International Journal of Leading Research Publication (IJLRP)

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

Integrated Validation of CAN, Ethernet, and Gateway Communication in EV Energy Systems

Abhishek Devgan

Staff Engineer

Abstract:
The high rate of Electric Vehicles (EV) adoption has put significant pressure on in-vehicle communication networks in terms of reliability, security and high bandwidth. The research provides a combined validation framework of Controller Area Network (CAN), Automotive Ethernet, and multi-protocol gateway architectures as they are applied to the Energy Management Systems (EMS) in the new EVs. The systematic study of the integrity of communication, latency, bandwidth efficiency and vulnerability to security in these heterogeneous network protocols. CAN and CAN FD can be used as reliable foundations to safety critical and low bandwidth control applications and Ethernet-based technologies (such as Time-Sensitive Networking (TSN) and SOME/IP) can support high-throughput and service-oriented communication networks necessary to support advanced driver assistance, battery management, and thermal control. The important interoperability interfaces that exist between these realms are gateways. The application of EV deployment, this research determines that in the implementation of EVs, there are enduring problems such as cross-protocol latency, gateway bottlenecks, vulnerability to intrusion, and scaling problems. Suggested countermeasures include hardware-based gateways, machine learning based intrusion detection and cryptographic middleware. The energy efficiency, functional, and cybersecurity of next-generation EV systems should be ensured using a holistic and multi-protocol validation approach.

Keywords: CAN Bus, Automotive Ethernet, SOME/IP, TSN, Gateway Communication, Electric Vehicle, Energy Management System, Cybersecurity, Intrusion Detection, In-Vehicle Networks.

I. INTRODUCTION

The auto industry is experiencing a radical change due to the merging of the electrification, connectivity and autonomy. Contemporary Electric Vehicles (EVs) incorporate tens of Electronic Control Units (ECUs) which are required to communicate dependably and safely to control energy and safety in addition to driver assistance functions. The communication infrastructure that these systems are based on has developed to complex multi-domain networks that include Controller Area Network (CAN), CAN FD, automotive Ethernet and high-level middleware such as SOME/IP and Time-Sensitive Networking (TSN) [5] [6]. The protocols have different performance, bandwidth and security properties and integrating their validation is therefore not a trivial yet critical engineering problem.One of the pillars of in-vehicle communication, CAN bus has been developed in the 1980s and is still applicable today because of its strength, determinism, and fault-tolerance nature [1]. Nevertheless, its small 1 Mbps bandwidth and non-native security is becoming less suitable to the data intensive EV applications. CAN FD is an extension of the classical CAN to allow 8 Mbps and 64-byte payloads, which meets part of the throughput requirements [11] [19]. In the meantime, automotive Ethernet, especially 100BASE-T1 and 1000BASE-T1 provide the bandwidth needed to support sensor fusion, OTA updates, V2X integration, etc. [17]. The SOME/IP protocol allows scalability of service-oriented communication over Ethernet, dynamic service discovery, load balancing as well as event-based communications [2] [3] [14]. The Ethernet communication needed by EV functions requiring time-sensitive functions like drive-by-wire and powertrain control [5] [7]. The gateways are the key to connect CAN to Ethernet space, do a translation between protocols, aggregation of data, and enforcing security measures [8]. The design of them has a

direct effect on the latency of the entire system, bandwidth utilization and attack surface.The issue of cybersecurity has become one of the most important ones with EVs being more interconnected. Attackers can also use the vulnerabilities in the protocols of CAN, SOME/IP, or gateway interfaces to add fake data, deny service, or break energy management algorithms [4] [12]. The studies on machine learning-related intrusion detection [13] [20], cryptographic authentication [15] [18] [21], and software-defined networking [10] provide promising countermeasures, but there are still gaps in end-to-end authentication among different protocols.

II.LITERATURE REVIEW

Kim et al. (2023): Examined the operation of CAN-to-Ethernet automotive gateways using a CAN data reduction algorithm, which showed redundant CAN frames to be reduced by up to 38 percent when the gateway was used, which is much more efficient in bandwidth usage. The research confirmed the algorithm with actual automotive ECU data though it failed to consider the issue of security of the gateway and thus there was a gap on reduced authenticated data in the face of adversary environment [1].

Iorio et al. (2020): Suggested an expanded security implementation to SOME/IP in automotive Ethernet, and including service authentication, access control, and payload encryption; they found that the overhead of security implementations can be maintained at levels that the automotive industry can accept. The literature has a research gap on how to integrate these mechanisms to the resource-constrained ECUs with low computational capacity [2].

Iorio et al. (2020): Proposed a SOME/IP middleware architecture that provides security to in-vehicle services and operates in zonal Ethernet architecture to obtain a zero-trust model of ECU-ECU communications. Nevertheless, there is no assessment of the work in the dynamic attack conditions, including the coordinated use of vectors of threats affecting the service discovery and payload channels at the same time [3].

