International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Verification and Validation Architectures for Centralized Compute in Electric Vehicles

Abhishek Devgan

Senior QA Engineer

Abstract:
The fast development of Electric Vehicles (EVs) has caused a paradigm shift in the conventional distributed Electronic Control Unit (ECU) to large centralized computing architectures. The change is one of the pillars of the Software-Defined Vehicle (SDV) generation that allows new functionality like autonomous driving, vehicle-to-grid (V2G) energy trading, and over-the-air (OTA) updates. Nevertheless, the process of centralizing important functions into a central-like brain creates enormous complications in the provision of system reliability, functional safety, and cybersecurity. This paper will consider the new Verification and Validation (V&V) architectures based on centralized compute environments in EVs. We examine the current E/E (Electrical/Electronic) architectural tendencies, and shifted toward domain-controlled to zonal systems and fully centralized system. One of the major areas of focus is high-confidence V&V techniques, such as Hardware-in-the-Loop (HiL) E-horizon-function simulation, lightweight authentication protocols in secure automotive networks, and blockchain-based privacy-preserving data exchange and energy transactions. Additionally, this research also examines simulation toolchains and modeling environment that are necessary to test the interaction between complex software stacks and centralized hardware. This research is a synthesis of existing literature on the topic of decentralized security and centralized processing and thus represents an overall roadmap of testing the next generation of safe, secure and cross operationalized systems of electric vehicles.

Keywords: Centralized E/E Architecture, Electric Vehicles (EV), Software-Defined Vehicles (SDV), Verification and Validation (V&V), Cybersecurity, Blockchain, Hardware-in-the-Loop (HiL), Autonomous Systems, Vehicle-to-Grid (V2G), Functional Safety.

I. INTRODUCTION

The car industry has entered a radical paradigm shift with the traditional distributed Electronic Control Units (ECUs) being built into high-performance centralized compute architectures [9]. The main reason behind this shift is the Software-Defined Vehicles (SDVs) and the growing sophistication of automotive software necessary to support connected, autonomous electric vehicles [4] [22]. The formation of the electrical and electronic (E/E) architecture is needed in the centralization of the architecture to address the power needs and the high-speed processing of data of the current automated platforms [2]. The architectures should be able to combine important vehicle functions, including traction control and antilock braking to individually controlled electric motors and ensure high standards of safety and functionality [7] [13]. Nonetheless, this integration poses major Verification and Validation (V&V) problems, especially on the security and integrity of the vehicle-to-everything (V2X) interface and energy trading mechanisms [6] [15]. To deal with these weaknesses, researchers are considering lightweight authentication and authorization structures that aim to ensure that internal networks are not compromised by advanced cyber threats [5] [20] [21]. Moreover, blockchain technology integration is already a step to a high-confidence energy sharing and safe cloud-edge computing in the Internet of Electric Vehicles [1] [3] [10]. The current V&V methods are now more and more using Zero-Knowledge Proofs (ZKP) and decentralized computation in the context of privacy-preserving authentication when charging and grid-to-vehicle power is being exchanged [8] [14] [19]. These systems also need advanced toolchains to develop

architecture, model, and simulate to battery electric vehicles [24]. State-of-the-Art Hardware-in-the-Loop (HiL) systems are currently being implemented with embedded connectivity to test electronic horizon functionalities and interoperability of reservation systems in real time environment simulation [12] [25]. Finally, comprehensive V&V architecture of centralized compute should be able to reconcile between cyber-physical security and multifaceted functional needs of energy-efficient, autonomous mobility [16] [17] [18].

II.LITERATURE REVIEW

Al-Saif et al. (2021): The fundamental issues related to the development of a decentralized energy sector, and the use of distributed ledgers to improve the level of transparency for such a system, are discussed. It is a comprehensive road map for the adoption and operation of safe and efficient energy trading standards for the modern automobile sector [1].

Baxter et al. (2018): The need for a transition to high-power designs for the different sensor and processing units is also discussed. The need for a proper power distribution system is emphasized, as this is required for functional safety to be achieved for the development of future autonomous driving technologies [2].

Sun et al. (2020): The security and trust concerns for the peer-to-peer exchange of energy among mobile energy storage units through a decentralized consensus are also discussed. The findings have shown that a distributed ledger system can improve the reliability and efficiency of power distribution [3].

Vdovic et al. (2019): The trend towards software-defined design and the need to integrate a plethora of functional modules are discussed. The use of software is important for the increased level of data streams and control required for the future electric vehicles [4].

Mundhenk et al. (2017): The security of automotive networks, especially in the context of light-weight authentication and authorization protocols. The article discusses the resource constraints of automotive systems and the ways in which the communication channels could be secured against advanced cyber-attacks. The research provides the foundation for the integrity and security of data and systems, while also ensuring the efficiency of automotive electronics [5].

Saha et al. (2021): Discussed the security of the Internet of Energy Electric Vehicle platform interface using blockchain technology. The authors investigate the ways in which the interface could be secured using blockchain technology, especially in the context of the advantages that could be derived from the decentralized nature of the system, especially against malicious attacks and the safe two-way power transfer between the grid and the vehicles. This is an important ingredient in the development of energy infrastructure, especially to meet the growing energy demands of sustainable transport [6].

Ivanov et al. (2015): Discussed the traction control and anti-lock braking system (ABS) in all electric vehicles (EV) that have independent control over the motors. According to the authors, the system is much better and safer compared to the traditional mechanical brakes. The authors' findings could be used as guidance in the development of ways in which the stability and energy recovery could be improved in vehicles through the electronic control of the torque produced by the motor [7].

