**IAES Journal of Electrical and Electronics Engineering**
Vol. 6, No. 2, December 2019, pp. 23~27
ISSN: 2338-7432, DOI: 10.11591/jeee.v6i2.pp23-27 

# On-board diagnostics and electric vehicle safety: diagnostic architecture, battery monitoring, fault detection, and cybersecurity

**Tole Sutikno[1], Muladi[2], Tri Wahono[2]**
[1]Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

**Article Info**

***Article history:***

Received May 25, 2018
Revised Dec 29, 2018
Accepted Apr 21, 2019

***Keywords:***

Automotive cybersecurity
Battery management system
CAN bus
Electric vehicles
Fault diagnosis
On-board diagnostics
Vehicle safety

**ABSTRACT**

Electric vehicles (EVs) introduce safety requirements that extend beyond conventional engine diagnostics because their operation depends on high-voltage power electronics, traction batteries, battery-management systems, and networked electronic control units. On-board diagnostics (OBD) can provide a practical access point for retrieving diagnostic trouble codes and selected operating parameters, but its coverage of EV-specific subsystems varies across manufacturers and vehicle platforms. This review examines the relationship between OBD-based diagnostics and electric-vehicle safety, focusing on diagnostic architecture, battery monitoring, fault detection, high-voltage hazards, thermal runaway, and cybersecurity. Literature published no later than 2018 is considered, including research on battery-management systems, state estimation, thermal protection, automotive network vulnerabilities, and OBD-assisted CAN analysis. The review distinguishes diagnostic visibility from active safety protection: an OBD interface may expose evidence of a fault, whereas safe operation depends on validated sensing, supervisory control, isolation devices, and protective responses within the vehicle. The literature shows that battery state estimation and fault diagnosis can support early identification of abnormal conditions, while insecure diagnostic access may create an attack path to in-vehicle networks. Effective EV safety therefore requires coordinated electrical, thermal, functional, and cybersecurity engineering.

*This is an open access article under the CC BY-SA license.*

## 1. INTRODUCTION

The transition from internal combustion engine vehicles to electric vehicles (EVs) has changed the technical requirements of automotive monitoring and safety. EVs depend on high-voltage traction batteries, electric motors, power converters, charging systems, and electronic control units that continuously exchange operational information. These components create new diagnostic requirements because faults may affect electrical, thermal, mechanical, and electronic subsystems simultaneously. On-board diagnostics (OBD) can support vehicle condition monitoring by providing access to diagnostic information, but its capabilities must be understood in relation to the architecture of an electric powertrain [1]–[4].

A major research problem is that conventional OBD concepts were developed primarily around vehicle emissions and powertrain monitoring, whereas EV safety involves additional high-voltage and battery-related hazards. An OBD interface may provide diagnostic trouble codes and selected operating parameters, but the availability of battery voltage, temperature, state of charge, and other manufacturer-specific parameters is not identical across vehicles. Furthermore, access to diagnostic data does not automatically mean that an external diagnostic device can control or protect the battery system. This review examines how OBD-related diagnostics can contribute to EV safety, with emphasis on battery monitoring, fault detection, high-voltage protection, thermal safety, and cybersecurity.

## 2. OBD ARCHITECTURE AND ITS ROLE IN ELECTRIC VEHICLES

### 2.1. Diagnostic interface and vehicle communication

OBD provides a standardized approach for accessing selected diagnostic information from vehicle electronic systems. In conventional vehicles, this information commonly includes diagnostic trouble codes and parameters associated with engine and emission-control performance. Modern vehicles use electronic control units connected through communication networks, particularly the Controller Area Network (CAN), to exchange sensor readings, control commands, and diagnostic messages. Research on automotive electronic networks has demonstrated that these communication systems are essential for vehicle operation but can also introduce security vulnerabilities [5], [6].

In an EV, diagnostic information may originate from the BMS, motor controller, inverter, onboard charger, thermal management controller, and other electronic modules. The diagnostic connector can provide access to some of this information, depending on the manufacturer's implementation and supported diagnostic services. However, standardized OBD parameters should not be assumed to expose every EV-specific measurement or internal battery-management function. Kang *et al.* [7] demonstrated that OBD-II access can be used to analyze and reverse-engineer CAN messages, illustrating both the diagnostic value and potential security implications of the interface.

