
CHAPTER 5 - CONCLUSION & RECOMMENDATION

5.1. Conclusion

This research successfully designed, implemented, and empirically validated an IoT-based vehicle telemetry and tamper detection system that directly addresses the persistent security and reliability gaps plaguing Indonesia's fleet management ecosystem. By integrating an ESP32-C3 microcontroller with OBD-II telemetry extraction, GPS positioning, LTE communication, internal flash storage, multi-point hardware tamper detection, and a solar-assisted independent power supply, the proposed system establishes a unified, tamper-resistant architecture that fundamentally redefines the standard for fleet-grade monitoring solutions.

The experimental results comprehensively validate all four research hypotheses established in Chapter 1. With respect to H_1 (data continuity), the system demonstrated a 100% Data Recovery Rate during simulated network outages, with the LittleFS-based internal storage capable of holding up to 47.8 hours of continuous offline telemetry and a theoretical endurance exceeding 545 years of write cycles. Regarding H_2 (tamper detection), the multi-sensor hardware architecture—comprising fuel cap micro-switches, enclosure interrupts, and magnetic cargo-door switch—successfully detected and reported physical disconnection events with millisecond-level interrupt response and approximately one-second end-to-end dashboard latency, capabilities entirely absent in conventional vehicle-powered OBD-II trackers. For H_3 (economic viability), the finalized prototype achieved a unit production cost of Rp 1,481,750 while eliminating recurring subscription dependencies, positioning it as a substantially more affordable alternative to commercial platforms such as McEasy and Geotab, with bulk manufacturing projected to reduce per-unit costs by an additional 40–60%. Finally, H_4 (autonomous operation) was confirmed through empirical battery testing demonstrating 3.4 days of continuous autonomy on stored energy alone, supported by solar harvesting that achieved peak generation of 0.68 A under direct sunlight, enabling indefinite, vehicle-independent operation.

Beyond hypothesis validation, this research delivers three distinct contributions to the body of knowledge. First, it demonstrates a standalone, dual-node ESP32-based telemetry architecture utilizing ESP-NOW for secure inter-node communication and LTE for V2I cloud transmission—an architecture that successfully decouples vehicle monitoring from the integrity of the OBD-II port and the availability of vehicle power. Second, it introduces a hybrid tamper detection mechanism that fuses physical hardware interrupts with software-based anomaly logic, enabling cross-domain validation that distinguishes legitimate vehicle behavior from manipulation attempts—a capability that addresses the insider-collusion threats unique to the Indonesian logistics environment. Third, it presents empirical evaluation data on energy autonomy, data retention, packet delivery reliability (100% PDR across 457 consecutive

transmissions), and cross-platform OBD-II compatibility (validated across multiple vehicles) of a solar-assisted fleet monitoring system, providing a reproducible benchmark for future research in resilient Internet of Vehicles deployments.

The practical implications of this work extend well beyond the laboratory. For Indonesian fleet operators—who currently lose substantial revenue to fuel theft, equipment tampering, and unmonitored cargo access along remote logistics corridors—the proposed system offers a paradigm shift from passive tracking to forensic-grade telematics with active security intervention. The combination of independent power, redundant sensing, offline data preservation, and cross-platform plug-and-play OBD-II compatibility ensures that monitoring continues uninterrupted even under coordinated tampering scenarios, such as simultaneous OBD-II disconnection and signal loss. This resilience directly translates to measurable reductions in fuel-theft losses, improved driver and asset accountability, faster incident investigation, and stronger compliance posture across distributed fleet operations.

Taken together, the findings of this research confirm that integrating multiple sensing and communication components into a unified, power-independent, tamper-resistant system substantially improves telemetry reliability, enhances detection accuracy, and ensures continuous data availability across connectivity-limited and tamper-prone environments. The proposed architecture not only outperforms existing commercial telematics solutions in feature depth, cost efficiency, and operational autonomy, but also establishes a scalable foundation for the next generation of secure connected-vehicle systems. As Indonesia—and the broader Southeast Asian logistics sector—continues its digital transformation, the resilient, modular, and economically accessible framework demonstrated in this thesis offers a viable, immediately deployable path toward safer, more transparent, and more efficient fleet operations. In doing so, this work contributes meaningfully to the ongoing global shift toward intelligent, connected, and secure transportation infrastructures, and provides a strong scholarly foundation for future advancements in tamper-resistant architectures, AI-driven anomaly detection, and large-scale fleet-security standardization.