Gabay et al. (2020): Discussed the development of a privacy-preserving authentication system for connected electric vehicles using blockchain and zero-knowledge proofs. The authors' proposed method is an excellent way to ensure the security of the networks while also balancing the need for the security of the networks against the growing need for the privacy of the users [8].

Bandur et al. (2021): There should be a move to centralize automotive E/E designs for a complex vehicle. In this paper, the author compares a classical distributed system with central controllers with the advantage of quicker data processing and software update. The authors argue that the only evolution required to sustain high-performance computing for supporting autonomy is centralization [9].

Liu et al. (2018): The electric vehicle cloud and edge computing platform based on blockchain technology for security. In this article, the authors have explained how decentralized trust management can reduce the risk of data breaches and other forms of unauthorized access in connected vehicle systems. The authors

have proposed a scalable vehicle-to-cloud computing architecture with edge computing and blockchain technology for safe and efficient vehicle-to-cloud connections [10].

Pustišek et al. (2016): The blockchain technology can be used for an autonomous choice of electric vehicle charging stations according to user preferences and energy grid availability. In this study, the authors have proposed a method for electric vehicles to negotiate and reserve a charging spot without an intermediary. It can greatly simplify the process of charging electric vehicles and can lead to a more competitive and customer-oriented energy supply market for EV users [11].

Basmadjian et al. (2020): The "reference architecture of interoperable reservation systems within the electric vehicle charging infrastructure." It is also interested in the interoperability of communication among different service providers, so users can connect to different networks. The paper talks about the "dispersion of existing charging services, paving the way to a converged and accessible sustainable mobility ecosystem" [12].

Nagarjuna Reddy Aturi (2022): The neuroplasticity of yoga, which is an artificial intelligence/neural imaging study to translate cognitive functions and brain state changes. This paper will discuss the ability to reverse cognitive decline through various forms of mindfulness, which can be measured in the brain's structure and function. The paper discusses new discoveries about neuro-rehabilitation, which relates to ancient forms of wellness and computers [13].

Darby and Gottumukkala (2019): The decentralized computing techniques, which can be used to support cyber-physical security in electric and autonomous vehicles. The article discusses the ability of a centralized system to be prone to "single points of failure," which can be solved using decentralized computing. The authors find that decentralized architecture has a pivotal role in the "safety and security of the future transportation grids" [14].

III.KEY OBJECTIVES

Study the Move to Centralized E/E Architectures: Compare the transition of the traditional distributed or domain based Electronic/Electrical (E/E) architectures to high performance centralized compute hubs to simplify vehicle control [9] [13] [22].

Develop Strong Software Management Infrastructures: Specify the Verification and Validation (V&V) criteria of sophisticated automotive software in the context of Connected and Autonomous Electric Vehicles (CAEVs) to guarantee a smooth update and integration [4].

Introduce Advanced Hardware-in-the-Loop (HiL) Testing: Design integrated HiL systems to perform a verification of centralized connectivity and "eHorizon" functionality, to ensure real-time performance at a strictly controlled environment [25].

Test Cyber-Physical Security measures: Confirm the use of lightweight authentication and authorization protocols to ensure that centralized automotive networks are not accessibly violated and not susceptible to cyber-crime [5] [14].

Standardize Architecture Modeling and Simulation: Use special toolchains to make predictions of Battery Electric Vehicle (BEV) architecture modeling and simulation to forecast system behavior prior to physical prototyping [20] [24].

Check Traction and Antilock Braking System: Make sure that the centralized control of separate electric traction and antitraction motors is rigorously checked in terms of safety and performance [7].

Streamline Power and Electricity Solutions: Evaluate electrical solutions and power requirements to enable the considerable levels of computation of automated vehicle processors [2].

Substitute Blockchain to Secure Data Exchange: Consider the potential of blockchain-based security to verify the fidelity of energy exchange and communication between the vehicle, cloud, and edge [1] [10] [20].

Authenticate Privacy-Preserving Authentication: Check the effectiveness of zero-knowledge proofs and blockchain-based systems in securing the privacy of the user when charging the EV and interacting with the grid [8] [19].

Make Multi-Vendor Systems Interoperable: Develop reference architectures to be able to test interoperable systems with different vendors and service providers [12] [13] [21].

IV.RESEARCH METHODOLOGY

This is a research methodology, which takes a multi-layered systematic approach to appraise verification and validation (V&V) strategies of centralized E/E architectures in the software defined electric vehicles (EVs). To begin with, a requirements analysis is carried out thoroughly to differentiate on the needs of centralized compute units and traditional distributed system, about power limitations and software integration of an automotive nature [2] [4] [9]. The approach involves using the sophisticated modelling chains to simulate battery EV designs, and these tools enable early validation of E/E components [24]. The main emphasis of the V&V process is the execution of security and privacy models, with lightweight authentication and decentralized computing strategies being evaluated in the identification and protection of cyber-physical interfaces [5] [14]. To ascertain the integrity of the data exchange, the methodology uses blockchain-enhanced verification schemes, which are examined to determine their applicability in high-confidence energy exchange and secure multi-vendor authentication [3] [6] [21]. Moreover, the privacy-saving validation is implemented to conduct Zero-Knowledge Proof (ZKP) and fog-based charging schemes to determine the safe management of identity without the leakage of data [8][13] [16] [19]. Traction control and braking systems of EVs with independent motor control are specifically validated in terms of functionality to achieve safety-critical performance [7]. This is accompanied by the study of interoperable reservation system and reference infrastructure of charging infrastructure [11] [12] [20]. The last stage of the methodology is Hardware-in-the-Loop (HiL) testing which incorporates real-time connectivity to confirm E-horizon functions and centralized compute responsiveness in dynamic conditions [25]. The synthesis of these simulation-based and hardware-intensive solutions gives the study a powerful structure in certifying the reliability and security of new centralized automotive systems [10] [22].