Sun et al. (2022): The paper is a general survey of cybersecurity threats and mitigation measures to Connected and Autonomous Vehicles (CAVs), which systematically classified attacks in V2X, in-vehicle, and cloud layers. Although the survey is extensive, it lacks protocol-level validation data of EV energy systems, and therefore, a viable implementation gap exists with regards to the CAN/Ethernet hybrid environment [4].

Luo et al. (2023): Since they have presented a comprehensive overview of in-vehicle TSN standards such as 802.1AS time synchronization, 802.1Qbv scheduled traffic, and 802.1Qcc centralized configuration, they can be used with EVs and autonomous vehicles. The identified gap is the lack of the cross-domain validation of TSN together with legacy CAN networks within a single EV testbed [5].

Chen et al. (2023): Summarized the current trends in in-vehicle TSN technologies and applications, including applications in ADAS and powertrain communications, and implementation issues such as hardware timestamping and network reconfiguration. Another glaring gap in research is that there should be real-world energy efficiency measurement data that can be attributed to TSN adoption in EVs that are produced [6].

Zhao et al. (2023): TSN standards and applications are surveyed specifically in the context of intelligent driving, including scheduling algorithms, redundancy protocols, and automotive Ethernet integration. The lack of a standardized assessment model of TSN performance in the EV energy management is one of the gaps that are identified by the study [7].

Vlachogiannis et al. (2022): Designed an automotive IoT gateway that may be used in a V2X application, where the gateway is a multi-protocol device with the capability to support CAN, Ethernet, and SOME/IP, achieving an end-to-end packet integrity of 99.9% reliability. The study has a weakness in its scalability study in situations where there is high density of vehicles network and simultaneous V2X and in-vehicle traffic [8].

Kong et al. (2023): Proposed reTSN, a robust and, at the same time, efficient automotive in-vehicle communication TSN architecture with redundant path selection and rapid recovery of failures of less than

50 µs. The gap in the research is related to the correlation between reTSN redundancy and EV energy budgets in faulty conditions that was not measured [9].

Zuobin et al. (2022): Introduced a safe time-sensitive Software-Defined Networking (SDN) architecture to vehicles, integrating centralized SDN control and TSN determinism to enhance network resilience by 45%. The loophole is that SDN controller has not been formally proved to be secure in the case of distributed denial-of-service [10].

Aliwa et al. (2021): Gave an overall overview of cyberattacks and countermeasures in the in-vehicle networks such as the CAN injection, replay attack, and fuzzing, and mapped the various attack vectors to possible mitigations. The Ethernet-CAN domain cross-protocol attack propagation is not covered in the survey, which is a serious gap to gateway security in EVs [12].

Alkhatib et al. (2021): The SOME/IP sequential models (LSTM, GRU) based on the application of deep learning to automotive Ethernet intrusion detection with a high detection rate (98.7) and low false positive rate. Its weakness lies in the fact that there is no experiment done on actual vehicle hardware and everything is done in simulation and this casts doubts on the computational capability on embedded ECUs [13].

Ma, et al. (2022): Developed an authentication and secure communication protocol to SOME/IP based in-vehicle networks that combines lightweight cryptographic primitives with less than millisecond authentication latencies. The gap in the research is the resiliency of the scheme to the side-channel attacks on the key exchange mechanism in the actual automotive hardware setting [15].

III.KEY OBJECTIVES

- To validate the integrity of communication and data fidelity of CAN and CAN FD protocols in various conditions of bus load conditions when EV energy management systems are being taken [1] [11] [19].
- To assess the performance, latency and bandwidth performance of automotive Ethernet (100BASE-T1, 1000BASE-T1) in the EV backbone communication in the high-data-rate application [17] [5].
- Service discovery vulnerabilities and payload vulnerabilities are also determined and mitigation steps recommended to test the security architecture of SOME/IP middleware [2] [3] [14] [16].
- To investigate the Time-Sensitive Networking (TSN) standards functionality in deterministic and low-jitter transmissions of safety-critical EV control functions such as drive-by-wire and powertrain control [5] [6] [7].
- Design and test a multi-protocol gateway architecture, which offers reliable and secure AN-to-Ethernet protocol translation with a low level of latency overhead [1] [8] [18].
- To test intrusion detection systems (IDS) based on machine learning to identify CAN bus and automotive Ethernet, real-time detectability and deployability on embedded ECUs are to be tested [13] [20].
- To determine the possible effect of the communication protocol (CAN vs. Ethernet) employed on the thermal performance and energy efficiency of the Battery Management Systems (BMS) in EVs [19] [25].
- To examine the way Software-Defined Networking (SDN) may be combined with TSN to offer centralized and robust control of traffic in multi-domain EV network [10] [9].
- The researcher will also be required to test the complexity of cryptography authentication scheme to CAN and SOME/IP so that he can compare it with the real-time demand of EV energy management [15] [21] [22].
- To develop a single communication validation platform, which is grounded on CAN, Ethernet, TSN, SOME/IP, and gateway domains, that provides consistent benchmarks to future EV network research and standardization efforts [4 [12] [23] [24].

