i.e., use case analysis, functional concept analysis, FSM generation, dynamic synchronous simulation and functional validation, are discussed in the following subsection.

A. Use case analysis

We may only have information about legal requirements, vehicle attributes and user intentions at the beginning of the EV design process. These preliminary materials are the inputs to build customer requirements, which consist of use cases and functional behaviors, as shown in **Definition 1**. Therefore, it is necessary to perform use case analysis based on the aforementioned inputs to generate use cases and functional behaviors, which constitute the basis of follow-up analyses. Via use case analysis, the knowledge at the customer function (CF) level can be broken down to the product function (PF) level.

Definition 1:

$$CustomerReq = \{UC, FB\}, \tag{1}$$

where $CustomerReq$ represents the set of customer requirements, UC denotes the set of use cases and FB is the set of functional behaviors.

B. Functional concept analysis

In order to acquire a clear understanding on the use cases and functional behaviors of the system, and facilitate their implementation in physical design, it is indispensable to further perform the functional concept analysis to identify the PF requirements followed by generating the functional capability (FC) as defined in **Definition 2**, with the inputs of use cases and functional behaviors generated from the previous stage. It is worth noticing that the FC represents an ability to provide the corresponding PF with a functionality or service and opens a way to reflect the contribution of a product module (PM) to the PF considered. Additionally, a PM consists of several function-correlated FCs. Therefore, we can use FC to understand the behavior of functionality crossing various modules. Moreover, the FC attribute (FCA) needs to be defined to contain the functionality or service of the corresponding FC. Namely, FCA is the carrier of the FC requirements.

During the functional concept analysis phase, the boundary of design needs to be defined firstly. Then, PF requirements shall be identified based on the use cases and functional behaviors. Note that the PF requirements contain safety and non-safety requirements. Hazard analysis has to be performed to distinguish safety requirements. Subsequently, FTA needs to be carried out to refine the PF requirements and break

down them to the FC level downstream. Meanwhile, based on the functional behaviors and PF requirements, FCs can be generated to carry the requirements that are broken down from PF level through FCAs. On the other hand, test cases can be designed to validate corresponding FC requirements as well.

Definition 2:

$$FC = \{FCA, FC\_Req\}, \tag{2}$$

where FCA is the set of functional capability attributes, and FC_Req is the set of functional capability requirements. As shown in Fig. 2, FC requirements are broken down from PF requirements.

C. FSM generation

Based on the obtained FCs, one can define the elements of the FSM, namely, functional states, transitions and actions on the entry/exit of functional states, and decide the relationships between these elements, so as to generate the FSM. The FSM needs to be reviewed by domain experts. In the present study, we leverage the *Rational Rhapsody* tool to build the FSM. In particular, we have originally developed a novel quadruple-category engine to formalize the feature of transitions between functional states, which is called Transition Engine (TE), as shown in **Definition 3**.

Definition 3:

$$TE = \{UI, LS, UL, VS\}, \tag{3}$$

where UI, LS, UL and VS denote the four categories Usage Intention, Lifecycle State, User Location and Vehicle Status, which are defined in Tables II, III, IV and V, respectively.

As shown in Tables II, III, IV and V, TE takes into account holistic aspects related to usage features and vehicle functionality features. Thus, this engine has a strong capacity to provide a thorough cognition when it comes to depicting the conditions of transitions and guiding the design of actions on entry/exit of functional states. Moreover, there is no doubt that with its versatility, TE can be applied to the whole automotive industry by having, not only a merely comprehensive but also in-depth understanding on the interaction between users and vehicles while considering all usage scenarios. The mode of thinking to develop this engine can also be migrated to other similar fields. Note that it is not mandatory to use all the four categories to constrain a transition if any of them is not applicable for a specific scenario, but at least one of them shall be used.

D. Dynamic synchronous simulation

In this stage, we originally propose a novel User Interaction Generation (UIG) algorithm to generate functional validation configurations automatically, as shown in **Algorithm 1**. The functional validation configuration file contains the information about TE, functional states, transitions and pairs of entry and exit conditions. Moreover, actions on entry/exit of functional states in the FSM are designed as data subscribers of the Message Queuing Telemetry Transport (MQTT) protocol to implement data exchange between the FSM and the simulation platform. Besides, the simulation platform is developed by the *Unity game engine*. The configuration file can be imported to *Unity game engine* based simulation platform directly, which can realize the automation of dynamic synchronous simulation by combining with actions on entry/exit of functional states. Additionally, the simulation platform is a virtual demonstrator that can represent a digital environment with a high degree of realism and industrial relevance.

Overall, with the novel UIG algorithm, we can create a

TABLE II Usage Intentions.

Usage Intention	Description
Approach	User intention to approach the vehicle;
Enter	User intention to enter the vehicle, including opening any door and getting inside the vehicle;
Settle in	User being inside vehicle and making preparations before taking off;
Drive	User or autopilot system being responsible for driving the vehicle with more or less support;
Communicate in Vehicle	User interacting with others inside or outside the vehicle, including, e.g., talking to riders in the back seat from the front seat;
Exit	User getting out of vehicle;
Leave	User intention to leave the vehicle;
Load Vehicle	User loading or unloading vehicle;
Offboard Control	User intention to use car service or view car status away from vehicle, including, e.g., preclimatization, monitoring, diagnostics and supervision;
Ride	User using vehicle for riding, rather than being responsible for driving task;
Passive Use of Vehicle	User being inside vehicle with no intention to use the vehicle for transport, including, e.g., sleeping or waiting in the vehicle;
Maintain Vehicle	User intention to keep vehicle in conditions ready for use, including refueling, charging, filling engine oil/abluent/washer fluid, etc., and having a possibility to clean the vehicle;
Produce Product	User intention to manufacture a product and perform needed activities in vehicle production.

TABLE III Lifecycle States.

Lifecycle State	Description
Normal	The nominal state of the vehicle;
Factory	The state when vehicle is produced in the factory (after the electrical system has been started up);
Transport	The state when vehicle is transported from the factory to the dealer;
Dyno	The state when vehicle is tested on a dynamometer;
Show	The state when vehicle is on show or in a dealer showroom;
Service	The state at service;
Crash	The state after a crash.

dynamic synchronous interaction between the FSM and the simulation platform.

TABLE IV User Locations.

User Location	Description
User in Zone 4	Distance $\geq$ 10 m from vehicle
User in Zone 3	10 m >Distance $\geq$ 6 m from vehicle
User in Zone 2	6 m >Distance $\geq$ 2 m from vehicle
User in Zone 1	Distance <2 m from vehicle
User in driver seat	
User in co-pilot seat	
User in 2nd row left seat	
User in 2nd row middle seat	
User in 2nd row right seat	
User in 3rd row left seat	
User in 3rd row right seat	

Note: here, we consider the vehicle with a maximum of seven seats (three rows).

E. Functional validation

After the dynamic synchronous interconnection between the FSM and the simulation platform is created, one can perform a dynamic functional validation by executing physical operations in the simulation platform. It is worth mentioning that the physical operations simulate the actions in reality according to the user behavior cover list extracted from the customer function requirement specification and the product function requirement specification. Meanwhile, the dynamic functional validation can be implemented and monitored through the visualization of the simulation platform that the physical operations are triggering corresponding transitions and activating corresponding functional states in the FSM.