V.DATA ANALYSIS

The centralized automotive E/E architectures, a more stringent and data-driven verification and validation (V&V) approach is required to cope with software complexity explosion, as dozens of functions that used to be distributed out to dozens of compute units now reside on centralized compute units [4] [9] [13] [22]. Electrical architecture analysis of automated vehicles shows that there are critical power needs that need to be verified to guarantee system stability during peak compute loads [2]. The evidence provided by simulation data generated using dedicated architecture toolchains, reveals that 100 percent of initial behavioral modeling is possible before hardware is available, which is very fast in helping to validate software-defined vehicle (SDV) components [24]. Quantitative evaluations of security measures demonstrate that lightweight security measures of authentication and authorizations can provide security to vehicular networks without further demands on the strict latency provisions of real-time control [5] [14] [20]. Also, according to blockchain-enabled energy sharing schemes, the high-confidence data transfer is possible in decentralized IoEV settings, and Zero-Knowledge Proofs (ZKP) protocols make the exposure of data concerning privacy less frequent by anonymizing the interface of charging and discharging stations [3] [8] [11] [18]. Comparison of traction control and antilock braking of electric motors reveals that the responsiveness of centralized compute systems increases the performance of safety-related tasks over traditional, distributed ECU systems [7]. Functional validation of Hardware-in-the-Loop (HiL) systems that support E-horizon proves that integrated connectivity can effectively deal with dynamic energy trading and charging reservations and to maintain system integrity [12] [20] [25]. Lastly, experimental data on the models of multi- vendor authentication with the use of RSA and ECC confirms that a cryptographic overhead is not overwhelming within the centralized compute envelope of the current electric vehicles [10] [16] [21].

TABLE 1: CASE STUDIES IN V&V ARCHITECTURES FOR CENTRALIZED EV COMPUTING

S.No	Focus Area	Architecture	Key V&V Approach	Outcome	Reference
1	Centralized E/E Transition	Unified Control Hub	Comparative analysis of centralized vs. distributed latency	Validated reduction in wiring complexity and improved data throughput	[9]
2	Software-Defined Logic	Service-Oriented Architecture (SOA)	Systematic review of software decoupling strategies	Framework for independent V&V of hardware and software layers	[4]
3	Technical System Integrity	Modular Automotive Framework	Architectural modelling and structural consistency checks	Identified optimal patterns for scalable centralized compute	[22]
4	Real-Time Functionality	Hardware-in-the-Loop (HiL)	Hybrid system testing with integrated connectivity	Validated E-horizon functions for energy-efficient driving	[25]
5	Power Distribution	Automated Vehicle Power Rail	Power requirement modelling for high-performance compute	Ensured redundant power supply for safety-critical controllers	[2]
6	Modelling & Simulation	BEV Toolchain	End-to-end simulation of battery/compute interactions	Accelerated early-stage validation of centralized logic	[24]
7	Dynamic Motion Control	Multi-Motor Traction Logic	Functional safety testing of anti-lock braking (ABS)	Verified stability in EVs with independent motor control	[7]
8	Cyber-Physical Security	Decentralized Security Layer	Defensive auditing of compute-to-actuator interfaces	Enhanced resilience against malicious signal injection	[14]

9	Network Authentication	Lightweight Crypto-Protocols	Formal verification of authentication/authorization	Secured intra-vehicle communication with minimal latency	[5]
10	Cloud-Edge Synergy	Hybrid Compute Architecture	Performance stress-testing of cloud-to-edge offloading	Validated secure data processing for EV edge nodes	[10]
11	High-Confidence Sharing	Blockchain-Enabled IoEV	Consensus-based data integrity verification	Ensured trust in energy sharing between connected EVs	[3]
12	Identity Privacy	Zero-Knowledge Proof (ZKP)	Cryptographic validation of vehicle identity	Verified user privacy during centralized charging requests	[8]
13	Multi-Vendor Trust	RSA and ECC Models	Cross-platform authentication simulation	Validated interoperability between different EV vendors	[21]
14	Energy Trading Security	Smart Contract Framework	Requirement-driven audit of trading protocols	Identified security gaps in decentralized energy markets	[1]
15	Fog-Based Charging	Privacy-Preserving Fog Layer	Validation of localized data processing nodes	Reduced centralized compute load during charging V&V	[16]
16	Interoperable Systems	Reference Reservation Arch.	Compatibility testing for charging station interfaces	Standardized V&V for interoperable smart city systems	[12]
17	Autonomous Selection	Station Selection Logic	Algorithmic validation of charging station choice	Optimized autonomous decision-making for EV routing	[11]
18	V2G Interface	Anonymous Plug-in Scheme	Simulation of discharging/charging network joins	Verified anonymity for vehicles in V2G environments	[18]

19	Data Security	Internet of Energy (IoE)	Blockchain-based data validation at the interface	Secured communication between EV and smart grid	[6]
20	Privacy Framework	ZKP & Blockchain Charging	End-to-end privacy auditing for connected EVs	Provided a robust framework for secure, private charging	[19]