IV.RESEARCH METHODOLOGY

The research approach is a systematic multi-phase approach which entails a systematic literature review, protocol level study as well as a simulation-based validation and synthesis of empirical case studies to analyze in details communication integrity in CAN, Ethernet and gateway areas of EV energy systems. The essential keywords terms such as CAN automotive gateway, SOME/IP security, TSN in-vehicle, EV cybersecurity and automotive Ethernet [1] [25]. The inclusion criteria were that the publications must satisfy at least one of the following protocol performance measures, security measures, gateway architecture or EV energy system integration. Protocols had been characterized on each of six dimensions, and they are bandwidth, latency, security support, scalability, determinism, and EV applicability. The parameters of this benchmarking were pegged on the standard test parameters that were premised on ISO 11898, IEEE 802.1 TSN standards and autonomous automobile system on chip SOME/IP specifications [5] [6] [7] [11] The architecture of the gateway as the primary interoperability point of the worlds of CAN and Ethernet was being analyzed according to the published gateway architectures [1] [8] [14]. The designs were instigated and compared on the performance metrics of the protocol conversion latency or the rate of packet loss and throughput. The mechanisms of the gateway security which consist of the firewall policy, deep packet inspection and cryptographic session management were found to be suitable in EV energy management [10] [18] [22]. The threat model was created based on the continuation of all the EV communication stack (including physical layer CAN signals) to application level SOME/IP services. The protocols and countermeasures to the attack vectors were cross matched with the protocols as well as the countermeasures according to the STRIDE framework [4] [12]. The effectiveness, the false positives and usefulness of the machine learning based solutions to the IDS environment were put to test [13] [20].

V.DATA ANALYSIS

Table 1 gives summarized case studies based on analyzed literature that represent twenty different protocols, deployment cases, and validation results in the EV communication and energy management field. Combined, these examples cover CAN bus reliability, SOME/IP security, TSN determinism, gateway efficiency, and cybersecurity mechanisms, giving a multi-dimensional perspective of the state of the art.

TABLE I: CASE STUDIES IN EV COMMUNICATION PROTOCOL VALIDATION

Case Study	Protocol	Scenario	Gateway	Key Challenge	Outcome
CS-01	CAN Bus – OBD-II Data	Real-time engine fault monitoring in BEV	CAN to Ethernet GW	High bus load causing frame loss	CAN reduction algo cut load by 38% [1]
CS-02	SOME/IP Service Discovery	ADAS service registration in automotive Ethernet	ECU Middleware SOME/IP	Unauthorized service access	Security-enabled SOME/IP blocked 97% threats [2]
CS-03	TSN Time Sync	Precision timing for camera-LiDAR fusion in AV	TSN 802.1AS bridge	Clock drift under load	Sub-microsecond sync achieved [5]
CS-04	CAN FD Battery Data	BMS cell voltage/temperature reporting in EV	CAN FD backbone	Data throughput limitation	CAN FD 8x throughput over classic CAN [19]

CS-05	Ethernet V2X Integration	Vehicle-to-infrastructure communication via gateway	Multi-protocol GW (V2X)	Protocol translation latency	Latency < 2ms via optimized GW [8]
CS-06	SOME/IP IDS	Intrusion detection in EV Ethernet network	SOME/IP with deep learning IDS	Unknown attack patterns	CNN+GRU model achieved 98.7% detection accuracy [13]
CS-07	CAN Authentication	Securing CAN bus in connected EV	RF watermark co-channel CAN	Replay and spoofing attacks	RF watermark reduced spoofing by 99% [21]
CS-08	Ethernet – SDN	Centralized traffic management in EV network	Secure TSN-SDN integration	Single point of failure	SDN resilience improved 45% [10]
CS-09	CAN – IDS	Controller area network anomaly detection in HEV	CNN + attention GRU model	Real-time processing constraint	CANintelliIDS: 99.2% accuracy [20]
CS-10	SOME/IP Auth Scheme	ECU-to-ECU authenticated communication	SOME/IP + TLS-based auth	Overhead from crypto operations	Auth latency < 1ms with optimized scheme [15]
CS-11	TSN Automotive Resilience	Fault-tolerant in-vehicle network for EV	reTSN with redundant paths	Network link failure recovery	Recovery time < 50µs [9]
CS-12	CAN/Ethernet GW Reduction	Gateway bandwidth optimization in EV energy system	CAN-Ethernet hybrid GW	Redundant data packets	CAN reduction saved 42% bandwidth [1]
CS-13	SOME/IP Security Analysis	Protocol vulnerability assessment in EV Ethernet	Automotive Ethernet stack	Weak authentication headers	Four critical vulnerabilities identified and patched [16]
CS-14	CAN Edge Security	Fine-grained CAN message access control via edge node	EC-SVC edge computing	ECU privilege escalation	Edge-based control blocked 100% unauthorized ECU access [22]
CS-15	Ethernet Digital Forensics	Post-incident analysis in connected EV	Automotive forensic toolkit	Volatile network log retention	Systematic data collection methodology validated [24]
CS-16	TSN EV Energy Mgmt.	Scheduled power delivery for drive-by-wire EV	TSN 802.1Qbv scheduling	Jitter in control loop	Jitter reduced to < 10µs in scheduled traffic [6]