### 2.2. OBD and battery management systems

The BMS is one of the most important electronic systems in an EV because it monitors and manages the traction battery. Its functions include measuring cell voltage, pack current, and temperature, estimating battery state of charge (SoC) and state of health (SoH), and controlling charging and discharging limits. It also supports cell balancing and protection against abnormal operating conditions. Research on EV battery management has identified accurate measurement, state estimation, fault diagnosis, and cell equalization as essential requirements for safe and reliable battery operation [1]–[4].

OBD can provide a useful external diagnostic view of selected BMS information without replacing the internal functions of the BMS. For example, diagnostic information may indicate abnormal battery temperature, voltage imbalance, insulation-related faults, or charging-system problems when the vehicle exposes the corresponding data. Nevertheless, the exact parameters and diagnostic codes depend on vehicle design and manufacturer-specific implementation. A robust diagnostic strategy should therefore distinguish standardized OBD information from enhanced diagnostic services and proprietary battery data [2], [3], [7].

## 3. BATTERY MONITORING AND FAULT DIAGNOSIS

### 3.1. State estimation and battery condition

Accurate battery state estimation is important because an EV depends on the battery's available energy and power to operate safely. SoC estimation indicates the remaining charge, while SoH estimation provides information about battery degradation and its ability to retain or deliver energy. Measurement uncertainty, temperature variation, aging, and changing load conditions can affect the accuracy of these estimates. Reviews by Hannan et al. and Xiong et al. discuss different estimation techniques and emphasize the importance of reliable battery-state information for EV operation [2]–[4].

Diagnostic systems can use battery measurements to identify abnormal conditions before they develop into serious failures. Voltage deviations between cells may indicate imbalance or degradation, while unusual temperature readings can suggest cooling problems or abnormal electrochemical activity. Current-sensor errors can also affect state estimation and lead to inappropriate battery-control decisions. Research on sensor fault detection in lithium-ion battery systems has demonstrated the importance of identifying and isolating voltage, current, and temperature measurement faults [8], [9].

### 3.2. Fault detection and diagnostic information

Fault detection involves identifying deviations from expected operating behavior, whereas fault diagnosis attempts to determine their possible causes. In EV battery systems, relevant faults include sensor failures, abnormal cell voltage, excessive temperature, internal short circuits, and battery degradation. Model-based methods compare measured behavior with predicted system responses, while data-driven methods identify abnormal patterns from collected operating data. Research on battery health monitoring and prognostics has shown that combining condition monitoring with fault analysis can improve the assessment of battery reliability and remaining useful life [9], [10].

OBD can help make some diagnostic results accessible to technicians and vehicle owners. Diagnostic trouble codes may identify a subsystem or fault category, while live data can provide additional context for troubleshooting. However, a diagnostic code does not always identify the physical root cause, and multiple faults can produce similar symptoms. Consequently, effective EV maintenance requires diagnostic

interpretation supported by manufacturer documentation, suitable test equipment, and validation of the suspected fault [1], [8], [10].

## 4. ELECTRICAL AND THERMAL SAFETY IN ELECTRIC VEHICLES

### 4.1. High-voltage electrical protection

High-voltage electrical systems introduce hazards that differ from those associated with conventional low-voltage vehicle electronics. Battery packs, inverters, motor drives, and charging circuits operate at voltages that can cause severe electric shock or electrical arcing if handled improperly. EV designs therefore require insulation monitoring, contactors, protective interlocks, fuses, and controlled isolation procedures. Diagnostic information can help identify abnormal electrical conditions, but safe maintenance still requires appropriate isolation procedures and specialized equipment [1], [11].

The battery protection system must respond directly to dangerous electrical conditions rather than relying on an external diagnostic reader. For example, the BMS and associated control units may restrict charging or discharging when voltage or temperature exceeds defined operating limits. Contactors and other protection devices can disconnect the high-voltage battery from selected parts of the powertrain when necessary. These functions demonstrate why OBD should be treated as a monitoring and troubleshooting interface rather than the primary mechanism for electrical protection [1], [8], [11].

### 4.2. Thermal runaway and battery safety

Thermal runaway is a serious safety concern for lithium-ion batteries because internal heat generation can accelerate chemical reactions and cause further temperature increases. Mechanical damage, electrical abuse, and excessive temperature can initiate conditions that lead to cell failure and thermal propagation. Feng et al. reviewed the mechanisms associated with thermal runaway in EV lithium-ion batteries and emphasized the importance of understanding abuse conditions. Battery safety research also highlights the need for thermal management, early warning, and appropriate responses to abnormal battery behavior [12]–[14].