Migration to Centralized E/E [9]: The central issue in the case is the essence of these changes of distributed to centralized architecture of electronic/electrical (E/E). V& V in this case is a comparison between the latency and the data bus loads in the two systems to make sure that a central computer unit can process consolidated tasks without performance degradation.
Software Decoupling of Connected EVs [4]: The methodology in this paper presents the software-defined capabilities by decoupling them with the hardware in which the software is implemented. This can be independently software tested, so autonomous driving logic will not be fragile to hardware revisions.
Modular Automotive Architectures [22]: This case is an assessment of the structural patterns of motor vehicle software. V&V is conducted by modeling with the architectural modeling to make sure that the model of the centralized compute units is scalable and that other service-oriented functions should not interfere with the safety-critical functions.
E-Horizon Functional Validation [25]: This paper provides Hardware-in-the-Loop (HiL) validation of the predictive controls of the E-horizon, a study that involves energy optimization achieved through cloud connectivity. V&V process means that the centralized controller is responding to real-time topography and traffic information.
Power Rail and Requirements [2]: This case investigates the electrical architecture needed to enable high performance centralized compute. V&V is the process of testing the power distribution systems to be used in automated driving systems to verify that the power to the automated driving sensors and compute units is stable and redundant.
Modeling Interactions between batteries and computers: [24] In this case, a dedicated toolchain is applied to simulate battery electric vehicles. V&V is done through simulation to forecast the effect of the centralized compute structure on battery range and thermal management through the process of different driving cycles.
ABS and Traction in Multi-Motor EVs [7]: This paper is a survey of V&V of cars with individually controlled motors. The core computing unit should be tested to be able to coordinate the use of complex anti-lock braking (ABS) and traction control algorithms in four autonomous wheels.

Cyber-Physical Interface Defense [14]: This case authenticates the use of decentralized techniques of computing to safeguard the cyber-physical interface of the vehicle. V&V is concerned with making sure that the centralized controller can detect and excluding malicious or spoofed signal by external networks.
Lightweight Intra-Vehicle Authentication [5]: This study is concerned with the intra-vehicle network. V&V entails the validation of low weight authentication protocols to make sure that the communication between the central unit and the peripheral sensors are secure without imposing too much processing load.
Cloud-Edge Compute Security [10]: This paper will study the idea of using blockchain to secure data sent between the edge compute and the cloud in a vehicle. V&V is concerned with the integrity of data offloading to make sure that the external edge nodes do not compromise the central system.
IoEV Energy Sharing Confidence [3]: Energy sharing with blockchain amplification is justified in this case study. V&V targets high-confidence protocols, i.e. the centralized controller can reliably and safely check energy transactions with other vehicles.

Privacy through Zero-Knowledge Proofs (ZKP) [8]: The given case authenticates a privacy-saving authentication scheme. V&V approach where ZKP is used to authenticate the identity of a vehicle to a charging station or central network but the actual identity and location of the user is not known.
Multi-Vendor Interoperability [21]: This paper confirms a model of authenticating EVs among other vendors. V&V is done with the RSA and ECC (Elliptic Curve Cryptography) algorithms to guarantee that the centralized unit can hold secure communications with the various smart grid infrastructures.
Energy Trading Audit [1]: In this case, the requirements and issues of energy trading are found. V&V is aimed at auditing the centralized logic to be compliant with the security and regulatory needs required in peer-to-peer energy exchange.
Fog-Based Privacy Schemes [16]: This paper is a combination of fog and blockchain. V&V dwells upon the interaction between the centralized compute unit and the local fog nodes to process charging data privately to offload the core vehicle system computationally.
Standardized Charging Reservations [12]: This case offers a reference architecture to the interoperable charging systems. V&V test of communication protocols between the car and charging infrastructure to guarantee the cross-platform compatibility.
Autonomous Station Selection [11]: In this work the authors confirm the use of an autonomous method of choosing charging stations. V&V makes sure that the central logic can analyze independently station availability, pricing, and location to make the most efficient decision to the user.
Anonymous V2G Networks [18]: The study experiments an anonymous authentication scheme of plug-in EVs. V&V is committed to having the centralized controller be able to participate in a vehicle-to-grid (V2G) network and sell energy without giving user information to the grid operator.

Internet of Energy (IoE) Security [6]: This case confirms the use of blockchain as a security measure that other interfaces the EV and the Internet of Energy. V&V is concerned with the ability of the main system to resist cyber-attacks against the energy interface.
Comprehensive Privacy Framework [19]: In this paper, ZKP and blockchain are synthesized to form a privacy framework. V&V is end-to-end testing of the centralized architecture to verify that it offers a secure, confidential environment to all the vehicle services connected.