Thus, one can assess if each user behavior triggers one transition and activates the corresponding functional state, and whether each state and each transition can be covered by at least one user behavior, so as to evaluate the correctness of bidirectional coverage between them. The validation is passed if the coverage is complete and correct; otherwise, the reasons for a failed validation need to be identified and the use case analysis shall be iterated, in reverse. Here, we assume that the user behavior cover list is correct as it is reviewed by domain experts. To sum up, the CL-DSFV provides a closed-loop control of dynamic synchronous interactive functional validation methodology to avoid the deviation between the user (customer) intention and the functional/system design.

IV. Industrial application

EEM is in charge of balancing, monitoring and distributing the power and energy between consumer domains and energy domains in EVs, whose internal functional blocks are shown in Fig. 3. Namely, EEM consists of the functionality blocks: Electrical energy coordination (EEC), Electrical energy conversion control (EECC), Low voltage energy control (LVEC),

TABLE V Vehicle Statuses.

Vehicle Feature	Status
Locks	Locked, Unlocked;
Alarm	Alarmed, Unalarmed;
Mirrors	Folded, Unfolded;
Door Handles	Deployed, Retracted;
Driver Door	Opened, Closed;
Co-pilot Door	Opened, Closed;
Second Row Left Door	Opened, Closed;
Second Row Right Door	Opened, Closed;
Driver Window	Opened, Closed;
Co-pilot Window	Opened, Closed;
Second Row Left Window	Opened, Closed;
Second Row Right Window	Opened, Closed;
Driver Seat	Occupied, Free;
Co-pilot Seat	Occupied, Free;
Second Row Seats (any)	Occupied, Unoccupied;
Third Row Seats (either)	Occupied, Unoccupied;
Third Row Backrest	Folded, Unfolded;
Hood	Opened, Closed;
Roof	Opened, Closed;
Trunk	Opened, Closed;
Driver Belt	In Use, Not in Use;
Co-pilot Belt	In Use, Not in Use;
Second Row Belts (any)	In Use, Not in Use;
Third Row Belt (either)	In Use, Not in Use;
Vehicle Movement	Parked, Standstill, Moving;
Brake Pedal	Depressed, Released;
Accelerator Pedal	Depressed, Released;
Trailer	Connected, Not Connected;
Power Level	Normal, Reduced, Critical;
Energy Level	Normal, Reduced, Critical;
VCU	PowerUp, PowerDown;
Charging Cable	Connected, Not Connected;
Thermal Activity	Request, Not Request;
Charging Condition	SWDL, AC Charging, DC Charging, Solar Charging.

Note: VCU represents vehicle computation unit, which is the core computer and controller of the vehicle. SWDL, AC and DC represent software download, alternating current and direct current, respectively. Here, we consider the vehicle with a maximum of seven seats (three rows).

HLCM, SLCM, BMS, HV battery system, Solar system and LV battery system. In this section, the CL-DSFV methodology is applied to the EEM function of EVs by collaborating with an original equipment manufacturer (OEM) in automotive industry, according to the corresponding stages described in

Algorithm 1: UIG Algorithm

Input: $UserBehavior$
/* inputting user behaviors from the ``user behavior cover list'' */
Parameters: $Entry$, $Exit$, $FunState$, $UsageIntention$, $Lifecycle$, $UserLocation$, $VehicleStatus$
/* defining initial variables of Entry, Exit, Functional State, Usage Intention, Lifecycle, User Location, and Vehicle Status */
Define $UserBehavior$ list ->{$UserBehavior$[$Entry$, $Exit$]}
/* defining the list of user behaviors that includes the variables Entry and Exit */
for each $UserBehavior$ **do**
    Search $UserBehavior$ in $UserBehavior$ list
    /* using UserBehavior as an index to find the corresponding UserBehavior[Entry, Exit] */
    Get $FunState$ according to $Entry$ and $Exit$
    /* obtaining the functional state of each user behavior according to corresponding Entry and Exit */
    Get input TE list ->{$UsageIntention$, $Lifecycle$, $UserLocation$, $VehicleStatus$} according to $FunState$
    /* generating the input TE list that includes variables Usage Intention, Lifecycle, User Location and Vehicle Status according to the functional state */
    Get output TE list ->{$UsageIntention$, $Lifecycle$, $UserLocation$, $VehicleStatus$} according to $FunState$
    /* generating the output TE list that includes variables Usage Intention, Lifecycle, User Location and Vehicle Status according to the functional state */
end for
Return $DataItem$->{$FunState$, $Entry$, $Exit$, input TE list, output TE list}
/* obtaining the data configuration file that includes Functional State, Entry, Exit, input TE list and output TE list for each user behavior */

Section III, which is discussed as follows.

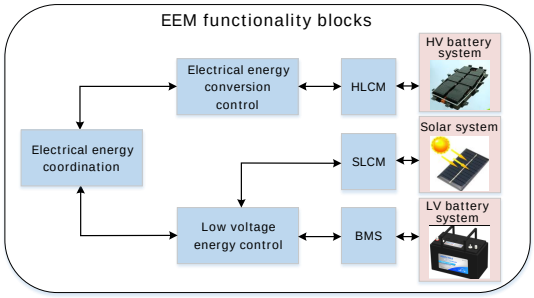


Fig. 3. EEM functionality block diagram.

A. Use case analysis and functional concept analysis

The use case analysis (refer to Section III-A) and functional concept analysis (refer to Section III-B) are carried out based on the legal requirements, vehicle attributes, user intentions, domain expertise and functional scenario decomposition flow chart. The process of requirement breakdown from CFs to the PF-EEM, then to FCs, is shown in Fig. 4. It is worth mentioning that the CF "Product Availability" handles the user intention of changing lifecycle modes and enabling vehicles for driving. The CF "Vehicle Charging" aims to provide users with an intuitive and easy way of accomplishing electrical energy transfer between an external energy provider and the high voltage battery. For space limitations, we directly give the FCs generated from functional concept analysis, without showing the intermediate process. The generated FCs are described in Table VI, which are the basis for the successive modeling work.

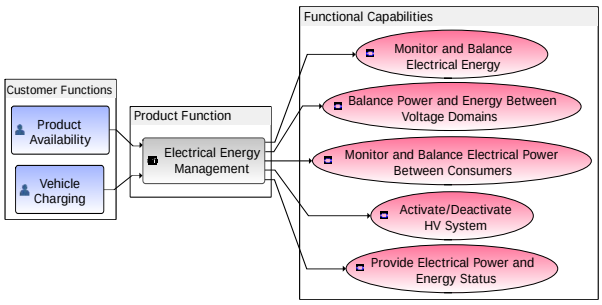


Fig. 4. The process of requirement breakdown from CFs to EEM, then to FCs.