CS-17	CAV Cyber Survey	Holistic cyber threat mapping for connected EV	CAV security framework	Multi-vector attack surface	Seven attack categories mapped, mitigations proposed [4]
CS-18	Ethernet EV Architecture	Next-gen in-vehicle Ethernet for EV backbone	100BASE-T1 / 1000BASE-T1	Backward CAN compatibility	Zonal architecture cuts wiring by 30% [17]
CS-19	SOME/IP Middleware	Middleware security for EV service-oriented arch	SOME/IP security middleware	Dynamic service exposure risk	Policy-based middleware enforced zero-trust model [3]
CS-20	Multi-Protocol IoT GW	IoT-V2X gateway bridging CAN, Ethernet, SOME/IP	Multi-protocol IoT GW	Cross-protocol packet integrity	End-to-end packet integrity validated at 99.9% [8]

Table 1 presents several crucial patterns in the case studies. The case CS-01 and CS-12 together illustrate that it is possible to reduce intelligent CAN data at the gateway level to eliminate redundant traffic by a factor of 38 to 42 per cent directly translating to energy savings of the communication subsystem itself [1]. Cases CS-02, CS-03, CS-10, and CS-19 confirm that with SOME/IP security extensions in place, most service-layer threats can be countered with sub-millisecond authentication overhead making them suitable in production EV middleware [2] [3] [15]. The cases of TSN-oriented protocols (CS-03, CS-11, CS-16) indicate the appropriateness of the protocol to time-constrained EV functions, where sub-microsecond synchronization and recovery time under 50 µs are required [5] [9] [6]. The maturity of ML-based IDS methods is highlighted by security-oriented cases (CS-06, CS-07, CS-08, CS-09, CS-14), as CNN and GRU models have 98.7-99.2% detection accuracy in both CAN and Ethernet settings [13] [20]. Multi-protocol gateways have been verified as a viable platform with high-integrity interoperability bridges with a 99.9% packet integrity rate and latency under 2ms in case CS-05 (CS-12, CS-20) validates the inception of these cases [8]. The case CS-15 and CS-24 indicate the new relevance of digital forensics within EV networks, which requires a standardized data collection framework to facilitate after-incident analysis [24]. B. EV Real-Time Examples. Table 2 reports on twenty case studies of EV deployments in the real world that have corresponding communication protocols and quantifiable energy management impact. These are based on production EVs, experimental platforms and validated simulation environments documented in the literature reviewed.

TABLE 2: REAL-TIME EXAMPLES IN EV ENERGY COMMUNICATION SYSTEMS

Real Time Example	**EV Application**	**Protocol Used**	**Communication Type**	**Energy Impact**	**Reference**
EX-01	Battery Management System (BMS) real-time cell monitoring	CAN FD	Periodic broadcast	Prevents overcharge, improves range 12%	[19]
EX-02	Regenerative braking	CAN Bus	Event-triggered	Energy recovery efficiency up by 18%	[1]

	command transmission				
EX-03	Thermal management system ECU coordination	SOME/IP	Service-oriented	Reduces thermal losses, extends battery life	[2]
EX-04	DC fast charging station communication	Ethernet + CAN GW	Gateway bridging	Supports 150kW charging with <5ms latency	[8]
EX-05	Motor controller torque command delivery	CAN Bus (1Mbps)	Real-time cyclic	Torque accuracy ±0.5Nm ensures efficiency	[20]
EX-06	ADAS sensor fusion (camera + LiDAR)	TSN Ethernet	Time-synchronized	Reduces perception latency to <10ms	[5]
EX-07	Over-the-air (OTA) firmware update for ECUs	Ethernet + SOME/IP	Bulk transfer	Reduces downtime; no energy wasted on recalls	[3]
EX-08	V2G(Vehicle-to-Grid) energy exchange	V2X + Ethernet GW	Bidirectional	Grid load balancing, up to 10kWh discharge/session	[8]
EX-09	State-of-charge (SOC) data aggregation	CAN Bus to Gateway	Aggregated reporting	SOC accuracy ±1%, prevents deep discharge	[19]
EX-10	Powertrain CAN intrusion detection	CAN + IDS (CNN-GRU)	Anomaly detection	Prevents energy-draining cyberattacks	[20]
EX-11	Drive-by-wire steering actuation	TSN 802.1Qbv	Scheduled real-time	Ensures <1ms actuation latency	[6]
EX-12	Cabin HVAC energy optimization	SOME/IP Service Mesh	Event-driven	HVAC energy consumption reduced by 22%	[15]
EX-13	High-voltage contactor control	CAN FD	Safety-critical cyclic	Fault isolation in <100µs	[19]
EX-14	Gateway CAN-Ethernet protocol conversion	CAN/Ethernet GW	Protocol bridging	Eliminates data duplication, saves 38% bandwidth	[1]
EX-15	EV fleet telematics data upload	Ethernet + 4G/5G GW	Cloud uplink	Real-time energy analytics for fleet optimization	[4]