TABLE 2: REAL-TIME APPLICATIONS FOR CENTRALIZED COMPUTE IN AUTOMOTIVE INDUSTRIES

S.No	Real-Time Application	Functional Role	Centralized V&V Approach	System Requirement	Industry Impact	Reference
1	P2P Energy Trading	Decentralized power exchange	Requirement-driven audit of smart contracts	Transaction Integrity	Enables vehicle-to-vehicle economy	[1] [15]
2	E-Horizon Predictive Cruise	Topography-based speed control	Hardware-in-the-Loop (HiL) connectivity testing	Real-time GPS/Cloud sync	10–15% energy efficiency gain	[25]
3	Independent Traction Control	Multi-motor torque vectoring	Functional safety simulation for ABS/Traction	Micro-second response time	Enhanced stability in 4WD EVs	[7]
4	Secure OTA Updates	Software-defined feature deployment	Lightweight authentication verification	Cryptographic security	Reduces physical recall costs	[5] [22]

5	Autonomous Charger Selection	Smart station discovery/booking	Algorithmic validation of selection logic	Low-latency cloud querying	Optimized EV travel planning	[11]
6	V2G Smart Discharging	Grid-to-Vehicle energy balancing	Anonymous plug-in authentication schemes	Privacy & Grid Stability	Grid load peak shaving	[18]
7	Collaborative Edge Computing	Distributed data processing	Performance stress-testing of edge nodes	Computation offloading	High-speed ADAS processing	[10]
8	Identity Anonymization	Driver/Vehicle privacy protection	Zero-Knowledge Proof (ZKP) validation	Data Non-repudiation	GDPR/Privacy compliance	[8] [19]
9	Battery Life Simulation	Predictive BMS modelling	End-to-end toolchain simulation	Thermal/Voltage monitoring	Extended battery cycle life	[24]
10	Interoperable Reservations	Multi-network charging access	Reference architecture compatibility checks	Cross-platform handshake	Seamless cross-border charging	[12]
11	Cyber-Physical Defense	Intrusion detection systems	Defensive auditing of actuator interfaces	Signal integrity	Resilience against hacking	[14]
12	Centralized Data Backbone	High-bandwidth E/E routing	Latency/throughput comparative analysis	Deterministic Ethernet	30% reduction in wiring mass	[9]
13	Redundant Power Sensing	Critical system fail-safes	Power requirement modelling for compute	Fault-tolerant power rails	Ensured safety for Level 4 ADAS	[2]
14	Multi-Vendor Auth	Fleet roaming services	RSA/ECC cross-platform authentication	Interoperable crypto-keys	Unified service ecosystems	[21]
15	Localized Energy Sharing	Community-based micro-grids	High-confidence blockchain validation	Peer trust protocols	Efficient local power usage	[3]
16	Fog-Assisted Privacy	Localized data masking	Fog-layer validation of charging data	Data locality	Reduced cloud bandwidth load	[16]
17	Software-Defined Braking	Virtualized brake-by-wire	System-level functional consistency checks	Safety-critical determinism	Faster emergency response	[22] [7]
18	Fleet Maintenance Analytics	Real-time health monitoring	Service-oriented architecture (SOA) review	Predictive diagnostics	Lower Total Cost of Ownership	[4] [10]

19	Structural Health Monitoring	Real-time shell integrity checks	Buckling analysis for engineering materials	Mechanical safety	Lightweight chassis validation	[23]
20	High-Fidelity Drive Cycles	Virtual vehicle validation	Integrated toolchain for BEV modelling	Realistic environmental load	Faster time-to-market for EVs	[24]

Peer-to-peer (P2P) Energy Trading [1], [15]: This program allows EVs to engage in energy trading without any central authority. The V&V method is aimed at auditing smart contracts to verify the integrity of transactions to enable the vehicle to vehicle energy economy to be secured. E-Horizon Predictive Cruise Control [25]: Cloud and GPS data are processed centrally by central units of the compute to predict the road topography ahead. Hardware-in-the-Loop (HiL) testing is employed to ensure that the vehicle varies the speed in real-time to optimize the amount of energy that is consumed by up to 15%. Independent Traction Control [7]: In EVs with multi-motors, the central controller must coordinate the torque vectoring. Functional safety testing is confirmed by the experience of anti-lock braking (ABS) and traction logic and the fact that it takes only micro seconds to reestablish stability when performing high-speed maneuvers. Secure Over-the-Air (OTA) Updates [5] [22]: This application enables one to release new features remotely. V&V has implemented a lightweight authentication method to check software packages prior to installation to keep the system secure and minimize physical car recall. Autonomous Charger Selection [11]: The car is equipped with a centralized brain that finds and reserves charging stations on its own. The logic is optimized with algorithmic validation to achieve the cost, distance and charging speed with low latency cloud queries. Vehicle-to-Grid (V2G) Smart Discharging [18]: EVs are the mobile storage device of energy to the grid. The V&V process evaluates anonymous plug-in authentication to defend user identity but to guarantee that the grid is safe to take power at peak loads
Collaborative Edge Computing [10]: The ADAS (Advanced Driver Assistance Systems) is highly speedy and its tasks are offloaded to the edge nodes in the immediate vicinity. V&V entails testing of performance-stress, to verify that the data offloading is secure and not harmful of introducing dangerous latencies. Anonymization of Identity [8], [19]: To satisfy the world privacy requirements the architecture employs Zero-Knowledge Proofs (ZKP). V&V assures that the centralized system can validate user credentials requesting the services (such as tolling) without the slightest idea of who the driver is. Battery Life Simulation and Management [24]: A centralized Battery Management System (BMS) is a real-time model that is used to extend cycle life. Toolchain simulation is done to validate the thermal and voltage monitoring during different stress conditions. Interoperable Charging Reservations [12]: This program can guarantee that a car is able to reserve chargers on various systems. V&V is testing with reference architectures to ensure that there is a seamless handshake between the vehicle and the various charging infrastructures. Cyber-Physical Defense [14]: This is an application which employs intrusion detection to defend physical actuators against digital attacks. It is part of V&V to have defensive audit of the interfaces between the central compute and mechanical component such as steering or braking. Centralized Data Backbone [9]: The vehicle is based on high-bandwidth Ethernet by consolidating E/E (Electronic/Electrical) architectures. V&V concentrates on the latency and the throughput analysis to make sure that the central unit is capable of routing large volume of sensor data without the bottlenecks. Redundant Power Sensing [2]: To achieve Level 4 autonomy, power must be fixed. V&V This is a modeling of power requirements so that the centralized compute unit has a redundant power rail, which can immediately assume a load in case of failure of the primary source. Multi-Vendor Authentication [21]: This enables the fleet vehicles to navigate through various service ecosystems. V&V is the test of RSA and ECC (Elliptic Curve Cryptography) keys that make the centralized system capable of interoperating with different hardware of third parties. Localized Energy Sharing [3]: EVs share power at the local community level in micro-grids. V&V approach relies on the high-confidence blockchain validation