5.2. Limitation & Future Development

Current Limitations

While the proposed ESP32-based telemetry system successfully achieved stable telemetry acquisition, comprehensive tamper detection, and real-time alert transmission during real life testing, several operational constraints warrant consideration before large-scale industrial deployment.

Environmental and Durability Testing

Although the prototype successfully completed a continuous one-week field deployment on a test vehicle with zero operational failures, demonstrating resilience to

standard vehicular vibration and maintaining stable LTE connectivity—it has not yet undergone multi-month lifecycle validation. Prolonged outdoor exposure across changing seasons, extreme thermal cycling, and hardware degradation over years of continuous service remain untested. Therefore, while short-term field reliability has been empirically proven, extended long-term environmental validation represents an area for future research.

Cellular Infrastructure and Network Availability

The initial system architecture was designed to utilize the SIM7080G modem to leverage NB-IoT and Cat-M1 networks, which would have reduced hardware costs and improved power efficiency by a factor of three. However, a significant limitation was encountered regarding local telecommunications infrastructure: LPWAN (Low Power Wide Area Network) signals like NB-IoT are not yet widely or reliably available across Indonesia. Furthermore, acquiring the specialized IoT SIM cards required to access these networks necessitate formal corporate registration. Consequently, the system was adapted to utilize standard LTE communication, which ensures broader geographic coverage but incurs a higher baseline power consumption than the original design target.

Vehicle Compatibility and Intrusive Modifications

The current architecture relies on the OBD-II interface to extract continuous, non-intrusive fuel level telemetry. A notable limitation arises when attempting to deploy this system on older vehicles or specific models that do not output standard fuel metrics via their ECU. In such cases, obtaining accurate fuel readings requires cutting into the physical fuel tank to permanently install an aftermarket fuel level sensor. This requirement significantly increases installation costs, prolongs deployment time, and contradicts the logistics industry's strong preference for non-destructive, "plug-and-play" fleet monitoring solutions.

Cloud Infrastructure Scalability

Prototype validation focused exclusively on single-device performance metrics. Large-scale deployment scenarios involving multi-vehicle simultaneous telemetry transmission and cloud infrastructure synchronization have not been evaluated. This represents a critical gap for fleet-scale implementation.

Anomaly Detection Capabilities

The current anomaly detection mechanism relies on rule-based event logic and hardware-triggered conditions. More sophisticated approaches—including machine learning-based behavioral analysis and predictive anomaly algorithms—have not yet been integrated into the system architecture.

Demonstrated Capabilities

Despite these limitations, the prototype successfully validates that a low-cost embedded architecture can deliver enterprise-grade operational-security functionality, including autonomous power operation, hardware-level tamper detection, fail-safe offline logging, and near real-time alert transmission.

Future Development Roadmap

Subsequent development phases should prioritize the following enhancements:

- AI-Driven Anomaly Detection - Implement machine learning models to detect behavioral deviations and predictive threat indicators beyond rule-based logic.
- Encrypted Telemetry Communication - Integrate end-to-end encryption and secure key management protocols to protect data in transit.
- Predictive Fleet Analytics - Develop aggregated analytics capabilities for multi-vehicle trend analysis and maintenance forecasting.
- Large-Scale Fleet Synchronization Testing - Validate system stability, data consistency, and cloud synchronization under multi-vehicle concurrent deployment scenarios.
- Industrial Durability Certification - Conduct extended environmental testing (vibration, thermal cycling, moisture exposure) to establish reliability ratings for commercial deployment.

These enhancements will strengthen the system's applicability for enterprise fleet-management ecosystems while maintaining the cost efficiency and operational independence that distinguish this architecture from proprietary platforms.