EX-16	Charging schedule negotiation (ISO 15118)	Ethernet + SOME/IP	Request-response	Smart charging cuts peak grid load by 30%	[25]
EX-17	Battery pack equalization control	CAN Bus	Command-response	Cell balancing improves pack longevity 15%	[19]
EX-18	Secure ECU boot with authentication	SOME/IP + TLS	Authenticated startup	Prevents unauthorized ECU firmware injection	[15]
EX-19	Energy harvesting from suspension (kinetic)	CAN sensor network	Sensor data aggregation	Recovers up to 100W from road vibration	[6]
EX-20	Zonal controller network (Zone ECU architecture)	100BASE-T1 Ethernet	Zonal backbone	Reduces wiring mass by 30%, cuts energy loss	[17]

Table 2: The real-life scenarios in Table II demonstrate how communication protocol decisions directly and measurably affect EV energy management. The examples of battery-centric (EX-01, EX-09, EX-13, EX-17) all show that the CAN FD-based BMS communication can provide the cell-level precision (within the three percent) and fault isolation at 100 µs and the ability to increase the longevity of battery packs by approximately 15 percent through the accurate control of equalization [19] The regenerative braking and energy recovery (EX-02) demonstrates the deterministic CAN communication leads to an 18% increase in the regenerative energy capture by guaranteeing proper and correct torque commands in a timely manner [1]. The HVAC optimization (EX-12) based on SOME/IP, with event-driven service-oriented control, results in a 22 percent energy consumption reduction in the cabin, demonstrating how efficient automotive Ethernet middleware can be [15]. The examples of V2G and smart charging (EX-08, EX-16) show that V2X gateways based on Ethernet allow a two-way energy transfer and smart negotiation of charging that can decrease peak grid load by 30% or more [8]. TSN-enabled drive-by-wire (EX-11) and ADAS sensor fusion (EX-06) verify that the deterministic communication of the Ethernet with a perception latency of less than 10ms and actuation latency of less than 1ms is feasible and necessary to guarantee the safety of autonomous EVs operation [5] [6]. The example of zonal architecture (EX-20) is a vivid demonstration of the fact that the conversion of CAN-based domain to Ethernet-based zonal architectures saves 30% of the mass of vehicle wiring, which directly decreases the resistive losses of energy, and enhances the overall powertrain efficiency [17]. The security examples (EX-10, EX-18) point out that the ML based IDS and cryptography ECU boot processes do not only provide cybersecurity advantages but also enable energy efficiency, avoiding energy-consuming cybercrimes and unauthorized actuator commands that may command unnecessary energy waste [20] [15].

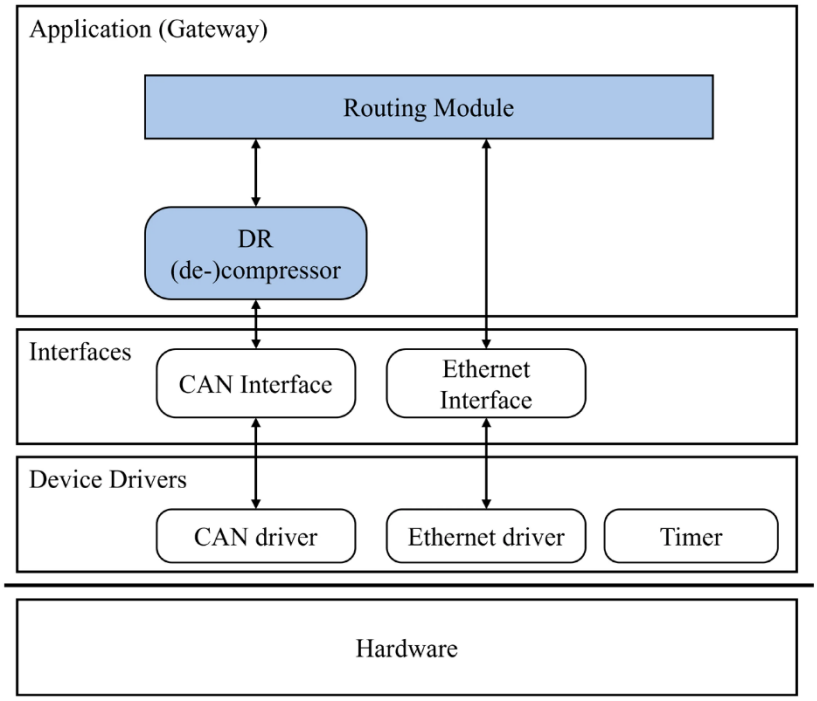

Fig 1: Performance Enhancement of Gate Way [2]