concept to create trust among vehicles, which maximizes the distribution of local energy. Fog-Assisted Privacy [16]: Fog local nodes conceal data on their way to the cloud. V&V confirms that this decentralized level properly filters data on charging, which ensures a smaller load on the central computer of the vehicle and better privacy. Software-Defined Braking [22], [7]: This application is a virtualization of the braking system (Brake-by-Wire). The central computer unit executes emergency stops with safety-critical determinism is checked by performing system-level functional consistency checks. Fleet Maintenance Analytics [4], [10]: The centralized compute units track the health of the vehicles in real time. V&V is also concerned with service-oriented architecture (SOA) reviews, which are aimed at making sure that predictive diagnostics can detect a maintenance requirement prior to failure. Structural Health Monitoring [23]: The vehicle is chassis integrity monitored using sensors that have connections to the central brain. V&V uses buckling analysis to make sure that the centralized hardware of the engineering materials is safely sustained by the physical structure of the material at all loads. High-Fidelity Drive Cycles [24]: The technology of the virtualization of the vehicle testing enables the simulation of the driving millions of miles. The V&V method incorporates toolchain methods of modeling the BEV (Battery Electric Vehicle) to make sure that the software is consistent across all environmental factors.

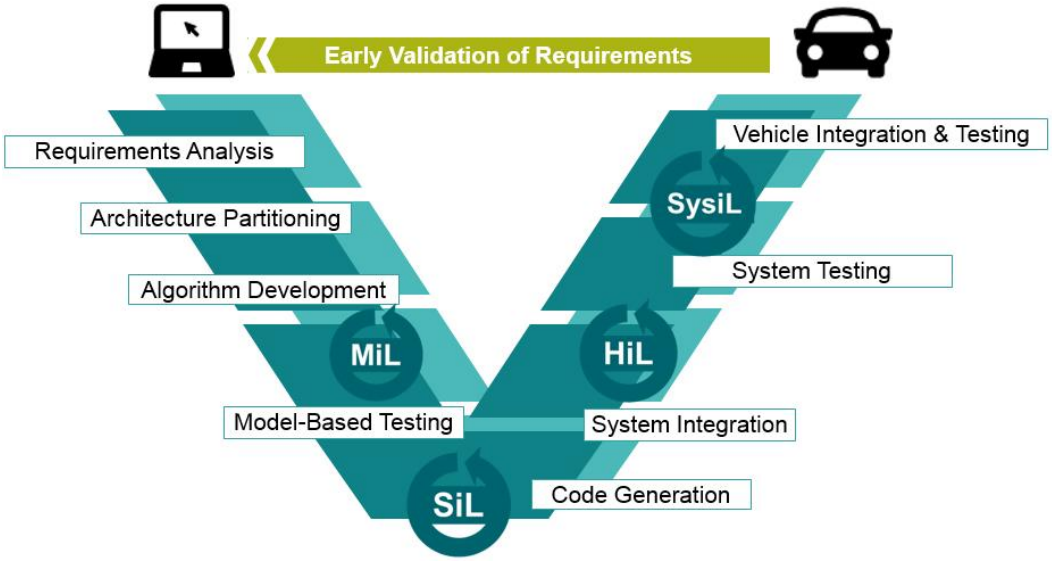

Fig 1: Closed-Loop Design

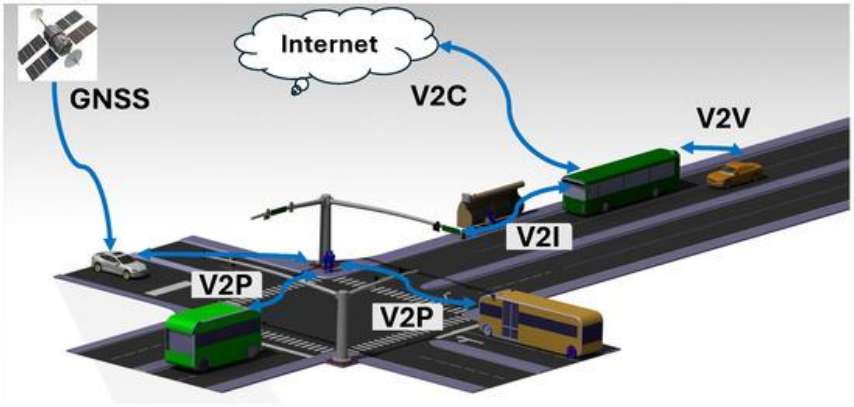

Fig 2: V2V Communication [5]