Furthermore, the FTA is brought into play to investigate the safety goals at the FC level. Namely, FTA is carried out to break down safety requirements from the PF level to a specific FC. Taking "FC1-Monitor and Balance Electrical Power Between Consumers" for instance, Fig. 5 shows the FTA performed on the safety goal, namely, the safety requirement "REQ_138872" that "the HV battery discharge power limits shall be distributed correctly and timely in the degradation situation" (see the top event) at the PF level, and visualizes the process for breaking down "REQ_138872" to FC1. Specifically, the top event corresponding to the violation of "REQ_138872" is refined to the child requirements related

TABLE VI Description of FCs.

FC	Description
FC1-Monitor and Balance Electrical Power Between Consumers	Handling load control;
FC2-Balance Power and Energy Between Voltage Domains	Balancing power/energy among HV, LV and solar domains via HLCM and SLCM, and controlling the working modes of HLCM and SLCM;
FC3-Monitor and Balance Electrical Energy	Providing energy budget during parking and deactivating loads when the energy level is too low;
FC4-Provide Electrical Power and Energy Status	Monitoring electrical energy/power and reporting actual status to the vehicle, including LV electrical health;
FC5-Activate/Deactivate HV System	Handling the request to close/open contactors linked with power supply and enabling/disabling HV loads;

Note: HV, LV, HLCM and SLCM represent high voltage, low voltage, high to low voltage conversion management and solar to low voltage conversion management, respectively.

to thermal and propulsive (i.e., Longitudinal Vehicle Control, LVC) power limits (see bottom events), which are further allocated to the FC level through the FTA.

B. FSM modeling and dynamic synchronous simulation

Referring to Sections III-C and III-D, with the help of FCs and TE, the corresponding FSM is built as shown in Fig. 6. Here, we focus on the "EEMAvailable" part, which is divided into the parking and driving scenarios. One can notice that there are two parallel blocks within the "EEM_Parking" state, namely, "ElectricalConversion_Parking" and "HVEnergySystem_Parking". "EEM_Driving" is composed of two parallel blocks as well. Taking "ElectricalConversion_Parking" as an instance (the left block of "EEM_Parking"), it is refined from FC2, and contains four sub-states. The four sub-states represent four conversion modes, respectively; and the TE is employed to define the transitions among the four conversion modes.

Furthermore, the actions on entry/exit are defined for sub-states to implement the MQTT based communication interface between the FSM and the simulation platform. Taking the "HVPowerUp_Parking" sub-state inside "HVEnergySystem_Parking" (the right block of "EEM_Parking") as an example, the actions on entry/exit are designed as shown in Fig. 7. On the other hand, user interaction is generated automatically through the UIG algorithm (see **Algorithm 1**). Taking the user behavior "open the first left door" as an instance (see the red dashed-line box in Fig. 8), the configuration file and implementation in the simulation platform are shown in Fig. 8. Thus, by executing actions on entry/exit and UIG generated configurations, one can have a dynamic observation that the "HVPowerUp_Parking" sub-state is activated synchronously when the physical operation "Plug in charging cable" is performed in the simulation platform, as shown in the red dashed-line box in Fig. 9. The detailed interpretation of the FSM modeling is elaborated in Section V-B.

C. Functional validation

The functional validation according to the user behavior cover list and test cases (refer to Sections III-E) is performed based on dynamic synchronous simulation. Namely, we need to verify if each user behavior triggers one transition and activates the corresponding functional state, and whether each state and each transition can be covered by at least one user behavior, so as to assess the correctness of bidirectional coverage between them. Additionally, as we mentioned before, the user behavior cover list is extracted from the customer function requirement specification and the product function requirement specification, and reviewed by domain experts. With the help of the innovative functional validation process of the proposed CL-DSFV, we improved the physical design of the HV electrical system (compared to the preliminary design) in an all-wheel drive (AWD) EV, as shown in Fig. 10(a). Taking "FC5-Activate/Deactivate HV System" for instance, it shall realize the functionality to control HV battery main contactors, i.e., C1, C2 and C3 in the HV battery system as shown in Fig. 10(a). The interpretation on the design of controlling HV battery main contactors is elaborated in Section V-C.

V. Analysis and Discussion

The CL-DSFV performance evaluation, and the interpretation on the FSM modeling and the improvement on the physical design of controlling HV battery main contactors according to our approach will be elaborated in this section.

A. CL-DSFV performance evaluation

Based on the industrial application, we first assessed the superiority of our CL-DSFV approach by comparing with the quite relevant methods when considering the assessment metrics: FBV, UBV, SBS, ECKI and SBIDSV (see the definitions in Section II). The results are shown in Table VII. It is worth noticing that our CL-DSFV can achieve all the assessment metrics, and particularly, can implement SBIDSV. However, other methods can only fulfill two or three of the five metrics; especially, only two of other methods can achieve ECKI, and none of them can achieve SBIDSV.