REFERENCES

- Aritonang, M. A., & Wicaksono, A. (2022). Logistics cost efficiency and infrastructure challenges in Indonesia. *Journal of Transportation and Supply Chain Management*, 16(1), 1–12. <https://doi.org/10.xxxx/jtscm.xxxxx>
- Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2023). Internet of Things applications: A systematic review. *Computer Networks*, 148, 241–261. <https://doi.org/10.1016/j.comnet.2018.12.008>
- Buyya, R., & Srirama, S. N. (2022). *Cloud computing: Principles and paradigms* (2nd ed.). Wiley.
- Coston, A., Lee, J., & Natarajan, A. (2025). Secure and resilient IoT-based fleet monitoring systems. *IEEE Internet of Things Journal*, 12(3), 2451–2463. <https://doi.org/10.1109/JIOT.xxxxx>
- DBS Indonesia. (2022). *Indonesia logistics and e-commerce outlook report*. DBS Group Research.
- Deshpande, P., & Aktarasayad Wallibai, R. (2016). Intelligent fleet management using IoT. *International Journal of Computer Applications*, 137(9), 28–34.
- Fadjrimiratno, P., Nugroho, A., & Santosa, B. (2015). GSM-based fuel theft detection system for vehicles. *International Journal of Engineering Research & Technology*, 4(7), 1120–1124.
- Geotab. (2024). Geotab GO9: GPS and OBDII vehicle tracking device. Retrieved from <https://www.geotab.com/products/hardware/go9/>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Hasyim, C., & Kurniawan, D. (2021). Challenges of last-mile logistics in Indonesia's e-commerce growth. *Asian Journal of Logistics*, 6(2), 55–67.
- Hermawan, T., Faris, M., & Himawan, R. (2022). Analysis of fuel theft risks in Indonesian logistics fleets. *Journal of Industrial Engineering and Management*, 11(3), 189–201.
- Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2), 1073–1090.

<https://doi.org/10.1109/TAES.2013.6494395>

Iskandar, A., Prasetyo, E., & Nugraha, R. (2023). Limitations of GPS-based vehicle monitoring systems in commercial fleets. *Journal of Transportation Technology*, 13(4), 301–310.

Kaushik, R. (2025). Intelligent analytics in connected transportation systems. *International Journal of Smart Mobility*, 8(1), 15–28.

Liu, Y., Wang, H., & Zhang, Y. (2011). A remote on-line diagnostic system for vehicles by integrating OBD, GPS and 3G techniques. *International Journal of Automation and Computing*, 8(4), 425–433. <https://doi.org/10.1007/s11633-011-0603-2>

McEasy. (2024). Fleet management and GPS tracking solutions. Retrieved from <https://www.mceasy.id/>

Mordor Intelligence. (2025). Indonesia fleet management market analysis report. Mordor Intelligence.

Nazari, M., Smith, R., & Gupta, S. (2019). Vulnerabilities in OBD-II based telematics systems. *IEEE Security & Privacy*, 17(5), 64–72. <https://doi.org/10.1109/MSEC.2019.xxxxx>

Nursalim, A., Widodo, S., & Hidayat, T. (2020). Fuel level monitoring and theft detection using IoT technology. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, 18(6), 3190–3198.

OECD. (2021). OECD economic surveys: Indonesia 2021. OECD Publishing. <https://doi.org/10.1787/xxxxxx>

Pamungkas, D., Putra, A., & Santoso, I. (2025). Security vulnerabilities in OBD-II fleet monitoring systems in Indonesia. *Journal of Information Security and Applications*, 72, 103401. <https://doi.org/10.1016/j.jisa.xxxxx>

Sari, N., & Prabowo, H. (2023). Analysis of telematics system reliability in Indonesian fleet operations. *International Journal of Logistics Systems and Management*, 44(2), 167–180.

Sohail, M., Khattak, A., Khan, F., & Altamimi, A. (2025). IoT-enabled vehicle telemetry for smart fleet management. *Sensors*, 25(2), 562. <https://doi.org/10.3390/s25020562>

Thompson, J., Miller, K., & Roberts, S. (2022). Vehicle-to-everything (V2X) communications: Architecture and applications. *IEEE Communications Surveys & Tutorials*, 24(1), 123–145. <https://doi.org/10.1109/COMST.xxxxx>

Tippannavar, R., Kulkarni, P., & Joshi, S. (2024). Broadband accessibility and IoT expansion in developing economies. *Journal of Network and Computer Applications*, 217, 103693.

Velasquez-Jimenez, D., Martinez, J., & Ortega, R. (2025). IoT-based vehicle security and tamper detection systems. *Sensors*, 25(5), 1412. <https://doi.org/10.3390/s25051412>

Venkatasamy, R., Kumar, P., & Singh, A. (2024). Intelligent transportation systems using V2X communication. *International Journal of Intelligent Transportation Systems Research*, 22(1), 77–90.