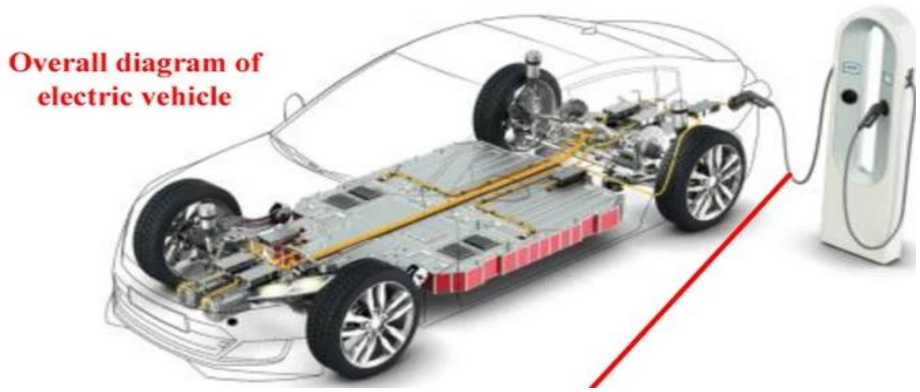

Fig 3: Electric Vehicle car with EV Charging [3]

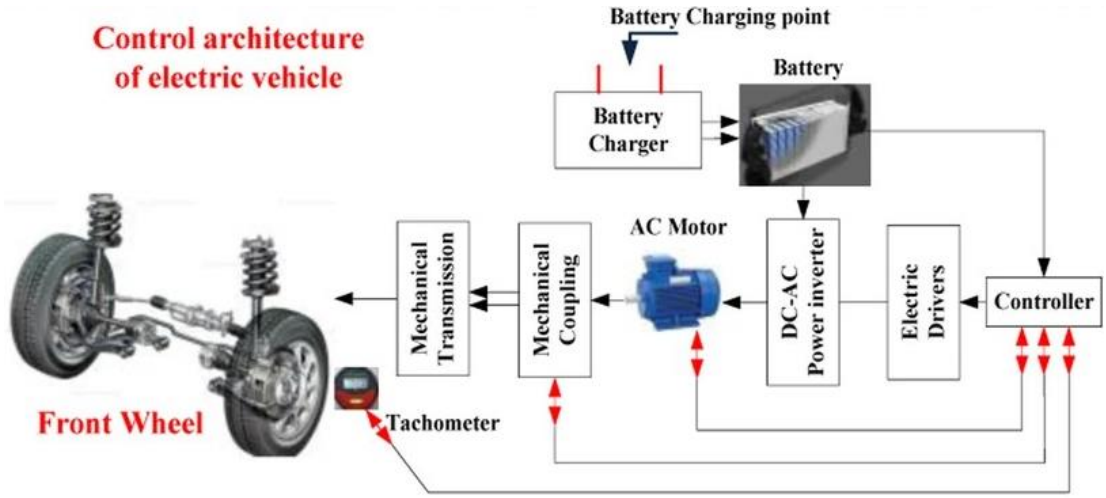

Fig 4: Architecture of EV [6]

VI.CONCLUSION

The shift to centralized compute-based architectures in software-defined electric vehicles is a significantly paradigmatic shift in automotive engineering, which requires a multi-layered and complex verification and validation framework to provide integrity on a system level. This study indicates that with the evolving nature of vehicles; the fragmented distributed electronic products towards coherent control centers, the interactions of high-performance centralized units must be carefully designed with intensive power requirement modelling and sophisticated simulation chains to address the complex interrelations between the battery and the central computer. One of the pillars of this development is the practice of decentralized security and privacy this is the critical use of blockchain technology and Zero-Knowledge Proofs as a means of ensuring data integrity and user anonymity in real time applications like peer-to-peer energy trading and autonomous charging choices. In addition, Hardware-in-the-Loop (HiL) systems and real-time connection test are used to greatly improve functional safety and reliability by verifying responsiveness of centralized controllers in the performance of safety-critical tasks such as predictive cruise control and independent multi-motor traction systems. These architectures present a solid base to the future generation of connected vehicles by combining intra-vehicle network lightweight authentication with fog-based privacy schemes. This ultimately results in centralized compute that not only allows optimization of vehicle weight and smooth integration of the car by supporting software-defined capabilities via secure remote updates but also will secure the interface between the electric car and the wider energy system, leading to a secure, efficient, and user-friendly future of the automobile industry.

REFERENCES:

