From Concept to Road: Building an Electric Van with Embedded Telemetry and Diagnostics for System Resilience and Cybersecurity

Benjamin Villa
College of Engineering
Cal Poly Pomona
Pomona, United States
bbvilla@cpp.edu

Valerio Formicola
College of Engineering
Cal Poly Pomona
Pomona, United States
vformicola@cpp.edu

***Abstract*— The increasing complexity of electronics in electric vehicles (EVs) demands improved resilience against failures and cyberattacks. This work presents the ground-up design of an open-source electric van featuring embedded telemetry and diagnostic systems for resilience and cybersecurity. The system is designed to integrate onboard intelligence to detect and analyze anomalous conditions in power, electronics, and communications, enabling early identification of failures or malicious alterations by hackers. By monitoring operational signals in real-time, the approach enhances fault tolerance and anticipates safety-critical conditions. Embodying a security-by-design strategy, our preliminary results include a smart fuse board and an optical control board. Our strategy is unique as intelligence is created on a custom electric van developed from concept to road, hence allowing us to tune and train the best architecture and intelligence with fast iterations.**

Keywords—Electric vehicles, machine learning, cybersecurity, AI predictability

I. Introduction

With the increase in complexity in electronics for electric vehicles (EV), resilience of hardware and software must be improved against natural or maliciously induced failures (cyberattacks). The problem is even more critical with introduction of upgraded intelligence onboard and within automotive electronics, de facto introducing more attack entrance points for hackers with risks for safety and operational functionalities of EVs (accounting, billing, compliance). In this work with propose the design and development of onboard intelligence to detect and diagnose anomalous conditions in system operation, especially in the power and electronics functionalities. Our strategy shortens the time for anticipating failures induced by cyberattacks or from targeted alteration to onboard electronics and communications, hence significantly increasing the safety of vehicle. With our approach, we aim at recognizing changes in operational behavior over time from signals and electronics, rather than a per session or periodic review basis (offline or post-mortem). Our approach anticipates safety critical situations and proactively defend against escalation of problems within system components, such as propagation from the infotainment system and from peripheral sensors to the critical ECUs and high priority controllers on the vehicle. Our approach is even more unique because we build an open source electric van with security-by-design strategy: We design system electronics with fault tolerance and diagnosis capabilities and test analytical and protective countermeasures in operation.

Challenges in this project include determining processing algorithms able to analyze deterministically multiple variables from the volume of data obtained from the vehicle. The designed instrumentation and measurement points enable fault tolerance strategies for abnormal circumstances, especially concerning the mechanical stability, power consumption and distribution, metering system, sensors and actuators.

II. Smart Van Design

The work is based on the integration of enhanced intelligence on top of high priority functionalities required for the safe operation of the electric van. As such, the boards we design comprise a number of gateways and connectivity elements to interface with automated intelligence, humans and closed loop controls (Figure 1).

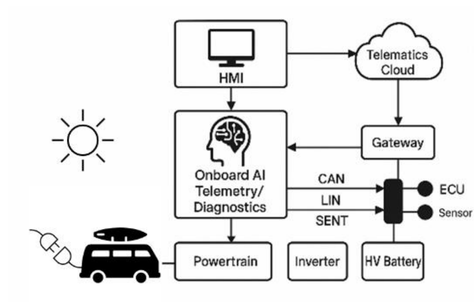

Figure 1 - Smart electric van connectivity for enhanced intelligence

III. Methods and Materials

A. Methods

Delving into the electronics of a vehicle is typically challenging due to proprietary electronics designs and communication specifications. As a matter of fact, experimental studies follow a reverse engineering approach. In order to create an environment where systems can easily be tracked and debugged, we had the unique opportunity to create an entire vehicle from the ground up (Figure 2). Using industry standards for communication (CAN, LIN, SENT) and best-practices for hardware design, we developed boards to provide a simple and clear testing ground for designing against malicious alteration of onboard software and cyberattacks from surrounding space.

Figure 2 - Custom electric van and board integration.

B. Materials

There are many individual circuit boards in an electric vehicle. These boards must be tested for harsh operational conditions, further containing failure propagation to not impact other systems. Circuit boards installed in our vehicle include: Thermal sensor collection boards, optical sensor boards, battery management boards, dashboard control boards, infotainment boards, instrument cluster boards, power distribution boards, mood lighting control boards and TPMS boards.