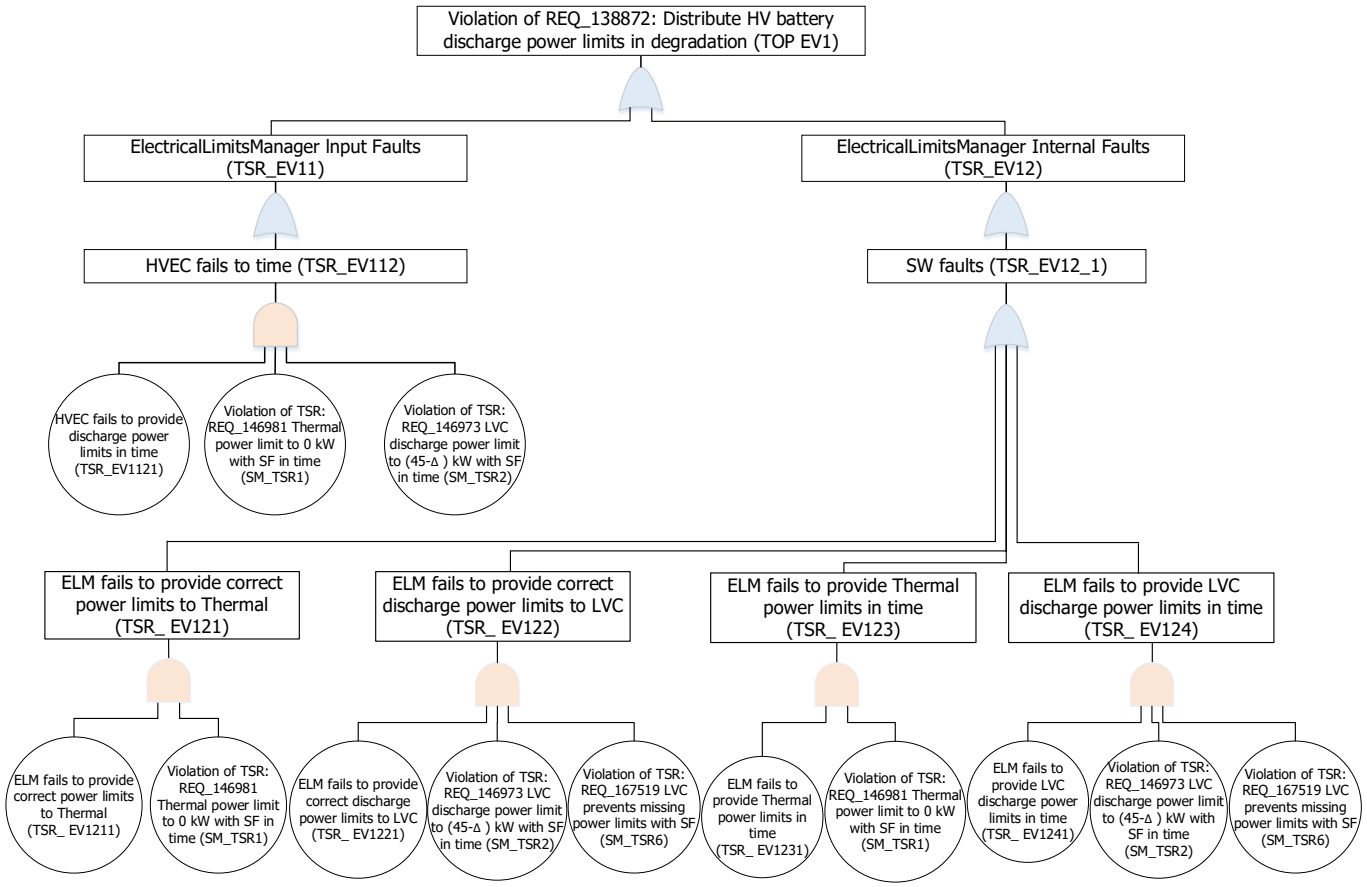


Fig. 5. The instance of FTA for breaking down "REQ_138872" to FC1 (REQ: requirement, EV: event, TSR: technical safety requirement, SM: safety mechanism).

TABLE VII Superiority assessment.

Methods	**FBV**	**UBV**	**SBS**	**ECKI**	**SBIDSV**
Wang et al. [24]	✓		✓		
Pal et al. [26]	✓			✓	
Jiang et al. [28]	✓		✓		
Peng et al. [30]	✓			✓	
Netjasov et al. [32]	✓	✓			
Morita et al. [33]	✓	✓	✓		
Marmaras et al. [36]	✓	✓			
Meltz et al. [38]	✓		✓		
Proposed CL-DSFV	✓	✓	✓	✓	✓

Moreover, we compared the detailed performance of our CL-DSFV approach with the State-Machine-UML combined (SM-UML) method proposed in [26], the dynamic evidential Petri net (PN-DE) method proposed in [30] and the UML based Crossing Check (UML-CC) method proposed in [33], which are the most similar approaches to our CL-DSFV among the methods referred in Table VII. Namely, we applied CL-DSFV, SM-UML, PN-DE and UML-CC approaches to the functional validation of EEM function for EVs. To implement the comparison, we considered 8 user behaviors relevant to thermal activity, charging, initiating driving and parking extracted from the user behavior cover list, which are opening/closing driver door, turning on/off engine, turning on/off air conditioner and plugging in/off charging cable. The comparison results are shown in Table VIII.

TABLE VIII Performance comparison between CL-DSFV and other referred methods.

Metrics	CL-DSFV	SM-UML	PN-DE	UML-CC
# UBC	8/8 (100%)	8/8 (100%)	7/8 (87.5%)	7/8 (87.5%)
# FSC	16/16 (100%)	21/21 (100%)	31/33 (94%)	24/24 (100%)
# TC	18/18 (100%)	33/36 (91.7%)	46/52 (88.5%)	44/46 (95.7%)
SBIDSV	Yes	No	No	No

UBC, FSC and TC are User Behavior Coverage, Functional State Coverage, and Transition Coverage, respectively.

One can notice that the UBC metric for EEM functional validation of our CL-DSFV outperforms that of PN-DE and UML-CC. The TC metric of CL-DSFV outperforms that of all the other three methods. The FSC metric of CL-DSFV outperforms that of PN-DE. Moreover, CL-DSFV can cover all user behaviors with much less functional states and transitions

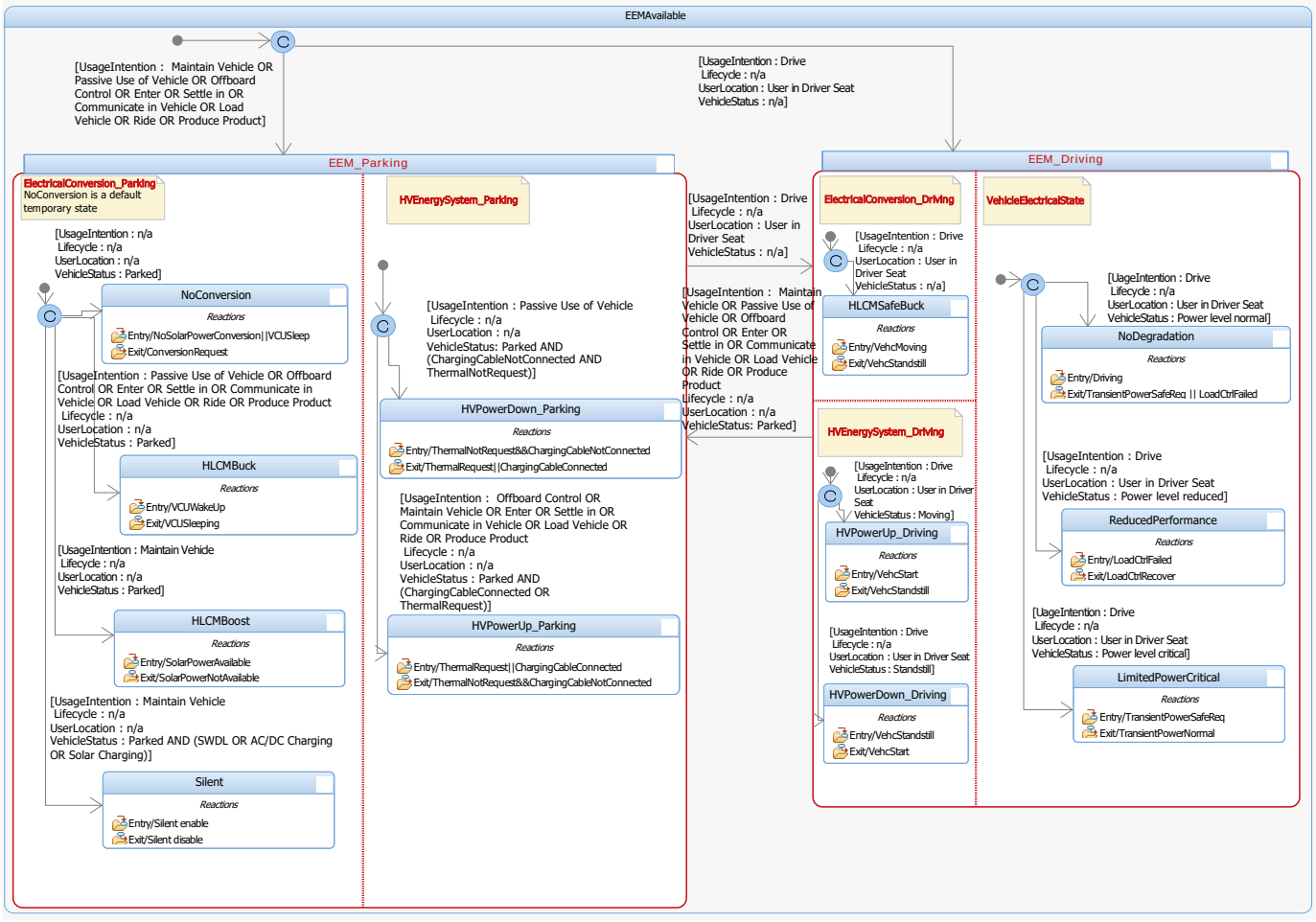


Fig. 6. The FSM of EEM ("n/a" means "not applicable").