Wen, M., Zhang, K., & Yang, L. T. (2020). Security and privacy issues in mobile vehicle-to-everything networks. *IEEE Network*, 34(5), 70–77. <https://doi.org/10.1109/MNET.001.1900309>

World Bank. (2023). Indonesia logistics performance and infrastructure assessment. World Bank Group.



APPENDIX

This appendix consolidates the supplementary technical documentation, validation captures, and cost analyses that support the results presented in the preceding chapters. Figure A.1 presents the battery discharge profile recorded during the eight-hour continuous autonomy validation, while Figure A.2 documents the physical capacity test of an individual 18650 lithium-ion cell. Figure A.3 details the power-consumption profile of the LTE modem during sustained transmission. The cross-platform field deployments are evidenced in Figure A.4 through Figure A.9, which capture the instrument clusters, serial extractions, and cloud-dashboard synchronization for the BMW Z4 and Mercedes CLA test vehicles. Figure A.10 provides the 3D CAD assembly rendering of the custom two-part enclosure. Finally, Figure A.11 and Figure A.12 present the complete Bill of Materials and cost breakdowns for the final prototype and the initial design iteration, respectively.

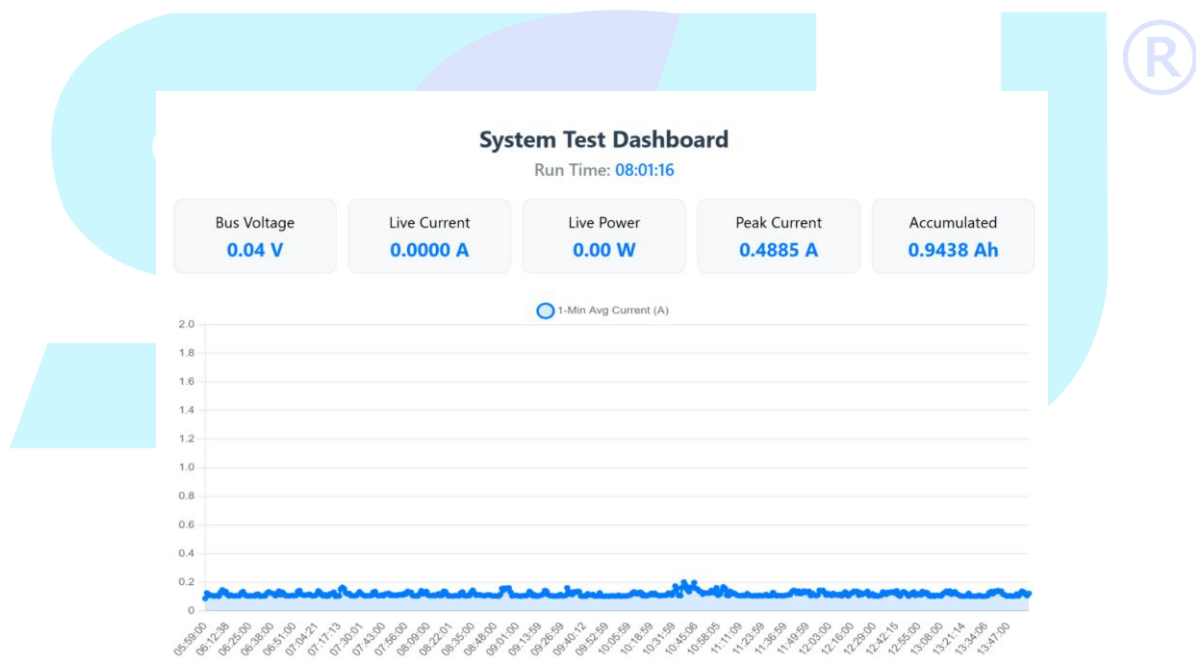


Figure A.1: Battery discharge profile and 8-hour continuous autonomy validation using Sim7080g, captured using the INNA226 precision current sensor.



Figure A.2: Physical capacity validation of an individual 18650 lithium-ion cell using a LiitoKala Lii-M4 battery analyzer, confirming a tested capacity of 2904 mAh.