IV. Development and Preliminary Experiments

A. Smart Fuse Board

A smart fuse board was created with several improvements of traditional fuse boards in mind. This fuse board has 16 independently controlled and fused power outputs with a max amperage of 30A per output. This fuse board also has onboard diagnostics and data collection for daylight sensing and temperature sensing. It is also capable of communicating with the rest of the vehicle in order to control the drive time ignition signal and any fused outputs that need to be set (Figure 3). A sample of signal collection from the CAN bus (Figure 4).

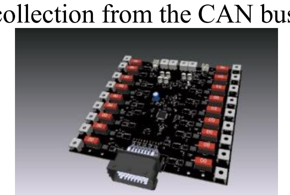

Figure 3 – Example of custom board: smart fuse board

What sets this fuse board apart is that it is capable of predicting the failure of a cars low voltage battery by monitoring the long term health of it (lead acid fault prediction) [2]. Such an approach is not well established in current EV industry in the close loop of onboard monitoring, especially if integrated with enhanced intelligence for cybersecurity and resilience. In our concept model, we integrated our custom board with the BQ34Z110 from Texas Instruments [3]. The BQ34Z110 board is a battery fuel gauge module designed to measure and report a battery pack's state of charge (SoC), state of health (SoH), voltage, and current. Further, the observation of electrical patterns can support evidence of alterations in the electrical drainage and anomalous patterns. Such an approach is very common in the cybersecurity monitoring of cyber-physical systems [2] [4].

B. Optical Control Board

This control board uses 12 optocouplers to sense digital switches such as door locks and switches. This board also contains 8 analog inputs for monitoring thermistors located on coolant lines and air intake systems. Lastly, this board is equipped with PWM drivers necessary to transmit and receive PWM signals that allow control of the coolant pumps throughout the vehicle. PWM signals are received from the pumps themselves that show the current speed of them, which is useful for predicting errors.

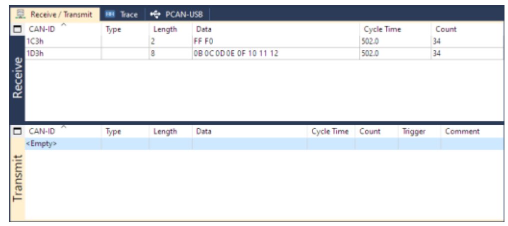

Figure 4 - Signal monitoring control board equipped for testing and monitoring on vehicle bus systems

C. Dashboard Control Board

The Dashboard Control Board contains a total of 32 inputs for supporting a large dash panel with many buttons. As industry moves towards touchscreen control of cars, the large majority of consumers prefer more robust and easier to identify buttons. This board also manages the routing and transceiving of audio signals to the car's speaker amplifier. This board sends status information to the rest of the vehicle, so that the appropriate dashboard buttons are handled adequately.

V. UPCOMING ACTIVITIES AND FUTURE WORK

As development of the vehicle continues, some future additions include: 360-degree camera vision, air suspension and pneumatics, an improved audio environment, and deployment of secondary devices (such as land and air drones). As for intelligence, we will develop closed loop algorithms in addition to smart capabilities to produce onboard cybersecurity and safety risk assessment.

References

[1] Y. Zhao, Y. Fan, H. Luo, W. Jiang and C. Li, "Vehicular Lead-Acid Battery Fault Prediction Method based on A-DeepFM," 2024 International Conference on New Trends in Computational Intelligence (NTCI), Qingdao, China, 2024, pp. 111-116, doi: 10.1109/NTCI64025.2024.10776118.

[2] V. Formicola, A. Di Pietro, A. Alsubaie, S. D'antonio, and J. Marti. "Assessing the impact of cyber attacks on wireless sensor nodes that monitor interdependent physical systems." In International Conference on Critical Infrastructure Protection, pp. 213-229. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[3] https://www.ti.com/product/BQ34Z110

[4] L. Romano, S. D'Antonio, V. Formicola, and L. Coppolino. "Protecting the wsn zones of a critical infrastructure via enhanced siem technology." In *International Conference on Computer Safety, Reliability, and Security*, pp. 222-234. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.