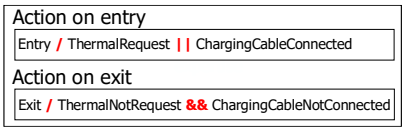


Fig. 7. The instance of actions on entry/exit.

due to the benefit of the proposed TE. Besides, the proposed CL-DSFV holds the unique advantage of "State-Behavior Interconnected Dynamic Synchronous Validation", which is not considered by any of the other three methods.

B. Interpretation on FSM modeling

The functionality of the five modules, i.e., "ElectricalConversion_Parking", "HVEnergySystem_Parking", "ElectricalConversion_Driving", "VehicleElectricalState" and "HVEnergySystem_Driving" as shown in Fig. 6, is elaborated as follows.

1) **"ElectricalConversio_Parking"** is refined from FC2, which contains four functional sub-states, i.e., "NoConversion", "HLCMBuck", "HLCMBoost" and "Silent". The function of "ElectricalConversion_Parking" is to balance power/energy among HV, LV and solar domains through HLCM and SLCM, control the working modes of HLCM and SLCM and provide them with setpoint voltages during parking. "NoConversion" is the default state and will transfer to "HLCMBuck" when the "Usage Intention" fulfills *Passive Use of Vehicle*, *Offboard Control*, *Enter*, *Settle in*, *Communicate in Vehicle*, *Load Vehicle*, *Ride* or *Produce Product*. The two categories "Lifecycle" and "User Location" are not applicable for this transition since they won't have different impacts on the transition when taking various values. Similarly, the transitions to other sub-states shall also follow the conditions defined by the TE, which are not garrulously described here.
2) **"HVEnergySystem_Parking"** is refined from FC1, FC3 and FC5. It contains two sub-states, i.e., "HVPower-Down_ Parking" and "HVPowerUp_Parking", to control HV loads and provide energy budget during parking. The EV will keep in the sub-state "HVPowerDown_Parking" when the "Usage Intention" is *Passive Use of Vehicle* and for "Vehicle Status", the vehicle is *parked*, the charging cable is *not connected* and the thermal activity is *not requested*. Otherwise, the EV will transfer to "HVPowerUp_Parking" if the "Usage Intention" is *Offboard Control*, *Maintain Vehicle*, *Enter*, *Settle in*,

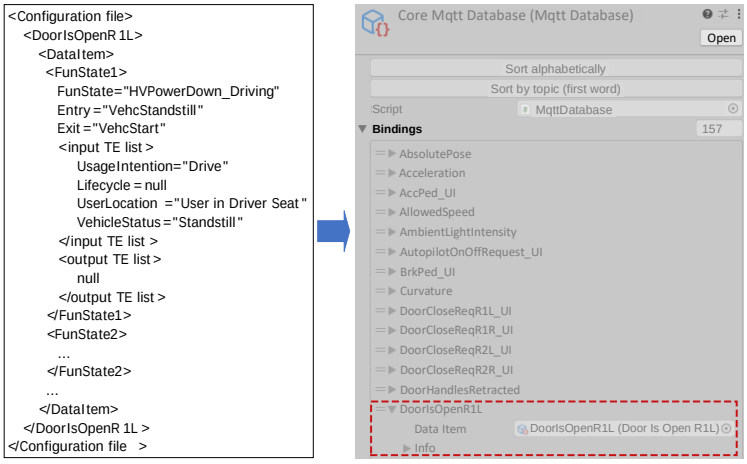


Fig. 8. The instance of UIG generated configuration file and implementation.

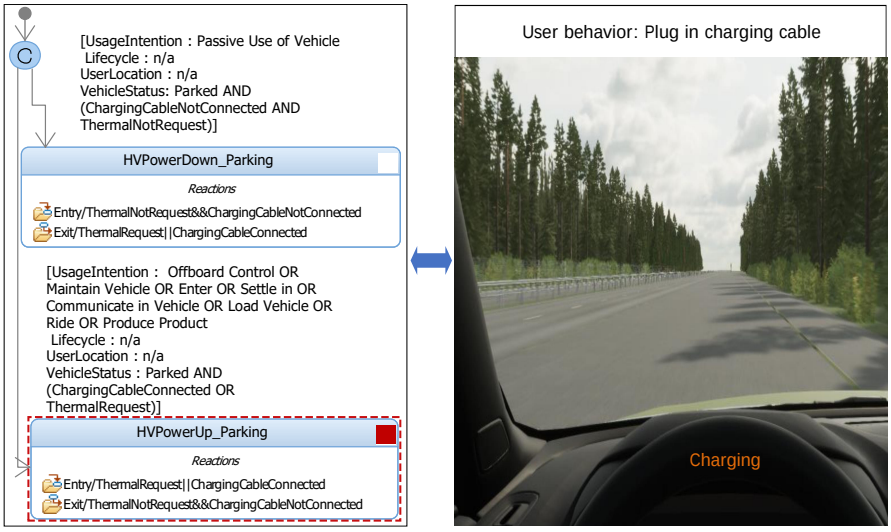
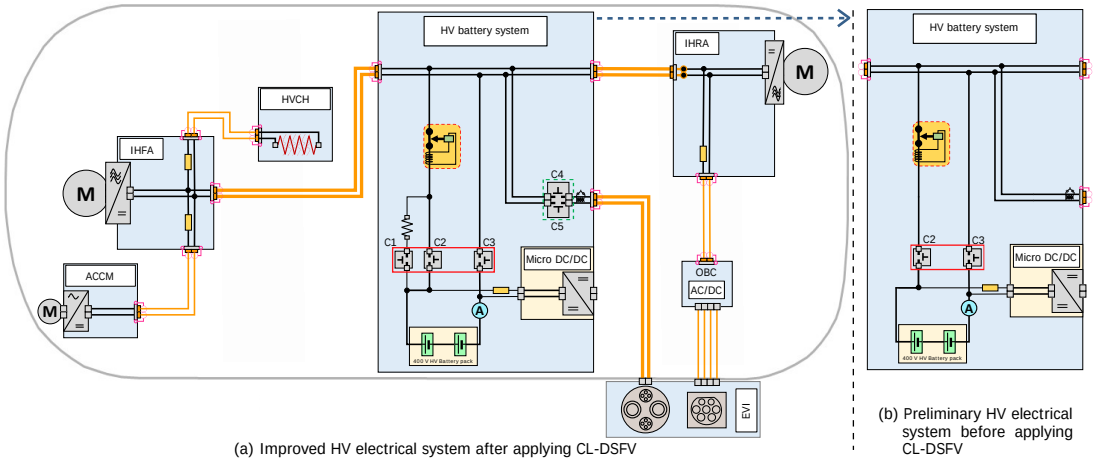


Fig. 9. The instance of Dynamic synchronous simulation.