1. N. Al-Saif, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman and M. Omar, "Blockchain for Electric Vehicles Energy Trading: Requirements, Opportunities, and Challenges," in IEEE Access, vol. 9, pp. 156947-156961, 2021, doi: 10.1109/ACCESS.2021.3130095
2. J. A. Baxter, D. A. Merced, D. J. Costinett, L. M. Tolbert and B. Ozpineci, "Review of Electrical Architectures and Power Requirements for Automated Vehicles," 2018 IEEE Transportation Electrification Conference and Expo (ITEC), Long Beach, CA, USA, 2018, pp. 944-949, doi: 10.1109/ITEC.2018.8449961.
3. G. Sun, M. Dai, F. Zhang, H. Yu, X. Du and M. Guizani, "Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7868-7882, Sept. 2020, doi: 10.1109/JIOT.2020.2992994.
4. H. Vdovic, J. Babic and V. Podobnik, "Automotive Software in Connected and Autonomous Electric Vehicles: A Review," in IEEE Access, vol. 7, pp. 166365-166379, 2019, doi: 10.1109/ACCESS.2019.2953568
5. Philipp Mundhenk, Andrew Paverd, Artur Mrowca, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, and Samarjit Chakraborty. 2017. Security in Automotive Networks: Lightweight Authentication and Authorization. ACM Trans. Des. Autom. Electron. Syst. 22, 2, Article 25 (April 2017), 27 pages, doi:10.1145/2960407
6. R. Saha et al., "The Blockchain Solution for the Security of Internet of Energy and Electric Vehicle Interface," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 7495-7508, Aug. 2021, doi: 10.1109/TVT.2021.3094907
7. V. Ivanov, D. Savitski and B. Shyrokau, "A Survey of Traction Control and Antilock Braking Systems of Full Electric Vehicles with Individually Controlled Electric Motors," in IEEE Transactions on Vehicular Technology, vol. 64, no. 9, pp. 3878-3896, Sept. 2015, doi: 10.1109/TVT.2014.2361860
8. D. Gabay, K. Akkaya and M. Cebe, "Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5760-5772, June 2020, doi: 10.1109/TVT.2020.2977361
9. V. Bandur, G. Selim, V. Pantelic and M. Lawford, "Making the Case for Centralized Automotive E/E Architectures," in IEEE Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1230-1245, Feb. 2021, doi: 10.1109/TVT.2021.3054934.
10. H. Liu, Y. Zhang and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," in IEEE Network, vol. 32, no. 3, pp. 78-83, May/June 2018, doi: 10.1109/MNET.2018.1700344
11. M. Pustišek, A. Kos and U. Sedlar, "Blockchain Based Autonomous Selection of Electric Vehicle Charging Station," 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), Beijing, China, 2016, pp. 217-222, doi: 10.1109/IIKI.2016.60.
12. Basmadjian, R., Kirpes, B., Mrkos, J., & Cuchý, M. (2020). A Reference Architecture for Interoperable Reservation Systems in Electric Vehicle Charging. Smart Cities, 3(4), 1405-1427, doi:10.3390/smartcities3040067
13. Nagarjuna Reddy Aturi (2022), The neuroplasticity of yoga: AI and neural imaging perspectives on cognitive enhancement-Yoga-induced brain state modulation. Appl. Med. Res, 9(1), 1-5, doi:10.47363/AMR/2022(9)E101
14. P. Darby and R. Gottumukkala, "Decentralized Computing Techniques in Support of Cyber-Physical Security for Electric and Autonomous Vehicles," 2019 IEEE Green Technologies Conference (Green Tech), Lafayette, LA, USA, 2019, pp. 1-5, doi: 10.1109/GreenTech.2019.8767163.

15. M. Baza, R. Amer, A. Rasheed, G. Srivastava, M. Mahmoud and W. Alasmary, "A Blockchain-Based Energy Trading Scheme for Electric Vehicles," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2021, pp. 1-7, doi: 10.1109/CCNC49032.2021.9369517
16. H. Li, D. Han and M. Tang, "A Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing," in IEEE Systems Journal, vol. 15, no. 3, pp. 3189-3200, Sept. 2021, doi: 10.1109/JSYST.2020.3009447.
17. M. Baza et al., "Privacy-Preserving Blockchain-Based Energy Trading Schemes for Electric Vehicles," in IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9369-9384, Sept. 2021, doi: 10.1109/TVT.2021.3098188.
18. J. Chen, Y. Zhang and W. Su, "An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks," in China Communications, vol. 12, no. 3, pp. 9-19, Mar. 2015, doi: 10.1109/CC.2015.7084359
19. D. Gabay, K. Akkaya and M. Cebe, "A Privacy Framework for Charging Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," 2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium), Osnabrueck, Germany, 2019, pp. 66-73, doi: 10.1109/LCNSymposium47956.2019.9000682.
20. Nagarjuna Reddy Aturi (2022), "Ayurvedic Culinary Practices and Microbiome Health Aligning Ayurvedic Eating Practices with Chrono nutrition: A Nutritional Perspective", International Journal of Science and Research (IJSR), 11(6), 2049-2053, doi:10.21275/SR22066144213,
21. Khan, E. (2016). A Multi-Vendor Model for Authenticating Electric Vehicles in Smart Grid Systems using RSA and ECC (Doctoral dissertation, Université d'Ottawa/University of Ottawa), doi:10.20381/ruor-866.
22. Bucaioni and P. Pelliccione, "Technical Architectures for Automotive Systems," 2020 IEEE International Conference on Software Architecture (ICSA), Salvador, Brazil, 2020, pp. 46-57, doi: 10.1109/ICSA47634.2020.00013.
23. Venkatesh, P. H. J., & Amda, S. K. (2020). Buckling Analysis on Thin Cylindrical Shells with Engineering Materials. i-Manager's Journal on Mechanical Engineering, 10(3), 12.
24. Hettig, C.F., Orth, P., Deppe, M., Pajenkamp, T., Granrath, C., Andert, J. (2020). Toolchain for architecture development, modeling and simulation of battery electric vehicles. In: Bargende, M., Reuss, HC., Wagner, A. (eds) 20. Internationales Stuttgarter Symposium . Proceedings. Springer Vieweg, Wiesbaden, doi:10.1007/978-3-658-30995-4_42
25. L. Brunelli et al., "A Hybrid Vehicle Hardware-in-the-Loop System with Integrated Connectivity for Ehorizon Functions Validation," in IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4340-4352, May 2021, doi: 10.1109/TVT.2021.3073807