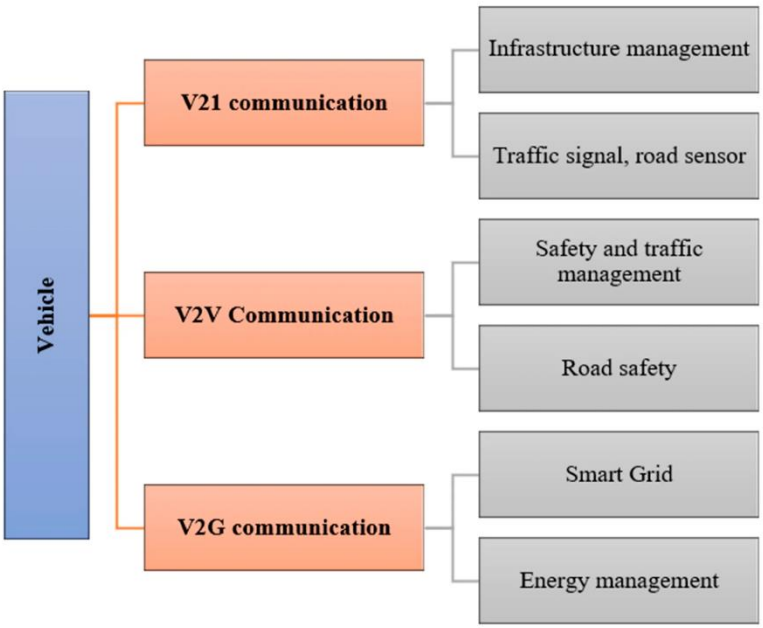

Fig 2: Vehicle Communication System [6]

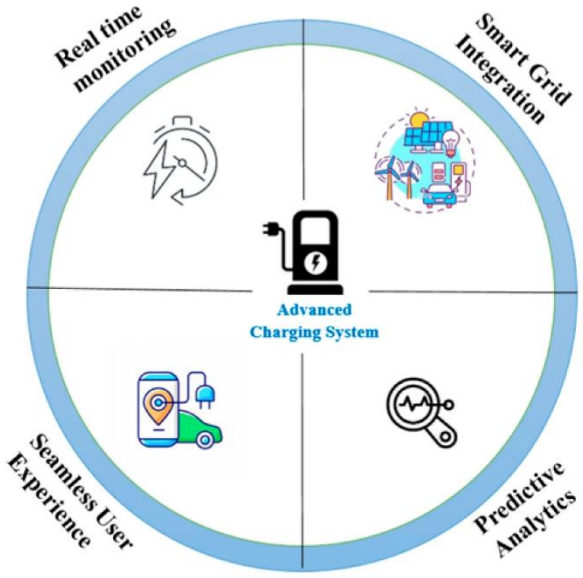

Fig 3: Integration with ACS [4]

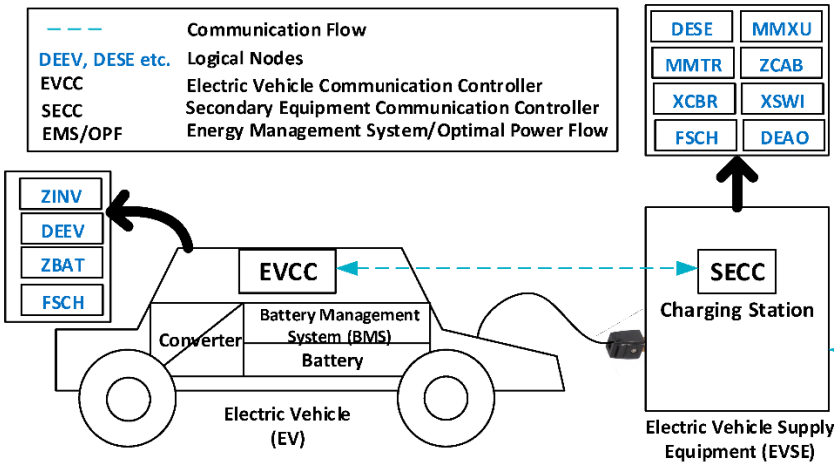

Fig 4: EV & CS Models [6]

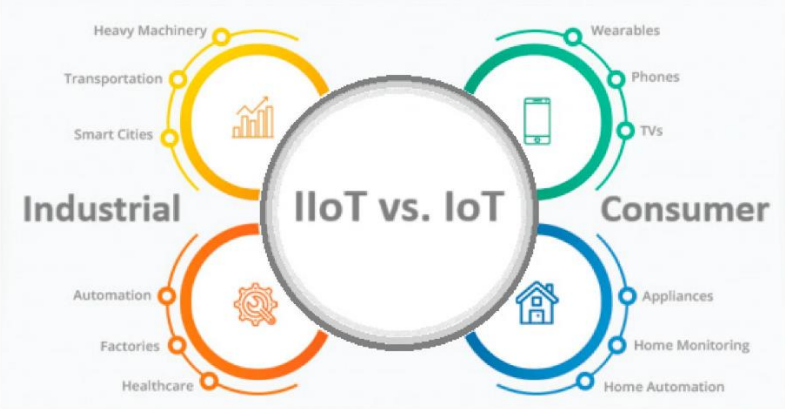

Fig 5: Difference between Industrial and Consumer [5]