(a) Improved HV electrical system after applying CL-DSFV

(b) Preliminary HV electrical system before applying CL-DSFV

Fig. 10. The HV Electrical system of an AWD EV (ACCM, EVI, HVCH, IHFA, IHRA, and OBC represent air conditioning control module, electrical vehicle inlet, high voltage coolant heater, inverter high-voltage front axle, inverter high-voltage rear axle, and on-board charger).

Communicate in Vehicle, *Load Vehicle*, *Ride* or *Produce Product* and for "Vehicle Status", the charging cable is *connected* or the thermal activity is *requested*.

3) **"ElectricalConversion_Driving"** is refined from FC2. It provides the sub-state "HLCMSafeBuck" to balance power/energy among HV, LV and solar domains through HLCM and SLCM, control the working modes of HLCM and SLCM and provide them with setpoint voltages during driving. The difference between "ElectricalConversion_Driving" and "ElectricalConversion_Parking" is that the "HLCMSafeBuck" is the unique functional state during driving, and it shall fulfill Automotive Safety Integrity Level (ASIL) C requested by the driving scenario. However, the four sub-states inside "ElectricalConversion_Parking" are required as Quality Management (QM, i.e., non-safety related). In detail, in "HLCMSafeBuck" state, HLCM shall convert HV power to safety-related LV network while regulating the voltage in the LV network according to the setpoint voltage with the fulfillment of ASIL C.
4) **"VehicleElectricalState"** is refined from FC1 and FC4. It contains three sub-states, i.e., "NoDegradation", "ReducedPerformance" and "LimitedPowerCritical", to control loads, provide LV power status to LV loads, and monitor and report actual power status to the EV. The EV will be in the state "NoDegradation", "ReducedPerformance" or "LimitedPowerCritical" when the "Vehicle Status" is equal to *Power level normal*, *Power level reduced* or *Power level critical*, respectively. When the power level reduces to the degradation level or critical limitation level, the EV shall take actions to ensure safe operation, e.g., shutting down the thermal system in a degradation situation or ensuring a safe stop in a critical limitation situation.
5) **"HVEnergySystem_Driving"** is refined from FC1 and FC5. It provides two sub-states "HVPowerUp_Driving" and "HVPowerDown_Driving" to enable/disable HV loads and provide energy budget during driving. The EV will be in the state "HVPowerUp_Driving" or "HVPowerDown_Driving" when the "Vehicle Status" is equal to *Moving* or *Standstill*, respectively, during driving.

C. Interpretation on physical design of controlling HV battery main contactors

As shown in Fig. 10(a), the HV Battery System is in the middle of the figure. The group of main contactors in the red solid-line rectangle consists of C1, C2 and C3, which are used for connecting the HV battery whenever EV loads need to consume HV energy, or the EV needs to be charged. Specifically, C1 and C2 are used for pre-charging and energy transfer, respectively. C3 is used for connecting the minus pole. C4 and C5 in the green dashed-line rectangle work together for fast-charging.

In the subsequent content, we take the thermal event, charging event, propulsion event and HV battery fault event as instances to clarify how the CL-DSFV approach guides and improves the physical design of HV battery main contactor control according to requirements. Through performing the use case analysis and the functional concept analysis, the FC5 is obtained (see Table VI), which is responsible for controlling HV battery main contactors as we mentioned in Section IV-C. Moreover, requirements related to thermal/charging/propulsion/HV battery fault events of FC5 are identified as follows:

- Req1-Thermal: when EEMS receives the thermal request, EEMS shall request to close the main contactors to connect the HV battery.
- Req2-Charging: when the charging cable is connected and EEMS receives the charging request, EEMS shall request to close the main contactors to initiate charging.
- Req3-Propulsion: when EEMS receives the vehicle start request, EEMS shall request to close the main contactors to initiate driving.
- Req4-HV battery fault: when EEMS receives the HV battery fault signal, EEMS shall request to open the main contactors to disconnect the HV battery.

Then, the correctness of design in terms of functions and the consistency between the physical design and the requirements above are validated based on the FSM, dynamic synchronous simulation, and coverage validation (see Section IV-C) according to the user behavior cover list and test cases (confidential documents of the OEM). Here, the user behaviors defined in the user behavior cover list to activate the functional states of the FSM are "Heating vehicle" for Req1, "Plug in charging cable" for Req2, "Press start button" for Req3, and any of the three user behaviors above combined with HV battery fault injection test cases for Req4.

Fig. 10(b) shows the preliminary design before we apply the CL-DSFV approach. One can notice that contactors C1, C4 and C5 are missing in the preliminary design, compared with Fig. 10(a) that the CL-DSFV approach has been applied. Actually, in the preliminary design the short circuit of main contactors has failed to be considered while fast-charging is initiated in an HV battery fault event, which can cause a single point failure. With the help of the CL-DSFV, we identified this flaw, added the contactor C1 and improved the preliminary design. Moreover, we added the fast-charging contactor group (i.e., C4 and C5), designed the combination of C1 and the fast-charging contactor group to prohibit charging in the HV battery fault event, and enabled the notification "Battery warning, service urgent" to users as well, so as to eliminate the single point failure, during the iteration of the CL-DSFV framework.

D. Discussion

By collaborating with the OEM in automotive industry (unfortunately due to the OEM's confidential policy, we are not able to provide more detailed materials), we have applied the CL-DSFV approach to the development of certain products, which testified to the effectiveness of the proposed approach. More importantly, the transition engine provides a way to construct a relatively comprehensive causal knowledge flow from parent states to child states with the integration of domain

expertise, since it has considered holistic aspects related to usage features and vehicle functionality features.

In the present study, the domain expertise has been introduced to the process of use case/functional concept analyses, transition engine design and user behavior cover list development. Academic researches have over the years developed a plethora of design methods and tools with the intention of improving the efficiency and effectiveness of the product development process. There is a well-recognized challenge to successfully bridge the step from researches into practices. The bilateral transfer of knowledge between academia and practitioners poses a key question to the research community about how research can be made more actionable. It is worth noticing that leveraging domain expertise wisely is the very bridge crossing the gap that one wants to eliminate. In details, the integration of domain expertise can provide a sound interpretation on causal knowledge between parent functional states and child states, and during the process of use case analysis and functional concept analysis. On the other hand, since academic research often focuses on theoretical advancements and innovations, while industrial practices prioritize practical and cost-effective solutions; taking that into consideration, we strongly recommend establishing partnerships between academic institutions and industries, and encouraging domain experts to participate in academic research. For example, in our case we require the analyses, modeling process, development of the user behavior cover list and test cases, and validation process to be reviewed by domain experts to transfer the domain knowledge into actionable real-world design.