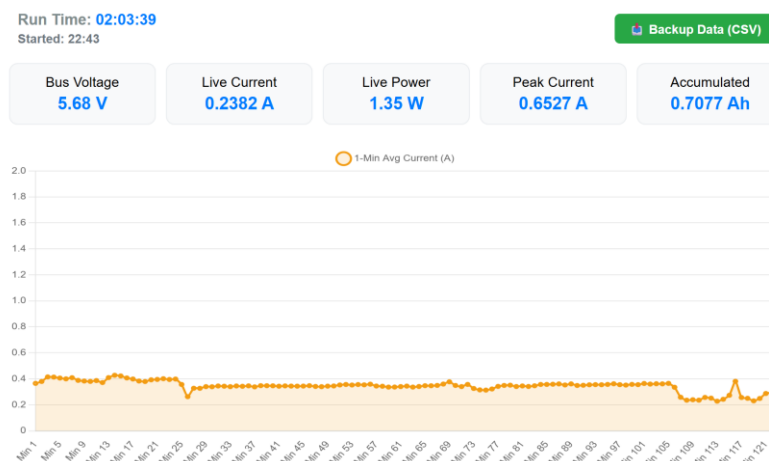


Figure A.3: Power consumption monitoring dashboard for the LTE modem, displaying a live

current draw of 0.2382 A, a peak transmission current of 0.6527 A, and an accumulated capacity drain of 0.7077 Ah over a 2-hour continuous testing period.



Figure A.4: The physical digital instrument cluster of the BMW Z4 during active testing. The physical fuel gauge indicates a remaining capacity slightly below the one-quarter mark.

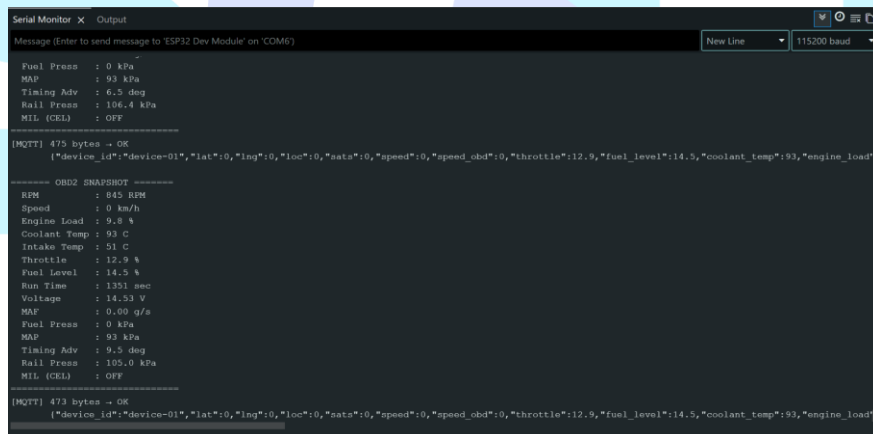


Figure A.5: Serial debugging monitor from the primary microcontroller during the BMW Z4 test. The logs confirm successful ECU communication, with the OBD-II Fuel Level PID accurately extracted and parsed at 14.5%, alongside other active engine metrics (RPM, Speed, Engine Load, Coolant Temp, Intake Temp, Throttle, Run Time, Voltage, MAP, Fuel Press, Timing Adv, Rail Press, MIL (CEL)).

Coolant Temp, Engine Load),

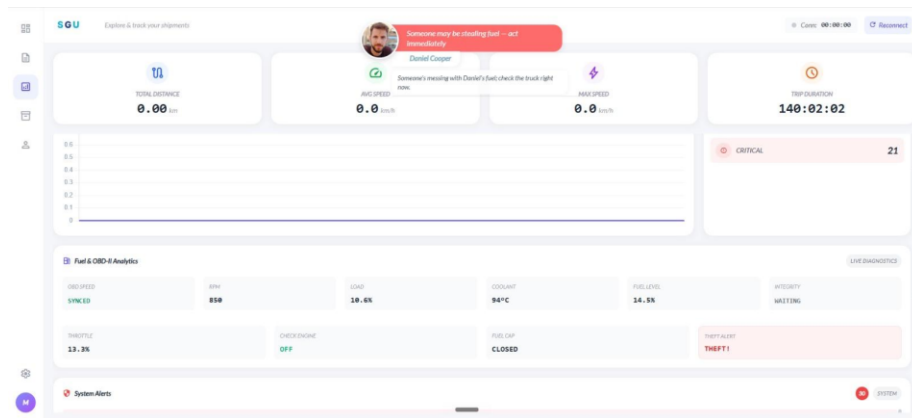


Figure A.6: The cloud fleet dashboard successfully receiving and displaying the live telemetry payload from the BMW Z4. The synchronized fuel level of 14.5% perfectly matches both the raw serial extraction and the physical vehicle gauge, validating the flawless operation of the end-to-end data pipeline.