Thermal management systems regulate battery temperature and help maintain operating conditions that support performance and safety. Cooling strategies include air cooling, liquid cooling, and other thermal-control arrangements selected according to battery configuration and vehicle requirements. Temperature sensors and BMS algorithms are important because ineffective measurement or control may delay the identification of hazardous conditions. OBD-accessible temperature data can support troubleshooting, but the actual prevention of thermal runaway depends on internal sensing, control, thermal design, and protective mechanisms [12]–[15].

## 5. CYBERSECURITY AND DIAGNOSTIC ACCESS

### 5.1. Vulnerabilities in vehicle networks

The growing number of electronic control units and connected services has expanded the potential attack surface of modern vehicles. CAN was designed primarily for reliable communication and does not inherently provide strong message authentication or encryption. An attacker who gains access to an in-vehicle network may attempt to inject, modify, or disrupt messages exchanged between electronic modules. Experimental automotive security research has demonstrated that weaknesses in vehicle networks can affect safety-critical functions, making cybersecurity an essential part of vehicle safety engineering [5], [6], [16].

The OBD connector is particularly relevant because it provides physical access to diagnostic communication within the vehicle. Kang et al. demonstrated how OBD-II can support automated reverse engineering and analysis of CAN messages, showing that diagnostic access may also be misused. Other research has investigated intrusion detection through message patterns, communication timing, and electrical characteristics of CAN signals. These studies indicate that protecting EV diagnostic access requires attention to both the physical interface and the communication network behind it [7], [16]–[18].

### 5.2 Security measures and safety implications

A secure diagnostic architecture should limit access according to the user's authorization and the function being performed. Authentication, access control, secure gateways, and monitoring of unusual network traffic can reduce the risk of unauthorized diagnostic activity. Intrusion detection systems can identify abnormal CAN message patterns, although their effectiveness depends on detection accuracy and the ability to operate without disrupting normal vehicle communication. Research on deep-neural-network detection, distributed anomaly detection, and VoltageIDS has demonstrated different approaches to identifying suspicious activity in automotive networks [17]–[19].

Cybersecurity is directly related to physical safety because malicious manipulation of vehicle communication can affect control and monitoring functions. In EVs, this concern extends to battery-management messages, charging functions, and high-voltage supervisory systems. Security controls should therefore be designed together with functional safety measures rather than added after the vehicle architecture has been completed. Research on connected-vehicle cybersecurity further emphasizes that risk assessment must consider communication interfaces, external connectivity, and the potential consequences of compromised vehicle information [16], [20].

## 6. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

The reviewed literature reveals that OBD-based EV diagnostics face limitations in data accessibility, interoperability, and diagnostic interpretation. Different manufacturers may expose different battery parameters, diagnostic codes, and communication services, making universal diagnostic applications difficult to develop. Battery-state estimates also depend on sensor accuracy, operating conditions, and the quality of the estimation algorithms. Future diagnostic platforms should combine standardized data access with validated manufacturer-specific information while clearly distinguishing diagnostic indicators from safety-critical control functions [2]–[4], [7].

Another priority is the integration of battery fault diagnosis with cybersecurity monitoring and safety supervision. Diagnostic systems should be able to identify sensor faults, abnormal battery behavior, and suspicious communication without interfering with the vehicle's protective responses. Validation should include realistic operating conditions, communication faults, temperature variations, battery aging, and representative cyberattack scenarios. Research on battery safety testing and automotive intrusion detection provides a foundation for developing more comprehensive diagnostic and protection strategies [11], [14], [17]–[20].

## 7. CONCLUSION

OBD can contribute to electric-vehicle safety by providing access to diagnostic trouble codes and selected operating parameters from networked vehicle systems. Its value is particularly relevant when diagnostic information is interpreted alongside BMS measurements, battery-state estimation, and fault-detection methods. However, OBD does not replace high-voltage isolation, battery protection, thermal management, or internal safety supervision. EV safety therefore requires coordinated diagnostic, electrical, thermal, functional, and cybersecurity measures, supported by reliable measurements and validated protective responses.

## REFERENCES

[1] L. Lu, X. Han, J. Li, J. Hua, and M. Ouyang, "A review on the key issues for lithium-ion battery management in electric vehicles," *Journal of Power Sources*, vol. 226, pp. 272–288, 2013. doi: 10.1016/j.jpowsour.2012.10.060.