Furthermore, the developed virtual synchronous simulation in our work realizes the interconnection between product FSM states and customer behaviors. Namely, it gives a perceptual intuition on the dynamic connection between industrial design and customer behavior features based on the TE flow, and alleviates the cost of physical testing. Via the dynamic synchronous validation and the closed loop of function decomposition/reversed updating, one can obtain a deeper understanding on customer requirements and functional behavior features to develop a more practical product.

VI. Conclusions

In the present study, an effective and comprehensive approach for functional validation, called CL-DSFV, is proposed. In theory, the CL-DSFV methodology achieves a holistic and closed-loop feedback functional validation, and consists of the original UIG algorithm, user intention oriented dynamic synchronous interaction method, the proposed TE method, and domain expertise and causal knowledge integration. Additionally, mainly due to the design of TE, and integration of domain expertise and causal knowledge, our approach holds both academic contributions and industrial engineering practicability. Namely, we bridge the gap between academic research and industrial practices, to some extent; taking that into consideration, our approach is quite meaningful. The performance evaluation (see Section V-A) shows its superiority regarding the aspects of FBV, UBV, SBS, ECKI and SBIDSV, compared with existing reviewed works. The industrial application (see Sections IV and V) improves the design of HV battery system of the EV, and show its strong capacity for dealing with a complete end-to-end design optimization process based on a low-cost virtual validation.

The CL-DSFV is a general methodology that can be migrated to other similar domains in terms of functional validation. Namely, one just needs to perform corresponding analyses, create the FSM model and user behavior cover list for the specific product function.

A. Major contributions compared with reviewed papers

The major contributions compared with existing reviewed papers are as follows:

1) A novel and comprehensive transition engine, called TE is a medium to deliver comprehensive causal knowledge from parent states to child states. In addition, it can be generally applied to other functions or systems in the automotive industry.
2) As investigated in Section II, only our approach can achieve the user intention oriented state-behavior interconnected dynamic synchronous validation, based on the UIG algorithm and actions on entry/exit of functional states, compared with existing relevant works reviewed, which gives a visualization on the dynamic connection between industrial designs and customer behavior features, moreover, decreases the cost of realization of physical testing.
3) The integration of domain expertise and causal knowledge into the use case/functional concept analyses, transition engine design and user behavior cover list development can optimize the decomposition from customer behaviors to functional behaviors and the reversed updating of functional design in the closed-loop process, and can eliminate the knowledge gap between academic researches and industrial practices.

B. Limitations and future work

Several limitations of the proposed approach need to be addressed: a) the validity of safety requirements identified from the functional concept analysis can be impacted by the depth and spectrum of operators' knowledge; b) for a complex functional system, the functional state space might be huge, which will be result in a high computation cost of coverage tests. Thereby, to respond to the limitations above, the directions of future work can be expected in what follows: i) CNNs will be introduced to learn safety requirements and design safety constrain regularizers to recognize safety patterns; ii) the functional state space shall be minimized by optimizing the functional concept analysis, functional architecture and decomposition, and enhancing semantic capacity of model language.

References

[1] H. B. Wang, Y. Li, Q. Z. Wang, Z. M. Du, X. N. Feng, "Mechanisms causing thermal runaway-related electric vehicle accidents and accident investigation strategies," *Energy Storage Science and Technology*, vol. 10, no. 2, pp. 544–557, 2021.

[2] Albero project, "Evaluation of accident statistics on electric vehicles regarding to the cause of the accident," *Work package 2.2*, Federal Ministry of Education and Research, Germany, 2021.

[3] R. Irle, Global EV Sales for 2021. [Online]. Available: https://www.ev-volumes.com/

[4] VIRTA, "The global electric vehicle market overview in 2022: statistics & forecasts." [Online]. Available: https://www.virta.global/en/global-electric-vehicle-market

[5] IEA, Global EV Outlook 2022. [Online]. Available: https://www.iea.org/data-and-statistics/data-product/global-ev-outlook-2022

[6] D. Goswami, M. Lukasiewycz, M. Kauer, S. Steinhorst, A. Masrur, S. Chakraborty, S. Ramesh, "Model-based development and verification of control software for electric vehicles," in *Proceedings of the 50th Annual Design Automation Conference*, NY, USA, pp. 1–9, 2013.

[7] P. Bhagdikar, J. Sarlashkar, S. Gankov, S. Rengarajan, W. Downing, W., S. Hotz," Model Based Validation of Intelligent Powertrain Strategies for Connected and Automated Vehicles,"in *2023 IEEE International Systems Conference (SysCon)*, pp. 1–3, IEEE, 2023.

[8] J. Guo, Y. Li, H. Li, S. Li, Y. Zhu, "Construction of user abnormal behavior detection model based on smart charging platform for electric vehicles," in *International Conference on Electronic Information Engineering and Data Processing (EIEDP 2023)*, vol. 12700, pp. 827–836, SPIE, 2023.

[9] P. Dini, G. Ariaudo, G. Botto, F. L. Greca, S. Saponara, "Real-time electro-thermal modelling & predictive control design of resonant power converter in full electric vehicle applications," *IET Power Electronics*, vol. 16, pp. 2045-2064, 2023.

[10] D. Stephens, P. Shawcross, G. Stout, E. Sullivan, J. Saunders, S. Risser, J. Sayre, "Lithium-ion battery safety issues for electric and plug-in hybrid vehicles (Report No. DOT HS 812 418)," Washington, DC: National Highway Traffic Safety Administration, 2017.

[11] F. Lambert, 2016. Tesla says Model S fire in France was due to electrical connection improperly tightened' by a human instead of robots. Electrek.co. [Online]. Available: https://electrek.co/2016/09/09/tesla-fire-france-electrical-connection-improperly-tightened-human-robot/

[12] National Highway Traffic Safety Administration, "NHTSA defect petition DP19-005," 2019.

[13] S. Graham, Everything we know about the Chevy Bolt EV fires. Electrek.co., 2021. [Online]. Available: https://electrek.co/2021/07/28/everything-we-know-about-the-chevy-bolt-ev-fires/#h-october-6-2020-port-st-lucie-fl

[14] National Fire Data Center (NFDC), Highway Vehicle Fires. [Online]. Available: https://www.usfa.fema.gov/downloads/pdf/statistics /v19i2.pdf, 2018.

[15] J. Q. Chen, M. M. Liu, Y. J. Zhou, "Experimental study on safety of automotive NCM battery under different abuse conditions," *Automotive Engineering*, vol. 42, no. 1, pp. 66–73, 2020.

[16] X. N. Feng, S. Q. Zheng, D. S. Ren, "Investigating the thermal runaway mechanisms of lithium-ion batteries based on thermal analysis database," *Applied Energy*, vol. 246, pp. 53–64, 2019.

[17] W. F. Li, H. W. Wang, M. G. Ouyang, "Theoretical and experimental analysis of the lithium-ion battery thermal runaway process based on the internal combustion engine combustion theory," *Energy Conversion and Management*, vol. 185, pp. 211–222, 2019.

[18] C. Liang, M. Ghazel, "A risk assessment study on accidents at French level crossings using Bayesian belief networks," *International journal of injury control and safety promotion*, vol. 25, no. 2, pp. 162–172, 2018.