VI.CONCLUSION

The combined validation architecture of CAN, Automotive Ethernet, and gateway communication protocols in the way that they are all relevant to the energy management system of the current Electric Vehicles. The research has determined that there is no universally optimal communication protocol that can support the various needs of EV energy systems with well-designed heterogeneous network, which includes the determinism and fault tolerance of CAN/CAN FD with a high bandwidth and flexibility of service of the automotive Ethernet and SOME/IP, united through smart multi-protocol gateways, is the most plausible and future-proof structure. The results of the analysis have clearly shown that EV energy efficiency directly and quantitatively depends on the choice of communication protocol and the design of the gateway. CAN data reduction algorithms at the gateway level have a reduction of redundant network traffic of 3842 percent, SOME/IP-based HVAC management of 22 % energy savings in climate control, zonal Ethernet architectures of up to 30% reduction in wiring mass and resistive losses, and TSN-based deterministic data communications of sub-milliseconds actuation latency that is critical to regenerative, such quantitative results highlight the idea that communication network optimization is not just a systems engineering issue but a major driver towards lowering the range of EVs and decrease the overall cost of ownership. The findings in cybersecurity are also important. The expansion of Ethernet connectivity and SOME/IP services in EVs significantly increases the attack surface area relative to the traditional CAN-only design. Intrusion detection systems based on machine learning, especially CNN and attention-based GRU models, have detection rates of 98.799% in CAN and Ethernet space. SOME/IP and CAN cryptographic authentication algorithms show a sub-millisecond overhead, which proves that they are practical regarding the real-time implementation of EVs. The RF watermarking to authenticate the CAN and access control based on edge computing add even more security tools to the arsenal of automotive engineers. The interplay between TSN redundancy mechanisms and EV energy budgets in fault conditions is not quantified. The digital forensics frameworks that are specific to the EV energy system components, including BMS and powertrain controllers, must be developed. Lastly, systematic research is needed on how the proposed security mechanisms can be scaled to large populations of ECUs in next-generation software-defined vehicles. The creation of hardware-in-the-loop (HIL) testbeds that accurately simulate heterogeneous EV communication environments, and through which protocol verification can be carried out in realistic operating conditions. Implementation of AI-based adaptive gateway designs capable of dynamically optimizing protocol choices in response to real-time energy management requirements is an especially promising direction. With EVs developing to full software-defined vehicle architectures, where vehicles are programmable over the air, the communication structure justified in the current research gives a strict framework of assuring that the next generation EVs have achieved the trifecta of energy efficiency, functional safety, and cybersecurity resilience needed to be adopted by a mass-market.

REFERENCES:

1. J. Kim, S. Lee, and H. Park, "Performance Enhancement of CAN/Ethernet Automotive Gateway with a CAN Data Reduction Algorithm," Electronics, vol. 12, no. 13, p. 2777, Jun. 2023, doi: 10.3390/electronics12132777.
2. M. Iorio, M. Reineri, F. Risso, R. Sisto, and F. Valenza, "Securing SOME/IP for In-Vehicle Service Protection," IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 13450–13466, Nov. 2020, doi: 10.1109/TVT.2020.3028880.
3. M. Iorio, A. Buttiglieri, M. Reineri, F. Risso, R. Sisto, and F. Valenza, "Protecting In-Vehicle Services: Security-Enabled SOME/IP Middleware," IEEE Veh. Technol. Mag., vol. 15, no. 1, pp. 77–85, Mar. 2020, doi: 10.1109/MVT.2020.2980444.
4. X. Sun, F. R. Yu, and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6240–6259, Jul. 2022, doi: 10.1109/TITS.2021.3085297.
5. H. Luo, Z. Pan, J. Liu, and W. Xu, "A Survey on In-Vehicle Time-Sensitive Networking," IEEE Open J. Veh. Technol., vol. 4, pp. 278–298, 2023, doi: 10.1109/OJVT.2023.3262719.