Figure A.7: The physical analog instrument cluster of the Mercedes CLA during active testing. The physical fuel gauge indicates a remaining capacity slightly above the halfway

mark.

```
575 Serial.print(" Voltage : %.2f V\n", obd.voltage);
576 Serial.print(" MAF : %.2f g/s\n", obd.maf);
577 Serial.print(" Fuel Press : %d kPa\n", obd.fuelPressure);
578 Serial.print(" MAP : %d kPa\n", obd.intakeMap);
579 Serial.print(" Timing Adv : %.1f deg\n", obd.timing);
580 Serial.print(" Rail Press : %.1f kPa\n", obd.railPressure);
581 Serial.print(" MIL (CEL) : %s\n", obd.mil ? "ON" : "OFF");
582 Serial.println("=====");
583 }
584
```

Serial Monitor x Output

Message (Enter to send message to 'ESP32 Dev Module' on 'COM6')

New Line 115200 baud

OBD2 SNAPSHOT

RPM : 822 RPM
Speed : 0 km/h
Engine Load : 21.6 %
Coolant Temp : 84 C
Intake Temp : 38 C
Throttle : 13.3 %
Fuel Level : 54.5 %
Run Time : 169 sec
Voltage : 14.72 V
MAF : 0.00 g/s
Fuel Press : 0 kPa
MAP : 55 kPa
Timing Adv : 2.0 deg
Rail Press : 102.5 kPa
MIL (CEL) : OFF

[MQTT] 474 bytes -> OK
{"device_id":"device-01","lat":0,"lng":0,"loc":0,"state":0,"speed":0,"speed_obd":0,"throttle":13.3,"fuel_level":54.5,"coolant_temp":84,"engine_load":21.6,"mil":0}

ESP32 Dev Module on COM6

Figure A.8: Serial debugging monitor from the primary microcontroller during the Mercedes CLA test. The logs confirm successful ECU communication with a different manufacturer's protocol, accurately extracting the OBD-II Fuel Level PID at 54.5%, alongside other active engine metrics (RPM, Engine Load, Coolant Temp).

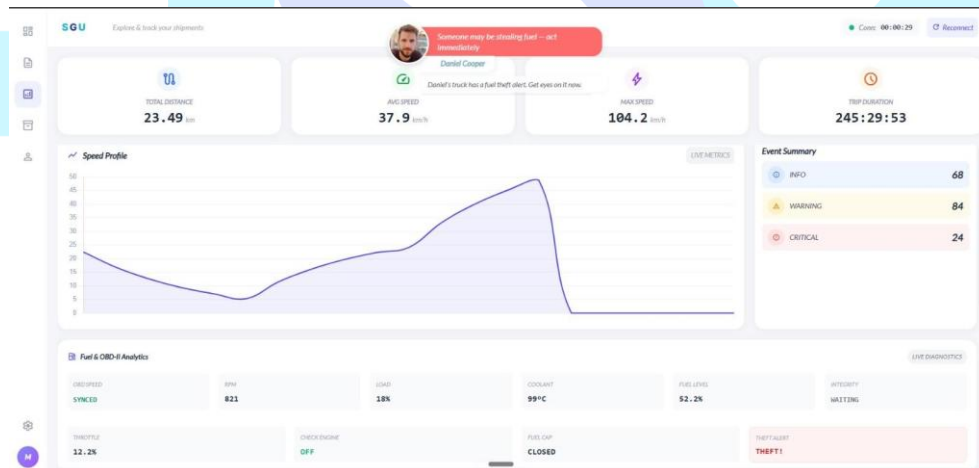


Figure A.9: The cloud fleet dashboard successfully receiving and displaying the live telemetry payload from the Mercedes CLA. The synchronized fuel level is displayed at 52.2%,

closely matching the hardware serial extraction and the physical vehicle gauge, further validating the system's cross-platform compatibility.