[2] M. A. Hannan, M. S. H. Lipu, A. Hussain, and A. Mohamed, "A review of lithium-ion battery state of charge estimation and management system in electric vehicle applications: Challenges and recommendations," *Renewable and Sustainable Energy Reviews*, vol. 78, pp. 834–854, 2017. doi: 10.1016/j.rser.2017.05.001.

[3] M. A. Hannan, M. S. H. Lipu, A. Hussain, and A. Mohamed, "State-of-the-art and energy management system of lithium-ion batteries in electric vehicle applications: Issues and recommendations," *IEEE Access*, vol. 6, pp. 19362–19378, 2018. doi: 10.1109/ACCESS.2018.2817655.

[4] R. Xiong, J. Cao, Q. Yu, H. He, and F. Sun, "Critical review on the battery state of charge estimation methods for electric vehicles," *IEEE Access*, vol. 6, pp. 1832–1843, 2018. doi: 10.1109/ACCESS.2017.2780258.

[5] K. Koscher *et al*., "Experimental security analysis of a modern automobile," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 447–462. doi: 10.1109/SP.2010.34.

[6] S. Checkoway *et al*., "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Security Symposium*, 2011.

[7] T. U. Kang, H. M. Song, S. Jeong, and H. K. Kim, "Automated reverse engineering and attack for CAN using OBD-II," in *Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, pp. 1–7. doi: 10.1109/VTCFall.2018.8690781.

[8] Y. Liu and H. He, "Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended Kalman filter," *Applied Energy*, vol. 185, pp. 2033–2044, 2017. doi: 10.1016/j.apenergy.2016.02.071.

[9] M. A. Rahman, M. S. H. Lipu, M. A. Hannan, and A. Hussain, "Review and recent advances in battery health monitoring and prognostics technologies for electric vehicle (EV) safety and mobility," *Journal of Power Sources*, vol. 256, pp. 110–124, 2014. doi: 10.1016/j.jpowsour.2014.01.085.

[10] S. Abada, G. Marlair, A. Lecocq, M. Petit, V. Sauvant-Moynot, and F. Huet, "Safety focused modeling of lithium-ion batteries: A review," *Journal of Power Sources*, vol. 306, pp. 178–192, 2016. doi: 10.1016/j.jpowsour.2015.11.100.

[11] V. Ruiz, A. Pfrang, A. Kriston, N. Omar, P. Van den Bossche, and L. Boon-Brett, "A review of international abuse testing standards and regulations for lithium ion batteries in electric and hybrid electric vehicles," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 1427–1452, 2018. doi: 10.1016/j.rser.2017.05.195.

[12] X. Feng, M. Ouyang, X. Liu, L. Lu, Y. Xia, and X. He, "Thermal runaway mechanism of lithium ion battery for electric vehicles: A review," *Energy Storage Materials*, vol. 10, pp. 246–267, 2018. doi: 10.1016/j.ensm.2017.05.013.
[13] Q. Wang, B. Jiang, B. Li, and Y. Yan, "A critical review of thermal management models and solutions of lithium-ion batteries for the development of pure electric vehicles," *Renewable and Sustainable Energy Reviews*, vol. 64, pp. 106–128, 2016. doi: 10.1016/j.rser.2016.05.033.
[14] Y. Wang, Q. Gao, G. Wang, P. Lu, M. Zhao, and W. Bao, "A review on research status and key technologies of battery thermal management and its enhanced safety," *International Journal of Energy Research*, vol. 42, no. 13, pp. 4008–4033, 2018. doi: 10.1002/er.4158.
[15] S. Arora "Selection of thermal management system for modular battery packs of electric vehicles: A review of existing and emerging technologies," *Journal of Power Sources*, vol. 400, pp. 621–640, 2018. doi: 10.1016/j.jpowsour.2018.08.020.
[16] A. Stevens, M. Emre, and P. Vermaat, "Cybersecurity in the connected-vehicle environment," *Engineering & Technology Reference*, 2016. doi: 10.1049/etr.2016.0003.
[17] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLOS ONE*, vol. 11, no. 6, Art. no. e0155781, 2016. doi: 10.1371/journal.pone.0155781.
[18] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, "A distributed anomaly detection system for in-vehicle network using HTM," *IEEE Access*, vol. 6, pp. 9091–9098, 2018. doi: 10.1109/ACCESS.2018.2799210.
[19] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2114–2129, 2018. doi: 10.1109/TIFS.2018.2812149.
[20] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in *Proceedings of the 2017 IEEE Intelligent Vehicles Symposium*, 2017, pp. 1577–1583. doi: 10.1109/IVS.2017.7995934.