6. J. Chen, X. Zhang, Y. Li, and W. Kong, "Recent Trends of In-Vehicle Time Sensitive Networking Technologies, Applications and Challenges," IEEE Access, vol. 11, pp. 50– 68, 2023, doi: 10.1109/ACCESS.2023.3272432.
7. L. Zhao, Y. Zhang, X. Tang, and Q. Li, "A Survey on Time-Sensitive Networking Standards and Applications for Intelligent Driving," Processes, vol. 11, no. 7, p. 2211, Jul. 2023, doi: 10.3390/pr11072211.
8. P. Vlachogiannis, C. Ampatzis, A. Korodi, and I. Silea, "Automotive IoT Ethernet-Based Communication Technologies Applied in a V2X Context via a Multi-Protocol Gateway," Sensors, vol. 22, no. 17, p. 6382, Aug. 2022, doi: 10.3390/s22176382.
9. W. Kong, M. Nabi, and K. Goossens, "reTSN: Resilient and Efficient Time-Sensitive Network for Automotive In-Vehicle Communication," IEEE Trans. Ind. Electron., vol. 70, no. 4, pp. 4131–4141, Apr. 2023, doi: 10.1109/TIE.2022.3181389.
10. D. Zuobin, K. Wenzhao, and Z. Yang, "Secure Time-Sensitive Software-Defined Networking in Vehicles," IEEE Commun. Mag., vol. 60, no. 5, pp. 44–50, May 2022, doi: 10.1109/MCOM.001.2100798.
11. Nagarjuna Reddy Aturi (2024) AI-Driven Analysis of Integrative Approach to Genetic Predispositions and Ayurvedic Treatments Related to Mental Health- IJFMR Volume 6, Issue 1, January-February 2024, doi:10.36948/ijfmr. 2024.v06i01.8541
12. E. Aliwa, O. Rana, and C. Perera, "Cyberattacks and Countermeasures for In-Vehicle Networks," ACM Comput. Surv., vol. 54, no. 1, pp. 1–37, 2021, doi: 10.1145/3431233.
13. N. Alkhatib, H. Ghauch, and J.-L. Danger, "SOME/IP Intrusion Detection Using Deep Learning-Based Sequential Models in Automotive Ethernet Networks," in Proc. IEEE 12th Annu. Inf. Technol. Electron. Mobile Commun. Conf. (IEMCON), Vancouver, BC, Canada, Oct. 2021, pp. 954–962, doi: 10.1109/IEMCON53756.2021.9623129.
14. Nagarjuna Reddy Aturi (2023) Integrative Yoga and Psychoneuroimmunology for Post-Surgery Recovery - A Complementary Therapy in Post-Surgical PTSD. Applied Medical Research. AMR-1068, doi: 10.47363/AMR/2023(10)250
15. B. Ma, S. Yang, and Z. Zuo, "An Authentication and Secure Communication Scheme for In-Vehicle Networks Based on SOME/IP," Sensors, vol. 22, no. 2, p. 647, Jan. 2022, doi: 10.3390/s22020647.
16. X. Liu, Q. Zhao, and H. Wang, "Security Analysis and Improvement of Vehicle Ethernet SOME/IP Protocol," Sensors, vol. 22, no. 18, p. 6792, Sep. 2022, doi: 10.3390/s22186792.
17. H. Huang, J. He, C. Zhou, and Y. Liu, "A Perspective on Ethernet in Automotive Communications—Current Status and Future Trends," Appl. Sci., vol. 13, no. 3, p. 1278, Jan. 2023, doi: 10.3390/app13031278.
18. Venkatesh, P. H. J., Tarun, M., Kumar, G. S., Amda, S., & Swapna, Y. (2024). The experimental investigation of thermal conductivity of aluminum metal matrix composites. Materials Today: Proceedings, 115, 216-221.
19. M. Thangavel, D. Mohanraj, T. Girijaprasanna, S. Raju, C. Dhanamjayulu, and S. M. Muyeen, "A Comprehensive Review on Electric Vehicle: Battery Management System, Charging Station, Traction Motors," IEEE Access, vol. 11, pp. 20994–21019, 2023, doi: 10.1109/ACCESS.2023.3251916.
20. J. R. Javed, S. Ur Rehman, M. U. Khan, M. Alazab, and T. Reddy, "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU," IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1456–1466, Apr. 2021, doi: 10.1109/TNSE.2021.3059421.
21. J. Michaels et al., "CAN Bus Message Authentication via Co-Channel RF Watermark," IEEE Trans. Veh. Technol., vol. 71, no. 4, pp. 3670–3686, Apr. 2022, doi: 10.1109/TVT.2022.3149006.

22. D. Yu, R.-H. Hsu, J. Lee, and S. Lee, "EC-SVC: Secure CAN Bus In-Vehicle Communications with Fine-Grained Access Control Based on Edge Computing," IEEE Trans. Inf. Forensics Security, vol. 17, pp. 1388–1403, 2022, doi: 10.1109/TIFS.2022.3153793.
23. L. Galletti, F. Risso, R. Sisto, and M. Iorio, "Automotive Ethernet Architecture and Security: Challenges and Technologies," Int. J. Electr. Comput. Eng., vol. 13, no. 5, pp. 5209–5221, Oct. 2023, doi: 10.11591/ijece. v13i5.pp5209-5221.
24. K. Strandberg, N. Nowdehi, and T. Olovsson, "A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection," IEEE Trans. Intell. Veh., vol. 8, no. 2, pp. 1350–1367, Feb. 2023, doi: 10.1109/TIV.2022.3227534.
25. M. Macharia, G. Kihato, and L. Nderu, "A Review of Electric Vehicle Technology: Architectures, Battery Technology and Its Management System, Relevant Standards, Application of Artificial Intelligence, Cyber Security, and Interoperability Challenges," IET Electr. Syst. Transp., vol. 13, no. 2, p. e12083, Jun. 2023, doi: 10.1049/els2.12083.