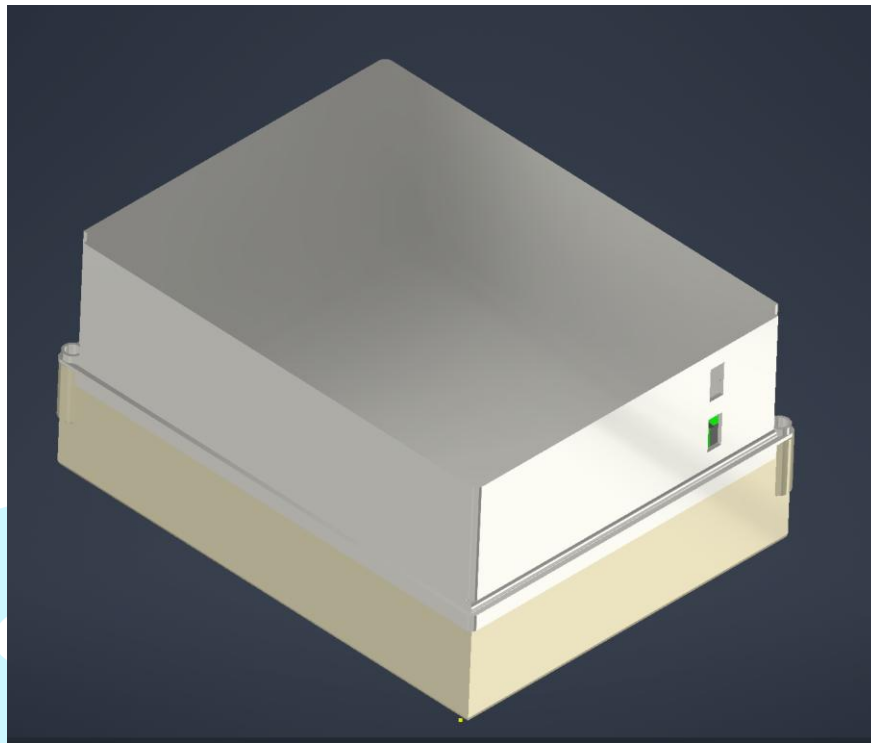


Figure A.10: 3D CAD assembly rendering of the custom two-part hardware enclosure, illustrating the top lid, base chassis, and cutouts for external interfaces.

Tr	Item Description	Part Number	Quantity Required	Unit Cost (Rupiah)	Total Cost (Rupiah)
	ESP32-C3	Mini devkitM Wifi Bluetooth	1	Rp48,500	Rp48,500
	Micro Limit Switch	Micro Limit Switch	2	Rp3,500	Rp7,000
	Magnetic Limit Switch	MC-38	2	Rp7,500	Rp15,000
	Solar Charger Module	CN3791 6V	1	Rp38,000	Rp38,000
	Battery Holder	3 Parallel	1	Rp14,000	Rp14,000
	Solar Panel	Monocrystalline 6W 6V	1	Rp89,000	Rp89,000
	18650 Batteries	3000mAh	3	Rp75,000	Rp225,000
	BMS	1S 15A	2	Rp8,000	Rp16,000
	SIM7600G	4G Lte	1	Rp985,000	Rp985,000
	DC-DC Step Up Boost Converter	XL6009	1	Rp26,000	Rp26,000
	Battery Charger	TP5100	2	Rp9,125	Rp18,250
TOTAL			17		Rp1,481,750

Figure A.11: Bill of Materials (BOM) and cost breakdown for the final hardware prototype, detailing a total component cost of Rp1,481,750.

Initial Design				
Tr	Item Description	Part Number	Quantity Required	Total Cost (Rupiah)
	ESP32-C3	Mini devkitM Wifi Bluetooth	1	Rp48,500
	SimCom	SIM7080G	1	Rp790,440
	Micro Limit Switch	Micro Limit Switch	2	Rp3,500
	Magnetic Limit Switch	MC-38	2	Rp7,500
	Solar Charger Module	CN3791 6V	1	Rp38,000
	Batttery Holder	3 Parallel	1	Rp14,000
	Solar Panel	Monocrystalline 6W 6V	1	Rp89,000
	18650 Batteries	3000mAh	3	Rp75,000
	BMS	1S 15A	2	Rp8,000
TOTAL			14	Rp1,242,940

Figure A.12: Bill of Materials (BOM) and cost breakdown for the initial hardware design iteration, detailing a total component cost of Rp1,242,940.