[19] H. Shi, L. Wang, X. Y. Li, H. C. Liu, "A novel method for failure mode and effects analysis using fuzzy evidential reasoning and fuzzy Petri nets," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 6, pp. 2381–2395, 2020.

[20] L. Baresi, A. Morzenti, A. Motta, M. Rossi, M., "A logic-based approach for the verification of UML timed models," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 26, no. 2, pp. 1–47, 2017.

[21] Z. Daw, J. Mangino, R. Cleaveland, "UML-VT: A formal verification environment for UML activity diagrams," in *MoDELS 2015 Demo and Poster Session co-located with ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MoDELS 2015)*, 2015, pp. 48–51.

[22] T. S. Gasheva, D. I. Vlasov, A. V. Otinov, N. N. Datsun, "Validation automation of UML diagrams created by students," *ISP RAS (Russian)*, vol. 33, no. 4, pp. 7–18, 2021.

[23] M. Ghazel, A. Toguyéni, M. Bigand, "A semi-formal approach to build the functional graph of an automated production system for supervision purposes," *International Journal of Computer Integrated Manufacturing*, vol. 19, no. 3, pp. 234–247, 2006.

[24] J. Wang, J. Song, M. Chen, Z. Yang, 2015. "Road network extraction: A neural-dynamic framework based on deep learning and a finite state machine," *International Journal of Remote Sensing*, vol. 36, no. 12, pp. 3144–3169, 2015.

[25] A. Boussif, M. Ghazel, J. C. Basilio, "Intermittent fault diagnosability of discrete event systems: an overview of automaton-based approaches," *Discrete Event Dynamic Systems*, vol. 31, no. 1, pp. 59–102, 2021.

[26] Y. Pal, S. Kumar, M. Singh, S. Dwivedi, "Validation of DNAFIDs model through Finite State Machine," *Reliability: Theory & Applications*, vol. 16. no. 3 (63), pp. 160–167, 2021.

[27] A. Boussif, M. Ghazel, K. Klai, "A semi-symbolic diagnoser for fault diagnosis of bounded labeled petri nets," *Asian Journal of Control*, vol. 23, no 2, pp. 648–660, 2021.

[28] T. Jiang, C. Du, S. Guo, T. Yin, "Microgrid fault diagnosis model based on Weighted Fuzzy Neural Petri

Net," in *IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2020, vol. 1, pp. 2361–2365.
[29] B. Liu, M. Ghazel, A. Toguyéni, "On-the-fly and incremental technique for fault diagnosis of discrete event systems modeled by labeled petri nets," *Asian Journal of Control*, vol. 19, no. 5, pp. 1659–1671, 2017.
[30] W. Peng, J. Zhang, J. Zhang, "Novel dynamic evidential Petri net for system reliability analysis," *Journal of Systems Engineering and Electronics*, vol. 28, no. 5, pp. 1019–1027, 2017.
[31] C. Liang, M. Ghazel, O. Cazier, L. Bouillaut, "Advanced model-based risk reasoning on automatic railway level crossings," *Safety science*, vol. 124, 104592, 2020.
[32] F. Netjasov, A. Vidosavljevic, V. Tosic, M. H. Everdij, H. A. Blom, "Development, validation and application of stochastically and dynamically coloured Petri net model of ACAS operations for safety assessment purposes," *Transportation Research part C: emerging technologies*, vol. 33, pp. 167–195, 2013.
[33] H. Morita, S. Matsuura, "Validation method to improve behavioral flows on UML requirements analysis model by cross-checking with state transition model," *arXiv preprint arXiv:2103.00781*, 2021.
[34] N. Przigoda, P. Niemann, J. Gomes Filho, R. Wille, R. Drechsler, "Frame conditions in the automatic validation and verification of UML/OCL models: A symbolic formulation of modifies only statements," *Computer Languages, Systems & Structures*, vol. 54, pp. 512–527, 2018.
[35] Y. Zhang, W. Wu, "Flight mission modeling based on BDI Petri net," *Journal of Systems Engineering and Electronics* vol. 28, no. 4, pp. 776–783, 2017.
[36] C. Marmaras, E. Xydas, L. Cipcigan, "Simulation of electric vehicle driver behaviour in road transport and electric power networks," *Transportation Research Part C: Emerging Technologies*, vol. 80, pp. 239–256, 2017.
[37] W. Bin, W. Fang, M. Kai, H. Xin, X. Kun, R. Shan, "Functional Safety Verification and Validation Platform for Electric Drive System Based on X-in-the-Loop," in *International Joint Conference on Energy, Electrical and Power Engineering,* Singapore: Springer Nature Singapore, pp. 1195-1203, 2022.
[38] D. Meltz, H. Guterman, "Functional safety verification for autonomous UGVs—Methodology presentation and implementation on a full-scale system," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 3, pp. 472–485, 2019.

Ci Liang (Senior Member, IEEE) is currently a tenured Associate Professor and the Ph.D. Supervisor with Harbin Institute of Technology. Ci Liang received the Ph.D. degree from Université de Lille in 2018. Ci Liang serves as a committee member of the IFAC TC 7.4 Transportation Systems, the guest editor of SAE International Journal of CAV, Chair of SafeComp workshop. Ci Liang has been nominated for the 8th Abertis Traffic Safety International Award in 2019, and the first European "Women's Railway Research and Innovation Award" in 2018.

Mohamed Ghazel is Director of the ESTAS group with the University Gustave Eiffel (previously IFSTTAR). He received the Master and Ph.D. degrees from The École Centrale de Lille in 2002 and 2005, respectively. His research mainly focuses on the engineering, safety and interoperability of transportation systems. Dr. Ghazel is a member of the IFAC technical committees TC 7.4 on Transportation Systems and TC 9.2 on Social Impact of Automation. He acts as an expert for the European Commission in the framework of innovation programs since 2016.

Chi Xie is currently a Tenured Professor in the School of Transportation Engineering at Tongji University. He obtained his B.Eng., M.Eng., and Ph.D. from Tsinghua University, National University of Singapore, University of Massachusetts, and Cornell University, respectively. Prof. Xie was a recipient of the Young Talent Award from the China Recruitment Program of Global Experts in 2013. At present, Prof. Xie serves as an Associate Editor of Socio-Economic Planning Sciences, Transportation Letters, and Transportation Science and Technology. His current research interests focus on analyzing and optimizing large-scale transportation and infrastructure networks, transportation-electricity megasystems.

Wei Zheng is currently a Professor and the vice Director of National Research Center of Rail Transportation Safety Assessment, Beijing Jiaotong University. He received the B.Sc., M.Sc., and Ph.D. degrees in control science and engineering from Harbin Institute of Technology, China, in 1997, 1999, and 2002, respectively. He was the Alexander von Humboldt Fellow from 2013 to 2014. His research interests include safety assessment and assurance of safety-critical systems.

Wei Chen (Senior Member, IEEE) is currently the Technical Manager of overseas region of Ruijie Network Co., LTD. He received the B.S. in control technology & instrumentation from Beijing Institute of Technology in 2011. Since 2017, he has been working at Ruijie Network Co., LTD. He is mainly responsible for data communication and network artificial intelligence for ITS, and switch protocol stack pre-research.