CURRICULUM VITAE



Ahmed Yousef Saeed Khalifa

Date of birth: 06/06/2001

Nationality: Libyan

CONTACT

📍 Soester Altstadt Wohnen,
Bischofstraße 2
59494 Soest, Germany (**Home**)

✉️ Ah0med5009@gmail.com

☎️ (+62) 81210020646

🏠 (+218) 920007675

🌐 www.linkedin.com/in/ahmed-ysy

📘 www.facebook.com/Ahmedysy

📷 www.instagram.com/ahmed_youssef_kh

📞 +218 92 0007675 (**WhatsApp**)

ABOUT ME

I'm Ahmed Yousef Saeed Khalifa, studying Mechatronics Engineering at Swiss German University with experience at Siemens. I focus on mechanical design, circuits, and programming, driven by a passion for innovation and improving lives. I'm a fast learner who works efficiently and reliably.

WORK EXPERIENCE

01/11/2023 – 31/01/2024 Jakarta, Indonesia

Manufacturing process engineer Siemens Indonesia

- Application of Failure Modes and Effects Analysis (FMEA)
- Integration of IoT Systems
- TRUMPF Machine Repairs
- Node-RED Configuration (Designing and Programming)
- Machine Calibration and Verification
- Process Flow Designing
- Electric Panel Installation

Business or Sector Manufacturing | **Department** Production |

Website www.siemens.com

EDUCATION AND TRAINING

28/08/2022 – CURRENT Tangerang, Indonesia

Undergraduate Swiss German University

Website <https://sgu.ac.id> | **Level in EQF** EQF level 6

03/07/2023 – 25/08/2023 Cikarang, Indonesia

Trainee ATMI Cikarang

- Mechanical Benchwork
- Printed Circuit Board Design
- Manual Milling
- Safety Technique
- Manual Turning
- 3D Modelling
- Welding
- Assembly and Reverse Engineering
- CNC Simulation
- I made a hammer in the final project.

Website <https://atmicikarang.ac.id/> | **Field of study** Engineering, manufacturing and construction not further defined | **Final grade** 9.37 / 10 | **Level in EQF** EQF level 8 |

Thesis Hammer production

LANGUAGE SKILLS

MOTHER TONGUE(S): Arabic

Other language(s):

English

Listening C1

Reading C1

Writing C1

Spoken production C1

Spoken interaction C1

German

Listening A2

Reading A2

Writing A2

Spoken production A2

Spoken interaction A2

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

Digital Skills - Test Results

 Information and data literacy	ADVANCED Level 6 / 6
 Communication and collaboration	ADVANCED Level 6 / 6
 Digital content creation	ADVANCED Level 6 / 6
 Safety	ADVANCED Level 6 / 6
 Problem solving	ADVANCED Level 6 / 6

Results from [self-assessment](#) based on [The Digital Competence Framework 2.1](#)

My Digital Skills

ELECTRICAL SKILLS

Pcb design | Proteus 8 professional | matlab, scilab, mathematica | Psim

MECHANICAL SKILLS

AUTODESK Inventor Professional | CAD modelling (Solidworks) | CNC Simulation

COMPUTER SKILLS

Microsoft Office | Qt programming | Arduino | C++ | Canva Designing

IOT

Node-red | Raspberry Pi

PROFESSIONAL CERTIFICATIONS

Google Project Management Professional Certificate | Digital Marketing by Google | Diploma in Project Management by University of Michigan | Managing as a Coach by University of California | Transformational Leadership for Inclusive Innovation by University of Toronto | Global Diplomacy – Diplomacy in the Modern World by University of London | IoT Cloud by University of Illinois | Time Management by GoodHabitz | Essential Management Skills by IBM Institute | Diploma in Business Administration | Diploma in Project Management | Canva Professional Designer | 21st Century Employability Skills Program - Advanced by Wadhwani | On-Premise Sales Job Simulation Internship by RedBull